信

xìn

https://scale.qihardware.org

2019 . Week 8 . Feb 24 - Mar 2

This page left intentionally blank
to power your imagination
of what interesting art, ads,
sponsorship, standard
frontmatter or blank space
should be included in
future editions of scale.

信 xìn

信 xìn is a Chinese character that means 'to trust/believe' and 'a message'. It is made of two components : *people* (人) and *word* (言)。

Wikipedia: Systemic Bias

Why does it matter?

Systemic Bias means that a full representation of the World's diversity is not reflected in Wikipedia's current projects. Less than 1/5th of the World's population has access to the Internet, meaning that large segments are not participating in the discussion.

RODLIBRARY
University of Northern Iowa

The "average Wikipedian" is:

- Male
- Technically inclined
- Formally educated
- English speaker
- Aged 15-49
- From a majority Christian country
- From a developed nation
- From the Northern Hemisphere
- Likely employed as white-collar worker or enrolled as a student

Underrepresentation of Wikipedians:

- Less than 15% of Wikipedians are women
- Minority demographic groups have less access to information technology, IT education:
  - African Americans and Latinos in US
  - Indigenous peoples in Canada
  - Aborigines of Australia
- Groups with statistically less access to internet
  - People of developing nations
  - Disabled
  - Elderly
- Lack of availability of sources

What can you do?

- Read about perspectives and issues of concern to others and attempt to represent them in your editing.
- Invite others to edit.
- Respect others.
- Avoid biased topics
- Read newspapers, magazines of other countries

Nick Rossman, Waterloo Public Library

Berkeley Open Infrastructure for Network Computing

From Wikipedia, the free encyclopedia

Main page
Contents
Featured content
Current events
Random article
Donate to Wikipedia
Wikipedia store

Interaction
Help
About Wikipedia
Community portal
Recent changes
Contact page

Tools
What links here
Related changes
Upload file
Special pages
Permanent link
Page information
Wikidata item
Cite this page

Print/export
Create a book
Download as PDF
Printable version

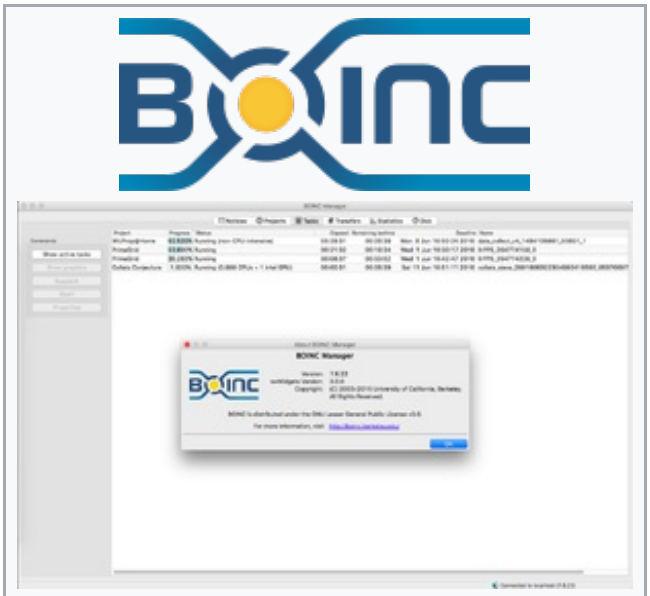
In other projects
Wikimedia Commons
Wikibooks

Languages
العربية
বাংলা
Беларуская (тарашкевіца)
Català
Čeština
Dansk
Deutsch
Español
Euskara

The **Berkeley Open Infrastructure for Network Computing** (**BOINC**, pronounced /bɔɪŋk/ – rhymes with "oink"[2]), an open-source middleware system, supports volunteer and grid computing.[3] Originally developed to support the SETI@home project, it became generalized as a platform for other distributed applications in areas as diverse as mathematics, linguistics, medicine, molecular biology, climatology, environmental science, and astrophysics, among others.[4] BOINC aims to enable researchers to tap into the enormous processing resources of multiple personal computers around the world.

BOINC development originated with a team based at the Space Sciences Laboratory (SSL) at the University of California, Berkeley and led by David Anderson, who also leads SETI@home. As a high-performance distributed computing platform, BOINC brings together about 311,742 active participants and 834,343 active computers (hosts) worldwide processing on average 26.431 PetaFLOPS as of 9 June 2018.[5] (it would be the fourth largest processing

BOINC



Developer(s)	University of California, Berkeley
Initial release	10 April 2002; 16 years ago
Stable release	7.14.2 Windows 11 October 2018; 4 months ago 7.14.2 macOS 11 October 2018; 4 months ago 7.2.42 Linux 28 February 2014; 5 years ago 7.4.53 Android 3 July 2016; 2 years ago
Preview release	7.4.22 Linux 17 September 2014; 4 years ago
Repository	github.com/BOINC/boinc
Written in	C++ (client/server) PHP (project CMS) Java (Android client)
Operating system	Windows macOS Linux Android
Type	Grid computing and volunteer computing

فارسی
Français
□□□
Hrvatski
Ido
Bahasa Indonesia
Italiano
עברית
Қазақша
Lietuvių
Magyar
മലയാളം
Nederlands
□□□
Polski
Português
Română
Русский
Simple English
Slovenčina
Српски / srpski
Suomi
Svenska
ไทย
Українська
Vèneto
Tiếng Việt
□□
□□
□□
Edit links

License	GNU Lesser General Public License[1] Project licensing varies
Website	boinc.berkeley.edu

capability in the world compared with an individual supercomputer Supercomputer TOP500 list) The National Science Foundation (NSF) funds BOINC through awards SCI/0221529,[6] SCI/0438443[7] and SCI/0721124.[8] *Guinness World Records* ranks BOINC as the largest computing grid in the world.[9]

BOINC code runs on various operating systems, including Microsoft Windows, macOS, Android,[10] Linux and FreeBSD.[11] BOINC is free software released under the terms of the GNU Lesser General Public License (LGPL).

Contents [hide]

History [edit]

BOINC was originally developed to manage the SETI@home project.

The original SETI client was a non-BOINC software exclusively for SETI@home. As one of the first volunteer grid computing projects, it was not designed with a high level of security. As a result, some participants in the project attempted to cheat the project to gain "credits," while some others submitted entirely falsified work. BOINC was designed, in part, to combat these security breaches.[12]

The BOINC project started in February 2002, and the first version was released on April 10, 2002. The first BOINC-based project was Predictor@home launched on June 9, 2004. In 2009, AQUA@home deployed multi-threaded CPU applications for the first time,[13] followed by the first OpenCL application in 2010.

As of 2 January 2018, 37 BOINC projects are active.[14]

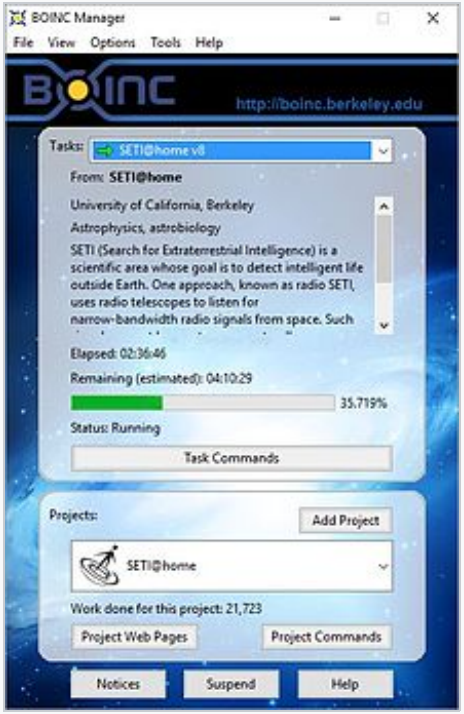
Design and structure [edit]

This article **needs additional citations for verification**. Please help improve this article by adding citations to reliable sources. Unsourced material may be challenged and removed.

Find sources: "Berkeley Open Infrastructure for Network Computing" – news · newspapers · books · scholar · JSTOR

(July 2014) (Learn how and when to remove this template

message)



The BOINC Manager working on the SETI@home project (v 7.6.22)

Main article: BOINC client–server technology


BOINC Manager icon

In essence, BOINC is software that can use the unused CPU and GPU cycles on a computer to do scientific computing—what one individual does not use of his/her computer, BOINC uses. In late 2008, BOINC's official website announced that Nvidia had developed a system called CUDA that uses GPUs for scientific computing. With NVIDIA's assistance, some BOINC-based projects (e.g., SETI@home, MilkyWay@home) now have applications that run on NVIDIA GPUs using CUDA. Beginning in October 2009, BOINC added support for the ATI/AMD family of GPUs also. These applications run from 2 to 10 times faster than the former CPU-only versions. In 7.x preview versions, GPU support (via OpenCL) was added for computers using Mac OS X with AMD Radeon graphic cards.

BOINC consists of a server system and client software that communicate with each other to distribute and process work units and return the results.

User interfaces [edit]

BOINC can be controlled remotely by remote procedure calls (RPC), from the command line, and from the BOINC Account Manager.

BOINC Manager currently has two "views": the *Advanced View* and the *Simplified GUI*. The *Grid View* was removed in the 6.6.x clients as it was redundant.

The appearance (skin) of the Simplified GUI is user-customizable, in that users can create their own designs.

Mobile Application [edit]

A BOINC app also exists for Android, allowing every person owning an Android device – smartphone, tablet and Kindle – to share their unused computing power. The user is allowed to select the research projects they want to support, if it is in the app's available project list.

By default, the application will allow computing only when the device is connected to a WiFi network, is being charged, and the battery has a charge of at least 90%.[15] Only some of the BOINC projects are available,[16] including Asteroids@home,

Collatz Conjecture, Einstein@home, Enigma@home, LHC@home, Moo! Wrapper, Quake Catcher Network, Rosetta@home, SETI@home, theSkyNet POGS, Universe@Home, World Community Grid and Yoyo@home.

Account managers [edit]

A BOINC Account Manager is an application that manages multiple BOINC project accounts across multiple computers (CPUs) and operating systems. Account managers were designed for people who are new to BOINC or have several computers participating in several projects. The account manager concept was conceived and developed jointly by GridRepublic and BOINC. Current account managers include:

- BAM! (BOINC Account Manager) (The first publicly available Account Manager, released for public use on May 30, 2006)
- GridRepublic (Follows the idea of keeping it simple and keep it neat when it comes to account management)
- Charity Engine (Non-profit account manager for hire, uses prize draws and continuous charity fundraising to motivate people to join the grid)
- Dazzler (Open-source Account Manager, to ease institutional management resources)

Credit system [edit]

Main article: BOINC Credit System

The BOINC Credit System is designed to avoid cheating by validating results before granting credit.

- A credit management system helps to ensure that users are returning results which are both scientifically and statistically accurate.
- Online distributed computing is almost entirely a volunteer endeavor. For this reason, projects are dependent on a complicated and variable mix of new users, long-term users, and retiring users.

Projects [edit]

There are about 35 projects currently listed,[14] of which about half yield published reports.[17] The licensing of the projects varies.

Gridcoin [edit]

Main article: Gridcoin

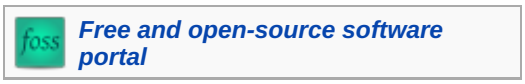
This section **needs expansion**. You can help by adding to it. *(August 2016)*

Since 2013, the cryptocurrency Gridcoin has been associated with BOINC as a remunerative coin.[18] Gridcoin uses a modified proof-of-stake timestamping system[19] called proof-of-research to reward participants for computational work completed on BOINC.[20][21] The proof-of-research system was implemented on October 11, 2014.[22] The system takes into account a parameter supplied with the limited number of white-listed projects called RAC (Recent Average Credit), and

distributes the coin according to the proportion of RAC acquired in the project to the people who are computing in it. Each whitelisted project gets the same amount of GRC to distribute among its contributors.

See also [edit]

- BOINC client–server technology
- BOSSA
- Citizen Cyberscience Centre
- Great Internet Mersenne Prime Search
- grid.org
- Gridcoin
- List of distributed computing projects
- distributed.net



References [edit]

1. ^ *BOINC is now distributed under the Lesser GPL*, BOINC, University of California, Berkeley, 2005-01-15, retrieved 2012-08-19
2. ^ Gonzalez, Laura Lynn, ed. (7 January 2007). "Rosetta@home". *YouTube*. Rosetta@home. Retrieved 26 August 2015.
3. ^ "Save the world using your PC or phone". *CNET*. Retrieved 2017-06-01.
4. ^ Scoles, Sarah. "A Brief History of SETI@Home". *The Atlantic*. Retrieved 2017-06-01.
5. ^ "BOINC". Boinc.berkeley.edu. Retrieved 2018-06-09.
6. ^ Research and Infrastructure Development for Public-Resource Scientific Computing, The National Science Foundation
7. ^ SCI: NMI Development for Public-Resource Computing and Storage, The National Science Foundation
8. ^ SDCI NMI Improvement: Middleware for Volunteer Computing, The National Science Foundation
9. ^ "Largest computing grid". *Guinness World Records*. Retrieved 2016-01-04.
10. ^ "Put your Android device to work on World Community Grid!". July 22, 2013.
11. ^ "Manual sites of FreeBSD system". January 2, 2015.
12. ^ Anderson, David P. "Public Computing: Reconnecting People to Science". Retrieved 2007-06-13.
13. ^ Kamran Karimi; Neil Dickson & Firas Hamze (2010). "High-Performance Physics Simulations Using Multi-Core CPUs and GPGPUs in a Volunteer Computing Context" (PDF). *International Journal of High Performance Computing Applications*. **25**: 61. arXiv:1004.0023 . doi:10.1177/1094342010372928.
14. ^ [a] [b] "Choosing BOINC projects". *BOINC*. Retrieved January 2, 2018.
15. ^ "Android FAQ". *BOINC*. UC Berkeley. 12 April 2018 . Retrieved 29 June 2018.
16. ^ "Projects". *BOINC*.
17. ^ *Publications by BOINC projects*, BOINC wiki, University of California, Berkeley, retrieved 2012-08-19
18. ^ Swan, Melanie (2015). *Blockchain: Blueprint for a New Economy* (1st ed.). O'Reilly Media.
19. ^ "Gridcoin Crowdfunds for PiGrid PnP Network Rewarding Scientific Research". *allcoinsnews.com*. Retrieved 10 April 2016.
20. ^ Wagner, Andrew. "Putting the Blockchain to Work For Science!". *Bitcoin*

Magazine. Retrieved 10 April 2016.

21. ^ Halford, Rob (2013-10-06). "GRIDCOIN – GRC (The environmentally conscious coin)". *cryptocointalk.com*. Retrieved 2014-11-14.
22. ^ "Proof-of-Research - Gridcoin". *wiki.gridcoin.us*. Retrieved 2018-01-02.

- Vance, Ashlee (2003-12-17). "Sun and UC Berkeley are about to BOINC". The Register. Retrieved 2006-11-13.

External links [edit]

- Official website
- BOINC developer Rom Walton's Blog
- The Big BOINC! Projects and Chronology Page written by BOINC User John Koulouris, (Esq.), and Web resources for BOINC participants from the Berkeley University Website.

Wikimedia Commons has media related to ***Berkeley Open Infrastructure for Network Computing***.

V · T · E	**Berkeley Open Infrastructure for Network Computing (BOINC) projects**
Current	Climateprediction.net · Cosmology@Home · Einstein@Home · GPUGRID.net · LHC@home · MilkyWay@home · Moo! Wrapper · PrimeGrid · Quake-Catcher Network · Rosetta@home · SETI@home (sub project Astropulse) · World Community Grid · Yoyo@home
Beta	Big and Ugly Rendering Project · Charity Engine · Ibercivis · MindModeling@Home · RNA world · SETI@home beta
Alpha	DENIS@Home · QMC@Home
Tools, technology	BOINC client–server technology · BOINC Credit System
Inactive, ended	ABC@Home · AQUA@home · Artificial Intelligence System · BBC Climate Change Experiment · Cell Computing · DistrRTgen · DNETC@HOME · Docking@Home · eOn · FreeHAL · HashClash · Ibercivis · The Lattice Project · Leiden Classical · µFluids@Home · Malaria Control Project · Orbit@home · POEM@Home · Predictor@home · Proteins@home · Reversi · Riesel Sieve (merged with PrimeGrid) · Seasonal Attribution Project · SIMAP · SLinCA@Home · Spinhenge@Home · SZTAKI Desktop Grid · TANPAKU · theSkyNet
Authority control	GND: 1025312678

Categories: Berkeley Open Infrastructure for Network Computing projects | Cross-platform free software | Free science software | Software that uses wxWidgets | Volunteer computing | Science software for MacOS | Science software for Windows | Science software for Linux | 2002 software | Free and open-source Android software

This page was last edited on 23 December 2018, at 22:51 (UTC).

Text is available under the Creative Commons Attribution-ShareAlike License; additional terms may apply. By using this site, you agree to the Terms of Use and Privacy Policy. Wikipedia® is a registered trademark of the Wikimedia Foundation, Inc., a non-profit organization.

Privacy policy About Wikipedia Disclaimers Contact Wikipedia Developers Cookie statement

Mobile view

ISACA® Glossary of Terms

English-Chinese Simplified

Third edition (2015)

ACKNOWLEDGMENTS

The ISACA® Glossary of Terms has been translated into Chinese Simplified (terms only) by a professional translation vendor and reviewed by volunteers. The verified and approved translation of this glossary will help reduce the time, cost, and inconsistencies of ISACA Chinese Simplified translations. All of the ISACA members who participated in the review of the three editions of the translated glossary deserve our thanks and gratitude.

Expert Translation Reviewers

Ms. Jean Chu Wang, CISA, CISM, Hong Kong, China
Mr. Michael Wai-Kee Yung, CISA, CISM, Hong Kong, China
Mr. Shek Fung, CISA, Hong Kong, China
Mr. Tong Diao, CISA, CISM, CRISC, Hong Kong, China
Mr. Yunfei Zhang, CISA, Hong Kong, China
Mr. Chengye Gu, CISA, CIA, CCSA, PMP, Bei Jing, China
Mr. Hui Zhang, CISA, ISO27001 LA, Bei Jing, China
Mr. Baohui Yang, CISA, PMP, Bei Jing, China
Mr. Jingdan Li, CISA, Bei Jing, China
Ms. Danna Yin, CISA, Shen Yang, China
Mr. Yang Tang, MCSE, Nan Jing, China
Mr. Ximing Wang, PMP, Chang Chun, China
Ms. Xiaomei Che, CISA, PMP, Shen Zhen, China
Mr. Qinghua Wang, CISA, Su Zhou, China
Ms. Jing Liu, CISA, PMP, Tai Yuan, China
Mr. Bin Cheng, CISA, Luo Yang, China
Ms. Xiaoguang Chai, CISA, CIA, Ji Nan, China
Mr. Xiaochen Wang, CISA, CIA, Ji Nan, China
Mr. Yuan Yan, CISA, Cheng Du, China
Ms. Yun Xiao, CISA, Cheng Du, China
Ms. Lipeng Yang, CISA, CIA, Kun Ming, China
Mr. Jie Meng, CISA, Kun Ming, China

FEEDBACK

Please contact the ISACA Translation Manager at asalzano@isaca.org for any comments or suggested changes.

ISACA®
Trust in, and value from, information systems

A

Abend An abnormal end to a computer job; termination of a task prior to its completion because of an error condition that cannot be resolved by recovery facilities while the task is executing
CHINESE SIMPLIFIED: 异常终止

Acceptable interruption window The maximum period of time that a system can be unavailable before compromising the achievement of the enterprise's business objectives
CHINESE SIMPLIFIED: 可接受的中断时限

Acceptable use policy A policy that establishes an agreement between users and the enterprise and defines for all parties' the ranges of use that are approved before gaining access to a network or the Internet
CHINESE SIMPLIFIED: 可接受使用策略

Access control The processes, rules and deployment mechanisms that control access to information systems, resources and physical access to premises
CHINESE SIMPLIFIED: 访问控制

Access control list (ACL) An internal computerized table of access rules regarding the levels of computer access permitted to logon IDs and computer terminals Scope Note: Also referred to as access control tables
CHINESE SIMPLIFIED: 访问控制列表（ACL）

Access control table An internal computerized table of access rules regarding the levels of computer access permitted to logon IDs and computer terminals
CHINESE SIMPLIFIED: 访问控制表

Access method The technique used for selecting records in a file, one at a time, for processing, retrieval or storage
The access method is related to, but distinct from, the file organization, which determines how the records are stored.
CHINESE SIMPLIFIED: 访问方法

Access path The logical route that an end user takes to access computerized information Scope Note: Typically includes a route through the operating system, telecommunications software, selected application software and the access control system
CHINESE SIMPLIFIED: 访问路径

Access rights The permission or privileges granted to users, programs or workstations to create, change, delete or view data and files within a system, as defined by rules established by data owners and the information security policy
CHINESE SIMPLIFIED: 访问权限

Access server Provides centralized access control for managing remote access dial-up services
CHINESE SIMPLIFIED: 访问服务器

Accountability The ability to map a given activity or event back to the responsible party
CHINESE SIMPLIFIED: 问责制

Accountability of governance Governance ensures that enterprise objectives are achieved by evaluating stakeholder needs, conditions and options; setting direction through prioritization and decision making; and monitoring performance, compliance and progress against plans. In most enterprises, governance is the responsibility of the board of directors under the leadership of the chairperson. Scope Note: COBIT 5 Perspective
CHINESE SIMPLIFIED: 治理责任

Accountable party The individual, group or entity that is ultimately responsible for a subject matter, process or scope Scope Note: Within the IT Assurance Framework (ITAF), the term "management" is equivalent to "accountable party."
CHINESE SIMPLIFIED: 责任方

Acknowledgment (ACK) A flag set in a packet to indicate to the sender that the previous packet sent was accepted correctly by the receiver without errors, or that the receiver is now ready to accept a transmission
CHINESE SIMPLIFIED: 确认（ACK）

Active recovery site (Mirrored) A recovery strategy that involves two active sites, each capable of taking over the other's workload in the event of a disaster Scope Note: Each site will have enough idle processing power to restore data from the other site and to accommodate the excess workload in the event of a disaster.
CHINESE SIMPLIFIED: 活动恢复站点（镜像）

Active response A response in which the system either automatically, or in concert with the user, blocks or otherwise affects the progress of a detected attack Scope Note: Takes one of three forms: amending the environment, collecting more information or striking back against the user
CHINESE SIMPLIFIED: 主动响应

Activity The main actions taken to operate the COBIT process
CHINESE SIMPLIFIED: 活动

Address Within computer storage, the code used to designate the location of a specific piece of data
CHINESE SIMPLIFIED: 地址

Address space The number of distinct locations that may be referred to with the machine address Scope Note: For most binary machines, it is equal to 2n, where n is the number of bits in the machine address.
CHINESE SIMPLIFIED: 地址空间

Addressing The method used to identify the location of a participant in a network Scope Note: Ideally, specifies where the participant is located rather than who they are (name) or how to get there (routing)
CHINESE SIMPLIFIED: 寻址

© 2015 ISACA All rights reserved.

Adjusting period The calendar can contain "real" accounting periods and/or adjusting accounting periods. The "real" accounting periods must not overlap and cannot have any gaps between them. Adjusting accounting periods can overlap with other accounting periods. Scope Note: For example, a period called DEC-93 can be defined that includes 01-DEC-1993 through 31-DEC-1993. An adjusting period called DEC31-93 can also be defined that includes only one day: 31-DEC-1993 through 31-DEC-1993.
CHINESE SIMPLIFIED: **调整期**

Administrative control The rules, procedures and practices dealing with operational effectiveness, efficiency and adherence to regulations and management policies
CHINESE SIMPLIFIED: **管理控制**

Advanced Encryption Standard (AES) A public algorithm that supports keys from 128 bits to 256 bits in size
CHINESE SIMPLIFIED: **高级加密标准**

Advanced persistent threat (APT) An adversary that possesses sophisticated levels of expertise and significant resources which allow it to create opportunities to achieve its objectives using multiple attack vectors (NIST SP800-61) Scope Note: The APT:
. pursues its objectives repeatedly over an extended period of time
. adapts to defenders' efforts to resist it
. is determined to maintain the level of interaction needed to execute its objectives
CHINESE SIMPLIFIED: **高级持续性威胁**

Adversary A threat agent
CHINESE SIMPLIFIED: **威胁方**

Adware A software package that automatically plays, displays or downloads advertising material to a computer after the software is installed on it or while the application is being used Scope Note: In most cases, this is done without any notification to the user or without the user's consent. The term adware may also refer to software that displays advertisements, whether or not it does so with the user's consent; such programs display advertisements as an alternative to shareware registration fees. These are classified as adware in the sense of advertising supported software, but not as spyware. Adware in this form does not operate surreptitiously or mislead the user, and it provides the user with a specific service.
CHINESE SIMPLIFIED: **广告软件**

Alert situation The point in an emergency procedure when the elapsed time passes a threshold and the interruption is not resolved. The enterprise entering into an alert situation initiates a series of escalation steps.
CHINESE SIMPLIFIED: **警报状态**

Alignment A state where the enablers of governance and management of enterprise IT support the goals and strategies of the enterprise Scope Note: COBIT 5 Perspective
CHINESE SIMPLIFIED: **调整**

Allocation entry A recurring journal entry used to allocate revenues or costs Scope Note: For example, an allocation entry could be defined to allocate costs to each department based on head count.
CHINESE SIMPLIFIED: **分配分录**

Alpha The use of alphabetic characters or an alphabetic character string
CHINESE SIMPLIFIED: **Alpha**

Alternate facilities Locations and infrastructures from which emergency or backup processes are executed, when the main premises are unavailable or destroyed Scope Note: Includes other buildings, offices or data processing centers
CHINESE SIMPLIFIED: **备用设施**

Alternate process Automatic or manual process designed and established to continue critical business processes from point-of-failure to return-to-normal
CHINESE SIMPLIFIED: **备用流程**

Alternative routing A service that allows the option of having an alternate route to complete a call when the marked destination is not available Scope Note: In signaling, alternative routing is the process of allocating substitute routes for a given signaling traffic stream in case of failure(s) affecting the normal signaling links or routes of that traffic stream.
CHINESE SIMPLIFIED: **替换路由**

American Standard Code for Information Interchange See ASCII
CHINESE SIMPLIFIED: **美国信息交换标准码**

Amortization The process of cost allocation that assigns the original cost of an intangible asset to the periods benefited; calculated in the same way as depreciation
CHINESE SIMPLIFIED: **摊销**

Analog A transmission signal that varies continuously in amplitude and time and is generated in wave formation Scope Note: Analog signals are used in telecommunications
CHINESE SIMPLIFIED: **模拟**

Analytical technique The examination of ratios, trends, and changes in balances and other values between periods to obtain a broad understanding of the enterprise's financial or operational position and to identify areas that may require further or closer investigation Scope Note: Often used when planning the assurance assignment
CHINESE SIMPLIFIED: **分析技术**

Anomaly Unusual or statistically rare
CHINESE SIMPLIFIED: **异常**

Anomaly detection Detection on the basis of whether the system activity matches that defined as abnormal
CHINESE SIMPLIFIED: **异常检测**

© 2015 ISACA All rights reserved.

Anonymity The quality or state of not being named or identified
CHINESE SIMPLIFIED: 匿名

Antivirus software An application software deployed at multiple points in an IT architecture. It is designed to detect and potentially eliminate virus code before damage is done and repair or quarantine files that have already been infected
CHINESE SIMPLIFIED: 防病毒软件

Appearance The act of giving the idea or impression of being or doing something
CHINESE SIMPLIFIED: 表象

Appearance of independence Behavior adequate to meet the situations occurring during audit work (interviews, meetings, reporting, etc.) Scope Note: An IS auditor should be aware that appearance of independence depends on the perceptions of others and can be influenced by improper actions or associations.
CHINESE SIMPLIFIED: 形式独立性

Applet A program written in a portable, platform-independent computer language, such as Java, JavaScript or Visual Basic Scope Note: An applet is usually embedded in an HyperText Markup Language (HTML) page downloaded from web servers and then executed by a browser on client machines to run any web-based application (e.g., generate web page input forms, run audio/video programs, etc.). Applets can only perform a restricted set of operations, thus preventing, or at least minimizing, the possible security compromise of the host computers. However, applets expose the user's machine to risk if not properly controlled by the browser, which should not allow an applet to access a machine's information without prior authorization of the user.
CHINESE SIMPLIFIED: 小程序

Application A computer program or set of programs that performs the processing of records for a specific function Scope Note: Contrasts with systems programs, such as an operating system or network control program, and with utility programs, such as copy or sort
CHINESE SIMPLIFIED: 应用程序

Application acquisition review An evaluation of an application system being acquired or evaluated, that considers such matters as: appropriate controls are designed into the system; the application will process information in a complete, accurate and reliable manner; the application will function as intended; the application will function in compliance with any applicable statutory provisions; the system is acquired in compliance with the established system acquisition process
CHINESE SIMPLIFIED: 应用程序采购审查

Application architecture Description of the logical grouping of capabilities that manage the objects necessary to process information and support the enterprise's objectives. Scope Note: COBIT 5 perspective
CHINESE SIMPLIFIED: 应用架构

Application benchmarking The process of establishing the effective design and operation of automated controls within an application
CHINESE SIMPLIFIED: 应用程序基准测试

Application controls The policies, procedures and activities designed to provide reasonable assurance that objectives relevant to a given automated solution (application) are achieved
CHINESE SIMPLIFIED: 应用控制

Application development review An evaluation of an application system under development that considers matters such as: appropriate controls are designed into the system; the application will process information in a complete, accurate and reliable manner; the application will function as intended; the application will function in compliance with any applicable statutory provisions; the system is developed in compliance with the established system development life cycle process
CHINESE SIMPLIFIED: 应用程序开发审查

Application implementation review An evaluation of any part of an implementation project Scope Note: Examples include project management, test plans and user acceptance testing (UAT) procedures.
CHINESE SIMPLIFIED: 应用程序实施审查

Application layer In the Open Systems Interconnection (OSI) communications model, the application layer provides services for an application program to ensure that effective communication with another application program in a network is possible. Scope Note: The application layer is not the application that is doing the communication; a service layer that provides these services.
CHINESE SIMPLIFIED: 应用层

Application maintenance review An evaluation of any part of a project to perform maintenance on an application system Scope Note: Examples include project management, test plans and user acceptance testing (UAT) procedures.
CHINESE SIMPLIFIED: 应用程序维护审查

Application or managed service provider (ASP/MSP) A third party that delivers and manages applications and computer services, including security services to multiple users via the Internet or a private network
CHINESE SIMPLIFIED: 应用服务供应商或管理服务供应商 (ASP/MSP)

Application program A program that processes business data through activities such as data entry, update or query Scope Note: Contrasts with systems programs, such as an operating system or network control program, and with utility programs such as copy or sort
CHINESE SIMPLIFIED: 应用程序

Application programming The act or function of developing and maintaining application programs in production
CHINESE SIMPLIFIED: 应用程序编程

© 2015 ISACA All rights reserved.

Application programming interface (API) A set of routines, protocols and tools referred to as "building blocks" used in business application software development Scope Note: A good API makes it easier to develop a program by providing all the building blocks related to functional characteristics of an operating system that applications need to specify, for example, when interfacing with the operating system (e.g., provided by Microsoft Windows, different versions of UNIX). A programmer utilizes these APIs in developing applications that can operate effectively and efficiently on the platform chosen.
CHINESE SIMPLIFIED: **应用程序编程接口 (API)**

Application proxy A service that connects programs running on internal networks to services on exterior networks by creating two connections, one from the requesting client and another to the destination service
CHINESE SIMPLIFIED: **应用代理**

Application security Refers to the security aspects supported by the application, primarily with regard to the roles or responsibilities and audit trails within the applications
CHINESE SIMPLIFIED: **应用安全**

Application service provider (ASP) Also known as managed service provider (MSP), it deploys, hosts and manages access to a packaged application to multiple parties from a centrally managed facility. Scope Note: The applications are delivered over networks on a subscription basis.
CHINESE SIMPLIFIED: **应用服务供应商**

Application software tracing and mapping Specialized tools that can be used to analyze the flow of data through the processing logic of the application software and document the logic, paths, control conditions and processing sequences Scope Note: Both the command language or job control statements and programming language can be analyzed. This technique includes program/system: mapping, tracing, snapshots, parallel simulations and code comparisons.
CHINESE SIMPLIFIED: **应用软件跟踪和映射**

Application system An integrated set of computer programs designed to serve a particular function that has specific input, processing and output activities Scope Note: Examples include general ledger, manufacturing resource planning and human resource (HR) management.
CHINESE SIMPLIFIED: **应用程序系统**

Architecture Description of the fundamental underlying design of the components of the business system, or of one element of the business system (e.g., technology), the relationships among them, and the manner in which they support enterprise objectives
CHINESE SIMPLIFIED: **架构**

Architecture board A group of stakeholders and experts who are accountable for guidance on enterprise-architecture-related matters and decisions, and for setting architectural policies and standards Scope Note: COBIT 5 perspective
CHINESE SIMPLIFIED: **架构委员会**

Arithmetic logic unit (ALU) The area of the central processing unit (CPU) that performs mathematical and analytical operations
CHINESE SIMPLIFIED: **算术逻辑单元 (ALU)**

Artificial intelligence Advanced computer systems that can simulate human capabilities, such as analysis, based on a predetermined set of rules
CHINESE SIMPLIFIED: **人工智能**

ASCII Representing 128 characters, the American Standard Code for Information Interchange (ASCII) code normally uses 7 bits. However, some variations of the ASCII code set allow 8 bits. This 8-bit ASCII code allows 256 characters to be represented.
CHINESE SIMPLIFIED: **美国信息交换标准码**

Assembler A program that takes as input a program written in assembly language and translates it into machine code or machine language
CHINESE SIMPLIFIED: **汇编程序**

Assembly Language A low-level computer programming language which uses symbolic code and produces machine instructions
CHINESE SIMPLIFIED: **汇编语言**

Assertion Any formal declaration or set of declarations about the subject matter made by management Scope Note: Assertions should usually be in writing and commonly contain a list of specific attributes about the subject matter or about a process involving the subject matter.
CHINESE SIMPLIFIED: **声明**

Assessment A broad review of the different aspects of a company or function that includes elements not covered by a structured assurance initiative Scope Note: May include opportunities for reducing the costs of poor quality, employee perceptions on quality aspects, proposals to senior management on policy, goals, etc.
CHINESE SIMPLIFIED: **评估**

Asset Something of either tangible or intangible value that is worth protecting, including people, information, infrastructure, finances and reputation
CHINESE SIMPLIFIED: **资产**

Assurance Pursuant to an accountable relationship between two or more parties, an IT audit and assurance professional is engaged to issue a written communication expressing a conclusion about the subject matters for which the accountable party is responsible. Assurance refers to a number of related activities designed to provide the reader or user of the report with a level of assurance or comfort over the subject matter. Scope Note: Assurance engagements could include support for audited financial statements, reviews of controls, compliance with required standards and practices, and compliance with agreements, licenses, legislation and regulation.
CHINESE SIMPLIFIED: **鉴证**

© 2015 ISACA All rights reserved.

Assurance engagement An objective examination of evidence for the purpose of providing an assessment on risk management, control or governance processes for the enterprise. Scope Note: Examples may include financial, performance, compliance and system security engagements
CHINESE SIMPLIFIED: 鉴证业务

Assurance initiative An objective examination of evidence for the purpose of providing an assessment on risk management, control or governance processes for the enterprise Scope Note: Examples may include financial, performance, compliance and system security engagements.
CHINESE SIMPLIFIED: 鉴证机制

Asymmetric key (public key) A cipher technique in which different cryptographic keys are used to encrypt and decrypt a message Scope Note: See Public key encryption.
CHINESE SIMPLIFIED: 非对称式密钥 (公开密钥)

Asynchronous Transfer Mode (ATM) A high-bandwidth low-delay switching and multiplexing technology that allows integration of real-time voice and video as well as data. It is a data link layer protocol. Scope Note: ATM is a protocol-independent transport mechanism. It allows high-speed data transfer rates at up to 155 Mbit/s.
The acronym ATM should not be confused with the alternate usage for ATM, which refers to an automated teller machine.
CHINESE SIMPLIFIED: 异步传输模式 (ATM)

Asynchronous transmission Character-at-a-time transmission
CHINESE SIMPLIFIED: 异步传输

Attack An actual occurrence of an adverse event
CHINESE SIMPLIFIED: 攻击

Attack mechanism A method used to deliver the exploit. Unless the attacker is personally performing the attack, an attack mechanism may involve a payload, or container, that delivers the exploit to the target.
CHINESE SIMPLIFIED: 攻击机制

Attack vector A path or route used by the adversary to gain access to the target (asset) Scope Note: There are two types of attack vectors: ingress and egress (also known as data exfiltration)
CHINESE SIMPLIFIED: 攻击路径

Attenuation Reduction of signal strength during transmission
CHINESE SIMPLIFIED: 衰减

Attest reporting engagement An engagement in which an IS auditor is engaged to either examine management's assertion regarding a particular subject matter or the subject matter directly Scope Note: The IS auditor's report consists of an opinion on one of the following: The subject matter. These reports relate directly to the subject matter itself rather than to an assertion. In certain situations management will not be able to make an assertion over the subject of the engagement. An example of this situation is when IT services are outsourced to third party. Management will not ordinarily be able to make an assertion over the controls that the third party is responsible for. Hence, an IS auditor would have to report directly on the subject matter rather than on an assertion.
CHINESE SIMPLIFIED: 基于责任方认定的鉴证业务

Attitude Way of thinking, behaving, feeling, etc.
CHINESE SIMPLIFIED: 态度

Attribute sampling Method to select a portion of a population based on the presence or absence of a certain characteristic
CHINESE SIMPLIFIED: 属性抽样

Audit Formal inspection and verification to check whether a standard or set of guidelines is being followed, records are accurate, or efficiency and effectiveness targets are being met Scope Note: May be carried out by internal or external groups
CHINESE SIMPLIFIED: 审计

Audit accountability Performance measurement of service delivery including cost, timeliness and quality against agreed service levels
CHINESE SIMPLIFIED: 审计问责

Audit authority A statement of the position within the enterprise, including lines of reporting and the rights of access
CHINESE SIMPLIFIED: 审计机构

Audit charter A document approved by those charged with governance that defines the purpose, authority and responsibility of the internal audit activity Scope Note: The charter should:
Establish the internal audit funtion's position within the enterprise
Authorise access to records, personnel and physical properties relevant to the performance of IS audit and assurance engagementsDefine the scope of audit function's activities
CHINESE SIMPLIFIED: 审计章程

Audit evidence The information used to support the audit opinion
CHINESE SIMPLIFIED: 审计证据

Audit expert systems Expert or decision support systems that can be used to assist IS auditors in the decision-making process by automating the knowledge of experts in the field Scope Note: This technique includes automated risk analysis, systems software and control objectives software packages.
CHINESE SIMPLIFIED: 审计专家系统

© 2015 ISACA All rights reserved.

Audit objective The specific goal(s) of an audit Scope Note: These often center on substantiating the existence of internal controls to minimize business risk.
CHINESE SIMPLIFIED: 审计目标

Audit plan 1. A plan containing the nature, timing and extent of audit procedures to be performed by engagement team members in order to obtain sufficient appropriate audit evidence to form an opinion Scope Note: Includes the areas to be audited, the type of work planned, the high-level objectives and scope of the work, and topics such as budget, resource allocation, schedule dates, type of report and its intended audience and other general aspects of the work 2. A high-level description of the audit work to be performed in a certain period of time
CHINESE SIMPLIFIED: 审计计划

Audit program A step-by-step set of audit procedures and instructions that should be performed to complete an audit
CHINESE SIMPLIFIED: 审计程序

Audit responsibility The roles, scope and objectives documented in the service level agreement (SLA) between management and audit
CHINESE SIMPLIFIED: 审计责任

Audit risk The risk of reaching an incorrect conclusion based upon audit findings Scope Note: The three components of audit risk are:
Control risk
Detection risk
Inherent risk
CHINESE SIMPLIFIED: 审计风险

Audit sampling The application of audit procedures to less than 100 percent of the items within a population to obtain audit evidence about a particular characteristic of the population
CHINESE SIMPLIFIED: 审计抽样

Audit subject matter risk Risk relevant to the area under review:
Business risk (customer capability to pay, credit worthiness, market factors, etc.)
Contract risk (liability, price, type, penalties, etc.)
Country risk (political, environment, security, etc.)
Project risk (resources, skill set, methodology, product stability, etc.)
Technology risk (solution, architecture, hardware and software infrastructure network, delivery channels, etc.)
Scope Note: See inherent risk
CHINESE SIMPLIFIED: 审计主体风险

Audit trail A visible trail of evidence enabling one to trace information contained in statements or reports back to the original input source
CHINESE SIMPLIFIED: 审计轨迹

Audit universe An inventory of audit areas that is compiled and maintained to identify areas for audit during the audit planning process Scope Note: Traditionally, the list includes all financial and key operational systems as well as other units that would be audited as part of the overall cycle of planned work. The audit universe serves as the source from which the annual audit schedule is prepared. The universe will be periodically revised to reflect changes in the overall risk profile.
CHINESE SIMPLIFIED: 审计域

Auditability The level to which transactions can be traced and audited through a system
CHINESE SIMPLIFIED: 可审计性

Auditable unit Subjects, units or systems that are capable of being defined and evaluated Scope Note: Auditable units may include:
Policies, procedures and practices
Cost centers, profit centers and investment centers
General ledger account balances
Information systems (manual and computerized)
Major contracts and programs
Organizational units, such as product or service lines
Functions, such as information technology (IT), purchasing, marketing, production, finance, accounting and human resources (HR)
Transaction systems for activities, such as sales, collection, purchasing, disbursement, inventory and cost accounting, production, treasury, payroll, and capital assets
Financial statements
Laws and regulations
CHINESE SIMPLIFIED: 可审计的单位

Auditor's opinion A formal statement expressed by the IS audit or assurance professional that describes the scope of the audit, the procedures used to produce the report and whether or not the findings support that the audit criteria have been met. Scope Note: The types of opinions are:
Unqualified opinion: Notes no exceptions or none of the exceptions noted aggregate to a significant deficiency
Qualified opinion: Notes exceptions aggregated to a significant deficiency (but not a material weakness)
Adverse opinion: Notes one or more significant deficiencies aggregating to a material weakness
CHINESE SIMPLIFIED: 审计意见

Authentication 1. The act of verifying identity (i.e., user, system) Scope Note: Risk: Can also refer to the verification of the correctness of a piece of data 2. The act of verifying the identity of a user and the user's eligibility to access computerized information Scope Note: Assurance: Authentication is designed to protect against fraudulent logon activity. It can also refer to the verification of the correctness of a piece of data.
CHINESE SIMPLIFIED: 身份认证

Authenticity Undisputed authorship
CHINESE SIMPLIFIED: 真实性

© 2015 ISACA All rights reserved.

Automated application controls Controls that have been programmed and embedded within an application
CHINESE SIMPLIFIED: 自动化应用程序控制

Availability Ensuring timely and reliable access to and use of information
CHINESE SIMPLIFIED: 可用性

Awareness Being acquainted with, mindful of, conscious of and well informed on a specific subject, which implies knowing and understanding a subject and acting accordingly
CHINESE SIMPLIFIED: 意识

B

Back door A means of regaining access to a compromised system by installing software or configuring existing software to enable remote access under attacker-defined conditions
CHINESE SIMPLIFIED: 后门

Backbone The main communication channel of a digital network. The part of a network that handles the major traffic Scope Note: Employs the highest-speed transmission paths in the network and may also run the longest distances. Smaller networks are attached to the backbone, and networks that connect directly to the end user or customer are called "access networks." A backbone can span a geographic area of any size from a single building to an office complex to an entire country. Or, it can be as small as a backplane in a single cabinet.
CHINESE SIMPLIFIED: 主干网

Backup Files, equipment, data and procedures available for use in the event of a failure or loss, if the originals are destroyed or out of service
CHINESE SIMPLIFIED: 备份

Backup center An alternate facility to continue IT/IS operations when the primary data processing (DP) center is unavailable
CHINESE SIMPLIFIED: 备份中心

Badge A card or other device that is presented or displayed to obtain access to an otherwise restricted facility, as a symbol of authority (e.g., the police), or as a simple means of identification Scope Note: Also used in advertising and publicity
CHINESE SIMPLIFIED: 证章

Balanced scorecard (BSC) Developed by Robert S. Kaplan and David P. Norton as a coherent set of performance measures organized into four categories that includes traditional financial measures, but adds customer, internal business process, and learning and growth perspectives
CHINESE SIMPLIFIED: 平衡计分卡

Bandwidth The range between the highest and lowest transmittable frequencies. It equates to the transmission capacity of an electronic line and is expressed in bytes per second or Hertz (cycles per second).
CHINESE SIMPLIFIED: 带宽

Bar code A printed machine-readable code that consists of parallel bars of varied width and spacing
CHINESE SIMPLIFIED: 条形码

Base case A standardized body of data created for testing purposes Scope Note: Users normally establish the data. Base cases validate production application systems and test the ongoing accurate operation of the system.
CHINESE SIMPLIFIED: 基础案例

Baseband A form of modulation in which data signals are pulsed directly on the transmission medium without frequency division and usually utilize a transceiver Scope Note: The entire bandwidth of the transmission medium (e.g., coaxial cable) is utilized for a single channel.
CHINESE SIMPLIFIED: 基带

Baseline architecture The existing description of the fundamental underlying design of the components of the business system before entering a cycle of architecture review and redesign Scope Note: COBIT 5 perspective
CHINESE SIMPLIFIED: 基线结构

Bastion System heavily fortified against attacks
CHINESE SIMPLIFIED: 堡垒

Batch control Correctness checks built into data processing systems and applied to batches of input data, particularly in the data preparation stage Scope Note: There are two main forms of batch controls: sequence control, which involves numbering the records in a batch consecutively so that the presence of each record can be confirmed; and control total, which is a total of the values in selected fields within the transactions.
CHINESE SIMPLIFIED: 批量控制

Batch processing The processing of a group of transactions at the same time Scope Note: Transactions are collected and processed against the master files at a specified time.
CHINESE SIMPLIFIED: 批处理

Baud rate The rate of transmission for telecommunications data, expressed in bits per second (bps)
CHINESE SIMPLIFIED: 波特率

Benchmark A test that has been designed to evaluate the performance of a system Scope Note: In a benchmark test, a system is subjected to a known workload and the performance of the system against this workload is measured. Typically, the purpose is to compare the measured performance with that of other systems that have been subject to the same benchmark test.
CHINESE SIMPLIFIED: 基准指标

© 2015 ISACA All rights reserved.

Benchmarking A systematic approach to comparing enterprise performance against peers and competitors in an effort to learn the best ways of conducting business Scope Note: Examples include benchmarking of quality, logistic efficiency and various other metrics.
CHINESE SIMPLIFIED: **基准检测**

Benefit In business, an outcome whose nature and value (expressed in various ways) are considered advantageous by an enterprise
CHINESE SIMPLIFIED: **效益**

Benefits realization One of the objectives of governance. The bringing about of new benefits for the enterprise, the maintenance and extension of existing forms of benefits, and the elimination of those initiatives and assets that are not creating sufficient value Scope Note: COBIT 5 perspective
CHINESE SIMPLIFIED: **效益实现**

Binary code A code whose representation is limited to 0 and 1
CHINESE SIMPLIFIED: **二进制码**

Biometric locks Door and entry locks that are activated by such biometric features as voice, eye retina, fingerprint or signature
CHINESE SIMPLIFIED: **生物锁**

Biometrics A security technique that verifies an individual's identity by analyzing a unique physical attribute, such as a handprint
CHINESE SIMPLIFIED: **生物特征识别**

Bit-stream image Bit-stream backups, also referred to as mirror image backups, involve the backup of all areas of a computer hard disk drive or other type of storage media. Scope Note: Such backups exactly replicate all sectors on a given storage device including all files and ambient data storage areas.
CHINESE SIMPLIFIED: **比特流映像**

Black box testing A testing approach that focuses on the functionality of the application or product and does not require knowledge of the code intervals
CHINESE SIMPLIFIED: **黑盒测试**

Block cipher A public algorithm that operates on plaintext in blocks (strings or groups) of bits
CHINESE SIMPLIFIED: **分组密码**

Botnet A term derived from "robot network;" is a large automated and distributed network of previously compromised computers that can be simultaneously controlled to launch large-scale attacks such as a denial-of-service attack on selected victims
CHINESE SIMPLIFIED: **僵尸网络**

Boundary Logical and physical controls to define a perimeter between the organization and the outside world
CHINESE SIMPLIFIED: **边界**

Bridge Data link layer device developed in the early 1980s to connect local area networks (LANs) or create two separate LAN or wide area network (WAN) network segments from a single segment to reduce collision domains Scope Note: A bridge acts as a store-and-forward device in moving frames toward their destination. This is achieved by analyzing the MAC header of a data packet, which represents the hardware address of an NIC.
CHINESE SIMPLIFIED: **网桥**

Bring your own device (BYOD) An enterprise policy used to permit partial or full integration of user-owned mobile devices for business purposes
CHINESE SIMPLIFIED: **自带设备**

Broadband Multiple channels are formed by dividing the transmission medium into discrete frequency segments. Scope Note: Broadband generally requires the use of a modem.
CHINESE SIMPLIFIED: **宽带**

Broadcast A method to distribute information to multiple recipients simultaneously
CHINESE SIMPLIFIED: **广播**

Brouter Device that performs the functions of both a bridge and a router Scope Note: A brouter operates at both the data link and the network layers. It connects same data link type LAN segments as well as different data link ones, which is a significant advantage. Like a bridge, it forwards packets based on the data link layer address to a different network of the same type. Also, whenever required, it processes and forwards messages to a different data link type network based on the network protocol address. When connecting same data link type networks, it is as fast as a bridge and is able to connect different data link type networks.
CHINESE SIMPLIFIED: **桥接路由器**

Browser A computer program that enables the user to retrieve information that has been made publicly available on the Internet; also, that permits multimedia (graphics) applications on the World Wide Web
CHINESE SIMPLIFIED: **浏览器**

Brute force A class of algorithms that repeatedly try all possible combinations until a solution is found
CHINESE SIMPLIFIED: **穷举**

Brute force attack Repeatedly trying all possible combinations of passwords or encryption keys until the correct one is found
CHINESE SIMPLIFIED: **穷举攻击或暴力攻击**

Budget Estimated cost and revenue amounts for a given range of periods and set of books Scope Note: There can be multiple budget versions for the same set of books.
CHINESE SIMPLIFIED: **预算**

© 2015 ISACA All rights reserved.

Budget formula A mathematical expression used to calculate budget amounts based on actual results, other budget amounts and statistics. Scope Note: With budget formulas, budgets using complex equations, calculations and allocations can be automatically created.
CHINESE SIMPLIFIED: 预算公式

Budget hierarchy A group of budgets linked together at different levels such that the budgeting authority of a lower-level budget is controlled by an upper-level budget
CHINESE SIMPLIFIED: 预算层级

Budget organization An entity (department, cost center, division or other group) responsible for entering and maintaining budget data
CHINESE SIMPLIFIED: 预算组织

Buffer Memory reserved to temporarily hold data to offset differences between the operating speeds of different devices, such as a printer and a computer Scope Note: In a program, buffers are reserved areas of random access memory (RAM) that hold data while they are being processed.
CHINESE SIMPLIFIED: 缓冲区

Buffer overflow Occurs when a program or process tries to store more data in a buffer (temporary data storage area) than it was intended to hold Scope Note: Since buffers are created to contain a finite amount of data, the extra information—which has to go somewhere—can overflow into adjacent buffers, corrupting or overwriting the valid data held in them. Although it may occur accidentally through programming error, buffer overflow is an increasingly common type of security attack on data integrity. In buffer overflow attacks, the extra data may contain codes designed to trigger specific actions, in effect sending new instructions to the attacked computer that could, for example, damage the user's files, change data, or disclose confidential information. Buffer overflow attacks are said to have arisen because the C programming language supplied the framework, and poor programming practices supplied the vulnerability.
CHINESE SIMPLIFIED: 缓冲区溢出

Bulk data transfer A data recovery strategy that includes a recovery from complete backups that are physically shipped offsite once a week Scope Note: Specifically, logs are batched electronically several times daily, and then loaded into a tape library located at the same facility as the planned recovery.
CHINESE SIMPLIFIED: 批量数据传输

Bus Common path or channel between hardware devices Scope Note: Can be located between components internal to a computer or between external computers in a communication network.
CHINESE SIMPLIFIED: 总线

Bus configuration All devices (nodes) are linked along one communication line where transmissions are received by all attached nodes. Scope Note: This architecture is reliable in very small networks, as well as easy to use and understand. This configuration requires the least amount of cable to connect the computers together and, therefore, is less expensive than other cabling arrangements. It is also easy to extend, and two cables can be easily joined with a connector to make a longer cable for more computers to join the network. A repeater can also be used to extend a bus configuration.
CHINESE SIMPLIFIED: 总线配置

Business balanced scorecard A tool for managing organizational strategy that uses weighted measures for the areas of financial performance (lag) indicators, internal operations, customer measurements, learning and growth (lead) indicators, combined to rate the enterprise
CHINESE SIMPLIFIED: 业务平衡计分卡

Business case Documentation of the rationale for making a business investment, used both to support a business decision on whether to proceed with the investment and as an operational tool to support management of the investment through its full economic life cycle
CHINESE SIMPLIFIED: 业务案例

Business continuity Preventing, mitigating and recovering from disruption. Scope Note: The terms 'business resumption planning', 'disaster recovery planning' and 'contingency planning' also may be used in this context; they focus on recovery aspects of continuity, and for that reason the 'resilience' aspect should also be taken into account.
COBIT 5 perspective
CHINESE SIMPLIFIED: 业务连续性管理

Business continuity plan (BCP) A plan used by an enterprise to respond to disruption of critical business processes. Depends on the contingency plan for restoration of critical systems
CHINESE SIMPLIFIED: 业务持续计划

Business control The policies, procedures, practices and organizational structures designed to provide reasonable assurance that the business objectives will be achieved and undesired events will be prevented or detected
CHINESE SIMPLIFIED: 业务控制

Business dependency assessment A process of identifying resources critical to the operation of a business process
CHINESE SIMPLIFIED: 业务依赖性评估

Business function An activity that an enterprise does, or needs to do, to achieve its objectives
CHINESE SIMPLIFIED: 业务功能

Business goal The translation of the enterprise's mission from a statement of intention into performance targets and results
CHINESE SIMPLIFIED: 企业目标

© 2015 ISACA All rights reserved.

Business impact The net effect, positive or negative, on the achievement of business objectives
CHINESE SIMPLIFIED: **业务影响**

Business impact analysis (BIA) A process to determine the impact of losing the support of any resource Scope Note: The BIA assessment study will establish the escalation of that loss over time. It is predicated on the fact that senior management, when provided reliable data to document the potential impact of a lost resource, can make the appropriate decision.
CHINESE SIMPLIFIED: **业务影响分析**

Business impact analysis/assessment (BIA) Evaluating the criticality and sensitivity of information assets.
An exercise that determines the impact of losing the support of any resource to an enterprise, establishes the escalation of that loss over time, identifies the minimum resources needed to recover, and prioritizes the recovery of processes and the supporting system Scope Note: This process also includes addressing:
Income loss
Unexpected expense
Legal issues (regulatory compliance or contractual)
Interdependent processes
Loss of public reputation or public confidence
CHINESE SIMPLIFIED: **业务影响分析/评估 (BIA)**

Business interruption Any event, whether anticipated (i.e., public service strike) or unanticipated (i.e., blackout) that disrupts the normal course of business operations at an enterprise
CHINESE SIMPLIFIED: **业务中断**

Business Model for Information Security (BMIS) A holistic and business-oriented model that supports enterprise governance and management information security, and provides a common language for information security professionals and business management
CHINESE SIMPLIFIED: **信息安全业务模型**

Business objective A further development of the business goals into tactical targets and desired results and outcomes
CHINESE SIMPLIFIED: **业务目标**

Business process An inter-related set of cross-functional activities or events that result in the delivery of a specific product or service to a customer
CHINESE SIMPLIFIED: **业务流程**

Business process control The policies, procedures, practices and organizational structures designed to provide reasonable assurance that a business process will achieve its objectives. Scope Note: COBIT 5 perspective
CHINESE SIMPLIFIED: **业务流程控制**

Business process integrity Controls over the business processes that are supported by the enterprise resource planning system (ERP)
CHINESE SIMPLIFIED: **业务流程完整性**

Business process owner The individual responsible for identifying process requirements, approving process design and managing process performance Scope Note: Must be at an appropriately high level in the enterprise and have authority to commit resources to process-specific risk management activities
CHINESE SIMPLIFIED: **业务流程所有者**

Business process reengineering (BPR) The thorough analysis and significant redesign of business processes and management systems to establish a better performing structure, more responsive to the customer base and market conditions, while yielding material cost savings
CHINESE SIMPLIFIED: **业务流程再造**

Business risk A probable situation with uncertain frequency and magnitude of loss (or gain)
CHINESE SIMPLIFIED: **业务风险**

Business service provider (BSP) An application service provider (ASP) that also provides outsourcing of business processes such as payment processing, sales order processing and application development
CHINESE SIMPLIFIED: **业务服务提供商 (BSP)**

Business sponsor The individual accountable for delivering the benefits and value of an IT-enabled business investment program to the enterprise
CHINESE SIMPLIFIED: **业务发起人**

Business-to-business Transactions in which the acquirer is an enterprise or an individual operating in the ambits of his/her professional activity. In this case, laws and regulations related to consumer protection are not applicable. Scope Note: The contract's general terms should be communicated to the other party and specifically approved. Some companies require the other party to fill out check-boxes where there is a description such as "I specifically approve the clauses" This is not convincing; the best solution is the adoption of a digital signature scheme, which allows the approval of clauses and terms with the non-repudiation condition.
CHINESE SIMPLIFIED: **企业对企业**

Business-to-consumer Selling processes in which the involved parties are the enterprise, which offers goods or services, and a consumer. In this case there is comprehensive legislation that protects the consumer. Scope Note: Comprehensive legislation includes:
Regarding contracts established outside the merchant's property (such as the right to end the contract with full refund or the return policy for goods)
Regarding distance contracts (such as rules that establish how a contract should be written, specific clauses and the need to transmit to the consumer and approve it)
Regarding electronic form of the contract (such as on the Internet, the possibility for the consumer to exit from the procedure without having his/her data recorded)
CHINESE SIMPLIFIED: **企业对消费者**

© 2015 ISACA All rights reserved.

Business-to-consumer e-commerce (B2C)
Refers to the processes by which enterprises conduct business electronically with their customers and/or public at large using the Internet as the enabling technology
CHINESE SIMPLIFIED: **企业对消费者电子商务 (B2C)**

Bypass label processing (BLP) A technique of reading a computer file while bypassing the internal file/data set label. This process could result in bypassing of the security access control system.
CHINESE SIMPLIFIED: **旁路标签处理**

C

Cadbury The Committee on the Financial Aspects of Corporate Governance, set up in May 1991 by the UK Financial Reporting Council, the London Stock Exchange and the UK accountancy profession, was chaired by Sir Adrian Cadbury and produced a report on the subject commonly known in the UK as the Cadbury Report.
CHINESE SIMPLIFIED: **Cadbury**

Capability An aptitude, competency or resource that an enterprise may possess or require at an enterprise, business function or individual level that has the potential, or is required, to contribute to a business outcome and to create value
CHINESE SIMPLIFIED: **能力**

Capability Maturity Model (CMM)
1. Contains the essential elements of effective processes for one or more disciplines.
It also describes an evolutionary improvement path from ad hoc, immature processes to disciplined, mature processes with improved quality and effectiveness.
2. CMM for software, from the Software Engineering Institute (SEI), is a model used by many enterprises to identify best practices useful in helping them assess and increase the maturity of their software development processes Scope Note: CMM ranks software development enterprises according to a hierarchy of five process maturity levels. Each level ranks the development environment according to its capability of producing quality software. A set of standards is associated with each of the five levels. The standards for level one describe the most immature or chaotic processes and the standards for level five describe the most mature or quality processes.
A maturity model that indicates the degree of reliability or dependency the business can place on a process achieving the desired goals or objectives.
A collection of instructions that an enterprise can follow to gain better control over its software development process.
CHINESE SIMPLIFIED: **成熟度模型**

Capacity stress testing Testing an application with large quantities of data to evaluate its performance during peak periods. Also called volume testing
CHINESE SIMPLIFIED: **容量压力测试**

Capital expenditure/expense (CAPEX) An expenditure that is recorded as an asset because it is expected to benefit more than the current period. The asset is then depreciated or amortized over the expected useful life of the asset.
CHINESE SIMPLIFIED: **资本性支出(CAPEX)**

Card swipe A physical control technique that uses a secured card or ID to gain access to a highly sensitive location. Scope Note: If built correctly, card swipes act as a preventive control over physical access to those sensitive locations. After a card has been swiped, the application attached to the physical card swipe device logs all card users who try to access the secured location. The card swipe device prevents unauthorized access and logs all attempts to enter the secured location.
CHINESE SIMPLIFIED: **卡片识别**

Cathode ray tube (CRT) A vacuum tube that displays data by means of an electron beam striking the screen, which is coated with suitable phosphor material or a device similar to a television screen on which data can be displayed
CHINESE SIMPLIFIED: **阴极射线管 (CRT)**

Central processing unit (CPU) Computer hardware that houses the electronic circuits that control/direct all operations of the computer system
CHINESE SIMPLIFIED: **中央处理器**

Centralized data processing Identified by one central processor and databases that form a distributed processing configuration
CHINESE SIMPLIFIED: **集中式数据处理**

Certificate (Certification) authority (CA) A trusted third party that serves authentication infrastructures or enterprises and registers entities and issues them certificates
CHINESE SIMPLIFIED: **认证颁发机构 (CA)**

Certificate revocation list (CRL) An instrument for checking the continued validity of the certificates for which the certification authority (CA) has responsibility Scope Note: The CRL details digital certificates that are no longer valid. The time gap between two updates is very critical and is also a risk in digital certificates verification.
CHINESE SIMPLIFIED: **证书撤消清单（CRL）**

Certification practice statement (CPS) A detailed set of rules governing the certificate authority's operations. It provides an understanding of the value and trustworthiness of certificates issued by a given certificate authority (CA). Scope Note: In terms of the controls that an enterprise observes, the method it uses to validate the authenticity of certificate applicants and the CA's expectations of how its certificates may be used
CHINESE SIMPLIFIED: **认证实施细则 (CPS)**

© 2015 ISACA All rights reserved.

Chain of custody A legal principle regarding the validity and integrity of evidence. It requires accountability for anything that will be used as evidence in a legal proceeding to ensure that it can be accounted for from the time it was collected until the time it is presented in a court of law. Scope Note: Includes documentation as to who had access to the evidence and when, as well as the ability to identify evidence as being the exact item that was recovered or tested. Lack of control over evidence can lead to it being discredited. Chain of custody depends on the ability to verify that evidence could not have been tampered with. This is accomplished by sealing off the evidence, so it cannot be changed, and providing a documentary record of custody to prove that the evidence was at all times under strict control and not subject to tampering.
CHINESE SIMPLIFIED: **监管链**

Challenge/response token A method of user authentication that is carried out through use of the Challenge Handshake Authentication Protocol (CHAP) Scope Note: When a user tries to log into the server using CHAP, the server sends the user a "challenge," which is a random value. The user enters a password, which is used as an encryption key to encrypt the "challenge" and return it to the server. The server is aware of the password. It, therefore, encrypts the "challenge" value and compares it with the value received from the user. If the values match, the user is authenticated. The challenge/response activity continues throughout the session and this protects the session from password sniffing attacks. In addition, CHAP is not vulnerable to "man-in-the-middle" attacks because the challenge value is a random value that changes on each access attempt.
CHINESE SIMPLIFIED: **挑战/响应令牌**

Change management A holistic and proactive approach to managing the transition from a current to a desired organizational state, focusing specifically on the critical human or "soft" elements of change Scope Note: Includes activities such as culture change (values, beliefs and attitudes), development of reward systems (measures and appropriate incentives), organizational design, stakeholder management, human resources (HR) policies and procedures, executive coaching, change leadership training, team building and communication planning and execution
CHINESE SIMPLIFIED: **变更管理**

Channel service unit/digital service unit (CSU/DSU) Interfaces at the physical layer of the open systems interconnection (OSI) reference model, data terminal equipment (DTE) to data circuit terminating equipment (DCE), for switched carrier networks
CHINESE SIMPLIFIED: **通道服务单元/数据服务单元 (CSU/DSU)**

Chargeback The redistribution of expenditures to the units within a company that gave rise to them. Scope Note: Chargeback is important because without such a policy, misleading views may be given as to the real profitability of a product or service because certain key expenditures will be ignored or calculated according to an arbitrary formula.
CHINESE SIMPLIFIED: **拒付**

Check digit A numeric value, which has been calculated mathematically, is added to data to ensure that original data have not been altered or that an incorrect, but valid match has occurred. Scope Note: Check digit control is effective in detecting transposition and transcription errors.
CHINESE SIMPLIFIED: **校验数字位**

Check digit verification (self-checking digit) A programmed edit or routine that detects transposition and transcription errors by calculating and checking the check digit
CHINESE SIMPLIFIED: **校验数字位检测（自查位）**

Checklist A list of items that is used to verify the completeness of a task or goal Scope Note: Used in quality assurance (and in general, in information systems audit), to check process compliance, code standardization and error prevention, and other items for which consistency processes or standards have been defined
CHINESE SIMPLIFIED: **检查清单**

Checkpoint restart procedures A point in a routine at which sufficient information can be stored to permit restarting the computation from that point
CHINESE SIMPLIFIED: **检查点重新激活程序**

Checksum A mathematical value that is assigned to a file and used to “test” the file at a later date to verify that the data contained in the file has not been maliciously changed Scope Note: A cryptographic checksum is created by performing a complicated series of mathematical operations (known as a cryptographic algorithm) that translates the data in the file into a fixed string of digits called a hash value, which is then used as the checksum. Without knowing which cryptographic algorithm was used to create the hash value, it is highly unlikely that an unauthorized person would be able to change data without inadvertently changing the corresponding checksum. Cryptographic checksums are used in data transmission and data storage. Cryptographic checksums are also known as message authentication codes, integrity check-values, modification detection codes or message integrity codes.
CHINESE SIMPLIFIED: **校验和**

Chief executive officer (CEO) The highest ranking individual in an enterprise
CHINESE SIMPLIFIED: **首席执行官 (CEO)**

Chief financial officer (CFO) The individual primarily responsible for managing the financial risk of an enterprise
CHINESE SIMPLIFIED: **首席财务官 (CFO)**

Chief information officer (CIO) The most senior official of the enterprise who is accountable for IT advocacy, aligning IT and business strategies, and planning, resourcing and managing the delivery of IT services, information and the deployment of associated human resources Scope Note: In some cases, the CIO role has been expanded to become the chief knowledge officer (CKO) who deals in knowledge, not just information. Also see chief technology officer (CTO).
CHINESE SIMPLIFIED: **首席信息官**

© 2015 ISACA All rights reserved.

Chief Information Security Officer (CISO)
The person in charge of information security within the enterprise
CHINESE SIMPLIFIED: **首席信息安全官(CISO)**

Chief Security Officer (CSO) The person usually responsible for all security matters both physical and digital in an enterprise
CHINESE SIMPLIFIED: **首席安全官(CSO)**

Chief technology officer (CTO) The individual who focuses on technical issues in an enterprise Scope Note: Often viewed as synonymous with chief information officer (CIO)
CHINESE SIMPLIFIED: **首席技术官 (CTO)**

Cipher An algorithm to perform encryption
CHINESE SIMPLIFIED: **加密**

Ciphertext Information generated by an encryption algorithm to protect the plaintext and that is unintelligible to the unauthorized reader.
CHINESE SIMPLIFIED: **密文**

Circuit-switched network A data transmission service requiring the establishment of a circuit-switched connection before data can be transferred from source data terminal equipment (DTE) to a sink DTE Scope Note: A circuit-switched data transmission service uses a connection network.
CHINESE SIMPLIFIED: **电路交换网络**

Circular routing In open systems architecture, circular routing is the logical path of a message in a communication network based on a series of gates at the physical network layer in the open systems interconnection (OSI) model.
CHINESE SIMPLIFIED: **循环路由**

Cleartext Data that is not encrypted. Also known as plaintext.
CHINESE SIMPLIFIED: **明文**

Client-server A group of computers connected by a communication network, in which the client is the requesting machine and the server is the supplying machine Scope Note: Software is specialized at both ends. Processing may take place on either the client or the server, but it is transparent to the user.
CHINESE SIMPLIFIED: **客户端 / 服务器**

Cloud computing Convenient, on-demand network access to a shared pool of resources that can be rapidly provisioned and released with minimal management effort or service provider interaction
CHINESE SIMPLIFIED: **云计算**

Cluster controller A communication terminal control hardware unit that controls a number of computer terminals Scope Note: All messages are buffered by the controller and then transmitted to the receiver.
CHINESE SIMPLIFIED: **集群控制器**

Coaxial cable Composed of an insulated wire that runs through the middle of each cable, a second wire that surrounds the insulation of the inner wire like a sheath, and the outer insulation which wraps the second wire Scope Note: Has a greater transmission capacity than standard twisted-pair cables, but has a limited range of effective distance
CHINESE SIMPLIFIED: **同轴电缆**

COBIT
1. COBIT 5: Formerly known as Control Objectives for Information and related Technology (COBIT); now used only as the acronym in its fifth iteration. A complete, internationally accepted framework for governing and managing enterprise information and technology (IT) that supports enterprise executives and management in their definition and achievement of business goals and related IT goals. COBIT describes five principles and seven enablers that support enterprises in the development, implementation, and continuous improvement and monitoring of good IT-related governance and management practices Scope Note: Earlier versions of COBIT focused on control objectives related to IT processes, management and control of IT processes and IT governance aspects. Adoption and use of the COBIT framework are supported by guidance from a growing family of supporting products. (See www.isaca.org/cobit for more information.)
2. COBIT 4.1 and earlier: Formally known as Control Objectives for Information and related Technology (COBIT). A complete, internationally accepted process framework for IT that supports business and IT executives and management in their definition and achievement of business goals and related IT goals by providing a comprehensive IT governance, management, control and assurance model. COBIT describes IT processes and associated control objectives, management guidelines (activities, accountabilities, responsibilities and performance metrics) and maturity models. COBIT supports enterprise management in the development, implementation, continuous improvement and monitoring of good IT-related practices. Scope Note: Adoption and use of the COBIT framework are supported by guidance for executives and management (Board Briefing on IT Governance, 2nd Edition), IT governance implementers (COBIT Quickstart, 2nd Edition; IT Governance Implementation Guide: Using COBIT and Val IT, 2nd Edition; and COBIT Control Practices: Guidance to Achieve Control Objectives for Successful IT Governance), and IT assurance and audit professionals (IT Assurance Guide Using COBIT). Guidance also exists to support its applicability for certain legislative and regulatory requirements (e.g., IT Control Objectives for Sarbanes-Oxley, IT Control Objectives for Basel II) and its relevance to information security (COBIT Security Baseline). COBIT is mapped to other frameworks and standards to illustrate complete coverage of the IT management life cycle and support its use in enterprises using multiple IT-related framework and standards.
CHINESE SIMPLIFIED: **COBIT (信息及相关技术的控制目标)**

CoCo Criteria of Control, published by the Canadian Institute of Chartered Accountants in 1995
CHINESE SIMPLIFIED: **COCO**

© 2015 ISACA All rights reserved.

Code of ethics A document designed to influence individual and organizational behavior of employees, by defining organizational values and the rules to be applied in certain situations. Scope Note: A code of ethics is adopted to assist those in the enterprise called upon to make decisions understand the difference between 'right' and 'wrong' and to apply this understanding to their decisions.
COBIT 5 perspective
CHINESE SIMPLIFIED: **职业道德规范**

Coevolving Originated as a biological term, refers to the way two or more ecologically interdependent species become intertwined over time Scope Note: As these species adapt to their environment they also adapt to one another. Today's multi-business companies need to take their cue from biology to survive. They should assume that links among businesses are temporary and that the number of connections-not just their content-matters. Rather than plan collaborative strategy from the top, as traditional companies do, corporate executives in coevolving companies should simply set the context and let collaboration (and competition) emerge from business units.
CHINESE SIMPLIFIED: **共同进化**

Coherence Establishing a potent binding force and sense of direction and purpose for the enterprise, relating different parts of the enterprise to each other and to the whole to act as a seemingly unique entity
CHINESE SIMPLIFIED: **相干性**

Cohesion The extent to which a system unit--subroutine, program, module, component, subsystem--performs a single dedicated function. Scope Note: Generally, the more cohesive the unit, the easier it is to maintain and enhance a system because it is easier to determine where and how to apply a change.
CHINESE SIMPLIFIED: **内聚力**

Cold site An IS backup facility that has the necessary electrical and physical components of a computer facility, but does not have the computer equipment in place Scope Note: The site is ready to receive the necessary replacement computer equipment in the event that the users have to move from their main computing location to the alternative computer facility.
CHINESE SIMPLIFIED: **冷站**

Collision The situation that occurs when two or more demands are made simultaneously on equipment that can handle only one at any given instant (Federal Standard 1037C)
CHINESE SIMPLIFIED: **碰撞**

Combined Code on Corporate Governance The consolidation in 1998 of the "Cadbury," "Greenbury" and "Hampel" Reports Scope Note: Named after the Committee Chairs, these reports were sponsored by the UK Financial Reporting Council, the London Stock Exchange, the Confederation of British Industry, the Institute of Directors, the Consultative Committee of Accountancy Bodies, the National Association of Pension Funds and the Association of British Insurers to address the financial aspects of corporate governance, directors' remuneration and the implementation of the Cadbury and Greenbury recommendations.
CHINESE SIMPLIFIED: **公司治理综合准则**

Common Attack Pattern Enumeration and Classification (CAPEC) A catalogue of attack patterns as "an abstraction mechanism for helping describe how an attack against vulnerable systems or networks is executed" published by the MITRE Corporation
CHINESE SIMPLIFIED: **通用攻击模式枚举与分类**

Communication processor A computer embedded in a communications system that generally performs the basic tasks of classifying network traffic and enforcing network policy functions Scope Note: An example is the message data processor of a defense digital network (DDN) switching center. More advanced communication processors may perform additional functions.
CHINESE SIMPLIFIED: **通信处理器**

Communications controller Small computers used to connect and coordinate communication links between distributed or remote devices and the main computer, thus freeing the main computer from this overhead function
CHINESE SIMPLIFIED: **通讯控制器**

Community strings Authenticate access to management information base (MIB) objects and function as embedded passwords Scope Note: Examples are:
Read-only (RO)-Gives read access to all objects in the MIB except the community strings, but does not allow write access
Read-write (RW)-Gives read and write access to all objects in the MIB, but does not allow access to the community strings
Read-write-all-Gives read and write access to all objects in the MIB, including the community strings (only valid for Catalyst 4000, 5000 and 6000 series switches)
Network Management Protocol (SNMP) community strings are sent across the network in cleartext. The best way to protect an operating system (OS) software-based device from unauthorized SNMP management is to build a standard IP access list that includes the source address of the management station(s). Multiple access lists can be defined and tied to different community strings. If logging is enabled on the access list, then log messages are generated every time that the device is accessed from the management station. The log message records the source IP address of the packet.
CHINESE SIMPLIFIED: **团体字符串**

© 2015 ISACA All rights reserved.

Comparison program A program for the examination of data, using logical or conditional tests to determine or to identify similarities or differences
CHINESE SIMPLIFIED: 对照程序

Compartmentalization A process for protecting very-high value assets or in environments where trust is an issue. Access to an asset requires two or more processes, controls or individuals.
CHINESE SIMPLIFIED: 隔离

Compensating control An internal control that reduces the risk of an existing or potential control weakness resulting in errors and omissions
CHINESE SIMPLIFIED: 补偿性控制

Competence The ability to perform a specific task, action or function successfully Scope Note: COBIT 5 perspective
CHINESE SIMPLIFIED: 能力

Competencies The strengths of an enterprise or what it does well Scope Note: Can refer to the knowledge, skills and abilities of the assurance team or individuals conducting the work.
CHINESE SIMPLIFIED: 能力

Compiler A program that translates programming language (source code) into machine executable instructions (object code)
CHINESE SIMPLIFIED: 编译器

Completely Automated Public Touring test to tell Computers and Humans Apart (CAPTCHA) A type of challenge-response test used in computing to ensure that the response is not generated by a computer. An example is the site request for web site users to recognize and type a phrase posted using various challenging-to-read fonts.
CHINESE SIMPLIFIED: 全自动区分计算机和人类的图灵测试 (CAPTCHA)

Completely connected (mesh) configuration A network topology in which devices are connected with many redundant interconnections between network nodes (primarily used for backbone networks)
CHINESE SIMPLIFIED: 完全连接（网状）配置

Completeness check A procedure designed to ensure that no fields are missing from a record
CHINESE SIMPLIFIED: 完整性检查

Compliance Adherence to, and the ability to demonstrate adherence to, mandated requirements defined by laws and regulations, as well as voluntary requirements resulting from contractual obligations and internal policies
CHINESE SIMPLIFIED: 合规性

Compliance documents Policies, standard and procedures that document the actions that are required or prohibited. Violations may be subject to disciplinary actions.
CHINESE SIMPLIFIED: 合规性文件

Compliance testing Tests of control designed to obtain audit evidence on both the effectiveness of the controls and their operation during the audit period
CHINESE SIMPLIFIED: 符合性测试

Component A general term that is used to mean one part of something more complex Scope Note: For example, a computer system may be a component of an IT service, or an application may be a component of a release unit. Components are co-operating packages of executable software that make their services available through defined interfaces. Components used in developing systems may be commercial off-the-shelf software (COTS) or may be purposely built. However, the goal of component-based development is to ultimately use as many pre-developed, pretested components as possible.
CHINESE SIMPLIFIED: 组件

Comprehensive audit An audit designed to determine the accuracy of financial records as well as to evaluate the internal controls of a function or department
CHINESE SIMPLIFIED: 全面审计

Computationally greedy Requiring a great deal of computing power; processor intensive
CHINESE SIMPLIFIED: 贪占计算资源

Computer emergency response team (CERT) A group of people integrated at the enterprise with clear lines of reporting and responsibilities for standby support in case of an information systems emergency.
This group will act as an efficient corrective control, and should also act as a single point of contact for all incidents and issues related to information systems.
CHINESE SIMPLIFIED: 计算机紧急事件响应组

Computer forensics The application of the scientific method to digital media to establish factual information for judicial review Scope Note: This process often involves investigating computer systems to determine whether they are or have been used for illegal or unauthorized activities. As a discipline, it combines elements of law and computer science to collect and analyze data from information systems (e.g., personal computers, networks, wireless communication and digital storage devices) in a way that is admissible as evidence in a court of law.
CHINESE SIMPLIFIED: 计算机取证

Computer sequence checking Verifies that the control number follows sequentially and that any control numbers out of sequence are rejected or noted on an exception report for further research
CHINESE SIMPLIFIED: 计算机序列检验

© 2015 ISACA All rights reserved.

Computer server 1. A computer dedicated to servicing requests for resources from other computers on a network. Servers typically run network operating systems. 2. A computer that provides services to another computer (the client)
CHINESE SIMPLIFIED: 计算机服务器

Computer-aided software engineering (CASE) The use of software packages that aid in the development of all phases of an information system Scope Note: System analysis, design programming and documentation are provided. Changes introduced in one CASE chart will update all other related charts automatically. CASE can be installed on a microcomputer for easy access.
CHINESE SIMPLIFIED: 计算机辅助软件工程

Computer-assisted audit technique (CAAT) Any automated audit technique, such as generalized audit software (GAS), test data generators, computerized audit programs and specialized audit utilities
CHINESE SIMPLIFIED: 计算机辅助审计技术

Concurrency control Refers to a class of controls used in a database management system (DBMS) to ensure that transactions are processed in an atomic, consistent, isolated and durable manner (ACID). This implies that only serial and recoverable schedules are permitted, and that committed transactions are not discarded when undoing aborted transactions.
CHINESE SIMPLIFIED: 并行控制

Concurrent access A fail-over process, in which all nodes run the same resource group (there can be no [Internet Protocol] IP or [mandatory access control] MAC address in a concurrent resource group) and access the external storage concurrently
CHINESE SIMPLIFIED: 并发访问

Confidentiality Preserving authorized restrictions on access and disclosure, including means for protecting privacy and proprietary information
CHINESE SIMPLIFIED: 机密性

Configurable control Typically, an automated control that is based on, and therefore dependent on, the configuration of parameters within the application system
CHINESE SIMPLIFIED: 可配置控制项

Configuration item (CI) Component of an infrastructure-or an item, such as a request for change, associated with an infrastructure-which is (or is to be) under the control of configuration management Scope Note: May vary widely in complexity, size and type, from an entire system (including all hardware, software and documentation) to a single module or a minor hardware component
CHINESE SIMPLIFIED: 配置项 (CI)

Configuration management The control of changes to a set of configuration items over a system life cycle
CHINESE SIMPLIFIED: 配置管理

Console log An automated detail report of computer system activity
CHINESE SIMPLIFIED: 主机控制台日志

Consulted In a RACI (responsible, accountable, consulted, informed) chart, refers to those people whose opinions are sought on an activity (two-way communication)
CHINESE SIMPLIFIED: 被咨询者

Consumerization A new model in which emerging technologies are first embraced by the consumer market and later spread to the business
CHINESE SIMPLIFIED: 消费化

Containment Actions taken to limit exposure after an incident has been identified and confirmed
CHINESE SIMPLIFIED: 抑制

Content filtering Controlling access to a network by analyzing the contents of the incoming and outgoing packets and either letting them pass or denying them based on a list of rules Scope Note: Differs from packet filtering in that it is the data in the packet that are analyzed instead of the attributes of the packet itself (e.g., source/target IP address, transmission control protocol [TCP] flags)
CHINESE SIMPLIFIED: 内容过滤

Context The overall set of internal and external factors that might influence or determine how an enterprise, entity, process or individual acts Scope Note: Context includes:
technology context (technological factors that affect an enterprise's ability to extract value from data)
data context (data accuracy, availability, currency and quality)
skills and knowledge (general experience and analytical, technical and business skills),
organizational and cultural context (political factors and whether the enterprise prefers data to intuition)
strategic context (strategic objectives of the enterprise)
COBIT 5 perspective
CHINESE SIMPLIFIED: 上下文

Contingency plan A plan used by an enterprise or business unit to respond to a specific systems failure or disruption
CHINESE SIMPLIFIED: 连续性计划

Contingency planning Process of developing advance arrangements and procedures that enable an enterprise to respond to an event that could occur by chance or unforeseen circumstances.
CHINESE SIMPLIFIED: 应急计划

Continuity Preventing, mitigating and recovering from disruption Scope Note: The terms "business resumption planning," "disaster recovery planning" and "contingency planning" also may be used in this context; they all concentrate on the recovery aspects of continuity.
CHINESE SIMPLIFIED: 连续性

© 2015 ISACA All rights reserved.

Continuous auditing approach This approach allows IS auditors to monitor system reliability on a continuous basis and to gather selective audit evidence through the computer.
CHINESE SIMPLIFIED: 连续性审计方法

Continuous availability Nonstop service, with no lapse in service; the highest level of service in which no downtime is allowed
CHINESE SIMPLIFIED: 连续可用性

Continuous improvement The goals of continuous improvement (Kaizen) include the elimination of waste, defined as "activities that add cost, but do not add value;" just-in-time (JIT) delivery; production load leveling of amounts and types; standardized work; paced moving lines; and right-sized equipment Scope Note: A closer definition of the Japanese usage of Kaizen is "to take it apart and put it back together in a better way." What is taken apart is usually a process, system, product or service. Kaizen is a daily activity whose purpose goes beyond improvement. It is also a process that, when done correctly, humanizes the workplace, eliminates hard work (both mental and physical), and teaches people how to do rapid experiments using the scientific method and how to learn to see and eliminate waste in business processes.
CHINESE SIMPLIFIED: 持续改进

Control The means of managing risk, including policies, procedures, guidelines, practices or organizational structures, which can be of an administrative, technical, management, or legal nature. Scope Note: Also used as a synonym for safeguard or countermeasure.
See also Internal control.
CHINESE SIMPLIFIED: 控制

Control center Hosts the recovery meetings where disaster recovery operations are managed
CHINESE SIMPLIFIED: 控制中心

Control framework A set of fundamental controls that facilitates the discharge of business process owner responsibilities to prevent financial or information loss in an enterprise
CHINESE SIMPLIFIED: 控制框架

Control group Members of the operations area who are responsible for the collection, logging and submission of input for the various user groups
CHINESE SIMPLIFIED: 控制小组

Control objective A statement of the desired result or purpose to be achieved by implementing control procedures in a particular process
CHINESE SIMPLIFIED: 控制目标

Control Objectives for Enterprise Governance A discussion document that sets out an "enterprise governance model" focusing strongly on both the enterprise business goals and the information technology enablers that facilitate good enterprise governance, published by the Information Systems Audit and Control Foundation in 1999.
CHINESE SIMPLIFIED: 企业治理控制目标

Control perimeter The boundary defining the scope of control authority for an entity Scope Note: For example, if a system is within the control perimeter, the right and ability exist to control it in response to an attack.
CHINESE SIMPLIFIED: 控制边界

Control practice Key control mechanism that supports the achievement of control objectives through responsible use of resources, appropriate management of risk and alignment of IT with business
CHINESE SIMPLIFIED: 控制措施

Control risk The risk that a material error exists that would not be prevented or detected on a timely basis by the system of internal controls (See Inherent risk)
CHINESE SIMPLIFIED: 控制风险

Control risk self-assessment A method/process by which management and staff of all levels collectively identify and evaluate risk and controls with their business areas. This may be under the guidance of a facilitator such as an auditor or risk manager.
CHINESE SIMPLIFIED: 控制风险自我评估

Control section The area of the central processing unit (CPU) that executes software, allocates internal memory and transfers operations between the arithmetic-logic, internal storage and output sections of the computer
CHINESE SIMPLIFIED: 控制区域

Control weakness A deficiency in the design or operation of a control procedure. Control weaknesses can potentially result in risk relevant to the area of activity not being reduced to an acceptable level (relevant risk threatens achievement of the objectives relevant to the area of activity being examined). Control weaknesses can be material when the design or operation of one or more control procedures does not reduce to a relatively low level the risk that misstatements caused by illegal acts or irregularities may occur and not be detected by the related control procedures.
CHINESE SIMPLIFIED: 控制弱点

© 2015 ISACA All rights reserved.

Cookie A message kept in the web browser for the purpose of identifying users and possibly preparing customized web pages for them Scope Note: The first time a cookie is set, a user may be required to go through a registration process. Subsequent to this, whenever the cookie's message is sent to the server, a customized view based on that user's preferences can be produced. The browser's implementation of cookies has, however, brought several security concerns, allowing breaches of security and the theft of personal information (e.g., user passwords that validate the user identity and enable restricted web services).
CHINESE SIMPLIFIED: **Cookie**

Corporate exchange rate An exchange rate that can be used optionally to perform foreign currency conversion. The corporate exchange rate is generally a standard market rate determined by senior financial management for use throughout the enterprise.
CHINESE SIMPLIFIED: **公司汇率**

Corporate governance The system by which enterprises are directed and controlled. The board of directors is responsible for the governance of their enterprise. It consists of the leadership and organizational structures and processes that ensure the enterprise sustains and extends strategies and objectives.
CHINESE SIMPLIFIED: **公司治理**

Corporate security officer (CSO) Responsible for coordinating the planning, development, implementation, maintenance and monitoring of the information security program
CHINESE SIMPLIFIED: **企业安全官 (CSO)**

Corrective control Designed to correct errors, omissions and unauthorized uses and intrusions, once they are detected
CHINESE SIMPLIFIED: **改正性控制**

COSO Committee of Sponsoring Organizations of the Treadway Commission Scope Note: Its 1992 report "Internal Control--Integrated Framework" is an internationally accepted standard for corporate governance. See www.coso.org.
CHINESE SIMPLIFIED: **COSO**

Countermeasure Any process that directly reduces a threat or vulnerability
CHINESE SIMPLIFIED: **对策**

Coupling Measure of interconnectivity among structure of software programs.
Coupling depends on the interface complexity between modules. This can be defined as the point at which entry or reference is made to a module, and what data pass across the interface. Scope Note: In application software design, it is preferable to strive for the lowest possible coupling between modules. Simple connectivity among modules results in software that is easier to understand and maintain and is less prone to a ripple or domino effect caused when errors occur at one location and propagate through the system.
CHINESE SIMPLIFIED: **耦合力**

Coverage The proportion of known attacks detected by an intrusion detection system (IDS)
CHINESE SIMPLIFIED: **覆盖范围**

Crack To "break into" or "get around" a software program Scope Note: For example, there are certain newsgroups that post serial numbers for pirated versions of software. A cracker may download this information in an attempt to crack the program so he/she can use it. It is commonly used in the case of cracking (unencrypting) a password or other sensitive data.
CHINESE SIMPLIFIED: **破解**

Credentialed analysis In vulnerability analysis, passive monitoring approaches in which passwords or other access credentials are required Scope Note: Usually involves accessing a system data object
CHINESE SIMPLIFIED: **认证分析**

Criteria The standards and benchmarks used to measure and present the subject matter and against which an IS auditor evaluates the subject matter Scope Note: Criteria should be: Objective--free from bias, Measurable--provide for consistent measurement, Complete--include all relevant factors to reach a conclusion, Relevant--relate to the subject matter.
In an attestation engagement, benchmarks against which management's written assertion on the subject matter can be evaluated. The practitioner forms a conclusion concerning subject matter by referring to suitable criteria.
CHINESE SIMPLIFIED: **衡量标准**

Critical functions Business activities or information that could not be interrupted or unavailable for several business days without significantly jeopardizing operation of the enterprise
CHINESE SIMPLIFIED: **关键职能**

Critical infrastructure Systems whose incapacity or destruction would have a debilitating effect on the economic security of an enterprise, community or nation.
CHINESE SIMPLIFIED: **关键基础设施**

Critical success factor (CSF) The most important issue or action for management to achieve control over and within its IT processes
CHINESE SIMPLIFIED: **关键成功因素 (CSF)**

Criticality The importance of a particular asset or function to the enterprise, and the impact if that asset or function is not available
CHINESE SIMPLIFIED: **关键性**

Criticality analysis An analysis to evaluate resources or business functions to identify their importance to the enterprise, and the impact if a function cannot be completed or a resource is not available
CHINESE SIMPLIFIED: **重要性分析**

© 2015 ISACA All rights reserved.

Cross-certification A certificate issued by one certificate authority (CA) to a second CA so that users of the first certification authority are able to obtain the public key of the second CA and verify the certificates it has created Scope Note: Often refers to certificates issued to each other by two CAs at the same level in a hierarchy
CHINESE SIMPLIFIED: **交叉认证**

Cross-site request forgery (CSRF) A type of malicious exploit of a web site whereby unauthorized commands are transmitted from a user that the web site trusts (also known as a one-click attack or session riding); acronym pronounced "sea-surf"
CHINESE SIMPLIFIED: **跨站点请求伪造 (CSRF)**

Cross-site scripting (XSS) A type of injection, in which malicious scripts are injected into otherwise benign and trusted web sites Scope Note: Cross-site scripting (XSS) attacks occur when an attacker uses a web application to send malicious code, generally in the form of a browser side script, to a different end user. Flaws that allow these attacks to succeed are quite widespread and occur anywhere a web application uses input from a user within the output it generates without validating or encoding it. (OWASP)
CHINESE SIMPLIFIED: **跨站脚本攻击**

Cryptography The art of designing, analyzing and attacking cryptographic schemes
CHINESE SIMPLIFIED: **密码学**

Cryptosystem A pair of algorithms that take a key and convert plaintext to ciphertext and back
CHINESE SIMPLIFIED: **密码系统**

Culture A pattern of behaviors, beliefs, assumptions, attitudes and ways of doing things Scope Note: COBIT 5 perspective
CHINESE SIMPLIFIED: **文化**

Customer relationship management (CRM) A way to identify, acquire and retain customers. CRM is also an industry term for software solutions that help an enterprise manage customer relationships in an organized manner.
CHINESE SIMPLIFIED: **客户关系管理系统**

Cybercop An investigator of activities related to computer crime
CHINESE SIMPLIFIED: **网络警察**

Cyberespionage Activities conducted in the name of security, business, politics or technology to find information that ought to remain secret. It is not inherently military.
CHINESE SIMPLIFIED: **网络间谍**

Cybersecurity The protection of information assets by addressing threats to information processed, stored, and transported by internetworked information systems
CHINESE SIMPLIFIED: **网络安全**

Cybersecurity architecture Describes the structure, components and topology (connections and layout) of security controls within an enterprise's IT infrastructure Scope Note: The security architecture shows how defense-in-depth is implemented and how layers of control are linked and is essential to designing and implementing security controls in any complex environment.
CHINESE SIMPLIFIED: **网络安全架构**

Cyberwarfare Activities supported by military organizations with the purpose to threat the survival and well-being of society/foreign entity
CHINESE SIMPLIFIED: **网络战**

D

Damage evaluation The determination of the extent of damage that is necessary to provide for an estimation of the recovery time frame and the potential loss to the enterprise
CHINESE SIMPLIFIED: **损害评估**

Dashboard A tool for setting expectations for an enterprise at each level of responsibility and continuous monitoring of the performance against set targets
CHINESE SIMPLIFIED: **仪表盘**

Data analysis Typically in large enterprises in which the amount of data processed by the enterprise resource planning (ERP) system is extremely voluminous, analysis of patterns and trends proves to be extremely useful in ascertaining the efficiency and effectiveness of operations Scope Note: Most ERP systems provide opportunities for extraction and analysis of data (some with built-in tools) through the use of tools developed by third parties that interface with the ERP systems.
CHINESE SIMPLIFIED: **数据分析**

Data classification The assignment of a level of sensitivity to data (or information) that results in the specification of controls for each level of classification. Levels of sensitivity of data are assigned according to predefined categories as data are created, amended, enhanced, stored or transmitted. The classification level is an indication of the value or importance of the data to the enterprise.
CHINESE SIMPLIFIED: **数据分类**

Data classification scheme An enterprise scheme for classifying data by factors such as criticality, sensitivity and ownership
CHINESE SIMPLIFIED: **数据分类方案**

Data communications The transfer of data between separate computer processing sites/devices using telephone lines, microwave and/or satellite links
CHINESE SIMPLIFIED: **数据通信**

Data custodian The individual(s) and department(s) responsible for the storage and safeguarding of computerized data
CHINESE SIMPLIFIED: **数据保管员**

© 2015 ISACA All rights reserved.

Data dictionary A database that contains the name, type, range of values, source and authorization for access for each data element in a database.
It also indicates which application programs use those data so that when a data structure is contemplated, a list of the affected programs can be generated Scope Note: May be a stand-alone information system used for management or documentation purposes, or it may control the operation of a database
CHINESE SIMPLIFIED: 数据字典

Data diddling Changing data with malicious intent before or during input into the system
CHINESE SIMPLIFIED: 数据欺骗

Data Encryption Standard (DES) An algorithm for encoding binary data Scope Note: It is a secret key cryptosystem published by the National Bureau of Standards (NBS), the predecessor of the US National Institute of Standards and Technology (NIST). DES and its variants has been replaced by the Advanced Encryption Standard (AES)
CHINESE SIMPLIFIED: 数据加密标准

Data flow The flow of data from the input (in Internet banking, ordinarily user input at his/her desktop) to output (in Internet banking, ordinarily data in a bank's central database).
Data flow includes travel through the communication lines, routers, switches and firewalls as well as processing through various applications on servers, which process the data from user fingers to storage in a bank's central database.
CHINESE SIMPLIFIED: 数据流

Data integrity The property that data meet with a priority expectation of quality and that the data can be relied on
CHINESE SIMPLIFIED: 数据完整性

Data leakage Siphoning out or leaking information by dumping computer files or stealing computer reports and tapes
CHINESE SIMPLIFIED: 数据泄露

Data normalization A structured process for organizing data into tables in such a way that it preserves the relationships among the data
CHINESE SIMPLIFIED: 数据规范化

Data owner The individual(s), normally a manager or director, who has responsibility for the integrity, accurate reporting and use of computerized data
CHINESE SIMPLIFIED: 数据所有者

Data retention Refers to the policies that govern data and records management for meeting internal, legal and regulatory data archival requirements
CHINESE SIMPLIFIED: 数据存储策略

Data security Those controls that seek to maintain confidentiality, integrity and availability of information
CHINESE SIMPLIFIED: 数据安全

Data structure The relationships among files in a database and among data items within each file
CHINESE SIMPLIFIED: 数据结构

Data warehouse A generic term for a system that stores, retrieves and manages large volumes of data Scope Note: Data warehouse software often includes sophisticated comparison and hashing techniques for fast searches as well as for advanced filtering.
CHINESE SIMPLIFIED: 数据仓库

Database A stored collection of related data needed by enterprises and individuals to meet their information processing and retrieval requirements
CHINESE SIMPLIFIED: 数据库

Database administrator (DBA) An individual or department responsible for the security and information classification of the shared data stored on a database system.
This responsibility includes the design, definition and maintenance of the database.
CHINESE SIMPLIFIED: 数据库管理员

Database management system (DBMS) A software system that controls the organization, storage and retrieval of data in a database
CHINESE SIMPLIFIED: 数据库管理系统

Database replication The process of creating and managing duplicate versions of a database Scope Note: Replication not only copies a database but also synchronizes a set of replicas so that changes made to one replica are reflected in all of the others. The beauty of replication is that it enables many users to work with their own local copy of a database, but have the database updated as if they were working on a single centralized database. For database applications in which, geographically users are distributed widely, replication is often the most efficient method of database access.
CHINESE SIMPLIFIED: 数据库复制

Database specifications These are the requirements for establishing a database application. They include field definitions, field requirements and reporting requirements for the individual information in the database.
CHINESE SIMPLIFIED: 数据库规格说明

Datagram A packet (encapsulated with a frame containing information), that is transmitted in a packet-switching network from source to destination
CHINESE SIMPLIFIED: 数据报文

Data-oriented systems development Focuses on providing ad hoc reporting for users by developing a suitable accessible database of information and to provide useable data rather than a function
CHINESE SIMPLIFIED: 面向数据的系统开发

Decentralization The process of distributing computer processing to different locations within an enterprise
CHINESE SIMPLIFIED: 分布式处理

© 2015 ISACA All rights reserved.

Decision support systems (DSS) An interactive system that provides the user with easy access to decision models and data, to support semi structured decision-making tasks
CHINESE SIMPLIFIED: 决策支持系统

Decryption A technique used to recover the original plaintext from the ciphertext so that it is intelligible to the reader.
The decryption is a reverse process of the encryption.
CHINESE SIMPLIFIED: 解密

Decryption key A digital piece of information used to recover plaintext from the corresponding ciphertext by decryption
CHINESE SIMPLIFIED: 解密密钥

Default A computer software setting or preference that states what will automatically happen in the event that the user has not stated another preference.
For example, a computer may have a default setting to launch or start Netscape whenever a GIF file is opened; however, if using Adobe Photoshop is the preference for viewing a GIF file, the default setting can be changed to Photoshop. In the case of default accounts, these are accounts that are provided by the operating system vendor (e.g., root in UNIX).
CHINESE SIMPLIFIED: 默认值

Default deny policy A policy whereby access is denied unless it is specifically allowed; the inverse of default allow
CHINESE SIMPLIFIED: 默认拒绝策略

Default password The password used to gain access when a system is first installed on a computer or network device Scope Note: There is a large list published on the Internet and maintained at several locations. Failure to change these after the installation leaves the system vulnerable.
CHINESE SIMPLIFIED: 默认密码

Defense in depth The practice of layering defenses to provide added protection.
Defense in depth increases security by raising the effort needed in an attack. This strategy places multiple barriers between an attacker and an enterprise's computing and information resources.
CHINESE SIMPLIFIED: 纵深防御

Degauss The application of variable levels of alternating current for the purpose of demagnetizing magnetic recording media Scope Note: The process involves increasing the alternating current field gradually from zero to some maximum value and back to zero, leaving a very low residue of magnetic induction on the media. Degauss loosely means to erase.
CHINESE SIMPLIFIED: 消磁

Demilitarized zone (DMZ) A screened (firewalled) network segment that acts as a buffer zone between a trusted and untrusted network Scope Note: A DMZ is typically used to house systems such as web servers that must be accessible from both internal networks and the Internet.
CHINESE SIMPLIFIED: 非军事区

Demodulation The process of converting an analog telecommunications signal into a digital computer signal
CHINESE SIMPLIFIED: 解调

Demographic A fact determined by measuring and analyzing data about a population; it relies heavily on survey research and census data.
CHINESE SIMPLIFIED: 人口统计

Denial-of-service attack (DoS) An assault on a service from a single source that floods it with so many requests that it becomes overwhelmed and is either stopped completely or operates at a significantly reduced rate
CHINESE SIMPLIFIED: 拒绝服务攻击

Depreciation The process of cost allocation that assigns the original cost of equipment to the periods benefited Scope Note: The most common method of calculating depreciation is the straight-line method, which assumes that assets should be written off in equal amounts over their lives.
CHINESE SIMPLIFIED: 折旧

Detailed IS controls Controls over the acquisition, implementation, delivery and support of IS systems and services made up of application controls plus those general controls not included in pervasive controls
CHINESE SIMPLIFIED: 详细 IS 控制

Detection risk The risk that the IS audit or assurance professional's substantive procedures will not detect an error that could be material, individually or in combination with other errors Scope Note: See audit risk
CHINESE SIMPLIFIED: 检查风险

Detective application controls Designed to detect errors that may have occurred based on predefined logic or business rules.
Usually executed after an action has taken place and often cover a group of transactions
CHINESE SIMPLIFIED: 检测性应用程序控制

Detective control Exists to detect and report when errors, omissions and unauthorized uses or entries occur
CHINESE SIMPLIFIED: 检测性控制

Device A generic term for a computer subsystem, such as a printer, serial port or disk drive.
A device frequently requires its own controlling software, called a device driver.
CHINESE SIMPLIFIED: 设备

© 2015 ISACA All rights reserved.

Dial-back Used as a control over dial-up telecommunications lines. The telecommunications link established through dial-up into the computer from a remote location is interrupted so the computer can dial back to the caller. The link is permitted only if the caller is calling from a valid phone number or telecommunications channel.
CHINESE SIMPLIFIED: 回拨

Dial-in access control Prevents unauthorized access from remote users who attempt to access a secured environment.
Ranges from a dial-back control to remote user authentication
CHINESE SIMPLIFIED: 拨入访问控制

Digital certificate A piece of information, a digitized form of signature, that provides sender authenticity, message integrity and non-repudiation. A digital signature is generated using the sender's private key or applying a one-way hash function.
CHINESE SIMPLIFIED: 数字证书

Digital certification A process to authenticate (or certify) a party's digital signature; carried out by trusted third parties
CHINESE SIMPLIFIED: 数字认证

Digital code signing The process of digitally signing computer code to ensure its integrity
CHINESE SIMPLIFIED: 数字代码签名

Digital forensics The process of identifying, preserving, analyzing and presenting digital evidence in a manner that is legally acceptable in any legal proceedings
CHINESE SIMPLIFIED: 数字取证

Digital signature A piece of information, a digitized form of signature, that provides sender authenticity, message integrity and non-repudiation.
A digital signature is generated using the sender's private key or applying a one-way hash function.
CHINESE SIMPLIFIED: 数字签名

Direct reporting engagement An engagement in which management does not make a written assertion about the effectiveness of their control procedures and an IS auditor provides an opinion about subject matter directly, such as the effectiveness of the control procedures
CHINESE SIMPLIFIED: 直接报告业务

Disaster 1. A sudden, unplanned calamitous event causing great damage or loss. Any event that creates an inability on an enterprise's part to provide critical business functions for some predetermined period of time. Similar terms are business interruption, outage and catastrophe. 2. The period when enterprise management decides to divert from normal production responses and exercises its disaster recovery plan (DRP). It typically signifies the beginning of a move from a primary location to an alternate location.
CHINESE SIMPLIFIED: 灾难

Disaster declaration The communication to appropriate internal and external parties that the disaster recovery plan (DRP) is being put into operation
CHINESE SIMPLIFIED: 灾难宣告

Disaster notification fee The fee that the recovery site vendor charges when the customer notifies them that a disaster has occurred and the recovery site is required Scope Note: The fee is implemented to discourage false disaster notifications.
CHINESE SIMPLIFIED: 灾难声明费用

Disaster recovery Activities and programs designed to return the enterprise to an acceptable condition.
The ability to respond to an interruption in services by implementing a disaster recovery plan (DRP) to restore an enterprise's critical business functions
CHINESE SIMPLIFIED: 灾难恢复

Disaster recovery plan (DRP) desk checking Typically a read-through of a disaster recovery plan (DRP) without any real actions taking place Scope Note: Generally involves a reading of the plan, discussion of the action items and definition of any gaps that might be identified
CHINESE SIMPLIFIED: 灾难恢复计划（DRP）桌面演练

Disaster recovery plan (DRP) A set of human, physical, technical and procedural resources to recover, within a defined time and cost, an activity interrupted by an emergency or disaster
CHINESE SIMPLIFIED: 灾难恢复计划

Disaster recovery plan (DRP) walk-through Generally a robust test of the recovery plan requiring that some recovery activities take place and are tested.
A disaster scenario is often given and the recovery teams talk through the steps that they would need to take to recover. As many aspects of the plan as possible should be tested
CHINESE SIMPLIFIED: 灾难恢复计划（DRP）穿行测试

Disaster tolerance The time gap during which the business can accept the non-availability of IT facilities
CHINESE SIMPLIFIED: 容灾

Disclosure controls and procedures The processes in place designed to help ensure that all material information is disclosed by an enterprise in the reports that it files or submits to the U.S. Security and Exchange Commission (SEC) Scope Note: Disclosure Controls and Procedures also require that disclosures be authorized, complete and accurate, and recorded, processed, summarized and reported within the time periods specified in the SEC rules and forms. Deficiencies in controls, and any significant changes to controls, must be communicated to the enterprise's audit committee and auditors in a timely manner. An enterprise's principal executive officer and financial officer must certify the existence of these controls on a quarterly basis.
CHINESE SIMPLIFIED: 披露控制和程序

© 2015 ISACA All rights reserved.

Discount rate An interest rate used to calculate a present value which might or might not include the time value of money, tax effects, risk or other factors
CHINESE SIMPLIFIED: **贴现率**

Discovery sampling A form of attribute sampling that is used to determine a specified probability of finding at least one example of an occurrence (attribute) in a population
CHINESE SIMPLIFIED: **发现取样**

Discretionary access control (DAC) A means of restricting access to objects based on the identity of subjects and/or groups to which they belong Scope Note: The controls are discretionary in the sense that a subject with a certain access permission is capable of passing that permission (perhaps indirectly) on to any other subject.
CHINESE SIMPLIFIED: **自主访问控制 (DAC)**

Disk mirroring The practice of duplicating data in separate volumes on two hard disks to make storage more fault tolerant. Mirroring provides data protection in the case of disk failure because data are constantly updated to both disks.
CHINESE SIMPLIFIED: **磁盘镜像**

Diskless workstations A workstation or PC on a network that does not have its own disk, but instead stores files on a network file server
CHINESE SIMPLIFIED: **无盘工作站**

Distributed data processing network A system of computers connected together by a communication network Scope Note: Each computer processes its data and the network supports the system as a whole. Such a network enhances communication among the linked computers and allows access to shared files.
CHINESE SIMPLIFIED: **分布式数据处理网络**

Distributed denial-of-service attack (DDoS) A denial-of-service (DoS) assault from multiple sources
CHINESE SIMPLIFIED: **分布式拒绝服务攻击 (DDoS)**

Diverse routing The method of routing traffic through split cable facilities or duplicate cable facilities Scope Note: This can be accomplished with different and/or duplicate cable sheaths. If different cable sheaths are used, the cable may be in the same conduit and, therefore, subject to the same interruptions as the cable it is backing up. The communication service subscriber can duplicate the facilities by having alternate routes, although the entrance to and from the customer premises may be in the same conduit. The subscriber can obtain diverse routing and alternate routing from the local carrier, including dual entrance facilities. However, acquiring this type of access is time-consuming and costly. Most carriers provide facilities for alternate and diverse routing, although the majority of services are transmitted over terrestrial media. These cable facilities are usually located in the ground or basement. Ground-based facilities are at great risk due to the aging infrastructures of cities. In addition, cable-based facilities usually share room with mechanical and electrical systems that can impose great risk due to human error and disastrous events.
CHINESE SIMPLIFIED: **多样化路由**

Domain In COBIT, the grouping of control objectives into four logical stages in the life cycle of investments involving IT (Plan and Organise, Acquire and Implement, Deliver and Support, and Monitor and Evaluate)
CHINESE SIMPLIFIED: **领域**

Domain name system (DNS) A hierarchical database that is distributed across the Internet that allows names to be resolved into IP addresses (and vice versa) to locate services such as web and e-mail servers
CHINESE SIMPLIFIED: **域名系统 (DNS)**

Domain name system (DNS) exfiltration
Tunneling over DNS to gain network access. Lower-level attack vector for simple to complex data transmission, slow but difficult to detect.
CHINESE SIMPLIFIED: **域名系统渗出**

Domain name system (DNS) poisoning
Corrupts the table of an Internet server's DNS, replacing an Internet address with the address of another vagrant or scoundrel address Scope Note: If a web user looks for the page with that address, the request is redirected by the scoundrel entry in the table to a different address. Cache poisoning differs from another form of DNS poisoning in which the attacker spoofs valid e-mail accounts and floods the "in" boxes of administrative and technical contacts. Cache poisoning is related to URL poisoning or location poisoning, in which an Internet user behavior is tracked by adding an identification number to the location line of the browser that can be recorded as the user visits successive pages on the site. It is also called DNS cache poisoning or cache poisoning.
CHINESE SIMPLIFIED: **域名系统（DNS）中毒攻击**

Double-loop step Integrates the management of tactics (financial budgets and monthly reviews) and the management of strategy Scope Note: A reporting system, based on the balanced scorecard (BSC), that allows process to be monitored against strategy and corrective actions to be taken as required
CHINESE SIMPLIFIED: **双循环措施**

© 2015 ISACA All rights reserved.

Downloading The act of transferring computerized information from one computer to another computer
CHINESE SIMPLIFIED: 下载

Downtime report A report that identifies the elapsed time when a computer is not operating correctly because of machine failure
CHINESE SIMPLIFIED: 故障报告

Driver (value and risk) A driver includes an event or other activity that results in the identification of an assurance/audit need
CHINESE SIMPLIFIED: 驱动因素（价值和风险）

Dry-pipe fire extinguisher system Refers to a sprinkler system that does not have water in the pipes during idle usage, unlike a fully charged fire extinguisher system that has water in the pipes at all times Scope Note: The dry-pipe system is activated at the time of the fire alarm and water is emitted to the pipes from a water reservoir for discharge to the location of the fire.
CHINESE SIMPLIFIED: 干管灭火系统

Dual control A procedure that uses two or more entities (usually persons) operating in concert to protect a system resource so that no single entity acting alone can access that resource
CHINESE SIMPLIFIED: 双重控制

Due care The level of care expected from a reasonable person of similar competency under similar conditions
CHINESE SIMPLIFIED: 适当关注

Due diligence The performance of those actions that are generally regarded as prudent, responsible and necessary to conduct a thorough and objective investigation, review and/or analysis
CHINESE SIMPLIFIED: 适当调查

Due professional care Diligence that a person, who possesses a special skill, would exercise under a given set of circumstances
CHINESE SIMPLIFIED: 应有的职业谨慎

Dumb terminal A display terminal without processing capability Scope Note: Dumb terminals are dependent on the main computer for processing. All entered data are accepted without further editing or validation.
CHINESE SIMPLIFIED: 哑终端

Duplex routing The method or communication mode of routing data over the communication network
CHINESE SIMPLIFIED: 复用路由

Dynamic analysis Analysis that is performed in a real-time or continuous form
CHINESE SIMPLIFIED: 动态分析

Dynamic Host Configuration Protocol (DHCP) A protocol used by networked computers (clients) to obtain IP addresses and other parameters such as the default gateway, subnet mask and IP addresses of domain name system (DNS) servers from a DHCP server Scope Note: The DHCP server ensures that all IP addresses are unique (e.g., no IP address is assigned to a second client while the first client's assignment is valid [its lease has not expired]). Thus, IP address pool management is done by the server and not by a human network administrator.
CHINESE SIMPLIFIED: 动态主机配置协议

Dynamic partitioning The variable allocation of central processing unit (CPU) processing and memory to multiple applications and data on a server
CHINESE SIMPLIFIED: 动态分区

Dynamic ports Dynamic and/or private ports--49152 through 65535: Not listed by IANA because of their dynamic nature.
CHINESE SIMPLIFIED: 动态端口

E

Eavesdropping Listening a private communication without permission
CHINESE SIMPLIFIED: 窃听

Echo checks Detects line errors by retransmitting data back to the sending device for comparison with the original transmission
CHINESE SIMPLIFIED: 回送校验

E-commerce The processes by which enterprises conduct business electronically with their customers, suppliers and other external business partners, using the Internet as an enabling technology Scope Note: E-commerce encompasses both business-to-business (B2B) and business-to-consumer (B2C) e-commerce models, but does not include existing non-Internet e-commerce methods based on private networks such as electronic data interchange (EDI) and Society for Worldwide Interbank Financial Telecommunication (SWIFT).
CHINESE SIMPLIFIED: 电子商务

Economic value add (EVA) Technique developed by G. Bennett Stewart III and registered by the consulting firm of Stern, Stewart, in which the performance of the corporate capital base (including depreciated investments such as training, research and development) as well as more traditional capital investments such as physical property and equipment are measured against what shareholders could earn elsewhere
CHINESE SIMPLIFIED: 经济附加值 (EVA)

Edit control Detects errors in the input portion of information that is sent to the computer for processing. May be manual or automated and allow the user to edit data errors before processing
CHINESE SIMPLIFIED: 编辑控制

© 2015 ISACA All rights reserved.

Editing Ensures that data conform to predetermined criteria and enable early identification of potential errors
CHINESE SIMPLIFIED: **编辑**

Egress Network communications going out
CHINESE SIMPLIFIED: **出口**

Electronic data interchange (EDI) The electronic transmission of transactions (information) between two enterprises.
EDI promotes a more efficient paperless environment. EDI transmissions can replace the use of standard documents, including invoices or purchase orders.
CHINESE SIMPLIFIED: **电子数据交换 (EDI)**

Electronic document An administrative document (a document with legal validity, such as a contract) in any graphical, photographic, electromagnetic (tape) or other electronic representation of the content Scope Note: Almost all countries have developed legislation concerning the definition, use and legal validity of an electronic document. An electronic document, in whatever media that contains the data or information used as evidence of a contract or transaction between parties, is considered together with the software program capable to read it. The definition of a legally valid document as any representation of legally relevant data, not only those printed on paper, was introduced into the legislation related to computer crime. In addition, many countries in defining and disciplining the use of such instruments have issued regulations defining specifics, such as the electronic signature and data interchange formats.
CHINESE SIMPLIFIED: **电子文档**

Electronic funds transfer (EFT) The exchange of money via telecommunications.
EFT refers to any financial transaction that originates at a terminal and transfers a sum of money from one account to another
CHINESE SIMPLIFIED: **电子资金转账**

Electronic signature Any technique designed to provide the electronic equivalent of a handwritten signature to demonstrate the origin and integrity of specific data.
Digital signatures are an example of electronic signatures.
CHINESE SIMPLIFIED: **电子签名**

Electronic vaulting A data recovery strategy that allows enterprises to recover data within hours after a disaster Scope Note: Typically used for batch/journal updates to critical files to supplement full backups taken periodically; includes recovery of data from an offsite storage media that mirrors data via a communication link
CHINESE SIMPLIFIED: **电子链接 数据恢复 电子传送（异地备份）**

Elliptical curve cryptography (ECC) An algorithm that combines plane geometry with algebra to achieve stronger authentication with smaller keys compared to traditional methods, such as RSA, which primarily use algebraic factoring. Scope Note: Smaller keys are more suitable to mobile devices.
CHINESE SIMPLIFIED: **椭圆曲线加密算法**

Embedded audit module (EAM) Integral part of an application system that is designed to identify and report specific transactions or other information based on pre-determined criteria.
Identification of reportable items occurs as part of real-time processing. Reporting may be real-time online or may use store and forward methods. Also known as integrated test facility or continuous auditing module.
CHINESE SIMPLIFIED: **嵌入式审计模块**

Encapsulation (objects) The technique used by layered protocols in which a lower-layer protocol accepts a message from a higher-layer protocol and places it in the data portion of a frame in the lower layer
CHINESE SIMPLIFIED: **封装 (对象)**

Encapsulation security payload (ESP) Protocol, which is designed to provide a mix of security services in IPv4 and IPv6. ESP can be used to provide confidentiality, data origin authentication, connectionless integrity, an anti-replay service (a form of partial sequence integrity), and (limited) traffic flow confidentiality. (RFC 4303) Scope Note: The ESP header is inserted after the IP header and before the next layer protocol header (transport mode) or before an encapsulated IP header (tunnel mode).
CHINESE SIMPLIFIED: **封装安全有效载荷**

Encryption The process of taking an unencrypted message (plaintext), applying a mathematical function to it (encryption algorithm with a key) and producing an encrypted message (ciphertext)
CHINESE SIMPLIFIED: **加密**

Encryption algorithm A mathematically based function orthat encrypts/decrypts data
CHINESE SIMPLIFIED: **加密算法**

Encryption key A piece of information, in a digitized form, used by an encryption algorithm to convert the plaintext to the ciphertext
CHINESE SIMPLIFIED: **密钥**

End-user computing The ability of end users to design and implement their own information system utilizing computer software products
CHINESE SIMPLIFIED: **最终用户计算**

Engagement letter Formal document which defines an IS auditor's responsibility, authority and accountability for a specific assignment
CHINESE SIMPLIFIED: **审计业务约定书**

Enterprise A group of individuals working together for a common purpose, typically within the context of an organizational form such as a corporation, public agency, charity or trust
CHINESE SIMPLIFIED: **企业**

© 2015 ISACA All rights reserved.

Enterprise architecture (EA) Description of the fundamental underlying design of the components of the business system, or of one element of the business system (e.g., technology), the relationships among them, and the manner in which they support the enterprise's objectives
CHINESE SIMPLIFIED: **企业架构 (EA)**

Enterprise architecture (EA) for IT Description of the fundamental underlying design of the IT components of the business, the relationships among them, and the manner in which they support the enterprise's objectives
CHINESE SIMPLIFIED: **企业 IT 架构**

Enterprise goal Scope Note: See Business goal
CHINESE SIMPLIFIED: **企业目标**

Enterprise governance A set of responsibilities and practices exercised by the board and executive management with the goal of providing strategic direction, ensuring that objectives are achieved, ascertaining that risk is managed appropriately and verifying that the enterprise's resources are used responsibly
CHINESE SIMPLIFIED: **企业治理**

Enterprise risk management (ERM) The discipline by which an enterprise in any industry assesses, controls, exploits, finances and monitors risk from all sources for the purpose of increasing the enterprise's short- and long-term value to its stakeholders
CHINESE SIMPLIFIED: **企业风险管理**

Eradication When containment measures have been deployed after an incident occurs, the root cause of the incident must be identified and removed from the network. Scope Note: Eradication methods include: restoring backups to achieve a clean state of the system, removing the root cause, improving defenses and performing vulnerability analysis to find further potential damage from the same root cause.
CHINESE SIMPLIFIED: **根除**

ERP (enterprise resource planning) system A packaged business software system that allows an enterprise to automate and integrate the majority of its business processes, share common data and practices across the entire enterprise, and produce and access information in a real-time environment Scope Note: Examples of ERP include SAP, Oracle Financials and J.D. Edwards.
CHINESE SIMPLIFIED: **ERP（企业资源规划）系统**

Error A deviation from accuracy or correctness Scope Note: As it relates to audit work, errors may relate to control deviations (compliance testing) or misstatements (substantive testing).
CHINESE SIMPLIFIED: **错误**

Escrow agent A person, agency or enterprise that is authorized to act on behalf of another to create a legal relationship with a third party in regard to an escrow agreement; the custodian of an asset according to an escrow agreement Scope Note: As it relates to a cryptographic key, an escrow agent is the agency or enterprise charged with the responsibility for safeguarding the key components of the unique key.
CHINESE SIMPLIFIED: **第三方托管代理**

Escrow agreement A legal arrangement whereby an asset (often money, but sometimes other property such as art, a deed of title, web site, software source code or a cryptographic key) is delivered to a third party (called an escrow agent) to be held in trust or otherwise pending a contingency or the fulfillment of a condition or conditions in a contract Scope Note: Upon the occurrence of the escrow agreement, the escrow agent will deliver the asset to the proper recipient; otherwise the escrow agent is bound by his/her fiduciary duty to maintain the escrow account. Source code escrow means deposit of the source code for the software into an account held by an escrow agent. Escrow is typically requested by a party licensing software (e.g., licensee or buyer), to ensure maintenance of the software. The software source code is released by the escrow agent to the licensee if the licensor (e.g., seller or contractor) files for bankruptcy or otherwise fails to maintain and update the software as promised in the software license agreement.
CHINESE SIMPLIFIED: **第三方托管协议**

Ethernet A popular network protocol and cabling scheme that uses a bus topology and carrier sense multiple access/collision detection (CSMA/CD) to prevent network failures or collisions when two devices try to access the network at the same time
CHINESE SIMPLIFIED: **以太网络**

Event Something that happens at a specific place and/or time
CHINESE SIMPLIFIED: **事件**

Event type For the purpose of IT risk management, one of three possible sorts of events: threat event, loss event and vulnerability event Scope Note: Being able to consistently and effectively differentiate the different types of events that contribute to risk is a critical element in developing good risk-related metrics and well-informed decisions. Unless these categorical differences are recognized and applied, any resulting metrics lose meaning and, as a result, decisions based on those metrics are far more likely to be flawed.
CHINESE SIMPLIFIED: **事件类型**

Evidence 1. Information that proves or disproves a stated issue 2. Information that an auditor gathers in the course of performing an IS audit; relevant if it pertains to the audit objectives and has a logical relationship to the findings and conclusions it is used to support Scope Note: Audit perspective
CHINESE SIMPLIFIED: **证据**

© 2015 ISACA All rights reserved.

Exception reports An exception report is generated by a program that identifies transactions or data that appear to be incorrect. Scope Note: Exception reports may be outside a predetermined range or may not conform to specified criteria.
CHINESE SIMPLIFIED: **异常报告**

Exclusive-OR (XOR) The exclusive-OR operator returns a value of TRUE only if just one of its operands is TRUE. Scope Note: The XOR operation is a Boolean operation that produces a 0 if its two Boolean inputs are the same (0 and 0 or 1 and 1) and that produces a 1 if its two inputs are different (1 and 0). In contrast, an inclusive-OR operator returns a value of TRUE if either or both of its operands are TRUE.
CHINESE SIMPLIFIED: **异或 (XOR)**

Executable code The machine language code that is generally referred to as the object or load module
CHINESE SIMPLIFIED: **可执行代码**

Expert system The most prevalent type of computer system that arises from the research of artificial intelligence Scope Note: An expert system has a built in hierarchy of rules, which are acquired from human experts in the appropriate field. Once input is provided, the system should be able to define the nature of the problem and provide recommendations to solve the problem.
CHINESE SIMPLIFIED: **专家系统**

Exploit Full use of a vulnerability for the benefit of an attacker
CHINESE SIMPLIFIED: **利用**

Exposure The potential loss to an area due to the occurrence of an adverse event
CHINESE SIMPLIFIED: **暴露（风险）**

Extended Binary-coded for Decimal Interchange Code (EBCDIC) An 8-bit code representing 256 characters; used in most large computer systems
CHINESE SIMPLIFIED: **扩展二进制编码的十进制交换码 (EBCDIC)**

Extended enterprise Describes an enterprise that extends outside its traditional boundaries. Such enterprise concentrate on the processes they do best and rely on someone outside the entity to perform the remaining processes.
CHINESE SIMPLIFIED: **扩展型企业**

eXtensible Access Control Markup Language (XACML) A declarative online software application user access control policy language implemented in Extensible Markup Language (XML)
CHINESE SIMPLIFIED: **可扩展式访问控制标记语言 (XACML)**

eXtensible Markup Language (XML) Promulgated through the World Wide Web Consortium, XML is a web-based application development technique that allows designers to create their own customized tags, thus, enabling the definition, transmission, validation and interpretation of data between applications and enterprises.
CHINESE SIMPLIFIED: **可扩展标记语言**

External router The router at the extreme edge of the network under control, usually connected to an Internet service provider (ISP) or other service provider; also known as border router.
CHINESE SIMPLIFIED: **外部路由器**

External storage The location that contains the backup copies to be used in case recovery or restoration is required in the event of a disaster
CHINESE SIMPLIFIED: **外部存储**

Extranet A private network that resides on the Internet and allows a company to securely share business information with customers, suppliers or other businesses as well as to execute electronic transactions Scope Note: Different from an Intranet in that it is located beyond the company's firewall. Therefore, an extranet relies on the use of securely issued digital certificates (or alternative methods of user authentication) and encryption of messages. A virtual private network (VPN) and tunneling are often used to implement extranets, to ensure security and privacy.
CHINESE SIMPLIFIED: **外联网**

F

Fail-over The transfer of service from an incapacitated primary component to its backup component
CHINESE SIMPLIFIED: **故障切换**

Fail-safe Describes the design properties of a computer system that allow it to resist active attempts to attack or bypass it
CHINESE SIMPLIFIED: **故障保险**

Fallback procedures A plan of action or set of procedures to be performed if a system implementation, upgrade or modification does not work as intended Scope Note: May involve restoring the system to its state prior to the implementation or change. Fallback procedures are needed to ensure that normal business processes continue in the event of failure and should always be considered in system migration or implementation.
CHINESE SIMPLIFIED: **回退程序**

Fall-through logic An optimized code based on a branch prediction that predicts which way a program will branch when an application is presented
CHINESE SIMPLIFIED: **贯穿逻辑**

False authorization Also called false acceptance, occurs when an unauthorized person is identified as an authorized person by the biometric system
CHINESE SIMPLIFIED: **伪授权**

© 2015 ISACA All rights reserved.

False enrollment Occurs when an unauthorized person manages to enroll into the biometric system Scope Note: Enrollment is the initial process of acquiring a biometric feature and saving it as a personal reference on a smart card, a PC or in a central database.
CHINESE SIMPLIFIED: 伪登记

False negative In intrusion detection, an error that occurs when an attack is misdiagnosed as a normal activity
CHINESE SIMPLIFIED: 负误识

False positive A result that has been mistakenly identified as a problem when, in reality, the situation is normal
CHINESE SIMPLIFIED: 正误识

Fault tolerance A system's level of resilience to seamlessly react to hardware and/or software failure
CHINESE SIMPLIFIED: 容错

Feasibility study A phase of a system development life cycle (SDLC) methodology that researches the feasibility and adequacy of resources for the development or acquisition of a system solution to a user need
CHINESE SIMPLIFIED: 可行性分析

Fiber-optic cable Glass fibers that transmit binary signals over a telecommunications network Scope Note: Fiber-optic systems have low transmission losses as compared to twisted-pair cables. They do not radiate energy or conduct electricity. They are free from corruption and lightning-induced interference, and they reduce the risk of wiretaps.
CHINESE SIMPLIFIED: 光纤传输线路（光缆）

Field An individual data element in a computer record Scope Note: Examples include employee name, customer address, account number, product unit price and product quantity in stock.
CHINESE SIMPLIFIED: 字段

File A named collection of related records
CHINESE SIMPLIFIED: 文件

File allocation table (FAT) A table used by the operating system to keep track of where every file is located on the disk Scope Note: Since a file is often fragmented and thus subdivided into many sectors within the disk, the information stored in the FAT is used when loading or updating the contents of the file.
CHINESE SIMPLIFIED: 文件分配表（FAT）

File layout Specifies the length of the file record and the sequence and size of its fields Scope Note: Also will specify the type of data contained within each field; for example, alphanumeric, zoned decimal, packed and binary.
CHINESE SIMPLIFIED: 文件结构

File server A high-capacity disk storage device or a computer that stores data centrally for network users and manages access to those data Scope Note: File servers can be dedicated so that no process other than network management can be executed while the network is available; file servers can be non-dedicated so that standard user applications can run while the network is available.
CHINESE SIMPLIFIED: 文件服务器

File Transfer Protocol (FTP) A protocol used to transfer files over a Transmission Control Protocol/Internet Protocol (TCP/IP) network (Internet, UNIX, etc.)
CHINESE SIMPLIFIED: 文件传输协议

Filtering router A router that is configured to control network access by comparing the attributes of the incoming or outgoing packets to a set of rules
CHINESE SIMPLIFIED: 过滤路由器

FIN (Final) A flag set in a packet to indicate that this packet is the final data packet of the transmission
CHINESE SIMPLIFIED: FIN（最终）

Financial audit An audit designed to determine the accuracy of financial records and information
CHINESE SIMPLIFIED: 财务审计

Finger A protocol and program that allows the remote identification of users logged into a system
CHINESE SIMPLIFIED: Finger

Firewall A system or combination of systems that enforces a boundary between two or more networks, typically forming a barrier between a secure and an open environment such as the Internet
CHINESE SIMPLIFIED: 防火墙

Firmware Memory chips with embedded program code that hold their content when power is turned off
CHINESE SIMPLIFIED: 固件

Fiscal year Any yearly accounting period without regard to its relationship to a calendar year
CHINESE SIMPLIFIED: 财政年度

Foreign key A value that represents a reference to a tuple (a row in a table) containing the matching candidate key value Scope Note: The problem of ensuring that the database does not include any invalid foreign key values is known as the referential integrity problem. The constraint that values of a given foreign key must match values of the corresponding candidate key is known as a referential constraint. The relation (table) that contains the foreign key is referred to as the referencing relation and the relation that contains the corresponding candidate key as the referenced relation or target relation. (In the relational theory it would be a candidate key, but in real database management systems (DBMSs) implementations it is always the primary key.)
CHINESE SIMPLIFIED: 外键

© 2015 ISACA All rights reserved.

Forensic examination The process of collecting, assessing, classifying and documenting digital evidence to assist in the identification of an offender and the method of compromise
CHINESE SIMPLIFIED: **司法鉴定**

Format checking The application of an edit, using a predefined field definition to a submitted information stream; a test to ensure that data conform to a predefined format
CHINESE SIMPLIFIED: **格式检验**

Fourth-generation language (4GL) High-level, user-friendly, nonprocedural computer language used to program and/or read and process computer files
CHINESE SIMPLIFIED: **第四代语言 (4GL)**

Frame relay A packet-switched wide-area-network (WAN) technology that provides faster performance than older packet-switched WAN technologies Scope Note: Best suited for data and image transfers. Because of its variable-length packet architecture, it is not the most efficient technology for real-time voice and video. In a frame-relay network, end nodes establish a connection via a permanent virtual circuit (PVC).
CHINESE SIMPLIFIED: **帧中继**

Framework Scope Note: See Control framework and IT governance framework.
CHINESE SIMPLIFIED: **框架**

Freeware Software available free of charge
CHINESE SIMPLIFIED: **免费软件**

Frequency A measure of the rate by which events occur over a certain period of time
CHINESE SIMPLIFIED: **频率**

Full economic life cycle The period of time during which material business benefits are expected to arise from, and/or during which material expenditures (including investments, running and retirement costs) are expected to be incurred by, an investment program Scope Note: COBIT 5 perspective
CHINESE SIMPLIFIED: **完整经济生命周期**

Function point analysis A technique used to determine the size of a development task, based on the number of function points Scope Note: Function points are factors such as inputs, outputs, inquiries and logical internal sites.
CHINESE SIMPLIFIED: **功能指数分析**

G

Gateway A device (router, firewall) on a network that serves as an entrance to another network
CHINESE SIMPLIFIED: **网关**

General computer control A Control, other than an application control, that relates to the environment within which computer-based application systems are developed, maintained and operated, and that is therefore applicable to all applications.
The objectives of general controls are to ensure the proper development and implementation of applications and the integrity of program and data files and of computer operations. Like application controls, general controls may be either manual or programmed. Examples of general controls include the development and implementation of an IS strategy and an IS security policy, the organization of IS staff to separate conflicting duties and planning for disaster prevention and recovery.
CHINESE SIMPLIFIED: **通用计算机控制**

Generalized audit software (GAS)
Multipurpose audit software that can be used for general processes, such as record selection, matching, recalculation and reporting
CHINESE SIMPLIFIED: **通用审计软件**

Generic process control A control that applies to all processes of the enterprise
CHINESE SIMPLIFIED: **通用流程控制**

Geographic disk mirroring A data recovery strategy that takes a set of physically disparate disks and synchronously mirrors them over high-performance communication lines.
Any write to a disk on one side will result in a write on the other side. The local write will not return until the acknowledgment of the remote write is successful.
CHINESE SIMPLIFIED: **地理磁盘镜像**

Geographical information system (GIS) A tool used to integrate, convert, handle, analyze and produce information regarding the surface of the earth Scope Note: GIS data exist as maps, tri-dimensional virtual models, lists and tables
CHINESE SIMPLIFIED: **地理信息系统 (GIS)**

Good practice A proven activity or process that has been successfully used by multiple enterprises and has been shown to produce reliable results
CHINESE SIMPLIFIED: **良好实践**

Governance Ensures that stakeholder needs, conditions and options are evaluated to determine balanced, agreed-on enterprise objectives to be achieved; setting direction through prioritization and decision making; and monitoring performance and compliance against agreed-on direction and objectives Scope Note: Conditions can include the cost of capital, foreign exchange rates, etc. Options can include shifting manufacturing to other locations, sub-contracting portions of the enterprise to third-parties, selecting a product mix from many available choices, etc.
CHINESE SIMPLIFIED: **治理**

Governance enabler Something (tangible or intangible) that assists in the realization of effective governance Scope Note: COBIT 5 perspective
CHINESE SIMPLIFIED: **治理启动者**

© 2015 ISACA All rights reserved.

Governance framework A framework is a basic conceptual structure used to solve or address complex issues. An enabler of governance. A set of concepts, assumptions and practices that define how something can be approached or understood, the relationships amongst the entities involved, the roles of those involved, and the boundaries (what is and is not included in the governance system). Scope Note: Examples: COBIT, COSO's Internal Control--Integrated Framework
CHINESE SIMPLIFIED: 治理框架

Governance of enterprise IT A governance view that ensures that information and related technology support and enable the enterprise strategy and the achievement of enterprise objectives; this also includes the functional governance of IT, i.e., ensuring that IT capabilities are provided efficiently and effectively. Scope Note: COBT 5 perspective
CHINESE SIMPLIFIED: 企业 IT 治理

Governance, Risk Management and Compliance (GRC) A business term used to group the three close-related disciplines responsible for the protection of assets, and operations
CHINESE SIMPLIFIED: 治理、风险管理和合规

Governance/ management practice For each COBIT process, the governance and management practices provide a complete set of high-level requirements for effective and practical governance and management of enterprise IT. They are statements of actions from governance bodies and management. Scope Note: COBIT 5 perspective
CHINESE SIMPLIFIED: 治理/管理实践

Guideline A description of a particular way of accomplishing something that is less prescriptive than a procedure
CHINESE SIMPLIFIED: 准则

H

Hacker An individual who attempts to gain unauthorized access to a computer system
CHINESE SIMPLIFIED: 黑客

Handprint scanner A biometric device that is used to authenticate a user through palm scans
CHINESE SIMPLIFIED: 掌纹扫描仪

Harden To configure a computer or other network device to resist attacks
CHINESE SIMPLIFIED: 加固

Hardware The physical components of a computer system
CHINESE SIMPLIFIED: 硬件

Hash function An algorithm that maps or translates one set of bits into another (generally smaller) so that a message yields the same result every time the algorithm is executed using the same message as input Scope Note: It is computationally infeasible for a message to be derived or reconstituted from the result produced by the algorithm or to find two different messages that produce the same hash result using the same algorithm.
CHINESE SIMPLIFIED: 哈希函数

Hash total The total of any numeric data field in a document or computer file.
This total is checked against a control total of the same field to facilitate accuracy of processing.
CHINESE SIMPLIFIED: 散列校验和

Hashing Using a hash function (algorithm) to create hash valued or checksums that validate message integrity
CHINESE SIMPLIFIED: 散列

Help desk A service offered via telephone/Internet by an enterprise to its clients or employees that provides information, assistance and troubleshooting advice regarding software, hardware or networks. Scope Note: A help desk is staffed by people who can either resolve the problem on their own or escalate the problem to specialized personnel. A help desk is often equipped with dedicated customer relationship management (CRM) software that logs the problems and tracks them until they are solved.
CHINESE SIMPLIFIED: 服务台

Heuristic filter A method often employed by antispam software to filter spam using criteria established in a centralized rule database Scope Note: Every e-mail message is given a rank, based on its header and contents, which is then matched against preset thresholds. A message that surpasses the threshold will be flagged as spam and discarded, returned to its sender or put in a spam directory for further review by the intended recipient.
CHINESE SIMPLIFIED: 启发式过滤

Hexadecimal A numbering system that uses a base of 16 and uses 16 digits: 0, 1, 2, 3, 4, 5, 6, 7, 8, 9, A, B, C, D, E and F.
Programmers use hexadecimal numbers as a convenient way of representing binary numbers.
CHINESE SIMPLIFIED: 十六进制

Hierarchical database A database structured in a tree/root or parent/child relationship Scope Note: Each parent can have many children, but each child may have only one parent.
CHINESE SIMPLIFIED: 层次型数据库

Hijacking An exploitation of a valid network session for unauthorized purposes
CHINESE SIMPLIFIED: 劫持

© 2015 ISACA All rights reserved.

Honeypot A specially configured server, also known as a decoy server, designed to attract and monitor intruders in a manner such that their actions do not affect production systems Scope Note: Also known as "decoy server"
CHINESE SIMPLIFIED: **蜜罐**

Horizontal defense-in depth Controls are placed in various places in the path to access an asset (this is functionally equivalent to concentric ring model above).
CHINESE SIMPLIFIED: **水平纵深防御**

Hot site A fully operational offsite data processing facility equipped with both hardware and system software to be used in the event of a disaster
CHINESE SIMPLIFIED: **热站**

Hub A common connection point for devices in a network, hubs are used to connect segments of a local area network (LAN) Scope Note: A hub contains multiple ports. When a packet arrives at one port, it is copied to the other ports so that all segments of the LAN can see all packets.
CHINESE SIMPLIFIED: **集线器**

Human firewall A person prepared to act as a network layer of defense through education and awareness
CHINESE SIMPLIFIED: **人身防火墙**

Hurdle rate Also known as required rate of return, above which an investment makes sense and below which it does not Scope Note: Often based on the cost of capital, plus or minus a risk premium, and often varied based on prevailing economic conditions
CHINESE SIMPLIFIED: **最低投资回报率**

Hybrid application controls Consist of a combination of manual and automated activities, all of which must operate for the control to be effective Scope Note: Sometimes referred to as computer-dependent application controls
CHINESE SIMPLIFIED: **混合应用程序控制**

Hyperlink An electronic pathway that may be displayed in the form of highlighted text, graphics or a button that connects one web page with another web page address
CHINESE SIMPLIFIED: **超链接**

Hypertext A language that enables electronic documents that present information to be connected by links instead of being presented sequentially, as is the case with normal text
CHINESE SIMPLIFIED: **超文本**

Hypertext Markup Language (HTML) A language designed for the creation of web pages with hypertext and other information to be displayed in a web browser; used to structure information--denoting certain text sure as headings, paragraphs, lists--and can be used to describe, to some degree, the appearance and semantics of a document
CHINESE SIMPLIFIED: **超文本链接标示语言**

Hypertext Transfer Protocol Secure (HTTPS) A protocol for accessing a secure web server, whereby all data transferred are encrypted.
CHINESE SIMPLIFIED: **安全超文本传输协议 (HTTPS)**

Hypertext Transfer Protocol (HTTP) A communication protocol used to connect to servers on the World Wide Web. Its primary function is to establish a connection with a web server and transmit hypertext markup language (HTML), extensible markup language (XML) or other pages to client browsers
CHINESE SIMPLIFIED: **超文本传输协议 (HTTP)**

I

Identity access management (IAM) Encapsulates people, processes and products to identify and manage the data used in an information system to authenticate users and grant or deny access rights to data and system resources. The goal of IAM is to provide appropriate access to enterprise resources.
CHINESE SIMPLIFIED: **身份识别访问管理 (IAM)**

Idle standby A fail-over process in which the primary node owns the resource group and the backup node runs idle, only supervising the primary node Scope Note: In case of a primary node outage, the backup node takes over. The nodes are prioritized, which means that the surviving node with the highest priority will acquire the resource group. A higher priority node joining the cluster will thus cause a short service interruption.
CHINESE SIMPLIFIED: **空闲待机**

IEEE (Institute of Electrical and Electronics Engineers) Pronounced I-triple-E; IEEE is an organization composed of engineers, scientists and students Scope Note: Best known for developing standards for the computer and electronics industry
CHINESE SIMPLIFIED: **IEEE（美国电气和电子工程师协会）**

IEEE 802.11 A family of specifications developed by the Institute of Electrical and Electronics Engineers (IEEE) for wireless local area network (WLAN) technology. 802.11 specifies an over-the-air interface between a wireless client and a base station or between two wireless clients.
CHINESE SIMPLIFIED: **802.11协议簇**

Image processing The process of electronically inputting source documents by taking an image of the document, thereby eliminating the need for key entry
CHINESE SIMPLIFIED: **图像处理**

Imaging A process that allows one to obtain a bit-for-bit copy of data to avoid damage of original data or information when multiple analyses may be performed. Scope Note: The imaging process is made to obtain residual data, such as deleted files, fragments of deleted files and other information present, from the disk for analysis. This is possible because imaging duplicates the disk surface, sector by sector.
CHINESE SIMPLIFIED: **数据镜像**

© 2015 ISACA All rights reserved.

Impact Magnitude of loss resulting from a threat exploiting a vulnerability
CHINESE SIMPLIFIED: **影响**

Impact analysis A study to prioritize the criticality of information resources for the enterprise based on costs (or consequences) of adverse events.
In an impact analysis, threats to assets are identified and potential business losses determined for different time periods. This assessment is used to justify the extent of safeguards that are required and recovery time frames. This analysis is the basis for establishing the recovery strategy.
CHINESE SIMPLIFIED: **影响分析**

Impact assessment A review of the possible consequences of a risk Scope Note: See also Impact analysis.
CHINESE SIMPLIFIED: **影响评估**

Impairment A condition that causes a weakness or diminished ability to execute audit objectives Scope Note: Impairment to organisational independence and individual objectivity may include personal conflict of interest; scope limitations; restrictions on access to records, personnel, equipment, or facilities; and resource limitations (such as funding or staffing).
CHINESE SIMPLIFIED: **减损**

Impersonation A security concept related to Windows NT that allows a server application to temporarily "be" the client in terms of access to secure objects Scope Note: Impersonation has three possible levels: identification, letting the server inspect the client's identity; impersonation, letting the server act on behalf of the client; and delegation, the same as impersonation but extended to remote systems to which the server connects (through the preservation of credentials). Impersonation by imitating or copying the identification, behavior or actions of another may also be used in social engineering to obtain otherwise unauthorized physical access.
CHINESE SIMPLIFIED: **模拟**

Implement In business, includes the full economic life cycle of the investment program through retirement; (i.e., when the full expected value of the investment is realized, as much value as is deemed possible has been realized, or it is determined that the expected value cannot be realized and the program is terminated)
CHINESE SIMPLIFIED: **实施**

Implementation life cycle review Refers to the controls that support the process of transformation of the enterprise's legacy information systems into the enterprise resource planning (ERP) applications Scope Note: Largely covers all aspects of systems implementation and configuration, such as change management
CHINESE SIMPLIFIED: **实施生命周期审查**

Incident Any event that is not part of the standard operation of a service and that causes, or may cause, an interruption to, or a reduction in, the quality of that service
CHINESE SIMPLIFIED: **事件**

Incident response The response of an enterprise to a disaster or other significant event that may significantly affect the enterprise, its people, or its ability to function productively.
An incident response may include evacuation of a facility, initiating a disaster recovery plan (DRP), performing damage assessment, and any other measures necessary to bring an enterprise to a more stable status.
CHINESE SIMPLIFIED: **事件响应**

Incident response plan The operational component of incident management Scope Note: The plan includes documented procedures and guidelines for defining the criticality of incidents, reporting and escalation process, and recovery procedures.
CHINESE SIMPLIFIED: **应急响应计划**

Inconsequential deficiency A deficiency is inconsequential if a reasonable person would conclude, after considering the possibility of further undetected deficiencies, that the deficiencies, either individually or when aggregated with other deficiencies, would clearly be trivial to the subject matter. If a reasonable person could not reach such a conclusion regarding a particular deficiency, that deficiency is more than inconsequential.
CHINESE SIMPLIFIED: **无关紧要缺陷**

Incremental testing Deliberately testing only the value-added functionality of a software component
CHINESE SIMPLIFIED: **增量测试**

Independence 1. Self-governance 2. The freedom from conditions that threaten objectivity or the appearance of objectivity. Such threats to objectivity must be managed at the individual auditor, engagement, functional and organizational levels. Independence includes Independence of mind and Independence in appearance. Scope Note: See Independence of mind and Independence in appearance.
CHINESE SIMPLIFIED: **独立性**

Independence in appearance The avoidance of facts and circumstances that are so significant that a reasonable and informed third party would be likely to conclude, weighing all the specific facts and circumstances, that a firm's, audit function's, or a member of the audit team's, integrity, objectivity or professional skepticism has been compromised.
CHINESE SIMPLIFIED: **形式独立性**

Independence of mind The state of mind that permits the expression of a conclusion without being affected by influences that compromise professional judgement, thereby allowing an individual to act with integrity and exercise objectivity and professional skepticism.
CHINESE SIMPLIFIED: **实质性独立**

Independent appearance The outward impression of being self-governing and free from conflict of interest and undue influence
CHINESE SIMPLIFIED: **独立外观**

© 2015 ISACA All rights reserved.

Independent attitude Impartial point of view which allows an IS auditor to act objectively and with fairness
CHINESE SIMPLIFIED: 中立态度

Indexed Sequential Access Method (ISAM) A disk access method that stores data sequentially while also maintaining an index of key fields to all the records in the file for direct access capability
CHINESE SIMPLIFIED: 索引顺序存取法（ISAM）

Indexed sequential file A file format in which records are organized and can be accessed, according to a pre-established key that is part of the record
CHINESE SIMPLIFIED: 索引顺序文件

Information An asset that, like other important business assets, is essential to an enterprise's business. It can exist in many forms. It can be printed or written on paper, stored electronically, transmitted by post or by using electronic means, shown on films, or spoken in conversation. Scope Note: COBIT 5 perspective
CHINESE SIMPLIFIED: 信息

Information architecture Information architecture is one component of IT architecture (together with applications and technology)
CHINESE SIMPLIFIED: 信息架构

Information criteria Attributes of information that must be satisfied to meet business requirements
CHINESE SIMPLIFIED: 信息衡量标准

Information engineering Data-oriented development techniques that work on the premise that data are at the center of information processing and that certain data relationships are significant to a business and must be represented in the data structure of its systems
CHINESE SIMPLIFIED: 信息工程

Information processing facility (IPF) The computer room and support areas
CHINESE SIMPLIFIED: 信息处理场所

Information security Ensures that within the enterprise, information is protected against disclosure to unauthorized users (confidentiality), improper modification (integrity), and non-access when required (availability)
CHINESE SIMPLIFIED: 信息安全

Information security governance The set of responsibilities and practices exercised by the board and executive management with the goal of providing strategic direction, ensuring that objectives are achieved, ascertaining that risk is managed appropriately and verifying that the enterprise's resources are used responsibly
CHINESE SIMPLIFIED: 信息安全治理

Information security program The overall combination of technical, operational and procedural measures and management structures implemented to provide for the confidentiality, integrity and availability of information based on business requirements and risk analysis
CHINESE SIMPLIFIED: 信息安全方案

Information systems (IS) The combination of strategic, managerial and operational activities involved in gathering, processing, storing, distributing and using information and its related technologies Scope Note: Information systems are distinct from information technology (IT) in that an information system has an IT component that interacts with the process components.
CHINESE SIMPLIFIED: 信息系统 (IS)

Information technology (IT) The hardware, software, communication and other facilities used to input, store, process, transmit and output data in whatever form
CHINESE SIMPLIFIED: 信息技术

Informed In a RACI chart (Responsible, Accountable, Consulted, Informed), Informed refers to those people who are kept up to date on the progress of an activity (one-way communication)
CHINESE SIMPLIFIED: 知情人

Infrastructure as a Service (IaaS) Offers the capability to provision processing, storage, networks and other fundamental computing resources, enabling the customer to deploy and run arbitrary software, which can include operating systems (OSs) and applications
CHINESE SIMPLIFIED: 基础架构即服务 (IaaS)

Ingestion A process to convert information extracted to a format that can be understood by investigators. Scope Note: See also Normalization.
CHINESE SIMPLIFIED: 规范化

Ingress Network communications coming in
CHINESE SIMPLIFIED: 入口

Inherent risk The risk level or exposure without taking into account the actions that management has taken or might take (e.g., implementing controls)
CHINESE SIMPLIFIED: 固有风险

Inheritance (objects) Database structures that have a strict hierarchy (no multiple inheritance). Inheritance can initiate other objects irrespective of the class hierarchy, thus there is no strict hierarchy of objects
CHINESE SIMPLIFIED: 继承(对象)

Initial program load (IPL) The initialization procedure that causes an operating system to be loaded into storage at the beginning of a workday or after a system malfunction.
CHINESE SIMPLIFIED: 初始程序加载

© 2015 ISACA All rights reserved.

Initialization vector (IV) collisions A major concern is the way that wired equivalent privacy (WEP) allocates the RC4 initialization vectors (IVs) used to create the keys that are used to drive a pseudo random number generator that is eventually used for encryption of the wireless data traffic. The IV in WEP is a 24-bit field--a small space that practically guarantees reuse, resulting in key reuse. The WEP standard also fails to specify how these IVs are assigned. Many wireless network cards reset these IVs to zero and then increment them by one for every use. If an attacker can capture two packets using the same IV (the same key if the key has not been changed), mechanisms can be used to determine portions of the original packets. This and other weaknesses result in key reuse, resulting in susceptibility to attacks to determine the keys used. These attacks require a large number of packets (5-6 million) to actually fully derive the WEP key, but on a large, busy network this can occur in a short time, perhaps in as quickly as 10 minutes (although, even some of the largest corporate networks will likely require much more time than this to gather enough packets). In WEP-protected wireless networks, many times multiple, or all, stations use the same shared key. This increases the chances of IV collisions greatly. The result of this is that the network becomes insecure if the WEP keys are not changed often. This furthers the need for a WEP key management protocol.
CHINESE SIMPLIFIED: **初始向量（IV）冲突**

Injection A general term for attack types which consist of injecting code that is then interpreted/executed by the application. (OWASP)
CHINESE SIMPLIFIED: **注入**

Input control Techniques and procedures used to verify, validate and edit data to ensure that only correct data are entered into the computer
CHINESE SIMPLIFIED: **输入控制**

Inputs and outputs The process work products/artifacts considered necessary to support operation of the process Scope Note: Inputs and outputs enable key decisions, provide a record and audit trail of process activities, and enable follow-up in the event of an incident. They are defined at the key management practice level, may include some work products used only within the process and are often essential inputs to other processes. The illustrative COBIT 5 inputs and outputs should not be regarded as an exhaustive list since additional information flows could be defined depending on a particular enterprise's environment and process framework.
COBIT 5 perspective
CHINESE SIMPLIFIED: **输入和输出**

Instant messaging (IM) An online mechanism or a form of real-time communication between two or more people based on typed text and multimedia data Scope Note: Text is conveyed via computers or another electronic device (e.g., cellular phone or handheld device) connected over a network, such as the Internet.
CHINESE SIMPLIFIED: **即时通讯（IM）**

Intangible asset An asset that is not physical in nature Scope Note: Examples include: intellectual property (patents, trademarks, copyrights, processes), goodwill, and brand recognition
CHINESE SIMPLIFIED: **无形资产**

Integrated services digital network (ISDN) A public end-to-end digital telecommunications network with signaling, switching and transport capabilities supporting a wide range of service accessed by standardized interfaces with integrated customer control Scope Note: The standard allows transmission of digital voice, video and data over 64-Kpbs lines.
CHINESE SIMPLIFIED: **综合服务数字网**

Integrated test facilities (ITF) A testing methodology in which test data are processed in production systems Scope Note: The data usually represent a set of fictitious entities such as departments, customers or products. Output reports are verified to confirm the correctness of the processing.
CHINESE SIMPLIFIED: **集成测试工具**

Integrity The guarding against improper information modification or destruction, and includes ensuring information non-repudiation and authenticity
CHINESE SIMPLIFIED: **完整性**

Intellectual property Intangible assets that belong to an enterprise for its exclusive use Scope Note: Examples include: patents, copyrights, trademarks, ideas, and trade secrets.
CHINESE SIMPLIFIED: **知识产权**

Interface testing A testing technique that is used to evaluate output from one application while the information is sent as input to another application
CHINESE SIMPLIFIED: **接口测试**

Internal control environment The relevant environment on which the controls have effect
CHINESE SIMPLIFIED: **内部控制环境**

© 2015 ISACA All rights reserved.

Internal control over financial reporting A process designed by, or under the supervision of, the registrant's principal executive and principal financial officers, or persons performing similar functions, and effected by the registrant's board of directors, management and other personnel to provide reasonable assurance regarding the reliability of financial reporting and the preparation of financial statements for external purposes in accordance with generally accepted accounting principals..
Includes those policies and procedures that:
Pertain to the maintenance of records that in reasonable detail accurately and fairly reflect the transactions and dispositions of the assets of the registrant
Provide reasonable assurance that transactions are recorded as necessary to permit preparation of financial statements in accordance with generally accepted accounting principles, and that receipts and expenditures of the registrant are being made only in accordance with authorizations of management and directors of the registrant
Provide reasonable assurance regarding prevention or timely detection of unauthorized acquisition, use or disposition of the registrant's assets that could have a material effect on the financial statements
CHINESE SIMPLIFIED: **财务报告内部控制**

Internal control structure The dynamic, integrated processes--effected by the governing body, management and all other staff--that are designed to provide reasonable assurance regarding the achievement of the following general objectives:
Effectiveness, efficiency and economy of operations
Reliability of management
Compliance with applicable laws, regulations and internal policies
Management's strategies for achieving these general objectives are affected by the design and operation of the following components:
Control environment
Information system
Control procedures
CHINESE SIMPLIFIED: **内部控制架构**

Internal controls The policies, procedures, practices and organizational structures designed to provide reasonable assurance that business objectives will be achieved and undesired events will be prevented or detected and corrected
CHINESE SIMPLIFIED: **内部控制**

Internal penetrators Authorized user of a computer system who oversteps his/her legitimate access rights Scope Note: This category is divided into masqueraders and clandestine users.
CHINESE SIMPLIFIED: **内部入侵者**

Internal rate of return (IRR) The discount rate that equates an investment cost with its projected earnings Scope Note: When discounted at the IRR, the present value of the cash outflow will equal the present value of the cash inflow. The IRR and net present value (NPV) are measures of the expected profitability of an project.
CHINESE SIMPLIFIED: **内部收益率**

Internal storage The main memory of the computer's central processing unit (CPU)
CHINESE SIMPLIFIED: **内部储存器**

International Standards Organization (ISO) The world's largest developer of voluntary International Standards
CHINESE SIMPLIFIED: **国际标准化组织**

Internet 1. Two or more networks connected by a router 2. The world's largest network using Transmission Control Protocol/Internet Protocol (TCP/IP) to link government, university and commercial institutions
CHINESE SIMPLIFIED: **互联网**

Internet Assigned Numbers Authority (IANA) Responsible for the global coordination of the DNS root, IP addressing, and other Internet protocol resources
CHINESE SIMPLIFIED: **互联网号码分配机构**

Internet banking Use of the Internet as a remote delivery channel for banking services Scope Note: Services include traditional ones, such as opening an account or transferring funds to different accounts, and new banking services, such as electronic bill presentment and payment (allowing customers to receive and pay bills on a bank's web site).
CHINESE SIMPLIFIED: **网上银行**

Internet Control Message Protocol (ICMP) A set of protocols that allow systems to communicate information about the state of services on other systems Scope Note: For example, ICMP is used in determining whether systems are up, maximum packet sizes on links, whether a destination host/network/port is available. Hackers typically use (abuse) ICMP to determine information about the remote site.
CHINESE SIMPLIFIED: **互联网控制消息协议 (ICMP)**

Internet Engineering Task Force (IETF) An organization with international affiliates as network industry representatives that sets Internet standards. This includes all network industry developers and researchers concerned with the evolution and planned growth of the Internet.
CHINESE SIMPLIFIED: **互联网工程任务组 (IETF)**

Internet Inter-ORB Protocol (IIOP) Developed by the object management group (OMG) to implement Common Object Request Broker Architecture (CORBA) solutions over the World Wide Web Scope Note: CORBA enables modules of network-based programs to communicate with one another. These modules or program parts, such as tables, arrays, and more complex program subelements, are referred to as objects. Use of IIOP in this process enables browsers and servers to exchange both simple and complex objects. This differs significantly from HyperText Transfer Protocol (HTTP), which only supports the transmission of text.
CHINESE SIMPLIFIED: **互联网内部对象请求代理协议 (IIOP)**

Internet protocol (IP) Specifies the format of packets and the addressing scheme
CHINESE SIMPLIFIED: **IP协议**

© 2015 ISACA All rights reserved.

Internet Protocol (IP) packet spoofing An attack using packets with the spoofed source Internet packet (IP) addresses. Scope Note: This technique exploits applications that use authentication based on IP addresses. This technique also may enable an unauthorized user to gain root access on the target system.
CHINESE SIMPLIFIED: **IP协议包欺骗**

Internet service provider (ISP) A third party that provides individuals and enterprises with access to the Internet and a variety of other Internet-related services
CHINESE SIMPLIFIED: **互联网服务提供商**

Internetwork Packet Exchange/Sequenced Packet Exchange (IPX/SPX) IPX is layer 3 of the open systems interconnect (OSI) model network protocol; SPX is layer 4 transport protocol. The SPX layer sits on top of the IPX layer and provides connection-oriented services between two nodes on the network.
CHINESE SIMPLIFIED: **互联网包交换/流交换协议(IPX/SPX)**

Interrogation Used to obtain prior indicators or relationships, including telephone numbers, IP addresses and names of individuals, from extracted data
CHINESE SIMPLIFIED: **询问**

Interruption window The time that the company can wait from the point of failure to the restoration of the minimum and critical services or applications. After this time, the progressive losses caused by the interruption are excessive for the enterprise.
CHINESE SIMPLIFIED: **中断时限**

Intranet A private network that uses the infrastructure and standards of the Internet and World Wide Web, but is isolated from the public Internet by firewall barriers
CHINESE SIMPLIFIED: **内联网**

Intruder Individual or group gaining access to the network and it's resources without permission
CHINESE SIMPLIFIED: **入侵者**

Intrusion Any event during which unauthorized access occurs
CHINESE SIMPLIFIED: **入侵**

Intrusion detection The process of monitoring the events occurring in a computer system or network to detect signs of unauthorized access or attack
CHINESE SIMPLIFIED: **入侵检测**

Intrusion detection system (IDS) Inspects network and host security activity to identify suspicious patterns that may indicate a network or system attack
CHINESE SIMPLIFIED: **入侵检测系统**

Intrusion prevention A preemptive approach to network security used to identify potential threats and respond to them to stop, or at least limit, damage or disruption
CHINESE SIMPLIFIED: **入侵防御**

Intrusion prevention system (IPS) A system designed to not only detect attacks, but also to prevent the intended victim hosts from being affected by the attacks
CHINESE SIMPLIFIED: **入侵防御系统**

Intrusive monitoring In vulnerability analysis, gaining information by performing checks that affect the normal operation of the system, and even by crashing the system
CHINESE SIMPLIFIED: **侵入性监控**

Investigation The collection and analysis of evidence with the goal to identifying the perpetrator of an attack or unauthorized use or access
CHINESE SIMPLIFIED: **调查**

Investment portfolio The collection of investments being considered and/or being made Scope Note: COBIT 5 perspective
CHINESE SIMPLIFIED: **投资组合**

IP address A unique binary number used to identify devices on a TCP/IP network
CHINESE SIMPLIFIED: **IP地址**

IP Authentication Header (AH) Protocol used to provide connectionless integrity and data origin authentication for IP datagrams (hereafter referred to as just "integrity") and to provide protection against replays. (RFC 4302). Scope Note: AH ensures data integrity with a checksum that a message authentication code, such as MD5, generates. To ensure data origin authentication, AH includes a secret shared key in the algorithm that it uses for authentication. To ensure replay protection, AH uses a sequence number field within the IP authentication header.
CHINESE SIMPLIFIED: **IP数据包认证头**

IP Security (IPSec) A set of protocols developed by the Internet Engineering Task Force (IETF) to support the secure exchange of packets
CHINESE SIMPLIFIED: **安全IP协议(IPSec)**

Irregularity Violation of an established management policy or regulatory requirement. It may consist of deliberate misstatements or omission of information concerning the area under audit or the enterprise as a whole, gross negligence or unintentional illegal acts.
CHINESE SIMPLIFIED: **违规**

ISO 9001:2000 Code of practice for quality management from the International Organization for Standardization (ISO). ISO 9001:2000 specifies requirements for a quality management system for any enterprise that needs to demonstrate its ability to consistently provide products or services that meet particular quality targets.
CHINESE SIMPLIFIED: **ISO 9001:2000**

© 2015 ISACA All rights reserved.

ISO/IEC 17799 This standard defines information's confidentiality, integrity and availability controls in a comprehensive information security management system. Scope Note: Originally released as part of the British Standard for Information Security in 1999 and then as the Code of Practice for Information Security Management in October 2000, it was elevated by the International Organization for Standardization (ISO) to an international code of practice for information security management. The latest version is ISO/IEC 17799:2005.
CHINESE SIMPLIFIED: **ISO/IEC 17799**

ISO/IEC 27001 Information Security Management--Specification with Guidance for Use; the replacement for BS7799-2. It is intended to provide the foundation for third-party audit and is harmonized with other management standards, such as ISO/IEC 9001 and 14001.
CHINESE SIMPLIFIED: **ISO/IEC 27001**

IT application Electronic functionality that constitutes parts of business processes undertaken by, or with the assistance of, IT Scope Note: COBIT 5 perspective
CHINESE SIMPLIFIED: **IT 应用程序**

IT architecture Description of the fundamental underlying design of the IT components of the business, the relationships among them, and the manner in which they support the enterprise's objectives
CHINESE SIMPLIFIED: **IT架构**

IT goal A statement describing a desired outcome of enterprise IT in support of enterprise goals. An outcome can be an artifact, a significant change of a state or a significant capability improvement. Scope Note: COBIT 5 perspective
CHINESE SIMPLIFIED: **IT 目标**

IT governance The responsibility of executives and the board of directors; consists of the leadership, organizational structures and processes that ensure that the enterprise's IT sustains and extends the enterprise's strategies and objectives
CHINESE SIMPLIFIED: **IT 治理**

IT governance framework A model that integrates a set of guidelines, policies and methods that represent the organizational approach to IT governance Scope Note: Per COBIT, IT governance is the responsibility of the board of directors and executive management. It is an integral part of institutional governance and consists of the leadership and organizational structures and processes that ensure that the enterprise's IT sustains and extends the enterprise's strategy and objectives.
CHINESE SIMPLIFIED: **IT 治理框架**

IT Governance Institute® (ITGI®) Founded in 1998 by the Information Systems Audit and Control Association (now known as ISACA). ITGI strives to assist enterprise leadership in ensuring long-term, sustainable enterprise success and to increase stakeholder value by expanding awareness.
CHINESE SIMPLIFIED: **IT 治理研究院 (ITGI®)**

IT incident Any event that is not part of the ordinary operation of a service that causes, or may cause, an interruption to, or a reduction in, the quality of that service
CHINESE SIMPLIFIED: **IT事件**

IT infrastructure The set of hardware, software and facilities that integrates an enterprise's IT assets Scope Note: Specifically, the equipment (including servers, routers, switches and cabling), software, services and products used in storing, processing, transmitting and displaying all forms of information for the enterprise's users
CHINESE SIMPLIFIED: **IT基础设施**

IT investment dashboard A tool for setting expectations for an enterprise at each level and continuous monitoring of the performance against set targets for expenditures on, and returns from, IT-enabled investment projects in terms of business values
CHINESE SIMPLIFIED: **IT 投资仪表板**

IT risk The business risk associated with the use, ownership, operation, involvement, influence and adoption of IT within an enterprise
CHINESE SIMPLIFIED: **IT 风险**

IT risk issue 1. An instance of IT risk 2. A combination of control, value and threat conditions that impose a noteworthy level of IT risk
CHINESE SIMPLIFIED: **IT 风险问题**

IT risk profile A description of the overall (identified) IT risk to which the enterprise is exposed
CHINESE SIMPLIFIED: **IT 风险概况**

IT risk register A repository of the key attributes of potential and known IT risk issues.
Attributes may include name, description, owner, expected/actual frequency, potential/actual magnitude, potential/actual business impact, disposition.
CHINESE SIMPLIFIED: **IT 风险登记表**

IT risk scenario The description of an IT-related event that can lead to a business impact
CHINESE SIMPLIFIED: **IT 风险场景**

IT service The day-to-day provision to customers of IT infrastructure and applications and support for their use—e.g., service desk, equipment supply and moves, and security authorizations Scope Note: COBIT 5 perspective
CHINESE SIMPLIFIED: **IT 服务**

IT steering committee An executive-management-level committee that assists in the delivery of the IT strategy, oversees day-to-day management of IT service delivery and IT projects, and focuses on implementation aspects
CHINESE SIMPLIFIED: **IT 指导委员会**

© 2015 ISACA All rights reserved.

IT strategic plan A long-term plan (i.e., three- to five-year horizon) in which business and IT management cooperatively describe how IT resources will contribute to the enterprise's strategic objectives (goals)
CHINESE SIMPLIFIED: **IT 战略计划**

IT strategy committee A committee at the level of the board of directors to ensure that the board is involved in major IT matters and decisions Scope Note: The committee is primarily accountable for managing the portfolios of IT-enabled investments, IT services and other IT resources. The committee is the owner of the portfolio.
CHINESE SIMPLIFIED: **IT 战略委员会**

IT tactical plan A medium-term plan (i.e., six- to 18-month horizon) that translates the IT strategic plan direction into required initiatives, resource requirements and ways in which resources and benefits will be monitored and managed
CHINESE SIMPLIFIED: **IT 战术计划**

IT user A person who uses IT to support or achieve a business objective
CHINESE SIMPLIFIED: **IT 用户**

ITIL (IT Infrastructure Library) The UK Office of Government Commerce (OGC) IT Infrastructure Library. A set of guides on the management and provision of operational IT services
CHINESE SIMPLIFIED: **ITIL (IT Infrastructure Library)**

IT-related incident An IT-related event that causes an operational, developmental and/or strategic business impact
CHINESE SIMPLIFIED: **IT 相关事故**

J

Job control language (JCL) Used to control run routines in connection with performing tasks on a computer
CHINESE SIMPLIFIED: **作业控制语言 (JCL)**

Journal entry A debit or credit to a general ledger account, in Oracle.
See also Manual Journal Entry.
CHINESE SIMPLIFIED: **日记帐分录**

Judgment sampling Any sample that is selected subjectively or in such a manner that the sample selection process is not random or the sampling results are not evaluated mathematically
CHINESE SIMPLIFIED: **判断抽样**

K

Kernel mode Used for execution of privileged instructions for the internal operation of the system. In kernel mode, there are no protections from errors or malicious activity and all parts of the system and memory are accessible.
CHINESE SIMPLIFIED: **内核模式**

Key goal indicator (KGI) A measure that tells management, after the fact, whether an IT process has achieved its business requirements; usually expressed in terms of information criteria
CHINESE SIMPLIFIED: **关键目标指标 (KGI)**

Key length The size of the encryption key measured in bits
CHINESE SIMPLIFIED: **密钥长度**

Key management practice Management practices that are required to successfully execute business processes
CHINESE SIMPLIFIED: **关键管理实务**

Key performance indicator (KPI) A measure that determines how well the process is performing in enabling the goal to be reached Scope Note: A lead indicator of whether a goal will likely be reached, and a good indicator of capabilities, practices and skills. It measures an activity goal, which is an action that the process owner must take to achieve effective process performance.
CHINESE SIMPLIFIED: **关键绩效指标 (KPI)**

Key risk indicator (KRI) A subset of risk indicators that are highly relevant and possess a high probability of predicting or indicating important risk Scope Note: See also Risk Indicator.
CHINESE SIMPLIFIED: **关键风险指标 (KRI)**

Keylogger Software used to record all keystrokes on a computer
CHINESE SIMPLIFIED: **键盘记录器**

Knowledge portal Refers to the repository of a core of information and knowledge for the extended enterprise Scope Note: Generally a web-based implementation containing a core repository of information provided for the extended enterprise to resolve any issues
CHINESE SIMPLIFIED: **知识门户网站**

L

Lag indicator Metrics for achievement of goals-An indicator relating to the outcome or result of an enabler Scope Note: This indicator is only available after the facts or events.
CHINESE SIMPLIFIED: **滞后指标**

© 2015 ISACA All rights reserved.

Latency The time it takes a system and network delay to respond Scope Note: More specifically, system latency is the time that a system takes to retrieve data. Network latency is the time it takes for a packet to travel from the source to the final destination.
CHINESE SIMPLIFIED: 延迟

Layer 2 switches Data link level devices that can divide and interconnect network segments and help to reduce collision domains in Ethernet-based networks
CHINESE SIMPLIFIED: 第二层交换机

Layer 3 and 4 switches Switches with operating capabilities at layer 3 and layer 4 of the open systems interconnect (OSI) model. These switches look at the incoming packet's networking protocol, e.g., IP, and then compare the destination IP address to the list of addresses in their tables, to actively calculate the best way to send a packet to its destination.
CHINESE SIMPLIFIED: 第三层和第四层交换

Layer 4-7 switches Used for load balancing among groups of servers Scope Note: Also known as content-switches, content services switches, web-switches or application-switches.
CHINESE SIMPLIFIED: 第四至七层交换机

Lead indicator Metrics for application of good practice-An indicator relating to the functioning of an enabler Scope Note: This indicator will provide an indication on possible outcome of the enabler.
CHINESE SIMPLIFIED: 领先指标

Leadership The ability and process to translate vision into desired behaviors that are followed at all levels of the extended enterprise
CHINESE SIMPLIFIED: 领导力

Leased line A communication line permanently assigned to connect two points, as opposed to a dial-up line that is only available and open when a connection is made by dialing the target machine or network. Also known as a dedicated line
CHINESE SIMPLIFIED: 专线

Legacy system Outdated computer systems
CHINESE SIMPLIFIED: 遗产系统

Level of assurance Refers to the degree to which the subject matter has been examined or reviewed
CHINESE SIMPLIFIED: 鉴证级别

Librarian The individual responsible for the safeguard and maintenance of all program and data files
CHINESE SIMPLIFIED: 程序包管理员

Licensing agreement A contract that establishes the terms and conditions under which a piece of software is being licensed (i.e., made legally available for use) from the software developer (owner) to the user
CHINESE SIMPLIFIED: 许可协议

Life cycle A series of stages that characterize the course of existence of an organizational investment (e.g., product, project, program)
CHINESE SIMPLIFIED: 生命周期

Likelihood The probability of something happening
CHINESE SIMPLIFIED: 可能性

Limit check Tests specified amount fields against stipulated high or low limits of acceptability Scope Note: When both high and low values are used, the test may be called a range check.
CHINESE SIMPLIFIED: 极限检查

Link editor (linkage editor) A utility program that combines several separately compiled modules into one, resolving internal references between them
CHINESE SIMPLIFIED: 链接编辑器

Literals Any notation for representing a value within programming language source code (e.g., a string literal); a chunk of input data that is represented "as is" in compressed data
CHINESE SIMPLIFIED: 文字

Local area network (LAN) Communication network that serves several users within a specified geographic area Scope Note: A personal computer LAN functions as a distributed processing system in which each computer in the network does its own processing and manages some of its data. Shared data are stored in a file server that acts as a remote disk drive for all users in the network.
CHINESE SIMPLIFIED: 局域网

Log To record details of information or events in an organized record-keeping system, usually sequenced in the order in which they occurred
CHINESE SIMPLIFIED: 日志

Logical access Ability to interact with computer resources granted using identification, authentication and authorization.
CHINESE SIMPLIFIED: 逻辑访问

Logical access controls The policies, procedures, organizational structure and electronic access controls designed to restrict access to computer software and data files
CHINESE SIMPLIFIED: 逻辑访问控制

Logoff The act of disconnecting from the computer
CHINESE SIMPLIFIED: 退出登录

Logon The act of connecting to the computer, which typically requires entry of a user ID and password into a computer terminal
CHINESE SIMPLIFIED: 登录

© 2015 ISACA All rights reserved.

Logs/log file Files created specifically to record various actions occurring on the system to be monitored, such as failed login attempts, full disk drives and e-mail delivery failures
CHINESE SIMPLIFIED: **日志/日志文件**

Loss event Any event during which a threat event results in loss Scope Note: From Jones, J.; "FAIR Taxonomy," Risk Management Insight, USA, 2008
CHINESE SIMPLIFIED: **丢失事件**

M

MAC header Represents the hardware address of an network interface controller (NIC) inside a data packet
CHINESE SIMPLIFIED: **MAC报文头**

Machine language The logical language that a computer understands
CHINESE SIMPLIFIED: **机器语言**

Magnetic card reader Reads cards with a magnetic surface on which data can be stored and retrieved
CHINESE SIMPLIFIED: **磁卡读取机**

Magnetic ink character recognition (MICR) Used to electronically input, read and interpret information directly from a source document Scope Note: MICR requires the source document to have specially-coded magnetic ink
CHINESE SIMPLIFIED: **磁墨水字符识别 (MICR)**

Magnitude A measure of the potential severity of loss or the potential gain from realized events/scenarios
CHINESE SIMPLIFIED: **程度**

Mail relay server An electronic mail (e-mail) server that relays messages so that neither the sender nor the recipient is a local user
CHINESE SIMPLIFIED: **邮件中继服务器**

Mainframe A large high-speed computer, especially one supporting numerous workstations or peripherals
CHINESE SIMPLIFIED: **大型机**

Malware Short for malicious software.
Designed to infiltrate, damage or obtain information from a computer system without the owner's consent Scope Note: Malware is commonly taken to include computer viruses, worms, Trojan horses, spyware and adware. Spyware is generally used for marketing purposes and, as such, is not malicious, although it is generally unwanted. Spyware can, however, be used to gather information for identity theft or other clearly illicit purposes.
CHINESE SIMPLIFIED: **恶意软件**

Management Plans, builds, runs and monitors activities in alignment with the direction set by the governance body to achieve the enterprise objectives.
CHINESE SIMPLIFIED: **管理**

Management information system (MIS) An organized assembly of resources and procedures required to collect, process and distribute data for use in decision making
CHINESE SIMPLIFIED: **管理信息系统 (MIS)**

Mandatory access control (MAC) A means of restricting access to data based on varying degrees of security requirements for information contained in the objects and the corresponding security clearance of users or programs acting on their behalf
CHINESE SIMPLIFIED: **强制访问控制 (MAC)**

Man-in-the-middle attack An attack strategy in which the attacker intercepts the communication stream between two parts of the victim system and then replaces the traffic between the two components with the intruder's own, eventually assuming control of the communication
CHINESE SIMPLIFIED: **中间人攻击**

Manual journal entry A journal entry entered at a computer terminal Scope Note: Manual journal entries can include regular, statistical, inter-company and foreign currency entries. See also Journal Entry.
CHINESE SIMPLIFIED: **人工日记帐分录**

Mapping Diagramming data that are to be exchanged electronically, including how they are to be used and what business management systems need them.
See also Application Tracing and Mapping. Scope Note: Mapping is a preliminary step for developing an applications link.
CHINESE SIMPLIFIED: **映射**

Masking A computerized technique of blocking out the display of sensitive information, such as passwords, on a computer terminal or report
CHINESE SIMPLIFIED: **掩码**

Masqueraders Attackers that penetrate systems by using the identity of legitimate users and their logon credentials
CHINESE SIMPLIFIED: **冒充者**

Master file A file of semi permanent information that is used frequently for processing data or for more than one purpose
CHINESE SIMPLIFIED: **主文件**

Material misstatement An accidental or intentional untrue statement that affects the results of an audit to a measurable extent
CHINESE SIMPLIFIED: **重大失实陈述**

© 2015 ISACA All rights reserved.

Material weakness A deficiency or a combination of deficiencies in internal control, such that there is a reasonable possibility that a material misstatement will not be prevented or detected on a timely basis. Weakness in control is considered 'material' if the absence of the control results in failure to provide reasonable assurance that the control objective will be met. A weakness classified as material implies that: Controls are not in place and/or controls are not in use and/or controls are inadequate
Escalation is warranted
There is an inverse relationship between materiality and the level of audit risk acceptable to the IS audit or assurance professional, i.e., the higher the materiality level, the lower the acceptability of the audit risk, and vice versa.
CHINESE SIMPLIFIED: **重大缺陷**

Materiality An auditing concept regarding the importance of an item of information with regard to its impact or effect on the functioning of the entity being audited.
An expression of the relative significance or importance of a particular matter in the context of the enterprise as a whole.
CHINESE SIMPLIFIED: **重要性**

Maturity In business, indicates the degree of reliability or dependency that the business can place on a process achieving the desired goals or objectives
CHINESE SIMPLIFIED: **成熟度**

Maturity model Scope Note: See Capability Maturity Model (CMM).
CHINESE SIMPLIFIED: **成熟度模型**

Maximum tolerable outages (MTO) Maximum time that an enterprise can support processing in alternate mode
CHINESE SIMPLIFIED: **最长可容忍中断时间**

Measure A standard used to evaluate and communicate performance against expected results Scope Note: Measures are normally quantitative in nature capturing numbers, dollars, percentages, etc., but can also address qualitative information such as customer satisfaction. Reporting and monitoring measures help an enterprise gauge progress toward effective implementation of strategy.
CHINESE SIMPLIFIED: **衡量指标**

Media access control (MAC) Applied to the hardware at the factory and cannot be modified, MAC is a unique, 48-bit, hard-coded address of a physical layer device, such as an Ethernet local area network (LAN) or a wireless network card
CHINESE SIMPLIFIED: **介质访问控制（MAC）**

Media access control (MAC) address A unique identifier assigned to network interfaces for communications on the physical network segment
CHINESE SIMPLIFIED: **介质访问控制地址**

Media oxidation The deterioration of the media on which data are digitally stored due to exposure to oxygen and moisture Scope Note: Tapes deteriorating in a warm, humid environment are an example of media oxidation. Proper environmental controls should prevent, or significantly slow, this process.
CHINESE SIMPLIFIED: **介质氧化**

Memory dump The act of copying raw data from one place to another with little or no formatting for readability Scope Note: Usually, dump refers to copying data from the main memory to a display screen or a printer. Dumps are useful for diagnosing bugs. After a program fails, one can study the dump and analyze the contents of memory at the time of the failure. A memory dump will not help unless each person knows what to look for because dumps are usually output in a difficult-to-read form (binary, octal or hexadecimal).
CHINESE SIMPLIFIED: **内存转储**

Message authentication code An American National Standards Institute (ANSI) standard checksum that is computed using Data Encryption Standard (DES)
CHINESE SIMPLIFIED: **消息验证码**

Message digest A smaller extrapolated version of the original message created using a message digest algorithm
CHINESE SIMPLIFIED: **消息摘要**

Message digest algorithm Message digest algorithms are SHA1, MD2, MD4 and MD5. These algorithms are one-way functions unlike private and public key encryption algorithms. Scope Note: All digest algorithms take a message of arbitrary length and produce a 128-bit message digest.
CHINESE SIMPLIFIED: **消息摘要算法**

Message switching A telecommunications methodology that controls traffic in which a complete message is sent to a concentration point and stored until the communications path is established
CHINESE SIMPLIFIED: **消息交换**

Metric A quantifiable entity that allows the measurement of the achievement of a process goal Scope Note: Metrics should be SMART--specific, measurable, actionable, relevant and timely. Complete metric guidance defines the unit used, measurement frequency, ideal target value (if appropriate) and also the procedure to carry out the measurement and the procedure for the interpretation of the assessment.
CHINESE SIMPLIFIED: **指标**

Metropolitan area network (MAN) A data network intended to serve an area the size of a large city
CHINESE SIMPLIFIED: **城域网**

Microwave transmission A high-capacity line-of-sight transmission of data signals through the atmosphere which often requires relay stations
CHINESE SIMPLIFIED: **微波传送**

© 2015 ISACA All rights reserved.

Middleware Another term for an application programmer interface (API).
It refers to the interfaces that allow programmers to access lower- or higher-level services by providing an intermediary layer that includes function calls to the services.
CHINESE SIMPLIFIED: 中间件

Milestone A terminal element that marks the completion of a work package or phase Scope Note: Typically marked by a high-level event such as project completion, receipt, endorsement or signing of a previously-defined deliverable or a high-level review meeting at which the appropriate level of project completion is determined and agreed to. A milestone is associated with a decision that outlines the future of a project and, for an outsourced project, may have a payment to the contractor associated with it.
CHINESE SIMPLIFIED: 里程碑

Miniature fragment attack Using this method, an attacker fragments the IP packet into smaller ones and pushes it through the firewall, in the hope that only the first of the sequence of fragmented packets would be examined and the others would pass without review.
CHINESE SIMPLIFIED: 微型碎片攻击

Mirrored site An alternate site that contains the same information as the original Scope Note: Mirrored sites are set up for backup and disaster recovery and to balance the traffic load for numerous download requests. Such download mirrors are often placed in different locations throughout the Internet.
CHINESE SIMPLIFIED: 镜像站点

Mission-critical application An application that is vital to the operation of the enterprise. The term is very popular for describing the applications required to run the day-to-day business.
CHINESE SIMPLIFIED: 关键任务应用程序

Misuse detection Detection on the basis of whether the system activity matches that defined as "bad"
CHINESE SIMPLIFIED: 误用检测

Mobile computing Extends the concept of wireless computing to devices that enable new kinds of applications and expand an enterprise network to reach places in circumstances that could never have been done by other means Scope Note: Mobile computing is comprised of personal digital assistants (PDAs), cellular phones, laptops and other technologies of this kind.
CHINESE SIMPLIFIED: 移动计算

Mobile device A small, handheld computing devices, typically having a display screen with touch input and/or a miniature keyboard and weighing less than two pounds
CHINESE SIMPLIFIED: 移动设备

Mobile site The use of a mobile/temporary facility to serve as a business resumption location.
The facility can usually be delivered to any site and can house information technology and staff.
CHINESE SIMPLIFIED: 移动站点

Model A way to describe a given set of components and how those components relate to each other in order to describe the main workings of an object, system, or concept Scope Note: COBIT 5 perspective
CHINESE SIMPLIFIED: 模式

MODEM (modulator/demodulator) Connects a terminal or computer to a communications network via a telephone line.
Modems turn digital pulses from the computer into frequencies within the audio range of the telephone system. When acting in the receiver capacity, a modem decodes incoming frequencies.
CHINESE SIMPLIFIED: 调制解调器

Modulation The process of converting a digital computer signal into an analog telecommunications signal
CHINESE SIMPLIFIED: 调制

Monetary unit sampling A sampling technique that estimates the amount of overstatement in an account balance
CHINESE SIMPLIFIED: 货币单位抽样

Monitoring policy Rules outlining or delineating the way in which information about the use of computers, networks, applications and information is captured and interpreted
CHINESE SIMPLIFIED: 监控策略

Multifactor authentication A combination of more than one authentication method, such as token and password (or personal identification number [PIN] or token and biometric device).
CHINESE SIMPLIFIED: 多因素认证

Multiplexor A device used for combining several lower-speed channels into a higher-speed channel
CHINESE SIMPLIFIED: 多路复用器

Mutual takeover A fail-over process, which is basically a two-way idle standby: two servers are configured so that both can take over the other node's resource group. Both must have enough central processing unit (CPU) power to run both applications with sufficient speed, or expected performance losses must be taken into account until the failed node reintegrates.
CHINESE SIMPLIFIED: 相互接管

N

National Institute for Standards and Technology (NIST) Develops tests, test methods, reference data, proof-of concept implementations, and technical analyses to advance the development and productive use of information technology Scope Note: NIST is a US government entity that creates mandatory standards that are followed by federal agencies and those doing business with them.
CHINESE SIMPLIFIED: 美国国家标准与技术研究院(NIST)

© 2015 ISACA All rights reserved.

Net present value (NPV) Calculated by using an after-tax discount rate of an investment and a series of expected incremental cash outflows (the initial investment and operational costs) and cash inflows (cost savings or revenues) that occur at regular periods during the life cycle of the investment Scope Note: To arrive at a fair NPV calculation, cash inflows accrued by the business up to about five years after project deployment also should be taken into account.
CHINESE SIMPLIFIED: **净现值 (NPV)**

Net return The revenue that a project or business makes after tax and other deductions; often also classified as net profit
CHINESE SIMPLIFIED: **净收益**

Netcat A simple UNIX utility, which reads and writes data across network connections using Transmission Control Protocol (TCP) or User Datagram Protocol (UDP). It is designed to be a reliable back-end tool that can be used directly or is easily driven by other programs and scripts. At the same time, it is a feature-rich network debugging and exploration tool, because it can create almost any kind of connection needed and has several interesting built-in capabilities. Netcat is now part of the Red Hat Power Tools collection and comes standard on SuSE Linux, Debian Linux, NetBSD and OpenBSD distributions.
CHINESE SIMPLIFIED: **Netcat**

Net-centric technologies The contents and security of information or objects (software and data) on the network are now of prime importance compared with traditional computer processing that emphasizes the location of hardware and its related software and data. Scope Note: An example of net-centric technologies is the Internet, where the network is its primary concern.
CHINESE SIMPLIFIED: **网络为中心的技术**

Netware A popular local area network (LAN) operating system (OS) developed by the Novell Corp.
CHINESE SIMPLIFIED: **Netware**

Network A system of interconnected computers and the communication equipment used to connect them
CHINESE SIMPLIFIED: **网络**

Network address translation (NAT) A methodology of modifying network address information in IP datagram packet headers while they are in transit across a traffic routing device for the purpose of remapping one IP address space into another
CHINESE SIMPLIFIED: **网络地址转换**

Network administrator Responsible for planning, implementing and maintaining the telecommunications infrastructure; also may be responsible for voice networks Scope Note: For smaller enterprises, the network administrator may also maintain a local area network (LAN) and assist end users.
CHINESE SIMPLIFIED: **网络管理员**

Network attached storage (NAS) Utilizes dedicated storage devices that centralize storage of data Scope Note: NA storage devices generally do not provide traditional file/print or application services.
CHINESE SIMPLIFIED: **网络连接存储 (NAS)**

Network basic input/output system (NetBIOS) A program that allows applications on different computers to communicate within a local area network (LAN).
CHINESE SIMPLIFIED: **网路基本输入输出系统(NetBIOS)**

Network hop An attack strategy in which the attacker successively hacks into a series of connected systems, obscuring his/her identify from the victim of the attack
CHINESE SIMPLIFIED: **网络跳数**

Network interface card (NIC) A communication card that when inserted into a computer, allows it to communicate with other computers on a network Scope Note: Most NICs are designed for a particular type of network or protocol.
CHINESE SIMPLIFIED: **网卡(NIC)**

Network news transfer protocol (NNTP) Used for the distribution, inquiry, retrieval, and posting of Netnews articles using a reliable stream-based mechanism. For news-reading clients, NNTP enables retrieval of news articles that are stored in a central database, giving subscribers the ability to select only those articles they wish to read. (RFC 3977)
CHINESE SIMPLIFIED: **网络消息传输协议(NNTP)**

Network segmentation A common technique to implement network security is to segment an organization's network into separate zones that can be separately controlled, monitored and protected.
CHINESE SIMPLIFIED: **网络分区**

Network traffic analysis Identifies patterns in network communications Scope Note: Traffic analysis does not need to have the actual content of the communication but analyzes where traffic is taking place, when and for how long communications occur and the size of information transferred.
CHINESE SIMPLIFIED: **网络流量分析**

Node Point at which terminals are given access to a network
CHINESE SIMPLIFIED: **节点**

Noise Disturbances in data transmissions, such as static, that cause messages to be misinterpreted by the receiver
CHINESE SIMPLIFIED: **噪声**

© 2015 ISACA All rights reserved.

Nondisclosure agreement (NDA) A legal contract between at least two parties that outlines confidential materials that the parties wish to share with one another for certain purposes, but wish to restrict from generalized use; a contract through which the parties agree not to disclose information covered by the agreement Scope Note: Also called a confidential disclosure agreement (CDA), confidentiality agreement or secrecy agreement. An NDA creates a confidential relationship between the parties to protect any type of trade secret. As such, an NDA can protect non-public business information. In the case of certain governmental entities, the confidentiality of information other than trade secrets may be subject to applicable statutory requirements, and in some cases may be required to be revealed to an outside party requesting the information. Generally, the governmental entity will include a provision in the contract to allow the seller to review a request for information that the seller identifies as confidential and the seller may appeal such a decision requiring disclosure. NDAs are commonly signed when two companies or individuals are considering doing business together and need to understand the processes used in one another's businesses solely for the purpose of evaluating the potential business relationship. NDAs can be "mutual," meaning that both parties are restricted in their use of the materials provided, or they can only restrict a single party. It is also possible for an employee to sign an NDA or NDA-like agreement with a company at the time of hiring; in fact, some employment agreements will include a clause restricting "confidential information" in general.
CHINESE SIMPLIFIED: **保密协议 (NDA)**

Nonintrusive monitoring The use of transported probes or traces to assemble information, track traffic and identify vulnerabilities
CHINESE SIMPLIFIED: **非侵入式监控**

Nonrepudiable transaction Transaction that cannot be denied after the fact
CHINESE SIMPLIFIED: **不可否认的交易**

Nonrepudiation The assurance that a party cannot later deny originating data; provision of proof of the integrity and origin of the data and that can be verified by a third party Scope Note: A digital signature can provide non-repudiation.
CHINESE SIMPLIFIED: **不可否认性**

Non-statistical sampling Method of selecting a portion of a population, by means of own judgement and experience, for the purpose of quickly confirming a proposition. This method does not allow drawing mathematical conclusions on the entire population.
CHINESE SIMPLIFIED: **非统计抽样**

Normalization The elimination of redundant data
CHINESE SIMPLIFIED: **标准化**

Numeric check An edit check designed to ensure that the data element in a particular field is numeric.
CHINESE SIMPLIFIED: **数值字段检查**

O

Obfuscation The deliberate act of creating source or machine code that is difficult for humans to understand
CHINESE SIMPLIFIED: **混淆**

Object code Machine-readable instructions produced from a compiler or assembler program that has accepted and translated the source code
CHINESE SIMPLIFIED: **目标代码**

Object management group (OMG) A consortium with more than 700 affiliates from the software industry whose purpose is to provide a common framework for developing applications using object-oriented programming techniques Scope Note: For example, OMG is known principally for promulgating the Common Object Request Broker Architecture (CORBA) specification.
CHINESE SIMPLIFIED: **对象管理组 (OMG)**

Object orientation An approach to system development in which the basic unit of attention is an object, which represents an encapsulation of both data (an object's attributes) and functionality (an object's methods) Scope Note: Objects usually are created using a general template called a class. A class is the basis for most design work in objects. A class and its objects communicate in defined ways. Aggregate classes interact through messages, which are directed requests for services from one class (the client) to another class (the server). A class may share the structure or methods defined in one or more other classes--a relationship known as inheritance.
CHINESE SIMPLIFIED: **面向对象**

Objective Statement of a desired outcome Scope Note: COBIT 5 perspective
CHINESE SIMPLIFIED: **目标**

Objectivity The ability to exercise judgment, express opinions and present recommendations with impartiality
CHINESE SIMPLIFIED: **客观性**

Object-oriented system development A system development methodology that is organized around "objects" rather than "actions," and "data" rather than "logic" Scope Note: Object-oriented analysis is an assessment of a physical system to determine which objects in the real world need to be represented as objects in a software system. Any object-oriented design is software design that is centered around designing the objects that will make up a program. Any object-oriented program is one that is composed of objects or software parts.
CHINESE SIMPLIFIED: **面向对象的系统开发**

Offline files Computer file storage media that are not physically connected to the computer; typical examples are tapes or tape cartridges used for backup purposes.
CHINESE SIMPLIFIED: **离线文件**

© 2015 ISACA All rights reserved.

Offsite storage A facility located away from the building housing the primary information processing facility (IPF), used for storage of computer media such as offline backup data and storage files
CHINESE SIMPLIFIED: 异地储存

Online data processing Achieved by entering information into the computer via a video display terminal Scope Note: With online data processing, the computer immediately accepts or rejects the information as it is entered.
CHINESE SIMPLIFIED: 在线数据处理

Open Source Security Testing Methodology An open and freely available methodology and manual for security testing
CHINESE SIMPLIFIED: 开源安全测试方法

Open system System for which detailed specifications of the composition of its component are published in a nonproprietary environment, thereby enabling competing enterprises to use these standard components to build competitive systems Scope Note: The advantages of using open systems include portability, interoperability and integration.
CHINESE SIMPLIFIED: 开放系统

Open Systems Interconnect (OSI) model A model for the design of a network. The open systems interconnect (OSI) model defines groups of functionality required to network computers into layers. Each layer implements a standard protocol to implement its functionality. There are seven layers in the OSI model.
CHINESE SIMPLIFIED: 开放系统互联模型

Open Web Application Security Project (OWASP) An open community dedicated to enabling organizations to conceive, develop, acquire, operate, and maintain applications that can be trusted
CHINESE SIMPLIFIED: 开放式Web应用程序安全项目

Operating system (OS) A master control program that runs the computer and acts as a scheduler and traffic controller Scope Note: The operating system is the first program copied into the computer's memory after the computer is turned on; it must reside in memory at all times. It is the software that interfaces between the computer hardware (disk, keyboard, mouse, network, modem, printer) and the application software (word processor, spreadsheet, e-mail), which also controls access to the devices and is partially responsible for security components and sets the standards for the application programs that run in it.
CHINESE SIMPLIFIED: 操作系统

Operating system audit trail Record of system events generated by a specialized operating system mechanism
CHINESE SIMPLIFIED: 操作系统审计轨迹

Operational audit An audit designed to evaluate the various internal controls, economy and efficiency of a function or department
CHINESE SIMPLIFIED: 操作审计

Operational control Deals with the everyday operation of a company or enterprise to ensure that all objectives are achieved
CHINESE SIMPLIFIED: 操作控制

Operational level agreement (OLA) An internal agreement covering the delivery of services that support the IT organization in its delivery of services
CHINESE SIMPLIFIED: 操作水平协议（OLA）

Operator console A special terminal used by computer operations personnel to control computer and systems operations functions Scope Note: Operator console terminals typically provide a high level of computer access and should be properly secured.
CHINESE SIMPLIFIED: 操作员主控台

Optical character recognition (OCR) Used to electronically scan and input written information from a source document
CHINESE SIMPLIFIED: 光学字符识别

Optical scanner An input device that reads characters and images that are printed or painted on a paper form into the computer
CHINESE SIMPLIFIED: 光学扫描仪

Organization The manner in which an enterprise is structured; can also mean the entity
CHINESE SIMPLIFIED: 组织

Organization for Economic Cooperation and Development (OECD) An international organization helping governments tackle the economic, social and governance challenges of a global economy Scope Note: The OECD groups 30 member countries in a unique forum to discuss, develop, and refine economic and social policies.
CHINESE SIMPLIFIED: 经济合作与发展组织 (OECD)

Organizational structure An enabler of governance and of management. Includes the enterprise and its structures, hierarchies and dependencies. Scope Note: Example: Steering committee
COBIT 5 perspective
CHINESE SIMPLIFIED: 组织结构

Outcome Result
CHINESE SIMPLIFIED: 成果

Outcome measure Represents the consequences of actions previously taken; often referred to as a lag indicator Scope Note: Outcome measure frequently focuses on results at the end of a time period and characterize historic performance. They are also referred to as a key goal indicator (KGI) and used to indicate whether goals have been met. These can be measured only after the fact and, therefore, are called "lag indicators."
CHINESE SIMPLIFIED: 成果衡量指标

© 2015 ISACA All rights reserved.

Output analyzer Checks the accuracy of the results produced by a test run Scope Note: There are three types of checks that an output analyzer can perform. First, if a standard set of test data and test results exist for a program, the output of a test run after program maintenance can be compared with the set of results that should be produced. Second, as programmers prepare test data and calculate the expected results, these results can be stored in a file and the output analyzer compares the actual results of a test run with the expected results. Third, the output analyzer can act as a query language; it accepts queries about whether certain relationships exist in the file of output results and reports compliance or noncompliance.
CHINESE SIMPLIFIED: 输出分析仪

Outsourcing A formal agreement with a third party to perform IS or other business functions for an enterprise
CHINESE SIMPLIFIED: 外包

Owner Individual or group that holds or possesses the rights of and the responsibilities for an enterprise, entity or asset. Scope Note: Examples: process owner, system owner.
COBIT 5 perspective
CHINESE SIMPLIFIED: 所有者

P

Packet Data unit that is routed from source to destination in a packet-switched network Scope Note: A packet contains both routing information and data. Transmission Control Protocol/Internet Protocol (TCP/IP) is such a packet-switched network.
CHINESE SIMPLIFIED: 数据包

Packet filtering Controlling access to a network by analyzing the attributes of the incoming and outgoing packets and either letting them pass, or denying them, based on a list of rules
CHINESE SIMPLIFIED: 数据包过滤

Packet internet groper (PING) An Internet program (Internet Control Message Protocol [ICMP]) used to determine whether a specific IP address is accessible or online.
It is a network application that uses User Datagram Protocol (UDP) to verify reachability of another host on the connected network. Scope Note: It works by sending a packet to the specified address and waiting for a reply. PING is used primarily to troubleshoot Internet connections. In addition, PING reports the number of hops required to connect two Internet hosts. There are both freeware and shareware PING utilities available for personal computers (PCs).
CHINESE SIMPLIFIED: 互联网数据包探索 (PING)

Packet switching The process of transmitting messages in convenient pieces that can be reassembled at the destination
CHINESE SIMPLIFIED: 数据包交换

Paper test A walk-through of the steps of a regular test, but without actually performing the steps Scope Note: Usually used in disaster recovery and contingency testing; team members review and become familiar with the plans and their specific roles and responsibilities
CHINESE SIMPLIFIED: 纸面测试

Parallel simulation Involves an IS auditor writing a program to replicate those application processes that are critical to an audit opinion and using this program to reprocess application system data Scope Note: The results produced by parallel simulation are compared with the results generated by the application system and any discrepancies are identified.
CHINESE SIMPLIFIED: 并行模拟

Parallel testing The process of feeding test data into two systems, the modified system and an alternative system (possibly the original system), and comparing results to demonstrate the consistency and inconsistency between two versions of the application
CHINESE SIMPLIFIED: 并行测试

Parity check A general hardware control that helps to detect data errors when data are read from memory or communicated from one computer to another Scope Note: A 1-bit digit (either 0 or 1) is added to a data item to indicate whether the sum of that data item's bit is odd or even. When the parity bit disagrees with the sum of the other bits, the computer reports an error. The probability of a parity check detecting an error is 50 percent.
CHINESE SIMPLIFIED: 奇偶校验

Partitioned file A file format in which the file is divided into multiple sub files and a directory is established to locate each sub file
CHINESE SIMPLIFIED: 分割文件

Passive assault Intruders attempt to learn some characteristic of the data being transmitted Scope Note: With a passive assault, intruders may be able to read the contents of the data so the privacy of the data is violated. Alternatively, although the content of the data itself may remain secure, intruders may read and analyze the plaintext source and destination identifiers attached to a message for routing purposes, or they may examine the lengths and frequency of messages being transmitted.
CHINESE SIMPLIFIED: 被动式攻击

Passive response A response option in intrusion detection in which the system simply reports and records the problem detected, relying on the user to take subsequent action
CHINESE SIMPLIFIED: 被动响应

Password A protected, generally computer-encrypted string of characters that authenticate a computer user to the computer system
CHINESE SIMPLIFIED: 密码

© 2015 ISACA All rights reserved.

Password cracker A tool that tests the strength of user passwords by searching for passwords that are easy to guess.
It repeatedly tries words from specially crafted dictionaries and often also generates thousands (and in some cases, even millions) of permutations of characters, numbers and symbols.
CHINESE SIMPLIFIED: **密码破解器**

Patch Fixes to software programming errors and vulnerabilities
CHINESE SIMPLIFIED: **补丁**

Patch management An area of systems management that involves acquiring, testing and installing multiple patches (code changes) to an administered computer system in order to maintain up-to-date software and often to address security risk Scope Note: Patch management tasks include the following: maintaining current knowledge of available patches; deciding what patches are appropriate for particular systems; ensuring that patches are installed properly; testing systems after installation; and documenting all associated procedures, such as specific configurations required. A number of products are available to automate patch management tasks. Patches are sometimes ineffective and can sometimes cause more problems than they fix. Patch management experts suggest that system administrators take simple steps to avoid problems, such as performing backups and testing patches on non-critical systems prior to installations. Patch management can be viewed as part of change management.
CHINESE SIMPLIFIED: **补丁管理**

Payback period The length of time needed to recoup the cost of capital investment Scope Note: Financial amounts in the payback formula are not discounted. Note that the payback period does not take into account cash flows after the payback period and therefore is not a measure of the profitability of an investment project. The scope of the internal rate of return (IRR), net present value (NPV) and payback period is the useful economic life of the project up to a maximum of five years.
CHINESE SIMPLIFIED: **投资回收期**

Payload The section of fundamental data in a transmission. In malicious software this refers to the section containing the harmful data/code.
CHINESE SIMPLIFIED: **负载**

Payment system A financial system that establishes the means for transferring money between suppliers and users of funds, ordinarily by exchanging debits or credits between banks or financial institutions
CHINESE SIMPLIFIED: **支付系统**

Payroll system An electronic system for processing payroll information and the related electronic (e.g., electronic timekeeping and/or human resources [HR] system), human (e.g., payroll clerk), and external party (e.g., bank) interfaces.
In a more limited sense, it is the electronic system that performs the processing for generating payroll checks and/or bank direct deposits to employees.
CHINESE SIMPLIFIED: **工资系统**

Penetration testing A live test of the effectiveness of security defenses through mimicking the actions of real-life attackers
CHINESE SIMPLIFIED: **渗透测试**

Performance In IT, the actual implementation or achievement of a process
CHINESE SIMPLIFIED: **性能**

Performance driver A measure that is considered the "driver" of a lag indicator.
It can be measured before the outcome is clear and, therefore, is called a "lead indicator." Scope Note: There is an assumed relationship between the two that suggests that improved performance in a leading indicator will drive better performance in the lagging indicator. They are also referred to as key performance indicators (KPIs) and are used to indicate whether goals are likely to be met.
CHINESE SIMPLIFIED: **绩效驱动因素**

Performance indicators A set of metrics designed to measure the extent to which performance objectives are being achieved on an on-going basis Scope Note: Performance indicators can include service level agreements (SLAs), critical success factors (CSFs), customer satisfaction ratings, internal or external benchmarks, industry best practices and international standards.
CHINESE SIMPLIFIED: **绩效指标**

Performance management In IT, the ability to manage any type of measurement, including employee, team, process, operational or financial measurements. The term connotes closed-loop control and regular monitoring of the measurement.
CHINESE SIMPLIFIED: **绩效管理**

Performance testing Comparing the system's performance to other equivalent systems, using well-defined benchmarks
CHINESE SIMPLIFIED: **性能测试**

Peripherals Auxiliary computer hardware equipment used for input, output and data storage Scope Note: Examples of peripherals include disk drives and printers.
CHINESE SIMPLIFIED: **外围设备**

Personal digital assistant (PDA) Also called palmtop and pocket computer, PDA is a handheld device that provide computing, Internet, networking and telephone characteristics.
CHINESE SIMPLIFIED: **个人数字助理设备(PDA)**

Personal identification number (PIN) A type of password (i.e., a secret number assigned to an individual) that, in conjunction with some means of identifying the individual, serves to verify the authenticity of the individual Scope Note: PINs have been adopted by financial institutions as the primary means of verifying customers in an electronic funds transfer (EFT) system.
CHINESE SIMPLIFIED: **个人识别码**

© 2015 ISACA All rights reserved.

Pervasive IS control General control designed to manage and monitor the IS environment and which, therefore, affects all IS-related activities
CHINESE SIMPLIFIED: **普遍性 IS 控制**

Phase of BCP A step-by-step approach consisting of various phases Scope Note: Phase of BCP is usually comprised of the following phases: pre-implementation phase, implementation phase, testing phase, and post-implementation phase.
CHINESE SIMPLIFIED: **BCP 阶段**

Phishing This is a type of electronic mail (e-mail) attack that attempts to convince a user that the originator is genuine, but with the intention of obtaining information for use in social engineering Scope Note: Phishing attacks may take the form of masquerading as a lottery organization advising the recipient or the user's bank of a large win; in either case, the intent is to obtain account and personal identification number (PIN) details. Alternative attacks may seek to obtain apparently innocuous business information, which may be used in another form of active attack.
CHINESE SIMPLIFIED: **网络钓鱼**

Phreakers Those who crack security, most frequently telephone and other communication networks
CHINESE SIMPLIFIED: **电话线路盗用者**

Piggybacking 1. Following an authorized person into a restricted access area 2. Electronically attaching to an authorized telecommunications link to intercept and possibly alter transmissions
CHINESE SIMPLIFIED: **骑肩跟入法（跟随经授权的人员进入管制区域）**

Plain old telephone service (POTS) A wired telecommunications system.
CHINESE SIMPLIFIED: **普通老式电话服务**

Plaintext Digital information, such as cleartext, that is intelligible to the reader
CHINESE SIMPLIFIED: **明文**

Platform as a Service (PaaS) Offers the capability to deploy onto the cloud infrastructure customer-created or -acquired applications that are created using programming languages and tools supported by the provider
CHINESE SIMPLIFIED: **平台即服务 (PaaS)**

PMBOK (Project Management Body of Knowledge) A project management standard developed by the Project Management Institute (PMI)
CHINESE SIMPLIFIED: **项目管理知识体系 (PMBOK)**

Point-of-presence (POP) A telephone number that represents the area in which the communication provider or Internet service provider (ISP) provides service
CHINESE SIMPLIFIED: **存在点 (POP)**

Point-of-sale (POS) systems Enables the capture of data at the time and place of transaction Scope Note: POS terminals may include use of optical scanners for use with bar codes or magnetic card readers for use with credit cards. POS systems may be online to a central computer or may use stand-alone terminals or microcomputers that hold the transactions until the end of a specified period when they are sent to the main computer for batch processing.
CHINESE SIMPLIFIED: **销售终端系统**

Point-to-point Protocol (PPP) A protocol used for transmitting data between two ends of a connection
CHINESE SIMPLIFIED: **点对点协议 (PPP)**

Point-to-point Tunneling Protocol (PPTP) A protocol used to transmit data securely between two end points to create a virtual private network (VPN).
CHINESE SIMPLIFIED: **点对点隧道协议 (PPTP)**

Policy
1. Generally, a document that records a high-level principle or course of action that has been decided on. The intended purpose is to influence and guide both present and future decision making to be in line with the philosophy, objectives and strategic plans established by the enterprise's management teams. Scope Note: In addition to policy content, policies need to describe the consequences of failing to comply with the policy, the means for handling exceptions, and the manner in which compliance with the policy will be checked and measured. 2. Overall intention and direction as formally expressed by management Scope Note: COBIT 5 perspective
CHINESE SIMPLIFIED: **政策**

Polymorphism (Objects) Polymorphism refers to database structures that send the same command to different child objects that can produce different results depending on their family hierarchical tree structure
CHINESE SIMPLIFIED: **多态性**

Population The entire set of data from which a sample is selected and about which an IS auditor wishes to draw conclusions
CHINESE SIMPLIFIED: **总体**

Port (Port number) A process or application-specific software element serving as a communication endpoint for the Transport Layer IP protocols (UDP and TCP)
CHINESE SIMPLIFIED: **端口**

Port scanning The act of probing a system to identify open ports
CHINESE SIMPLIFIED: **端口扫描**

Portfolio A grouping of "objects of interest" (investment programs, IT services, IT projects, other IT assets or resources) managed and monitored to optimize business value.
(The investment portfolio is of primary interest to Val IT. IT service, project, asset and other resource portfolios are of primary interest to COBIT.)
CHINESE SIMPLIFIED: **组合**

© 2015 ISACA All rights reserved.

Posting The process of actually entering transactions into computerized or manual files Scope Note: Posting transactions might immediately update the master files or may result in memo posting, in which the transactions are accumulated over a period of time and then applied to master file updating.
CHINESE SIMPLIFIED: 计账

Preventive application control Application control that is intended to prevent an error from occurring. Preventive application controls are typically executed at the transaction level, before an action is performed.
CHINESE SIMPLIFIED: 预防性应用程序控制

Preventive control An internal control that is used to avoid undesirable events, errors and other occurrences that an enterprise has determined could have a negative material effect on a process or end product
CHINESE SIMPLIFIED: 预防性控制

Prime number A natural number greater than 1 that can only be divided by 1 and itself.
CHINESE SIMPLIFIED: 素数

PRINCE2 (Projects in a Controlled Environment) Developed by the Office of Government Commerce (OGC), PRINCE2 is a project management method that covers the management, control and organization of a project.
CHINESE SIMPLIFIED: PRINCE2 (受控环境下的项目管理)

Principle An enabler of governance and of management. Comprises the values and fundamental assumptions held by the enterprise, the beliefs that guide and put boundaries around the enterprise's decision making, communication within and outside the enterprise, and stewardship--caring for assets owned by another. Scope Note: Examples: Ethics charter, social responsibility charter.
COBIT 5 perspective
CHINESE SIMPLIFIED: 原则

Principle of least privilege/access Controls used to allow the least privilege access needed to complete a task
CHINESE SIMPLIFIED: 最小特权原则/访问

Privacy Freedom from unauthorized intrusion or disclosure of information about an individual
CHINESE SIMPLIFIED: 隐私权

Private branch exchange (PBX) A telephone exchange that is owned by a private business, as opposed to one owned by a common carrier or by a telephone company
CHINESE SIMPLIFIED: 专用分组交换机

Private key A mathematical key (kept secret by the holder) used to create digital signatures and, depending on the algorithm, to decrypt messages or files encrypted (for confidentiality) with the corresponding public key
CHINESE SIMPLIFIED: 私钥

Private key cryptosystems Used in data encryption, it utilizes a secret key to encrypt the plaintext to the ciphertext. Private key cryptosystems also use the same key to decrypt the ciphertext to the corresponding plaintext. Scope Note: In this case, the key is symmetric such that the encryption key is equivalent to the decryption key.
CHINESE SIMPLIFIED: 对称加密体系

Privilege The level of trust with which a system object is imbued
CHINESE SIMPLIFIED: 特权

Probe Inspect a network or system to find weak spots
CHINESE SIMPLIFIED: 探针

Problem In IT, the unknown underlying cause of one or more incidents
CHINESE SIMPLIFIED: 问题

Problem escalation procedure The process of escalating a problem up from junior to senior support staff, and ultimately to higher levels of management Scope Note: Problem escalation procedure is often used in help desk management, when an unresolved problem is escalated up the chain of command, until it is solved.
CHINESE SIMPLIFIED: 问题升级流程

Procedure A document containing a detailed description of the steps necessary to perform specific operations in conformance with applicable standards. Procedures are defined as part of processes.
CHINESE SIMPLIFIED: 程序

Process Generally, a collection of activities influenced by the enterprise's policies and procedures that takes inputs from a number of sources, (including other processes), manipulates the inputs and produces outputs Scope Note: Processes have clear business reasons for existing, accountable owners, clear roles and responsibilities around the execution of the process, and the means to measure performance.
CHINESE SIMPLIFIED: 流程

Process goals A statement describing the desired outcome of a process. Scope Note: An outcome can be an artifact, a significant change of a state or a significant capability improvement of other processes.
COBIT 5 perspective
CHINESE SIMPLIFIED: 流程目标

Process maturity assessment A subjective assessment technique derived from the Software Engineering Institute (SEI) capability maturity model integration (CMMI) concepts and developed as a COBIT management tool.
It provides management with a profile of how well developed the IT management processes are. Scope Note: It enables management to easily place itself on a scale and appreciate what is required if improved performance is needed. It is used to set targets, raise awareness, capture broad consensus, identify improvements and positively motivate change.
CHINESE SIMPLIFIED: 流程成熟度评估

© 2015 ISACA All rights reserved.

Process maturity attribute The different aspects of a process covered in an assurance initiative
CHINESE SIMPLIFIED: 流程成熟度属性

Production program Program used to process live or actual data that were received as input into the production environment
CHINESE SIMPLIFIED: 生产程序

Production software Software that is being used and executed to support normal and authorized organizational operations Scope Note: Production software is to be distinguished from test software, which is being developed or modified, but has not yet been authorized for use by management.
CHINESE SIMPLIFIED: 生产软件

Professional competence Proven level of ability, often linked to qualifications issued by relevant professional bodies and compliance with their codes of practice and standards
CHINESE SIMPLIFIED: 专业能力

Professional judgement The application of relevant knowledge and experience in making informed decisions about the courses of action that are appropriate in the circumstances of the IS audit and assurance engagement
CHINESE SIMPLIFIED: 专业判断

Professional skepticism An attitude that includes a questioning mind and a critical assessment of audit evidence Scope Note: Source: American Institute of Certified Public Accountants (AICPA) AU 230.07
CHINESE SIMPLIFIED: 专业质疑

Professional standards Refers to standards issued by ISACA.
The term may extend to related guidelines and techniques that assist the professional in implementing and complying with authoritative pronouncements of ISACA. In certain instances, standards of other professional organizations may be considered, depending on the circumstances and their relevance and appropriateness.
CHINESE SIMPLIFIED: 专业标准

Program A structured grouping of interdependent projects that is both necessary and sufficient to achieve a desired business outcome and create value.
These projects could include, but are not limited to, changes in the nature of the business, business processes and the work performed by people as well as the competencies required to carry out the work, the enabling technology, and the organizational structure.
CHINESE SIMPLIFIED: 计划

Program and project management office (PMO) The function responsible for supporting program and project managers, and gathering, assessing and reporting information about the conduct of their programs and constituent projects
CHINESE SIMPLIFIED: 计划与项目管理办公室 (PMO)

Program Evaluation and Review Technique (PERT) A project management technique used in the planning and control of system projects
CHINESE SIMPLIFIED: 计划评估和审查技术

Program flowchart Shows the sequence of instructions in a single program or subroutine Scope Note: The symbols used in program flowcharts should be the internationally accepted standard. Program flowcharts should be updated when necessary.
CHINESE SIMPLIFIED: 程序流程图

Program narrative Provides a detailed explanation of program flowcharts, including control points and any external input
CHINESE SIMPLIFIED: 程序注释

Project A structured set of activities concerned with delivering a defined capability (that is necessary but not sufficient, to achieve a required business outcome) to the enterprise based on an agreed-on schedule and budget
CHINESE SIMPLIFIED: 项目

Project management officer (PMO) The individual function responsible for the implementation of a specified initiative for supporting the project management role and advancing the discipline of project management
CHINESE SIMPLIFIED: 项目管理经理 (PMO)

Project portfolio The set of projects owned by a company Scope Note: It usually includes the main guidelines relative to each project, including objectives, costs, time lines and other information specific to the project.
CHINESE SIMPLIFIED: 项目组合

Project team Group of people responsible for a project, whose terms of reference may include the development, acquisition, implementation or maintenance of an application system Scope Note: The project team members may include line management, operational line staff, external contractors and IS auditors.
CHINESE SIMPLIFIED: 项目团队

Promiscuous mode Allows the network interface to capture all network traffic irrespective of the hardware device to which the packet is addressed
CHINESE SIMPLIFIED: 混杂模式

Protection domain The area of the system that the intrusion detection system (IDS) is meant to monitor and protect
CHINESE SIMPLIFIED: 保护领域

Protocol The rules by which a network operates and controls the flow and priority of transmissions
CHINESE SIMPLIFIED: 通讯协议

Protocol converter Hardware devices, such as asynchronous and synchronous transmissions, that convert between two different types of transmission
CHINESE SIMPLIFIED: 协议转换器

© 2015 ISACA All rights reserved.

Protocol stack A set of utilities that implement a particular network protocol Scope Note: For instance, in Windows machines a Transmission Control Protocol/Internet Protocol (TCP/IP) stack consists of TCP/IP software, sockets software and hardware driver software.
CHINESE SIMPLIFIED: 协议堆栈

Prototyping The process of quickly putting together a working model (a prototype) in order to test various aspects of a design, illustrate ideas or features and gather early user feedback Scope Note: Prototyping uses programmed simulation techniques to represent a model of the final system to the user for advisement and critique. The emphasis is on end-user screens and reports. Internal controls are not a priority item since this is only a model.
CHINESE SIMPLIFIED: 原型设计

Proxy server A server that acts on behalf of a user Scope Note: Typical proxies accept a connection from a user, make a decision as to whether the user or client IP address is permitted to use the proxy, perhaps perform additional authentication, and complete a connection to a remote destination on behalf of the user.
CHINESE SIMPLIFIED: 代理服务器

Public key In an asymmetric cryptographic scheme, the key that may be widely published to enable the operation of the scheme
CHINESE SIMPLIFIED: 公钥

Public key cryptosystem Used in data encryption, it uses an encryption key, as a public key, to encrypt the plaintext to the ciphertext. It uses the different decryption key, as a secret key, to decrypt the ciphertext to the corresponding plaintext. Scope Note: In contrast to a private key cryptosystem, the decryption key should be secret; however, the encryption key can be known to everyone. In a public key cryptosystem, two keys are asymmetric, such that the encryption key is not equivalent to the decryption key.
CHINESE SIMPLIFIED: 公钥加密体系

Public key encryption A cryptographic system that uses two keys: one is a public key, which is known to everyone, and the second is a private or secret key, which is only known to the recipient of the message
See also Asymmetric Key.
CHINESE SIMPLIFIED: 公钥加密

Public key infrastructure (PKI) A series of processes and technologies for the association of cryptographic keys with the entity to whom those keys were issued
CHINESE SIMPLIFIED: 公共密钥基础结构（PKI）

Public switched telephone network (PSTN) A communications system that sets up a dedicated channel (or circuit) between two points for the duration of the transmission.
CHINESE SIMPLIFIED: 公用交换电话网(PSTN)

Q

Quality Being fit for purpose (achieving intended value) Scope Note: COBIT 5 perspective
CHINESE SIMPLIFIED: 质量

Quality assurance (QA) A planned and systematic pattern of all actions necessary to provide adequate confidence that an item or product conforms to established technical requirements. (ISO/IEC 24765)
CHINESE SIMPLIFIED: 质量保证

Quality management system (QMS) A system that outlines the policies and procedures necessary to improve and control the various processes that will ultimately lead to improved enterprise performance
CHINESE SIMPLIFIED: 质量管理系统

Queue A group of items that is waiting to be serviced or processed
CHINESE SIMPLIFIED: 队列

Quick ship A recovery solution provided by recovery and/or hardware vendors and includes a pre-established contract to deliver hardware resources within a specified number amount of hours after a disaster occurs Scope Note: The quick ship solution usually provides enterprises with the ability to recover within 72 or more hours.
CHINESE SIMPLIFIED: 快速付运

R

RACI chart Illustrates who is Responsible, Accountable, Consulted and Informed within an organizational framework
CHINESE SIMPLIFIED: RACI 表

Radio wave interference The superposition of two or more radio waves resulting in a different radio wave pattern that is more difficult to intercept and decode properly
CHINESE SIMPLIFIED: 无线电波干扰

Random access memory (RAM) The computer's primary working memory Scope Note: Each byte of RAM can be accessed randomly regardless of adjacent bytes.
CHINESE SIMPLIFIED: 随机访问内存

Range check Range checks ensure that data fall within a predetermined range
CHINESE SIMPLIFIED: 范围检查

Ransomware Malware that restricts access to the compromised systems until a ransom demand is satisfied
CHINESE SIMPLIFIED: 勒索软件

© 2015 ISACA All rights reserved.

Rapid application development A methodology that enables enterprises to develop strategically important systems faster, while reducing development costs and maintaining quality by using a series of proven application development techniques, within a well-defined methodology
CHINESE SIMPLIFIED: 快速应用开发

Real-time analysis Analysis that is performed on a continuous basis, with results gained in time to alter the run-time system
CHINESE SIMPLIFIED: 实时分析

Real-time processing An interactive online system capability that immediately updates computer files when transactions are initiated through a terminal
CHINESE SIMPLIFIED: 实时处理

Reasonable assurance A level of comfort short of a guarantee, but considered adequate given the costs of the control and the likely benefits achieved
CHINESE SIMPLIFIED: 合理的保证

Reasonableness check Compares data to predefined reasonability limits or occurrence rates established for the data
CHINESE SIMPLIFIED: 合理性检查

Reciprocal agreement Emergency processing agreement between two or more enterprises with similar equipment or applications Scope Note: Typically, participants of a reciprocal agreement promise to provide processing time to each other when an emergency arises.
CHINESE SIMPLIFIED: 互惠协议

Record A collection of related information that is treated as a unit Scope Note: Separate fields within the record are used for processing of the information.
CHINESE SIMPLIFIED: 记录

Record, screen and report layouts Record layouts provide information regarding the type of record, its size and the type of data contained in the record. Screen and report layouts describe what information is provided and necessary for input.
CHINESE SIMPLIFIED: 记录、屏幕和报表配置

Recovery The phase in the incident response plan that ensures that affected systems or services are restored to a condition specified in the service delivery objectives (SDOs) or business continuity plan (BCP)
CHINESE SIMPLIFIED: 恢复

Recovery action Execution of a response or task according to a written procedure
CHINESE SIMPLIFIED: 恢复操作

Recovery point objective (RPO) Determined based on the acceptable data loss in case of a disruption of operations.
It indicates the earliest point in time that is acceptable to recover the data. The RPO effectively quantifies the permissible amount of data loss in case of interruption.
CHINESE SIMPLIFIED: 恢复点目标

Recovery strategy An approach by an enterprise that will ensure its recovery and continuity in the face of a disaster or other major outage Scope Note: Plans and methodologies are determined by the enterprise's strategy. There may be more than one methodology or solution for an enterprise's strategy.
Examples of methodologies and solutions include: contracting for hot site or cold site, building an internal hot site or cold site, identifying an alternate work area, a consortium or reciprocal agreement, contracting for mobile recovery or crate and ship, and many others.
CHINESE SIMPLIFIED: 恢复策略

Recovery testing A test to check the system's ability to recover after a software or hardware failure
CHINESE SIMPLIFIED: 恢复测试

Recovery time objective (RTO) The amount of time allowed for the recovery of a business function or resource after a disaster occurs
CHINESE SIMPLIFIED: 恢复时间目标

Redo logs Files maintained by a system, primarily a database management system (DBMS), for the purpose of reapplying changes following an error or outage recovery
CHINESE SIMPLIFIED: 重做日志

Redundancy check Detects transmission errors by appending calculated bits onto the end of each segment of data
CHINESE SIMPLIFIED: 冗余检查

Redundant Array of Inexpensive Disks (RAID) Provides performance improvements and fault-tolerant capabilities via hardware or software solutions, by writing to a series of multiple disks to improve performance and/or save large files simultaneously
CHINESE SIMPLIFIED: 廉价磁盘冗余阵列

Redundant site A recovery strategy involving the duplication of key IT components, including data or other key business processes, whereby fast recovery can take place
CHINESE SIMPLIFIED: 冗余站点

Reengineering A process involving the extraction of components from existing systems and restructuring these components to develop new systems or to enhance the efficiency of existing systems Scope Note: Existing software systems can be modernized to prolong their functionality. An example is a software code translator that can take an existing hierarchical database system and transpose it to a relational database system.
Computer-aided software engineering (CASE) includes a source code reengineering feature.
CHINESE SIMPLIFIED: 再造

Registered ports Registered ports--1024 through 49151: Listed by the IANA and on most systems can be used by ordinary user processes or programs executed by ordinary users
CHINESE SIMPLIFIED: 注册端口

© 2015 ISACA All rights reserved.

Registration authority (RA) The individual institution that validates an entity's proof of identity and ownership of a key pair
CHINESE SIMPLIFIED: **注册机构（RA）**

Regression testing A testing technique used to retest earlier program abends or logical errors that occurred during the initial testing phase
CHINESE SIMPLIFIED: **回归测试**

Regulation Rules or laws defined and enforced by an authority to regulate conduct
CHINESE SIMPLIFIED: **规则**

Regulatory requirements Rules or laws that regulate conduct and that the enterprise must obey to become compliant
CHINESE SIMPLIFIED: **监管要求**

Relational database management system (RDBMS) The general purpose of a database is to store and retrieve related information. Scope Note: Database management systems have evolved from hierarchal to network to relational models. Today, the most widely accepted database model is the relational model. The relational model has three major aspects: structures, operations and integrity rules. An Oracle database is a collection of data that is treated as a unit.
CHINESE SIMPLIFIED: **关系数据库管理系统（RDBMS）**

Relevant audit evidence Audit evidence is relevant if it pertains to the audit objectives and has a logical relationship to the findings and conclusions it is used to support.
CHINESE SIMPLIFIED: **相关的审计证据**

Relevant information Relating to controls, tells the evaluator something meaningful about the operation of the underlying controls or control component. Information that directly confirms the operation of controls is most relevant. Information that relates indirectly to the operation of controls can also be relevant, but is less relevant than direct information. Scope Note: Refer to COBIT 5 information quality goals
CHINESE SIMPLIFIED: **相关信息**

Reliable audit evidence Audit evidence is reliable if, in the IS auditor's opinion, it is valid, factual, objective and supportable.
CHINESE SIMPLIFIED: **可靠的审计证据**

Reliable information Information that is accurate, verifiable and from an objective source Scope Note: Refer to COBIT 5 information quality goals
CHINESE SIMPLIFIED: **可靠信息**

Remediation After vulnerabilities are identified and assessed, appropriate remediation can take place to mitigate or eliminate the vulnerability
CHINESE SIMPLIFIED: **重整**

Remote access service (RAS) Refers to any combination of hardware and software to enable the remote access to tools or information that typically reside on a network of IT devices Scope Note: Originally coined by Microsoft when referring to their built-in NT remote access tools, RAS was a service provided by Windows NT which allowed most of the services that would be available on a network to be accessed over a modem link. Over the years, many vendors have provided both hardware and software solutions to gain remote access to various types of networked information. In fact, most modern routers include a basic RAS capability that can be enabled for any dial-up interface.
CHINESE SIMPLIFIED: **远程接入服务**

Remote Authentication Dial-in User Service (RADIUS) A type of service providing an authentication and accounting system often used for dial-up and remote access security
CHINESE SIMPLIFIED: **远程拨入用户认证服务（RADIUS）**

Remote job entry (RJE) The transmission of job control language (JCL) and batches of transactions from a remote terminal location
CHINESE SIMPLIFIED: **远程作业输入**

Remote procedure call (RPC) The traditional Internet service protocol widely used for many years on UNIX-based operating systems and supported by the Internet Engineering Task Force (IETF) that allows a program on one computer to execute a program on another (e.g., server) Scope Note: The primary benefit derived from its use is that a system developer need not develop specific procedures for the targeted computer system. For example, in a client-server arrangement, the client program sends a message to the server with appropriate arguments, and the server returns a message containing the results of the program executed. Common Object Request Broker Architecture (CORBA) and Distributed Component Object Model (DCOM) are two newer object-oriented methods for related RPC functionality.
CHINESE SIMPLIFIED: **远程过程调用（RPC）**

Removable media Any type of storage device that can be removed from the system while is running
CHINESE SIMPLIFIED: **可移动介质**

Repeaters A physical layer device that regenerates and propagates electrical signals between two network segments Scope Note: Repeaters receive signals from one network segment and amplify (regenerate) the signal to compensate for signals (analog or digital) distorted by transmission loss due to reduction of signal strength during transmission (i.e., attenuation)
CHINESE SIMPLIFIED: **中继器**

Replay The ability to copy a message or stream of messages between two parties and replay (retransmit) them to one or more of the parties
CHINESE SIMPLIFIED: **重放**

© 2015 ISACA All rights reserved.

Replication In its broad computing sense, involves the use of redundant software or hardware elements to provide availability and fault-tolerant capabilities. In a database context, replication involves the sharing of data between databases to reduce workload among database servers, thereby improving client performance while maintaining consistency among all systems.
CHINESE SIMPLIFIED: **重复**

Repository An enterprise database that stores and organizes data
CHINESE SIMPLIFIED: **贮存库**

Representation A signed or oral statement issued by management to professionals, where management declares that a current or future fact (e.g., process, system, procedure, policy) is or will be in a certain state, to the best of management's knowledge.
CHINESE SIMPLIFIED: **陈述**

Repudiation The denial by one of the parties to a transaction, or participation in all or part of that transaction, or of the content of communication related to that transaction
CHINESE SIMPLIFIED: **否认性**

Reputation risk The current and prospective effect on earnings and capital arising from negative public opinion Scope Note: Reputation risk affects a bank's ability to establish new relationships or services, or to continue servicing existing relationships. It may expose the bank to litigation, financial loss or a decline in its customer base. A bank's reputation can be damaged by Internet banking services that are executed poorly or otherwise alienate customers and the public. An Internet bank has a greater reputation risk as compared to a traditional brick-and-mortar bank, because it is easier for its customers to leave and go to a different Internet bank and since it cannot discuss any problems in person with the customer.
CHINESE SIMPLIFIED: **声誉风险**

Request for comments (RFC) A document that has been approved by the Internet Engineering Task Force (IETF) becomes an RFC and is assigned a unique number once published Scope Note: If the RFC gains enough interest, it may evolve into an Internet standard.
CHINESE SIMPLIFIED: **请求注解 (RFC)**

Request for proposal (RFP) A document distributed to software vendors requesting them to submit a proposal to develop or provide a software product
CHINESE SIMPLIFIED: **需求建议书**

Requirements definition A technique used in which the affected user groups define the requirements of the system for meeting the defined needs Scope Note: Some of these are business-, regulatory-, and security-related requirements as well as development-related requirements.
CHINESE SIMPLIFIED: **需求定义**

Residual risk The remaining risk after management has implemented a risk response
CHINESE SIMPLIFIED: **剩余风险**

Resilience The ability of a system or network to resist failure or to recover quickly from any disruption, usually with minimal recognizable effect
CHINESE SIMPLIFIED: **恢复能力**

Resource Any enterprise asset that can help the organization achieve its objectives Scope Note: COBIT 5 perspective
CHINESE SIMPLIFIED: **资源**

Resource optimization One of the governance objectives. Involves effective, efficient and responsible use of all resources—human, financial, equipment, facilities, etc. Scope Note: COBIT 5 perspective
CHINESE SIMPLIFIED: **资源优化**

Responsible In a Responsible, Accountable, Consulted, Informed (RACI) chart, refers to the person who must ensure that activities are completed successfully
CHINESE SIMPLIFIED: **负责人**

Return on investment (ROI) A measure of operating performance and efficiency, computed in its simplest form by dividing net income by the total investment over the period being considered
CHINESE SIMPLIFIED: **投资回报率（ROI）**

Return-oriented attacks An exploit technique in which the attacker uses control of the call stack to indirectly execute cherry-picked machine instructions immediately prior to the return instruction in subroutines within the existing program code
CHINESE SIMPLIFIED: **迂回攻击**

Reverse engineering A software engineering technique whereby an existing application system code can be redesigned and coded using computer-aided software engineering (CASE) technology
CHINESE SIMPLIFIED: **逆向工程**

Ring configuration Used in either token ring or fiber distributed data interface (FDDI) networks, all stations (nodes) are connected to a multi-station access unit (MSAU), that physically resembles a star-type topology. Scope Note: A ring configuration is created when MSAUs are linked together in forming a network. Messages in the network are sent in a deterministic fashion from sender and receiver via a small frame, referred to as a token ring. To send a message, a sender obtains the token with the right priority as the token travels around the ring, with receiving nodes reading those messages addressed to it.
CHINESE SIMPLIFIED: **环形配置**

Ring topology A type of local area network (LAN) architecture in which the cable forms a loop, with stations attached at intervals around the loop Scope Note: In ring topology, signals transmitted around the ring take the form of messages. Each station receives the messages and each station determines, on the basis of an address, whether to accept or process a given message. However, after receiving a message, each station acts as a repeater, retransmitting the message at its original signal strength.
CHINESE SIMPLIFIED: **环形拓扑**

© 2015 ISACA All rights reserved.

Risk The combination of the probability of an event and its consequence. (ISO/IEC 73)
CHINESE SIMPLIFIED: 风险

Risk acceptance If the risk is within the enterprise's risk tolerance or if the cost of otherwise mitigating the risk is higher than the potential loss, the enterprise can assume the risk and absorb any losses
CHINESE SIMPLIFIED: 风险接受度

Risk aggregation The process of integrating risk assessments at a corporate level to obtain a complete view on the overall risk for the enterprise
CHINESE SIMPLIFIED: 风险聚合

Risk analysis 1. A process by which frequency and magnitude of IT risk scenarios are estimated 2. The initial steps of risk management: analyzing the value of assets to the business, identifying threats to those assets and evaluating how vulnerable each asset is to those threats Scope Note: It often involves an evaluation of the probable frequency of a particular event, as well as the probable impact of that event.
CHINESE SIMPLIFIED: 风险分析

Risk appetite The amount of risk, on a broad level, that an entity is willing to accept in pursuit of its mission
CHINESE SIMPLIFIED: 风险偏好

Risk assessment A process used to identify and evaluate risk and its potential effects Scope Note: Risk assessments are used to identify those items or areas that present the highest risk, vulnerability or exposure to the enterprise for inclusion in the IS annual audit plan. Risk assessments are also used to manage the project delivery and project benefit risk.
CHINESE SIMPLIFIED: 风险评估

Risk avoidance The process for systematically avoiding risk, constituting one approach to managing risk
CHINESE SIMPLIFIED: 风险规避

Risk culture The set of shared values and beliefs that governs attitudes toward risk-taking, care and integrity, and determines how openly risk and losses are reported and discussed
CHINESE SIMPLIFIED: 风险文化

Risk evaluation The process of comparing the estimated risk against given risk criteria to determine the significance of the risk. [ISO/IEC Guide 73:2002]
CHINESE SIMPLIFIED: 风险评估

Risk factor A condition that can influence the frequency and/or magnitude and, ultimately, the business impact of IT-related events/scenarios
CHINESE SIMPLIFIED: 风险因素

Risk indicator A metric capable of showing that the enterprise is subject to, or has a high probability of being subject to, a risk that exceeds the defined risk appetite
CHINESE SIMPLIFIED: 风险指标

Risk management 1. The coordinated activities to direct and control an enterprise with regard to risk Scope Note: In the International Standard, the term "control" is used as a synonym for "measure." (ISO/IEC Guide 73:2002) 2. One of the governance objectives. Entails recognizing risk; assessing the impact and likelihood of that risk; and developing strategies, such as avoiding the risk, reducing the negative effect of the risk and/or transferring the risk, to manage it within the context of the enterprise's risk appetite. Scope Note: COBIT 5 perspective
CHINESE SIMPLIFIED: 风险管理

Risk map A (graphic) tool for ranking and displaying risk by defined ranges for frequency and magnitude
CHINESE SIMPLIFIED: 风险地图

Risk mitigation The management of risk through the use of countermeasures and controls
CHINESE SIMPLIFIED: 风险缓解

Risk owner The person in whom the organization has invested the authority and accountability for making risk-based decisions and who owns the loss associated with a realized risk scenario Scope Note: The risk owner may not be responsible for the implementation of risk treatment.
CHINESE SIMPLIFIED: 风险所有者

Risk portfolio view 1. A method to identify interdependencies and interconnections among risk, as well as the effect of risk responses on multiple types of risk 2. A method to estimate the aggregate impact of multiple types of risk (e.g., cascading and coincidental threat types/scenarios, risk concentration/correlation across silos) and the potential effect of risk response across multiple types of risk
CHINESE SIMPLIFIED: 风险组合观点

Risk reduction The implementation of controls or countermeasures to reduce the likelihood or impact of a risk to a level within the organization's risk tolerance.
CHINESE SIMPLIFIED: 风险缓释

Risk response Risk avoidance, risk acceptance, risk sharing/transfer, risk mitigation, leading to a situation that as much future residual risk (current risk with the risk response defined and implemented) as possible (usually depending on budgets available) falls within risk appetite limits
CHINESE SIMPLIFIED: 风险应对

Risk scenario The tangible and assessable representation of risk Scope Note: One of the key information items needed to identify, analyze and respond to risk (COBIT 5 Process APO12)
CHINESE SIMPLIFIED: 风险场景

Risk sharing Scope Note: See Risk transfer
CHINESE SIMPLIFIED: 风险分担

© 2015 ISACA All rights reserved.

Risk statement A description of the current conditions that may lead to the loss; and a description of the loss : Software Engineering Institute (SEI) Scope Note: For a risk to be understandable, it must be expressed clearly. Such a treatment must include a description of the current conditions that may lead to the loss; and a description of the loss.
CHINESE SIMPLIFIED: **风险声明**

Risk tolerance The acceptable level of variation that management is willing to allow for any particular risk as the enterprise pursues its objectives
CHINESE SIMPLIFIED: **风险容忍度**

Risk transfer The process of assigning risk to another enterprise, usually through the purchase of an insurance policy or by outsourcing the service
CHINESE SIMPLIFIED: **风险转移**

Risk treatment The process of selection and implementation of measures to modify risk (ISO/IEC Guide 73:2002)
CHINESE SIMPLIFIED: **风险处置**

Root cause analysis A process of diagnosis to establish the origins of events, which can be used for learning from consequences, typically from errors and problems
CHINESE SIMPLIFIED: **根本原因分析**

Rootkit A software suite designed to aid an intruder in gaining unauthorized administrative access to a computer system
CHINESE SIMPLIFIED: **Rootkit**

Rotating standby A fail-over process in which there are two nodes (as in idle standby but without priority) Scope Note: The node that enters the cluster first owns the resource group, and the second will join as a standby node.
CHINESE SIMPLIFIED: **轮替待机**

Rounding down A method of computer fraud involving a computer code that instructs the computer to remove small amounts of money from an authorized computer transaction by rounding down to the nearest whole value denomination and rerouting the rounded off amount to the perpetrator's account
CHINESE SIMPLIFIED: **去尾法**

Router A networking device that can send (route) data packets from one local area network (LAN) or wide area network (WAN) to another, based on addressing at the network layer (Layer 3) in the open systems interconnection (OSI) model Scope Note: Networks connected by routers can use different or similar networking protocols. Routers usually are capable of filtering packets based on parameters, such as source addresses, destination addresses, protocol and network applications (ports).
CHINESE SIMPLIFIED: **路由器**

RS-232 interface An interface between data terminal equipment and data communications equipment employing serial binary data interchange
CHINESE SIMPLIFIED: **RS-232 接口**

RSA A public key cryptosystem developed by R. Rivest, A. Shamir and L. Adleman used for both encryption and digital signatures Scope Note: The RSA has two different keys, the public encryption key and the secret decryption key. The strength of the RSA depends on the difficulty of the prime number factorization. For applications with high-level security, the number of the decryption key bits should be greater than 512 bits.
CHINESE SIMPLIFIED: **RSA加密系统**

Rulebase The list of rules and/or guidance that is used to analyze event data
CHINESE SIMPLIFIED: **规则库**

Run instructions Computer operating instructions which detail the step-by-step processes that are to occur so an application system can be properly executed; also identifies how to address problems that occur during processing
CHINESE SIMPLIFIED: **运行说明**

Run-to-run totals Provide evidence that a program processes all input data and that it processed the data correctly
CHINESE SIMPLIFIED: **运行总计**

S

Safeguard A practice, procedure or mechanism that reduces risk
CHINESE SIMPLIFIED: **保护措施**

Salami technique A method of computer fraud involving a computer code that instructs the computer to slice off small amounts of money from an authorized computer transaction and reroute this amount to the perpetrator's account
CHINESE SIMPLIFIED: **色拉米技术 (腊肠术) (一种计算机舞弊方法)**

Sampling risk The probability that an IS auditor has reached an incorrect conclusion because an audit sample, rather than the entire population, was tested Scope Note: While sampling risk can be reduced to an acceptably low level by using an appropriate sample size and selection method, it can never be eliminated.
CHINESE SIMPLIFIED: **抽样风险**

Sampling stratification The process of dividing a population into subpopulations with similar characteristics explicitly defined, so that each sampling unit can belong to only one stratum
CHINESE SIMPLIFIED: **分层抽样**

Scheduling A method used in the information processing facility (IPF) to determine and establish the sequence of computer job processing
CHINESE SIMPLIFIED: **日程计划安排**

© 2015 ISACA All rights reserved.

Scope creep Also called requirement creep, this refers to uncontrolled changes in a project's scope. Scope Note: Scope creep can occur when the scope of a project is not properly defined, documented and controlled. Typically, the scope increase consists of either new products or new features of already approved products. Hence, the project team drifts away from its original purpose. Because of one's tendency to focus on only one dimension of a project, scope creep can also result in a project team overrunning its original budget and schedule. For example, scope creep can be a result of poor change control, lack of proper identification of what products and features are required to bring about the achievement of project objectives in the first place, or a weak project manager or executive sponsor.
CHINESE SIMPLIFIED: **（项目）范围偏离**

Scoping process Identifying the boundary or extent to which a process, procedure, certification, contract, etc., applies
CHINESE SIMPLIFIED: **范围界定流程**

Screening routers A router configured to permit or deny traffic based on a set of permission rules installed by the administrator
CHINESE SIMPLIFIED: **用于扫描的路由器**

Secure Electronic Transaction (SET) A standard that will ensure that credit card and associated payment order information travels safely and securely between the various involved parties on the Internet.
CHINESE SIMPLIFIED: **安全电子交易标准(SET)**

Secure Multipurpose Internet Mail Extensions (S/MIME) Provides cryptographic security services for electronic messaging applications: authentication, message integrity and non-repudiation of origin (using digital signatures) and privacy and data security (using encryption) to provide a consistent way to send and receive MIME data. (RFC 2311)
CHINESE SIMPLIFIED: **安全多用途Internet邮件扩展协议(S/MIME)**

Secure Shell (SSH) Network protocol that uses cryptography to secure communication, remote command line login and remote command execution between two networked computers
CHINESE SIMPLIFIED: **安全外壳协议**

Secure Sockets Layer (SSL) A protocol that is used to transmit private documents through the Internet Scope Note: The SSL protocol uses a private key to encrypt the data that are to be transferred through the SSL connection.
CHINESE SIMPLIFIED: **安全套接字层**

Security administrator The person responsible for implementing, monitoring and enforcing security rules established and authorized by management
CHINESE SIMPLIFIED: **安全管理员**

Security as a Service (SecaaS) The next generation of managed security services dedicated to the delivery, over the Internet, of specialized information-security services.
CHINESE SIMPLIFIED: **安全即服务(SecaaS)**

Security awareness The extent to which every member of an enterprise and every other individual who potentially has access to the enterprise's information understand:
Security and the levels of security appropriate to the enterprise
The importance of security and consequences of a lack of security
Their individual responsibilities regarding security (and act accordingly) Scope Note: This definition is based on the definition for IT security awareness as defined in Implementation Guide: How to Make Your Organization Aware of IT Security, European Security Forum (ESF), London, 1993
CHINESE SIMPLIFIED: **安全意识**

Security awareness campaign A predefined, organized number of actions aimed at improving the security awareness of a special target audience about a specific security problem.
Each security awareness program consists of a number of security awareness campaigns.
CHINESE SIMPLIFIED: **安全意识活动**

Security awareness coordinator The individual responsible for setting up and maintaining the security awareness program and coordinating the different campaigns and efforts of the various groups involved in the program.
He/she is also responsible for making sure that all materials are prepared, advocates/trainers are trained, campaigns are scheduled, events are publicized and the program as a whole moves forward.
CHINESE SIMPLIFIED: **安全意识协调人**

Security awareness program A clearly and formally defined plan, structured approach, and set of related activities and procedures with the objective of realizing and maintaining a security-aware culture Scope Note: This definition clearly states that it is about realizing and maintaining a security-aware culture, meaning attaining and sustaining security awareness at all times. This implies that a security awareness program is not a one-time effort, but a continuous process.
CHINESE SIMPLIFIED: **安全意识计划**

© 2015 ISACA All rights reserved.

Security forum Responsible for information security governance within the enterprise Scope Note: A security forum can be part of an existing management body. Because information security is a business responsibility shared by all members of the executive management team, the forum needs to involve executives from all significant parts of the enterprise. Typically, a security forum has the following tasks and responsibilities:
Defining a security strategy in line with the business strategy
Identifying security requirements
Establishing a security policy
Drawing up an overall security program or plan
Approving major initiatives to enhance information security
Reviewing and monitoring information security incidents
Monitoring significant changes in the exposure of information assets to major threats
CHINESE SIMPLIFIED: 安全论坛

Security incident A series of unexpected events that involves an attack or series of attacks (compromise and/or breach of security) at one or more sites.
A security incident normally includes an estimation of its level of impact. A limited number of impact levels are defined and, for each, the specific actions required and the people who need to be notified are identified.
CHINESE SIMPLIFIED: 安全事故

Security management The process of establishing and maintaining security for a computer or network system Scope Note: The stages of the process of security management include prevention of security problems, detection of intrusions, and investigation of intrusions and resolution. In network management, the stages are: controlling access to the network and resources, finding intrusions, identifying entry points for intruders and repairing or otherwise closing those avenues of access.
CHINESE SIMPLIFIED: 安全管理

Security metrics A standard of measurement used in management of security-related activities
CHINESE SIMPLIFIED: 安全指标

Security perimeter The boundary that defines the area of security concern and security policy coverage
CHINESE SIMPLIFIED: 安全边界

Security policy A high-level document representing an enterprise's information security philosophy and commitment
CHINESE SIMPLIFIED: 安全政策

Security procedures The formal documentation of operational steps and processes that specify how security goals and objectives set forward in the security policy and standards are to be achieved
CHINESE SIMPLIFIED: 安全程序

Security software Software used to administer security, which usually includes authentication of users, access granting according to predefined rules, monitoring and reporting functions
CHINESE SIMPLIFIED: 安全软件

Security standards Practices, directives, guidelines, principles or baselines that state what needs to be done and focus areas of current relevance and concern; they are a translation of issues already mentioned in the security policy
CHINESE SIMPLIFIED: 安全标准

Security testing Ensuring that the modified or new system includes appropriate controls and does not introduce any security holes that might compromise other systems or misuses of the system or its information
CHINESE SIMPLIFIED: 安全测试

Security/transaction risk The current and prospective risk to earnings and capital arising from fraud, error and the inability to deliver products or services, maintain a competitive position, and manage information Scope Note: Security risk is evident in each product and service offered, and it encompasses product development and delivery, transaction processing, systems development, computing systems, complexity of products and services and the internal control environment. A high level of security risk may exist with Internet banking products, particularly if those lines of business are not adequately planned, implemented and monitored.
CHINESE SIMPLIFIED: 安全/交易风险

Segregation/separation of duties (SoD) A basic internal control that prevents or detects errors and irregularities by assigning to separate individuals the responsibility for initiating and recording transactions and for the custody of assets Scope Note: Segregation/separation of duties is commonly used in large IT organizations so that no single person is in a position to introduce fraudulent or malicious code without detection.
CHINESE SIMPLIFIED: 职责分离 (SoD)

Sensitivity A measure of the impact that improper disclosure of information may have on an enterprise
CHINESE SIMPLIFIED: 敏感度

Sequence check Verification that the control number follows sequentially and any control numbers out of sequence are rejected or noted on an exception report for further research Scope Note: Can be alpha or numeric and usually utilizes a key field
CHINESE SIMPLIFIED: 顺序检查

Sequential file A computer file storage format in which one record follows another Scope Note: Records can be accessed sequentially only. It is required with magnetic tape.
CHINESE SIMPLIFIED: 顺序文件

Service bureau A computer facility that provides data processing services to clients on a continual basis
CHINESE SIMPLIFIED: 服务中心

Service catalogue Structured information on all IT services available to customers Scope Note: COBIT 5 perspective
CHINESE SIMPLIFIED: 服务目录

© 2015 ISACA All rights reserved.

Service delivery objective (SDO) Directly related to the business needs, SDO is the level of services to be reached during the alternate process mode until the normal situation is restored
CHINESE SIMPLIFIED: **服务交付目标 (SDO)**

Service desk The point of contact within the IT organization for users of IT services
CHINESE SIMPLIFIED: **服务台**

Service level agreement (SLA) An agreement, preferably documented, between a service provider and the customer(s)/user(s) that defines minimum performance targets for a service and how they will be measured
CHINESE SIMPLIFIED: **服务水平协议**

Service provider An organization supplying services to one or more (internal or external) customers
CHINESE SIMPLIFIED: **服务提供商**

Service Set Identifier (SSID) A 32-character unique identifier attached to the header of packets sent over a wireless local area network (WLAN) that acts as a password when a mobile device tries to connect to the base station subsystem (BSS). Scope Note: The SSID differentiates one WLAN from another so all access points and all devices attempting to connect to a specific WLAN must use the same SSID. A device will not be permitted to join the BSS unless it can provide the unique SSID. Because an SSID can be sniffed in plaintext from a packet, it does not supply any security to the network. An SSID is also referred to as a network name, because it is a name that identifies a wireless network.
CHINESE SIMPLIFIED: **服务集标识符（SSID）**

Service user The organization using the outsourced service.
CHINESE SIMPLIFIED: **服务用户**

Service-oriented architecture (SOA) A cloud-based library of proven, functional software applets that are able to be connected together to become a useful online application
CHINESE SIMPLIFIED: **面向服务的体系结构 (SOA)**

Servlet A Java applet or a small program that runs within a web server environment Scope Note: A Java servlet is similar to a common gateway interface (CGI) program, but unlike a CGI program, once started, it stays in memory and can fulfill multiple requests, thereby saving server execution time and speeding up the services.
CHINESE SIMPLIFIED: **小服务程序**

Session border controller (SBC) Provide security features for voice-over IP (VoIP) traffic similar to that provided by firewalls Scope Note: SBCs can be configured to filter specific VoIP protocols, monitor for denial-of-service (DOS) attacks, and provide network address and protocol translation features.
CHINESE SIMPLIFIED: **会话边界控制器 (SBC)**

Shell The interface between the user and the system
CHINESE SIMPLIFIED: **Shell**

Shell programming A script written for the shell, or command line interpreter, of an operating system; it is often considered a simple domain-specific programming language Scope Note: Typical operations performed by shell scripts include file manipulation, program execution and printing text. Usually, shell script refers to scripts written for a UNIX shell, while command.com (DOS) and cmd.exe (Windows) command line scripts are usually called batch files. Many shell script interpreters double as a command line interface such as the various UNIX shells, Windows PowerShell or the MS-DOS command.com. Others, such as AppleScript, add scripting capability to computing environments lacking a command line interface. Other examples of programming languages primarily intended for shell scripting include digital command language (DCL) and job control language (JCL).
CHINESE SIMPLIFIED: **Shell 编程**

Significant deficiency A deficiency or a combination of deficiencies, in internal control, that is less severe than a material weakness, yet important enough to merit attention by those responsible for oversight Scope Note: A material weakness is a significant deficiency or a combination of significant deficiencies that results in more than a remote likelihood of an undesirable event(s) not being prevented or detected.
CHINESE SIMPLIFIED: **重大缺陷**

Sign-on procedure The procedure performed by a user to gain access to an application or operating system Scope Note: If the user is properly identified and authenticated by the system's security, they will be able to access the software.
CHINESE SIMPLIFIED: **登录流程**

Simple fail-over A fail-over process in which the primary node owns the resource group Scope Note: The backup node runs a non-critical application (e.g., a development or test environment) and takes over the critical resource group, but not vice versa.
CHINESE SIMPLIFIED: **简单故障切换**

Simple Mail Transfer Protocol (SMTP) The standard electronic mail (e-mail) protocol on the Internet
CHINESE SIMPLIFIED: **简单邮件传输协议 (SMTP)**

© 2015 ISACA All rights reserved.

Simple Object Access Protocol (SOAP) A platform-independent formatted protocol based on extensible markup language (XML) enabling applications to communicate with each other over the Internet Scope Note: Use of SOAP may provide a significant security risk to web application operations because use of SOAP piggybacks onto a web-based document object model and is transmitted via HyperText Transfer Protocol (HTTP) (port 80) to penetrate server firewalls, which are usually configured to accept port 80 and port 21 File Transfer Protocol (FTP) requests. Web-based document models define how objects on a web page are associated with each other and how they can be manipulated while being sent from a server to a client browser. SOAP typically relies on XML for presentation formatting and also adds appropriate HTTP-based headers to send it. SOAP forms the foundation layer of the web services stack, providing a basic messaging framework on which more abstract layers can build. There are several different types of messaging patterns in SOAP, but by far the most common is the Remote Procedure Call (RPC) pattern, in which one network node (the client) sends a request message to another node (the server), and the server immediately sends a response message to the client.
CHINESE SIMPLIFIED: **简单对象访问协议（SOAP）**

Single factor authentication (SFA) Authentication process that requires only the user ID and password to grant access
CHINESE SIMPLIFIED: **单因素认证**

Single point of failure A resource whose loss will result in the loss of service or production
CHINESE SIMPLIFIED: **单点故障**

Skill The learned capacity to achieve pre-determined results Scope Note: COBIT 5 perspective
CHINESE SIMPLIFIED: **技能**

Slack time (float) Time in the project schedule, the use of which does not affect the project's critical path; the minimum time to complete the project based on the estimated time for each project segment and their relationships Scope Note: Slack time is commonly referred to as "float" and generally is not "owned" by either party to the transaction.
CHINESE SIMPLIFIED: **松弛时间**

SMART Specific, measurable, attainable, realistic and timely, generally used to describe appropriately set goals
CHINESE SIMPLIFIED: **SMART**

Smart card A small electronic device that contains electronic memory, and possibly an embedded integrated circuit Scope Note: Smart cards can be used for a number of purposes including the storage of digital certificates or digital cash, or they can be used as a token to authenticate users.
CHINESE SIMPLIFIED: **智能卡**

Sniff The act of capturing network packets, including those not necessarily destined for the computer running the sniffing software
CHINESE SIMPLIFIED: **嗅探**

Sniffing The process by which data traversing a network are captured or monitored
CHINESE SIMPLIFIED: **嗅探**

Social engineering An attack based on deceiving users or administrators at the target site into revealing confidential or sensitive information
CHINESE SIMPLIFIED: **社会工程**

Software Programs and supporting documentation that enable and facilitate use of the computer Scope Note: Software controls the operation of the hardware and the processing of data.
CHINESE SIMPLIFIED: **软件**

Software as a service (SaaS) Offers the capability to use the provider's applications running on cloud infrastructure. The applications are accessible from various client devices through a thin client interface such as a web browser (e.g., web-based e-mail).
CHINESE SIMPLIFIED: **软件即服务 (SaaS)**

Software as a service, platform as a service and infrastructure as a service (SPI) The acronym used to refer to the three cloud delivery models
CHINESE SIMPLIFIED: **软件即服务、平台即服务与基础架构即服务 (SPI)**

Source code The language in which a program is written Scope Note: Source code is translated into object code by assemblers and compilers. In some cases, source code may be converted automatically into another language by a conversion program. Source code is not executable by the computer directly. It must first be converted into a machine language.
CHINESE SIMPLIFIED: **源代码**

Source code compare program Provides assurance that the software being audited is the correct version of the software, by providing a meaningful listing of any discrepancies between the two versions of the program
CHINESE SIMPLIFIED: **源代码比较程序**

Source document The form used to record data that have been captured Scope Note: A source document may be a piece of paper, a turnaround document or an image displayed for online data input.
CHINESE SIMPLIFIED: **原始文件(凭证)**

Source lines of code (SLOC) Often used in deriving single-point software-size estimations
CHINESE SIMPLIFIED: **源代码行数 (SLOC)**

Source routing specification A transmission technique where the sender of a packet can specify the route that packet should follow through the network
CHINESE SIMPLIFIED: **源路由规范**

Spam Computer-generated messages sent as unsolicited advertising
CHINESE SIMPLIFIED: **垃圾邮件**

© 2015 ISACA All rights reserved.

Spanning port A port configured on a network switch to receive copies of traffic from one or more other ports on the switch
CHINESE SIMPLIFIED: **映射端口**

Spear phishing An attack where social engineering techniques are used to masquerade as a trusted party to obtain important information such as passwords from the victim
CHINESE SIMPLIFIED: **鱼叉式网络钓鱼**

Split data systems A condition in which each of an enterprise's regional locations maintains its own financial and operational data while sharing processing with an enterprisewide, centralized database Scope Note: Split data systems permit easy sharing of data while maintaining a certain level of autonomy.
CHINESE SIMPLIFIED: **拆分数据系统**

Split domain name system (DNS) An implementation of DNS that is intended to secure responses provided by the server such that different responses are given to internal vs. external users
CHINESE SIMPLIFIED: **拆分式域名系统 (DNS)**

Split knowledge/split key A security technique in which two or more entities separately hold data items that individually convey no knowledge of the information that results from combining the items; a condition under which two or more entities separately have key components that individually convey no knowledge of the plain text key that will be produced when the key components are combined in the cryptographic module
CHINESE SIMPLIFIED: **拆分知识/拆分密钥**

Spoofing Faking the sending address of a transmission in order to gain illegal entry into a secure system
CHINESE SIMPLIFIED: **冒充**

SPOOL (simultaneous peripheral operations online) An automated function that can be based on an operating system or application in which electronic data being transmitted between storage areas are spooled or stored until the receiving device or storage area is prepared and able to receive the information Scope Note: Spool allows more efficient electronic data transfers from one device to another by permitting higher speed sending functions, such as internal memory, to continue on with other operations instead of waiting on the slower speed receiving device, such as a printer.
CHINESE SIMPLIFIED: **假脱机 (外围设备同时联机操作)**

Spyware Software whose purpose is to monitor a computer user's actions (e.g., web sites visited) and report these actions to a third party, without the informed consent of that machine's owner or legitimate user Scope Note: A particularly malicious form of spyware is software that monitors keystrokes to obtain passwords or otherwise gathers sensitive information such as credit card numbers, which it then transmits to a malicious third party. The term has also come to refer more broadly to software that subverts the computer's operation for the benefit of a third party.
CHINESE SIMPLIFIED: **间谍软件**

SQL injection Results from failure of the application to appropriately validate input. When specially crafted user-controlled input consisting of SQL syntax is used without proper validation as part of SQL queries, it is possible to glean information from the database in ways not envisaged during application design. (MITRE)
CHINESE SIMPLIFIED: **SQL注入**

Stage-gate A point in time when a program is reviewed and a decision is made to commit expenditures to the next set of activities on a program or project, to stop the work altogether, or to put a hold on execution of further work
CHINESE SIMPLIFIED: **阶段-关卡**

Stakeholder Anyone who has a responsibility for, an expectation from or some other interest in the enterprise. Scope Note: Examples: shareholders, users, government, suppliers, customers and the public
CHINESE SIMPLIFIED: **利益相关方**

Standard A mandatory requirement, code of practice or specification approved by a recognized external standards organization, such as International Organization for Standardization (ISO)
CHINESE SIMPLIFIED: **标准**

Standing data Permanent reference data used in transaction processing Scope Note: These data are changed infrequently, such as a product price file or a name and address file.
CHINESE SIMPLIFIED: **永久性数据**

Star topology A type of local area network (LAN) architecture that utilizes a central controller to which all nodes are directly connected Scope Note: With star topology, all transmissions from one station to another pass through the central controller which is responsible for managing and controlling all communication. The central controller often acts as a switching device.
CHINESE SIMPLIFIED: **星型拓扑**

Stateful inspection A firewall architecture that tracks each connection traversing all interfaces of the firewall and makes sure they are valid.
CHINESE SIMPLIFIED: **状态检测**

Static analysis Analysis of information that occurs on a non-continuous basis; also known as interval-based analysis
CHINESE SIMPLIFIED: **静态分析**

Statistical sampling A method of selecting a portion of a population, by means of mathematical calculations and probabilities, for the purpose of making scientifically and mathematically sound inferences regarding the characteristics of the entire population
CHINESE SIMPLIFIED: **统计抽样**

Statutory requirements Laws created by government institutions
CHINESE SIMPLIFIED: **法定要求**

© 2015 ISACA All rights reserved.

Storage area networks (SANs) A variation of a local area network (LAN) that is dedicated for the express purpose of connecting storage devices to servers and other computing devices Scope Note: SANs centralize the process for the storage and administration of data.
CHINESE SIMPLIFIED: **存储区域网络 (SAN)**

Strategic planning The process of deciding on the enterprise's objectives, on changes in these objectives, and the policies to govern their acquisition and use
CHINESE SIMPLIFIED: **战略计划**

Strengths, weaknesses, opportunities and threats (SWOT) A combination of an organizational audit listing the enterprise's strengths and weaknesses and an environmental scan or analysis of external opportunities and threats
CHINESE SIMPLIFIED: **优势、劣势、机会、威胁 (SWOT)**

Structured programming A top-down technique of designing programs and systems that makes programs more readable, more reliable and more easily maintained
CHINESE SIMPLIFIED: **结构化程序设计**

Structured Query Language (SQL) The primary language used by both application programmers and end users in accessing relational databases
CHINESE SIMPLIFIED: **结构化查询语言**

Subject matter The specific information subject to an IS auditor's report and related procedures, which can include things such as the design or operation of internal controls and compliance with privacy practices or standards or specified laws and regulations (area of activity)
CHINESE SIMPLIFIED: **主题**

Substantive testing Obtaining audit evidence on the completeness, accuracy or existence of activities or transactions during the audit period
CHINESE SIMPLIFIED: **实质性测试**

Sufficient audit evidence Audit evidence is sufficient if it is adequate, convincing and would lead another IS auditor to form the same conclusions.
CHINESE SIMPLIFIED: **充分的审计证据**

Sufficient evidence The measure of the quantity of audit evidence; supports all material questions to the audit objective and scope Scope Note: See evidence
CHINESE SIMPLIFIED: **充足的证据**

Sufficient information Information is sufficient when evaluators have gathered enough of it to form a reasonable conclusion. For information to be sufficient, however, it must first be suitable. Scope Note: Refer to COBIT 5 information quality goals
CHINESE SIMPLIFIED: **充足的信息**

Suitable information Relevant (i.e., fit for its intended purpose), reliable (i.e., accurate, verifiable and from an objective source) and timely (i.e., produced and used in an appropriate time frame)information Scope Note: Refer to COBIT 5 information quality goals
CHINESE SIMPLIFIED: **适当的信息**

Supervisory control and data acquisition (SCADA) Systems used to control and monitor industrial and manufacturing processes, and utility facilities
CHINESE SIMPLIFIED: **监控和数据采集(SCADA)**

Supply chain management (SCM) A concept that allows an enterprise to more effectively and efficiently manage the activities of design, manufacturing, distribution, service and recycling of products and service its customers
CHINESE SIMPLIFIED: **供应链管理 (SCM)**

Surge suppressor Filters out electrical surges and spikes
CHINESE SIMPLIFIED: **浪涌抑制器**

Suspense file A computer file used to maintain information (transactions, payments or other events) until the proper disposition of that information can be determined Scope Note: Once the proper disposition of the item is determined, it should be removed from the suspense file and processed in accordance with the proper procedures for that particular transaction. Two examples of items that may be included in a suspense file are receipt of a payment from a source that is not readily identified or data that do not yet have an identified match during migration to a new application.
CHINESE SIMPLIFIED: **挂起文件**

Switches Typically associated as a data link layer device, switches enable local area network (LAN) segments to be created and interconnected, which has the added benefit of reducing collision domains in Ethernet-based networks.
CHINESE SIMPLIFIED: **交换机**

Symmetric key encryption System in which a different key (or set of keys) is used by each pair of trading partners to ensure that no one else can read their messages.
The same key is used for encryption and decryption. See also Private Key Cryptosystem.
CHINESE SIMPLIFIED: **对称密钥加密**

Synchronize (SYN) A flag set in the initial setup packets to indicate that the communicating parties are synchronizing the sequence numbers used for the data transmission
CHINESE SIMPLIFIED: **同步 (SYN)**

Synchronous transmission Block-at-a-time data transmission
CHINESE SIMPLIFIED: **同步传输**

© 2015 ISACA All rights reserved.

System development life cycle (SDLC) The phases deployed in the development or acquisition of a software system Scope Note: SDLC is an approach used to plan, design, develop, test and implement an application system or a major modification to an application system. Typical phases of SDLC include the feasibility study, requirements study, requirements definition, detailed design, programming, testing, installation and post-implementation review, but not the service delivery or benefits realization activities.
CHINESE SIMPLIFIED: **系统开发生命周期 (SDLC)**

System exit Special system software features and utilities that allow the user to perform complex system maintenance Scope Note: Use of system exits often permits the user to operate outside of the security access control system.
CHINESE SIMPLIFIED: **系统退出**

System flowchart Graphic representations of the sequence of operations in an information system or program Scope Note: Information system flowcharts show how data from source documents flow through the computer to final distribution to users. Symbols used should be the internationally accepted standard. System flowcharts should be updated when necessary.
CHINESE SIMPLIFIED: **系统流程图**

System hardening A process to eliminate as many security risks as possible by removing all nonessential software programs, protocols, services and utilities from the system
CHINESE SIMPLIFIED: **系统加固**

System narrative Provides an overview explanation of system flowcharts, with explanation of key control points and system interfaces
CHINESE SIMPLIFIED: **系统叙述**

System of internal control The policies, standards, plans and procedures, and organizational structures designed to provide reasonable assurance that enterprise objectives will be achieved and undesired events will be prevented or detected and corrected Scope Note: COBIT 5 perspective
CHINESE SIMPLIFIED: **内部控制系统**

System software A collection of computer programs used in the design, processing and control of all applications Scope Note: The programs and processing routines that control the computer hardware, including the operating system and utility programs
CHINESE SIMPLIFIED: **系统软件**

System testing Testing conducted on a complete, integrated system to evaluate the system's compliance with its specified requirements Scope Note: System test procedures typically are performed by the system maintenance staff in their development library.
CHINESE SIMPLIFIED: **系统测试**

Systems acquisition process Procedures established to purchase application software, or an upgrade, including evaluation of the supplier's financial stability, track record, resources and references from existing customers
CHINESE SIMPLIFIED: **系统购置流程**

Systems analysis The systems development phase in which systems specifications and conceptual designs are developed based on end-user needs and requirements
CHINESE SIMPLIFIED: **系统分析**

T

Table look-up Used to ensure that input data agree with predetermined criteria stored in a table
CHINESE SIMPLIFIED: **表格检查**

Tangible asset Any assets that has physical form
CHINESE SIMPLIFIED: **有形资产**

Tape management system (TMS) A system software tool that logs, monitors and directs computer tape usage
CHINESE SIMPLIFIED: **磁带管理系统**

Taps Wiring devices that may be inserted into communication links for use with analysis probes, local area network (LAN) analyzers and intrusion detection security systems
CHINESE SIMPLIFIED: **分流器**

Target Person or asset selected as the aim of an attack
CHINESE SIMPLIFIED: **攻击目标**

Tcpdump A network monitoring and data acquisition tool that performs filter translation, packet acquisition and packet display
CHINESE SIMPLIFIED: **Tcpdump**

Technical infrastructure security Refers to the security of the infrastructure that supports the enterprise resource planning (ERP) networking and telecommunications, operating systems, and databases
CHINESE SIMPLIFIED: **技术基础设施的安全**

Technology infrastructure Technology, human resources (HR) and facilities that enable the processing and use of applications
CHINESE SIMPLIFIED: **技术基础设施**

Technology infrastructure plan A plan for the technology, human resources and facilities that enable the current and future processing and use of applications
CHINESE SIMPLIFIED: **技术基础设施计划**

Telecommunications Electronic communication by special devices over distances or around devices that preclude direct interpersonal exchange
CHINESE SIMPLIFIED: **电子通讯**

© 2015 ISACA All rights reserved.

Teleprocessing Using telecommunications facilities for handling and processing of computerized information
CHINESE SIMPLIFIED: **远程处理**

Telnet Network protocol used to enable remote access to a server computer Scope Note: Commands typed are run on the remote server.
CHINESE SIMPLIFIED: **Telnet**

Terminal Access Controller Access Control System Plus (TACACS+) An authentication protocol, often used by remote-access servers
CHINESE SIMPLIFIED: **终端访问控制器访问控制系统+ (TACACS+)**

Terms of reference A document that confirms a client's and an IS auditor's acceptance of a review assignment
CHINESE SIMPLIFIED: **职权范围**

Test data Simulated transactions that can be used to test processing logic, computations and controls actually programmed in computer applications.
Individual programs or an entire system can be tested. Scope Note: This technique includes Integrated Test Facilities (ITFs) and Base Case System Evaluations (BCSEs).
CHINESE SIMPLIFIED: **测试数据**

Test generators Software used to create data to be used in the testing of computer programs
CHINESE SIMPLIFIED: **测试生成器**

Test programs Programs that are tested and evaluated before approval into the production environment Scope Note: Test programs, through a series of change control moves, migrate from the test environment to the production environment and become production programs.
CHINESE SIMPLIFIED: **测试程序**

Test types Test types include:
Checklist test--Copies of the business continuity plan (BCP) are distributed to appropriate personnel for review
Structured walk through--Identified key personnel walk through the plan to ensure that the plan accurately reflects the enterprise's ability to recover successfully
Simulation test--All operational and support personnel are expected to perform a simulated emergency as a practice session
Parallel Test--Critical systems are run at alternate site (hot, cold, warm or reciprocal)
Complete interruption test--Disaster is replicated, normal production is shut down with real time recovery process
CHINESE SIMPLIFIED: **测试类型**

Testing The examination of a sample from a population to estimate characteristics of the population
CHINESE SIMPLIFIED: **测试**

Third-party review An independent audit of the control structure of a service organization, such as a service bureau, with the objective of providing assurance to the users of the service organization that the internal control structure is adequate, effective and sound
CHINESE SIMPLIFIED: **第三方审查**

Threat Anything (e.g., object, substance, human) that is capable of acting against an asset in a manner that can result in harm Scope Note: A potential cause of an unwanted incident (ISO/IEC 13335)
CHINESE SIMPLIFIED: **威胁**

Threat agent Methods and things used to exploit a vulnerability Scope Note: Examples include determination, capability, motive and resources.
CHINESE SIMPLIFIED: **威胁代理**

Threat analysis An evaluation of the type, scope and nature of events or actions that can result in adverse consequences; identification of the threats that exist against enterprise assets Scope Note: The threat analysis usually defines the level of threat and the likelihood of it materializing.
CHINESE SIMPLIFIED: **威胁分析**

Threat event Any event during which a threat element/actor acts against an asset in a manner that has the potential to directly result in harm
CHINESE SIMPLIFIED: **威胁事件**

Threat vector The path or route used by the adversary to gain access to the target
CHINESE SIMPLIFIED: **威胁路径**

Throughput The quantity of useful work made by the system per unit of time. Throughput can be measured in instructions per second or some other unit of performance. When referring to a data transfer operation, throughput measures the useful data transfer rate and is expressed in kbps, Mbps and Gbps.
CHINESE SIMPLIFIED: **吞吐量**

Timelines Chronological graphs where events related to an incident can be mapped to look for relationships in complex cases Scope Note: Timelines can provide simplified visualization for presentation to management and other non-technical audiences.
CHINESE SIMPLIFIED: **时间表**

Timely information Produced and used in a time frame that makes it possible to prevent or detect control deficiencies before they become material to an enterprise Scope Note: Refer to COBIT 5 information quality goals
CHINESE SIMPLIFIED: **适时信息**

Token A device that is used to authenticate a user, typically in addition to a username and password Scope Note: A token is usually a device the size of a credit card that displays a pseudo random number that changes every few minutes.
CHINESE SIMPLIFIED: **令牌**

© 2015 ISACA All rights reserved.

Token ring topology A type of local area network (LAN) ring topology in which a frame containing a specific format, called the token, is passed from one station to the next around the ring Scope Note: When a station receives the token, it is allowed to transmit. The station can send as many frames as desired until a predefined time limit is reached. When a station either has no more frames to send or reaches the time limit, it transmits the token. Token passing prevents data collisions that can occur when two computers begin transmitting at the same time.
CHINESE SIMPLIFIED: **令牌环拓扑**

Tolerable error The maximum error in the population that professionals are willing to accept and still conclude that the test objective has been achieved. For substantive tests, tolerable error is related to professionals' judgement about materiality. In compliance tests, it is the maximum rate of deviation from a prescribed control procedure that the professionals are willing to accept
CHINESE SIMPLIFIED: **可容忍误差**

Top-level management The highest level of management in the enterprise, responsible for direction and control of the enterprise as a whole (such as director, general manager, partner, chief officer and executive manager)
CHINESE SIMPLIFIED: **高层管理人员**

Topology The physical layout of how computers are linked together Scope Note: Examples of topology include ring, star and bus.
CHINESE SIMPLIFIED: **拓扑**

Total cost of ownership (TCO) Includes the original cost of the computer plus the cost of: software, hardware and software upgrades, maintenance, technical support, training, and certain activities performed by users
CHINESE SIMPLIFIED: **总拥有成本 (TCO)**

Transaction Business events or information grouped together because they have a single or similar purpose Scope Note: Typically, a transaction is applied to a calculation or event that then results in the updating of a holding or master file.
CHINESE SIMPLIFIED: **交易**

Transaction log A manual or automated log of all updates to data files and databases
CHINESE SIMPLIFIED: **交易日志**

Transaction protection Also known as "automated remote journaling of redo logs," a data recovery strategy that is similar to electronic vaulting except that instead of transmitting several transaction batches daily, the archive logs are shipped as they are created
CHINESE SIMPLIFIED: **交易保护**

Transmission Control Protocol (TCP) A connection-based Internet protocol that supports reliable data transfer connections Scope Note: Packet data are verified using checksums and retransmitted if they are missing or corrupted. The application plays no part in validating the transfer.
CHINESE SIMPLIFIED: **传输控制协议**

Transmission Control Protocol/Internet Protocol (TCP/IP) Provides the basis for the Internet; a set of communication protocols that encompass media access, packet transport, session communication, file transfer, electronic mail (e-mail), terminal emulation, remote file access and network management
CHINESE SIMPLIFIED: **传输控制协议/互联网协议 (TCP/IP)**

Transparency Refers to an enterprise's openness about its activities and is based on the following concepts:

How the mechanism functions is clear to those who are affected by or want to challenge governance decisions.
A common vocabulary has been established.
Relevant information is readily available. Scope Note: Transparency and stakeholder trust are directly related; the more transparency in the governance process, the more confidence in the governance.
CHINESE SIMPLIFIED: **透明度**

Transport Layer Security (TLS) A protocol that provides communications privacy over the Internet. The protocol allows client/server applications to communicate in a way that is designed to prevent eavesdropping, tampering, or message forgery. (RFC 2246) Scope Note: Transport Layer Security (TLS) is composed of two layers: the TLS Record Protocol and the TLS Handshake Protocol. The TLS Record Protocol provides connection security with some encryption method such as the Data Encryption Standard (DES). The TLS Record Protocol can also be used without encryption. The TLS Handshake Protocol allows the server and client to authenticate each other and to negotiate an encryption algorithm and cryptographic keys before data is exchanged.
CHINESE SIMPLIFIED: **传输层安全协议 (TLS)**

Trap door Unauthorized electronic exit, or doorway, out of an authorized computer program into a set of malicious instructions or programs
CHINESE SIMPLIFIED: **陷阱门**

Triple DES (3DES) A block cipher created from the Data Encryption Standard (DES) cipher by using it three times
CHINESE SIMPLIFIED: **三重DES加密 (3DES)**

Trojan horse Purposefully hidden malicious or damaging code within an authorized computer program Scope Note: Unlike viruses, they do not replicate themselves, but they can be just as destructive to a single computer.
CHINESE SIMPLIFIED: **特洛伊木马**

Trusted process A process certified as supporting a security goal
CHINESE SIMPLIFIED: **可信过程**

© 2015 ISACA All rights reserved.

Trusted system A system that employs sufficient hardware and software assurance measures to allow their use for processing a range of sensitive or classified information
CHINESE SIMPLIFIED: 可信系统

Tunnel The paths that the encapsulated packets follow in an Internet virtual private network (VPN)
CHINESE SIMPLIFIED: 隧道

Tunnel mode Used to protect traffic between different networks when traffic must travel through intermediate or untrusted networks. Tunnel mode encapsulates the entire IP packet with and AH or ESP header and an additional IP header.
CHINESE SIMPLIFIED: 隧道模式

Tunneling Commonly used to bridge between incompatible hosts/routers or to provide encryption, a method by which one network protocol encapsulates another protocol within itself Scope Note: When protocol A encapsulates protocol B, a protocol A header and optional tunneling headers are appended to the original protocol B packet. Protocol A then becomes the data link layer of protocol B. Examples of tunneling protocols include IPSec, Point-to-point Protocol Over Ethernet (PPPoE) and Layer 2 Tunneling Protocol (L2TP).
CHINESE SIMPLIFIED: 通道

Tuple A row or record consisting of a set of attribute value pairs (column or field) in a relational data structure
CHINESE SIMPLIFIED: 元组

Twisted pair A low-capacity transmission medium; a pair of small, insulated wires that are twisted around each other to minimize interference from other wires in the cable
CHINESE SIMPLIFIED: 双绞线

Two-factor authentication The use of two independent mechanisms for authentication, (e.g., requiring a smart card and a password) typically the combination of something you know, are or have
CHINESE SIMPLIFIED: 双因素验证

U

Uncertainty The difficulty of predicting an outcome due to limited knowledge of all components
CHINESE SIMPLIFIED: 不确定性

Unicode A standard for representing characters as integers Scope Note: Unicode uses 16 bits, which means that it can represent more than 65,000 unique characters; this is necessary for languages such as Chinese and Japanese.
CHINESE SIMPLIFIED: **Unicode**

Uniform resource locator (URL) The string of characters that form a web address
CHINESE SIMPLIFIED: 统一资源定位符 (URL)

Uninterruptible power supply (UPS) Provides short-term backup power from batteries for a computer system when the electrical power fails or drops to an unacceptable voltage level
CHINESE SIMPLIFIED: 不间断电源

Unit testing A testing technique that is used to test program logic within a particular program or module Scope Note: The purpose of the test is to ensure that the internal operation of the program performs according to specification. It uses a set of test cases that focus on the control structure of the procedural design.
CHINESE SIMPLIFIED: 单元测试

Universal description, discovery and integration (UDDI) A web-based version of the traditional telephone book's yellow and white pages enabling businesses to be publicly listed in promoting greater e-commerce activities
CHINESE SIMPLIFIED: 通用描述、发现和集成 (UDDI)

Universal Serial BUS (USB) An external bus standard that provides capabilities to transfer data at a rate of 12 Mbps Scope Note: A USB port can connect up to 127 peripheral devices.
CHINESE SIMPLIFIED: 通用串行总线 (USB)

UNIX A multi-user, multitasking operating system that is used widely as the master control program in workstations and especially servers
CHINESE SIMPLIFIED: **UNIX**

Untrustworthy host A host is referred to as untrustworthy because it cannot be protected by the firewall; therefore, hosts on trusted networks can place only limited trust in it. Scope Note: To the basic border firewall, add a host that resides on an untrusted network where the firewall cannot protect it. That host is minimally configured and carefully managed to be as secure as possible. The firewall is configured to require incoming and outgoing traffic to go through the untrustworthy host.
CHINESE SIMPLIFIED: 不可信任的主机

Uploading The process of electronically sending computerized information from one computer to another computer Scope Note: When uploading, most often the transfer is from a smaller computer to a larger one.
CHINESE SIMPLIFIED: 上传

User awareness A training process in security-specific issues to reduce security problems; users are often the weakest link in the security chain.
CHINESE SIMPLIFIED: 用户意识

User Datagram Protocol (UDP) A connectionless Internet protocol that is designed for network efficiency and speed at the expense of reliability Scope Note: A data request by the client is served by sending packets without testing to verify whether they actually arrive at the destination, not whether they were corrupted in transit. It is up to the application to determine these factors and request retransmissions.
CHINESE SIMPLIFIED: 用户数据报协议 (UDP)

© 2015 ISACA All rights reserved.

User interface impersonation Can be a pop-up ad that impersonates a system dialog, an ad that impersonates a system warning, or an ad that impersonates an application user interface in a mobile device.
CHINESE SIMPLIFIED: 用户界面模拟

User mode Used for the execution of normal system activities
CHINESE SIMPLIFIED: 用户模式

User provisioning A process to create, modify, disable and delete user accounts and their profiles across IT infrastructure and business applications
CHINESE SIMPLIFIED: 用户权限分配

Utility programs Specialized system software used to perform particular computerized functions and routines that are frequently required during normal processing Scope Note: Examples of utility programs include sorting, backing up and erasing data.
CHINESE SIMPLIFIED: 实用程序

Utility script A sequence of commands input into a single file to automate a repetitive and specific task Scope Note: The utility script is executed, either automatically or manually, to perform the task. In UNIX, these are known as shell scripts.
CHINESE SIMPLIFIED: 实用脚本

Utility software Computer programs provided by a computer hardware manufacturer or software vendor and used in running the system Scope Note: This technique can be used to examine processing activities; to test programs, system activities and operational procedures; to evaluate data file activity; and, to analyze job accounting data.
CHINESE SIMPLIFIED: 工具软件

V

Vaccine A program designed to detect computer viruses
CHINESE SIMPLIFIED: 免疫程序

Val IT The standard framework for enterprises to select and manage IT-related business investments and IT assets by means of investment programs such that they deliver the optimal value to the enterprise.
Based on COBIT.
CHINESE SIMPLIFIED: **Val IT**

Validity check Programmed checking of data validity in accordance with predetermined criteria
CHINESE SIMPLIFIED: 有效性检查

Value The relative worth or importance of an investment for an enterprise, as perceived by its key stakeholders, expressed as total life cycle benefits net of related costs, adjusted for risk and (in the case of financial value) the time value of money
CHINESE SIMPLIFIED: 价值

Value creation The main governance objective of an enterprise, achieved when the three underlying objectives (benefits realization, risk optimization and resource optimization) are all balanced Scope Note: COBIT 5 perspective
CHINESE SIMPLIFIED: 价值创造

Value-added network (VAN) A data communication network that adds processing services such as error correction, data translation and/or storage to the basic function of transporting data
CHINESE SIMPLIFIED: 增值网络

Variable sampling A sampling technique used to estimate the average or total value of a population based on a sample; a statistical model used to project a quantitative characteristic, such as a monetary amount
CHINESE SIMPLIFIED: 变量抽样

Verification Checks that data are entered correctly
CHINESE SIMPLIFIED: 校验

Vertical defense-in depth Controls are placed at different system layers – hardware, operating system, application, database or user levels
CHINESE SIMPLIFIED: 垂直纵深防御

Virtual local area network (VLAN) Logical segmentation of a LAN into different broadcast domains Scope Note: A VLAN is set up by configuring ports on a switch, so devices attached to these ports may communicate as if they were attached to the same physical network segment, although the devices are located on different LAN segments. A VLAN is based on logical rather than physical connections.
CHINESE SIMPLIFIED: 虚拟局域网

Virtual organizations Organization that has no official physical site presence and is made up of diverse, geographically dispersed or mobile employees
CHINESE SIMPLIFIED: 虚拟组织

Virtual private network (VPN) A secure private network that uses the public telecommunications infrastructure to transmit data Scope Note: In contrast to a much more expensive system of owned or leased lines that can only be used by one company, VPNs are used by enterprises for both extranets and wide areas of intranets. Using encryption and authentication, a VPN encrypts all data that pass between two Internet points, maintaining privacy and security.
CHINESE SIMPLIFIED: 虚拟专用网络

Virtual private network (VPN) concentrator A system used to establish VPN tunnels and handle large numbers of simultaneous connections. This system provides authentication, authorization and accounting services.
CHINESE SIMPLIFIED: 虚拟专用网络（VPN）集中器

© 2015 ISACA All rights reserved.

Virtualization The process of adding a "guest application" and data onto a "virtual server," recognizing that the guest application will ultimately part company from this physical server
CHINESE SIMPLIFIED: **虚拟化**

Virus A program with the ability to reproduce by modifying other programs to include a copy of itself Scope Note: A virus may contain destructive code that can move into multiple programs, data files or devices on a system and spread through multiple systems in a network.
CHINESE SIMPLIFIED: **病毒**

Virus signature file The file of virus patterns that are compared with existing files to determine whether they are infected with a virus or worm
CHINESE SIMPLIFIED: **病毒特征文件**

Voice mail A system of storing messages in a private recording medium which allows the called party to later retrieve the messages
CHINESE SIMPLIFIED: **语音邮件**

Voice-over Internet Protocol (VoIP) Also called IP Telephony, Internet Telephony and Broadband Phone, a technology that makes it possible to have a voice conversation over the Internet or over any dedicated Internet Protocol (IP) network instead of over dedicated voice transmission lines
CHINESE SIMPLIFIED: **互联网语音协议/ 网络电话 (VoIP)**

Volatile data Data that changes frequently and can be lost when the system's power is shut down
CHINESE SIMPLIFIED: **易失性数据**

Vulnerability A weakness in the design, implementation, operation or internal control of a process that could expose the system to adverse threats from threat events
CHINESE SIMPLIFIED: **漏洞**

Vulnerability analysis A process of identifying and classifying vulnerabilities
CHINESE SIMPLIFIED: **漏洞分析**

Vulnerability event Any event during which a material increase in vulnerability results.
Note that this increase in vulnerability can result from changes in control conditions or from changes in threat capability/force. Scope Note: From Jones, J.; "FAIR Taxonomy," Risk Management Insight, USA, 2008
CHINESE SIMPLIFIED: **漏洞事件**

Vulnerability scanning An automated process to proactively identify security weaknesses in a network or individual system
CHINESE SIMPLIFIED: **漏洞扫描**

W

Walk-through A thorough demonstration or explanation that details each step of a process
CHINESE SIMPLIFIED: **穿行测试**

War dialer Software packages that sequentially dial telephone numbers, recording any numbers that answer
CHINESE SIMPLIFIED: **战争拨号器**

Warm site Similar to a hot site but not fully equipped with all of the necessary hardware needed for recovery
CHINESE SIMPLIFIED: **温站**

Waterfall development Also known as traditional development, a procedure-focused development cycle with formal sign-off at the completion of each level
CHINESE SIMPLIFIED: **瀑布式开发**

Web hosting The business of providing the equipment and services required to host and maintain files for one or more web sites and provide fast Internet connections to those sites Scope Note: Most hosting is "shared," which means that web sites of multiple companies are on the same server to share/reduce costs.
CHINESE SIMPLIFIED: **网站托管**

Web page A viewable screen displaying information, presented through a web browser in a single view, sometimes requiring the user to scroll to review the entire page Scope Note: An enterprise's web page may display the enterprise's logo, provide information about the enterprise's products and services, or allow a customer to interact with the enterprise or third parties that have contracted with the enterprise.
CHINESE SIMPLIFIED: **Web 页面**

Web server Using the client-server model and the World Wide Web's HyperText Transfer Protocol (HTTP), Web Server is a software program that serves web pages to users.
CHINESE SIMPLIFIED: **Web服务器**

Web Services Description Language (WSDL) A language formatted with extensible markup language (XML).
Used to describe the capabilities of a web service as collections of communication endpoints capable of exchanging messages; WSDL is the language used by Universal Description, Discovery and Integration (UDDI). See also Universal Description, Discovery and Integration (UDDI).
CHINESE SIMPLIFIED: **Web 服务描述语言 (WSDL)**

Web site Consists of one or more web pages that may originate at one or more web server computers Scope Note: A person can view the pages of a web site in any order, as he/she would read a magazine.
CHINESE SIMPLIFIED: **网站**

© 2015 ISACA All rights reserved.

Well-know ports Well-known ports--0 through 1023: Controlled and assigned by the Internet Assigned Numbers Authority (IANA), and on most systems can be used only by system (or root) processes or by programs executed by privileged users. The assigned ports use the first portion of the possible port numbers. Initially, these assigned ports were in the range 0-255. Currently, the range for assigned ports managed by the IANA has been expanded to the range 0-1023.
CHINESE SIMPLIFIED: **标准端口地址**

White box testing A testing approach that uses knowledge of a program/module's underlying implementation and code intervals to verify its expected behavior
CHINESE SIMPLIFIED: **白盒测试**

Wide area network (WAN) A computer network connecting different remote locations that may range from short distances, such as a floor or building, to extremely long transmissions that encompass a large region or several countries
CHINESE SIMPLIFIED: **广域网**

Wide area network (WAN) switch A data link layer device used for implementing various WAN technologies such as asynchronous transfer mode, point-to-point frame relay solutions, and integrated services digital network (ISDN). Scope Note: WAN switches are typically associated with carrier networks providing dedicated WAN switching and router services to enterprises via T-1 or T-3 connections.
CHINESE SIMPLIFIED: **广域网（WAN）交换机**

Wi-Fi Protected Access (WPA) A class of systems used to secure wireless (Wi-Fi) computer networks Scope Note: WPA was created in response to several serious weaknesses that researchers found in the previous system, Wired Equivalent Privacy (WEP). WPA implements the majority of the IEEE 802.11i standard, and was intended as an intermediate measure to take the place of WEP while 802.11i was prepared. WPA is designed to work with all wireless network interface cards, but not necessarily with first generation wireless access points. WPA2 implements the full standard, but will not work with some older network cards. Both provide good security with two significant issues. First, either WPA or WPA2 must be enabled and chosen in preference to WEP; WEP is usually presented as the first security choice in most installation instructions. Second, in the "personal" mode, the most likely choice for homes and small offices, a pass phrase is required that, for full security, must be longer than the typical six to eight character passwords users are taught to employ.
CHINESE SIMPLIFIED: **Wi-Fi网络安全存取协议（WPA）**

Wi-Fi protected access II (WPA2) Wireless security protocol that supports 802.11i encryption standards to provide greater security. This protocol uses Advanced Encryption Standards (AES) and Temporal Key Integrity Protocol (TKIP) for stronger encryption.
CHINESE SIMPLIFIED: **Wi-Fi网络安全存取协议II (WPA2)**

Windows NT A version of the Windows operating system that supports preemptive multitasking
CHINESE SIMPLIFIED: **Windows NT**

Wired Equivalent Privacy (WEP) A scheme that is part of the IEEE 802.11 wireless networking standard to secure IEEE 802.11 wireless networks (also known as Wi-Fi networks) Scope Note: Because a wireless network broadcasts messages using radio, it is particularly susceptible to eavesdropping. WEP was intended to provide comparable confidentiality to a traditional wired network (in particular, it does not protect users of the network from each other), hence the name. Several serious weaknesses were identified by cryptanalysts, and WEP was superseded by Wi-Fi Protected Access (WPA) in 2003, and then by the full IEEE 802.11i standard (also known as WPA2) in 2004. Despite the weaknesses, WEP provides a level of security that can deter casual snooping.
CHINESE SIMPLIFIED: **有线等效加密（WEP）**

Wireless computing The ability of computing devices to communicate in a form to establish a local area network (LAN) without cabling infrastructure (wireless), and involves those technologies converging around IEEE 802.11 and 802.11b and radio band services used by mobile devices
CHINESE SIMPLIFIED: **无线计算**

Wireless local area network (WLAN) Two or more systems networked using a wireless distribution method
CHINESE SIMPLIFIED: **无线局域网(WLAN)**

Wiretapping The practice of eavesdropping on information being transmitted over telecommunications links
CHINESE SIMPLIFIED: **线路侦听**

World Wide Web (WWW) A sub network of the Internet through which information is exchanged by text, graphics, audio and video
CHINESE SIMPLIFIED: **万维网 (WWW)**

World Wide Web Consortium (W3C) An international consortium founded in 1994 of affiliates from public and private organizations involved with the Internet and the web Scope Note: The W3C's primary mission is to promulgate open standards to further enhance the economic growth of Internet web services globally.
CHINESE SIMPLIFIED: **万维网联盟 (W3C)**

Worm A programmed network attack in which a self-replicating program does not attach itself to programs, but rather spreads independently of users' action
CHINESE SIMPLIFIED: **蠕虫**

Write blocker A devices that allows the acquisition of information on a drive without creating the possibility of accidentally damaging the drive
CHINESE SIMPLIFIED: **只读锁**

Write protect The use of hardware or software to prevent data to be overwritten or deleted
CHINESE SIMPLIFIED: **写保护**

© 2015 ISACA All rights reserved.

X

X.25 A protocol for packet-switching networks
CHINESE SIMPLIFIED: **X.25**

X.25 Interface An interface between data terminal equipment (DTE) and data circuit-terminating equipment (DCE) for terminals operating in the packet mode on some public data networks
CHINESE SIMPLIFIED: **X.25 接口**

X.500 A standard that defines how global directories should be structured Scope Note: X.500 directories are hierarchical with different levels for each category of information, such as country, state and city.
CHINESE SIMPLIFIED: **X.500**

Z

Zero-day-exploit A vulnerability that is exploited before the software creator/vendor is even aware of it's existence
CHINESE SIMPLIFIED: **零日攻击**

© 2015 ISACA All rights reserved.

What are disadvantages of referendums?


William Jago, Graduate in law, business and computing
Updated Feb 27 · Author has **259** answers and **135.9k** answer views

Referenda are one way for an electorate to decide how to solve a problem, by choosing which proposal to implement. The most common alternative is the parliamentary process - but it is also found wanting in some situations. Technical expert panels are a more common feature in democracies requiring decisions to be made within well defined parameters. New experiments in democratic decision making in Europe and Australia are focusing on citizen juries.

WHAT ARE THE FEATURES OF A GOOD PROCESS?

Any decision is only as good as the process used to reach it. A good decision making process is only as good as :-

- The quality of the *information and analysis* available to the decision-makers;
- The *skills and experience* of the decision makers in understanding the evidence and separating fact from fiction and assumption;
- The *time and resources* allowed for the decision makers to investigate, understand and decide;
- The *quality of the solutions* proposed - how well the proposed solutions address the underlying problems if implemented following the method proposed;
- The stakeholders' perception of *process legitimacy*.

INFORMATION, ANALYSIS & SKILLS

Complex important decisions frequently require detailed analysis of information from many sources.

An investigation of an important issue by an impartial tribunal may produce a large amount of information - technical details that may require specialist skills to understand. The quantity of information may demand long periods of analysis. Gaps in the evidence may come to light requiring further investigation or new lines of enquiry.

Voters in a referendum are not selected based on their skill, thoroughness or commitment to making a well informed decision in the interests of the nation. Many voters may be preoccupied with daily life, or feel disinclined to commit the time and effort required to read and understand the arguments for each proposed alternative.

Many voters may choose to simply follow the last campaign slogan they heard or vote against the campaign supported by a person they dislike. This is a particular problem where campaigns are resourced with large advertising budgets that try to reduce the issue to a slogan and enlist celebrities to support their cause.

Voters harshly impacted by the issue and highly experienced in the subject count equally with voters who have no skill, experience or vested interest in the subject matter. When questioned afterwards, it is common to find voters whose decision had little to do with the precise referendum question, or who cast their vote for reasons that were not relevant to the issue.

Whilst it is compelling in a free democracy to accept that every voter is free to vote as they choose, and none are required to explain how or why they voted, anecdotal evidence indicating a failure by the electorate to understand and address the question does not enhance the legitimacy of the resulting decision.

Parliamentary and citizen jury processes allow for these problems by forming committees that can fully investigate the issues. Committees tend to be staffed by MPs or citizens with some interest or experience in the subject matter. MPs have the power to compel witnesses to attend and give evidence.

Interest groups are likely to prepare detailed facts for presentation to committees even though they may be technically detailed and too boring to be absorbed by the average voter. Interest groups that cannot afford to fund national advertising campaigns in a referendum context can ensure that their evidence is presented to and understood by individual MPs or committees. The committee can initiate new lines of enquiry, offer alternative solutions, or cross examine witnesses if appropriate.

Parliamentary parties are prone to suppress debate on issues that are well described in election manifestos or close to ideological ideals or sacred cows. This can result in sub-optimal outcomes. Citizen juries, and minority governments that must build wide coalitions in support of new initiatives, often produce better decisions precisely because of the diversity of viewpoints represented.

If a referendum decision is to maintain legitimacy through to implementation, the voters must be properly informed of the issues, and the full consequences, costs and benefits of each of the proposed solutions. Preparation of comprehensive evidence in an accessible format from all stakeholders is a critical part of the preparatory process for any referendum.

TIME AND RESOURCES

National decision making processes are always expensive. The costs are measured in the investments in the decision making infrastructure, the number of person hours consumed, and the elapsed time required to run the process. Long processes necessarily cause long periods of uncertainty and delay in implementation further increasing the stakes at risk.

The least optimal outcome to be avoided is to conduct a long contested referendum campaign that results in a decision that cannot be implemented to the satisfaction of any of the parties and must be revisited repeatedly - diminishing the benefits sought, extending the period of community division, and causing other important initiatives and adjustment processes to be postponed whilst national leadership is consumed in contentious debate.

The worst possible situation is a poorly defined referendum decision on a complex issue that must be implemented by a parliament that finds itself unable to deliver the promised result because of changed circumstances or unrealistic expectations. The conflict between satisfying the snapshot of the "***will of the people***" from the referendum and steering a course for the nation in the best interests of the people over the term of the parliament is impossible to resolve to the satisfaction of all parties, and inevitably leads to entrenchment of fundamentalist positions. In this situation, either the parliament will be deadlocked and require a new referendum, or an election of a new government with a mandate for a wiser policy.

In this respect, a referendum is the most expensive decision making process precisely because of the cost in terms of community conflict, the number of person hours consumed, and the elapsed time during which all other business is suspended.

Parliamentary processes are much cheaper to run, tend to make better quality decisions more quickly in fluid situations and are more able to refine or review their decisions, adjusting the infrastructure of the nation in response to changes in circumstances, but only if they are not preoccupied trying to resolve conflicts between the past decisions and the future objectives, or trying to reconcile entrenched ideological positions.

SOLUTIONS AND IMPLEMENTATION

Referenda are good for simple clear questions that cut across party lines, when the problem is well understood, the solution alternatives are clearly defined and facts are widely available.

Referenda are not ideally appropriate for exploring complex far-reaching questions with ill-defined boundaries, or problems where solutions are not accompanied by realistic or credible implementation plans.

In these situations it is often necessary to commit to a direction of change in order to engage stakeholders or reveal challenges that must be overcome. In these situations, a referendum campaign (that has not been preceded by an appropriate tribunal able to credibly establish the costs and benefits of the alternative proposals) may make the challenge appear to be quick and easy to resolve, falsely raising expectations of a simple and inexpensive resolution, when in fact the project requires significant long term

investment, and many subsequent decisions or course corrections before the final objective can be fully defined and achieved.

Parliamentary decision making process allows for the issues to be investigated by committees, details of the proposals to be repeatedly refined after debate, or deferred to committees for detailed consideration of evidence from witnesses. Subject to the parliamentary timetable, the final decision can be brought forward or delayed as circumstances dictate, ensuring the optimal steps can be taken towards the solution once all viewpoints have been heard, and all proposals adequately investigated and considered.

All bills put before parliament must be voted on at least three times - thereby ensuring that there is adequate opportunity for all parties to be heard and refinement of the solution at every stage to maximise the appeal of the electorate. This process can be, and often is, subverted when the subject is a sacred cow or core promise of an electoral platform and the parliament is dominated by a single party.

Citizen juries and technical expert panels (such as central bank monetary policy committees) are generally better able to develop and refine implementable solutions to well defined problems. Their representatives often have access to detailed relevant knowledge that may not be widely available to the public.

The temporary nature of citizen juries may be better suited to single event decision making rather than management of complex issues over long periods of time where technical expert panels and parliamentary processes allow transparency and accumulation of experience over their term of appointment.

The single referendum vote is a very rigid blunt process that prevents any revision or refinement during the process, especially if the voters cynically adopt the view that the subject of a referendum decision may not be revised, reviewed or presented to the electorate again.

PROCESS LEGITIMACY

The benefit of a good decision, and the cost of a bad decision that must be reversed, are very high because of the large scale of the consequences for the nation. These high costs demand that the decision making process retain legitimacy in every aspect.

Good national decision-making processes are characterised by growing unity and universal adoption of the decision. People accept the decision and move on because the process is regarded as legitimate and the decision is unlikely to be reversed. Legitimate objections have been heard, understood and allowed for.

In jurisdictions that use referenda seldom, there is a risk that the preparatory work - investigating problems, defining solutions and reaching consensus on implementation - is not done to an adequate level to meet the standards necessary to achieve legitimacy.

The consequences of this failure are evident before the vote in conflict and poor voter engagement, and after the referendum in challenges to the legitimacy of the campaigns, an extended period of resistance to change, and difficulties in reaching consensus in implementation.

In extreme cases, conspiracy theories and paranoia abound as a way of attributing implementation difficulties to saboteurs and external enemies rather than recognising the roots of the difficulties in poor preparation and inadequate or naive planning.

A referendum is a snapshot of opinion. Referenda occur so seldom in many jurisdictions that it is difficult for the electorate to build skill and experience to improve the process. The voter gets only one chance to express an opinion, and no opportunity to revise, enlarge or redefine the proposed solutions. The voters have no control of the decision making process once the referendum has been announced. These issues can only be avoided by good question design, and excellent management of the process by electoral authorities, including constant revision of management processes in light of past failures.

In jurisdictions with compulsory voting systems, extremists will vote predictably and can be safely ignored by the campaigners. Ergo, the campaign messaging and argument is usually focussed on moderate ‘swinging’ voters who are more likely to make a balanced decision that addresses the needs of a wider cross section of the community. These voters are less likely to be swayed by extremists or emotive appeals to fear or self-interest.

In jurisdictions with voluntary voting systems, the challenge for the campaigners is to get voters to turn out to vote on polling day. Therefore, the referendum campaigners often focus on emotional appeals that motivate their supporters to vote by voicing fears and promoting outrage. These campaigns often get distracted by arguments about whether the wildest claims are true rather than directing attention to the most relevant issues. Emotive campaigns deter moderate debate, polarise the community and undermine dialogue that could establish common ground and promote tolerance.

The referendum date cannot easily be deferred if events distract the voters or critical information is not available. And corrupting factors (e.g. breaches of campaigning or funding rules, or improper campaigning methods beyond existing rules) often come to light so much later that it is impossible to modify the decision because the context has changed.

Bad processes tend to cause internal conflict, and long periods of avoidable self-inflicted reputational damage that undermines the legitimacy of the decision and the credibility of the nation. Large parts of the community may refuse to accept the decision and resist change because they demand and expect the decision will be revised.

Adjustment programmes may be delayed during the period of uncertainty between the referendum and the final implementation. Affected parties may be paralysed by fear or indecision because they cannot see clearly what they should do to prepare for the future, and lack any way of appealing against the “will of the people” for a refinement in the result.

It is arguable that the polarisation and extremism witnessed around referenda would be diminished if referenda questions could be modified during the referendum process to assuage the fears expressed. Multiple rounds of voting or refinement of the solutions help to build unity in support of the proposals finally adopted.

IS A REFERENDUM THE BEST PROCESS AVAILABLE?

Good successful governance requires both tactical and strategic wisdom.

Strategic decisions are critical junctures that can disproportionately affect the success of the nation. Many tactical decisions must be made consistently well over the long term to address problems and exploit opportunities as they arise.

Success in the long term is less about making the right decision in any moment and more about following appropriate and legitimate processes that allow for the course of the nation to be adjusted to deal optimally with circumstances.

Unfortunately, referenda processes are prone to many rigidities that increase the risk and cost of the decision making process, whilst reducing the ability of the national government to make appropriate forward-looking decisions in the long term interests of the whole nation. For this reason, referenda are usually avoided by national leaders for all but the most important strategic issues, and experienced seldom by voters - arguably increasing the risk of bad decisions.

The deficiencies of referenda are not reflected in their reputation. Many naive voters consider referenda to be the highest expression of the will of the people. Close examination reveals many deficiencies suggesting that referenda should be avoided in favour of more appropriate processes in most cases.

Our view of the future cannot be perfect, and so we cannot easily decide what is the right decision for all possible futures. We can only decide to proceed in a direction and be willing to adjust our course as conditions change.

Following legitimate processes ensures that we can avoid the negative impacts of division and conflict that are inherent risks in every major decision. Parliamentary processes are mature and well suited to the many decisions required for national law making although they are prone to make suboptimal decisions on ideological subjects when dominated by single party majorities. Citizen juries and expert panels are generally better suited to complex decision making where the interests of the whole community must be taken into account in circumstances of uncertainty in addressing issues and refining solutions within a short time frame.

If course correction and constant improvement is a mark of good decision making processes, referenda - as currently conducted - fall well short of optimum for the most important issues facing the nation.

259 Views · View 1 Upvoter

View 1 other answer to this question >

About the Author

William Jago
Graduate in law, business and computing

Post Graduate Diploma E-Commerce, Kingston University
Graduated 2003

Lives in London

135.9k answer views
7.6k this month

WIKIPEDIA
The Free Encyclopedia

Main page
Contents
Featured content
Current events
Random article
Donate to Wikipedia
Wikipedia store

Interaction
Help
About Wikipedia
Community portal
Recent changes
Contact page

Tools
What links here
Related changes
Upload file
Special pages
Permanent link
Page information
Wikidata item
Cite this page

Print/export
Create a book
Download as PDF
Printable version

In other projects
Wikimedia Commons

Languages
Español
Français
Italiano
Русский
□□

Edit links

Gridcoin

From Wikipedia, the free encyclopedia

Gridcoin implements a "Proof-of-Research" (POR) scheme, which rewards users with Gridcoin for performing useful scientific computations on the Berkeley Open Infrastructure for Network Computing (BOINC),[1] a distributed computing platform. Gridcoin uses a more energy efficient[*clarification needed*] proof-of-stake system - although it fails to explicitly address the energy cost of computing power.[1]

Gridcoin attempts to ease the environmental energy impact of cryptocurrency mining through its Proof-of-Research and Proof-of-Stake protocols.[2][3]

References [edit]

1. ^ *a* *b* Dong, Zhongli; Lee, Young Choon; Zomaya, Albert Y (2015). "Crowdware: A Framework for GPU-Based Public-Resource Computing with Energy-Aware Incentive Mechanism". *2015 IEEE 7th International Conference on Cloud Computing Technology and Science (Cloud* Com). p. 266.

Gridcoin	
	
Denominations	
Subunit	
10^{-3}	milligridcoin
Symbol	GRC
milligridcoin	mGRC
Demographics	
Date of introduction	16 October 2013; 5 years ago
User(s)	Worldwide
Issuance	
Administration	Decentralized
Valuation	
Supply growth	6.5% Inflation. 1.5% Interest + 5% Research Payments APR. Approximate circulating coin supply: >395,203,265 GRC

Gridcoin Research	
Developer(s)	Rob Halförd
Stable release	4.0.1.0-Leisure / November 30, 2018
Repository	github.com/gridcoin-community/Gridcoin-Research
Written in	C++
Platform	Windows, Linux, macOS

Type	Cryptocurrency
Licence	MIT Licence
Website	https://gridcoin.us

doi:10.1109/CloudCom.2015.73. ISBN 978-1-4673-9560-1.

2. ^ Chohan, Usman. "Environmentalism in Cryptoanarchism: Gridcoin Case Study". *SSRN Electronic Journal*. Jan 2018. doi:10.2139/ssrn.3131232. Retrieved 8 October 2018.
3. ^ Tirone, Jonathan (10 Jan 2018). "A Prime Number Could Be the Answer to Bitcoin's Power Problem". *Bloomberg*. Retrieved 7 Oct 2018.

Business and economics portal

External links [edit]

- Official Gridcoin website

V · T · E	Cryptocurrencies	
Technology	Blockchain · Cryptocurrency tumbler · Cryptocurrency exchange · Cryptocurrency wallet · Cryptographic hash function · Distributed ledger · Fork · Lightning Network · Smart contract	
Consensus mechanisms	Proof-of-authority · Proof-of-space · Proof-of-stake · Proof-of-work	
Proof-of-work currencies	**SHA-256-based**	Bitcoin · Bitcoin Cash · Counterparty · MazaCoin · Namecoin · NeuCoin · Nxt · Peercoin · Steem · Titcoin
	Ethash-based	Ethereum · Ethereum Classic
	Scrypt-based	Auroracoin · Bitconnect · Bitcoin Gold · Coinye · Dogecoin · **Gridcoin** · Litecoin · PotCoin
	Equihash-based	Zcash · Zcoin
	CryptoNote-based	Monero
	X11-based	Dash · Petro
	Lyra2-based	Taler
	Other	Verge · Vertcoin
Proof-of-stake currencies	EOS.IO	
ERC-20 tokens	Augur · Aventus · Basic Attention Token · Centra · Kin · KodakCoin · Minds · Power Ledger · Publiq	
Other currencies	BitShares · Filecoin · NEM · NEO · NuBits · Primecoin · Ripple · Stellar · Tether	
Related topics	Airdrop · BitLicense · Blockchain game · Complementary currency · Crypto-anarchism · Cryptocurrency bubble (2018 cryptocurrency crash) · Digital currency · Double-spending · Initial coin offering · Initiative Q · List of cryptocurrencies · Stablecoin · Token money · Virtual currency	
Category · Commons · List		

Categories: Alternative currencies | Cryptocurrencies | Grid computing projects

This page was last edited on 9 February 2019, at 22:50 (UTC).

Text is available under the Creative Commons Attribution-ShareAlike License; additional terms may apply. By using this site, you agree to the Terms of Use and Privacy Policy. Wikipedia® is a registered trademark of the Wikimedia Foundation, Inc., a non-profit organization.

Privacy policy About Wikipedia Disclaimers Contact Wikipedia Developers Cookie statement

Mobile view

List of highest funded crowdfunding projects

From Wikipedia, the free encyclopedia

This is an incomplete list of the highest-funded crowdfunding projects (including projects which failed to achieve funding).

Over 10 million [edit]

Rank	Project	Category	Platform	Campaign end date	Campaign target	Amount raised	Notes
1	*EOS*	Blockchain	Ethereum	June 1, 2018	-	$4,000,000,000+[1]	EOS is a blockchain operating system designed to support commercial decentralized applications.
2	*Filecoin*	Blockchain	Ethereum	September 7, 2017[2][3]	-	$257,000,000[4]	Filecoin is a decentralized data storage application.
3	*Tezos*	Blockchain	Independent	July 14, 2017	-	$232,000,000[5]	Tezos is a self-governing blockchain.
4	*Star Citizen*	Video game	Kickstarter, Independent	Ongoing	$2M	$216,844,803+[6]	Space combat video game being developed by Chris Roberts, designer of *Wing Commander*. By April 19, 2013, a combined $9,061,882 had been raised on Kickstarter and Roberts' own website.[7] By March 2014, it had raised more than $40,680,576 through Roberts' own website and was listed as a Guinness World Record.[8] As of November 27, 2018, Roberts' own website lists the funds raised as $204+ million.[9] Most of this total comes from pre-purchased in-game items which are sold on Roberts' website.[10]
5	Sirin Labs (SRN)	Mobile	Ethereum, Bitcoin	December, 2017	-	$158,000,000[11]	A blockchain phone that makes it easier to use digital currency. Expected to sell for over $1000 with 25,000 units pre-ordered.[12]
6	*Bancor protocol*	Blockchain	Ethereum	June 12, 2017	$100M	$153,000,000[13]	The Bancor protocol is a smart contracts platform built on top of the Ethereum blockchain. Its goal is to solve a problem known in economics as the "Double Coincidence of Wants Problem"[14] and offer a liquidity mechanism for tokens.
7	*The DAO*	Blockchain	Ethereum	May 28, 2016[15]	$500K	$150,000,000[16]	A publicly created and crowdfunded Decentralized Autonomous Organization, built on the Ethereum blockchain, that stored and transmitted Ether and Ethereum-based assets. Funds were held programatically by design in the cryptocurrency known as Ether, the actual USD amount raised varied in line with the Ether|USD exchange rate at any given moment. Final raised amount was ETH 11.5 million.[16] The amount listed is the conversion value of the raised Ethereum at the campaign end date.
8	Polkadot	Blockchain	Ethereum	October 27, 2017[17]	-	$144,300,000[18]	Polkadot is a heterogeneous multichain which posits a trustless fully decentralised "federation" of

Main page
Contents
Featured content
Current events
Random article
Donate to Wikipedia
Wikipedia store

Interaction
Help
About Wikipedia
Community portal
Recent changes
Contact page

Tools
What links here
Related changes
Upload file
Special pages
Permanent link
Page information
Wikidata item
Cite this page

Print/export
Create a book
Download as PDF
Printable version

Languages
Add links

							public and private blockchains with trust-free access to each other.
9	Status	Blockchain	Ethereum	June 21, 2017	$12M	$103,000,000[19]	
10	*Elio Motors*	Other	Independent	Ongoing	-	$102,000,000[*citation needed*]	Elio Motors is designing a three-wheel vehicle that the company says will get up to 84 MPG.[20] In October 2016, the company said it had received over 60,000 reservations. Their goal is to reach 65,000 reservations, and until they reach their goal, early adopters are able to reserve one of the vehicles for a locked price of $7,300[21][22] ($7,000 by completing the binding purchase agreement). After surpassing that milestone, the targeted base price for anyone that hasn't locked in is now $7,450.
11	TenX	Blockchain	Ethereum	June 24, 2017	$80M	$80,000,000 (245,832 ETH)[23]	TenX mission is to make any blockchain asset spendable anytime and anywhere. They offer a debit card system as one of their frontend solutions to customers and combine that with an open-source backend called COMIT that allows TenX to connect any blockchain through hashed timelock contracts (HTLCs). TenX raised 100,000 ETH in a pre-sale and another 145,000 ETH equivalent during their token sale on June 24, 2017.[24]
12	BANKEX	Blockchain	Ethereum	December 26, 2017	$50M	$70,600,000[25]	BANKEX is a blockchain-based distributed financial technology platform.[26] It allows people and enterprises to create and trade their digital assets represented as smart asset tokens on a blockchain.[27] BANKEX has raised $70.6 million during its token sale becoming 13th largest token sale of all time.[28][29]
13	TRON	Blockchain	Ethereum	Sep 2, 2017	$70m	$70,000,000[30][31]	TRON is a blockchain project that supports the global digital entertainment system. As an open-source project, it supports various types of smart contracts and contract systems such as Bitcoin, Ethereum and EOS.
14	*æternity*	Blockchain	Ethereum	Jun 9, 2017	-	$62,500,000.00	æternity is a new type of open-source, public, Blockchain-based distributed computing platform that innovates and expands upon existing platforms such as Bitcoin, Ethereum. Real-world data can interface with smart contracts through decentralized oracles. True scalability and trust-less Turing-complete state channels sets æternity apart from all other Blockchain 2.0 projects. Contribution was divided into two phases and closed by 9 June 2017. Total amount raised in Phase 1 + Phase 2 is over $62.5 million (at ETH and BTC valuation on 9 June 2017).[*citation needed*]
15	*MobileGo*	Blockchain	Ethereum, Waves platform	May 24, 2017	-	$53,069,235[32]	MobileGo tokens will be used to gamify the mobile platform, and to incentivize gamers for loyalty and participation through rewards. MobileGo tokens will also allow for smart contract technology. MobileGo tokens will allow for the development of a decentralized virtual mobile gamer marketplace, the ability for gamer vs. gamer decentralized match

							play, and decentralized tournaments run on smart contracts.
16	Basic Attention Token	Blockchain	Ethereum	May 31, 2017	-	$35,000,000[33][34]	Basic Attention Token is a token on the Brave Browser. BAT allows marketers to sell and publishers to buy ads without exposing users to constant tracking. Targeting is handled by the browser. The user gets paid a small amount for viewing ads. The initial coin offering sold out in under 30 seconds.[1]
17	*Polybius*	Blockchain Bank	Bitcoin, Ethereum	July 5, 2017[35][36]	$25M for bank with Digital Pass. (Ladderized target with flexible plan.)	$31,645,088 (□12,379.689) = 3,650,521 PLBT	*Project: Polybius Bank* is a project aimed to create the world's first fully digital bank that is EU-regulated[37] and crowdfunded by its own users through tokens ($PLBT).[38]
18	CyberMiles	Blockchain, Ecommerce	Ethereum, Independent	November 22, 2017	$30M	$30,000,000 (71,850 ETH)[39]	CyberMiles is an in-development blockchain protocol specifically designed and optimized for e-commerce. Expected to be released by mid-2018, CyberMiles aims to democratize e-commerce and empower the decentralization of the online marketplace.[40]
19	Solve.Care	Blockchain, Healthcare	Ethereum	Apr 30, 2018 [41]	$30m[42]	30,000,000[42]	Solve. Care is a blockchain solution for more efficient coordination, administration and payments in the healthcare industry. Patients will be able to make reservations and share relevant data. Using a hybrid blockchain solution data is verified by the immutability of the blockchain without ever exposing private information.
20	Glowforge	3D Laser Printer	WordPress, Independent	Oct 24, 2015	$100,000	$27,907,995[43]	Glowforge uses a beam of light the width of a human hair to cut, engrave, and shape designs from a variety of materials. Called a "3D laser printer" by the makers, it actuality it is a laser cutter
21	BitClave	Blockchain	Ethereum	November 29, 2017	-	$25,547,000	In the current $550B ads market, too much money goes to the hidden ad network with too little added value for businesses and customers. BitClave is using blockchain to eliminate ad service “middlemen” and create a direct connection between businesses and customers. With BitClave, businesses have a direct relationship with customers and can offer a uniquely targeted promotion. With BitClave, an open search marketplace keeps prices fair, and elimination of intermediates brings all value to customers and businesses. On the BitClave Active Search Ecosystem (BASE), customers control their identity, decide who has access to their data, and are “paid” in BitClave's tokens each time businesses “use” their data to make them offers. In turn, customer can pay business for their products or services using BitClave's token.
							Aragon is a management platform for decentralized organizations. Aragon implements organizational features such as governance, fundraising,

22	*Aragon*	Blockchain	Ethereum	May 17, 2017	-	$25,000,000[44]	payroll and accounting. Aragon launched a token sale for the Aragon Network, the world's first decentralized jurisdiction. The Aragon Network will provide organizations subscribed to it with services such as a decentralized arbitration system or a code upgradeability mechanism. The token sale closed in about 15 minutes, peaking at a rate of $122,000 per second.[*citation needed*]
23	*Pebble Time*	Smartwatch	Kickstarter	Mar 27, 2015	$500K	$20,338,986[45]	The Pebble Time is the second generation version of the smartwatch called the Pebble. The Pebble itself was one of the highest backed projects on Kickstarter.
24	*Prison Architect*	Video game	Independent, Steam Early Access	Oct 6, 2015	-	$19,000,000[46]	Prison construction and management simulation game by Introversion Software. It was made available as a paid alpha pre-order on September 25, 2012 and was one of the initial games in Valve's Steam Early Access program when it was launched.
25	*We The People Will Fund The Wall*	Community	GoFundMe	N/A	$1.0B[47]	$18,371,025[48]	Construction of the Border barrier at the Mexico–United States border. The idea originated and gained popularity from the political platform of the Donald Trump 2016 presidential campaign.[49] The project has raised over $9 million in only 3 days since its launch.
26	*Ethereum*	Blockchain	Independent	Sep 2, 2014	-	$18,300,000[50]	Ethereum is a public blockchain-based distributed computing platform, featuring smart contract functionality and a cryptocurrency, Ether.
27	Power Ledger	Blockchain	Ethereum	October 6, 2017	-	$17,000,000 = 34,000,000 AUD[51][52]	POWR token sale is Australia's first initial coin offering.[53] The company raised half of the total funds in three days during its pre-sale.[54]
28	Cosmos	Blockchain	Bitcoin, Ethereum	Apr 6, 2017	$10m[55]	$16,800,000[56]	Cosmos aims to create a network of ledgers to solve long-standing problems in the cryptocurrency and blockchain communities. One of the most prominent use cases is decentralized exchanging from one currency to another. Currently this is largely done on centralized exchanges
29	*TokenCard*	Blockchain	Ethereum	May 3, 2017	-	$16,516,286[57][58]	TokenCard is a depositless Ethereum-based mobile banking platform that aims to integrate the Ethereum Economy into the daily life of consumers globally.
30	*Waves platform*	Blockchain	Independent	May 31, 2016[59]	-	$16,436,095[60]	Waves (stylised WAVES) is a non-permissioned, non-privatized blockchain that intends to deal with banks national currencies. It raised 2 million in 24 hours[59] and has a partnership with the Mycelium wallet.[61] It raised 29,636 bitcoins.[*citation needed*]
31	Qtum	Blockchain	hybrid blockchain platform	March 21, 2017.	-	$15,664,829.30[62]	Qtum [pronounced Quantum] is a hybrid blockchain platform that runs the EVM on bitcoins core allowing smart contracts to exist in a mobile environment. Qtum Raised $15,664,829.30 in a crowd sale campaign[63] that sold out in 5 days. The campaign started March 16, 2017 and ended in 117 hours when it was sold out March 21, 2017.
							A distributed VC ecosystem. Cofound.it is a distributed global

32	Cofound.it	Blockchain	Ethereum	June 7, 2017	56565 ETH ($~14.8M)	$14,700,000	platform that connects exceptional startups, experts and investors worldwide. It will first be built by the blockchain community for the blockchain community — and then for the whole world.[citation needed]
33	*Coolest Cooler*	Computing hardware	Kickstarter	Aug 29, 2014	$50K	$13,285,226[64]	Portable 60 quart cooler designed by Ryan Grepper that contains a battery powered rechargeable blender, waterproof Bluetooth speaker, USB charger, cutting board, plates, among other features.[65]
34	*Flow Hive*	Food	Indiegogo	Apr 19, 2015	$70K	$13,289,097[66]	Flow Hive is a new type of domesticated bee hive box with a valve, where the beekeeper can extract honey from the hive without disturbing the bees.
35	*Ubuntu Edge*	Computing hardware	Indiegogo	Aug 21, 2013	$32M	$12,814,196[67]	The Ubuntu Edge was a proposed "high concept" smartphone announced by Canonical Ltd. on 22 July 2013.
36	*Shroud of the Avatar: Forsaken Virtues*	Video game	Kickstarter, Independent, Steam Early Access	Ongoing	$1M	$12,658,636	Richard Garriott returns to the fantasy RPG genre.[68] Of the total amount, $1,919,275 was raised on Kickstarter.[69]
37	Gnosis	Other	Ethereum	Apr 24, 2017	$12.5M	$12,500,000[70]	
38	*Kingdom Death: Monster 1.5*	Board game	Kickstarter	January 7, 2017	-	$12,393,139[71]	A massive cooperative board game about survival in a nightmare-horror world. Original Kickstarter campaign that raised $2,049,721 was surpassed in 2 hours.[72]
39	iEx.ec	Other	Ethereum	April 19, 2017	10,000 BTC	$12,158,963	
40	*ICONOMI Digital Assets Management platform*	Other	Ethereum	Sep 29, 2016	2000 BTC ($~1.2M)	$10,682,516.42	ICONOMI Digital Assets Management platform enables simple access to a variety of digital assets and combined Digital Asset Arrays.[citation needed]
41	*BauBax*	Other	Kickstarter, Indiegogo	Ongoing	$20K	$10,271,965[citation needed]	The campaign was launched on July 7, 2015.[73] By August 2015, BauBax had raised $3.7 million and was the most funded clothing project in Kickstarter history.[74] By September 11, 2015, it had raised $9.7 million.[75] The Travel Jacket comes with 15 unique features including a built-in Neck Pillow, Eye Mask, Gloves, Earphone Holders, Drink Pocket and Tech Pockets of all sizes. Available in four styles: hoodie/sweatshirt, fleece lined bomber, wrinkle free blazer with removable hoodie, and a windbreaker.
42	*Pebble*	Smartwatch	Kickstarter	May 18, 2012	$100K	$10,266,845[76]	E-Paper smartwatch. Third highest funded project on Kickstarter.[citation needed] Shipping to backers began on 23 Jan 2013.

5–10 million [edit]

Rank	Project	Category	Platform	Campaign end date	Campaign target	Amount raised	Notes	References
43	*Exploding*	Board	Kickstarter	Feb 19, 2015	$10K[77]	$8,782,571[78]	Card game featuring exploding kittens, designed by Elan Lee, Matthew Inman, and Shane Small.[79] The project hit its primary goal in only 8 minutes, exceeded $100,000 (10x its goal) in less than one hour,	

	Kittens	game					$1,000,000 (100x its goal) in less than 8 hours, and $2,000,000 (200x its goal) in just over 24 hours. By January 28, 2015, it passed 107,000 backers, making it the most backed Kickstarter to date.[79]
44	*Golem*	Blockchain	Ethereum, Independent	Nov 11, 2016	$8.6M	$8,600,000[80]	Distributed, open sourced, supercomputer built on the Ethereum network. Made up of a global sharing economy network of computers that 'rent' out their computing power. Project hit its goal in 29 minutes.
45	*Ouya*	Video game	Kickstarter	Aug 9, 2012	$950K	$8,596,474[81]	Android-based video game console. Industrial design by Yves Béhar. Highest funded video game project entirely funded on Kickstarter. Development units began shipping in March 2013. Officially released in June 2013.
46	*Gut Weißenhaus*	Other	Companisto	Mar 27, 2015	$2M	$8,148,450[82]	Real estate
47	*Shenmue III*	Video game	Kickstarter, Independent	Sep 1, 2018	$2M	$7,063,329[83]	$6,333,295 was raised on Kickstarter, making *Shenmue III* the highest-funded video game project in Kickstarter history.
48	FirstBlood Crowdsale	Software	Ethereum	Sep 26, 2016	$5,500,000	$6,267,767.32[84][85]	FirstBlood is the first decentralized app, built on top of Ethereum, that allows eSports enthusiasts to compete in their favorite games through a decentralized, automated platform. The FirstBlood Token ("1ST"), sold during its crowdsale, is a utility token that can be used on FirstBlood's decentralized software. The campaign raised over $5 million in less than five minutes.[86]
49	*Pono Music*	Computing hardware	Kickstarter	Apr 15, 2014	$800K	$6,225,354[87]	Digital music player using the FLAC audio file format under development by musician Neil Young and his company Pono Music.
							Super PAC founded by Lawrence Lessig with the purpose of pushing for a United States Congress dedicated to reforming

50	*Mayday PAC*	Other	Independent	Jul 4, 2014	$6M	$6,132,554[*citation needed*]	campaign finance laws by 2016. The crowdfunding round took place in two cycles. The first $1M goal was started on May 1, and was reached on May 13,[88] and the second, $5M goal was started on June 4 and was reached on July 4, at 9:30 pm EST - 9 hours short of the deadline of 6 am, July 5, EST (or midnight in Hawaii.)[89] After the crowdfunding deadline, Mayday PAC raised an additional $4M from large donors. As of May 22, 2016, Mayday PAC is the largest crowdfunding campaign for non-profit purposes.[*citation needed*]
51	Lucyd	Blockchain, Wearables	Ethereum	Feb 28, 2019	$6m	$6,100,000[90]	Community-driven augmented reality project. Has since launched an eshop for advanced eyewear. Developing blockchain apps for augmented reality.
52	Fidget Cube	Other	Kickstarter	Oct 19, 2016[91]	$15K[91]	$6,038,945[91]	A desk toy designed to help users focus.[92]
53	*Veronica Mars*	Movie	Kickstarter	Apr 13, 2013	$2M	$5,702,153[93]	Feature-length film continuation of the *Veronica Mars* television series.
54	*Lisk*	Software	Bitcoin, Independent	Mar 21, 2016	-	$5,700,000[94]	Lisk is a crypto-currency and decentralized application platform. As a crypto-currency it provides a decentralized payment system and digital money network. The Lisk decentralized application platform allows the deployment, distribution and monetisation of decentralized applications and custom blockchains (sidechains) onto the Lisk blockchain.
55	*Bloodstained: Ritual of the Night*	Video game	Kickstarter	Jun 12, 2015	$500,000	$5,545,991[95]	Metroidvania video game, by former *Castlevania* producer Koji Igarashi. Succeeded *Torment: Tides of Numenera* as the highest funded Kickstarter video game, was succeeded by *Shenmue III* in July 2015.[95]
							DigixDAO crowdsale

56	*DigixDAO Crowdsale*	Blockchain	Ethereum	Mar 30, 2016	$500K	$5,500,000[*third-party source needed*]	offered DGD tokens where each DGD token entitles you to an apportioned return on DGX (first gold standard token on the Ethereum platform) transactional volume in the form of DGX tokens. The DGD token holder also gets a pledging say on the projects built around the DGX transactional system and there's a majority rule applied to release funds for business expenses paid to peripherals. The sale concluded in a mere 12 hours as the maximum was reached.	
57	*The Grid*	Software	Independent	Ongoing	$70K	$5,489,376[*citation needed*]	Website builder that uses Artificial intelligence algorithms to design and build websites based on content.[96]	
58	*Project Bring Back Reading Rainbow for Every Child, Everywhere*	Movie	Kickstarter	Jul 2, 2014	$1M	$5,408,916[97]	Make the iPad version of Reading Rainbow available on the web, other mobile devices, game consoles, and set-top boxes. In addition, create a classroom version and provide subscriptions for up to 7,500 disadvantaged classrooms for free.	
59	Chronicles of Elyria	Video Game	Kickstarter, Independent	Ongoing	$900k	$5,302,338	Epic Story MMORPG survival game with aging and perma-death. Fully destructible, evolving world with non-repeatable quests.	[98]
60	Augur	Blockchain	Ethereum, Independent	October 1, 2015	none	$5,133,000[*third-party source needed*]	An open-source, decentralized prediction market built using Blockchain technology. The project seeks to leverage the Wisdom of Crowds (also known as "collective intelligence") — and the open, global, peer-to-peer, distributed ledger functionality that blockchain technology provides — to generate better forecasts about any future event involving any major topic of widespread interest.	
61	*Restore King Chapel Now. Every Day & Dollar Counts*	Other	Indiegogo	May 22, 2015	$8M[99]	$5,048,213[99]	Restore Martin Luther King Jr. International Chapel, the only religious building named after Dr. King located at Morehouse	

							College.
62	*An Hour of Code for Every Student*	Other	Indiegogo	Dec 15, 2014[100]	$5M	$5,024,281[100]	Every student in every school should have the opportunity to learn computer science at Code.org.[*citation needed*]
63	*Mastercoin*	Software	Bitcoin, Independent	Sep 1, 2013	-	$5,000,000[101]	Mastercoin is a digital currency and communications protocol built on the Bitcoin block chain. It is one of several efforts to enable complex financial functions in a cryptocurrency.

1–5 million [edit]

This list includes a list of references, related reading or external links, **but its sources remain unclear because it lacks inline citations**. Please help to improve this list by introducing more precise citations.
(August 2016) (Learn how and when to remove this template message)

Rank	Project	Category	Platform	Campaign end date	Campaign target	Amount raised	Notes	References
64	*Filippo Loreti*	Watch	Kickstarter, Independent	29 Dec 2016	$20k[102]	€4,809,548[102]	Mechanical watch. Became the most crowdfunded timepiece in history with the first campaign raising 926'960 EUR. The second Kickstarter campaign beat the record again, raising 4,809,548 EUR.	[103][104]
65	*Torment: Tides of Numenera*	Video game	Kickstarter, Independent	13 May 2016	$4.5M[105]	$4,782,227[105]	Fantasy role-playing video game. Succeeded *Project Eternity* as the highest funded Kickstarter video game. It raised $4,188,927 on Kickstarter. Including private backers, the project's developers said they had enough to reach their goal of $4.5M. InXile's second Kickstarter project, after *Wasteland 2* in April 2012.	[106][107][105]
66	Synereo	Blockchain	BnktotheFuture, independent	18 Oct. 2016		$4,701,421	Decentralized computation and hosting platform, allowing Web-Application to exist without centralized servers. Synereo raised over $4.7M, selling AMPs, the organization's native cryptocurrency, as well as shares of Synereo LTD.	[108][109]
67	G-RO	Other	Indiegogo, Kickstarter	Dec 12, 2015	$125,000	$4,573,569[110]	Carry-on smart luggage with a built-in tablet stand, charging station, two USB ports, a 23,000 mAh battery pack, a location tracker and a wireless proximity tracker. In the first day of the funding campaign, G-RO raised $360,000 in pledges, nearly three times its initial $125,000 goal.	[111]
68	Neo	Blockchain	Ethereum	Sep, 2016		$4,500,000	The Chinese Ethereum as it is commonly known. It functions as a decentralized smart contract system. Was also backed by big names like	

							Microsoft and Alibab[112]	
69	*Super Troopers 2*	Movie	Indiegogo	Apr 25, 2015	$2M	$4,445,180	Sequel to the 2002 movie Super Troopers. Funding still in progress.	[113]
70	Pillars of Eternity II: Deadfire	Video Game	Fig	Feb 24, 2017	$1.1M	$4,407,598[114]	Sequel to Pillars of Eternity.	
71	ZrCoin	Blockchain	WAVES, Independent	Ongoing (planned to end Jun 9, 2017)	$3.5M	$4.2M	Funds earned from the ZrCoin crowdsale will be used to a fund zirconium dioxide plant in Russia	[115]
72	*Mighty No. 9*	Video game	Kickstarter	Oct 1, 2013	$900K	$4,046,579	Sci-fi action/platform video game. Including private backers, the project raised over $4M.	[116]
73	*Pillars of Eternity*	Video game	Kickstarter, Independent	Oct 16, 2012	$1.1M	$3,986,929	Fantasy role-playing video game. Succeeded *Double Fine Adventure* as the highest funded Kickstarter video game. Was succeeded by *Torment: Tides of Numenera* in April 2013. Including private backers, the project raised over $4.5M.	[117][118][119]
74	Psychonauts 2	Video Game	Fig	Jan 12, 2016	$3.3M	$3,829,024[120]	Sequel to Psychonauts (2005)	[121]
75	Micro Drone 3.0	Computing hardware	Indiegogo	August 16, 2015	$75k	$3,576,22	World's most advanced, small size Drone featuring a Camera, live streaming video and micro gimbal. Extreme Fliers is founded by Vernon Kerswell, a London-based robotics startup.	[122]
76	*Reaper Miniatures Bones*	Board game	Kickstarter	Aug 25, 2012	$30K	$3,429,235	Miniature figures by Reaper Miniatures with various miniature lines: Dark Heaven Legends, Pathfinder, Warlord, Legendary Encounters, Chronoscope, Savage Worlds, Bones, Legon of Justice, Master Series, Collect, Combat Assault Vehicle, Robot Supply Depot, The Boneyard	[123]
77	*The Micro*	3D printing	Kickstarter	May 7, 2014	$50K	$3,401,361	Consumer 3D printer supporting PLA or ABS, as well as proprietary Micro filament spools or standard 1.75 mm filament spools.	[124]
78	*The Dash*	Computing hardware	Kickstarter	Mar 31, 2014	$260K	$3,390,551		[125]
79	Double Fine Adventure (Subsequently renamed to *Broken Age*)	Video game	Kickstarter	Mar 13, 2012	$400K	$3,336,371	Point-and-click adventure game by Tim Schafer, designer of *Full Throttle* and *Grim Fandango*. Accompanied by a 2 Player Productions documentary. 87,142 backers, the most backers until surpassed by the *Veronica Mars Movie Project* in April 2013. Highest funded Kickstarter project until surpassed by the Pebble smartwatch in April 2012. Highest funded Kickstarter video game until surpassed by *Project Eternity* in October 2012. Credited with bringing in	[126][127][128][129]

							60,000 first time backers on the Kickstarter platform, increasing the viability of crowdfunding in video games.	
80	*Conan*	Board game	Kickstarter	Feb 11, 2015	$80K	$3,327,757	Miniatures board game based on the works of Robert E. Howard, in which players take on the roles of Conan the Barbarian and his heroic companions.	[130]
81	*Reaper Miniatures Bones II*	Board game	Kickstarter	Oct 26, 2013	$30K	$3,169,610	Continue expanding the Reaper's Bones line by Reaper Miniatures that was previously funded on Aug 25, 2012.	[131]
82	*Project CARS*	Video game	World of Mass Development	Nov 11, 2012	$3.1M	$3,142,808	Racing simulation video game by Slightly Mad Studios due to be released in November 2014. Note that Slightly Mad Studios themselves also contributed $2,072,400 to the overall funding for the game, amount raised is the total of public funding only.	[132]
83	Wasteland 3	Video Game	Fig	Nov 3, 2016	$2.75M	$3,121,716	Next iteration in the Wasteland franchise.	[133]
84	*Wish I Was Here*	Movie	Kickstarter	May 24, 2013	$2M	$3,105,473	Comedy drama film directed by Zach Braff and co-written with Adam J. Braff. Opening in Theaters 18 July 2014.	[134] [135]
85	*Battletech*	Video game	Kickstarter, BackerKit	early 2016	$250K	$2,996,286.08	A turn-based strategy video game by Harebrained Schemes set in the Battletech universe. Total includes $2,785,537.13 raised on Kickstarter (with an additional $79,850 raised through PayPal during the campaign) and $130,898.95 raised in BackerKit as of December 19, 2015. The Kickstarter campaign ended on November 3, 2015.	[136]
86	*FORM 1*	3D printing	Kickstarter	Oct 26, 2012	$100K	$2,945,885	Stereolithography (SLA) 3D printer created by Formlabs. High-resolution printing with plastic resin that creates layers as thin as 25 microns. Shipping began in May 2013.	[137]
87	*Wasteland 2*	Video game	Kickstarter	Apr 17, 2012	$900K	$2,933,252	Role-playing video game. Sequel to 1988's *Wasteland*, by members of the original team.	[138]
88	*Axent Wear Cat Ear Headphones*	Computing hardware	Indiegogo	Nov 22, 2014	$250K	$2,930,781	The latest fusion of fashion and functionality with external cat ear speakers and LED lights.	[139]
89	Växande hyresbestånd i centrala lägen	Other	Tessin	2016-08-01		$2,835,482	Real estate	
90	Opal Nugget Ice Maker	Computing hardware	Indiegogo	Aug 27, 2015	$150K	$2,778,019	Opal is an icemaker designed for the enthusiasts: people who drop by their favorite restaurant on the weekend to pick up a bag of that special soft ice	[140]
							On October 4 a campaign	

91	The Vegetarian Butcher Plant-Based Plant	Food	NPEX	October 27, 2015	€1M	€2.499.500 (legal limit)	was started to raise money for the Vegetarian Butcher plant-based plant in Breda. Bonds were issued at a value of €500 each. €2.5 M bonds were sold in three weeks.	[141]
92	*SCiO: Your Sixth Sense*	Computing hardware	Kickstarter	Jun 15, 2014	$200K	$2,762,571	A tiny spectrometer (molecular sensor) that allows one to receive instant relevant information about the chemical make-up of food, medicine, and plants, sent directly to one's smartphone.	[142]
93	Parcel Genie	Other	Angels Den	Feb 2012	$1M	$2,600,000	Parcel Genie raised enough funds to create a new gift delivery service, allowing customers to send gifts to family and friends without having to enter their address. The recipient receives a notification and arranges for the gift to be delivered to whatever address they enter.	[143]
94	Stone Groundbreaking Collaborations	Food	Indiegogo	Aug 29, 2014	$1M	$2,532,211	Stone Brewing Co. will open a brewery in Berlin, Germany and partially fund expansion by pre-selling beer from the Berlin brewery. The beer will be collaborations with other established breweries, released between late 2015 and 2017, and only available from the pre-sale.	[144]
95	*Jolla Tablet*	Computing hardware	Indiegogo	Dec 9, 2014	$380K	$2,506,418	Tablet powered with the MeeGo-based Linux Sailfish OS. It hit the goal for 380k in 2h15min. It reached the $1 million milestone by selling 4,467 tablets in less than 37 hours.	[145]
96	*Homestuck Adventure Game*	Video game	Kickstarter	Oct 4, 2012	$700K	$2,485,506	Adventure game based on the *Homestuck* webcomic. Succeeded *The Order of the Stick* as the highest funded comic-related Kickstarter project.	[146][147]
97	*Lazer Team*	Movie	Indiegogo	Jul 6, 2014	$650K	$2,480,334	Rooster Teeth, the company behind *Red vs. Blue*, Achievement Hunter, and *RWBY*, in their first feature-length movie tell the story of an extraterrestrial intelligence project that received a one-time signal from outer space. This is a live action sci-fi comedy that takes place decades later in the aftermath of that event. *Lazer Team* is the highest successfully funded film project on Indiegogo.	[148]
							Virtual reality head-mounted display designed for gaming. The campaign video featured support from Michael Abrash, Mark Bolas, John Carmack, Cliff	

98	*Oculus Rift*	Video game	Kickstarter	Sep 1, 2012	$250K	$2,437,429	Bleszinski, David Helgason, Jack McCauley, Gabe Newell, Chris Roberts and Tim Sweeney. Development units began shipping in March 2013. Sold to Facebook for $2 billion in March 2014.	[149][150]
99	*Kingdom Come: Deliverance*	Video game	Kickstarter, independent	Ongoing	$300K	$2,413,756	Open-world sandbox medieval RPG video game from Warhorse Studios lead designer Dan Vavra, writer and director of *Mafia: The City of Lost Heaven*. Set in the 15th century medieval Kingdom of Bohemia with a focus on historically accurate and realistic content. The game will be a single-player experience with branching quest lines and a highly interactive world encouraging emergent gameplay.	
100	*3Doodler*	3D printing	Kickstarter	Mar 25, 2013	$30K	$2,344,134	3D printing pen developed by Peter Dilworth and Maxwell Bogue of WobbleWorks LLC.	[151]
101	*Hex: Shards of Fate*	Video game	Kickstarter	Jun 7, 2013	$300K	$2,278,255	MMO fantasy trading card game.	[152][153]
102	PlexiDrone Camera Drone	Camera Gear	Indiegogo	Dec 3, 2015	$100K	$2,269,158	Ultra-Portable camera drone. Snap-together in 1 Minute. Capture Stunning Aerial Film & Photos with Ease!	[154]
103	*Gosnell: The Trial of America's Biggest Serial Killer*	Movie	Indiegogo	May 12, 2014	$2.1M	$2,241,043	Film about abortion doctor Kermit Gosnell who was convicted of 3 counts of first degree murder and one count of involuntary manslaughter and is currently serving a sentence of life in prison without the possibility of parole.	[155]
104	*Camelot Unchained*'	Video game	Kickstarter	May 2, 2013	$2M	$2,232,933	Realm versus realm MMORPG. The success of the Kickstarter allowed City State Entertainment to secure an additional $3M of private funding.	[156][157]
105	*Planetary Annihilation*	Video game	Kickstarter	Sep 14, 2012	$900K	$2,229,344	Real-time strategy video game by members of the *Total Annihilation* team.	[158]
106	*Solar Roadways*	Computing hardware	Indiegogo	Jun 20, 2014	$1M	$2,200,961	Solar panels that you can drive, park, and walk on. They melt snow and... cut greenhouse gases by 75-percent?!!!	[159]
107	*Bluesmart Inc.*	Computing hardware	Indiegogo	Dec 1, 2014	$50K	$2,121,650	Bluesmart Inc. created the world's first smart, connected carry-on luggage featuring location tracking, remote lock and battery charger.	[160]
108	*Soylent (drink)*	Food	Tilt.com	Apr 20, 2013	$100K	$2,100,000	The success of the campaign allowed the team to secure an additional $1.5M of private funding.[161]	[162]
	CHIP - The						A computer with a 1 GHz processor, 512MB RAM,	

109	*World's First 9 Dollar Computer*	Computing hardware	Kickstarter	Jun 6, 2015	$50K	$2,071,927	and 4GB onboard storage. It was successfully funded in its first 6 hours. It is the size of a payment card.	[163]
110	*Kingdom Death: Monster*	Board game	Kickstarter	Jan 8, 2013	$35K	$2,049,721	Cooperative board game set in a nightmare-horror world. Fight for your life, scavenge, craft, and band together to survive.	[164]
111	*Curing Batten Disease*	Other	Experiment.com	Sep 1, 2015	$1M	$1,972,706	Scientific research project to find a cure for CLN6-specific rare genetic disease, also called Batten disease, which has no cure.	[165][166]
112	*Canary home security*	Computing hardware	Indiegogo	Aug 26, 2013	$1M	$1,961,464	Canary is a device packed with smart sensors that empowers users to keep their homes safe and secure — controlled through mobile devices.	[167]
113	*Greek Bailout Fund*	Other	Indiegogo	Jul 6, 2015	€1,600,000,000	€1,930,577	Campaign to fund the bailout charge for the Greek financial crisis.	[168]
114	*Blue Mountain State: The Movie*	Movie	Kickstarter	May 15, 2014	$1.5M	$1,911,827	Feature length comedy based on the spike TV series	[169]
115	*Shadowrun Returns*	Video game	Kickstarter	Apr 29, 2012	$400K	$1,836,447	Single-player tactical role-playing game in the *Shadowrun* universe, not to be confused with *Shadowrun Online*.	[170]
116	*Elite: Dangerous*	Video game	Kickstarter, Independent	Jan 4, 2013	£1.25M[171]	£1,578,316[172]	Space trading and combat simulator from Frontier Developments, fourth game in the *Elite* series.	
117	*Scythe*	Board game	Kickstarter	Nov 6, 2015	$33K	$1,810,295	Scythe is a board game for 1-5 competitors by Jamey Stegmaier	[173]
118	*Oomi*	Computing hardware	Indiegogo	June 19, 2015	$50K	$1,767,042	Provides home security, entertainment enhancement, and ambiance control. The first smart home to incorporate NFC-based technology to simplify the device pairing process.	[174]
119	Crowfall	Video Game	Kickstarter	March 26, 2015	$800k	$1,766,204	Throne War PC MMO from ArtCraft Entertainment, Inc.	[175]
120	*TrackR bravo*	Computing hardware	Indiegogo	August 8, 2014	$30K	$1,739,149	Tracking device for effortless organization.	[176]
121	Ashes of Creation	Game	Intrepid Studios	Jun 3, 2017	$750k	$1,730,395	Upcoming MMORPG Ashes of Creation hit its goal of 750 thousand dollars in less than 12h	[177][178][179]
122	Rebel	Watch	LIV Swiss Watches	Jun 3, 2017	$30k	$1,703,914	The Most REBELLIOUS Swiss Automatic Watch Ever - LIV Watches Raised 470K in just 48 hours.	[180][181]
123	*Scanadu Scout*	Computing hardware	Indiegogo	Jul 20, 2013	$100K	$1,664,375	The first Medical Tricorder. A scanner packed with sensors designed to read your vital signs and send them wirelessly to your smartphone in a few seconds, any time, anywhere.	[182]
124	*Panono*	Computing hardware	Companisto		$100K	€1,618,945		[183]
125	*Warmachine: Tactics*	Video game	Kickstarter	Aug 10, 2013	$550K	$1,578,950	Fantasy turn-based tactics video game set in the Warmachine universe.	[184][185]

126	*Dreamfall Chapters: The Longest Journey*	Video game	Kickstarter	Mar 10, 2013	$850K	$1,538,425	Adventure game, third game in *The Longest Journey* series.	[186]
127	*LOVE ARMY FOR SOMALIA*	Other	GoFundMe	Ongoing	$1,000,000	$1,524,510	A charitable fundraiser partnering with Turkish Airlines to send aid to disadvantaged Somalian citizens.	[187]
128	*Kano*	Computing hardware	Kickstarter	Dec 19, 2013	$100K	$1,522,160	Mass manufacture a DIY computer kit	[188][189][190]
129	*ARKYD: A Space Telescope for Everyone*	Computing hardware	Kickstarter	Jun 30, 2013	$1M	$1,505,366	Launching and maintaining a publicly accessible Space Telescope. Partly funded by agreeing to take picture of funders' personal image from space with any background except for the sun. Launch is scheduled in 2015	[191]
130	*Kreyos*	Smartwatch	Indiegogo	Aug 12, 2013	$100K	$1,504,616	Smartwatch with voice and gesture control	[192]
131	*Freygeist*	Computing hardware	Companisto		$500K	€1,500,000	12 kg light E-Bike	[193]
132	*Mass Fidelity*	Computing hardware	Indiegogo	Nov 30, 2014	$48K	$1,489,071	A compact portable wireless speaker with claimed 'better than stereo' sound.	[194]
133	*Elevation Dock*	Computing hardware	Kickstarter	Feb 11, 2012	$75K	$1,464,706	Elevation Dock: The Best Dock For iPhone	[195]
134	*Noob, le jeu vidéo !*	Video game	Ulule	Nov 12, 2017	€90K	€1,246,153	Fantasy role-playing video game based on the French web series *Noob*, created by Fabien Fournier.	[196]
135	*Road Hard*	Movie	FundAnything	Aug 2, 2013	$1M	$1,445,889	American comedy-drama film co-written, produced, starring and directed by Adam Carolla and co-written with Kevin Hench. It is a comedy about the lives of aging road comics. Adam has since confirmed through a press conference that the film will co-star David Alan Grier, Illeana Douglas, Diane Farr, and Larry Miller.	[197]
136	*BIBLIOTHECA*	Other	Kickstarter	Jul 27, 2014	$37K	$1,440,435	A typography and publishing project by Adam Lewis Greene, consisting of "the Biblical Literature designed & crafted for reading, separated into four elegant volumes, and free of all numbers, notes, etc.," i.e., the Bible published in four volumes, using a modified American Standard Version and published without chapter or verse numbers.	[198][199]
137	*The Buccaneer*	3D printing	Kickstarter	Jun 29, 2013	$100K	$1,438,765	Consumer 3D Printer created by Pirate3D	[200]
138	*The Newest Hottest Spike Lee Joint*	Movie	Kickstarter	Aug 21, 2013	$1.25M	$1,418,910	Independent romantic horror comedy directed by Spike Lee	.[201]
139	*Tabletop Season 3 - With Wil Wheaton!*	Movie	Indiegogo	May 10, 2014	$500K	$1,414,154	Season 3 of Tabletop starring Wil Wheaton	[202]
	Petzval Portrait						Lomography recreation of the Petzval camera lens for	

140	*Lens*	Other	Kickstarter	Aug 24, 2013	$100K	$1,396,149	modern cameras. Shipped to backers in the first half of 2014.	[203]
141	*Tesla Museum*	Other	Indiegogo	Sep 29, 2012	$850K	$1,370,461	Buy Nikola Tesla's old laboratory, known as the Wardenclyffe Tower, for turning it into a museum. Property purchased on May 2, 2013.	[204]
142	*Million Dollars, But... The Game*	Board game	Kickstarter	Jun 10, 2016	$10K	$1,353,024	Card game version of the popular show produced by Rooster Teeth.	[205]
143	*System Shock*	Video game	Kickstarter	Nov 30, 2015	$900K	$1,350,700	A complete remake of the genre defining classic computer game from 1994	[206]
144	LimeSDR	Wireless hardware	Crowd Supply	Apr 5, 2017	$500k	$1,343,742	Software defined radio board for 2G, 3G 4G, 5G cellular / various IoT / WiFi / generic wireless systems between 100 kHz and 3.8 GHz. Backed by EE and Ubuntu. Crowd Supply's first $1m crowd fund.	[207]
145	*Ravean*	Other	Kickstarter	Nov 30, 2015	$100K	$1,330,293	Heated jacket	[208][209]
146	*Obduction*	Video game	Kickstarter	Nov 16, 2013	$1.1M	$1,321,306	Adventure game from the creators of Myst and Riven	[210]
147	*LIFX*	Computing hardware	Kickstarter	Nov 14, 2012	$100K	$1,314,542	WiFi enabled, multi-color, energy efficient LED light bulb controlled with an iPhone or Android.	[211]
148	*Airtame*	Computing hardware	Indiegogo	Jan 21, 2014	$160K	$1,260,148	Wireless HDMI screen-sharing on a TV, Projector or Monitor, compatible with almost all operating systems and computers.	[212][213]
149	*Muv-Luv*	Video game	Kickstarter	Nov 3, 2015	$250K	$1,255,444	English localization of Muv-Luv visual novel trilogy, consisting of *Muv-Luv* (which comes in two parts: "Muv-Luv Extra" and "Muv-Luv Unlimited") and its sequel *Muv-Luv Alternative*.	[214]
150	*The Order of the Stick*	Other	Kickstarter	Feb 21, 2012	$57.75K	$1,254,120	Reprint Rich Burlew's out-of-print "The Order of the Stick" comic books to reach new readers	[215]
151	*Lima*	Computing hardware	Kickstarter	Sep 8, 2013	$69K	$1,229,074	An OpenWRT Linux-based hardware adapter for unifying USB-connected storage as Network-attached storage.	[216][217]
152	*Massive Chalice*	Video game	Kickstarter	Jun 27, 2013	$725K	$1,229,015	Fantasy turn-based tactics video game. Double Fine Productions' second Kickstarter campaign, after *Double Fine Adventure* in March 2012.	[218][219]
153	*LIX*	3D printing	Kickstarter	May 29, 2014	£30K	£731,690	LIX is The Smallest 3D Printing Pen in the World, it enables you to doodle in the air. This professional tool offers you the comfort and pushes your creativity to another level.	[220][221]
154	SmartThings	Computing hardware	Kickstarter	Sep 22, 2012	$250K	$1,209,423		[222][223]
155	*Shadowrun:*	Video	Kickstarter	Feb 17, 2015	$100K	$1,204,726	Harebrained Schemes' next Single-player tactical role-playing game in the *Shadowrun* universe.	[224]

	Hong Kong	game					Developed with an improved version of the *Shadowrun Returns* engine.	
156	*Theatre Is Evil*	Other	Kickstarter	May 31, 2012	$100K	$1,192,793	Allows Amanda Palmer to create a new record, art book, and tour.	[225]
157	*Luna Sleep*	Computing hardware	Indiegogo	Mar 26, 2015	$100K	$1,190,672	"Smart" bed cover that allows for bed cooling/heating and IFTTT integrations to other integrated Internet of Things products.	[226]
158	*Robot Dragonfly*	Computing hardware	Indiegogo	Dec 31, 2012	$110K	$1,140,975	Palm-sized UAV that flies like a bird and hovers like an insect; Designed for aerial photography, advanced gaming, R&D and security.	[227]
159	Range 15	Movie	Indiegogo	Jun 26, 2015	$325K	$1,123,585	Military movie.	[228]
160	LIV Swiss Watches	Watches	Kickstarter	Feb 19 2016	$40,000	$1,119,029	At the time this campaign ended the LIV GX1-A was the most funded Swiss timepiece in crowdfunding HISTORY.	
161	*Turris Omnia*	Computing hardware	Indiegogo	Ongoing	$100K	$1,116,258	More than just a router. The open-source center of your home. Turris Omnia is a powerful and extensible open source router. It features an open Linux-based operating system with automatic updates and extra security measures. Besides being a router, Turris Omnia is powerful enough to serve as small home server.	[229]
162	Pulse	Camera Accessory	Kickstarter	Dec 11th, 2015	$50K	$1,110,820	Remote camera trigger which allows DSLR cameras to be controlled via a smartphone. Campaign funded between November and December 2015.	[230]
163	Omni	Video game	Kickstarter	Jul 22, 2013	$150K	$1,109,351	Omnidirectional treadmill-like device for use with virtual reality head-mounted displays such as the Oculus Rift.	[231][232]
164	*Friday the 13th: The Game*	Video game	Kickstarter BackerKit	13 May 2016	$700K / Pre-order on BackerKit	$1,095,143.40	A survival horror multiplayer video game in which 8 people play: 1 plays Jason Voorhees while the rest play counselors at Camp Crystal Lake trying to survive	[233][234]
165	*RigidBot*	3D printing	Kickstarter	May 10, 2013	$31.5K	$1,092,098	A sturdy, customizable 3D printer that is easy to use and affordable for all.	[235]
166	*Pathfinder Online*	Video game	Kickstarter	Jan 14, 2013	$1M	$1,091,194	Sandbox style MMORPG in the *Pathfinder Roleplaying Game* universe. Second successful Kickstarter campaign for the game, contributing towards the full version.	[236][237]
167	Kyl21	Food	Companisto		€250K	€940,650	Molecular ice cream	[238]
168	*THE 10-YEAR HOODIE*	Other	Kickstarter	Apr 21, 2013	$50K	$1,053,830	A unisex sweatshirt guaranteed for a decade	[239]

169	*Restore the Shore*	Other	Indiegogo	Jan 31, 2013	$1.25M	$1,047,827	As part of the effort to help rebuild Seaside Heights, New Jersey - the heart of the Jersey Shore, which was devastated by Hurricane Sandy	[240]
170	*CST-01*	Computing hardware	Kickstarter	Feb 22, 2013	$200K	$1,026,292	A 0.80mm thin flexible wristwatch with an E Ink display housed in a single piece of stainless steel.	[241]
171	*Structure Sensor*	Computing hardware	Kickstarter	Nov 1, 2013	$100K	$1,290,439	Created by Occipital, a Structured light 3D scanner for iPad and other mobile devices that captures objects, people and rooms in 3D for augmented reality games, 3D scanning and indoor mapping.	[242]
172	*Minds.com*	Open source social networking service	Equity Crowdfunding	Jun 10, 2017	$1M	$1,035,095[243]	Broke the regulation crowdfunding record for fastest to raise $1 million[244]	

See also [edit]

- List of highest-funded equity crowdfunding projects
- Kickstarter#Top projects by funds raised
- Indiegogo#Top projects by funds raised
- List of video game crowdfunding projects

References [edit]

1. ^ "A blockchain start-up just raised $4 billion without a live product". *www.cnbc.com*. 31 May 2018.
2. ^ "The 11 biggest ICO fundraises of 2017". *Business Insider*. Retrieved 2018-09-11.
3. ^ Vigna, Paul (2017-08-12). "Latest Hot Digital Coin Offering: $187 Million in One Hour for Filecoin". *Wall Street Journal*. ISSN 0099-9660. Retrieved 2018-09-11.
4. ^ "$257 Million: Filecoin Breaks All-Time Record for ICO Funding - CoinDesk". 7 September 2017.
5. ^ Barzilay, Omri. "Tezos' $232 Million ICO May Just Be The Beginning".
6. ^ Yin-Poole, Wesley (17 November 2018). "Star Citizen shoots through the $200m raised barrier". *Eurogamer*.
7. ^ Weber, Rachel (2013-04-30). "Star Citizen funding now over $9m". *GamesIndustry.biz*. Retrieved 2013-05-30.
8. ^ Glanday, Craig; Fall, Stephen; Mackey, Roxanne; Bebbington, Theresa; Lorimer, Marie, eds. (2014). "Crowdsourcing". *Guinness World Records 2015*. London: Guinness World Records Limited. p. 141. ISBN 978-1-90-884363-0. OCLC 869770714. Archived from the original on 6 October 2014. Retrieved 16 October 2014.
9. ^ "Stretch Goals - Roberts Space Industries | Follow the development of Star Citizen and Squadron 42". *Stretch Goals - Roberts Space Industries | Follow the development of Star Citizen and Squadron 42*. Retrieved 2018-07-18.
10. ^ Woolf, Nicky (3 December 2014). "Star Citizen sets crowdfunding record as players spend $65m on spaceships". *The Guardian*. Guardian Media Group. Retrieved 16 December 2016. "These spacecraft are being pre-purchased for use in an eagerly awaited multiplayer online PC game called Star Citizen, currently in development by Cloud Imperium Games. In their eagerness to play, people have been buying starships in huge numbers, which has helped the game's makers completely annihilate all previous crowdfunding records."
11. ^ "Foxconn will make the world's first blockchain smartphone". *CNET*. 2018-04-04. Retrieved 2018-09-11.
12. ^ "Terms of Service Violation". *www.bloomberg.com*. Retrieved 2018-09-11.
13. ^ "The hottest startups in Tel Aviv". *Wired*.
14. ^ "Bancor protocol FAQs". *Bancor.Network*.
15. ^ Chavez-Dreyfuss, Gertrude (18 May 2016). "Virtual company may raise $200 million, largest in crowdfunding". *Reuters*. Thomson Reuters. Retrieved 19 August 2016.
16. ^ [a] [b] Popper, Nathaniel (17 June 2016). "A Hacking of More Than $50 Million Dashes Hopes in the World of Virtual Currency". *The New York Times*. The New York Times Company. Retrieved 19 August 2016.
17. ^ "The 11 biggest ICO fundraises of 2017". *Business Insider*. Retrieved 2018-09-11.
18. ^ "Polkadot passes the $140M mark for its fund-raise to link private and public blockchains [October 23-29, 2017]". *techcrunch.com*. Retrieved September 10, 2018.
19. ^ D. Evans, Brian (21 June 2017). "Status ICO Raised More Than $100 Million for Ethereum-Powered DApps on iOS and Android". *Inc.* Inc Magazine. Retrieved 21 June 2017.
20. ^ Torchinsky, Jason (4 February 2015). "40,000 people have paid thousands for an Elio car - will it ever be built?". *Boing Boing*. Retrieved 10 October 2016
21. ^ "Elio Motors Offers $7,000 Pre-Orders for Three-Wheeled 'Autocycle'". *Fortune*. 2016-08-13. Retrieved 2016-08-13.
22. ^ "Another Milestone". Elio Motors. 7 October 2016. Retrieved 10 October 2016.
23. ^ Ellis, Jack (29 June 2017). "Singapore startup raises $80m in cryptocurrency sale; another follows suit". *Tech in Asia*. Tech in Asia. Retrieved 29 June 2017.
24. ^ Agrawal, AJ. "6 Lessons Marketers Can Learn From Cryptocurrency Initial Coin Offerings". *Forbes*. Retrieved 2018-09-11.
25. ^ "Token Data | News, data and analytics for all ICO's and tokens". *www.tokendata.io*. Retrieved 2018-01-03.
26. ^ "BANKEX, the Bank-as-a-Service Enterprise, Announces Token Sale Event". Retrieved 2018-01-03.
27. ^ "Hollywood Hitmaker Plans to Fund Next Blockbuster With Crypto". *Bloomberg.com*. 2017-11-17. Retrieved 2018-01-03.
28. ^ "Token Data | News, data and analytics for all ICO's and tokens". *www.tokendata.io*. Retrieved 2018-01-03.
29. ^ Bitcoinist. "BANKEX Ranked One of the Top 20 ICOs of All Time - Bitcoinist.com". *bitcoinist.com*. Retrieved 2018-01-03.
30. ^ "TRON Breaks Into Top 10 Cryptocurrencies, Displaces Dash". *Cointelegraph*. 2018-01-04. Retrieved 2018-09-11.
31. ^ "Tron (TRX) - All information about Tron ICO (Token Sale) - ICO Drops". *ICO Drops*. 2017-08-24. Retrieved 2018-09-11.
32. ^ *forbes* https://www.forbes.com/sites/goncalodevasconcelos/2018/05/31/icos-the-good-the-bad-and-the-ugly/. Retrieved 11 September 2018. Missing or empty |title= (help)
33. ^ *forbes* https://www.forbes.com/sites/laurashin/2017/07/10/the-emperors-new-coins-how-initial-coin-offerings-fueled-a-100-billion-crypto-bubble/. Retrieved

11 September 2018. Missing or empty |title= (help)
34. ^ Keane, Jonathan (2017-05-31). "$35 Million in 30 Seconds: Token Sale for Internet Browser Brave Sells Out". *Coindesk*.
35. ^ *Forbes* https://www.wsj.com/articles/forget-an-ipo-coin-offerings-are-new-road-to-startup-riches-1499425200. Retrieved 11 September 2018. Missing or empty |title= (help)
36. ^ "What's next: ICO report and plans of Polybius – Project: PolybiusBank". *PolybiusBankProject*. 2017-07-07. Retrieved 2017-12-13.
37. ^ "Polybius : la première banque pour les Cryptomonnaie". 2017-06-27. Retrieved 2017-06-28.. Translated into English.
38. ^ Bitcoin.com, News (2017-06-26). "Polybius ICO Climbs & Climbs - Bitcoin News". *Bitcoin News*. Retrieved 2017-07-04.
39. ^ "CyberMiles Successfully Completes ICO With Record Token Contribution Rush [November 22, 2017]". *venturebeat.com*.
40. ^ "5miles Launches CyberMiles Blockchain Project to Decentralize the Online Marketplace - Forbes". *www.forbes.com*. 2017-10-03.
41. ^ "Solve Care (CAN)". *CryptoSlate*. Retrieved 2018-09-11.
42. ^ [a] [b] "Solve.Care Token Sale is Successfully Complete - Solve.Care Foundation". *solve.care*. Retrieved 2018-09-11.
43. ^ GeekWire (2015-10-26). "Glowforge 3D laser printer breaks 30-day crowdfunding record after $27.9M in sales". Retrieved 2018-01-23.
44. ^ "Aragon ICO - Check The ANT Token Price & Performance - ICO Watch List". *ICO Watch List*.
45. ^ "Pebble Time". *Kickstarter*. Pebble Technology. 2015-03-01. Retrieved 2015-03-28.
46. ^ "Prison Architect earns $19m from 1.25m sales - but what's next?". Eurogamer.net. 2015-09-30. Retrieved 2015-10-13.
47. ^ Rosenkrantz, Holly. "GoFundMe for border wall raises over $8 million from 140k donors". *www.cbsnews.com*. CBS News. Retrieved 21 December 2018.
48. ^ Stauffer, McKenzie. "GoFundMe for Trump's border wall tops $18M before 2019". *KUTV News*. Retrieved 2 January 2019.
49. ^ Feuerherd, Ben. "GoFundMe for Trump's Mexican-U.S. border wall raises more than $3 million in a few days". *MarketWatch*. MarketWatch. Retrieved 21 December 2018.
50. ^ "Ethereum falls on report that the second-biggest cryptocurrency is under regulatory scrutiny". *cnbc*. Retrieved 11 September 2018.
51. ^ *forbes* https://www.forbes.com/sites/nguyenjames/2017/12/20/the-australian-startups-riding-the-wave-of-cryptocurrencies/. Retrieved 11 September 2018. Missing or empty |title= (help)
52. ^ "Blockchain Energy Trading Startup Power Ledger Raises $17M in Cryptocurrency 'ICO '". Retrieved 2017-12-07.
53. ^ Thomsen, Simon (2017-10-15). "Australia's first Initial Coin Offering raises $34 million". *Business Insider Australia*. Retrieved 2017-12-07.
54. ^ "$34 Million: Australian Blockchain Startup Power Ledger Completes ICO - CoinDesk". *CoinDesk*. 2017-10-06. Retrieved 2017-12-07.
55. ^ "Fundraiser Was a Resounding Success – Cosmos Blog". *Cosmos Blog*. 2017-04-06. Retrieved 2018-09-11.
56. ^ "Cosmos Brings Interoperability To Blockchains". *ETHNews.com*. Retrieved 2018-09-11.
57. ^ https://www.forbes.com/sites/julesschroeder/2017/12/21/heres-what-two-millennial-blockchain-founders-have-to-say-about-cryptocurrency/. Retrieved 11 September 2018. Missing or empty |title= (help)
58. ^ Contract, Smart (2 May 2017). "TokenCard raises $16.516m in 30 minutes for their banking replacement platform". *EtherScan*.
59. ^ [a] [b] Allison, Ian (14 April 2016). "WAVES raises $2m in 24 hours in bid to take on permissioned blockchains". *International Business Times*.
60. ^ *forbes* https://www.forbes.com/sites/rogeraitken/2017/11/08/waves-set-to-become-fastest-decentralized-blockchain-platform-globally/. Retrieved 11 September 2018. Missing or empty |title= (help)
61. ^ Allison, Ian (8 May 2016). "Blockchain platform WAVES partners with 'Swiss knife' Bitcoin wallet Mycelium". *International Business Times*.
62. ^ Allison, Ian (2017-03-21). "Qtum token sale raises over $15m in five days". *International Business Times UK*. Retrieved 2017-03-24.
63. ^ Kastelein, Richard (2017-03-24). "Qtum Shatters ICO Records Raising $15.6 Million". *Blockchain News*. Retrieved 2017-03-24.
64. ^ Ryan Grepper (2014-08-18). "COOLEST COOLER: 21st Century Cooler that's Actually Cooler". Kickstarter. Retrieved 2014-08-18.
65. ^ Anthony Volastro and Eric Rosenbaum (2014-08-28). "A new king of Kickstarter is crowned!". cnbc. Retrieved 2014-08-28.
66. ^ "Flow Hive: Honey on Tap Directly From Your Beehive?". IndieGoGo. 2015-04-20. Retrieved 2017-12-30.
67. ^ Ubuntu Edge, 2012-07-22, Canonical Ltd., Indiegogo, Retrieved 2013-09-07
68. ^ Louis Garcia (2013-04-08). "Shroud Of The Avatar Raises $2 Million In Crowdfunding". *Game Informer*. Archived from the original on 11 April 2013. Retrieved 23 August 2016.
69. ^ Portalarium (2013-03-08). "Shroud of the Avatar: Forsaken Virtues". Kickstarter. Retrieved 2013-05-31.
70. ^ Roger Aitken. "Gnosis' Prediction Market Scores $12.5M In 'Record-Breaking' Crypto Auction". Forbes. Retrieved 26 April 2017.
71. ^ "Kingdom Death: Monster 1.5". 2016-11-25. Retrieved 2018-01-15.
72. ^ "Kingdom-death-monster". 2012-11-23. Retrieved 2018-01-15.
73. ^ Kavilanz, Parija. "Baubax jacket sought $20,000 on Kickstarter, but got $9 million". *CNNMoney*. Retrieved 2015-09-21.
74. ^ Dallke, Jim (3 August 2015). "This Chicago-Based Jacket is Now the Most Funded Clothing Project Ever on Kickstarter". *ChicagoInno*. Retrieved 19 August 2016.
75. ^ "Hugely Successful Kickstarter Jacket BauBax Heads to Indiegogo to Keep Momentum Going". *Chicago Inno*. Retrieved 2015-09-21.
76. ^ Pebble: E-Paper Watch for iPhone and Android, 2012-04-11, Pebble Technology, Kickstarter, retrieved at 2013-09-07
77. ^ "Exploding Kittens sets fire to Kickstarter". CNN. 2015-01-21. Retrieved 2015-01-21. |first1= missing |last1= in Authors list (help)
78. ^ Elan Lee (2015-01-20). "Exploding Kittens". Kickstarter. Retrieved 2015-01-21.
79. ^ [a] [b] Vincent, James (2015-01-28). "Exploding Kittens becomes the most backed Kickstarter project of all time". *The Verge*. Retrieved 2015-01-28.
80. ^ Aitken, Roger. "Fintech Golem's 'Airbnb' For Computing Crowdsale Scores $8.6M In Minutes". *Forbes*. Retrieved 12 December 2016.
81. ^ "Ouya: A New Kind of Video Game Console". *Kickstarter*. Ouya. 2012-07-10. Retrieved 2013-05-31.
82. ^ "Crowdfunding and Equity-based Crowdfunding – Weißenhaus". *Companisto*.
83. ^ Yin-Poole, Wesley (23 November 2018). "Shenmue 3 dev declares $7.1m crowdfunding total". *Eurogamer.net*. Retrieved 24 November 2018.
84. ^ etherscan.io. "Ethereum Account 0xa5384627f6dcd3440298e2d8b0da9d5f0fcbcef7 Info". *etherscan.io*. Retrieved 2016-10-04.
85. ^ "Ethereum eSports Rewards Platform FirstBlood Raises $6m in Crowdsale | Finance Magnates". 2016-09-26. Retrieved 2016-10-04.
86. ^ "Public blockchain investments heat up: $5 million in 5 minutes". Retrieved 18 December 2016.
87. ^ Pono (digital music service) (2014-04-15). "Pono Music - Where Your Soul Rediscovers Music". Kickstarter. Retrieved 2014-06-02.
88. ^ Tau, Byron. "Mayday PAC secures matching pledges". *Politico*. Retrieved 1 August 2014.
89. ^ Lessig, Lawrence (4 July 2014). "At 9:30pm ET, 4 July, this happened". *LESSIG Blog, v2*. Retrieved 23 August 2016.
90. ^ "Press release on Lucyd crowdfund" (PDF).
91. ^ [a] [b] [c] "Fidget Cube: A Vinyl Desk Toy". *Kickstarter*. Retrieved 15 October 2016.
92. ^ Kuchera, Ben. "Fidgeted made this toy one of Kickstarter's most successful campaigns". *Polygon*. Retrieved 2016-09-13.
93. ^ Fritz, Ben (February 21, 2014). "'Veronica Mars' to Break the Mold for Movie Releases". *The Wall Street Journal*. Retrieved February 26, 2014.
94. ^ Lisk (29 March 2016). "Lisk Raises Over 5.7 Million USD in 2nd Most Successful Crypto-Currency Crowd-Fund to Date". *CoinDesk* (Press release). Retrieved 23 August 2016.
95. ^ [a] [b] Igarashi, Koji (2015-05-11). "Bloodstained: Ritual of the Night". Kickstarter. Retrieved 2015-05-11.
96. ^ Jordan Novet (2015-03-02). "Website builder The Grid gets Chrome extension". Venture Beat. Retrieved 2015-03-12.
97. ^ LeVar Burton & Reading Rainbow (2014-07-02). "Bring Reading Rainbow Back for Every Child, Everywhere". Kickstarter. Retrieved 2014-06-06.
98. ^ "Chronicles of Elyria". *Chronicles of Elyria*. Retrieved 2018-12-04.
99. ^ [a] [b] "Restore King Chapel Now. Every Day & Dollar Counts".
100. ^ [a] [b] "An Hour of Code for Every Student".
101. ^ "Backed by $5 Million in Funding (4,700 BTC), Mastercoin Is Building a Flexible, New Layer of Money on Bitcoin". Yahoo Finance. 2013-12-04. Retrieved 2015-08-07.
102. ^ [a] [b] (in English) "2nd Kickstarter Campaign of Filippo Loreti". Kickstarter. Retrieved 16 June 2017.

103. ^ (in English) "Filippo Loreti's first Kickstarter campaign". Kickstarter. Retrieved 16 June 2017.
104. ^ (in Italian) "Una startup "made in Italy" batte il record di crowdfunding su Kickstarter". Wired Italia. Retrieved 16 June 2017.
105. ^ [a] [b] [c] Phil Savage (2013-05-01). "Torment: Tides of Numenera makes final stretch goal, player strongholds now secured". *PC Gamer*.
106. ^ "Torment: Tides of Numenera is the most funded Kickstarter game ever, watch the wrap party live". Retrieved 18 December 2016.
107. ^ inXile entertainment (2013-03-06). "Torment: Tides of Numenera". Kickstarter. Retrieved 2013-05-31.
108. ^ Allison, Ian (2016-10-26). "Synereo raises $4.7m to meet its 'blockchain promise '". *International Business Times UK*. Retrieved 2016-11-06.
109. ^ Redman, Jamie (2016-10-31). "Synereo Aims to 'Fundamentally Redesign the Internet' - Bitcoin News". *Bitcoin News*. Retrieved 2016-11-06.
110. ^ "G-RO: Revolutionary Carry-on Luggage". *Indiegogo*. 13 December 2015. Retrieved 22 December 2016.
111. ^ Smith, Chris (October 16, 2015). "Smart carry-on luggage takes Kickstarter by storm". *BGR*. Retrieved 21 September 2016.
112. ^ "Top 10 ICOs With The Biggest ROI". *Cointelegraph*. Retrieved 2018-09-11.
113. ^ Broken Lizard Industries (2015-04-03). "Super Troopers 2". Indiegogo. Retrieved 2015-04-03.
114. ^ "Pillars of Eternity II: Deadfire – Now Available". *Fig*.
115. ^ Allison, Ian (2017-03-22). "ZrCoin crowdfunds first ever commodities option on the blockchain". *International Business Times UK*. Retrieved 2017-05-31.
116. ^ Comcept USA, LLC (2013-08-31). "Mighty No. 9". Kickstarter. Retrieved 2014-05-15.
117. ^ Obsidian Entertainment (2012-09-14). "Project Eternity". Kickstarter. Retrieved 2013-05-31.
118. ^ Winda Benedetti (2012-10-17). "'Project Eternity' raises $3.9 million, sets Kickstarter record". *NBC News*. Retrieved 2013-05-29.
119. ^ Eddie Makuch (2012-12-04). "Project Eternity closes with $4.3 million". *GameSpot*. Retrieved 2013-05-29.
120. ^ "Psychonauts 2 Crowdfunding Campaign". *Fig*.
121. ^ "Psychonauts 2 Crowdfunding Campaign". *Fig*. Retrieved 2018-01-09.
122. ^ "Micro Drone 3.0: Flight in the Palm of Your Hand". *Indiegogo*.
123. ^ Reaper Miniatures (2012-08-25). "Reaper Miniatures Bones: An Evolution Of Gaming Miniatures". Kickstarter. Retrieved 2013-09-12.
124. ^ M3D (2014-05-07). "The Micro: The First Truly Consumer 3D Printer". Kickstarter. Retrieved 2014-06-03.
125. ^ BRAGI LLC. (2014-03-31). "The Dash – Wireless Smart In Ear Headphones". Kickstarter. Retrieved 2014-06-03.
126. ^ Double Fine Productions (2012-02-08). "Double Fine Adventure". Kickstarter. Retrieved 2013-05-31.
127. ^ Melanie Hicken (2013-04-12). "Veronica Mars Kickstarter backed by record number of fans". *CNNMoney.com*. Retrieved 2013-05-30.
128. ^ Alexandra Chang (2012-04-17). "Pebble Smartwatch Breaks Kickstarter Record In Five Days". *Wired*. Retrieved 2013-05-30.
129. ^ Curtis, Tom (2012-03-29). "Double Fine Kickstarter brings huge boost to crowd-funded games". *Gamasutra*. Retrieved 2013-05-30.
130. ^ "Conan". *Kickstarter*. Monolith Board Games. Retrieved 2015-02-11.
131. ^ "Bones II: The Return of Mr Bones!". *Kickstarter*. Reaper Miniatures. 2013-10-26. Retrieved 2014-06-08.
132. ^ "Project CARS - Funding Goal Reached! - VirtualR - Sim Racing News". *VirtualR - Sim Racing News*.
133. ^ "Wasteland 3 Crowdfunding Campaign". *Fig*. Retrieved 2018-01-09.
134. ^ WISH I WAS HERE, 2013-04-24, Zach Braff, Kickstarter, retrieved at 2013-09-07
135. ^ "Wish I Was Here (2014)". imdb. Retrieved 2014-06-07.
136. ^ Harebrained Schemes LLC. "BATTLETECH by Harebrained Schemes LLC - Kickstarter". Kickstarter. Retrieved 2015-12-19.
137. ^ FORM 1: An affordable, professional 3D printer, 2012-09-26, Formlabs, Kickstarter, retrieved at 2013-09-07
138. ^ inXile entertainment (2012-03-13). "Wasteland 2". Kickstarter. Retrieved 2013-05-31.
139. ^ Consumer Physics, Inc. (2014-11-22). "The latest fusion of fashion and functionality with external cat ear speakers and LED lights". Indiegogo. Retrieved 2014-06-08.
140. ^ "Opal Nugget Ice Maker". *Indiegogo*. Retrieved 2016-06-10.
141. ^ "Archived copy". Archived from the original on 2015-11-17. Retrieved 2015-11-12.
142. ^ Consumer Physics, Inc. (2014-06-15). "SCiO: Your Sixth Sense. A Pocket Molecular Sensor For All !". Kickstarter. Retrieved 2014-06-08.
143. ^ "Business Owners To Pitch Ideas At Speed Funding Event". *www.londonlovesbusiness.com*. Retrieved 26 March 2015.
144. ^ "Stone Groundbreaking Collaborations". Indiegogo. 2014-08-29. Retrieved 2014-09-03.
145. ^ "Jolla Tablet - world's first crowdsourced tablet". Indiegogo. 2014-11-19. Retrieved 2014-11-22.
146. ^ MS Paint Adventures (2012-09-04). "Homestuck Adventure Game". Kickstarter. Retrieved 2013-05-31.
147. ^ Graeme McMillan (2012-09-06). "'Homestuck' heads towards new Kickstarter record". *Digital Trends*. Retrieved 2013-05-29.
148. ^ "Lazer Team - A Movie by Rooster Teeth". Rooster Teeth. 2014-07-06.
149. ^ Oculus (2012-08-01). "Oculus Rift: Step Into the Game". Kickstarter. Retrieved 2013-05-31.
150. ^ Kovach, Steve (March 25, 2014). "Facebook Buys Oculus VR For $2 Billion". Business Insider. Retrieved June 6, 2014.
151. ^ 3Doodler: The World's First 3D Printing Pen, 2013-02-19, WobbleWorks LLC, Kickstarter, retrieved at 2013-09-07
152. ^ Cryptozoic Entertainment (2013-05-08). "HEX MMO Trading Card Game". Kickstarter. Retrieved 2013-06-07.
153. ^ Martin Waterhouse (2013-05-28). "HEX: The MMO is in the cards". *Massively*. Retrieved 2013-05-30.
154. ^ DreamQii Inc. (2014-10-2014). "PlexiDrone". Indiegogo. Retrieved 2017-04-11. Check date values in: |date= (help)
155. ^ "Gosnell Movie: A historic crowdfunding campaign for a movie about America's biggest serial killer, abortionist Kermit Gosnell and the media cover-up". 2014-05-09. Indiegogo. retrieved at 2014-05-09.
156. ^ City State Entertainment (2013-04-02). "Camelot Unchained". Kickstarter. Retrieved 2013-05-31.
157. ^ Alexa Ray Corriea (2013-05-02). "Camelot Unchained funding closes with $2.2M, additional $3M coming from private investors". *Polygon*. Retrieved 2013-05-29.
158. ^ Uber Entertainment (2012-08-15). "Planetary Annihilation - A Next Generation RTS". Kickstarter. Retrieved 2013-05-31.
159. ^ Julie and Scott Brusaw (2014-04-21). "Solar Roadways". Indiegogo. Retrieved 2014-06-06.
160. ^ Bluesmart (2014-04-21). "Bluesmart". Indiegogo. Retrieved 2014-12-01.
161. ^ Crowdfunding Darling Soylent Nets $1.5 Million In VC Funding. October 22, 2013
162. ^ "Top Ten Crowdfunding Campaigns Built With Tilt Open". *Tilt.com*. Tilt.com. Archived from the original on 19 June 2015. Retrieved 28 August 2014.
163. ^ [1], 2015-5-7, CHIP - The world's first 9 dollar computer , Kickstarter, retrieved at 2015-09-03
164. ^ Kingdom Death: Monster, 2013-11-23, Kingdom Death, Kickstarter, retrieved at 2015-01-06
165. ^ "Cure Batten - NLC". Experiment.com. 2015-09-01. Retrieved 2015-09-01.
166. ^ "Producer Gordon Gray Hoping For A Facebook Miracle; Race Against Time To Save His Daughters From Rare Brain Disease". *Deadline Hollywood*. 2015-06-09. Retrieved 2015-06-09.
167. ^ Canary: The first smart home security device for everyone, 2013-07-22, Canary, Indiegogo, retrieved at 2013-09-07
168. ^ "Greek Bailout Fund - Indiegogo". *companisto.com*.
169. ^ "Blue Mountain State: The Movie". *Kickstarter*.
170. ^ Harebrained Schemes (2012-04-04). "Shadowrun Returns". Kickstarter. Retrieved 2013-05-31.
171. ^ Kit Eaton (2013-01-04). "Kickstarter Gets Serious: Space Game "Elite" Wins Record $2 Million Funding". *Fast Company*. Retrieved 2013-05-29.
172. ^ Frontier Developments (2012-11-05). "Elite: Dangerous". *Kickstarter*. Retrieved 2013-05-31.
173. ^ Jamey Stegmaier (2015-11-07). "Scythe". Kickstarter. Retrieved 2015-11-07.
174. ^ Oomi (2015-04-20). "Oomi: Smart Home. Simplified". Indiegogo. Retrieved 2015-10-12.
175. ^ "Crowfall - Throne War PC MMO". *Kickstarter*. Retrieved 2018-03-09.
176. ^ Chris Herbert (2014-08-08). "TrackR bravo: Lose Things? Relax, TrackR bravo has your back". Indiegogo. Retrieved 2014-08-08.
177. ^ "Fans invest 750 thousand dollars and hit the goal in less than 12hours" - MMOs.com "". 2017-05-12. Retrieved 2017-05-12.
178. ^ cite web|url=https://www.kickstarter.com/projects/1791520601/ashes-of-creation-new-mmorpg-by-intrepid-studios/ " Kickstarter"

178. ^ cite web|url=https://www.kicktraq.com/projects/1791529601/ashes-of-creation-new-mmorpg-by-intrepid-studios/ "Kicktraq"
179. ^ cite web|url=https://www.kickstarter.com/projects/1791529601/ashes-of-creation-new-mmorpg-by-intrepid-studios/ "Kickstarter"
180. ^ "LIV Rebel on Kickstarter". 2017-02-28. Retrieved 2017-02-28.
181. ^ "LIV Rebel on LIVwatches". LIV Swiss Watches. 2017-02-28. Retrieved 2017-02-28.
182. ^ Scanadu Scout, the first Medical Tricorder, July 20, 2013, Scanadu, Indiegogo, retrieved at 2013-09-12
183. ^ "Crowdfunding and Equity-based Crowdfunding - Panono -". *companisto.com*.
184. ^ Privateer Press Interactive (2013-07-10). "WARMACHINE: TACTICS". Kickstarter. Retrieved 2013-07-18.
185. ^ Mitch Dyer (2013-07-15). "Warmachine: Tactics Kickstarts the Tabletop Game's Digital Future". *IGN*. Retrieved 2013-07-18.
186. ^ Red Thread Games (2013-02-08). "Dreamfall Chapters: The Longest Journey". Kickstarter. Retrieved 2013-05-31.
187. ^ Jérôme Jarre (2017-03-17). "LOVE ARMY FOR SOMALIA". GoFundMe. Retrieved 2017-03-19.
188. ^ "Kano Computer Kit Lets Anyone Build a PC From Scratch". *Mashable*. 24 November 2013.
189. ^ "Brief: Kano Kickstarter Ends, Raises Over $1.5 Million". Crowdfund Insider. 20 December 2013.
190. ^ "Lighting fireworks in 2014". Kickstarter. 3 January 2014.
191. ^ Planetary Resources (2013-06-30). "ARKYD: A Space Telescope for Everyone". Kickstarter. Retrieved 2013-09-12.
192. ^ KREYOS: The ONLY Smartwatch With Voice & Gesture Control, August 12, 2013, The Kreyos Team, Indiegogo, retrieved at 2013-09-12
193. ^ "Crowdfunding and Equity-based Crowdfunding - FREYGEIST -". *companisto.com*.
194. ^ [2], July 7, 2015, The Mass Fidelity team, Indiegogo, retrieved at 2015-07-07
195. ^ Casey Hopkins + ElevationLab (2012-02-11). "Elevation Dock: The Best Dock For iPhone". Kickstarter. Retrieved 2013-09-12.
196. ^ Olydri Studio (2017-11-12). "Noob, le jeu vidéo !". Ulule.
197. ^ Adam Carolla (2013-08-02). "Road Hard - A Movie by Adam Carolla". FundAnything. Archived from the original on 2014-01-18.
198. ^ Adam Greene (2014-06-27). "BIBLIOTHECA". Kickstarter.
199. ^ "Bibliotheca, the ESV Reader's Bible, and the Future of Printed Bibles - Bible Design Blog". *Bible Design Blog*.
200. ^ Pirate3D Inc (2013-06-29). "The Buccaneer® - The 3D Printer that Everyone can use!". Kickstarter. Retrieved 2013-09-12.
201. ^ Spike Lee (2013-08-21). "The Newest Hottest Spike Lee Joint". Kickstarter. Retrieved 2013-09-12.
202. ^ Tabletop Season 3 - With Wil Wheaton!, May 10, 2014, Indiegogo, retrieved at 2015-02-06
203. ^ Lomography (2013-08-24). "The Lomography Petzval Portrait Lens". Kickstarter. Retrieved 2013-09-12.
204. ^ Let's Build a Goddamn Tesla Museum, September 29, 2013, Matthew Inman, Indiegogo, retrieved at 2013-09-12
205. ^ "Million Dollars, But... The Game on Kickstarter".
206. ^ [3], July 28, 2016, Nightdive Studios. Kickstarter, retrieved at 2015-12-27
207. ^ "LimeSDR". *Crowd Supply*.
208. ^ [4], November 30, 2015, Cyan Inc. Kickstarter, retrieved at 2015-12-27
209. ^ [5], Utahn's heated jacket becomes 2nd most-funded Kickstarter clothing project, retrieved at 2015-12-27
210. ^ [6], November 16, 2013, Cyan Inc. Kickstarter, retrieved at 2015-02-11
211. ^ Phil Bosua (2012-11-14). "LIFX: The Light Bulb Reinvented". Kickstarter. Retrieved 2013-09-12.
212. ^ Airtame (2014-01-21). "Airtame: Wireless HDMI". Oresundstartups. Retrieved 2014-01-21.
213. ^ "AIRTAME: Wireless HDMI for Everyone". indiegogo. Retrieved 8 June 2014.
214. ^ "The Muv-Luv Team" (2015-09-24). "Muv-Luv: A Pretty Sweet Visual Novel Series". Degica. Retrieved 2016-02-06.
215. ^ Rich Burlew (2012-02-21). "The Order of the Stick Reprint Drive". Kickstarter. Retrieved 2013-09-12.
216. ^ The CGC team (2013-09-08). "Lima: the brain of your devices". Kickstarter. Retrieved 2013-09-12.
217. ^ Dropbox Alternative Lima (Née Plug) Works With Chromecast, Breaks Into Kickstarter Tech Top 10, August 15th, 2013, Romain Dillet, *TechCrunch.com*, Retrieved at 2013-09-12
218. ^ Double Fine Productions (2013-05-30). "Double Fine's MASSIVE CHALICE". Kickstarter. Retrieved 2013-05-30.
219. ^ Jeffrey Matulef (2013-05-30). "Double Fine takes to Kickstarter yet again with strategy epic Massive Chalice". *Eurogamer*. Retrieved 2013-05-30.
220. ^ LIX (2014-05-29). "LIX - The Smallest 3D Printing Pen in the World". Kickstarter. Retrieved 2014-06-26.
221. ^ World's Smallest 3D-Printing Pen, April 10, 2014, Lance Ulanoff *Mashable*, Retrieved at 2014-06-26
222. ^ SmartThings (2012-09-22). "SmartThings: Make Your World Smarter". Kickstarter. Retrieved 2013-09-12.
223. ^ IFTTT flexes its muscle with new SmartThings channel, September 6, 2013, Ry Crist, *CNET*, Retrieved at 2013-09-12
224. ^ Harebrained Schemes (2015-01-13). "Shadowrun: Hong Kong". Kickstarter. Retrieved 2015-02-18.
225. ^ Amanda Palmer (2012-05-31). "Amanda Palmer: The new RECORD, ART BOOK, and TOUR". Kickstarter. Retrieved 2013-09-12.
226. ^ "Luna: Turn your Bed into a Smart Bed". Indiegogo. 2015-03-26. Retrieved 2015-10-06.
227. ^ "Robot Dragonfly - Micro Aerial Vehicle". Indiegogo. 2012-12-31. Retrieved 2013-09-12.
228. ^ "Range 15 Movie". Indiegogo.
229. ^ "Turris Omnia - More than just a router". Indiegogo. 2015-12-12. Retrieved 2016-01-12.
230. ^ "Pulse - Your Camera, Upgraded". *Kickstarter*.
231. ^ Virtuix (2013-06-04). "Omni: Move Naturally in Your Favorite Game". Kickstarter. Retrieved 2013-06-05.
232. ^ Hayden Dingman (2013-06-04). "Virtuix Omni gaming treadmill will let you walk through your favorite game worlds". *PC World*. Retrieved 2013-06-05.
233. ^ Greenback, Randy. "Friday the 13th: The Game by Randy Greenback - Gun Media - Kickstarter". Kickstarter. Retrieved 13 August 2016.
234. ^ "'Friday the 13th: The Game' is a Kickstarter Success". *BloodyDisgusting*. Retrieved November 11, 2015.
235. ^ Michael Lundwall (2013-05-10). "RigidBot 3D Printer". Kickstarter. Retrieved 2013-09-12.
236. ^ Goblinworks (2012-11-27). "Pathfinder Online: A Fantasy Sandbox MMO". Kickstarter. Retrieved 2013-05-31.
237. ^ Matt Daniel (2013-01-14). "Pathfinder Online Kickstarter now successfully funded". *Massively*. Retrieved 2013-05-29.
238. ^ "Crowdfunding and Equity-based Crowdfunding - Kyl - Overview". *companisto.com*.
239. ^ Jake Bronstein (2013-04-21). "THE 10-YEAR HOODIE: Built for Life, Backed for a Decade!". Kickstarter. Retrieved 2013-09-12.
240. ^ Restore the Shore, January 31, 2013, Cameron Sinclair, Indiegogo, retrieved at 2013-09-12
241. ^ Central Standard Timing (2013-02-22). "CST-01: The World's Thinnest Watch". Kickstarter. Retrieved 2013-09-12.
242. ^ Occipital (2013-11-01). "Structure Sensor: Capture the World in 3D". Kickstarter. Retrieved 2014-01-12.
243. ^ "Minds". Crunchbase. 2017-09-21. Retrieved 2018-01-31.
244. ^ Ottman, Bill (2017-05-31). "Minds Update | Thank you! Minds broke the regulation crowdfunding record for fastest to raise $1 million!". *wefunder.com*. Retrieved 2018-01-31.

Categories: Crowdfunding lists | Crowdfunded projects

This page was last edited on 16 February 2019, at 19:12 (UTC).

Text is available under the Creative Commons Attribution-ShareAlike License; additional terms may apply. By using this site, you agree to the Terms of Use and Privacy Policy. Wikipedia® is a registered trademark of the Wikimedia Foundation, Inc., a non-profit organization.

Privacy policy About Wikipedia Disclaimers Contact Wikipedia Developers Cookie statement Mobile view

EOS.IO

From Wikipedia, the free encyclopedia

EOS.IO is a blockchain protocol powered by the native cryptocurrency EOS. The protocol emulates most of the attributes of a real computer including hardware (CPU(s) & GPU(s) for processing, local/RAM memory, hard-disk storage) with the computing resources distributed equally among EOS cryptocurrency holders. EOSIO operates as a smart contract platform and decentralized operating system intended for the deployment of industrial-scale decentralized applications through a decentralized autonomous corporation model. The smart contract platform claims to eliminate transaction fees and also conduct millions of transactions per second.

Contents [hide]

EOS	
Ticker symbol	EOS
Development	
Original author(s)	Daniel Larimer, Brendan Blumer[2]
White paper	[2]
Initial release	Dawn 3.0.1-alpha[1] / January 31, 2018; 12 months ago
Latest release	EOSIO 1.1.4[1] / August 8, 2018; 6 months ago
Code repository	eos.io on GitHub
Development status	Currently under development
Written in	C++
Operating system	multi platform
Developer(s)	block.one
License	MIT License (open source)[3]
Website	eos.io
Ledger	
Timestamping scheme	delegated Proof-of-stake
Block time	500 ms
Block explorer	bloks.io
Circulating supply	896,149,492 (27th of July 2018)
Valuation	
Exchange rate	$8.40 (27th of July 2018)[4]
Market cap	$7.528 billion (27th of July 2018)[4]

block.one	
Type	Private
Industry	Blockchain
Area	Global

History

Based on a white paper published in 2017, the EOSIO platform was developed by the private company **block.one** and released as open-source software on June 1, 2018. In

Main page
Contents
Featured content
Current events
Random article
Donate to Wikipedia
Wikipedia store

Interaction
Help
About Wikipedia
Community portal
Recent changes
Contact page

Tools
What links here
Related changes
Upload file
Special pages
Permanent link
Page information
Wikidata item
Cite this page

Print/export
Create a book
Download as PDF
Printable version

Languages
Deutsch
Français
□□□
Italiano
Português
Русский
□□

Edit links

served	
Key people	Brendan Blumer (CEO), Dan Larimer (CTO)
Products	Decentralized applications
Website	block.one

order to ensure widespread distribution of the native cryptocurrency at the launch of the blockchain, one billion tokens were distributed as ERC-20 tokens by block.one. This provided the distribution to allow anyone to launch the EOS blockchain once the software was released. The CEO of block.one, Brendan Blumer, announced that block.one would support the EOSIO blockchain with over one billion USD in funding from the token sale and ultimately block.one raised over four billion USD to support the blockchain during the Initial Coin Offering (ICO) period.[5]

The original test net, Dawn 1.0, was released on September 3, 2017, with test net versions Dawn 2.0 released on December 4, 2017, Dawn 3.0 on January 25, 2018 and Dawn 4.0 on May 7, 2018.

EOSIO's Dawn 1.0 was launched on the EOSIO mainnet on June 1, 2018 and currently operating under version 1.1.4.[6]

Technical description

The aim of the platform is to provide decentralized application hosting, smart contract capability and decentralized storage of enterprise solutions that solve the scalability issues of blockchains like Bitcoin and Ethereum, as well as eliminating all fees for users. EOSIO accomplishes this by being both multi-threaded (able to run on multiple computer cores) as well as using delegated proof-of-stake for its consensus protocol. It aims to be the first decentralized operating system (EOSIO) that provides a development environment for decentralized applications like Steemit, a social network with monetary incentives and BitShares, a decentralized cryptocurrency exchange (DEX).

The main native token, EOS, is a utility token that provides both bandwidth and storage on the blockchain, in proportion to total stake (owning 1% of EOS tokens allows for usage of up to 1% of the total available bandwidth). EOS tokens also allow the owner to cast votes and participate in the on-chain governance of the blockchain, again in proportion to the owner's stake. The EOSIO platform will vote for 21 block producers during its launch, who will generate and validate blocks within a 500 ms block time. General purpose and smart contract language to build upon the EOS platform will be WebAssembly (Rust, C, C++), a portable stack machine that is developed at the World Wide Web Consortium (W3C).[7]

Accounts

The EOSIO software permits all accounts to be referenced by a unique human readable name of up to 12 characters in length. The name is chosen by the creator of the account. The account creator must reserve the RAM required to store the new account until the new account stakes tokens to reserve its own RAM.[2]

RAM Trading

EOSIO adopts a free-market approach to allocating scarce resources to their

highest purpose. To facilitate this market, the eosio system contract allows users to buy RAM from the system and sell RAM back to the system in exchange for the blockchains native tokens (e.g EOS). This provides liquidity in the RAM market while facilitating price discovery. The less unallocated RAM available to the market maker the higher the market maker prices the remaining RAM. The algorithm used for this market maker is known as a Bancor Relay. A Bancor Relay does not set the price of RAM but rather offers to buy and sell at previously established market rates. Anytime the current market rate is different than the current price offered by the Bancor Relay, traders will buy or sell RAM accordingly, reducing the market determined price gap.

EOS Resource Renting & Rent Distribution

EOS Resource Renting and Rent Distribution is a proposed solution for lowering the capital costs of using network and CPU resources on EOSIO based blockchains.

EOS.IO Storage

EOS.IO Storage is a proposed decentralized file system designed to give everyone the ability to permanently store and host files accessible by any web browser. Unlike some other proposed alternatives, there would be no upfront fee or ongoing charge for storage or bandwidth on EOS.IO Storage aside from a completely refundable deposit. Users must hold tokens while they need storage and bandwidth and may sell tokens when storage and bandwidth is no longer required. Built on the InterPlanetary File System (IPFS) and the EOS.IO software, EOS.IO Storage will be a service provided by block producers for those who hold tokens on a blockchain that adopts the EOS.IO software. The block producers would be incentivized to replicate and host these files, allowing anyone with an Internet browser to access them. With EOS.IO Storage block producers could provide high bandwidth serving of videos, music, images and for applications like Steemit and compete with services such as Amazon's AWS while utilizing an ownership, rather than subscription, model.

block.one, EOSIO Ecosystem and Everipedia

block.one is a company registered in the Cayman Islands, which began offering EOS tokens in June 2017 to the public, raising over $4 billion (a record for an ICO).[8] Daniel Larimer is currently the Chief Technology Officer of block.one, notable for his role in building Bitshares, a decentralized exchange, building Steemit, a decentralized social media platform, developing delegated proof-of-stake and proposing the idea of a decentralized autonomous corporation.[9]

On December 6, 2017, Everipedia, a for-profit, wiki-based online encyclopedia, announced plans using EOS blockchain technology and work on an airdrop of a cryptocurrency called IQ to encourage generating information.[10] The IQ tokens are intended to be exchangeable for Bitcoin.[11] One of the goals of the company is to stop certain countries from blocking the content, by the integration of the blockchain model.[12] Once Everipedia is decentralized and hosted on the EOSIO platform, countries such as Turkey and Iran that block Wikipedia will no longer be able to

block it, via Everipedia's fork.[13] Mike Novogratz, CEO of Galaxy Investment LP, a cryptocurrency investment firm, and block.one led a group of institutions that invested $30 million in Everipedia on February 8, 2018. Novogratz also funds EOSIO Ecosystem, a $325-million joint venture between his Galaxy Digital LP and block.one.[14]

References

1. ^ **a** **b** "eos: An open source smart contract platform". *GitHub*. 2 Oct 2018. Retrieved 2 Oct 2018.
2. ^ **a** **b** **c** "EOS.IO Technical White Paper v2". *GitHub*. 16 Mar 2018. Retrieved 3 October 2018.
3. **^** "EOSIO/eos is licensed under the MIT License". *GitHub*. Retrieved 2018-06-08.
4. ^ **a** **b** "EOS". *Coinmarketcap*. Retrieved 2 Oct 2018.
5. **^** Rooney, Kate (2018-05-31). "A blockchain start-up just raised $4 billion without a live product". *CNBC*. Retrieved 2018-08-12.
6. **^** "EOSIO/eos". *GitHub*. Retrieved 2018-08-12.
7. **^** Bright, Peter (18 June 2015). "The Web is getting its bytecode: WebAssembly". *Ars Technica*. Condé Nast.
8. **^** Nonninger, Lea. "Block.one just raised a $4 billion ICO". *Business Insider*.
9. **^** Kauflin, Jeff (7 Feb 2018). "Dan Larimer's Path From Working On Weapons To Minting Crypto Riches". *Forbes*. Retrieved 2 Oct 2018.
10. **^** del Castillo, Michael (6 December 2017). "Encyclopedia Blockchainica: Wikipedia Co-Founder to Disrupt His Own Creation". CoinDesk.
11. **^** Sitaraman, Viputheshwar (12 November 2015). "Q&A: Mahbod Moghadam — Cofounder, Everipedia". *HuffPost*.
12. **^** Wallenbergtorsdag, Björn (14 December 2017). "Wikipedia-grundare ansluter till utmanare startad av svensk 22-åring" [Wikipedia-founders Connect to challenger started by Swedish 22-year-old] (in Swedish). DiGITAL.
13. **^** Rubin, Peter (6 December 2017). "The Wikipedia Competitor That's Harnessing Blockchain For Epistemological Supremacy". *Wired*.
14. **^** "Novogratz's new fund, others invest $30 million in online encyclopedia". *Reuters*. 8 February 2018.

External links

- Official website
- eos.io Wiki on GitHub – eos.io related Wiki

v · t · e	**Cryptocurrencies**
	Blockchain · Cryptocurrency tumbler · Cryptocurrency exchange · Cryptocurrency wallet ·

Technology	Cryptographic hash function · Distributed ledger · Fork · Lightning Network · Smart contract	
Consensus mechanisms	Proof-of-authority · Proof-of-space · Proof-of-stake · Proof-of-work	
Proof-of-work currencies	**SHA-256-based**	Bitcoin · Bitcoin Cash · Counterparty · MazaCoin · Namecoin · NeuCoin · Nxt · Peercoin · Steem · Titcoin
	Ethash-based	Ethereum · Ethereum Classic
	Scrypt-based	Auroracoin · Bitconnect · Bitcoin Gold · Coinye · Dogecoin · Gridcoin · Litecoin · PotCoin
	Equihash-based	Zcash · Zcoin
	CryptoNote-based	Monero
	X11-based	Dash · Petro
	Lyra2-based	Taler
	Other	Verge · Vertcoin
Proof-of-stake currencies	**EOS.IO**	
ERC-20 tokens	Augur · Aventus · Basic Attention Token · Centra · Kin · KodakCoin · Minds · Power Ledger · Publiq	
Other currencies	BitShares · Filecoin · NEM · NEO · NuBits · Primecoin · Ripple · Stellar · Tether	
Related topics	Airdrop · BitLicense · Blockchain game · Complementary currency · Crypto-anarchism · Cryptocurrency bubble (2018 cryptocurrency crash) · Digital currency · Double-spending · Initial coin offering · Initiative Q · List of cryptocurrencies · Stablecoin · Token money · Virtual currency	
Category · **Commons** · **List**		

Categories: Cryptocurrencies | Companies of the Cayman Islands | 2017 software | Blockchains | Ethereum tokens | Alternative currencies

This page was last edited on 21 December 2018, at 14:07 (UTC).

Text is available under the Creative Commons Attribution-ShareAlike License; additional terms may apply. By using this site, you agree to the Terms of Use and Privacy Policy. Wikipedia® is a registered trademark of the Wikimedia Foundation, Inc., a non-profit organization.

Privacy policy About Wikipedia Disclaimers Contact Wikipedia Developers Cookie statement

Mobile view

Proofs of Useful Work

Marshall Ball* Alon Rosen† Manuel Sabin‡ Prashant Nalini Vasudevan§

February 27, 2017

Abstract

We give Proofs of Work (PoWs) whose hardness is based on a wide array of computational problems, including Orthogonal Vectors, 3SUM, All-Pairs Shortest Path, and any problem that reduces to them (this includes deciding any graph property that is statable in first-order logic). This results in PoWs whose completion does not waste energy but instead is *useful* for the solution of computational problems of practical interest.

The PoWs that we propose are based on delegating the evaluation of low-degree polynomials originating from the study of average-case fine-grained complexity. We prove that, beyond being hard on the average (based on worst-case hardness assumptions), the task of evaluating our polynomials *cannot be amortized* across multiple instances.

For applications such as Bitcoin, which use PoWs on a *massive* scale, energy is typically wasted in huge proportions. We give a framework that can utilize such otherwise wasteful work.

Keywords: Proofs of Work, Fine-Grained, Delegation, Blockchain.

*Columbia University, New York, NY, USA. Email: marshall@cs.columbia.edu.

†Efi Arazi School of Computer Science, IDC Herzliya, Israel. Email: alon.rosen@idc.ac.il.

‡UC Berkeley, Berkeley, CA, USA. Email: msabin@berkeley.edu.

§CSAIL, Massachusetts Institute of Technology, Cambridge, MA, USA. Email: prashvas@mit.edu.

1 Introduction

Proofs of Work (PoWs) were introduced [DN92] to enforce that a certain amount of energy was expended for doing some task in an easily verifiable way. In most applications, PoWs force malicious users to accrue a large workload, thus guarding against email spam, denial of service attacks, and, most recently, double-spending in cryptocurrencies such as Bitcoin [Nak08]. Unfortunately, existing PoW schemes are often disconnected from the task they are attached to, so that the work expended is not actually useful in accomplishing that task. More importantly, the work and energy expended is generally *not useful for anything except proving that work had in fact been done.*

To this end, PoWs are wasteful of real resources and energy and, in the massive use case of Bitcoin, have even been called an "environmental disaster" [And13]. Two early attempts to combat this are Primecoin [Kin13] and Permacoin [MJS+14]. The former suggests a Proof of Work system whose outcome enables the search for chains of prime numbers, whereas the latter repurposes Bitcoin mining resources to achieve distributed storage of archival data, based on Proofs of Retrievability (thus requiring clients to invest not just computational resources, but also storage).

Another line of work, studies Proofs of Space [ABFG14, DFKP15, KK14], where a user must dedicate a significant amount of disk space, instead of computing power, to perform their task. This accomplishes a similar constraint on malicious activity to PoWs since a group of users cannot over-perform a task without having access to massive amounts of memory. However, as a typical user has free disk space, such schemes will not similarly waste a resource like energy and pollute the environment.

In this work we present an alternative to these: Proofs of Work whose work is actually useful to solving *practical problems.*

1.1 Proofs of Work

At a high level, a *Proof of Work* involves three algorithms:

- $\mathsf{Gen}(1^n)$ is a randomized algorithm that produces a *challenge* $\boldsymbol{c}$.
- $\mathsf{Solve}(\boldsymbol{c})$ is an algorithm that solves the challenge $\boldsymbol{c}$, producing a solution $\boldsymbol{s}$.
- $\mathsf{Verify}(\boldsymbol{c}, \boldsymbol{s})$ is a (possibly randomized) algorithm that verifies the solution $\boldsymbol{s}$ to $\boldsymbol{c}$.

While Gen and Verify should run very quickly, there should be a notion of *hardness* for Solve's runtime. More specifically, for some pre-specified length of working time, say $t(n)$, Solve should be able to produce solutions that Verify accepts, but any attempted solutions produced by an algorithm running in less time (e.g. $t(n)^{1-\epsilon}$ for any $\epsilon > 0$) should be rejected by Verify with high probability. Thus valid solutions 'prove' that $t(n)$ work was completed in creating them. This hardness condition should also typically be extended for so that it is also not possible to amortize work over a large number of challenges.

Stated as is, however, these "solutions" don't actually solve anything. One of the most commonly used PoWs, such as in Bitcoin, is simply to find a value $\boldsymbol{s}$ so that hashing it together with the given challenge (e.g. with SHA-256) maps to anything with a certain amount of leading 0's. Not only is hardness for this based on the *heuristic* belief that SHA-256 seems to behave unpredictably, but such an arbitrarily defined value $\boldsymbol{s}$ is useless.

1.2 The Challenge: Proofs of Useful Work

One may hope to improve over the hash-based PoW in usefulness by considering a practical problem to begin with and allowing challenges to be instances of that problem. If solutions are easily

verifiable we may believe that we have created a useful PoW scheme, but we must keep in mind that we have two goals:

1. **Hardness**: Challenges can be issued such that responding to to them correctly is (conditionally) guaranteed to necessitate actual work.
2. **Usefulness**: Computational tasks can be delegated as challenges to the workers such that the solution to the delegated task can be quickly and verifiably reconstructed from the workers' response.

Achieving a PoW scheme that simultaneously attains both desiderata for a practical problem runs into two issues then. The first is that if we delegate arbitrary instances of the practical problem to be solved, *hardness* is no longer guaranteed as easy instances may be delegated; thus, some "challenges" may not actually require work. The second issue is that if we generate the challenges randomly we not only need an average-case hardness guarantee (which do not, in general, abound) but we lose our *usefulness* in our ability to delegate chosen instances of the problem we hope to have useful solutions for.

Prior work to this has only been concerned with one of these issues at a time. Hardness is exactly captured by PoWs, which have largely forsaken usefulness except for very specific tasks, such as heuristically recycling completed PoWs to be a weak source of randomness [BCG15] or to mint coins in older cryptocurrencies [JJ99]. Usefulness, on the other hand, can be viewed through the lens of verifiable delegation of computation [Wil16, BK16, GR17] which allows useful problem instances to be delegated with quickly reconstructible solutions, yet has not been concerned with any notion of average-case hardness.

The main challenge facing a designer of a Proof of Useful Work, then, is to marry *hardness* and *usefulness* for as large as possible a class of functions f, and with as much control as possible on the hardness parameter.

1.3 Our Results

We construct a Proof of Useful Work (uPoW) scheme based on the Orthogonal Vectors (OV) problem, which is a well-studied problem that is conjectured to take $n^{2-o(1)}$ time to solve in the worst-case [Wil15]. Further, the computation invested by workers in this scheme can be used to solve the OV problem itself. Roughly, we show the following.

Informal Theorem 1. *Suppose* OV *takes* $n^{2-o(1)}$ *time to decide. Given an instance* $\boldsymbol{x}$*, it is possible to (randomly) generate a challenge* $\boldsymbol{c_x}$ *such that:*

- *A valid solution* $\boldsymbol{s}$ *to* $\boldsymbol{c_x}$ *can be computed in* $\widetilde{O}(n^2)$ *time.*
- *The validity of a candidate solution to* $\boldsymbol{c_x}$ *can be verified in* $\widetilde{O}(n)$ *time.*
- *Any valid solution to* $\boldsymbol{c_x}$ *requires* $n^{2-o(1)}$ *time to compute. (Hardness)*
- *Given a valid solution to* $\boldsymbol{c_x}$*,* OV *can be decided on the instance* $\boldsymbol{x}$ *in* $\widetilde{O}(n)$ *time. (Usefulness)*

This is formally stated as Theorem 2 in Section 3, and the corresponding construction is Protocol 2. Theorem 2 is actually much more general – it applies analogously to generalizations of OV, called k-OV, allowing us to set the gap between the time taken to generate/verify and the time required to solve challenges to n^k for any k, assuming the hardness of these generalized problems (which is further implied by the Strong Exponential Time Hypothesis). This gives us *fine-grained*

control over the hardness at the cost of having an interactive uPoW, but we show how interaction can be removed in the Random Oracle Model (Section 6).

Theorem 2 is also stronger than the above informal statement in that it says not just that any valid solution to a challenge takes $n^{2-o(1)}$ time to compute, but also that for any ℓ that is polynomial in n, finding valid solutions to a set of $\ell(n)$ independently generated challenges, possibly starting from different OV (resp. k-OV) instances, takes $(\ell(n) \cdot n^{2-o(1)})$ (resp. $(\ell(n) \cdot n^{k-o(1)})$) time. That is, *it is not possible to amortize work* over a large number of challenges - a very important feature for PoWs to have.

We prove this by proving the non-amortizability of computing a certain low-degree polynomial gOV (Definition 4) that simultaneously has the property that computing it in the worst-case immediately decides OV, and that there are efficiently verifiable certificates for its evaluations. Roughly, the uPoW scheme is structured so that the challenges are randomly generated inputs to gOV, and the solutions are evalutations of gOV at these inputs.

Informal Theorem 2. *Suppose k-OV takes $n^{k-o(1)}$ time to decide. For any polynomial ℓ, and inputs $\boldsymbol{x}_1, \ldots, \boldsymbol{x}_{\ell(n)}$ of size n that are selected independently and uniformly at random, any algorithm that computes all the $\mathsf{gOV}(\boldsymbol{x}_i)$'s correctly with probability $1/n^{o(1)}$ takes time $\ell(n) \cdot n^{k-o(1)}$.*

Note that this in particular implies a worst-case to average-case reduction from OV to gOV (similar to the one shown in [BRSV17]), though it goes further than that with non-amortizability guarantees. The above is stated formally as Theorem 3, and again this theorem is more general and applies to the generalizations of OV mentioned earlier.

1.4 The Usefulness of Our PoWs

It is important to note that, besides just OV, the problems $\mathsf{3SUM}$, All-Pairs Shortest Path (APSP) [BRSV17], and many other problems [BK16, GR17, Wil16] can also be represented as low-degree polynomials whose evaluations can be verified efficiently, and so almost immediately fit into our protocol under assumptions of their hardness. One sufficient condition for a hard problem to have the above properties is presented in [GR17], which studies doubly efficient interactive proofs for these problems (and also for the related low-degree polynomials, enabling the requisite efficient verification).

Further, any problem that quickly reduces to any of these conjectured hard problems can now also use our uPoW scheme for delegating instances of that problem. Thus we achieve *hardness* (and non-amortizability) matching the conjectured worst-case hardness of whichever of these problems we base our uPoW on, and *usefulness* for any problems reducible to them.

To this point, many types of graph problems already have been shown to quickly reduce to these problems [AL13, WW10] and, of particular interest, the task of deciding whether or not a graph has a certain property *for any property that can be written in first-order logic* is reducible to (moderate-dimension) OV [GI16]. Thus, we further achieve uPoWs based on the hardness of OV and its generalizations such that *any* problem that can be phrased as a first-order graph property can be delegated.

We then have a rich framework for uPoWs: If you have a problem that is believed to be worst-case hard for some time bound, then if you can express it as a low-degree polynomial you can likely achieve a uPoW that will be useful for that problem and has a matching time bound for the hardness of its challenges. Alternatively, if you have any practical problem at all (even if it's easy or has no believed hardness assumptions) it may still fit our framework by having a fast reduction to any existing problems that already have a uPoW.

One interesting point here is that, while many reductions to these problems so far have been to bolster belief in the hardness of these problems (as was the motivation for showing OV complete for all first-order graph properties [GI16]), this now gives an *algorithmic* motivation to reduce interesting problems to them. By reducing to OV, 3SUM, or APSP, you can now delegate Proofs of Useful Work. Finding classes of problems for which the latter three are complete for now has a new and particularly strong motivation.

Our Proofs of Useful Work, then, may be viewed as a delegation of computation scheme for an expandable class of practical problems while still maintaining their PoW properties that prevent activities such as spam and double-spending. Moreover, the work we require can be distributed across a community, similar to 'mining pools' in Bitcoin, and can be done in a manner robust to Byzantine failures and noise (cf. [BK16]) and, further, identifies where the errors of malicious community members occurred.

This lends itself nicely to applications of PoW like for blockchains. We show what modifications need to be made to our uPoWs and give a delegation scheme to outsource problems to the massive computing organism of Bitcoin in Section 7. As a final note, we show that our uPoWs can be made zero-knowledge proofs in Appendix B. While this is the opposite direction of what one may want from *usefulness*, it not only is interesting that this possible but it can also enable interesting dynamics. For example, Bitcoin workers may 'go on strike while continuing to work' by doing their uPoWs in zero-knowledge, thus continuing to maintain the blockchain and receiving bitcoins for mining blocks while also withholding their answers from the delegators.

2 Proofs of Useful Work

Proofs of useful work aim to achieve the following two desiderata simultaneously:

1. **Hardness**: Challenges can be issued such that responding to to them correctly is (conditionally) guaranteed to necessitate actual work.

2. **Usefulness**: Computational tasks can be delegated as challenges to the workers such that the solution to the delegated task can be quickly and verifiably reconstructed from the workers' response.

A Proof of Work on its own typically achieves just the *hardness* property. As mentioned in Section 1.1, a PoW has a way to quickly generate challenges of desired difficulty such that a solver is guaranteed to expend a certain amount of (non-amortizable) work in producing an easily verifiable solution.

Unfortunately, the generated challenges are typically random and detached from any fixed delegatable instance x that someone may want to learn some $f(x)$ for. Thus - on top of generating, solving, and verifying challenges - we must further generate challenges dependent on x to define a *usefulness* property: that solutions to challenges generated according to x can allow for the *reconstruction* of $f(x)$. We formalize this and give a definition of Proofs of Useful Work (uPoWs). Syntactically, the definition involves four algorithms:

- $\mathsf{Gen}(\boldsymbol{x})$ is a randomized algorithm that takes an instance $\boldsymbol{x}$ and produces a *challenge* $\boldsymbol{c_x}$.
- $\mathsf{Solve}(\boldsymbol{c_x})$ is an algorithm that solves the challenge $\boldsymbol{c_x}$, producing a solution sketch $\boldsymbol{s}$.
- $\mathsf{Verify}(\boldsymbol{c_x}, \boldsymbol{s})$ is a randomized algorithm that verifies the solution sketch $\boldsymbol{s}$ to the challenge $\boldsymbol{c_x}$.
- $\mathsf{Recon}(\boldsymbol{c_x}, \boldsymbol{s})$ is an algorithm that given a valid $\boldsymbol{s}$ for $\boldsymbol{c_x}$ reconstructs $f(\boldsymbol{x})$.

Taken together, these algorithms should result in an efficient proof system whose proofs are hard to find *and* useful. (Our hardness condition will actually be quite strong, including many arbitrary instances at once to account against amortizability. This applies to arbitrary - even easy - delegated instances).

Definition 1 (Proof of Useful Work)**.** *A $(t(n), \delta(n))$-*Proof of Useful Work (uPoW) *for f consists of four algorithms $(\mathsf{Gen}, \mathsf{Solve}, \mathsf{Verify}, \mathsf{Recon})$. The algorithms must satisfy the following properties:*

Efficiency: *For any $|x| = n$*

- *For any $\boldsymbol{x}$, $\mathsf{Gen}(\boldsymbol{x})$ runs in time $\widetilde{O}(n)$.*
- *For any $\boldsymbol{c_x} \leftarrow \mathsf{Gen}(\boldsymbol{x})$, $\mathsf{Solve}(\boldsymbol{c_x})$ runs in time $\widetilde{O}(t(n))$.*
- *For any $\boldsymbol{c_x} \leftarrow \mathsf{Gen}(\boldsymbol{x})$ and any $\boldsymbol{s}$, $\mathsf{Verify}(\boldsymbol{c_x}, \boldsymbol{s})$ runs in time $\widetilde{O}(n)$.*
- *For any $\boldsymbol{c_x} \leftarrow \mathsf{Gen}(\boldsymbol{x})$ and $\boldsymbol{s} \leftarrow \mathsf{Solve}(\boldsymbol{c_x})$, $\mathsf{Recon}(\boldsymbol{c_x}, \boldsymbol{s})$ runs in time $\widetilde{O}(n)$.*

Completeness: *For any $\boldsymbol{c_x} \leftarrow \mathsf{Gen}(\boldsymbol{x})$ and any $\boldsymbol{s} \leftarrow \mathsf{Solve}(\boldsymbol{c_x})$,*

$$\Pr\left[\mathsf{Verify}(\boldsymbol{c}, \boldsymbol{s}) = \textit{accept}\ \right] = 1$$

Where the probability is taken over Verify's randomness.

Soundness: *For any $\boldsymbol{s}$ and $\boldsymbol{c_x} \leftarrow \mathsf{Gen}(\boldsymbol{x})$ such that $\mathsf{Recon}(\boldsymbol{c_x}, \boldsymbol{s}) \neq f(x)$,*

$$\Pr\left[\mathsf{Verify}(\boldsymbol{c_x}, \boldsymbol{s}) = \textit{accept}\right] < \mathrm{neg}(n)$$

Where the probability is taken over Verify's randomness and $|x| = n$.

Hardness: *For any polynomial ℓ, any $\boldsymbol{x}_1, \ldots, \boldsymbol{x}_{\ell(n)}$ each of size n, any constant $\epsilon > 0$, and any algorithm Solve^*_ℓ that runs in time $\ell(n) \cdot t(n)^{1-\epsilon}$ when given $\ell(n)$ challenges of size n as input,*

$$\Pr\left[\forall i : \mathsf{Verify}(\boldsymbol{c}_i, \boldsymbol{s}_i) = \textit{accept} \;\middle|\; \begin{array}{l} (\boldsymbol{c}_i \leftarrow \mathsf{Gen}(\boldsymbol{x}_i))_{i \in [\ell(n)]} \\ (\boldsymbol{s}_1, \ldots, \boldsymbol{s}_{\ell(n)}) \leftarrow \mathsf{Solve}^*_\ell(\boldsymbol{c}_1, \ldots, \boldsymbol{c}_{\ell(n)}) \end{array}\right] < \delta(n)$$

Where the probability is taken over Gen and Verify's randomness.

We note that this definition implies (by combining completeness and soundness) the following notion of *usefulness*:

Usefulness: *For any $\boldsymbol{c_x} \leftarrow \mathsf{Gen}(\boldsymbol{x})$ and $\boldsymbol{s} \leftarrow \mathsf{Solve}(\boldsymbol{c_x})$, we have*

$$\mathsf{Recon}(\boldsymbol{c_x}, \boldsymbol{s}) = f(x).$$

A Proof of Useful Work, then, is a strengthening of the notions of both PoWs and (non-interactive) verifiable delegation of computation. Namely, a PoW is a uPoW that doesn't require soundness (and thus *usefulness*), and a (non-interactive) verifiable delegation of computation scheme is a uPoW that doesn't require *hardness*.

For further context, without the *hardness* and *usefulness* condition we simply have a proof system, similar to the one described in [Wil16] which proved evaluations of low-degree polynomials (*usefulness* was implicit in this work). In [BRSV17], *hardness* is added to [Wil16]'s proof system to obtain PoWs and, in [BK16, GR17], this proof system's *usefulness* is explicitly explored to obtain verifiable delegation of computation. We now provide a framework to add both *hardness* and *usefulness* simultaneously to achieve Proofs of Useful Work.

Note that, as with the proof system, all of these definitions can - and often are in the delegation of computation framework - be made interactive.

Further note of the definition that a PoW does not typically need a Recon algorithm (and that any fixed choice of x would yield a valid PoW scheme) and that delegation of computation does not typically need a Gen algorithm (or Gen can become a fixed mapping to any one of its otherwise random outputs). We also reiterate that soundness is not required for a PoW: we don't necessarily care that a solution is correct so long as it took work (guaranteed in *hardness*) to produce. However, soundness is now crucial for the delegation of computation as a way to tell that the value we reconstruct is what we wanted and not some garbage value produced by a fake solution (even if *hardness* guarantees that it took time to find the fake solution).

3 A Useful PoW for Orthogonal Vectors

In this section, we present a Proof of Useful Work (uPoW) for the Orthogonal Vectors (OV) problem and its generalization k-OV, both defined below. The properties possessed by OV that enable this construction are also shared by other problems mentioned earlier, including 3SUM and APSP as noted in [BRSV17] and also for an array of other problems [BK16, GR17, Wil16]. Consequently, while we focus on OV, uPoWs for them can be constructed along the lines of the one here. Further, these constructions would immediately provide uPoW's for other problems that reduce to OV, 3SUM, etc. in a fine-grained manner with little, if any, degradation of security. Of particular interest, deciding graph properties that are statable in first-order logic all reduce to (moderate-dimension) OV [GI16] and so we obtain uPoWs useful for *any* problem statable as a first-order graph property.

All the algorithms we consider henceforth – reductions, adversaries, etc. – are *non-uniform Word-RAM algorithms* (with words of size $O(\log n)$ where n will be clear from context) unless stated otherwise, both in our hardness assumptions and our constructions. Security against such adversaries is necessary for PoWs to remain hard in the presence of pre-processing, which is typical in the case of Bitcoin, for instance, where specialized hardware is often used. In the case of reductions, this non-uniformity is mainly used to ensure that specific parameters determined completely by instance size (such as the prime $p(n)$ in Definition 4) are known to the reductions and delegators do not need to compute them afresh for each problem they delegate.

Definition 2 (Orthogonal Vectors)**.** *The* OV *problem on vectors of dimension d (denoted OV_d) is to determine, given two sets U, V of n vectors from $\{0,1\}^{d(n)}$ each, whether there exist $u \in U$ and $v \in V$ such that $\langle u, v\rangle = 0$ (over $\mathbb{Z}$). If left unspecified, d is to be taken to be $\lceil \log^2 n \rceil$.*

OV is commonly conjectured to require $\Omega(n^{2-o(1)})$ to decide, for which many conditional fine-grained hardness results are based on [Wil15], and has been to be true if the Strong Exponential Time Hypothesis (SETH) holds [Wil05]. This hardness and the hardness of its generalization to k-OV of requiring $\Omega(n^{k-o(1)})$ time (which also holds under SETH) are what we base the hardness of our uPoWs on. We now define k-OV.

Definition 3 (k-Orthogonal Vectors)**.** *For an integer $k \geq 2$, the k-OV problem on vectors of dimension d is to determine, given k sets $(U_1, \ldots, U_k)$ of n vectors from $\{0,1\}^{d(n)}$ each, whether there exist $u^s \in U_s$ for each $s \in [k]$ such that over $\mathbb{Z}$,*

$$\sum_{\ell \in [d(n)]} u^1_\ell \cdots u^k_\ell = 0$$

We say that such a set of vectors is k-orthogonal. *As with* OV*, if left unspecified,* d *is to be taken to be* $\lceil \log^2 n \rceil$.

While these problems are conjectured worst-case hard, there are currently no wide-held beliefs for distributions that it may be average-case hard over. [BRSV17], however, defines a related problem that is shown to be average-case hard when assuming the worst-case hardness of k-OV. The average-case hard problem is that of evaluating the following polynomial:

For any prime number p, we define the polynomial $\mathsf{gOV}^k_{n,d,p} : \mathbb{F}_p^{knd} \to \mathbb{F}_p$ as follows. Its inputs are parsed in the manner that those of k-OV are – below, for any $s \in [k]$ and $i \in [n]$, u^s_i represents the i^{th} vector in U_s, and for $\ell \in [d]$, $u^s_{i\ell}$ represents its ℓ^{th} coordinate.

$$\mathsf{gOV}^k_{n,d,p}(U_1, \ldots, U_k) = \sum_{i_1,\ldots,i_k \in [n]} \prod_{\ell \in [d]} \left(1 - u^1_{i_1 \ell} \cdots u^k_{i_k \ell}\right)$$

Note that the degree of this polynomial is kd. When given an instance of k-OV (from $\{0,1\}^{knd}$) as input, $\mathsf{gOV}^k_{n,d,p}$ counts the number of tuples of k-orthogonal vectors (modulo p).

For small d (e.g. $d = \lceil \log^2 n \rceil$), this is a fairly low-degree polynomial. The following definition gives the family of such polynomials parameterized by input size. This family was shown to be hard to compute on uniformly random inputs if k-OV is hard in the worst-case [BRSV17].

Definition 4 (GOV^k)**.** *Consider an integer* $k \geq 2$*. Let* $p(n)$ *be the smallest prime number larger than* $n^{\log n}$*, and* $d(n) = \lceil \log^2 n \rceil$*.* GOV^k *is the family of functions* $\left\{\mathsf{gOV}^k_{n,d(n),p(n)}\right\}$.

Remark 3.1. We note that most of our results would hold for a much smaller choice of $p(n)$ above – anything larger than n^k would do. The reason we choose p to be this large is to achieve negligible soundness error in interactive protocols we shall be designing for this family of functions (see Protocol 1). Another way to achieve this is to use large enough extension fields of $\mathbb{F}_p$ for smaller p's; this is in fact preferable as the value of $p(n)$ as defined now is much harder to compute for uniform algorithms.

While, assuming k-OV takes $\Omega(n^{k-o(1)})$ time in the worst-case implies that evaluating polynomials in GOV on points is just as hard, even on average, it is still easily delegate the evaluation of such points.

3.1 Preliminary Protocols

We describe here a protocol (Protocol 1) that proves the evaluation of polynomials in GOV on points (and can even delegate that evaluation) that will be used as a sub-routine in our final uPoW protocol, and which will also find use in proving its security. This protocol is an (k-1)-round interactive proof that, given $U_1, \ldots, U_k \in \mathbb{F}_p^{nd}$ and $y \in \mathbb{F}_p$, proves that $\mathsf{gOV}^k_{n,d,p}(U_1, \ldots, U_k) = y$.

The special case of $k = 2$ for OV was shown as a non-interactive (MA) protocol in [Wil16] and this was used to create PoWs based on OV, 3SUM, and APSP in [BRSV17], however with randomly generated challenges that were not *useful*. The following interactive proof is essentially the sum-check protocol, but in our case we need to pay close attention to the complexity of the prover and the verifier and so use ideas from [Wil16].

We will set up the following definitions before describing the protocol. For each $s \in [k]$, consider the univariate polynomials $\phi^s_1, \ldots, \phi^s_d : \mathbb{F}_p \to \mathbb{F}_p$, where ϕ^s_ℓ represents the ℓ^{th} column of U_s – that

is, for $i \in [n]$, $\phi^s_\ell(i) = u^s_{i\ell}$. Each such ϕ^s_ℓ has degree at most $(n-1)$. $\mathsf{gOV}^k_{n,d,p}$ can now be written as:

$$\begin{aligned}\mathsf{gOV}^k_{n,d,p}(U_1,\ldots,U_k) &= \sum_{i_1,\ldots,i_k\in[n]} \prod_{\ell\in[d]} \left(1 - u^1_{i_1\ell}\cdots u^k_{i_k\ell}\right) \\ &= \sum_{i_1,\ldots,i_k\in[n]} \prod_{\ell\in[d]} \left(1 - \phi^1_\ell(i_1)\cdots \phi^k_\ell(i_k)\right) \\ &= \sum_{i_1,\ldots,i_k\in[n]} q(i_1,\ldots,i_k)\end{aligned}$$

where q is defined for convenience as:

$$q(i_1,\ldots,i_k) = \prod_{\ell\in[d]} \left(1 - \phi^1_\ell(i_1)\cdots \phi^k_\ell(i_k)\right)$$

The degree of q is at most $D = k(n-1)d$. Note q can be evaluated at any point in $\mathbb{F}_p^k$ in time $\widetilde{O}(knd\log p)$, by evaluating all the $\phi^s_\ell(i_s)$'s, computing each term in the above product and then multiplying them.

For any $s \in [k]$ and $\alpha_1,\ldots,\alpha_{s-1} \in \mathbb{F}_p$, define the following univariate polynomial:

$$q_{s,\alpha_1,\ldots,\alpha_{s-1}}(x) = \sum_{i_{s+1},\ldots,i_k\in[n]} q(\alpha_1,\ldots,\alpha_{s-1},x,i_{s+1},\ldots,i_k)$$

Every such q_s has degree at most $(n-1)d$ – this can be seen by inspecting the definition of q. With these definitions, the interactive proof is described as Protocol 1 below. The completeness and soundness of this interactive proof is asserted by Theorem 1, which is proven in Section 4.

Interactive Proof for GOV^k:

- The prover sends the co-efficients of a univariate polynomial q_1^* of degree at most $(n-1)d$.
- The verifier checks that $\sum_{i_1\in[n]} q_1^*(i_1) = y$. If not, it rejects.
- For s from 1 up to $k-2$:
  - The verifier sends a random $\alpha_s \leftarrow \mathbb{F}_p$.
  - The prover sends the co-efficients of a polynomial $q^*_{s+1,\alpha_1,\ldots,\alpha_s}$ of degree at most $(n-1)d$.
  - The verifier checks that $\sum_{i_{s+1}\in[n]} q^*_{s+1,\alpha_1,\ldots,\alpha_s}(i_{s+1}) = q^*_{s,\alpha_1,\ldots,\alpha_{s-1}}(\alpha_s)$. If not, it rejects.
- The verifier picks $\alpha_{k-1} \leftarrow \mathbb{F}_p$ and checks that $q^*_{k-1,\alpha_1,\ldots,\alpha_{k-2}}(\alpha_{k-1}) = q_{k-1,\alpha_1,\ldots,\alpha_{k-2}}(\alpha_{k-1})$, which it computes using the fact that $q_{k-1,\alpha_1,\ldots,\alpha_{k-2}}(\alpha_{k-1}) = \sum_{i_k\in[n]} q_{k,\alpha_1,\ldots,\alpha_{k-1}}(i_k)$. If not, it rejects.
- If the verifier hasn't rejected yet, it accepts.

Protocol 1: Interactive Proof for GOV^k.

For this protocol we have the following guarantee. We will prove this in Section 4.

Theorem 1. *For any $k \geq 2$, let d and p be as in Definition 4. Protocol 1 is a $(k-1)$-round interactive proof for proving that $y = \mathsf{GOV}^k(x)$. This protocol has perfect completeness and soundness error at most $\left(\frac{knd}{p}\right)$. The prover runs in time $\widetilde{O}(n^k d \log p)$, and the verifier in time $\widetilde{O}(knd^2 \log p)$.*

As observed earlier, Protocol 1 is non-interactive when $k = 2$. We then get the following corollary for GOV.

Corollary 1. *For $k = 2$, let d and p be as in Definition 4. Protocol 1 is an MA proof for proving that $y = \mathsf{GOV}(x)$. This protocol has perfect completeness and soundness error at most $\left(\frac{2nd}{p}\right)$. The prover runs in time $\widetilde{O}(n^2)$, and the verifier in time $\widetilde{O}(n)$.*

We now currently have a proof system with completeness and soundness along with efficiency bounds on the prover and verifier. In the framework of uPoWs in Section 2, we still need a way to have *hardness* and *usefulness* to extend this proof system to a uPoW in some form.

3.2 The uPoW Protocol

We now present Protocol 2, which we show to be a Proof of Useful Work for k-OV.

Proof of Useful Work for k-OV:

- $\mathsf{Gen}(\boldsymbol{x})$:
  - Given an instance $\boldsymbol{x} \in \{0,1\}^{knd}$, interpret $\boldsymbol{x}$ as an element of $\mathbb{F}_p^{knd}$ (where $p = p(n)$ is as in Definition 4).
  - Pick a random $\boldsymbol{r} \in \mathbb{F}_p^{knd}$.
  - Output the set of vectors $\boldsymbol{c_x} = \{\boldsymbol{y}_t = \boldsymbol{x} + t\boldsymbol{r} \mid t \in [kd+1]\}$.
- $(\mathsf{Solve}, \mathsf{Verify})$ work as follows given $\boldsymbol{c_x} = \{\boldsymbol{y}_t\}$:
  - Solve computes $z_t = \mathsf{gOV}^k_{n,d,p}(\boldsymbol{y}_t)$ and outputs the set $\boldsymbol{s} = \{z_t\}_{t \in [kd+1]}$.
  - For each t in parallel: Solve and Verify run Protocol 1 with input $(\boldsymbol{y}_t, z_t)$.
  - Verify accepts iff all of the above instances of Protocol 1 accept.
- $\mathsf{Recon}(\boldsymbol{c_x}, \boldsymbol{s})$:
  - Interpret $z_1, \ldots, z_{kd+1}$ as the evaluations of a univariate polynomial $h(t)$ of degree kd at $t = 1, \ldots, kd+1$.
  - Interpolate to find the coefficients of h and compute $z = h(0)$.
  - If $z \neq 0$, output 1, else 0 as the answer to the k-OV instance.

Protocol 2: Proof of Useful Work for k-OV.

Theorem 2. *For any $k \geq 2$, suppose k-OV takes $n^{k-o(1)}$ time to decide for any $d = \omega(\log n)$. Then, Protocol 2 is an (n^k, δ)-Proof of Useful Work for k-OV for any function $\delta(n) > 1/n^{o(1)}$.*

Remark 3.2. As is, this will be an interactive uPoW. In the special case of $k = 2$, Corollary 1 gives us that we have a regular non-interactive uPoW. If we want to remove interaction for general k-OV, however, we could use the MA proof in [Wil16] at cost of verification and reconstruction

taking time $\widetilde{O}(n^{k/2})$. To keep verification and reconstruction time at $\widetilde{O}(n)$, we instead show how to remove interaction in the Random Oracle model in Section 6.

We will use Theorem 1 to argue for the completeness and soundness of Protocol 2. In order to prove the hardness, we will need lower bounds on how well the problem that Solve is required to solve can be amortized. We first define what it means for a function to be non-amortizable in the average-case in a manner compatible with the hardness requirement. Note that this requirement is stronger than being non-amortizable in the worst-case.

Definition 5. *Consider a function family $\mathcal{G} = \{g_n : \mathcal{X}_n \to \mathcal{Y}_n\}$, and a family of distributions $\mathcal{D} = \{D_n\}$, where D_n is over $\mathcal{X}_n$. $\mathcal{G}$ is* not *(ℓ, t, δ)*-amortizable on average over $\mathcal{D}$ *if, for any algorithm* Amort *that runs in time $\ell(n)t(n)$ when run on $\ell(n)$ inputs from $\mathcal{X}_n$, when it is given as input $\ell(n)$ independent samples from D_n,*

$$\Pr_{x_i \leftarrow D_n}\left[\mathsf{Amort}(x_1, \ldots, x_{\ell(n)}) = (g_n(x_1), \ldots, g_n(x_{\ell(n)}))\right] < \delta(n)$$

We will be concerned with the case where the amortized time $t(n)$ is less than the time it takes to compute f_n on a single instance. Theorem 3, then, claims that we achieve this non-amortizability and will let us prove the desired hardness of Protocol 2, as GOV^k is one of the things that Solve is required to compute there. We prove this theorem in Appendix A, and prove a weaker version for illustrative purposes in Section 5.

Theorem 3. *For any $k \geq 2$, suppose k-OV takes $n^{k-o(1)}$ time to decide for any $d = \omega(\log n)$. Then, for any constants $c, \epsilon > 0$ and $\delta < \epsilon/2$, GOV^k is* not *$(n^c, n^{k-\epsilon}, 1/n^\delta)$-amortizable on average over the uniform distribution over its inputs.*

We now put all the above together to prove Theorem 2 as follows.

Proof of Theorem 2. We prove that Protocol 2 satisfies the various requirements demanded of a Proof of Useful Work for k-OV in turn.

Efficiency is argued as follows:

- $\mathsf{Gen}(\boldsymbol{x})$ simply computes $(kd+1)$ linear combinations over $\mathbb{F}^{knd}$ to create all the elements of $\boldsymbol{c_x}$ and so takes the time of $O(kd)$ basic operations on $\mathbb{F}^{knd}$. As $d = \log^2 n$ and $p \leq 2n^{\log n}$ by Chebyshev's Theorem, this takes $\widetilde{O}(n)$ time.
- Solve computes $\mathsf{gOV}^k_{n,d,p}(\boldsymbol{y}_t)$ on $(kd+1)$ values of $\boldsymbol{y}_t$, each of which can be done in $\widetilde{O}(n^k)$ time. It then runs the prover in $(kd+1)$ instantiations of Protocol 1, each of which can be done in $\widetilde{O}(n^k)$ time by Theorem 1. So in all it takes takes $\widetilde{O}(n^k(kd+1)) = \widetilde{O}(n^k)$ time.
- Verify runs the verifier in $(kd+1)$ instantiations of Protocol 1, taking a total of $\widetilde{O}(n(kd+1)) = \widetilde{O}(n)$ time, again by Theorem 1.
- Recon does interpolation and evaluation of a univariate polynomial of degree kd over $\mathbb{F}_p$, which can be done in time $\widetilde{O}((kd)^2)$, which is much less than n.

Usefulness. Define the univariate polynomial $h_{\boldsymbol{x},\boldsymbol{r}}$ as $h_{\boldsymbol{x},\boldsymbol{r}}(t) = \mathsf{gOV}^k_{n,d,p}(\boldsymbol{x} + t\boldsymbol{r})$. Note that the degree of $h_{\boldsymbol{x},\boldsymbol{r}}$ is at most the degree of $\mathsf{gOV}^k_{n,d,p}$, which is kd. When Solve produces the correct evaluations $z_1, \ldots, z_{kd+1}$ of $\mathsf{gOV}^k_{n,d,p}$ at $(\boldsymbol{x}+\boldsymbol{r}), \ldots, (\boldsymbol{x}+(kd+1)\boldsymbol{r})$, these are also evaluations of $h_{\boldsymbol{x},\boldsymbol{r}}$ at $1, \ldots, (kd+1)$. So when Recon in Protocol 2 interpolates to find a polynomial, what it finds is $h_{\boldsymbol{x},\boldsymbol{r}}$, and its evaluation at 0 is $\mathsf{gOV}^k_{n,d,p}(\boldsymbol{x})$. As p is large enough, this value counts the number of k-orthogonal vectors in the k-OV instance $\boldsymbol{x} \in \{0,1\}^{knd}$. So $\boldsymbol{x}$ has k-orthgonal vectors iff this value is non-zero.

Completeness follows immediately from the completeness of Protocol 1 as an interactive proof for GOV^k, as stated in Theorem 1, as this is the protocol that Solve and Verify engage in. **Soundness** follows from the soundness of Protocol 1 and the correctness of Recon as argued above.

Hardness. We proceed by contradiction. On a high level, we will assume that there is in fact a set of instances that yield easy (amortizable) challenges on average and show that, given these instances as non-uniform advice, we can break GOV^k's average-case hardness:

Suppose there is an (interactive) algorithm Solve^*, a polynomial ℓ, a set of k-OV instances $\boldsymbol{x}_1, \ldots, \boldsymbol{x}_{\ell(n)} \in \{0,1\}^{knd}$, and an $\epsilon > 0$ such that Solve^* runs in time $\ell(n)n^{k-\epsilon}$ and makes Verify accept on all these instances with probability at least $\delta(n)$ that is $1/n^{o(1)}$. Let the gOV instances produced by $\mathsf{Gen}(\boldsymbol{x}_i)$ be $\left\{\boldsymbol{y}_t^i\right\}$, and the corresponding sets $\boldsymbol{s}_i$ produced by Solve^* be $\left\{z_t^i\right\}$. So Solve^* succeeds as a prover in Protocol 1 for *all* the instances $\left\{(\boldsymbol{y}_t^i, z_t^i)\right\}$ with probability at least $\delta(n)$.

By the negligible soundness of Protocol 1 guaranteed by Theorem 1, in order to do this, Solve^* has to use the correct values $\mathsf{gOV}^k_{n,d,p}(\boldsymbol{y}_t^i)$ for all z_t^i's with probability negligibly close to $\delta(n)$ and definitely more than, say, $\delta(n)/2$. In particular, with this probability, it has to explicitly compute $\mathsf{gOV}^k_{n,d,p}$ at $\boldsymbol{y}_1^1, \ldots, \boldsymbol{y}_1^{\ell(n)}$, all of which are independent uniform points in $\mathbb{F}_p^{knd}$.

Such a Solve^* can now be used as follows to compute $\mathsf{gOV}^k_{n,d,p}$ on any independently random $\boldsymbol{y}_1, \ldots, \boldsymbol{y}_{\ell(n)} \in \mathbb{F}_p^{knd}$ as follows. Take the points $\boldsymbol{x}_1, \ldots, \boldsymbol{x}_{\ell(n)}$ (on which Solve^* succeeds as above) as non-uniform advice. Now for each $i \in [\ell(n)]$, take $\boldsymbol{y}_1$ to be $\hat{\boldsymbol{y}}_1^i$, and generate the other $\hat{\boldsymbol{y}}_t^i$'s as the next kd points on the line joining $\boldsymbol{x}_i$ and $\boldsymbol{y}_i$. This set $\left\{\hat{\boldsymbol{y}}_t^i\right\}$ is distributed identically to $\left\{\boldsymbol{y}_t^i\right\}$ above, and so Solve^* computes $\mathsf{gOV}^k_{n,d,p}$ on all of these correctly with probability greater than $\delta(n)/2$.

Thus Solve^* can be used to construct a non-uniform algorithm that runs in time $\ell(n)n^{k-\epsilon}$ and computes $\mathsf{gOV}^k_{n,d,p}$ correctly on all of $\boldsymbol{y}_1, \ldots, \boldsymbol{y}_{\ell(n)}$ with probability at least $\delta(n)/2$ ($>> 1/n^{\epsilon/2}$) when all of these are distributed independently and uniformly. But this is exactly what Theorem 3 says is impossible. So such a Solve^* cannot exist, and this proves the hardness of Protocol 2.

We have thus proven all the properties necessary and hence Protocol 2 is indeed an (n^k, δ)-Proof of Useful Work for k-OV for any $\delta(n) > 1/n^{o(1)}$. □

4 Verifying GOV^k

In this section, we prove Theorem 1 (stated in Section 3), which is about Protocol 1 being a valid interactive proof for proving evaluations of GOV^k. We use here terminology from the theorem statement and protocol description. Recall the the input to the protocol is $U_1, \ldots, U_k \in \mathbb{F}_p^{nd}$ and $y \in \mathbb{F}_p$, and the prover wishes to prove that $y = \mathsf{gOV}^k_{n,d,p}(U_1, \ldots, U_k)$.

Completeness. If indeed $y = \mathsf{gOV}^k_{n,d,p}(U_1, \ldots, U_k)$, the prover can make the verifier in the protocol accept by using the polynomials $(q_1, q_{2,\alpha_1}, \ldots, q_{k,\alpha_1,\ldots,\alpha_k})$ in place of $(q_1^*, q_{2,\alpha_1}^*, \ldots, q_{k,\alpha_1,\ldots,\alpha_k}^*)$. Perfect completeness is then seen to follow from the definitions of these polynomials and their relation to q and hence $\mathsf{gOV}^k_{n,d,p}$.

Soundness. Suppose $y \neq \mathsf{gOV}^k_{n,d,p}(U_1, \ldots, U_k)$. We now analyze the probability with which a cheating prover could make the verifier accept.

To start with, note that the prover's q_1^* has to be different from q_1, as otherwise the check in the second step would fail. Further, as the degree of these polynomials is less than nd, the probability that the verifier will then choose an α_1 such that $q_1^*(\alpha_1) = q_1(\alpha_1)$ is less than $\frac{nd}{p}$.

If this event does not happen, then the prover has to again send a q^*_{2,α_1} that is different from q_{2,α_1}, which again agree on α_2 with probability less than $\frac{nd}{p}$. This goes on for $(k-1)$ rounds, at the end of which the verifier checks whether $q^*_{k-1}(\alpha_{k-1})$ is equal to $q_{k-1}(\alpha_{k-1})$, which it computes by itself. If at least one of these accidental equalities at a random point has not occurred throughout the protocol, the verifier will reject. The probability that at least one of these happens over the $(k-1)$ rounds is, by the union bound, less than $\frac{knd}{p}$.

Efficiency. Next we discuss details of how the honest prover and the verifier are implemented, and analyze their complexities. To this end, we will need the following algorithmic results about computations involving univariate polynomials over finite fields.

Lemma 1 (Fast Multi-point Evaluation [Fid72])**.** *Given the co-efficients of a univariate polynomial $q : \mathbb{F}_p \to \mathbb{F}_p$ of degree at most N, and N points $x_1, \ldots, x_N \in \mathbb{F}_p$, the set of evaluations $(q(x_1), \ldots, q(x_N))$ can be computed in time $O(N \log^3 N \log p)$.*

Lemma 2 (Fast Interpolation [Hor72])**.** *Given $D+1$ evaluations of a univariate polynomial $q : \mathbb{F}_p \to \mathbb{F}_p$ of degree at most D, the co-efficients of q can be computed in time $O(D \log^3 D \log p)$.*

To start with, both the prover and verifier compute the co-efficients of all the ϕ^s_ℓ's. Note that, by definition, they know the evaluation of each ϕ^s_ℓ on n points, given by $\{(i, u^s_{i\ell})\}_{i\in[n]}$. This can be used to compute the co-efficients of each ϕ^s_ℓ in time $\widetilde{O}(n \log p)$ by Lemma 2. The total time taken is hence $\widetilde{O}(knd \log p)$.

The proof of the following proposition specifies further details of the prover's workings.

Proposition 1. *The co-efficients of the polynomial $q_{s,\alpha_1,\ldots,\alpha_{s-1}}$ can be computed in time $\widetilde{O}((n^{k-s+1}d + nd^2) \log p)$ given the above preprocessing.*

- Fix some value of $s, \alpha_1, \ldots, \alpha_{s-1}$.
- For each $\ell \in [d]$, compute the evaluation of ϕ^s_ℓ on nd points, say $\{1, \ldots, nd\}$.
  - Since its co-efficients are known, the evaluations of each ϕ^s_ℓ on these nd points can be computed in time $\widetilde{O}(nd \log p)$ by Lemma 1, for a total of $\widetilde{O}(nd^2 \log p)$ for all the ϕ^s_ℓ's.
- For each setting of $i_{s+1}, \ldots, i_k$, compute the evaluations of the polynomial $\rho_{i_{s+1},\ldots,i_k}(x) = q(\alpha_1, \ldots, \alpha_{s-1}, x, i_{s+1}, \ldots, i_k)$, on the points $\{1, \ldots, nd\}$.
  - First substitute the constants $\alpha_1, \ldots, \alpha_{s-1}, i_{s+1}, \ldots, i_k$ into the definition of q.
  - This requires computing, for each $\ell \in [d]$ and $s' \in [k] \setminus \{s\}$, either $\phi^{s'}_\ell(\alpha_s)$ or $\phi^{s'}_\ell(i_s)$. All of this can be done in time $\widetilde{O}(knd \log p)$ by direct polynomial evaluations since the co-efficients of the $\phi^{s'}_\ell$'s are known.
  - This reduces q to a product of d univariate polynomials of degree less than n, whose evaluations on the nd points can now be computed in time $\widetilde{O}(knd \log p)$ by multiplying the constants computed in the above step with the evaluations of $\phi^{s'}_\ell$ on these points, and subtracting from 1.
  - The product of the evaluations can now be computed in time $\widetilde{O}(nd^2 \log p)$ to get what we need.
- Add up the evaluations of $\rho_{i_{s+1},\ldots,i_k}$ pointwise over all settings of $(i_{s+1}, \ldots, i_k)$.
  - There are n^{k-s} possible settings of $(i_{s+1}, \ldots, i_k)$, and for each of these we have nd evaluations. All the additions hence take $\widetilde{O}(n^{k-s+1}d \log p)$ time.

- This gives us nd evaluations of $q_{s,\alpha_1,\ldots,\alpha_{s-1}}$, which is a univariate polynomial of degree at most $(n-1)d$. So its coefficients can be computed in time $\widetilde{O}(nd \log p)$ by Lemma 2.
- It can be verified from the intermediate complexity computations above that all these operations together take $\widetilde{O}((n^{k-s+1}d + nd^2) \log p)$ time. This proves the proposition.

Recall that what the honest prover has to do is compute $q_1, q_{2,\alpha_1}, \ldots, q_{k,\alpha_1,\ldots,\alpha_{k-1}}$ for the α_s's specified by the verifier. By the above proposition, along with the preprocessing, the total time the prover takes is:

$$\widetilde{O}(knd \log p + (n^k d + nd^2) \log p) = \widetilde{O}(n^k d \log p)$$

The verifier's checks in steps (2) and (3) can each be done in time $\widetilde{O}(n \log p)$ using Lemma 1. Step (4) can be done by using the above proposition with $s = k$ in time $\widetilde{O}(nd^2 \log p)$. Even along with the preprocessing, this leads to a total time of $\widetilde{O}(knd^2 \log p)$.

5 Non-Amortizability of GOV

In this section we prove the following weaker version of Theorem 3, which itself is proven in Appendix A using an extension of the techniques employed here. The notion of non-amortizatbility used below is defined in Definition 5 in Section 3.

Theorem 4. *For any $k \geq 2$, suppose k-OV takes $n^{k-o(1)}$ time to decide for any $d = \omega(\log n)$. Then, for any constants $c, \epsilon > 0$, GOV^k is* not *$(n^c, n^{k-\epsilon}, 7/8)$-amortizable on average over the uniform distribution over its inputs.*

Throughout this section, $\mathcal{F}$, $\mathcal{F}'$ and $\mathcal{G}$ are families of functions $\{f_n : \mathcal{X}_n \to \mathcal{Y}_n\}$, $\{f'_n : \mathcal{X}'_n \to \mathcal{Y}'_n\}$ and $\left\{g_n : \hat{\mathcal{X}}_n \to \hat{\mathcal{Y}}_n\right\}$, and $\mathcal{D} = \{D_n\}$ is a family of distributions where D_n is over $\hat{\mathcal{X}}_n$. s, ℓ, t, by themselves or with various subscripts, are all functions from $\mathbb{N} \to \mathbb{N}$. All algorithms are to be taken to be randomised by default.

Theorem 4 is the result of two properties possessed by GOV^k. We define these properties below, prove a more general lemma about functions that have these properties, and use it to prove this theorem.

Definition 6. *$\mathcal{F}$ is said to be* (s, ℓ)-downward reducible *to $\mathcal{F}'$ in time t if there is a pair of algorithms* $(\mathsf{Split}, \mathsf{Merge})$ *satisfying:*

- *For all large enough n, $s(n) < n$.*
- Split *on input an $x \in \mathcal{X}_n$ outputs $\ell(n)$ instances from $\mathcal{X}'_{s(n)}$.*

$$\mathsf{Split}(x) = (x_1, \ldots, x_{\ell(n)})$$

- *Given the value of $\mathcal{F}'$ at these $\ell(n)$ instances,* Merge *can reconstruct the value of $\mathcal{F}$ at x.*

$$\mathsf{Merge}(x, f'_{s(n)}(x_1), \ldots, f'_{s(n)}(x_{\ell(n)})) = f_n(x)$$

- Split *and* Merge *together run in time at most $t(n)$.*

If $\mathcal{F}'$ is the same as $\mathcal{F}$, then $\mathcal{F}$ is said to be downward self-reducible.

Definition 7. *$\mathcal{F}$ is said to be* ℓ-robustly reducible *to $\mathcal{G}$ in time t if there is a pair of algorithms* $(\mathsf{Split}, \mathsf{Merge})$ *satisfying:*

- Split *on input an $x \in \mathcal{X}_n$ (and randomness r) outputs $\ell(n)$ instances from $\hat{\mathcal{X}}_n$.*

$$\mathsf{Split}(x; r) = (x_1, \ldots, x_{\ell(n)})$$

- *For such a tuple $(x_i)_{i\in[\ell(n)]}$ and any function g^* such that $g^*(x_i) = g_n(x_i)$ for at least $2/3$ of the x_i's,* Merge *can reconstruct the function value at x as:*

$$\mathsf{Merge}(x, r, g^*(x_1), \ldots, g^*(x_{\ell(n)})) = f_n(x)$$

- Split *and* Merge *together run in time at most $t(n)$.*
- *Each x_i is distributed according to D_n, and the x_i's are pairwise independent.*

The above is a more stringent notion than the related non-adaptive random self-reducibility as defined in [FF93]. We remark that to prove what we need it would have been sufficient if, in the above definition, the reconstruction above had worked for most r's (and not necessarily all r's), but we leave it as it is for simplicity of presentation.

Lemma 3. *Suppose $\mathcal{F}$, $\mathcal{F}'$ and $\mathcal{G}$ have the following properties:*

- *$\mathcal{F}$ is (s_d, ℓ_d)-downward reducible to $\mathcal{F}'$ in time t_d.*
- *$\mathcal{F}'$ is ℓ_r-robustly reducible to $\mathcal{G}$ over $\mathcal{D}$ in time t_r.*
- *$\mathcal{G}$ is $(\ell_a, t_a, 7/8)$-amortizable on average over $\mathcal{D}$, and $\ell_a(s_d(n)) = \ell_d(n)$.*

Then $\mathcal{F}$ can be computed in the worst-case in time:

$$t_d(n) + \ell_d(n)t_r(s_d(n)) + \ell_r(s_d(n))\ell_d(n)t_a(s_d(n))$$

The condition $\ell_a(s_d(n)) = \ell_d(n)$ above can be relaxed to $\ell_a(s_d(n)) \leq \ell_d(n)$ at the expense of a factor of 2 in the worst-case running time obtained for $\mathcal{F}$, but we leave it this way again for simplicity of presentation. We now show how to prove Theorem 4 using Lemma 3, and then prove the lemma itself.

Proof of Theorem 4. Fix any $k \geq 2$. Suppose, towards a contradiction, that for some $c, \epsilon > 0$, GOV^k is $(n^c, n^{k-\epsilon}, 7/8)$-amortizable on average over the uniform distribution. In our arguments we will refer to the following function families:

- $\mathcal{F}$ is k-OV with vectors of dimension $d = \left(\frac{k}{k+c}\right)^2 \log^2 n$.
- $\mathcal{F}'$ is k-OV with vectors of dimension $\log^2 n$.
- $\mathcal{G}$ is GOV^k (over $\mathbb{F}_p^{knd}$ for some p that definitely satisfies $p > n$).

Let $m = n^{k/(k+c)}$. Note the following two properties :

- $\frac{n}{m^{c/k}} = m$
- $d = \left(\frac{k}{k+c}\right)^2 \log^2 n = \log^2 m$

We now establish the following relationships among the above function families.

Proposition 2. *$\mathcal{F}$ is (m, m^c)-downward reducible to $\mathcal{F}'$ in time $\widetilde{O}(m^{c+1})$.*

Split_d, when given an instance $(U_1, \ldots, U_k) \in \{0,1\}^{k(n\times d)}$, first divides each U_i into $m^{c/k}$ partitions $U_{i1}, \ldots, U_{im^{c/k}} \in \{0,1\}^{m\times d}$. It then outputs the set of tuples $\{(U_{1j_1}, \ldots, U_{kj_k}) \mid j_i \in [m^{c/k}]\}$. Each U_{ij} is in $\{0,1\}^{m\times d}$ and, as noted earlier, $d = \log^2 m$. So each tuple in the set is indeed an instance of $\mathcal{F}'$ of size m. Further, there are $(m^{c/k})^c = m^c$ of these.

Note that the original instance has a set of k-orthogonal vectors if and only if at least one of the m^c smaller instances produced does. So Merge_d simply computes the disjunction of the $\mathcal{F}'$ outputs to these instances.

Both of these can be done in time $O(m^c \cdot k \cdot md + m^c) = \widetilde{O}(m^{c+1})$.

Proposition 3. *$\mathcal{F}'$ is $12kd$-robustly reducible to $\mathcal{G}$ over the uniform distribution in time $\widetilde{O}(m)$.*

Notice that for any $U_1, \ldots, U_k \in \{0,1\}^{m\times d}$, we have that $k\text{-}\mathsf{OV}(U_1, \ldots, U_k) = \mathsf{gOV}^k_m(U_1, \ldots, U_k)$. So it is sufficient to show such a robust reduction from $\mathcal{G}$ to itself. We do this now.

Given an input $\boldsymbol{x} \in \mathbb{F}_p^{knd}$, Split_r picks two uniformly random $\boldsymbol{x}_1, \boldsymbol{x}_2 \in \mathbb{F}_p^{knd}$ and outputs the set of vectors $\{\boldsymbol{x} + t\boldsymbol{x}_1 + t^2\boldsymbol{x}_2 \mid t \in \{1, \ldots, 12kd\}\}$. Recall that our choice of p is much larger than $12kd$ and hence this is possible. The distribution of each of these vectors is uniform over $\mathbb{F}_p^{knd}$, and they are also pairwise independent as they are points on a random quadratic curve through $\boldsymbol{x}$.

Define the univariate polynomial $g_{\boldsymbol{x},\boldsymbol{x}_1,\boldsymbol{x}_2}(t) = \mathsf{gOV}^k_m(\boldsymbol{x} + t\boldsymbol{x}_1 + t^2\boldsymbol{x}_2)$. Note that its degree is at most $2kd$. When Merge_r is given $(y_1, \ldots, y_{12kd})$ that are purported to be the evaluations of gOV^k_m on the points produced by Split, these can be seen as purported evaluations of $g_{\boldsymbol{x},\boldsymbol{x}_1,\boldsymbol{x}_2}$ on $\{1, \ldots, 12kd\}$. This can, in turn, be treated as a corrupt codeword of a Reed-Solomon code, which under these parameters has distance $10kd$.

The Berlekamp-Welch algorithm can be used to decode any codeword that has at most $5kd$ corruptions, and if at least $2/3$ of the evaluations are correct, then at most $4kd$ evaluations are wrong. Hence Merge_r uses the Berlekamp-Welch algorithm to recover $g_{\boldsymbol{x},\boldsymbol{x}_1,\boldsymbol{x}_2}$, which can be evaluated at 0 to obtain $\mathsf{gOV}^k_n(\boldsymbol{x})$.

Split_r takes $\widetilde{O}(12kd \cdot kmd) = \widetilde{O}(m)$ time to compute all the vectors it outputs. Merge_r takes $\widetilde{O}((12kd)^3)$ time to run Berlekamp-Welch, and $\widetilde{O}(12kd)$ time to evaluate the resulting polynomial at 0. So in all both algorithms take $\widetilde{O}(m)$ time.

By our assumption at the beginning, $\mathcal{G}$ is $(n^c, n^{k-\epsilon}, 7/8)$-amortizable on average over the uniform distribution. Together with the above propositions, this satisfies all the requirements in the hypothesis of Lemma 3, which now tells us that $\mathcal{F}$ can be computed in the worst-case in time:

$$\begin{aligned}\widetilde{O}(m^{c+1} + m^c \cdot m + 12kd \cdot m^c \cdot m^{k-\epsilon}) &= \widetilde{O}(m^{c+1} + m^{c+k-\epsilon}) \\ &= \widetilde{O}(n^{k(c+1)/(k+c)} + n^{k(k+c-\epsilon)/(k+c)}) \\ &= \widetilde{O}(n^{k-\epsilon'})\end{aligned}$$

for some $\epsilon' > 0$. But this is what the hypothesis of the theorem says is not possible. So GOV^k cannot be $(n^c, n^{k-\epsilon}, 7/8)$-amortizable on average, and this argument applies for any $c, \epsilon > 0$. □

Proof of Lemma 3. Given the hypothesised downward reduction $(\mathsf{Split}_d, \mathsf{Merge}_d)$, robust reduction $(\mathsf{Split}_r, \mathsf{Merge}_r)$ and amortization algorithm Amort for $\mathcal{F}$, f_n can be computed as follows (for large enough n) on an input $x \in \mathcal{X}_n$:

- Run $\mathsf{Split}_d(x)$ to get $x_1, \ldots, x_{\ell_d(n)} \in \mathcal{X}'_{s_d(n)}$.
- For each $i \in [\ell_d(n)]$, run $\mathsf{Split}_r(x_i; r_i)$ to get $x_{i1}, \ldots, x_{i\ell_r(s_d(n))} \in \hat{\mathcal{X}}_{s_d(n)}$.

- For each $j \in [\ell_r(s_d(n))]$, run $\mathsf{Amort}(x_{1j}, \ldots, x_{\ell_d(n)j})$ to get the outputs $y_{1j}, \ldots, y_{\ell_d(n)j} \in \hat{\mathcal{Y}}_{s_d(n)}$.
- For each $i \in [\ell_d(n)]$, run $\mathsf{Merge}_r(x_i, r_i, y_{i1}, \ldots, y_{i\ell_r(s_d(n))})$ to get $y_i \in \mathcal{Y}'_{s_d(n)}$.
- Run $\mathsf{Merge}_d(x, y_1, \ldots, y_{\ell_d(n)})$ to get $y \in \mathcal{Y}_n$, and output y as the alleged $f_n(x)$.

We will prove that with high probability, after the calls to Amort, enough of the y_{ij}'s produced will be equal to the respective $g_{s_d(n)}(x_{ij})$'s to be able to correctly recover all the $f'_{s_d(n)}(x_i)$'s and hence $f_n(x)$.

For each $j \in [\ell_r(s_d(n))]$, define I_j to be the indicator variable that is 1 if $\mathsf{Amort}(x_{1j}, \ldots, x_{\ell_d(n)j})$ is correct and 0 otherwise. Note that by the properties of the robust reduction of $\mathcal{F}'$ to $\mathcal{G}$, for a fixed j each of the x_{ij}'s is independently distributed according to $D_{s_d(n)}$ and further, for any two distinct j, j', the tuples (x_{ij}) and $(x_{ij'})$ are independent.

Let $I = \sum_j I_j$ and $m = \ell_r(s_d(n))$. By the aforementioned properties and the correctness of Amort, we have the following:

$$\begin{aligned} \mathrm{E}[I] &\geq \frac{7}{8}m \\ \mathrm{Var}[I] &\leq \frac{7}{64}m \end{aligned}$$

Note that as long as Amort is correct on more than a 2/3 fraction of the j's, Merge_r will get all of the y_i's correct, and hence Merge_d will correctly compute $f_n(x)$. The probability that this does not happen is bounded using Chebyshev's inequality as:

$$\begin{aligned} \Pr\left[I \leq \frac{2}{3}m\right] &\leq \Pr\left[|I - \mathrm{E}[I]| \geq \left(\frac{7}{8} - \frac{2}{3}\right)m\right] \\ &\leq \frac{\mathrm{Var}[I]}{(5m/24)^2} \\ &\leq \frac{63}{25 \cdot m} < \frac{3}{m} \end{aligned}$$

As long as $m > 9$, this probability of failure is less than 1/3, and hence $f_n(x)$ is computed correctly in the worst-case with probability at least 2/3. If it is the case that $\ell_r(s_d(n)) = m$ happens to be less than 9, then instead of using Merge_r directly in the above algorithm, we would use Merge'_r that runs Merge_r several times so as to get more than 9 samples in total and takes the majority answer from all these runs.

The time taken is $t_d(n)$ for the downward reduction, $t_r(s_d(n))$ for each of the $\ell_d(n)$ robust reductions on instances of size $s_d(n)$, and $\ell_d(n)t_a(s_d(n))$ for each of the $\ell_r(s_d(n))$ calls to Amort on sets of $\ell_d(n) = \ell_a(s_d(n))$ instances, summing up to the total time stated in the lemma. □

6 Removing Interaction

In this section we show how to remove the interaction in Protocol 2 via the Fiat-Shamir Heuristic, and prove security in the Random Oracle model. In what follows, we take H to be a random oracle that outputs an element of $\mathbb{F}_p$, where p will be as in Definition 4 of GOV^k, where the instance size n will be clear from context.

Recall the definition of the polynomials $q(i_1, \ldots, i_k)$ and $q_{s,\alpha_1,\ldots,\alpha_{s-1}}(x)$ from Section 3. The non-interactive Proof of Useful Work for k-OV is described as Protocol 3.

A Non-interactive uPoW for k-OV

$\mathsf{Gen}(\boldsymbol{x})$**:**

- Given an instance $\boldsymbol{x} \in \{0,1\}^{knd}$, interpret $\boldsymbol{x}$ as an element of $\mathbb{F}_p^{knd}$ (where $p = p(n)$ is as in Definition 4).
- Pick a random $\boldsymbol{r} \in \mathbb{F}_p^{knd}$.
- Output the set of vectors $\boldsymbol{c_x} = \{\boldsymbol{y}_t = \boldsymbol{x} + t\boldsymbol{r} \mid t \in [kd+1]\}$.

$\mathsf{Solve}(\boldsymbol{c}_x)$**:**

Given input $\boldsymbol{c}_x = \{\boldsymbol{y}_t\}$, for each $\boldsymbol{y} \in \boldsymbol{c}_x$ do the following:

- Compute $z_y = \mathsf{gOV}^k_{n,d,p}(\boldsymbol{y})$.
- Compute coefficients of q_1^y Let $\tau_1^y = (z^y, q_1^y)$
- For s from 1 to $k-2$:
  - Compute $\alpha_s^y = H(\boldsymbol{c}_x, \tau_s^y)$.
  - Compute coefficients of $q_{s+1}^y = q_{s+1,\alpha_1,\ldots,\alpha_s}$, with respect to $\boldsymbol{y}$.
  - Set $\tau_{s+1}^y = (\tau_s^y, q_{s+1}^y)$.

Output $T = \{\tau_{s+1}^y\}_{\boldsymbol{y} \in \boldsymbol{c}_x}$

$\mathsf{Verify}(\boldsymbol{c}_x, T^*)$:

Given $T^* = \{\tau^{y*} = (z^{y*}, q_1^{y*}, q_2^{y*}, \ldots, q_{k-1}^{y*})\}$, for each $\tau^{y*} \in T^*$ do the following:

- Check $\sum_{i_1 \in [n]} q_1^{y*}(i_1) = z^{y*}$. If check fails, reject.
- Compute $\alpha_1^{y*} = H(\boldsymbol{c}_x, z^{y*}, q_1^{y*})$.
- For s from 1 up to $k-2$:
  - Compute $\alpha_s^{y*} = H(\boldsymbol{c}_x, z^{y*}, q_1^{y*}, \ldots, q_s^{y*})$.
  - Check that $\sum_{i_{s+1} \in [n]} q_{s+1}^{y*}(i_{s+1}) = q_s^{y*}(\alpha_s^{y*})$. If check fails, reject.
- Compute $\alpha_{k-1}^{y^*} = H(\boldsymbol{c}_x, z^{y*}, q_1^{y*}, \ldots, q_{k-2}^{y*})$.
- Check that $q_{k-1}^{y*}(i_{s+1}) = \sum_{i_k \in [n]} q_k^y(i_k)$. If check fails, reject.

If verifier has yet to reject, accept.

$\mathsf{Recon}(\boldsymbol{c_x}, \{z_{y_t}\})$:

- Interpret $z_{y_1}, \ldots, z_{y_{kd+1}}$ as the evaluations of a univariate polynomial $h(t)$ of degree kd at $t = 1, \ldots, kd+1$.
- Interpolate to find the coefficients of h and compute $z = h(0)$.
- If $z \neq 0$, output 1, else 0 as the answer to the k-OV instance.

Protocol 3: A Non-interactive uPoW for k-OV

Theorem 5. *For any $k \geq 2$, suppose k-OV takes $n^{k-o(1)}$ time to decide for any $d = \omega(\log n)$. Then, Protocol 3 is a* non-interactive *(n^k, δ)-Proof of Useful Work for k-OV in the Random Oracle model for any function $\delta(n) > 1/n^{o(1)}$.*

Efficiency, correctness, usefulness (given soundness), and hardness of Protocol 3 follow from the corresponding arguments about Protocol 2 in the proof of Theorem 2 in Section 3. The following lemma implies that the protocol is sound as well, completing the proof of Theorem 5.

Lemma 4. *For any $k \geq 2$, if Protocol 2 is sound as a Proof of Useful Work for GOV^k, then Protocol 3 is sound as a non-interactive Proof of Useful Work for GOV^k in the Random Oracle model.*

Note that in the above uPoW, we can cluster the s^{th} oracle calls for each instance together, so that only k oracle calls need to be made.

Proof. Let P be a cheating prover for the non-interactive uPoW that breaks soundness with non-negligible probability $\varepsilon(n)$. We will construct a prover, P', that then also breaks the interactive uPoW soundness with non-negligible probability.

Notice that if P outputs a proof with a non-queried "challenge", by the Schwartz-Zippel Lemma the probability the transcript is accepted is negligible. Thus, any cheating prover must query for all "challenges."

Suppose P makes at most $m\mathsf{poly}(n)$ queries to the random oracle, H. We select k of the m query indices, $i_1, \ldots, i_k$. Let the verifier V (recall that our protocol is public coin) output the k indendently drawn uniform challenges $\alpha_1, \ldots, \alpha_k$ on randomness r. We then program a random oracle H_r to output α_j on the i_j query. Now, we define P' to be the interactive prover that is consistent with the transcript of P. Notice that P' will fool $V(r)$ with probability $\varepsilon(n)$ (when given H_r access to H_r), conditioned on the fact that the i_j's are chosen correctly (which happens with probability $(1/m)^k$). So, P' breaks soundness with probability $\varepsilon'(n) = \frac{\varepsilon(n)}{m^k}$, which is still non-negligible given k is constant.

Moreover, the distribution of random oracles $\{H\}$ is identical to the distribution of $\{H_r\}_r$. Therefore, P' cannot distinguish between the two cases. Thus, we can define P'' that simply flips the coins for output himself and breaks soundness with probability $\varepsilon'(n)$. □

7 A Blockchain Scheme

Bitcoin uses PoWs on a massive scale. In this light, having Proofs of Useful Work is much desired from the perspective of decreasing environmental costs and also from the perspective of having an enormous, incentivized computing community already existing that can be fed problems to solve.

Unfortunately, a generic uPoW does not immediately fit into the framework in which Bitcoin uses them. Namely, PoWs or uPoWs used in Bitcoin should be rendered invalid if Bitcoin transactions are altered. We give a brief overview of how PoWs are currently used and then describe how our uPoWs can be incorporated to a Blockchain-like mechanism.

Bitcoin's main innovation is a system implementing a public ledger on which transactions are recorded: the blockchain. The blockchain is a discretized timeline of transactions in which each discrete group of transactions is called a block and the blocks are then chained together by each block containing a hash of its previous block (enforcing its temporal structure). The role of PoWs in this framework is that for a malicious user to 'rewrite history' or change a block, they must produce a PoW that is *sensitive to changes in the block*. Thus, creating dishonest blocks requires work and, since the blockchain is always decided by majority, PoWs ensure that any adversarial community cannot reliably succeed without having the majority of computing power in the entire system.

A main point to notice here is that the PoW must be sensitive to changes in the block that the proof is made for. To account for this we show how our uPoWs can be made to be sensitive to such changes and give a scheme for which a blockchain based system such as Bitcoin can use our uPoWs to operate while dually serving as a source of computation for delegators.

As seen in Figure 1, there is a public board that delegators post problems to. We currently write each problem in the form $(f, \boldsymbol{x})$ where f is either an arithmetic circuit or simply a label of a commonly requested problem, such as OV, that the workers are familiar with and $\boldsymbol{x}$ is the instance being delegated to find $f(\boldsymbol{x})$ for (we assume for now that our practical problems are already in the

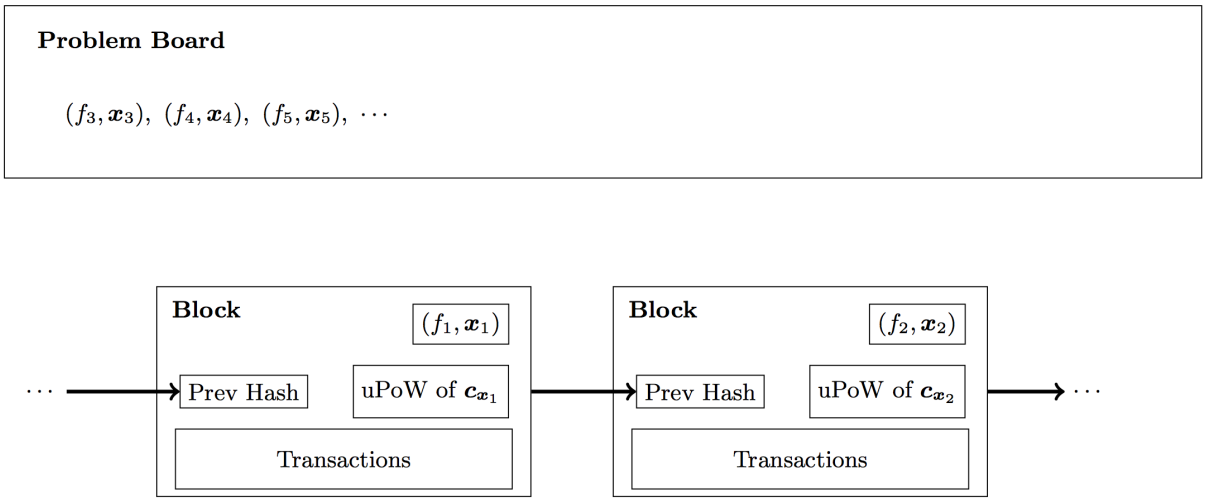


Figure 1: We present a framework for Blockchain to use uPoWs. Delegators post to a public Problem Board from which workers grab problems to mine a block with by producing a Proof of Useful Work that they attach to the block.

form of evaluating a low-degree polynomial). When a worker needs to perform a PoW, they grab a problem from the board according to any type of priority scheduling and keep it to mine their next block.

Notice that the worker currently has the actual delegated instance x. Using a Random Oracle H, the worker will generate the challenge $\boldsymbol{c}_{\boldsymbol{x}}$ themselves as usual except substituting $r = H(\text{current block})$ for the randomness usually used to generate the challenge: $\boldsymbol{c}_{\boldsymbol{x}} = \{\boldsymbol{x} + rt \mid t \in [D+1]\}$, where $r = H(\text{current block})$. For a truly Random Oracle H, r will be random and this becomes a standard challenge for a uPoW. Further, any altercations to the current block being mined will produce an entirely new random challenge and so a new uPoW will have to be made for changed blocks. Thus we attain uPoWs that are sensitive to changes in the block.

Note that this also means that if a party fails to mine a block before another party successfully does, they can still use the same problem $(f, \boldsymbol{x})$ on a new block they attempt to mine as the challenge will be 're-randomized' with respect to H and so parties will hold on to their problems until they complete a uPoW with it.

Substituting a standard cryptographic hash function such as SHA-256 for H, this falls very much in line with what Bitcion currently does. Current Bitcoin PoWs are essentially to find a nonce so that, when hashed along with the current block, the hash value has a prescribed number of leading 0's. Thus these current (useless) PoWs also rely on SHA-256 behaving as a Random Oracle (and this is also used to chain blocks together by hashing the previous block). We follow this approach in using H to generate our randomness for generation.

A block then, as seen in Figure 1, is composed of

1. The hash of the previous block,
2. The transactions that the block is recording,
3. The problem $(f, \boldsymbol{x})$ the block claims to have a proof for, and
4. The uPoW for f on challenge $\boldsymbol{c}_{\boldsymbol{x}} = \{\boldsymbol{x} + H(\text{current block})t \mid t \in [D+1]\}$.

To verify a block as a valid addition to the blockchain, a user simply checks that the hash of the previous block is correct, that the problem (f, x) hadn't been previously solved (this is to ensure that each PoW is useful in that no two people redundantly have the same problem and that miners constantly pull new problems from the problem board), and that the PoW is valid by deterministically computing the $\boldsymbol{c_x}$ challenge with H and then checking the uPoW for it. Further, the delegator upon seeing the uPoW can quickly reconstruct $f(x)$ by uPoW's Usefulness property.

We then have uPoWs for Bitcoin. As is common now, workers can still create 'mining pools' and parallelize the work amongst their pool and, in fact, our framework naturally enhances this joint effort to be robust to errors and Byzantine failures, even identifying non-cooperative members of the mining pool (this uses the fact that the solution sketch to our uPoWs are recovered by means of decoding a Reed-Muller code for which there is good error-correction for [BK16]). Further, while the total *combined* work done by a mining pool is still guaranteed to be of a certain amount by uPoW's Hardness condition, the time a delegator has to wait may be significantly shorter as they parallelize their work amongst themselves.

Acknowledgements

We are grateful to Guy Rothblum for his suggestion of using interaction to increase the gap between solution and verification in our uPoWs. We would also like to thank Tal Moran and Vinod Vaikuntanathan for several useful discussions.

The bulk of this work was performed while the authors were at IDC Herzliya's FACT center and supported by NSF-BSF Cyber Security and Privacy grant #2014/632, ISF grant #1255/12, and by the ERC under the EU's Seventh Framework Programme (FP/2007-2013) ERC Grant Agreement #07952. Marshall Ball is supported in part by the Defense Advanced Research Project Agency (DARPA) and Army Research Office (ARO) under Contract #W911NF-15-C-0236, and NSF grants #CNS-1445424 and #CCF-1423306. Manuel Sabin is also supported by the National Science Foundation Graduate Research Fellowship under Grant #DGE-1106400. Prashant Nalini Vasudevan is also supported by the IBM Thomas J. Watson Research Center (Agreement #4915012803).

References

[ABFG14] Giuseppe Ateniese, Ilario Bonacina, Antonio Faonio, and Nicola Galesi. Proofs of space: When space is of the essence. In *International Conference on Security and Cryptography for Networks*, pages 538–557. Springer, 2014.

[AL13] Amir Abboud and Kevin Lewi. Exact weight subgraphs and the k-sum conjecture. In *International Colloquium on Automata, Languages, and Programming*, pages 1–12. Springer, 2013.

[And13] Nate Anderson. Mining bitcoins takes power, but is it an "environmental disaster?". http://tinyurl.com/cdh95at, April 2013.

[BCG15] Joseph Bonneau, Jeremy Clark, and Steven Goldfeder. On bitcoin as a public randomness source. *IACR Cryptology ePrint Archive*, 2015:1015, 2015.

[BK16] Andreas Björklund and Petteri Kaski. How proofs are prepared at camelot. In *Proceedings of the 2016 ACM Symposium on Principles of Distributed Computing*, pages 391–400. ACM, 2016.

[BRSV17] Marshall Ball, Alon Rosen, Manuel Sabin, and Prashant Nalini Vasudevan. Average-case fine-grained hardness. to appear in Symposium on Theory of Computing (STOC'17), 2017.

[CPS99] Jin-yi Cai, Aduri Pavan, and D. Sivakumar. On the hardness of permanent. In Christoph Meinel and Sophie Tison, editors, *STACS 99, 16th Annual Symposium on Theoretical Aspects of Computer Science, Trier, Germany, March 4-6, 1999, Proceedings*, volume 1563 of *Lecture Notes in Computer Science*, pages 90–99. Springer, 1999.

[DFKP15] Stefan Dziembowski, Sebastian Faust, Vladimir Kolmogorov, and Krzysztof Pietrzak. Proofs of space. In *Annual Cryptology Conference*, pages 585–605. Springer, 2015.

[DN92] Cynthia Dwork and Moni Naor. Pricing via processing or combatting junk mail. In Ernest F. Brickell, editor, *Advances in Cryptology - CRYPTO '92, 12th Annual International Cryptology Conference, Santa Barbara, California, USA, August 16-20, 1992, Proceedings*, volume 740 of *Lecture Notes in Computer Science*, pages 139–147. Springer, 1992.

[FF93] Joan Feigenbaum and Lance Fortnow. Random-self-reducibility of complete sets. *SIAM J. Comput.*, 22(5):994–1005, 1993.

[Fid72] Charles M. Fiduccia. Polynomial evaluation via the division algorithm: The fast fourier transform revisited. In Patrick C. Fischer, H. Paul Zeiger, Jeffrey D. Ullman, and Arnold L. Rosenberg, editors, *Proceedings of the 4th Annual ACM Symposium on Theory of Computing, May 1-3, 1972, Denver, Colorado, USA*, pages 88–93. ACM, 1972.

[GI16] Jiawei Gao and Russell Impagliazzo. Orthogonal vectors is hard for first-order properties on sparse graphs. *Electronic Colloquium on Computational Complexity (ECCC)*, 23:53, 2016.

[GR17] Oded Goldreich and Guy Rothblum. Simple doubly-efficient interactive proof systems for locally-characterizable sets. Electronic Colloquium on Computational Complexity Report TR17-018, February 2017.

[Hor72] Ellis Horowitz. A fast method for interpolation using preconditioning. *Inf. Process. Lett.*, 1(4):157–163, 1972.

[JJ99] Markus Jakobsson and Ari Juels. Proofs of work and bread pudding protocols. In Bart Preneel, editor, *Secure Information Networks: Communications and Multimedia Security, IFIP TC6/TC11 Joint Working Conference on Communications and Multimedia Security (CMS '99), September 20-21, 1999, Leuven, Belgium*, volume 152 of *IFIP Conference Proceedings*, pages 258–272. Kluwer, 1999.

[Kin13] Sunny King. Primecoin: Cryptocurrency with prime number proof-of-work. *July 7th*, 2013.

[KK14] Nikolaos P Karvelas and Aggelos Kiayias. Efficient proofs of secure erasure. In *International Conference on Security and Cryptography for Networks*, pages 520–537. Springer, 2014.

[MJS+14] Andrew Miller, Ari Juels, Elaine Shi, Bryan Parno, and Jonathan Katz. Permacoin: Repurposing bitcoin work for data preservation. In *Security and Privacy (SP), 2014 IEEE Symposium on*, pages 475–490. IEEE, 2014.

[Nak08] Satoshi Nakamoto. Bitcoin: A peer-to-peer electronic cash system, 2008.

[RR00] Ron M. Roth and Gitit Ruckenstein. Efficient decoding of reed-solomon codes beyond half the minimum distance. *IEEE Trans. Information Theory*, 46(1):246–257, 2000.

[Wil05] Ryan Williams. A new algorithm for optimal 2-constraint satisfaction and its implications. *Theor. Comput. Sci.*, 348(2-3):357–365, 2005.

[Wil15] Virginia Vassilevska Williams. Hardness of easy problems: Basing hardness on popular conjectures such as the strong exponential time hypothesis. In *Proc. International Symposium on Parameterized and Exact Computation*, pages 16–28, 2015.

[Wil16] Richard Ryan Williams. Strong ETH breaks with merlin and arthur: Short non-interactive proofs of batch evaluation. In *31st Conference on Computational Complexity, CCC 2016, May 29 to June 1, 2016, Tokyo, Japan*, pages 2:1–2:17, 2016.

[WW10] Virginia Vassilevska Williams and Ryan Williams. Subcubic equivalences between path, matrix and triangle problems. In *Foundations of Computer Science (FOCS), 2010 51st Annual IEEE Symposium on*, pages 645–654. IEEE, 2010.

A Even Further Non-Amortizability of GOV

In this section, we show that a slightly stronger, but natural form of amortization is impossible for GOV^k. In particular, it is sufficient to define a notion of amortizability for parametrized families of functions with a monotonicity constraint. In our case, monotonicity will essentially say "adding more vectors of the same dimension and field size does not make the problem easier." This is a natural property of most algorithms. Namely, it is the case if for any fixed d, p, $\mathsf{GOV}^k_{n,d,p}$ is $(n, t, \delta) - amortizable$.

Instead, we simply generalize amortizability in a parametrized fashion for $\mathsf{GOV}^k_{n,d,p}$.

Definition 8. *A parametrized class, $\mathcal{G}_\rho$, is* not (ℓ, t, δ)-amortizable on average over $\mathcal{D}_\rho$, a parametrized family of distributions *if, for any fixed parameters N, ρ, and algorithm Amort_ρ that runs in time $\ell(\rho)t(\rho)$, when run on $\ell(\rho)$ inputs from $\hat{\mathcal{X}}_\rho$, when it is given as input $\ell(\rho)$ independent samples from D_ρ,*

$$\Pr_{x_i \leftarrow D_\rho}\left[\mathsf{Amort}(x_1, \ldots, x_{\ell(\rho)}) = (g_\rho(x_1), \ldots, g_\rho(x_{\ell(\rho)}))\right] < \delta(\rho)$$

We now show how a generalization of the list decoding reduction from [BRSV17] yields strong amortization bounds. Before we begin, we will present a few Lemmas from the literature to make certain bounds explicit.

First, we present an inclusion-exclusion bound from [CPS99] on the polynomials consistent with a fraction of m input-output pairs, $(x_1, y_1), \ldots, (x_m, y_m)$. We include a laconic proof here with the given notation for convenience.

Lemma 5 ([CPS99])**.** *Let q be a polynomial over $\mathbb{F}_p$, and define* $\mathrm{Graph}(q) := \{(i, p(i)) \mid i \in [p]\}$. *Let $c > 2$, $\delta/2 \in (0, 1)$, and $m \leq p$ such that $m > \frac{c^2(d-1)}{\delta^2(c-2)}$ for some d. Finally, let $I \subseteq [p]$ such that $|I| = m$. Then, for any set $S = \{(i, y_i) \mid i \in I\}$, there are less than $\lceil c/\delta \rceil$ polynomials q of degree at most d that satisfy $|\mathrm{Graph}(q) \cap S| \geq m\delta/2$.*

Corollary 2. *Let S be as in Lemma 5 with $I = \{m+1, \ldots, p\}$, for any $m < p$. Then for $m > 9d/\delta^2$, there are at most $3/\delta$ polynomials, q, of degree at most d such that $|\mathrm{Graph}(q) \cap S| \geq m\delta/2$.*

Proof. Reproduced from [CPS99] for convenience; see original for exposition.

Suppose there exist at least $\lceil c/\delta \rceil$ such polynomials. Consider a subset of exactly $N = \lceil c/\delta \rceil$ such polynomials, $\mathcal{F}$. Define $\mathsf{S}_f := \{(i, f(i)) \in \text{Graph}(f) \cap S\}$, for each $f \in \mathcal{F}$.

$$\begin{aligned} m \geq \left| \bigcup_{f \in \mathcal{F}} S_f \right| &\geq \sum_{f \in \mathcal{F}} |S_f| - \sum_{f, f' \in \mathcal{F} : f \neq f'} |S_f \cap S_{f'}| \\ &\geq N \frac{m\delta}{2} - \frac{N(N-1)(d-1)}{2} \\ &> \frac{N}{2} \left(m\delta - \frac{c(d-1)}{\delta} \right) \\ &\geq \frac{c}{2\delta} \left(m\delta - \frac{c(d-1)}{\delta} \right) \\ &= \frac{cm}{2} - \frac{c^2(d-1)}{2\delta^2} \\ &= m + \frac{1}{2} \left((c-2)m - \frac{c^2(d-1)}{\delta^2} \right) > m. \end{aligned}$$

□

Now, we give a theorem based on an efficient list-decoding algorithm, related to Sudan's, from Roth and Ruckenstein. [RR00]

Lemma 6 ([RR00])**.** *List decoding for $[n, k]$ Reed-Solomon (RS) codes over $\mathbb{F}_p$ given a code word with almost $n - \sqrt{2kn}$ errors (for $k > 5$), can be performed in*

$$O\left(n^{3/2} k^{-1/2} \log^2 n + (n-k)^2 \sqrt{n/k} + (\sqrt{nk} + \log q) n \log^2(n/k) \right)$$

operations over $\mathbb{F}_q$.

Plugging in specific parameters and using efficient, we get the following corollary which will be useful below.

Corollary 3. *For parameters $n \in \mathbb{N}$ and $\delta \in (0, 1)$, list decoding for $[m, k]$ RS over $\mathbb{F}_p$ where $m = \Theta(d \log n/\delta^2)$, $k = \Theta(d)$, $p = O(n^2)$, and $d = \Omega(\log n)$ can be performed in time*

$$O\left(\frac{d^2 \log^{5/2} n \, \text{Arith}(n)}{\delta^5} \right),$$

where $\text{Arith}(n)$ is a time bound on arithmetic operations over prime fields size $O(n)$.

Theorem 6. *Suppose k-OV takes $n^{k-o(1)}$ time to decide for any $d = \omega(\log n)$, for any $k \geq 2$. Then, for any positive constants $c, \epsilon > 0$ and $0 < \delta < \varepsilon/2$, GOV^k is* not

$$(n^c \mathsf{poly}(d, \log(p)), n^{k-\epsilon} \mathsf{poly}(d, \log(p)), n^{-\delta} \mathsf{poly}(d, \log(p)))$$

-amortizable on average over the uniform distribution over its inputs.

Proof. Let $k = 2c' + c$ and $p > n^k$. Suppose for the sake of contradiction that $\mathsf{GOV}_{n,d,p}$ is $(n^c\mathsf{poly}(d, \log(p)), n^{2c'+c-\epsilon}\mathsf{poly}(d, \log(p)), n^{-c'}\mathsf{poly}(d, \log(p)))$-amortizable on average over the uniform distribution.

Let $m = n^{k/(k+c)}$, as before. By Proposition 2, k-OV with vectors of dimension $d = (\frac{k}{k+c}))^2 \log^2 n$ is (m, m^c)-downward reducible to k-OV with vectors of dimension $\log^2(n)$, in time $\tilde{O}(m^{c+1})$.

For each $j \in [m^c]$ $X_j = (U^{j1}, \ldots, U^{jk}) \in \{0,1\}^{kmd}$ is the instance of boolean-valued orthogonal vectors from the above reduction. Now, consider splitting these lists in half, $U^{ji} = (U_0^{ji}, U_1^{ji})$ $(i \in [k])$, such that $(U_{a_1}^{j1}, \ldots, U_{a_k}^{jk}) \in \{0,1\}^{kmd/2}$ for $\boldsymbol{a} \in \{0,1\}^k$. Interpret $\boldsymbol{a}$ as binary number in $\{0, \ldots, 2^k - 1\}$. Then, define the following 2^k sub-problems:

$$A^{\boldsymbol{a}} = ((U_{a_1}^{j1}, \ldots, U_{a_k}^{jk})), \forall \boldsymbol{a} \in \{0, \ldots, 2^k - 1\}$$

Notice that given solutions to gOV_d^k on $\{A^{\boldsymbol{a}}\}_{\boldsymbol{a}\in\{0,1\}^k}$ we can trivially construct a solution to OV_d^k on X_j.

Now, draw random $B_j, C_j \in \mathbb{F}_p^{kmd/2}$ and consider the following degree 2^k polynomial in x:

$$D_j(x) = \sum_{i=1}^{2^k} \delta_i(x) A^{i-1} + (B_j + xC_j) \prod_{i=1}^{2^k} (x - i),$$

where δ_i is the unique degree $2^k - 1$ polynomial over $\mathbb{F}_p$ that takes value 1 at $i \in [2^k]$ and 0 on all other values in $[2^k]$. Notice that $D_j(i) = A^{i-1}$ for $i \in [2^k]$.

Let $r > 2^{k+1} d/\delta^2 \log m$. $D_j(2^k + 1), D_j(6), \ldots, D_j(r + 2^k)$. By the properties of Amort and because the $D_j(\cdot)$'s are independent, $D_1(i), \ldots, D_{m^c}(i)$ are independent for any fixed i. Thus,

$$\mathsf{Amort}(D_1(i), \ldots, D_{m^c}(i)) = \mathsf{gOV}^k(D_1(i)), \ldots, \mathsf{gOV}^k(D_{m^c}(i))$$

for $\delta r/2$ i's with probability at least $1 - \frac{4}{\delta r} = 1 - 1/\operatorname{polylog}(m)$, by Chebyshev.

Now, because $\delta r/2 > \sqrt{16dr}$, we can run the list decoding algorithm of Roth and Ruckenstein, [RR00], to get a list of all polynomials with degree $\leq 2^{k+1}d$ that agree with at least $\delta r/2$ of the values. By Corollary 2, there are at most $L = 3/\delta$ such polynomials.

By a counting argument, there can be at most $2^k d\binom{L}{2} = O(dL^2)$ points in $\mathbb{F}_p$ on which any two of the L polynomials agree. Because $p > n^k > 2^k d\binom{L}{2}$, we can find such a point, ℓ, by brute-force in $O(L \cdot dL^2 \log^3(dL^2) \log p)$ time, via batch univariate evaluation [Fid72]. Now, to identify the correct polynomials $\mathsf{gOV}^k(D_j(\cdot))$, one only needs to determine the value $\mathsf{gOV}^k(D_j(\ell))$. To do so, we can recursively apply the above reduction to all the $D_j(\ell)$s until the number of vectors, m, is constant and gOV^k can be evaluated in time $O(d \log p)$.

Because each recursive iteration cuts m in half, the depth of recursion is $\log(m)$. Additionally, because each iteration has error probability $< 4/(\delta r)$, taking a union bound over the $\log(m)$ recursive steps yields an error probability that is $\varepsilon < 4 \log m/(\delta r)$.

We can find the prime p via $O(\log m)$ random guesses in $\{m^k + 1, \ldots, 2m^k\}$ with overwhelming probability. By Corollary 3, taking $r = 8d \log m/\delta^2$, Roth and Ruckenstein's algorithm takes time $O(d^2/\delta^5 \log^{5/2} m \operatorname{Arith}(m^k))$ in each recursive call. The brute force procedure takes time $O(d/\delta^3 \log^3(d/\delta^2) \log m)$, which is dominated by list decoding time. Reconstruction takes time $O(\log m)$ in each round, and is also dominated. Thus the total run time is

$$T = O(m^c(m^{k-\varepsilon} d \log^2 m/\delta^2 + d^2/\delta^5 \log^{7/2} m \operatorname{Arith}(m^k))),$$

with error probability $\varepsilon < 4 \log m\delta/d$. □

B Zero-Knowledge Proofs of Work

We combine our PoW with ElGamal encryption and a zero-knowledge proof of discrete logarithm equality to get an non-repudiatable, non-transferable proof of work from the Decisional Diffie-Hellman assumption on Schnorr groups.

Protocol. Let $\mathbb{Z}_p$ be a Schnorr group such of size $p = qm + 1 \leq 2^{\text{polylog}(n)}$ such that DDH holds with generator g. (Assuming the DDH problem is hard for $o(|G|^{1/2})$-time probabilistic algorithms on a group G, we can take $|G| \approx n^4$.) Let (E, D) denote an ElGamal encryption system on G.

- Challenge is issued as before: $(U, V) \leftarrow \mathbb{Z}_q^{2nd}$.
- Prover generates a secret key $x \leftarrow \mathbb{Z}_{p-1}$, and sends encryptions of the coeffecients of the challenge response over the subgroup size q to Verifier with the public key $(g, h = g^x)$:

$$\begin{aligned}\mathsf{E}(R^*(\cdot); S(\cdot)) &= \mathsf{E}(mr_0^*; s_0), \ldots, \mathsf{E}(mr_{nd-1}^*; s_{nd-1}) \\ &= (g^{s_0}, g^{r_0^*} h^{xs_0}), \ldots, (g^{s_{nd-1}}, g^{mr_{nd-1}^*} h^{xs_{nd-1}}).\end{aligned}$$

  Prover additionally draws $t \leftarrow \mathbb{Z}_{p-1}$ and sends $a_1 = g^t, a_2 = h^t$.
- Verifier draws random $z \leftarrow \mathbb{Z}_q$ and challenge $c \leftarrow \mathbb{Z}_p^*$ and sends to Prover.
- Prover sends $w = t + cS(z)$ to verifier.
- Verifier evaluates $y = \mathsf{gOV}_V(\phi_1(z), \ldots, \phi_d(z))$ to get g^{my}. Then, homomorphically evaluates $\mathsf{E}(R^*; S)$ on z so that $\mathsf{E}(R^*(z); S(z))$ equals

$$\begin{aligned}&\left((g^{s_0})(g^{s_1})^z \cdots (g^{s_{nd-1}})^{z^d}, (g^{r_0^*} h^{s_0})(g^{mr_1^*} h^{s_1})^z \cdots (g^{mr_{nd-1}^*} h^{s_{nd-1}})^{z^d}\right) \\ &= (u_1, u_2)\end{aligned}$$

  Then, Verifier accepts if and only if

$$g^w = a_1 (u_1)^c \quad \& \quad h^w = a_2 (u_2 / g^{my})^c.$$

Recall that the success probability of a subquadratic prover (in the non-zero-knowledge case) does not have negligible success probability. Thus the above should be performed on $k = \text{polylog}(n)$ instances simultaneously and the verifier should accept iff an only if all instances accept.

Remark B.1. Note that the above protocol is public coin. Therefore, we can apply the Fiat-Shamir heuristic, and use a random oracle on partial transcripts to make the protocol non-interactive.

More explicitly, let H be a random oracle. Then:

- Prover computes

$$\begin{aligned}&(g, h), \\ &\mathsf{E}(R^*; S), \\ &a_1 = g^t, a_2 = h^t, \\ &z = H(U, V, g, h, \mathsf{E}(R^*; S), a_1, a_2), \\ &c = H(U, V, g, h, \mathsf{E}(R^*; S), a_1, a_2, z), \\ &w = t + cS(z)\end{aligned}$$

  and sends $(g, h, \mathsf{E}(R^*; S), a_1, a_2, w)$.

- Verifier calls random oracle twice to get

$$z = H(U, V, g, h, \mathsf{E}(R^*; S), a_1, a_2), c = H(U, V, g, h, \mathsf{E}(R^*; S), a_1, a_2, z).$$

  Then, the verifier homomorphically evaluates $\mathsf{E}(R^*; S)(z) = (u_1, u_2)$, it then computes the value $y = gOV_V(\phi_1(z), \ldots, \phi_d(z))$. Finally, accepts if and only if

$$g^w = a_1(u_1)^c \quad \& \quad h^w = a_2(u_2/g^{my})^c.$$

Correctness. From before, if $R^* \equiv R_{U,V}$ as is the case for an honest prover, then for any $z \in \mathbb{Z}_q$ we have $R^*(z) = R_{U,V}(z) = \mathsf{gOV}_V(\phi_1(z), \ldots, \phi_d(z))$. Moreover

$$g^w = g^{t+cS(z)} = g^t(g^{S(z)})^c = a_1 \left((g^{s_0})(g^{s_1})^z \cdots (g^{s_{nd-1}})^{z^d}\right)^c,$$

and

$$\begin{aligned} h^w &= h^{t+cS(z)} \\ &= h^t(g^0 h^{S(z)})^c \\ &= a_2 \left((g^{r_0^*} h^{s_0})(g^{mr_1^*} h^{s_1})^z \cdots (g^{mr_{nd-1}^*} h^{s_{nd-1}})^{z^d} g^{-\mathsf{gOV}_V(\phi_1(z),\ldots,\phi_d(z))}\right)^c. \end{aligned}$$

Soundness. Suppose Prover runs in subquadratic time, then with high probability $R^* \not\equiv R_{U,V}$, and so for random z, $R^*(z) \neq \mathsf{gOV}_V(\phi_1(z), \ldots, \phi_d(z))$ with overwhelming probability. Suppose this is the case in what follows, namely: $R^*(z) = y^* \neq y = \mathsf{gOV}_V(\phi_1(z), \ldots, \phi_d(z))$. In particular,

$$\log_g u_1 \neq \log_h u_2/g^{\mathsf{gOV}_V(\phi_1(z),\ldots,\phi_d(z))}.$$

Note that $u_1, u_2/g^{\mathsf{gOV}_V(\phi_1(z),\ldots,\phi_d(z))}$ can be calculated from the Prover's first message.

As is standard, we will fix the prover's first message and (assuming $y \neq y^*$) rewind any two accepting transcripts with distinct challenges to show that $\log_g u_1 = \log_h u_2/g^y$. Fix a_1, a_2 as above and let $(c, w), (c', w')$ be the two transcripts. Recall that if a transcript is accepted, $g^w = a_1 u_1^c$ and $h^w = a_2(u_2/g^y)^c$. Then,

$$g^{w-w'} = u_1^{c-c'} \Rightarrow \log_g u_1 = \frac{w - w'}{c - c'} = \log_h u_2/g^y \Leftarrow h^{w-w'} = (u_2/g^y)^{c-c'}.$$

Therefore, because $u_1 \neq u_2/g^y$ there can be at most one c for which a Prover can convince the verifier. Such a c is chosen with negligible probability.

Honest Verifier Zero Knowledge. Given the verifier's challenge z, c, we can simulate the transcript of an honest prover as follows:

- Draw public key (g, h).
- Compute the ElGamal Encryption $\mathsf{E}_{g,h}(R'; S)$ where R' is the polynomial with constant term $\mathsf{gOV}_V(\phi_1(z), \ldots, \phi_d(z))$ and zeros elsewhere.
- Draw random w.
- Compute $a_1 = \frac{g^w}{g^{cS(z)}}$ and $a_w = \frac{h^w}{h^{cS(z)}}$.
- Output $((g, h), a_1, a_2, z, c, w)$.

Notice that do to the semantic security of ElGamal, the transcript output is computationally indistinguishable from that of an honest Prover. Moreover, the simulator runs in $\tilde{O}(nd)$ time, the time to compute R', encrypt, evaluate S and exponentiate. Thus, the protocol is (honest verifier) zero-knowledge.

The usual trick allows us to remove the honest verifier condition.

Efficiency. The honest prover runs in time $\tilde{O}(n^2)$, because the nd encryptions can be performed in time polylog(n) each. The verfier takes $\tilde{O}(nd)$ time as well. Note that the homomorphic evaluation requires $O(d \log z^d) = O(d^2 \log z) = \text{polylog}(d)$ exponentiations and $d = \text{polylog}(n)$ multiplications.

NEWS

by **Jamie Redman**
Feb 5, 2019

Data Shows Ethereum is the 'Cryptocurrency of Choice for Scams'

Since the very early days, back when people learned how to create new cryptocurrencies or quickly build infrastructure models like digital asset trading platforms, many scams started to spawn frequently. According to the blockchain surveillance company Chainalysis, over the last two years fraud in the Ethereum ecosystem has run rampant and it's been the "cryptocurrency of choice for scams for

a variety of reasons," the company's latest Ethereum report highlights.

Also read: ***Cryptograffiti's Latest 'Running Bitcoin' Portrait Sees Auction Bids of Over $30K***

Scammers Flock to Ethereum Blockchain

The blockchain monitoring company Chainalysis has been releasing a series of reports concerning the recent "trends in crypto crime." The firm's report "Crypto Crime Series: Decoding Ethereum Scams" explains how ethereum (ETH) is the top choice for crypto-related scams throughout the ecosystem. In 2017, there was only $17 million worth of ETH stolen in scams but in 2018 roughly 0.01 percent of ETH was involved in swindles worth $36 million. "The number of scams declined through 2018, although those that remained were bigger, more sophisticated and vastly more lucrative," the Chainalysis report details.

"From late 2016 through the end of 2018, Chainalysis has identified over 2,000 scam addresses on Ethereum that have received funds from nearly 40,000 unique users — Scam activity increased dramatically in 2018 with nearly 75% of scamming activity taking place that year," the report explains.

There are four types of prevalent scams taking place within the Ethereum space – outright fraud, the ICO exit scam, a Ponzi product, and phishing attempts. Chainalysis also says the frequency and success rates of concepts like infection scams can change

over time.

“Innovative criminals executed more complex Ponzi and ICO exit scams that generated millions of dollars in income — These more sophisticated schemes dominated the second half of the year,” the crime series report summarizes.

The transformation of scam types and growth throughout 2017 and 2018.

From Giveaways to Ponzis – Etherscam’s Database Shows 924 Scams Are Currently Active

Chainalysis is not the only group watching the Ethereum network for scam related incidents. In fact, the website Etherscamdb.info which showcases a plethora of ETH-related scams can be seen by the entire cryptocurrency community. The Etherscam database has recorded 6,378 scams and 924 are currently active. The records show 1,975 scam-related ethereum addresses and out of the 6,378, roughly 5,454 are inactive. What also should be taken into consideration is that this information is only what Etherscam’s database can trace and there are lots of fraudulent acts that go unnoticed.

The vast list of cryptocurrency scams using ethereum.

Etherscam collects data on fake My Ether Wallet (MEW) websites, Punycode lookalike domains, phony exchanges, fraudulent impersonation giveaways, and ICO exit scams. Then there are Ponzi games tied to the Ethereum ecosystem with multi-level pyramid applications like Fomo 3D and Powh 3D. These platforms only make money by bringing new users into the fold and use all kinds of tactics like pay-per-bid methods, and multi-level marketing techniques. Back in March, the founder of Dapp Radar, Skirmantas Januskas gave a great breakdown of the Powh 3D Ponzi game and called it the "biggest pyramid scheme on Ethereum so far."

Even though there are many scams on the Ethereum network, there are various ways ETH users can protect themselves by not participating in blatant fraud. Veteran cryptocurrency participants will always illuminate the fact that holding your own keys, utilizing cold storage and multi-signature techniques are critical to keeping financial information safe. But there are many other methods that can be used like bookmarking official cryptocurrency websites, double-checking copy and pasted addresses, and not trusting "free giveaways" that will further help keep digital assets secure. As the Chainalysis crime series report details, blockchain criminals are executing petty crypto crimes far less than before, but the scams that still exist are becoming far more sophisticated.

What do you think about the number of scams attracted to the Ethereum network? Let us know what you think about this subject in the comments section below.

Image credits: Shutterstock, Ethereum logo, Pixabay, Brandon Arvanaghi, and Chainalysis.

Verify and track bitcoin cash transactions on our BCH Block Explorer, the best of its kind anywhere in the world. Also, keep up with your holdings, BCH, and other coins, on our market charts at Satoshi's Pulse, another original and free service from Bitcoin.com.

Promoted

KeepKey

KeepKey is a bitcoin hardware wallet that protects your money from hackers and thieves, while giving you convenient access.

Learn More

iPayYou

iPayYou is the worlds most useful bitcoin wallet. Buy/sell bitcoin, purchase gift cards, pay-by-email or Twitter, and more!

Learn More

SHARE THIS STORY:

TAGS IN THIS STORY

addresses, Brandon Arvanaghi, Chainalysis, Copy n Paste, Cryptocurrency, ETH, ether, Ethereum, Etherscam, Giveaways, ICO Exits, initial coin offerings, N-Featured, Phishing, Ponzi Games, scammer, scamming, Scams

RELATED

Bitcoin Early Adopters Build Seasteading Home off the Coast of Thailand

NEWS | 3 hours ago

Bitcoin Cash Supporter Convinces Chess.com to Accept BCH for

Memberships

NEWS | 24 hours ago

Jamie Redman

Jamie Redman is a financial tech journalist living in Florida. Redman has been an active member of the cryptocurrency community since 2011. He has a passion for Bitcoin, open source code, and decentralized applications. Redman has written thousands of articles for news.Bitcoin.com about the disruptive protocols emerging today.

In Case You Missed It

5 Featured Stories In 5 Minutes Digest five of the most interesting stories featured this week in our comprehensive Bitcoin news feed.

Latest Podcasts

Press releases

PR: LendaBit.com Launches Excellent P2P Service for Unverified Borrowers

Feb 25, 2019

PR: Roger Ver Joins Livenpay Advisory Board

Feb 25, 2019

PR: KuCoin Launches Platform 2.0 With Advanced API and Various Order...

Feb 21, 2019

Submit a Press Release

Latest Comments

GEORGE MARCOTTE

they need a new banking charter where its 100% reserve bank and the money is owned by the depositor...

Malta Might Be 'Blockchain Island' But Don't Try Opening a Crypto Bank Account

LJ

This keeps getting worse n worse and more dramatic. Will QuadrigaCX uses ever see their crypto/funds...

Report: Quadriga's 6 Cold Wallets Have Been Without Funds Since April 2018

GEGO KURA

ahahaha that's for sure! a lot of problems and all of them are critical

In the Daily: Coinbase Bug Bounty, Tradingview Crypto Dashboard, Bitfinex App Update

RISHI MAJUMDAR

Gold, Silver, Fiat all are used for corruption. Do we ban them too? After the PNB scam and the Vijay...

Indian Government Confirms Cryptocurrency Regulation in Final Stages

ALBERT ALBS

Expecting positive regulation. Instead of luring the citizens with crap regulation govt should think...

Indian Government Confirms Cryptocurrency Regulation in Final Stages

Your Ad Here

Most Popular

Most Commented This Week

00:00 00:00

McAfee to Be Portrayed in a Hollywood Movie, Travelling Entirely on Bitcoin Cash and More BCH News

The Bitcoin.com Wallet: Available on all platforms

> **https://t.co/UtJJm8netW** celebrates 2.5 million wallets created in less than a year. Get yours on **https://t.co/CNaJZzHtaZ pic.twitter.com/HJXJOVlhWy**
> — Bitcoin News (@BTCTN) July 18, 2018

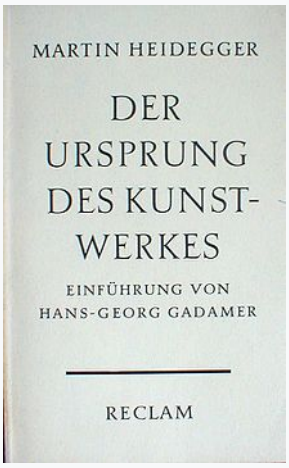
Download the **Bitcoin.com Wallet** right to your device for easy and secure access to your bitcoins.

Perfect for beginners, the Bitcoin.com Wallet makes using and holding bitcoins easy. No logins required.

The Origin of the Work of Art

The Origin of the Work of Art (German: *Der Ursprung des Kunstwerkes*) is an essay by the German philosopher Martin Heidegger. Heidegger drafted the text between 1935 and 1937, reworking it for publication in 1950 and again in 1960. Heidegger based his essay on a series of lectures he had previously delivered in Zurich and Frankfurt during the 1930s, first on the essence of the work of art and then on the question of the meaning of a "thing," marking the philosopher's first lectures on the notion of art.

The Origin of the Work of Art



Cover of the 1960 German edition

Author	Martin Heidegger
Original title	*Der Ursprung des Kunstwerkes*
Country	Germany
Language	German
Published	1950
Preceded by	*The Question Concerning Technology*
Followed by	*What Is Called Thinking?*

Content

In "The Origin of the Work of Art" Heidegger explains the essence of art in terms of the concepts of being and truth. He argues that art is not only a way of expressing the element of truth in a culture, but the means of creating it and providing a springboard from which "that which is" can be revealed. Works of art are not merely representations of the way things are, but actually produce a community's shared understanding. Each time a new artwork is added to any culture, the meaning of what it is to exist is inherently changed.

Heidegger begins his essay with the question of what the source of a work of art is. The artwork and the artist, he explains, exist in a dynamic where each appears to be a provider of the other. "Neither is without the other. Nevertheless, neither is the sole support of the other."[1] Art, a concept separate from both work and creator, thus exists as the source for them both. Rather than control lying with the artist, art becomes a force that uses the creator for art's own purposes. Likewise, the resulting work must be considered in the context of the world in which it exists, not that of its artist.[2] In discovering the essence, however, the problem of the hermeneutic circle arises. In sum, the hermeneutic circle raises the paradox that, in any work, without understanding the whole, you can't fully comprehend the individual parts, but without understanding the parts, you cannot comprehend the whole. Applied to art and artwork, we find that without knowledge of the essence of art, we cannot grasp the essence of the artwork, but without knowledge of the artwork, we cannot find the essence of art. Heidegger concludes that to take hold of this circle you either have to define the essence of art or of the artwork, and, as the artwork is simpler, we should start there.[3]

A Pair of Shoes[4] (1885), by Vincent van Gogh.

Artworks, Heidegger contends, are things, a definition that raises the question of the meaning of a "thing," such that works have a thingly character. This is a broad concept, so Heidegger chooses to focus on three dominant interpretations of things:

1. Things as substances with properties,[5] or as bearers of traits.

2. Things as the manifold of sense perceptions.[6]

3. Things as formed matter.[7]

The third interpretation is the most dominant (extended to all beings), but is derived from equipment: "This long familiar mode of thought preconceives all immediate experience of beings. The preconception shackles reflection on the Being of any given being."[8] The reason Heidegger selects a pair of peasant shoes painted by Vincent van Gogh is to establish a distinction between artwork and other "things," such as pieces of equipment, as well as to open up experience through phenomenological description. This was actually typical of Heidegger as he often chose to study shoes and shoe maker shops as an example for the analysis of a culture.[*citation needed*] Heidegger explains the viewer's responsibility to consider the variety of questions about the shoes, asking not only about form and matter—what are the shoes made of?—but bestowing the piece with life by asking of purpose—what are the shoes for? What world do they open up and belong to?[9] In this way we can get beyondcorrespondence theories of truth which posit truth as the correspondence of representations (form) to reality (matter).

Next, Heidegger writes of art's ability to set up an active struggle between "Earth" and "World."[10] "World" represents meaning which is disclosed, not merely the sum of all that is ready-to-hand for one being but rather the web of significant relations in whichDasein, or human being(s), exist (a table, for example, as part of the web of signification, points to those who customarily sit at it, the conversations once had around it, the carpenter who made it, and so on - all of which point to further and further things). So a family unit could be a world, or a career path could be a world, or even a large community or nation. "Earth" means something like the background against which every meaningful "worlding" emerges. It is outside (unintelligible to) the ready-to-hand. Both are necessary components for an artwork to function, each serving unique purposes. The artwork is inherently an object of "world", as it creates a world of its own; it opens up for us other worlds and cultures, such as worlds from the past like the ancient Greek or medieval worlds, or different social worlds, like the world of the peasant, or of the aristocrat. However, the very nature of art itself appeals to "Earth", as a function of art is to highlight the natural materials used to create it, such as the colors of the paint, the density of the language, or the texture of the stone, as well as the fact that everywhere an implicit background is necessary for every significant explicit representation. In this way, "World" is revealing the unintelligibility of "Earth", and so admits its dependence on the natural "Earth". This reminds us that concealment (hiddenness) is the necessary precondition for unconcealment (aletheia), i.e. truth. The existence of truth is a product of this struggle—the process of art—taking place within the artwork.

Heidegger uses the example of a Greek temple to illustrate his conception of world and earth. Such works as the temple help in capturing this essence of art as they go through a transition from artworks to art objects depending on the status of their world. Once the culture has changed, the temple no longer is able to actively engage with its surroundings and becomes passive—an art object. He holds that a working artwork is crucial to a community and so must be able to be understood. Yet, as soon as meaning is pinned down and the work no longer offers resistance to rationalization, the engagement is over and it is no longer active. While the notion appears contradictory, Heidegger is the first to admit that he was confronting a riddle—one that he did not intend to answer as much as to describe in regard to the meaning of art.

Influence and criticism

A main influence on Heidegger's conception of art wasFriedrich Nietzsche. In Nietzsche's *The Will to Power*, Heidegger struggled with his notions about the dynamic of truth and art. Nietzsche contends that art is superior to truth, something Heidegger eventually disagrees with not because of the ordered relationship Nietzsche puts forth but because of the philosopher's definition of truth itself, one he claims is overly traditional. Heidegger, instead, questioned traditional artistic methods. His criticism of museums, for instance, has been widely noted. Critics of Heidegger claim that he employs circuitous arguments and often avoids logical reasoning under the ploy that this is better for finding truth. (In fact, Heidegger is employing a revised version of the phenomenological method; see the hermeneutic circle). Meyer Schapiro argued that the Van Gogh boots discussed are not really peasant boots but those of Van Gogh himself, a detail that would undermine Heidegger's reading.[11] During the 1930s mentions of*soil* carried connotations which are lost for later readers (see Blood and Soil). Problems with both Heidegger and Schapiro's texts are further discussed inJacques Derrida's *Restitutions - On Truth to Size*[12] and in the writing ofBabette Babich. A recent refutation of Schapiro's critique has been given byIain Thomson (2011). Heidegger's notions about art have made a relevant contribution to discussions on artistic truth. Heidegger's reflections in this regard also affected architectural thinking, especially in terms of reflections on the question of dwelling. Refer to the influential work in architectural phenomenology of: Christian Norberg-Schulz, *Genius Loci, Towards a Phenomenology of Architecture* (New York: Rizzoli, 1980); and see also a recent treatment of the question of dwelling inNader El-Bizri, 'On Dwelling: Heideggerian Allusions to Architectural Phenomenology', *Studia UBB. Philosophia*, Vol. 60, No. 1 (2015): 5-30.

See also

- Being and Time
- Deconstruction
- Hermeneutics
- Postmodernism

Bibliography

Primary literature

- Heidegger, Martin. *Off the Beaten Track* (Cambridge: Cambridge University Press, 2002). Translation of*Holzwege* (Frankfurt: Vittorio Klostermann, 1950),

volume 5 in Heidegger's *Gesamtausgabe*.

- Heidegger, Martin. *Basic Writings,* "On the Origin of the Work of Art." 1st Harper Perennial Modern Thought Edition., ed. David Farrell Krell (New York: HarperCollins, 2008, pg. 143-212).

Secondary literature

- Renate Maas, Diaphan und gedichtet. Der künstlerische Raum bei Martin Heidegger und Hans Jantzen, Kassel 2015, 432 S., ISBN 978-3-86219-854-2.
- Harries, Karsten. "Art Matters: A Critical Commentary on Heidegger's Origin of the Work of Art",Springer Science and Business Media, 2009
- Babich, Babette E. "The Work of Art and the Museum: Heidegger, Schapiro, Gadamer," in Babich, 'Words In Blood, Like Flowers. Philosophy and Poetry, Music and Eros in Hoelderlin, Nietzsche and Heidegger' (SUNY Press, 2006)
- González Ruibal, Alfredo. “Heideggerian Technematology.” All Things Archaeological. Archaeolog, November 25, 2005.
- Inwood, Michael. *A Heidegger Dictionary.* Malden, Massachusetts: Blackwell Publishers Inc., 1999.
- Haar, Michel. “Critical Remarks on the Heideggarian reading of Nietzsche.”*Critical Heidegger*. London and New York: Routledge, 1996.
- Dahlstrom, Daniel O. “Heidegger’s Artworld.”*Martin Heidegger: Politics, Art, and Technology.* New York: Holmes & Meier Publishers, Inc., 1995.
- Van Buren, John. *The Young Heidegger*. Indianapolis, Indiana: Indiana University Press, 1994
- Guignon, Charles. *The Cambridge Companion to Heidegger.* New York, New York: Cambridge University Press, 1993.
- Bruin, John. “Heidegger and the World of the Work of Art.”*The Journal of Aesthetics and Art Criticism*, Vol. 50, No. 1. (Winter, 1992): 55-56.
- Lacoue-Labarthe, Philippe. *Heidegger, Art and Politics: The Fiction of the Political* Oxford: Blackwell Publishing, 1990.
- Derrida, Jacques. *Restitutions of the Truth in Pointing ['Pointure'].* Trans. Geoffrey Bennington & Ian McLeod, Chicago & London: Chicago University Press, 1987.
- Stulberg, Robert B. “Heidegger and the Origin of the Work of Art: An Explication.”*The Journal of Aesthetics and Art Criticism*, Vol. 32, No.2. (Winter, 1973): 257-265.
- Pöggeler, Otto.”Heidegger on Art.” *Martin Heidegger: Politics, Art, and Technology.* New York: Holmes
- Schapiro, Meyer. 1994. “The Still Life as a Personal Object - A Note on Heidegger and van Gogh”, ”Further Notes on Heidegger and van Gogh”, in: Theory and Philosophy of Art: Style, Artist, and Society, Selected papers 4, New York: George Braziller, 135-142; 143-151.
- Thomson, Iain D. (2011). *Heidegger, Art, and Postmodernity*. Cambridge University Press. ISBN 1-107-00150-1.

Notes

1. ^ Heidegger (2008), p. 143.
2. ^ Heidegger (2008), p. 167.
3. ^ Heidegger (2008), p. 144.
4. ^ Vangoghmuseum.nl
5. ^ Heidegger (2008), pp. 148–151.
6. ^ Heidegger (2008), pp. 151–152.
7. ^ Heidegger (2008), pp. 152–156.
8. ^ Heidegger (2008), p. 156.
9. ^ Heidegger (2008), pp. 146–165.

References

- Heidegger, Martin; trans. David Farrell Krell (2008). "The Origin of the Work of Art". *Martin Heidegger: The Basic Writings*. New York: HarperCollins.
- Thomson, Iain D. (2011). *Heidegger, Art, and Postmodernity*. Cambridge University Press. ISBN 1-107-00150-1.

External links

- Thomson, Iain, "Heidegger's Aesthetics" *The Stanford Encyclopedia of Philosophy* (Summer 2011 Edition), Edward N. Zalta (ed.)

Last edited on 3 October 2018, at 02:12

WIKIPEDIA

Content is available under CC BY-SA 3.0 unless otherwise noted.

Terms of Use • Privacy • Desktop

The State of Ethereum 2.0

Executive Summary

Research and development of Ethereum 2.0 continues at a rapid pace, with a testnet of the beacon chain scheduled for release in March of this year. However, a number of coordination problems are slowing implementation and the public's view of what will be delivered and when differs from reality. In this paper, we outline these problems and propose solutions for how Kyokan and the Moloch DAO can help fix them.

Overview

"Ethereum 2.0" refers to a set of specifications that will dramatically improve the performance characteristics of the Ethereum blockchain. As of this writing, it does so by merging and improving upon research from two older specifications: "Casper," which introduces a proof-of-stake consensus mechanism, and "sharding," which introduces the splitting of

transactions across a number of “shards” secured by the main chain. These specs confer the following benefits to Ethereum users:

1. Proof-of-stake removes the need to invest in equipment and burn electricity to secure the chain. Furthermore, it improves Ethereum’s finality characteristics by making certain types of 51% attacks dramatically more expensive and reducing reliance upon mining cartels to secure the chain.
2. Sharding improves the Ethereum network’s maximum transactions per second by orders of magnitude.

To determine the current state of the project, we interviewed the researchers and implementers working on the protocol.

Interview Methodology

We interviewed the following implementation teams via video call:

- Nimbus (Status)
- Lodestar (ChainSafe Systems)
- Artemis (PegaSys)
- Lighthouse (Sigma Prime)
- Prysm (Prysmatic)

Each implementation team was asked questions encompassing the following functional areas:

1. Team status;
2. Development status;
3. Roadmap;
4. Launch considerations;
5. Dependencies;
6. Comparisons to other implementation teams; and
7. Recommendations.

We also interviewed Danny Ryan, one of the core Ethereum Foundation researchers working on the project, via phone.

Observations and Potential Consequences

We now present our findings from the interviews described above. Quotes from individual interviewees are placed in quotation marks, and are reproduced verbatim.

Implementation Teams are Committed, But Funding Is A Concern

We asked each team their likelihood of and under what conditions they would give up development. All of the implementation teams we spoke to were committed to seeing Ethereum 2.0 through to completion as long as funding exists to continue development. This is an important point to underscore, as it implies two things. First, the implementation teams care deeply about shipping Ethereum 2.0, and are willing to weather the frustrations and problems that crop up along the way. Specifically, we received answers such as “We’d be dead before giving up.” and “This is going to happen no matter what.” in response to our questions around what it’d take for them to give up. However, the implementation teams are not immune to market realities. If EF funding dries up, or the larger entities funding individual implementation efforts (e.g., ConsenSys or Status) turn off funding, then there is a possibility that teams will be forced to find other work.

The Spec Continues To Churn, But It’s Getting Better

The Ethereum 2.0 spec has experienced a high level of churn over the past year. According to one person we interviewed, the spec has “entirely changed since the middle of last year” and continues to undergo regular “surgery” as issues are found and ironed out by the research team. Every aspect of the spec is subject to change. For example, until recently the names of important data structures were changing “emergently” - that is, a researcher would update their mental model of what a particular data structure represented, and change the spec accordingly without consideration of the effects that such a change would have on implementation efforts. For example Issue #358, 35 individual fields were renamed, yet the GitHub discussion received no participation from implementers. This has forced implementation teams to redo large swathes of work as the spec shifts under them - leading to frustration, wasted time, and in some cases a reduction of resources allocated to Ethereum 2.0 projects until the spec stabilizes.

There have been several promising developments over the past few weeks to reduce churn. First, according to the research team there is an ongoing effort to start versioning specific areas of the spec in order to make clear which areas are stable enough for implementation and which are still being actively researched (this first release was published the day this report was published for internal review). Second, the research team believes that “changes are slowing down” and that “deep reorgs” of the spec itself should be rarer now. A culture shift is occurring as well: the impact a particular change will have on implementation teams is now considered as part of new spec proposals (see this issue as an example). As a result of these developments, implementation teams unanimously agree that the spec in its current state is implementable.

Implementation Teams Do Not Push Back Against Researchers

Most implementation teams do not push back against the research team. They stated two reasons for this: implementers either feel unqualified to push back, or they feel like the chances

of successfully pushing back are too low to warrant doing so. These feelings are reinforced by how the research team describes the changes they have inserted into the spec: changes are usually described “clearly better” and “hard to push back against” given the qualifications of the people proposing the changes. While it is true that some areas of the spec can only be critiqued by a select few individuals, that feeling of “research exclusivity” currently extends to the entire spec as well as overall Ethereum 2.0 plan of execution.

The Definition Of Done Varies From Team To Team

All of the implementers we spoke to are working towards the testnet launch in March. What that launch looks like - and what happens afterwards - varies significantly from team to team. For example, it is unlikely that day one of the testnet will support inter-node peering because the peer protocol specification has not been fully accepted yet. Some teams have inter-node operability as a specific goal of the testnet launch, others do not. As a result, it is difficult to say with clarity what the actual deliverable in March will consist of.

Things become increasingly hazy past the testnet. None of the teams were able to estimate when Phase 2 - that is, the complete Ethereum 2.0 specification including cross-shard operations and EVM - would be mainnet-ready. Since some teams received grant money for the beacon chain specifically, it is likely that implementation teams will need additional funding to complete the spec.

Finally, only one of the teams we interviewed had user adoption - specifically, “100 validators staking using [their] software” - as one of their stated goals. The others were focused on completion of their respectively committed parts of the spec.

What Comes After Ethereum 2.0 Is Unclear For Implementers

Many teams expressed concerns around what comes next for their respective businesses after successfully delivering Ethereum 2.0. None of the teams we spoke to had a clear answer for how they would monetize post-implementation, so securing funding for continued maintenance (particularly if ETH continues to drop in price) is of major concern to implementation teams.

There Is No Ethereum 2.0 Lead

From an organizational perspective, no single person is responsible or accountable for making sure that Ethereum 2.0 lands and lands in a way that matters to the Ethereum community at large. Danny Ryan fills part of this role. He took it upon himself to be the liaison between the implementation and research teams, and his efforts are highly appreciated. Access to Danny isn’t consistent across implementation teams, however - some expressed that they wished that they could have more access to him.

Ethereum 2.0's Narrative Is Controlled By People Outside The R&D Process

Consider James Prestwich's popular post "What To Expect When ETH's Expecting." It includes claims like the following:

- "The tools and contracts we've written for ETH1.X will likely need to be completely redesigned and rewritten for ETH2.0."
- "Phase 1 doesn't have anything particularly interesting in it. Fundamentally it's a bootstrapping phase for crosslinking, and the symmetric mechanism by which shards reference the beacon chain. The designers seem confident that these mechanisms will work."
- "Interestingly, Phase 0 implementation has happened concurrently with specification. Even today, less than three months from testnet, the Phase 0 specification changes regularly. This implies that future ETH2.0 phases will have extremely high variance in development time. While optimists have told me six months, it is easy to see Phase 1 taking 12–18 months of development after Phase 0 enters testing."
- "[Beyond eWASM, EVM2, and storage rent] we don't know what to expect from Phase 2. It's still in very early stages of research and includes several major unsolved problems. Given the informal specification and development process, as well as Phase 2's expanded scope over Phase 1, it doesn't seem reasonable to suggest that Phase 2 could launch before 2020. Which is to say, while ETH2.0 may launch this year, don't expect ETH2.0 to support asset transfer or smart contracts until at least 2020."
- "We have very little information about ETH2.0's communication model. We know that it can't provide cross-shard contract calls without sacrificing almost all scaling benefits. I won't blame you if you stop reading here, as Phase 4 only has a mind map and a few vague links. A non-obvious consequence of this is that ETH2.0 will not provide significant scaling benefits to complex smart contract systems until Phase 4. Until then, contracts wishing to interact with other contracts must cohabitate a shard and are limited to the speed and scale of that shard."

These are concrete details about how developers can expect to make use of Ethereum 2.0. The post also includes plenty of technical detail about the spec, but as an Ethereum developer the most relevant information contained therein is about how the spec will impact my work and when to expect scalability improvements. Media created by the implementation teams and the EF, in contrast contrast, tends to focus instead on new research or the completion of specific pieces of the spec. Consider the following outline of Prysmatic's Development Update #20[1]:

[1] This isn't limited to Prysmatic specifically - the majority of public-facing media from implementers and researchers alike focuses on the tech. A Prysmatic development update was chosen because Prysmatic has the highest volume of public media.

- Latest Research
    - Phase 0 Validator Client Responsibilities
- Merged Code, Pull Requests, and Issues
    - State Transition Block Processing E2E Testing Complete
    - State Transition Epoch Processing Integration Complete
    - Implementing Deposit Listener For The Validator Deposit Contract
    - Implementer Validator Deposits Trie
- Upcoming Work
    - GHOST Fork-Choice Rule for the Ethereum Beacon Chain
    - Full End-to-End Testing of Beacon Chain With Validator Deposits
    - Deprecating Our Solidity Contract to Vyper
    - Creating the Beacon Chain's Transactions Pool
    - Refactor Validator Client
    - Validator Private Key Management and Other Secrets
- Misc
    - Ethereum 2.0 Implementers Call Jan 17, 2019
    - Blog Post on Ethereum 2.0 (which includes a link to Prestwich's post above)

The things that drive Ethereum 2.0's "narrative" - i.e., when it'll ship, what it'll be useful for, and how developers can use it - is driven more by posts like Prestwich's than Prysmatic's since the information is more directly relevant to the day-to-day work of Ethereum's users. We commend the Ethereum 2.0 teams for their commitment to transparency, and obviously want technically-focused updates such as the one above to continue. However, if nobody from the research or implementation teams provides additional context around when Ethereum 2.0 will be ready and what it will look like when it is, others will continue to step in and do it for them. As a result, it will be difficult for correct expectations to be set and lived up to.

Addendum: A conversation of Ethereum community members pointed us towards this high level outline of Ethereum's roadmap prepared by EthHub. The link to the official sharding roadmap, while instructive, isn't as helpful for setting the expectations of platformer developers who want to know what each phase of the spec means for them.

Open Questions

What Does The Community Expect?

Currently, the narrative around when Ethereum 2.0 will be delivered and what it will look like is somewhat like this:

- Ethereum 2.0 is coming, and will be ready for public use soon.
- Ethereum 2.0 will be on testnet starting in March.
- Ethereum 2.0 will solve the majority of Ethereum's scalability concerns.

Given what we know after talking to both the research team and the implementation teams, it's clear that delivery of an Ethereum 2.0 implementation with real utility to dApp developers is not feasible for at least another year and a half. From our understanding, the deliverables included in each phase of the Ethereum 2.0 roadmap are as follows[2]:

- **Phase 0:** The beacon chain.
- **Phase 1:** Shards without the EVM.
- **Phase 2:** EVM on shards and cross-shard communication.

For developers to derive the same level of utility from Ethereum 2.0 as they did on Ethereum 1.0, phase 2 must be delivered.

Furthermore, for the later phases of Ethereum 2.0's rollout it is possible that new research will invalidate or otherwise reshape the roadmap profoundly. It is unclear to us whether or not the Ethereum community at large is aware of this. A gap between what the community expects and what is actually delivered could hurt implementation efforts substantially by reinforcing the narrative that Ethereum will not be able to scale and cause new developers to begin exploring other blockchains.

Were Implementers Consulted When Designing The Rollout?

It is unclear to us how much, if any, implementer input was included in the decision to roll out Ethereum 2.0 in phases and what goes into each phase. While we understand the value of a phased deployment process - i.e., that it gives new technology like proof-of-stake time to "burn in" in a quasi-production environment - it stands to reason that the individuals responsible for implementing each phase are some of the most qualified people to design them in the first place. This includes which technology is introduced when, as well as when each phase is set to be delivered. If implementers were not consulted, would the launch of the beacon chain be a good time to reset and bring implementers into the process?

Would Making Danny Ryan Official "Ethereum 2.0 Lead" Help?

Many of the frustrations around Ethereum 2.0 stem from a lack of coordination between the research and implementation teams. The protocol consists of numerous disparate components that must be integrated as part of a plan spanning several years. Until Danny Ryan assumed the role of coordinator, there was no single person to whom both researchers and implementers alike could turn to to oversee that integration. Danny has already demonstrated his value as a lead. His name came up repeatedly during our interviews as someone that implementers would

[2] Note that the phases described on the Sharding Roadmap document are different. The development phases described to us during our interviews indicated that those phases are no longer canonical.

like to see more of, and his efforts on the early versions of the specification show that he is knowledgeable enough as a researcher to oversee the project.

It's important to be clear about what 'lead' means in this context. We are using 'lead' to mean the single person who is:

- Accountable for making sure that Ethereum 2.0 lands.
- Accessible to all implementation teams and researchers.
- Empowered with veto authority to act as a tiebreaker for critical decisions.
- Empowered with delegation authority to make sure that the right people are solving the right problems.

This is most definitely a centralization of control. However, given the role he is already filling empowering Danny with official leadership seems fitting, and could make sure that the entire project is integrated smoothly.

Recommendations

Include "Product Context" In Public-Facing Media

Given the importance of Ethereum 2.0 to the success of the network, clearly communicating what will be delivered and when as well as how to prepare for the release of Ethereum 2.0 is paramount. To make media produced by Ethereum 2.0 teams and researchers more relevant to the community and regain control of the Ethereum 2.0 narrative, we recommend clearly articulating the following things with new public updates:

1. How the latest update will impact developers.
2. How roadmap changes might impact Ethereum 2.0's timeline or roadmap.
3. Areas where research or product churn is expected.

Including the above things will go a long way towards returning control of the Ethereum 2.0 narrative to those working on it.

Provide Clear Avenues For Continued Funding

We believe that incentivizing long-term, continuous development on Ethereum 2.0 clients is critical to a successful Ethereum 2.0 launch. The source of continued funding for implementation is ambiguous and a source of worry. If the Ethereum Foundation or an alliance of other interested parties pooled money and provided clear funding amounts with associated timelines, it would remove many worries around how client projects will continue to fund maintenance and new features once Ethereum 2.0 is launched.

Rigorously Define And Enforce A Formal Standards Process

The coordination problems inherent to implementing a spec while it is being defined are exacerbated by the lack of a formal standards process. By developing and publishing specifications, the Ethereum Foundation is acting as the de-facto standards body for Ethereum 2.0. As such, defining a formal process through which research can go from proposal to implementable can further reduce the amount of churn around the spec. There are numerous standards bodies from whom the EF can draw examples, however we recommend a variant of ECMA'S TC39 Standards Process. Our reasoning is as follows:

1. The TC39 process is open, and embraces modern development practices such as pull requests on GitHub that contributors are already familiar with.
2. The TC39 process bakes acceptance tests and reference implementations into the process itself.
3. The TC39 process is more digestible and has less overhead than other standards processes.
4. The TC39 process favors incremental releases of new standards on an set cadence.
5. The TC39 process has a track record of success. As a result of the TC39 process, the JavaScript ecosystem successfully recovered from 10 years of language stagnation.
6. Many of Ethereum's developers come from a JavaScript background, and as such are already familiar with the TC39 process (specifically, proposal "stages") via Babel.

We recommend introducing, at the very least, the concept of "stages" from the TC39 process. For the unfamiliar, TC39 proposals go from stage 0 ("strawman") to stage 4 ("complete"), after which they are ratified as new standards at an annual meeting of TC39 members. The objective of having proposal stages is to make it extremely clear how ready an individual proposal is for implementation. Furthermore, since test vectors and reference implementations are requirements to transition from one phase to another, dialogue between researchers and implementers is encouraged. While an implementer may not be qualified to comment on the specifics of an individual algorithm, for example, they *are* qualified to comment on how that algorithm gets implemented. Under TC39, both the research and the implementation would be required to transition from stage 3 to 4.

How Kyokan/Moloch Can Help

Kyokan is a blockchain-native software consultancy based in the bay area. In the past, we have worked with MetaMask, SpankChain, Cosmos, Dfinity, and Uniswap. In addition, we received a grant from the Ethereum Foundation to build an implementation of Plasma MVP, which is currently preparing for mainnet launch. Our team has significant experience shipping production software at prominent consumer and enterprise tech companies.

Moloch is a grant-making DAO / Guild and a radical experiment in voluntary incentive alignment to overcome the "tragedy of the commons". Our objective is to accelerate the development of public Ethereum infrastructure that many teams need but don't want to pay for on their own. By pooling our ETH and ERC20 tokens, ETH investors and teams building on Ethereum can collectively fund open-source work we decide is in our common interest.

Kyokan, with funding from Moloch and others, is positioned to provide support for the ETH 2.0 effort in the following ways:

- Prepare reports and analysis, like this one, to inform the community of ETH 2.0 progress
- Evaluate the internal processes of the ETH 2.0 R&D effort
- Help develop organizational structure as needed
- Assist in coordinating standards across teams
- Help plan the development roadmap
- Provide launch coordination and prepare clients for production release
- Help with developer recruitment

Moloch is positioned to provide support for the ETH 2.0 effort as follows:

- Provide additional funding for ETH 2.0 teams
- Funding key hires to provide cross-team support
- Funding open-source tools (e.g. testing) to help 2.0 development

Conclusion

The ETH 2.0 effort may be unique, but the challenges it faces are generally what one might expect to observe in an emergently organized R&D effort of 8+ researchers and 50+ developers. With stronger coordination through leadership, a standards process, a well-communicated shared roadmap, and funding security, the ETH 2.0 effort is set to accelerate and meet the expectations of the Ethereum community.

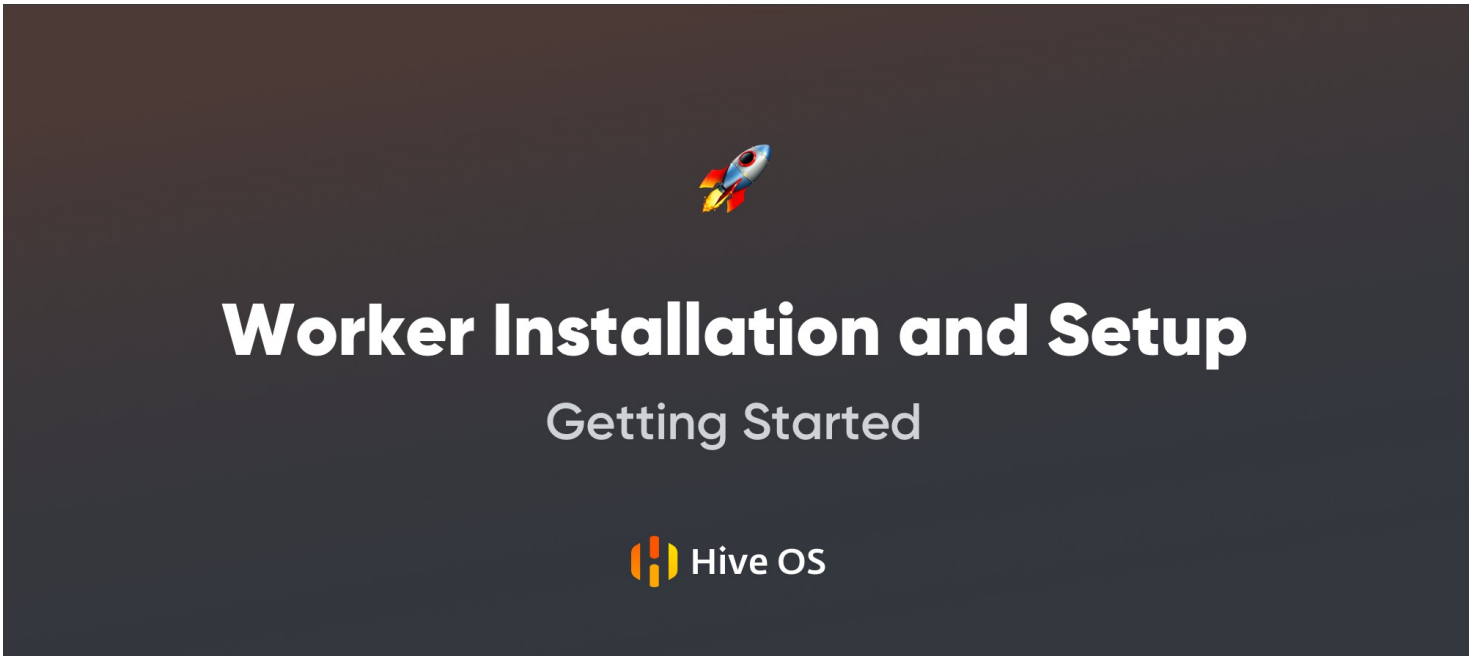
We're already seeing the beginnings of this acceleration taking place. In December, Vitalik (non-giver of ETH) said "YOLO" and gave a 1000 ETH grants to each of the Prysmatic, Lighthouse, and Lodestar teams. Another prominent ETH investor followed Vitalik and contributed 2,800 ETH to Prysmatic, helping Preston Van Loon leave Google to join the ETH 2.0 effort full-time. As more community members step up to share responsibility for ETH 2.0 delivery, we anticipate even greater results. We're all in this together.

Disclaimer

Funding for Kyokan's efforts in preparing this report is anticipated to come from the Moloch DAO, but has also been guaranteed personally by Ameen Soleimani, should there be complications. The report was authored primarily by Matt Slipper and Dan Tsui of Kyokan.

Getting Started with Hive OS—Worker Installation and Setup

John Ganchak
Aug 14, 2018 · 7 min read



Hive OS is an all-in-one monitoring and management tool for your mining rigs. Whether its a single rig or several thousands, you and your team can easily manage them all from a single dashboard.

In this article we'll walk you through the first time installation process and explain what different installation types there are and how to easily set up your rigs and connecting them to your account dashboard.

Creating An Account

Before installing Hive OS on your rig, we recommend creating an account first, or logging into your existing one. Make sure to create a secure password.

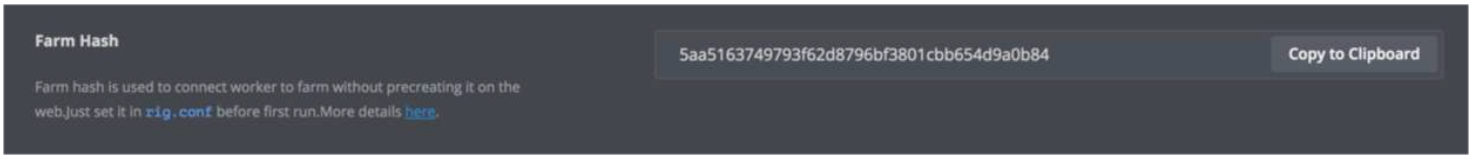
> *We strongly suggest setting up Two Factor Authentication (2FA) for additional account security. You can find these settings by clicking on your user name in the top right corner and then going to the Account tab. Scroll down to the Two-factor Authentication option and switch 2FA on then follow the onscreen instructions carefully.*

Adding Your Workers

As soon as you're done setting up your account, it's time to connect your rigs to the dashboard. GPU rigs and ASICs are uniformly referred to as workers. You will have two options of connecting your workers, via **Farm Hash** or via **manual setup**. Farm Hash is used for connecting your workers to a Farm without pre-creating the rig in the dashboard. This is our new and fast method of connecting a worker to a Farm, so we recommend this setup method for most users. We will go into more details on Farms and how to use them in our next articles.

1. Farm Hash

Each Farm has its unique Farm Hash. You can find your Farm Hash by going to your Farm's Settings tab. Once you write the installation image, you may then add your FARM_HASH to the rig.conf file which you will find in the root folder of the image. We'll explain this step in detail below.

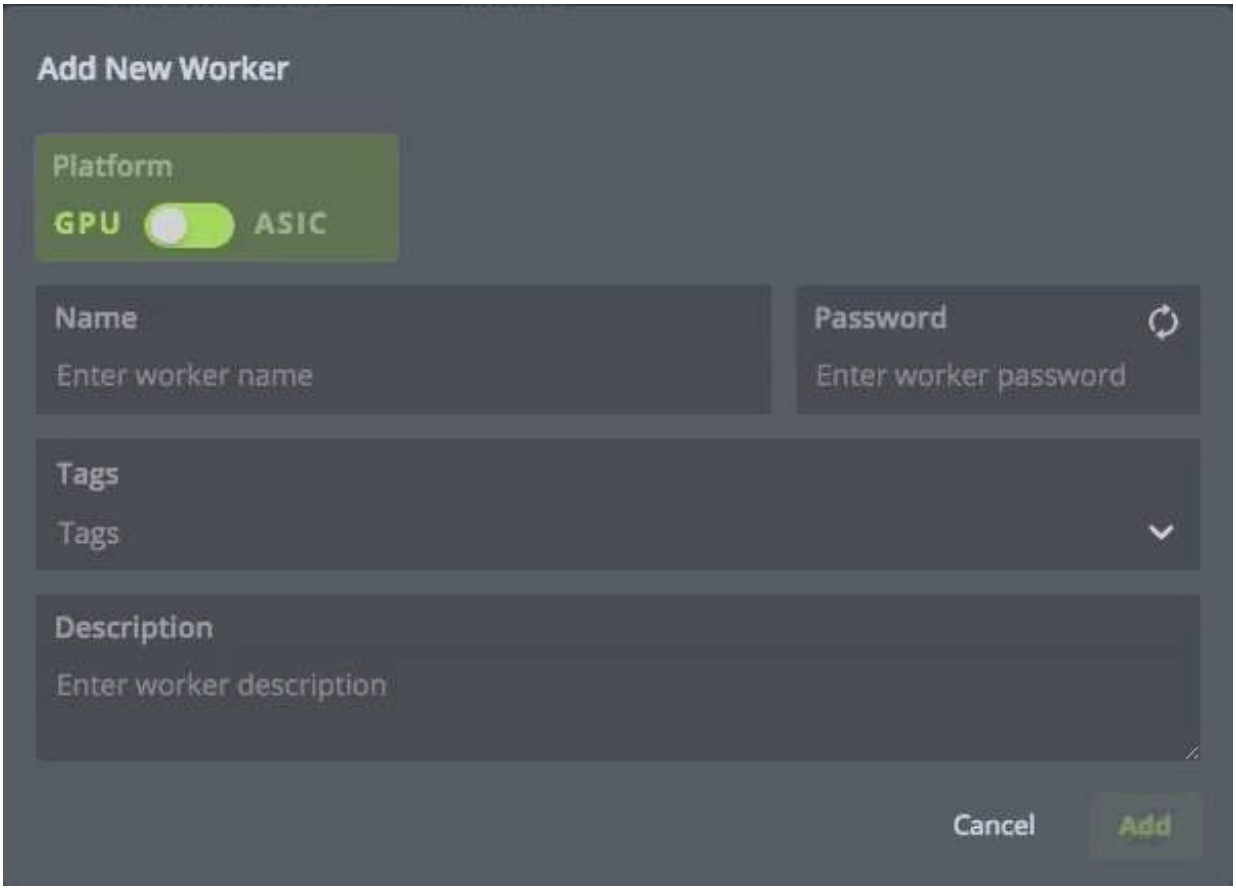


Farm Hash can be effectively used with Hive Flasher for bulk rig installations. More details on Hive Flasher are available here.

2. Manual Setup

Users that have previously used Hive OS will be familiar with this option of connecting their worker to the dashboard. It involves using a rig ID and a password for each miner to be configured. Although it's a bit more tedious than connecting workers via Farm Hash, we left it for our old school users' convenience.

Click on the plus in the top right corner and choose Add Worker option.



A window, Add New Worker, will pop up with the following fields:

1. Choose between **GPU** or **ASIC** type.
2. **Name**—your rig name. This can be anything. For example, rig01; garage_rig; etc. or leave it blank.
3. **Password**—your miner's password. You can enter a convenient password for you, or generate one by clicking the double arrow button instead.
4. **Tags**—custom tags to help you logically separate projects by filters for various farms and workers. Tags can be created by going to the Settings tab.
5. **Description**—your rigs description. This is for your convenience only. For Example: *The rig at my parent's garage*; *Store room rig*; *Rig on Park St. 251, that I only use for mining Monero*; etc.
6. Once done, click the **Add** button.

You will now see your rig added to the list of workers, but first you will need your rig ID. After you pre-created your worker, you will be forwarded to the worker's dashboard. Go to the worker's Settings tab and you should see the rig ID and the Password.

The ID of the rig and the password will be needed during the initial installation and first boot, in case you opted for this option instead of Farm Hash, so we recommend writing it down.

Choosing An Installation Type

Hive OS can be installed on both GPU rigs and ASICs as well.
Below we will describe the different types of installations:

- GPU—installs the OS unto GPU based rigs
- ASIC—installs the OS unto ASIC miners

Downloading The Image

Go to the download page to get the latest version of Hive OS. You can download the image from our website as a .zip file or via .torrent if you prefer. You will also have the option of downloading Hive OS for ASICs or our Bulk Installation tool.

> *We recommend installing the OS image to an SSD. SSDs are much more reliable and we advise using them in production environments. Because many users still prefer using a USB flash drive, we have the logs turned off by default. If you installed the OS on an SSD, you can optionally turn logging back on by running the* logs-on *command after installation.*

Check the Flash drive, SSD, HDD forum thread for additional information and also visit our Common booting problems forum thread for more details.

GPU Installation

Writing Disk Image

You will need to write Hive OS image onto an SSD. Although many user prefer to use USB drives, we recommend opting to an SSD instead. Start by extracting the image from the .zip file first and then writing the .img file onto a drive.

Windows user can write the image using HDD Raw Copy Tool, Win32 Disk Imager, Rufus or Etcher.

MacOS and **Linux** users can do it with ease using Etcher, or do it manually via

command line as described below.

> *Here's an example of the command:*
>
> `dd if=hive-xxx.img of=/dev/sdb bs=10M status=progress`
>
> *But be attentive when finding out the output disk* `of` *. Use* `fdisk -l` *command to list your partitions and select the correct one.*

After the image is flashed you will discover a newly created drive in your system where you will be able to pre-configure your worker with either Farm Hash or it's ID and password. Find *rig-config-example.txt* on HIVE drive and open it with a .txt editor. You can use the integrated text editors on Windows, MacOS and Linux or download a free alternative. For example, Notepad++ for Windows or Sublime Text for MacOS and Linux.

Now choose one of the two options below:

Optional Step—Farm Hash

Once the image copy is complete, you can go to your drive in Windows, Linux or Mac and find *rig-config-example.txt* file in the root folder. Here's how it looks:

```
# THIS IS A STARTING EXAMPLE, REAL CONFIG IS IN rig.conf
# Normally the rig will ask for password at first run.
# Optionally you can put rig ID and password and Save As to "rig.conf" for a fresh start

HIVE_HOST_URL="https://api.hiveos.farm"

# Find out your hash in farm's settings on the web
# The rig will autoregister itself in your account after the first run
FARM_HASH=<your farm hash goes here>

# Password used for the rig
RIG_PASSWD=

# If you know rig id before creation you can set it here leaving FARM_HASH blank
RIG_ID=

# Disable GUI (x server), uncomment to disable it
#X_DISABLED=1

# Linux system language, like zh_CN.UTF-8, pt_PT.UTF-8, de_DE.UTF-8
#SYSTEM_LANG=en_US.UTF-8
```

The contents of rig-config-example.txt file

Enter your Farm Hash in the `FARM_HASH=` field by copying the value from your Settings tab. Here's how the field should look like:

```
FARM_HASH=f019745da6ba65630b28ef3c92608e7022b4bf76
```

No need to set RIG_ID or RIG_PASSWD in this case. That’s it, just save your config file and rename it into *rig.conf*. Proceed by finishing the image installation and boot your worker. It will connect to the dashboard automatically.

Optional Step—Manual Setup

Once the image copy is complete, you can go to your drive in Windows, Linux or Mac and find *rig-config-example.txt* file in the root folder. Here’s how it looks:

```
# THIS IS A STARTING EXAMPLE, REAL CONFIG IS IN rig.conf
# Normally the rig will ask for password at first run.
# Optionally you can put rig ID and password and Save As to "rig.conf" for a fresh start

HIVE_HOST_URL="https://api.hiveos.farm"

# Find out your hash in farm's settings on the web
# The rig will autoregister itself in your account after the first run
FARM_HASH=

# Password used for the rig
RIG_PASSWD=

# If you know rig id before creation you can set it here leaving FARM_HASH blank
RIG_ID=

# Disable GUI (x server), uncomment to disable it
#X_DISABLED=1

# Linux system language, like zh_CN.UTF-8, pt_PT.UTF-8, de_DE.UTF-8
#SYSTEM_LANG=en_US.UTF-8

# Set system user password as rig's. Default is "1"
#SET_RIG_PASS=1
```

The contents of rig-config-example.txt file

Find and fill in the two fields:

```
RIG_PASSWD=

RIG_ID=
```

That’s it, just save your config file and rename it into *rig.conf*. Proceed by finishing the image installation and boot your worker. It will connect to the dashboard automatically.

ASIC Installation

Before proceeding with installation, make sure that your ASIC miner is supported. The current list of supported models:

- Antminer S9
- Antminer S9i
- Antminer L3+
- Antminer L3++
- Antminer D3
- Antminer A3
- Antminer T9+
- Antminer Z9-Mini

Installation

Remotely connect to your worker using SSH. Visit the Teleconsole forum thread for more details. Then run the following command:

```
cd /tmp && curl -L — insecure -s -O https://raw.githubusercontent.com/minershive/hiveos-asic/master/hive/bin/selfupgrade && sh selfupgrade
```

For Antminer D3 Blissz run the following command before installation:

```
ln -s /usr/lib/libcurl-gnutls.so.4 /usr/lib/libcurl.so.5
```

Promptless Installation

You can use `FARM_HASH` to add your ASIC workers automatically without entering rig ID and password. Copy your `FARM_HASH` from the Settings tab of your Farm and enter it into the command line as shown below:

```
cd /tmp && curl -L — insecure -s -O https://raw.githubusercontent.com/minershive/hiveos-asic/master/hive/bin/selfupgrade && FARM_HASH=your_hash_from_web sh selfupgrade
```

Replace the `your_hash_from_web` with your FARM_HASH.

For more details regarding ASIC installation, please refer to this GitHub page.

Finishing Setup

As soon as your worker connects to the dashboard, you're all done! Your worker should now be ready for you to make a few final adjustments in the dashboard, which we will describe in our next article.

Linux Cryptocurrency Mining Software Hive Os

117 claps

1

John Ganchak

Follow

Hiveon

The Ultimate Mining Network

Follow

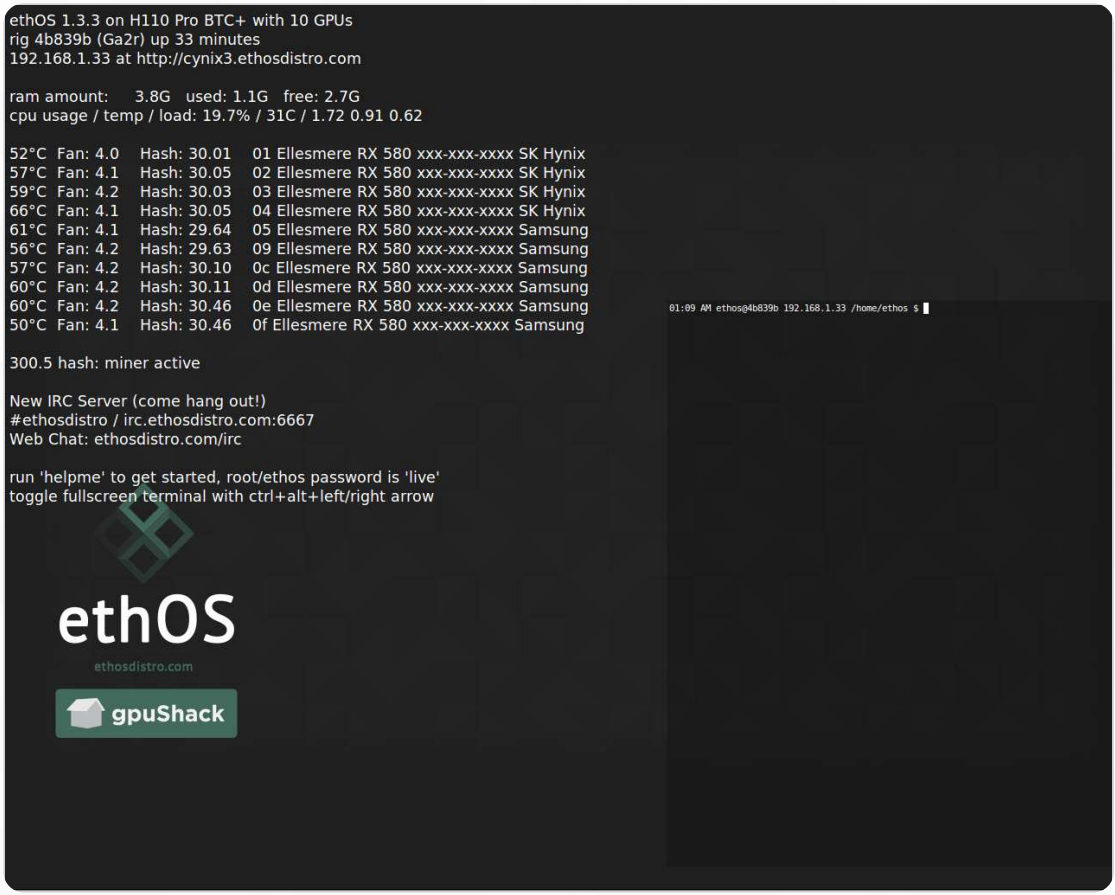
Never miss a story from **Hiveon**

GET UPDATES

ethOS is a 64-bit linux OS that mines **Ethereum**, **Zcash**, **Monero**, and other **GPU-minable coins**. Altcoins can be autotraded to Bitcoin. Please see the **ethOS knowledge base** for documentation and answers to common questions.

ethOS 1.3.3 can run **Tahiti/Tonga/Fiji with 50%-90% hashrate increases.**

There are **51,736** ethOS rigs mining on **322,034** GPUs.



- ethOS is **available pre-loaded on gpuShack.com**
- Buy it at **gpuShack.com**
- You must buy **one ethOS** for **each rig on which you plan to use ethOS**.

- **Free upgrades**: Get access to free ethOS upgrades for the lifetime of the product.
- **Boots and mines**: Automatic IP/hostname assignment, no need to install any drivers, configure XWindows, or compile any software.
- **Automatic alerts**: DisruptX Alerts ChatBot for ethOS sends automatic alerts about rig problems.
- **Supports up to 16 NVIDIA GPUs** : Any 2GB+ GTX 900 and GTX 1000 series.
- **Supports up to 13 AMD RX / VEGA GPUs** : Including support for **RX Series voltage control** and Z170/X/Z270/X/Ryzen Chipsets.
- **Supports up to 8 AMD R7/R9 GPUs** : Any 2GB+ HD 7000 series, any R9 200/300/Fury/Nano.
- **Supports multiple coins**: Ready to mine Ethereum, Zcash, Monero and many other gpu-minable coins.
- **Browser-based terminal**: allow setup and configuration of ethOS rigs by connecting to their IP addresses via your web browser.
- **Supports all hardforks and softforks**: No need for extra Blockchain storage, blockchain syncing handled by pools and wallets.
- **Works on your hardware**: Running on thousands of rigs with thousands of different components.
- **Remote configuration**: Instruct rig to remote reboot, set core clocks, mem clocks, fan control, pool info, and other settings remotely.
- **Extremely lightweight**: Works with weakest possible CPU made in the last 5 generations on only 2gb of ram.
- **GPU overheat protection**: GPUs will automatically throttle or turn off if they reach temperature thresholds.
- **Stratum enabled**: Automatically configured to mine via efficient stratum.
- **Automatic reporting**: Web panel with detailed rig statistics, charts, and event reports (example).
- **Easy KVM**: A terminal window opens with focus on boot, no mouse required.
- **Easy update**: Update to the latest ethOS version with a single command.
- **Fast startup**: Fast miner startup, low disk/cpu usage, and no out-of-space issues.
- **Bios flashing**: atiflash utility allows for quick gpu bios flashing.

ethOS was released in February of 2016. All proceeds from ethOS sales are distributed among the development team.

See ethOS changelog.

Version	Released on	Contributors
ethOS 1.3.3	October 9 2018	7
ethOS 1.3.2	July 31 2018	7
ethOS 1.3.1	Apr 4 2018	7
ethOS 1.3.0	Feb 28 2018	6
ethOS 1.2.9	Jan 6 2018	5
ethOS 1.2.7	Nov 19 2017	5
ethOS 1.2.6	Nov 17 2017	5
ethOS 1.2.5	Sep 15 2017	5
ethOS 1.2.4	Sep 3 2017	5
ethOS 1.2.3	Jul 4 2017	4
ethOS 1.2.2	May 26 2017	4
ethOS 1.2.1	April 30 2017	5
ethOS 1.2.0	Mar 16 2017	4
ethOS 1.1.9	Jan 19 2017	5
ethOS 1.1.8	Dec 22 2016	3
ethOS 1.1.7	Dec 21 2016	3
ethOS 1.1.6	Nov 18 2016	3
ethOS 1.1.5	Nov 15 2016	4

ethOS 1.1.4	Nov 5 2016	4
ethOS 1.1.3	Oct 31 2016	5
ethOS 1.1.2	Oct 8 2016	5
ethOS 1.1.1	Aug 21 2016	4
ethOS 1.1.0	Aug 15 2016	5
ethOS 1.0.7	Jul 24 2016	3
ethOS 1.0.6	Jun 20 2016	3
ethOS 1.0.5	May 4 2016	3
ethOS 1.0.4	Mar 31 2016	3
ethOS 1.0.3	Mar 18 2016	3
ethOS 1.0.2	Mar 14 2016	2
ethOS 1.0.1	Mar 4 2016	2
ethOS 1.0.0	Feb 15 2016	3

The following features are possible on ethOS, but must be done **without the support** of ethOS developers or staff. Performing the below actions should be done **at your own risk**.

- CPU Mining and ASIC Management.
- Mining via getwork over the Internet (causes loss of work due to latency, packet loss, and stale shares).
- Solo-mining (requires downloading the blockchain and running a node on another system).
- Wireless networking (causes packet loss, regardless of operating system, especially in large deployments).
- GUI-based rig management (all required management is done through config files).
- Dual mining mutiple coins (causes instability, extra power use, and possible melted/damaged

components).

- Dual-PSU systems (if any issue is resolved by using a single PSU, it is a hardware problem).
- Multi-Algo Switching (causes 10-20% chance of failure during switches, due to GPU crashes and power fluctuations).
- Mining coins below the "Top 30" minable coins list on CoinMarketCap (low-volume coins can crash quickly).
- VBIOS Flashing (has the potential to brick GPUs).
- Self-regulating reboots (does not fix any hardware, software, or configuration problem).
- Installing on HDDs or USB 2.0 drives (slow bootup may cause management script errors).
- Mining on Enterprise-Class GPUs (high cost/hash ratio GPUs will never ROI).
- Mixing AMD/NVIDIA in the same rig (they use different drivers that cannot work together).

- At least 8gb USB 3.0 / HDD / SSD
- 64-bit system
- GPUs

There is no email or skype support for ethOS. Please see the "Getting Support" section of the ethOS knowledge base.

ethOS is released under the "Small Goat with Red Eyes" license. You should buy one ethOS from gpuShack.com per each rig on which you intend to run ethOS. If you don't, a small goat with red eyes will visit you while you sleep.

ethOS is free software: you can redistribute it and/or modify it under the terms of the GNU General Public License as published by the Free Software Foundation, either version 3 of the License, or (at your option) any later version.

Certain files, that are distributed along-side ethOS, may be licensed under separate license agreements. The GNU General Public license does not extend to these files. End-users must remove these files prior to distributing ethOS itself.

ethOS is distributed in the hope that it will be useful, but WITHOUT ANY WARRANTY; without even the implied warranty of MERCHANTABILITY or FITNESS FOR A PARTICULAR PURPOSE. See the GNU General Public License for more details.

You should have received a copy of the GNU General Public License along with ethOS. If not, see http://www.gnu.org/licenses

ISSN 1551-3483

https://scale.qihardware.org