https://scale.qihardware.org

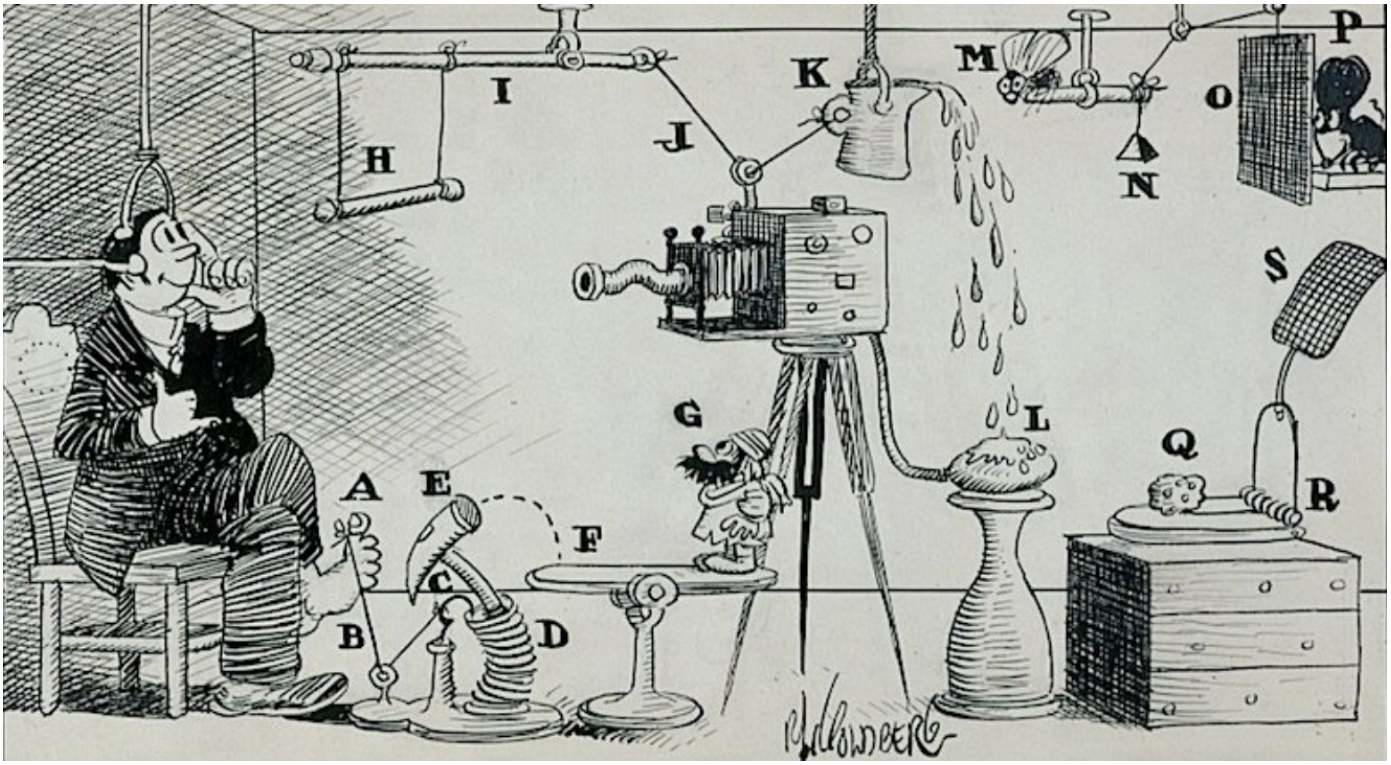
2019 . Week 05 . Feb 03 - Feb 09

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.

Validator Economics of Ethereum 2.0—Part One

Collin J.
Myers

Jan 10 · 9 min read



Since the formal announcement of Serenity at DevCon4 in November we have seen a strong self organization of minds come together to debate and better define the specs of Ethereum 2.0. Topics such as network inflation, economic incentives, slashing, withdrawal period, attack vectors and worst case scenarios are all receiving a healthy debate, amongst many others.

With the recent surge in participation in Ethereum 2.0, it is now timely and critical that we effectively incorporate diverse viewpoints to arrive at the best solution. The beauty of an open source protocol is that anyone can participate in its journey and shape the network. A blockchain protocol involves a symphony of differing yet overlapping motives, all of which must be aligned in harmony.

Over the past several weeks, I have focused on the economics of the spec from the perspective of a rational validator—both small scale and large scale.This piece will focus on the net yield of Ethereum 2.0 at the proposed spec from the viewpoint of a small scale validator. I will address the economics of a large scale validator in my next post. I hope that this preliminary analysis will lead to healthy discussions around the spec and inform further analysis across the blockchain community.

"In general, this is still an active area of research, and more research on counter-strategies is desired." Vitalik Buterin—Discouragement Attacks

Small Scale Validator (1 Validator Client)

- Cloud Based Approach
- Hardware Based Approach

Assumptions

Network Variables	
Validator Deposit (ETH)	32
Total at Stake	10,000,000
ETH Price	125.08
Network Fees/Day (ETH)	800
ETH Circulating Supply	104,100,000
Shards	1024
Slot Time (sec)	6
Epoch Length (slots)	64
Base Reward Quotient	1024

Calculations

Network Calcs	Value
Validators/Shards	305
Network Validators	312,500
epoch/year	82,125
reward quotient	3,237,888
reward/epoch	3.09
Generated ETH/Year	253,638
Network Inflation	0.24%
Implied Staker Interest	2.54%

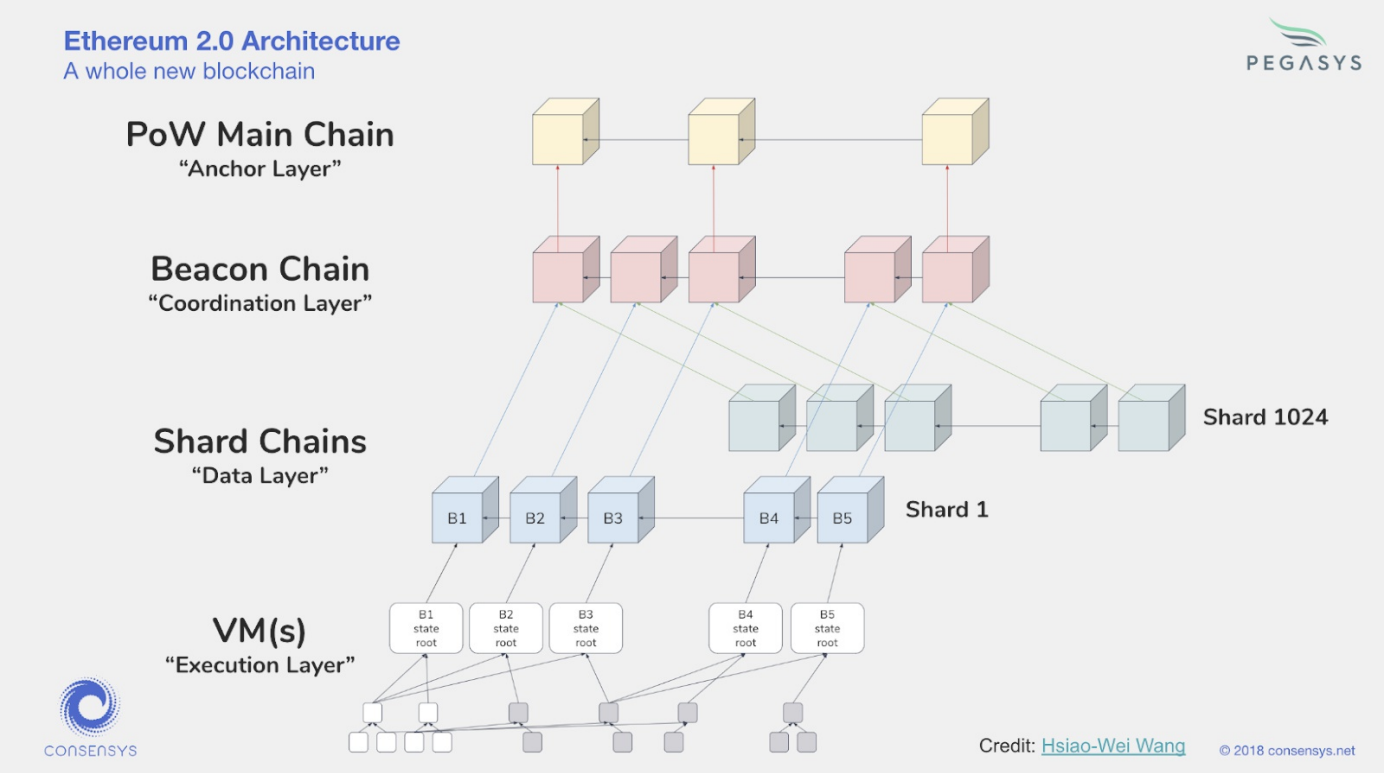
At the core of Ethereum 2.0 is a system chain called the "beacon chain". The beacon chain stores and manages the registry of validators. In the initial deployment phases of Ethereum 2.0 the only mechanism to become a validator is to make a one-way 32 ETH deposit contract on Ethereum 1.0.

Activation as a validator happens when deposit transaction receipts are processed by the beacon chain, the activation balance is reached, and after a queuing process. Exit is either voluntary or forced as a penalty for misbehavior.

In return for staking ETH, attesting to correct blocks, signing off on the validity of a block, and proposing blocks, the validator will be rewarded with ETH through a network wide interest rate as well as receive a portion of network transaction fees.

For more reading on Ethereum 2.0 check out the following articles:

- Two Point Oh: Explaining Validators
- Two Point Oh: The Beacon Chain
- Rocket Pool—Eth 2.0
- ETH 2.0 Master Spec
- State of Ethereum Protocol #2: The Beacon Chain



Below you will find a list of the teams actively researching or developing a beacon chain / shard client:

- Artemis—developed by PegaSys the protocol engineering group at ConsenSys, written in Java. The team is focused on key Ethereum challenges including scalability and privacy for both public and private chains.
- Prysm—developed by Prysmatic Labs, written in Go. They have an excellent bi-weekly update on their progress.
- Lighthouse—developed by Sigma Prime, written in Rust.
- Nimbus—developed by Status, written in Nim.
- Lodestar—developed by Chain Safe Systems in JavaScript.

- Harmony—developed by Ether Camp, written in Java.
- Trinity—developed by the Trinity team (led by Piper Merriam), written in Python.

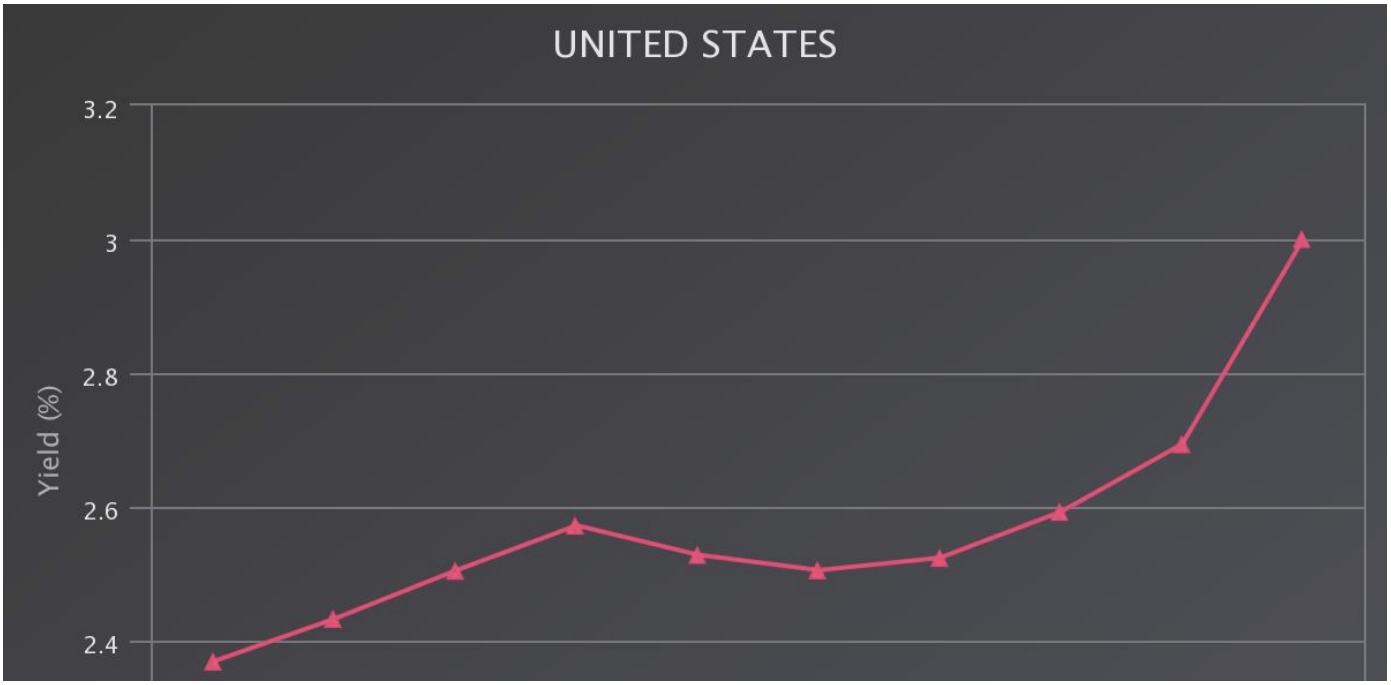
Economics & Risk

When discussing the economics of anything (especially financial products) one of the first areas we should address is the risk profile of an opportunity. Modern portfolio theory makes the assumptions that investors are risk-averse, meaning they prefer a less risky portfolio to a riskier one for a given level of return. In mature markets the risk return profile is normally (with a few exceptions) up and to the right—the more risk involved should lead to a higher reward.

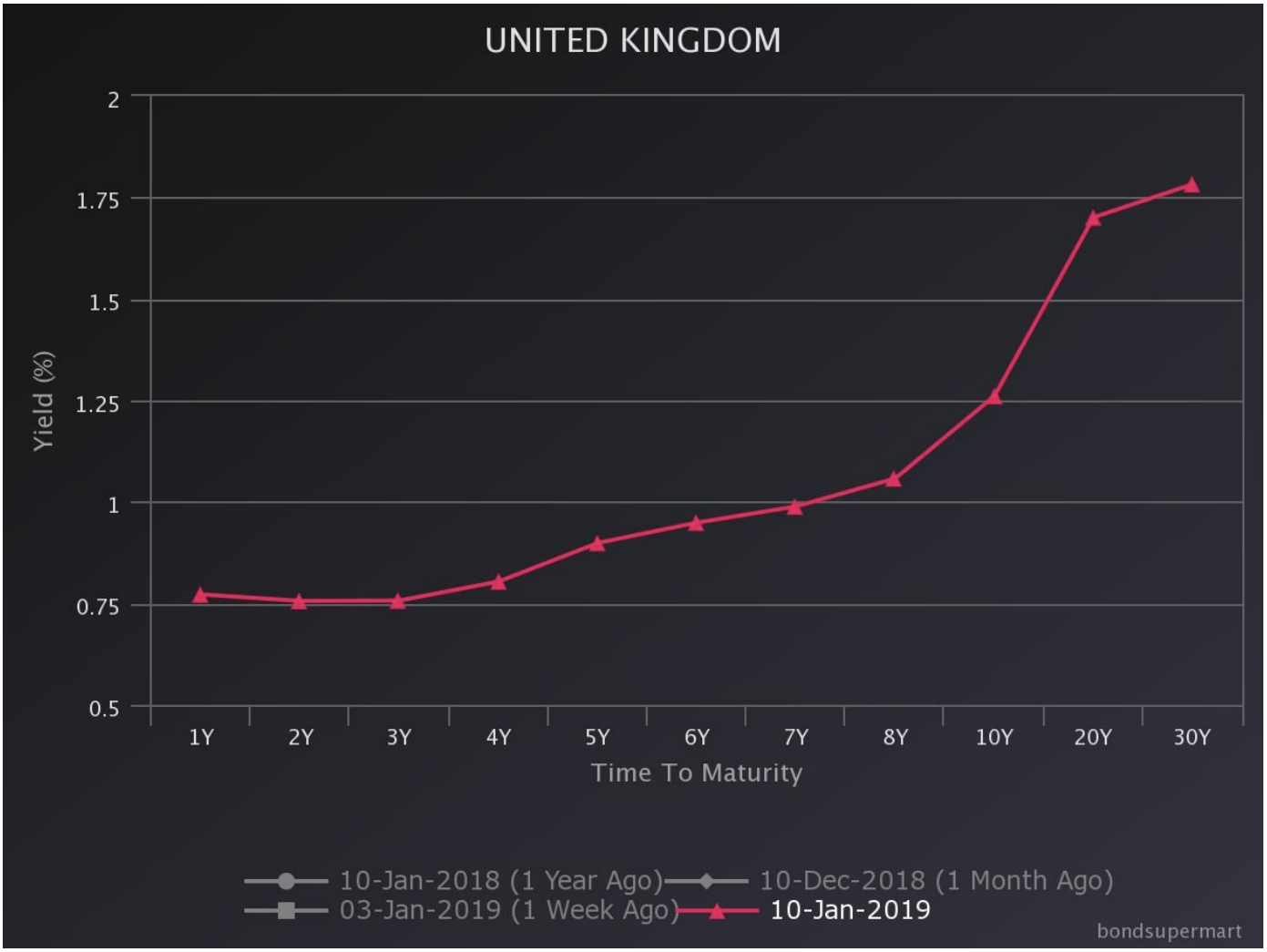
Sovereign Debt Yield Curves

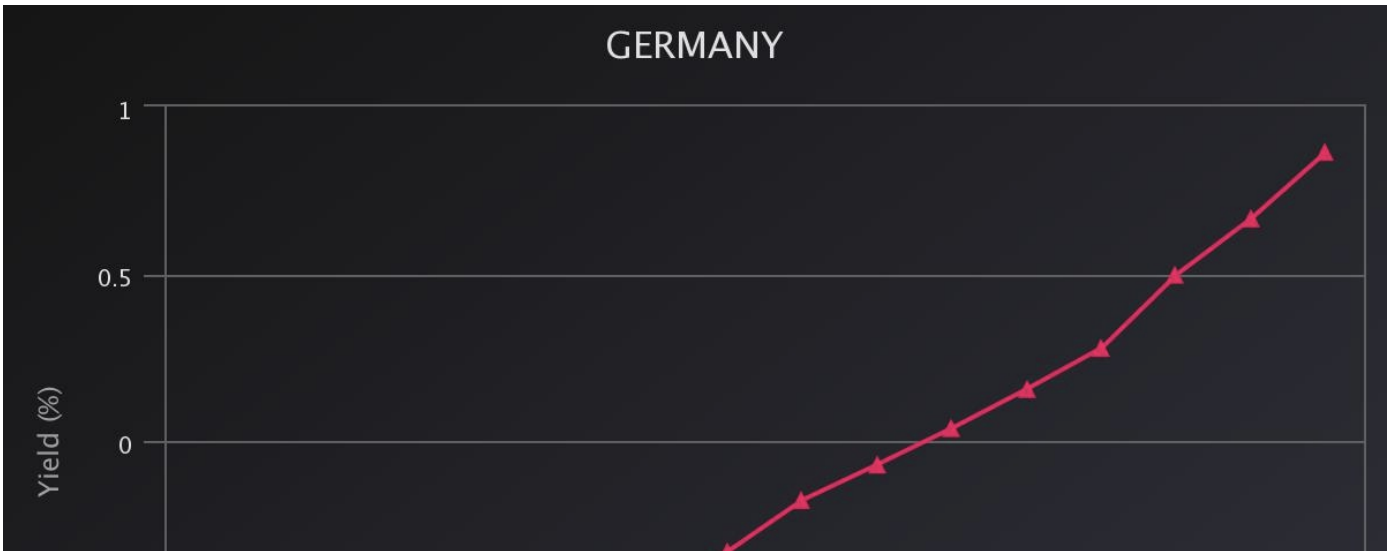
The graphs below represent the yield curves for different nations sovereign debt. Global sovereign debt markets are some of the most liquid and deep markets in the world. Magnitudes more liquid than ETH, especially ETH that is locked in a staking contract. In the examples below investors are compensated for the risk that a specific nation will be able to repay its national debt at maturity. Sovereign bond yields are primarily affected by creditworthiness, country risk, and exchange rates.

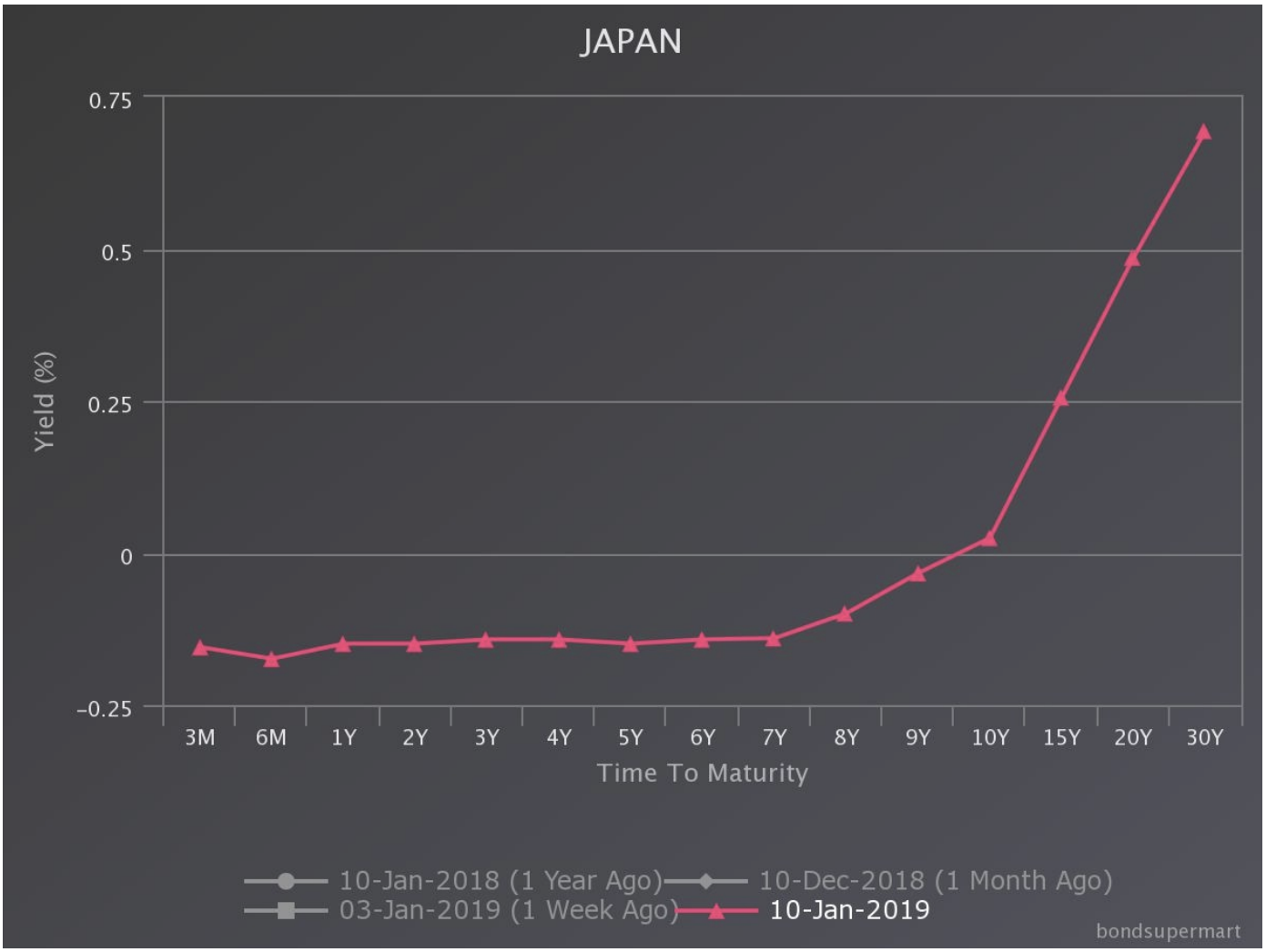
Investing in sovereign debt is considered to be the most 'riskless' investment in global financial markets, with the three-month US treasury yield (2.43%) used globally in various valuation models and risk adjusted return ratios every day as the 'risk-free rate'.




2.2
1M
3M
6M
1Y
2Y
3Y
5Y
7Y
10Y
30Y
Time To Maturity
10-Jan-2018 (1 Year Ago)
10-Dec-2018 (1 Month Ago)
03-Jan-2019 (1 Week Ago)
10-Jan-2019
bondsupermart


UNITED KINGDOM
2
1.75
1.5
1.25
1
0.75
0.5
Yield (%)
1Y
2Y
3Y
4Y
5Y
6Y
7Y
8Y
10Y
20Y
30Y
Time To Maturity
10-Jan-2018 (1 Year Ago)
10-Dec-2018 (1 Month Ago)
03-Jan-2019 (1 Week Ago)
10-Jan-2019
bondsupermart


GERMANY
1
0.5
0
Yield (%)



When incentivizing actions it is important to remember that a rational validator has a decreased chance of participation if the opportunity exhibits:

- Weak profitability
- Risks outweighing rewards
- High barriers to entry (knowledge, time or resource based)
- Uncompetitive yields (on a risk adjusted basis)

- Uncompetitive yields (on a risk adjusted basis)

Eric Connor recently published a piece on ethhub that addresses the risks of performing validation, which can be summarized below.

Staking Costs and Risks

Computing cost

- Users will need to run validator clients and likely beacon nodes. This requires computing resources.
- Beacon Node: similar to running geth/parity today
- Validator client: lightweight and need one per 32 ETH stake

Capital acquisition and lockup

- The user must first acquire 32 ETH..
- There exists a grace period before users may withdraw their funds. However, this time has come down considerably in the latest versions of the spec. The minimum withdraw queue wait is currently 18 hours, subject to delays imposed by network congestion.

Code Risk

- Programs may have been incorrectly constructed. This risk is mitigated over time through correct usage despite substantial economic incentive to compromise the system. Consensus-level code is simpler to remediate through forking, while client code running across thousands of nodes is prone to added difficulty in pinpointing defects and distributing changes.

General uptime and maintenance cost

- Users need to make sure their validator doesn't have downtime or they risk a quadratic leak on their stake.
- If a user has multiple validators, maintenance cost and worry of the infrastructure comes into play.

Security risk

- Beyond failures in the client code, stakers are responsible for the security environment of their validator clients (internet connection, operating system, hardware, etc.). If a validator client is compromised, there is no way to recover funds or returns.

Market Competition

In aggregate, participants staking on Ethereum 2.0 will face a universe of competing yield opportunities. It would be wise to assume that a portion of total stakers will be driven by return potential and not the joy of securing the Ethereum network. The macro categories of competing opportunities are laid out below:

Decentralized Finance

- Some of the most exciting adoption activity seen recently in the crypto space has been the volume increases in Defi applications. These applications offer users different ways to lock up their ETH and earn a reward (interest). Examples of current Defi applications are Compound Finance, Dharma, Maker and dYdX. Christopher DeLuca of Bloqboard recently wrote a great Defi lending report comparing the changes in volume seen month over month for the Defi applications listed above (highly recommended).

Traditional Investment Vehicles

- Mature interest based opportunities that have lower fiat denominated price volatility such as bonds (corporate & sovereign), CDs, and savings accounts should be considered when determining network opportunities. The crypto space could use a steady inclusion of institutional capital over time, but to achieve this risk profiles and returns of crypto based opportunities must be in line with traditional products—when discussing institutional capital I am referring to the type of money that is put to work on the behalf of someone else and driven by structured investment mandates (not pure crypto funds).

Alternative Staking Coins

- Currently there are over 500 alternative POS coins, with their own reward structure. The majority mindset for this category of staking participants is to dedicate their resources towards whatever is yielding the most and then liquidate immediately into their favorite major

immediately into their favorite major.

Total Incentive to Stake = Validator Rewards + Network Fees—Cost to Run a Validator

At a high level, the minimum requirements to stake are

- Minimum of 32 ETH (per validator)
- Computer
- Internet Connection

There are three different types of participants that can exist when running Ethereum 2.0 software. This article will focus on the net yield for small scale validators.

- Beacon node only
- Beacon node + validator client (small scale)
- Beacon node + multiple validator clients (large scale)

Small Scale Validator Analysis

The purpose of the sensitivity analysis' below is to look at the net yield potential for a small scale validator using a cloud or hardware infrastructure on a yearly basis. All network assumptions are based on the current ETH 2.0 Master Spec, while cost assumptions have been sourced independently. Further sensitivity analysis' for each infrastructure option can be found below.

Ethereum 2.0 Validator Staking Net Yields

Cloud

Network ETH at Stake \ Network Fees/Day	100	200	300	400	500	600	700	800	900	1000	1100	1200	1300
1,000,000	-11.7%	-8.0%	-4.4%	-0.7%	2.9%	6.6%	10.2%	13.9%	17.5%	21.2%	24.8%	28.5%	32.1%
2,000,000	-15.8%	-14.0%	-12.2%	-10.3%	-8.5%	-6.7%	-4.9%	-3.0%	-1.2%	0.6%	2.4%	4.3%	6.1%
3,000,000	-17.5%	-16.2%	-15.0%	-13.8%	-12.6%	-11.4%	-10.2%	-8.9%	-7.7%	-6.5%	-5.3%	-4.1%	-2.9%
4,000,000	-18.4%	-17.5%	-16.5%	-15.6%	-14.7%	-13.8%	-12.9%	-12.0%	-11.1%	-10.2%	-9.2%	-8.3%	-7.4%
5,000,000	-19.0%	-18.2%	-17.5%	-16.8%	-16.1%	-15.3%	-14.6%	-13.9%	-13.1%	-12.4%	-11.7%	-10.9%	-10.2%
6,000,000	-19.4%	-18.8%	-18.2%	-17.6%	-17.0%	-16.4%	-15.8%	-15.1%	-14.5%	-13.9%	-13.3%	-12.7%	-12.1%
7,000,000	-19.7%	-19.2%	-18.7%	-18.2%	-17.6%	-17.1%	-16.6%	-16.1%	-15.6%	-15.0%	-14.5%	-14.0%	-13.5%
8,000,000	-20.0%	-19.5%	-19.1%	-18.6%	-18.2%	-17.7%	-17.3%	-16.8%	-16.3%	-15.9%	-15.4%	-15.0%	-14.5%
9,000,000	-20.2%	-19.8%	-19.4%	-19.0%	-18.6%	-18.2%	-17.8%	-17.4%	-17.0%	-16.6%	-16.1%	-15.7%	-15.3%
10,000,000	-20.4%	-20.0%	-19.6%	-19.3%	-18.9%	-18.6%	-18.2%	-17.8%	-17.5%	-17.1%	-16.7%	-16.4%	-16.0%
11,000,000	-20.5%	-20.2%	-19.9%	-19.5%	-19.2%	-18.9%	-18.5%	-18.2%	-17.9%	-17.5%	-17.2%	-16.9%	-16.5%
12,000,000	-20.7%	-20.4%	-20.0%	-19.7%	-19.4%	-19.1%	-18.8%	-18.5%	-18.2%	-17.9%	-17.6%	-17.3%	-17.0%
13,000,000	-20.8%	-20.5%	-20.2%	-19.9%	-19.6%	-19.4%	-19.1%	-18.8%	-18.5%	-18.2%	-18.0%	-17.7%	-17.4%
14,000,000	-20.9%	-20.6%	-20.3%	-20.1%	-19.8%	-19.6%	-19.3%	-19.0%	-18.8%	-18.5%	-18.3%	-18.0%	-17.7%
15,000,000	-21.0%	-20.7%	-20.5%	-20.2%	-20.0%	-19.7%	-19.5%	-19.3%	-19.0%	-18.8%	-18.5%	-18.3%	-18.0%
16,000,000	-21.0%	-20.8%	-20.6%	-20.4%	-20.1%	-19.9%	-19.7%	-19.4%	-19.2%	-19.0%	-18.8%	-18.5%	-18.3%

17,000,000	-21.1%	-20.9%	-20.7%	-20.5%	-20.3%	-20.0%	-19.8%	-19.6%	-19.4%	-19.2%	-19.0%	-18.8%	-18.5%
18,000,000	-21.2%	-21.0%	-20.8%	-20.6%	-20.4%	-20.2%	-20.0%	-19.8%	-19.6%	-19.4%	-19.2%	-18.9%	-18.7%
19,000,000	-21.2%	-21.0%	-20.9%	-20.7%	-20.5%	-20.3%	-20.1%	-19.9%	-19.7%	-19.5%	-19.3%	-19.1%	-18.9%
20,000,000	-21.3%	-21.1%	-20.9%	-20.7%	-20.6%	-20.4%	-20.2%	-20.0%	-19.8%	-19.7%	-19.5%	-19.3%	-19.1%
21,000,000	-21.3%	-21.2%	-21.0%	-20.8%	-20.7%	-20.5%	-20.3%	-20.1%	-20.0%	-19.8%	-19.6%	-19.4%	-19.3%
22,000,000	-21.4%	-21.2%	-21.1%	-20.9%	-20.7%	-20.6%	-20.4%	-20.2%	-20.1%	-19.9%	-19.7%	-19.6%	-19.4%
23,000,000	-21.4%	-21.3%	-21.1%	-21.0%	-20.8%	-20.6%	-20.5%	-20.3%	-20.2%	-20.0%	-19.9%	-19.7%	-19.5%

Minimum Initial Capital Requirements	=	**$4,003**
		$4,403

Hardware

Network Fees/Day

Network ETH at Stake	100	200	300	400	500	600	700	800	900	1000	1100	1200	1300
1,000,000	6.5%	10.2%	13.8%	17.5%	21.1%	24.8%	28.4%	32.1%	35.7%	39.4%	43.0%	46.7%	50.3%
2,000,000	2.4%	4.2%	6.0%	7.8%	9.7%	11.5%	13.3%	15.1%	17.0%	18.8%	20.6%	22.4%	24.3%
3,000,000	0.7%	2.0%	3.2%	4.4%	5.6%	6.8%	8.0%	9.3%	10.5%	11.7%	12.9%	14.1%	15.3%
4,000,000	-0.2%	0.7%	1.6%	2.6%	3.5%	4.4%	5.3%	6.2%	7.1%	8.0%	8.9%	9.9%	10.8%
5,000,000	-0.8%	-0.1%	0.7%	1.4%	2.1%	2.9%	3.6%	4.3%	5.1%	5.8%	6.5%	7.2%	8.0%
6,000,000	-1.2%	-0.6%	0.0%	0.6%	1.2%	1.8%	2.4%	3.0%	3.6%	4.3%	4.9%	5.5%	6.1%
7,000,000	-1.5%	-1.0%	-0.5%	0.0%	0.5%	1.1%	1.6%	2.1%	2.6%	3.1%	3.7%	4.2%	4.7%
8,000,000	-1.8%	-1.3%	-0.9%	-0.4%	0.0%	0.5%	0.9%	1.4%	1.8%	2.3%	2.8%	3.2%	3.7%
9,000,000	-2.0%	-1.6%	-1.2%	-0.8%	-0.4%	0.0%	0.4%	0.8%	1.2%	1.6%	2.0%	2.4%	2.9%
10,000,000	-2.2%	-1.8%	-1.5%	-1.1%	-0.7%	-0.4%	0.0%	0.4%	0.7%	1.1%	1.5%	1.8%	2.2%
11,000,000	-2.3%	-2.0%	-1.7%	-1.3%	-1.0%	-0.7%	-0.4%	0.0%	0.3%	0.6%	1.0%	1.3%	1.6%
12,000,000	-2.5%	-2.2%	-1.9%	-1.6%	-1.3%	-1.0%	-0.6%	-0.3%	0.0%	0.3%	0.6%	0.9%	1.2%
13,000,000	-2.6%	-2.3%	-2.0%	-1.7%	-1.5%	-1.2%	-0.9%	-0.6%	-0.3%	-0.1%	0.2%	0.5%	0.8%
14,000,000	-2.7%	-2.4%	-2.2%	-1.9%	-1.6%	-1.4%	-1.1%	-0.9%	-0.6%	-0.3%	-0.1%	0.2%	0.4%
15,000,000	-2.8%	-2.5%	-2.3%	-2.0%	-1.8%	-1.6%	-1.3%	-1.1%	-0.8%	-0.6%	-0.3%	-0.1%	0.1%
16,000,000	-2.9%	-2.6%	-2.4%	-2.2%	-1.9%	-1.7%	-1.5%	-1.3%	-1.0%	-0.8%	-0.6%	-0.3%	-0.1%
17,000,000	-2.9%	-2.7%	-2.5%	-2.3%	-2.1%	-1.9%	-1.6%	-1.4%	-1.2%	-1.0%	-0.8%	-0.6%	-0.4%
18,000,000	-3.0%	-2.8%	-2.6%	-2.4%	-2.2%	-2.0%	-1.8%	-1.6%	-1.4%	-1.2%	-1.0%	-0.8%	-0.6%
19,000,000	-3.1%	-2.9%	-2.7%	-2.5%	-2.3%	-2.1%	-1.9%	-1.7%	-1.5%	-1.3%	-1.1%	-0.9%	-0.7%
20,000,000	-3.1%	-2.9%	-2.7%	-2.6%	-2.4%	-2.2%	-2.0%	-1.8%	-1.6%	-1.5%	-1.3%	-1.1%	-0.9%
21,000,000	-3.2%	-3.0%	-2.8%	-2.6%	-2.5%	-2.3%	-2.1%	-1.9%	-1.8%	-1.6%	-1.4%	-1.2%	-1.1%
22,000,000	-3.2%	-3.0%	-2.9%	-2.7%	-2.5%	-2.4%	-2.2%	-2.0%	-1.1%	-0.9%	-0.8%	-0.6%	-0.5%
23,000,000	-2.5%	-2.3%	-2.2%	-2.0%	-1.9%	-1.7%	-1.5%	-1.4%	-1.2%	-1.1%	-0.9%	-0.7%	-0.6%

Cloud Economics

Assumptions

Network Variables	
Validator Deposit (ETH)	32
Total at Stake	10,000,000
ETH Price	125.08
Network Fees/Day (ETH)	800
ETH Circulating Supply	104,100,000
Shards	1024
Slot Time (sec)	6
Epoch Length (slots)	64
Base Reward Quotient	1024

Validator Variables (Minimum Requirements)	
Validators Run	1
Uptime	99%
EC2 m4.large Monthly Costs	$73
S3 Monthly Cost (100GB)	$2
Additional Overhead (per client)	$50
Capacity of Validators Run/Client	10
Number of Clients	1
Initial Investment	**$4,003**

Calculations

Network Calcs	**Value**
Validators/Shards	305
Network Validators	312,500
epoch/year	82,125
reward quotient	3,237,888
reward/epoch	3.09
Generated ETH/Year	253,638
Network Inflation	0.24%
Implied Staker Interest	2.54%

Validator P&L	
ETH Staked	32
Staker Interest	2.54%
Staker interest ($)	$102
Gas Fee Rev	$117
Total Staker Rev	**$218**
Slashing Costs	$1
EC2 Costs	$878
S3 Costs	$2
Additional Overhead	$50
Total Validator Costs	**$932**
Annual Profit	**-$713**

Profit Margin	-326.62%
Net Yield	**-17.82%**

Validator Net Yield

Network Fees/Day

Network ETH at Stake	100	200	300	400	500	600	700	800	900	1000	1100	1200	1300
1,000,000	-11.7%	-8.0%	-4.4%	-0.7%	2.9%	6.6%	10.2%	13.9%	17.5%	21.2%	24.8%	28.5%	32.1%
2,000,000	-15.8%	-14.0%	-12.2%	-10.3%	-8.5%	-6.7%	-4.9%	-3.0%	-1.2%	0.6%	2.4%	4.3%	6.1%
3,000,000	-17.5%	-16.2%	-15.0%	-13.8%	-12.6%	-11.4%	-10.2%	-8.9%	-7.7%	-6.5%	-5.3%	-4.1%	-2.9%
4,000,000	-18.4%	-17.5%	-16.5%	-15.6%	-14.7%	-13.8%	-12.9%	-12.0%	-11.1%	-10.2%	-9.2%	-8.3%	-7.4%
5,000,000	-19.0%	-18.2%	-17.5%	-16.8%	-16.1%	-15.3%	-14.6%	-13.9%	-13.1%	-12.4%	-11.7%	-10.9%	-10.2%
6,000,000	-19.4%	-18.8%	-18.2%	-17.6%	-17.0%	-16.4%	-15.8%	-15.1%	-14.5%	-13.9%	-13.3%	-12.7%	-12.1%
7,000,000	-19.7%	-19.2%	-18.7%	-18.2%	-17.6%	-17.1%	-16.6%	-16.1%	-15.6%	-15.0%	-14.5%	-14.0%	-13.5%
8,000,000	-20.0%	-19.5%	-19.1%	-18.6%	-18.2%	-17.7%	-17.3%	-16.8%	-16.3%	-15.9%	-15.4%	-15.0%	-14.5%
9,000,000	-20.2%	-19.8%	-19.4%	-19.0%	-18.6%	-18.2%	-17.8%	-17.4%	-17.0%	-16.6%	-16.1%	-15.7%	-15.3%
10,000,000	-20.4%	-20.0%	-19.6%	-19.3%	-18.9%	-18.6%	-18.2%	-17.8%	-17.5%	-17.1%	-16.7%	-16.4%	-16.0%
11,000,000	-20.5%	-20.2%	-19.9%	-19.5%	-19.2%	-18.9%	-18.5%	-18.2%	-17.9%	-17.5%	-17.2%	-16.9%	-16.5%
12,000,000	-20.7%	-20.4%	-20.0%	-19.7%	-19.4%	-19.1%	-18.8%	-18.5%	-18.2%	-17.9%	-17.6%	-17.3%	-17.0%
13,000,000	-20.8%	-20.5%	-20.2%	-19.9%	-19.6%	-19.4%	-19.1%	-18.8%	-18.5%	-18.2%	-18.0%	-17.7%	-17.4%
14,000,000	-20.9%	-20.6%	-20.3%	-20.1%	-19.8%	-19.6%	-19.3%	-19.0%	-18.8%	-18.5%	-18.3%	-18.0%	-17.7%
15,000,000	-21.0%	-20.7%	-20.5%	-20.2%	-20.0%	-19.7%	-19.5%	-19.3%	-19.0%	-18.8%	-18.5%	-18.3%	-18.0%
16,000,000	-21.0%	-20.8%	-20.6%	-20.4%	-20.1%	-19.9%	-19.7%	-19.4%	-19.2%	-19.0%	-18.8%	-18.5%	-18.3%
17,000,000	-21.1%	-20.9%	-20.7%	-20.5%	-20.3%	-20.0%	-19.8%	-19.6%	-19.4%	-19.2%	-19.0%	-18.8%	-18.5%
18,000,000	-21.2%	-21.0%	-20.8%	-20.6%	-20.4%	-20.2%	-20.0%	-19.8%	-19.6%	-19.4%	-19.2%	-18.9%	-18.7%
19,000,000	-21.2%	-21.0%	-20.9%	-20.7%	-20.5%	-20.3%	-20.1%	-19.9%	-19.7%	-19.5%	-19.3%	-19.1%	-18.9%
20,000,000	-21.3%	-21.1%	-20.9%	-20.7%	-20.6%	-20.4%	-20.2%	-20.0%	-19.8%	-19.7%	-19.5%	-19.3%	-19.1%
21,000,000	-21.3%	-21.2%	-21.0%	-20.8%	-20.7%	-20.5%	-20.3%	-20.1%	-20.0%	-19.8%	-19.6%	-19.4%	-19.3%
22,000,000	-21.4%	-21.2%	-21.1%	-20.9%	-20.7%	-20.6%	-20.4%	-20.2%	-20.1%	-19.9%	-19.7%	-19.6%	-19.4%
23,000,000	-21.4%	-21.3%	-21.1%	-21.0%	-20.8%	-20.6%	-20.5%	-20.3%	-20.2%	-20.0%	-19.9%	-19.7%	-19.5%

Validator Net Yield

ETH Price

Network ETH at Stake	150	250	350	450	550	650	750	850	950	1050	1150	1250	1350
1,000,000	17.75%	25.51%	28.83%	30.68%	31.85%	32.67%	33.26%	33.72%	34.08%	34.37%	34.61%	34.81%	34.99%
2,000,000	0.83%	8.58%	11.91%	13.75%	14.93%	15.74%	16.34%	16.79%	17.15%	17.45%	17.69%	17.89%	18.06%
3,000,000	-5.07%	2.68%	6.01%	7.85%	9.03%	9.84%	10.44%	10.90%	11.26%	11.55%	11.79%	11.99%	12.16%
4,000,000	-8.12%	-0.36%	2.96%	4.81%	5.98%	6.80%	7.39%	7.85%	8.21%	8.50%	8.74%	8.94%	9.12%
5,000,000	-10.00%	-2.24%	1.08%	2.93%	4.10%	4.92%	5.51%	5.97%	6.33%	6.62%	6.86%	7.06%	7.24%
6,000,000	-11.28%	-3.53%	-0.20%	1.65%	2.82%	3.63%	4.23%	4.69%	5.05%	5.34%	5.58%	5.78%	5.95%
7,000,000	-12.22%	-4.46%	-1.14%	0.71%	1.89%	2.70%	3.30%	3.75%	4.11%	4.40%	4.64%	4.85%	5.02%
8,000,000	-12.93%	-5.18%	-1.85%	-0.01%	1.17%	1.98%	2.58%	3.04%	3.40%	3.69%	3.93%	4.13%	4.30%
9,000,000	-13.50%	-5.74%	-2.42%	-0.57%	0.60%	1.42%	2.01%	2.47%	2.83%	3.12%	3.36%	3.56%	3.74%
10,000,000	-13.96%	-6.20%	-2.88%	-1.03%	0.14%	0.96%	1.55%	2.01%	2.37%	2.66%	2.90%	3.10%	3.28%
11,000,000	-14.34%	-6.58%	-3.26%	-1.41%	-0.24%	0.57%	1.17%	1.63%	1.99%	2.28%	2.52%	2.72%	2.89%
12,000,000	-14.66%	-6.91%	-3.58%	-1.74%	-0.56%	0.25%	0.85%	1.30%	1.66%	1.96%	2.20%	2.40%	2.57%
13,000,000	-14.94%	-7.19%	-3.86%	-2.01%	-0.84%	-0.03%	0.57%	1.03%	1.39%	1.68%	1.92%	2.12%	2.29%
14,000,000	-15.18%	-7.43%	-4.10%	-2.26%	-1.08%	-0.27%	0.33%	0.79%	1.15%	1.44%	1.68%	1.88%	2.05%
15,000,000	-15.39%	-7.64%	-4.31%	-2.47%	-1.29%	-0.48%	0.12%	0.58%	0.94%	1.23%	1.47%	1.67%	1.84%
16,000,000	-15.58%	-7.82%	-4.50%	-2.65%	-1.48%	-0.66%	-0.07%	0.39%	0.75%	1.04%	1.28%	1.48%	1.66%
17,000,000	-15.75%	-7.99%	-4.67%	-2.82%	-1.64%	-0.83%	-0.23%	0.22%	0.58%	0.87%	1.11%	1.32%	1.49%
18,000,000	-15.90%	-8.14%	-4.82%	-2.97%	-1.79%	-0.98%	-0.38%	0.07%	0.43%	0.72%	0.96%	1.17%	1.34%
19,000,000	-16.03%	-8.28%	-4.95%	-3.10%	-1.93%	-1.12%	-0.52%	-0.06%	0.30%	0.59%	0.83%	1.03%	1.20%
20,000,000	-16.15%	-8.40%	-5.07%	-3.23%	-2.05%	-1.24%	-0.64%	-0.19%	0.17%	0.47%	0.71%	0.91%	1.08%
21,000,000	-16.27%	-8.51%	-5.19%	-3.34%	-2.16%	-1.35%	-0.75%	-0.30%	0.06%	0.35%	0.59%	0.80%	0.97%
22,000,000	-16.37%	-8.61%	-5.29%	-3.44%	-2.27%	-1.45%	-0.86%	-0.40%	-0.04%	0.25%	0.49%	0.69%	0.87%
23,000,000	-16.46%	-8.71%	-5.38%	-3.54%	-2.36%	-1.55%	-0.95%	-0.50%	-0.14%	0.16%	0.40%	0.60%	0.77%

Validator Net Yield

ETH Price \ Network Fees/Day	100	200	300	400	500	600	700	800	900	1000	1100	1200	1300
$150	-16.51%	-16.15%	-15.78%	-15.42%	-15.05%	-14.69%	-14.32%	-13.96%	-13.59%	-13.23%	-12.86%	-12.50%	-12.13%
$250	-8.76%	-8.39%	-8.03%	-7.66%	-7.30%	-6.93%	-6.57%	-6.20%	-5.84%	-5.47%	-5.11%	-4.74%	-4.38%
$350	-5.43%	-5.07%	-4.70%	-4.34%	-3.97%	-3.61%	-3.24%	-2.88%	-2.51%	-2.15%	-1.78%	-1.42%	-1.05%
$450	-3.59%	-3.22%	-2.86%	-2.49%	-2.13%	-1.76%	-1.40%	-1.03%	-0.67%	-0.30%	0.06%	0.43%	0.79%
$550	-2.41%	-2.05%	-1.68%	-1.32%	-0.95%	-0.59%	-0.22%	0.14%	0.51%	0.87%	1.24%	1.60%	1.97%
$650	-1.60%	-1.23%	-0.87%	-0.50%	-0.14%	0.23%	0.59%	0.96%	1.32%	1.69%	2.05%	2.42%	2.78%
$750	-1.00%	-0.64%	-0.27%	0.09%	0.46%	0.82%	1.19%	1.55%	1.92%	2.28%	2.65%	3.01%	3.38%
$850	-0.55%	-0.18%	0.18%	0.55%	0.91%	1.28%	1.64%	2.01%	2.37%	2.74%	3.10%	3.47%	3.83%
$950	-0.19%	0.18%	0.54%	0.91%	1.27%	1.64%	2.00%	2.37%	2.73%	3.10%	3.46%	3.83%	4.19%
$1,050	0.11%	0.47%	0.84%	1.20%	1.57%	1.93%	2.30%	2.66%	3.03%	3.39%	3.76%	4.12%	4.49%
$1,150	0.35%	0.71%	1.08%	1.44%	1.81%	2.17%	2.54%	2.90%	3.27%	3.63%	4.00%	4.36%	4.73%
$1,250	0.55%	0.91%	1.28%	1.64%	2.01%	2.37%	2.74%	3.10%	3.47%	3.83%	4.20%	4.56%	4.93%
$1,350	0.72%	1.09%	1.45%	1.82%	2.18%	2.55%	2.91%	3.28%	3.64%	4.01%	4.37%	4.74%	5.10%
$1,450	0.87%	1.24%	1.60%	1.97%	2.33%	2.70%	3.06%	3.43%	3.79%	4.16%	4.52%	4.89%	5.25%
$1,550	1.00%	1.36%	1.73%	2.09%	2.46%	2.82%	3.19%	3.55%	3.92%	4.28%	4.65%	5.01%	5.38%
$1,650	1.11%	1.48%	1.84%	2.21%	2.57%	2.94%	3.30%	3.67%	4.03%	4.40%	4.76%	5.13%	5.49%
$1,750	1.21%	1.58%	1.94%	2.31%	2.67%	3.04%	3.40%	3.77%	4.13%	4.50%	4.86%	5.23%	5.59%
$1,850	1.30%	1.67%	2.03%	2.40%	2.76%	3.13%	3.49%	3.86%	4.22%	4.59%	4.95%	5.32%	5.68%
$1,950	1.38%	1.75%	2.11%	2.48%	2.84%	3.21%	3.57%	3.94%	4.30%	4.67%	5.03%	5.40%	5.76%
$2,050	1.46%	1.82%	2.19%	2.55%	2.92%	3.28%	3.65%	4.01%	4.38%	4.74%	5.11%	5.47%	5.84%
$2,150	1.52%	1.89%	2.25%	2.62%	2.98%	3.35%	3.71%	4.08%	4.44%	4.81%	5.17%	5.54%	5.90%
$2,250	1.58%	1.95%	2.31%	2.68%	3.04%	3.41%	3.77%	4.14%	4.50%	4.87%	5.23%	5.60%	5.96%
$2,350	1.64%	2.00%	2.37%	2.73%	3.10%	3.46%	3.83%	4.19%	4.56%	4.92%	5.29%	5.65%	6.02%

Hardware Economics

Assumptions

Network Variables	
Validator Deposit (ETH)	32
Total at Stake	10,000,000
ETH Price	125.08
Network Fees/Day (ETH)	800
ETH Circulating Supply	104,100,000
Shards	1024
Slot Time (sec)	6
Epoch Length (slots)	64
Base Reward Quotient	1024

Validator Variables (Minimum Requirements)	
Validators Run	1
Uptime	99%
Cost of Computer Hardware	$250
Cost of Router Hardware	$100
Useful Life (yrs)	3.5
Watts	100
Cost per kwh	$0.15
ISP (Per month)	$40.00
Additional Overhead (per client)	$50
Exclude ISP Costs? (Sunk Cost)	Yes
Capacity of Validators Run/Client	10
Number of Clients	1
Initial Investment	**$4,402**

Calculations

Network Calcs	Value
Validators/Shards	305
Network Validators	312,500
epoch/year	82,125
reward quotient	3,237,888
reward/epoch	3.09
Generated ETH/Year	253,638
Network Inflation	0.24%

Validator P&L	
ETH Staked	32
Staker Interest	2.54%
Staker interest ($)	$102
Gas Fee Rev	$117
Total Staker Rev	**$218**
Slashing Costs	$1
Power Usage Costs	$131
Depreciation Costs	$71
Internet Costs	$0
Additional Overhead	$50
Total Validator Costs	**$204**
Annual Profit	**$15**
Profit Margin	**6.66%**

Initial Investment	$4,403
Profit Margin	6.66%
Net Yield	**0.36%**

Validator Net Yield

Network Fees/Day

Network ETH at Stake	100	200	300	400	500	600	700	800	900	1000	1100	1200	1300
1,000,000	6.5%	10.2%	13.8%	17.5%	21.1%	24.8%	28.4%	32.1%	35.7%	39.4%	43.0%	46.7%	50.3%
2,000,000	2.4%	4.2%	6.0%	7.8%	9.7%	11.5%	13.3%	15.1%	17.0%	18.8%	20.6%	22.4%	24.3%
3,000,000	0.7%	2.0%	3.2%	4.4%	5.6%	6.8%	8.0%	9.3%	10.5%	11.7%	12.9%	14.1%	15.3%
4,000,000	-0.2%	0.7%	1.6%	2.6%	3.5%	4.4%	5.3%	6.2%	7.1%	8.0%	8.9%	9.9%	10.8%
5,000,000	-0.8%	-0.1%	0.7%	1.4%	2.1%	2.9%	3.6%	4.3%	5.1%	5.8%	6.5%	7.2%	8.0%
6,000,000	-1.2%	-0.6%	0.0%	0.6%	1.2%	1.8%	2.4%	3.0%	3.6%	4.3%	4.9%	5.5%	6.1%
7,000,000	-1.5%	-1.0%	-0.5%	0.0%	0.5%	1.1%	1.6%	2.1%	2.6%	3.1%	3.7%	4.2%	4.7%
8,000,000	-1.8%	-1.3%	-0.9%	-0.4%	0.0%	0.5%	0.9%	1.4%	1.8%	2.3%	2.8%	3.2%	3.7%
9,000,000	-2.0%	-1.6%	-1.2%	-0.8%	-0.4%	0.0%	0.4%	0.8%	1.2%	1.6%	2.0%	2.4%	2.9%
10,000,000	-2.2%	-1.8%	-1.5%	-1.1%	-0.7%	-0.4%	0.0%	0.4%	0.7%	1.1%	1.5%	1.8%	2.2%
11,000,000	-2.3%	-2.0%	-1.7%	-1.3%	-1.0%	-0.7%	-0.4%	0.0%	0.3%	0.6%	1.0%	1.3%	1.6%
12,000,000	-2.5%	-2.2%	-1.9%	-1.6%	-1.3%	-1.0%	-0.6%	-0.3%	0.0%	0.3%	0.6%	0.9%	1.2%
13,000,000	-2.6%	-2.3%	-2.0%	-1.7%	-1.5%	-1.2%	-0.9%	-0.6%	-0.3%	-0.1%	0.2%	0.5%	0.8%
14,000,000	-2.7%	-2.4%	-2.2%	-1.9%	-1.6%	-1.4%	-1.1%	-0.9%	-0.6%	-0.3%	-0.1%	0.2%	0.4%
15,000,000	-2.8%	-2.5%	-2.3%	-2.0%	-1.8%	-1.6%	-1.3%	-1.1%	-0.8%	-0.6%	-0.3%	-0.1%	0.1%
16,000,000	-2.9%	-2.6%	-2.4%	-2.2%	-1.9%	-1.7%	-1.5%	-1.3%	-1.0%	-0.8%	-0.6%	-0.3%	-0.1%
17,000,000	-2.9%	-2.7%	-2.5%	-2.3%	-2.1%	-1.9%	-1.6%	-1.4%	-1.2%	-1.0%	-0.8%	-0.6%	-0.4%
18,000,000	-3.0%	-2.8%	-2.6%	-2.4%	-2.2%	-2.0%	-1.8%	-1.6%	-1.4%	-1.2%	-1.0%	-0.8%	-0.6%
19,000,000	-3.1%	-2.9%	-2.7%	-2.5%	-2.3%	-2.1%	-1.9%	-1.7%	-1.5%	-1.3%	-1.1%	-0.9%	-0.7%
20,000,000	-3.1%	-2.9%	-2.7%	-2.6%	-2.4%	-2.2%	-2.0%	-1.8%	-1.6%	-1.5%	-1.3%	-1.1%	-0.9%
21,000,000	-3.2%	-3.0%	-2.8%	-2.6%	-2.5%	-2.3%	-2.1%	-1.9%	-1.8%	-1.6%	-1.4%	-1.2%	-1.1%
22,000,000	-3.2%	-3.0%	-2.9%	-2.7%	-2.5%	-2.4%	-2.2%	-2.0%	-1.1%	-0.9%	-0.8%	-0.6%	-0.5%
23,000,000	-2.5%	-2.3%	-2.2%	-2.0%	-1.9%	-1.7%	-1.5%	-1.4%	-1.2%	-1.1%	-0.9%	-0.7%	-0.6%

Validator Net Yield

Network Fees/Day

ETH Price	100	200	300	400	500	600	700	800	900	1000	1100	1200	1300
$50	-9.8%	-9.4%	-9.1%	-8.7%	-8.3%	-8.0%	-7.6%	-7.2%	-6.9%	-6.5%	-6.2%	-5.8%	-5.4%
$100	-3.5%	-3.1%	-2.7%	-2.4%	-2.0%	-1.6%	-1.3%	-0.9%	-0.5%	-0.2%	0.2%	0.6%	0.9%
$150	-1.3%	-1.0%	-0.6%	-0.3%	0.1%	0.5%	0.8%	1.2%	1.6%	1.9%	2.3%	2.7%	3.0%
$200	-0.3%	0.1%	0.4%	0.8%	1.2%	1.5%	1.9%	2.3%	2.6%	3.0%	3.4%	3.7%	4.1%
$250	0.3%	0.7%	1.1%	1.4%	1.8%	2.2%	2.5%	2.9%	3.3%	3.6%	4.0%	4.4%	4.7%
$300	0.8%	1.1%	1.5%	1.9%	2.2%	2.6%	3.0%	3.3%	3.7%	4.0%	4.4%	4.8%	5.1%
$350	1.1%	1.4%	1.8%	2.2%	2.5%	2.9%	3.3%	3.6%	4.0%	4.4%	4.7%	5.1%	5.4%
$400	1.3%	1.7%	2.0%	2.4%	2.8%	3.1%	3.5%	3.8%	4.2%	4.6%	4.9%	5.3%	5.7%
$450	1.5%	1.8%	2.2%	2.6%	2.9%	3.3%	3.7%	4.0%	4.4%	4.8%	5.1%	5.5%	5.8%
$500	1.6%	2.0%	2.3%	2.7%	3.1%	3.4%	3.8%	4.2%	4.5%	4.9%	5.3%	5.6%	6.0%
$550	1.7%	2.1%	2.5%	2.8%	3.2%	3.5%	3.9%	4.3%	4.6%	5.0%	5.4%	5.7%	6.1%
$600	1.8%	2.2%	2.5%	2.9%	3.3%	3.6%	4.0%	4.4%	4.7%	5.1%	5.5%	5.8%	6.2%
$650	1.9%	2.3%	2.6%	3.0%	3.4%	3.7%	4.1%	4.5%	4.8%	5.2%	5.6%	5.9%	6.3%
$700	2.0%	2.3%	2.7%	3.1%	3.4%	3.8%	4.2%	4.5%	4.9%	5.3%	5.6%	6.0%	6.4%
$750	2.0%	2.4%	2.8%	3.1%	3.5%	3.9%	4.2%	4.6%	5.0%	5.3%	5.7%	6.0%	6.4%
$800	2.1%	2.4%	2.8%	3.2%	3.5%	3.9%	4.3%	4.6%	5.0%	5.4%	5.7%	6.1%	6.5%
$850	2.1%	2.5%	2.9%	3.2%	3.6%	4.0%	4.3%	4.7%	5.1%	5.4%	5.8%	6.1%	6.5%
$900	2.2%	2.5%	2.9%	3.3%	3.6%	4.0%	4.4%	4.7%	5.1%	5.5%	5.8%	6.2%	6.6%
$950	2.2%	2.6%	2.9%	3.3%	3.7%	4.0%	4.4%	4.8%	5.1%	5.5%	5.9%	6.2%	6.6%
$1,000	2.2%	2.6%	3.0%	3.3%	3.7%	4.1%	4.4%	4.8%	5.2%	5.5%	5.9%	6.3%	6.6%
$1,050	2.3%	2.6%	3.0%	3.4%	3.7%	4.1%	4.5%	4.8%	5.2%	5.6%	5.9%	6.3%	6.7%
$1,100	2.3%	2.7%	3.0%	3.4%	3.8%	4.1%	4.5%	4.9%	5.2%	5.6%	5.9%	6.3%	6.7%
$1,150	2.3%	2.7%	3.1%	3.4%	3.8%	4.1%	4.5%	4.9%	5.2%	5.6%	6.0%	6.3%	6.7%

Validator Net Yield

Network ETH at Stake \ ETH Price	150	250	350	450	550	650	750	850	950	1050	1150	1250	1350
1,000,000	36.56%	38.25%	38.98%	39.38%	39.64%	39.81%	39.94%	40.04%	40.12%	40.19%	40.24%	40.28%	40.32%
2,000,000	17.81%	19.50%	20.23%	20.63%	20.89%	21.07%	21.20%	21.29%	21.37%	21.44%	21.49%	21.53%	21.57%
3,000,000	11.31%	13.00%	13.72%	14.13%	14.38%	14.56%	14.69%	14.79%	14.87%	14.93%	14.98%	15.03%	15.06%
4,000,000	7.96%	9.65%	10.37%	10.77%	11.03%	11.21%	11.34%	11.44%	11.52%	11.58%	11.63%	11.68%	11.71%
5,000,000	5.90%	7.59%	8.31%	8.71%	8.97%	9.15%	9.28%	9.38%	9.45%	9.52%	9.57%	9.61%	9.65%
6,000,000	4.49%	6.18%	6.91%	7.31%	7.56%	7.74%	7.87%	7.97%	8.05%	8.11%	8.17%	8.21%	8.25%
7,000,000	3.47%	5.16%	5.88%	6.29%	6.54%	6.72%	6.85%	6.95%	7.03%	7.09%	7.14%	7.19%	7.23%
8,000,000	2.69%	4.38%	5.10%	5.51%	5.76%	5.94%	6.07%	6.17%	6.25%	6.31%	6.36%	6.41%	6.44%
9,000,000	2.07%	3.76%	4.49%	4.89%	5.14%	5.32%	5.45%	5.55%	5.63%	5.69%	5.75%	5.79%	5.83%
10,000,000	1.57%	3.26%	3.99%	4.39%	4.64%	4.82%	4.95%	5.05%	5.13%	5.19%	5.24%	5.29%	5.33%
11,000,000	1.16%	2.85%	3.57%	3.97%	4.23%	4.41%	4.54%	4.64%	4.71%	4.78%	4.83%	4.87%	4.91%
12,000,000	0.80%	2.49%	3.22%	3.62%	3.88%	4.05%	4.18%	4.28%	4.36%	4.43%	4.48%	4.52%	4.56%
13,000,000	0.50%	2.19%	2.92%	3.32%	3.58%	3.75%	3.88%	3.98%	4.06%	4.13%	4.18%	4.22%	4.26%
14,000,000	0.24%	1.93%	2.66%	3.06%	3.32%	3.49%	3.62%	3.72%	3.80%	3.87%	3.92%	3.96%	4.00%
15,000,000	0.01%	1.71%	2.43%	2.83%	3.09%	3.27%	3.40%	3.49%	3.57%	3.64%	3.69%	3.73%	3.77%
16,000,000	-0.19%	1.50%	2.23%	2.63%	2.89%	3.06%	3.19%	3.29%	3.37%	3.43%	3.49%	3.53%	3.57%
17,000,000	-0.37%	1.32%	2.05%	2.45%	2.71%	2.88%	3.01%	3.11%	3.19%	3.25%	3.31%	3.35%	3.39%
18,000,000	-0.53%	1.16%	1.89%	2.29%	2.54%	2.72%	2.85%	2.95%	3.03%	3.09%	3.15%	3.19%	3.23%
19,000,000	-0.67%	1.02%	1.74%	2.14%	2.40%	2.58%	2.71%	2.81%	2.88%	2.95%	3.00%	3.04%	3.08%
20,000,000	-0.81%	0.88%	1.61%	2.01%	2.27%	2.44%	2.57%	2.67%	2.75%	2.81%	2.87%	2.91%	2.95%
21,000,000	-0.93%	0.76%	1.49%	1.89%	2.14%	2.32%	2.45%	2.55%	2.63%	2.69%	2.75%	2.79%	2.83%
22,000,000	-1.04%	0.65%	1.38%	1.78%	2.03%	2.21%	2.34%	2.44%	2.52%	2.58%	2.63%	2.68%	2.72%
23,000,000	-1.14%	0.55%	1.27%	1.68%	1.93%	2.11%	2.24%	2.34%	2.42%	2.48%	2.53%	2.58%	2.61%

Conclusion

To wrap up, let’s look at a few scenarios that result in a ~2.59% net yield, which represents the current yield of a one year US treasury.

Cloud Economics

ETH Price = $125

Network ETH at Stake = 1,000,000

Network Fees/Day = 500

Net Yield = 2.90%

ETH Price = $350

Network ETH at Stake = 3,000,000

Network Fees/Day = 800

Net Yield = 2.68%

ETH Price = $750

Network ETH at Stake = 10,000,000

Network Fees/Day = 1100

Net Yield = 2.65%

Hardware Economics

ETH Price = $125

Network ETH at Stake = 7,000,000

Network Fees/Day = 900

Net Yield = 2.60%

ETH Price = $300

Network ETH at Stake = 10,000,000

Network Fees/Day = 600

Net Yield = 2.47%

ETH Price = $550

Network ETH at Stake = 18,000,000

Network Fees/Day = 800

Net Yield = 2.54%

The current spec of Ethereum 2.0 with ETH at $125 results in net yields that are highly unlikely to attract a small validator, a validator type that is crucial for a blockchain network to have proper distribution. Especially given the risk and barriers to entry that exist when staking on a blockchain network.

Overall, there are multiple moving pieces that could change the net yield to a small validator at the current spec (most of which cannot be accurately predicted), however the current analysis leaves me thinking……..Please, decentralized sir, I want some more?

The economics of Ethereum 2.0 is a topic we are very interested in at ConsenSys and will continue to do our part adding value to its reality. If any readers would like to take a deeper look at the models see here. Please use this as an opportunity to challenge what has been presented if you disagree with it and we can get a healthy debate started.

You can expect follow up articles on the economics of large scale validators and a layer 1 yield comparison in the near future.

Special thanks to Tanner Hoban, Jon Stevens, Jonny Rhea, Antoine Toulme, Eric Conner, and the Alpine team for providing suggestions/feedback for this piece.

What A Time To Be Alive!

Disclaimer

Nothing in this piece should be considered investment advice.

Blockchain Cryptocurrency Ethereum Bitcoin Investing

Collin J. Myers

Global Head of Business Development@tokenfoundry @consensys

Follow

Token Economy

Keeping track of new developments in the distributed ledger technology space. We'll feature interesting stories on our Medium channel, while the weekly newsletter will go straight to the inbox, so make sure you subscribe at weekly.tokeneconomy.co

Follow

Sep 14, 2017

Although the ideas behind the current Ethereum protocol have largely been stable for two years, Ethereum did not emerge all at once, in its current conception and fully formed. Before the blockchain has launched, the protocol went through a number of significant evolutions and design decisions. The purpose of this article will be to go through the various evolutions that the protocol went through from start to launch; the countless work that was done on the implementations of the protocol such as Geth, cppethereum, pyethereum, and EthereumJ, as well as the history of applications and businesses in the Ethereum ecosystem, is deliberately out of scope.

Also out of scope is the history of Casper and sharding research. While we can certainly make more blog posts talking about all of the various ideas Vlad, Gavin, myself and others came up with, and discarded, including “proof of proof of work”, hub-and-spoke chains, “hypercubes”, shadow chains (arguably a precursor to Plasma), chain fibers, and various iterations of Casper, as well as Vlad’s rapidly evolving thoughts on reasoning about incentives of actors in consensus protocols and properties thereof, this would also be far too complex a story to go through in one post, so we will leave it out for now.

Let us first begin with the very earliest version of what would eventually become Ethereum, back when it was not even called Ethereum. When I was visiting Israel in October 2013, I spent quite a bit of time with the Mastercoin team, and even suggested a few features for them. After spending a couple of times thinking about what they were doing, I sent the team a proposal to make their protocol more generalized and support more types of contracts without adding an equally large and complex set of features:

https://web.archive.org/web/20150627031414/http://vbuterin.com/ultimatescripting.html

Ultimate Scripting: A Platform for Generalized Financial Contracts on Mastercoin

0.1. Introduction

Perhaps the key advantage of Mastercoin over the raw Bitcoin protocol is the potential to include much more advanced transaction types, including transactions that specify behavior based on future information well off into the future. For example, Mastercoin joins Ripple in being one of the only two major cryptocurrency networks that include the ability for users to make binding exchange offers as a type of transaction. From there, the Mastercoin Foundation intends to integrate even more complex contracts, including bets, contracts for difference and on-blockchain dice rolls. However, up until this point Mastercoin has been taking a relatively unstructured process in developing these idea, essentially treating each one as a separate "feature" with its own transaction code and rules. This document outlines an alternative way of specifying Mastercoin contracts which follows an open-ended philosophy, specifying only the basic data and arithmetic building blocks and allowing anyone to craft arbitrarily complex Mastercoin contracts to suit their own needs, including needs which we may not even anticipate.

0.2. Specification

The underlying idea behind this specification is to allow anyone to create a contract which pays out according to an arbitrary formula. The formula will be defined in a Bitcoin-like stack-based scripting language, consisting of numbers and opcodes.

The evaluation algorithm is as follows:

```
dataStack = []
opStack = script
while len(opStack) > 0:
    var op = opStack.pop()
    if typeof(op) == 'opcode': eval(dataStack,op)
    else: dataStack.push(op)
return dataStack.pop()
```

Where `eval` is defined for each opcode below. Any error (eg. division by zero) will make the script return `FAIL`, and result in the entire transaction being treated as invalid by the Mastercoin network. All variables will be signed 64-bit integers, and all arithmetic operations wrap around (that is, if the underlying arithmetic operation returns `R`, the value pushed is `((R + 2^63) % 2^64) - 2^63`.

Notice that this is very far from the later and more expansive vision of Ethereum: it specialized purely in what Mastercoin was trying to specialize in already, namely two-party contracts where parties A and B would both put in money, and then they would later get money out according to some formula specified in the contract (eg. a bet would say “if X happens then give all the money to A, otherwise give all the money to B”). The scripting language was not Turing-complete.

The Mastercoin team was impressed, but they were not interested in dropping everything they were doing to go in this direction, which I was increasingly convinced is the correct choice. So here comes version 2, circa December:

https://web.archive.org/web/20131219030753/http://vitalik.ca/ethereum.html

Ethereum: The Ultimate Smart Contract and Autonomous Corporation Platform on the Blockchain

In the last few months, there has been a great amount of interest into the area of using the Bitcoin blockchain, the mechanism that allows for the entire world to agree on the state of a public ownership database, for more than just money. Perhaps the first, and oldest, such alternative application is colored coins, which is a protocol that allows users to label specific bitcoins and treat them as assets representing some real world value - whether company shares, collectibles or even existing currencies like gold and USD. A more independent alternative, Ripple, also includes the ability to create custom currencies and assets, but adds a decentralized exchange. More recently, Mastercoin has started to go even further, allowing more complex financial contracts such as hedging, trust-free dice rolls, binary options and self-stabilizing currencies - essentially, almost any common financial instrument imaginable. Taken together, all of these projects can be thought of as initial efforts toward a sort of "cryptocurrency 2.0" - they are to Bitcoin what Web 2.0 was to the World Wide Web circa 1995.

At the same time, there has been significant interest in "decentralized autonomous corporations" - autonomous entities that operate on the blockchain in a completely transparent and publicly managed way without any central control whatsoever. Rather than the relationships of the investors, owners and employees of the corporation being mediated by a legal contract or a set of organizational bylaws, the funds and corporate resources are managed directly on the blockchain. However, decentralized autonomous corporations are difficult to implement today, simply because the scripting systems of Bitcoin, and even proto-cryptocurrency 2.0 alternatives like Ripple and Mastercoin, are far too limited to allow the kind of arbitrarily complex computation that DACs require. Although these platforms have begun to offer increasingly complex contracts such as financial derivatives, order matching and trust-free bets, the way that the protocols are set up is inherently limited and closed-ended: each of these use cases is treated as a specific transaction type, not allowing any way for users to build contracts that the developers have not specifically chosen to include.

What this project intends to do is take cryptocurrency 2.0, and generalize it - create a fully-fledged, Turing-complete (but heavily fee-regulated) cryptographic ledger that allows participants to encode arbitrarily complex contracts, autonomous agents and relationships that will be mediated entirely by the blockchain. On-chain currencies, futures contracts, prediction markets, Namecoin-style domain name systems and even provably fair gambling sites will become trivial to implement, existing as simple, hundred-line-of-code contracts on the chain.

Basic Building Blocks

Here you can see the results of a substantial rearchitecting, largely a result of a long walk through San Francisco I took in November once I realized that smart contracts could potentially be fully generalized. Instead of the scripting language being simply a way of describing the terms of relations between two parties, contracts were themselves fully-fledged accounts, and had the ability to hold, send and receive assets, and even maintain a permanent storage (back then, the permanent storage was called “memory”, and the only temporary “memory” was the 256 registers). The language switched from being a stack-based machine to being a register-based one on my own volition; I had little argument for this other than that it seemed more

sophisticated.

Additionally, notice that there is now a built-in fee mechanism:

Whenever ether is sent to a script, the following happens:

1. The ether's endowment increases by the amount sent
2. All registers are reset to zero.
3. The sender is placed into R0.
4. The value sent is placed into R1.
5. The fee is placed into R2.
6. The index pointer is set to zero, and `STEPCOUNT = 0`
7. Repeat forever:
    - set `TOTALFEE = 0`
    - set `STEPCOUNT <- STEPCOUNT + 1`
    - if `STEPCOUNT > 16`, set `TOTALFEE <- TOTALFEE + STEPFEE`
    - see if the command at the index pointer is a valid command and not `STOP`. If it is invalid or `STOP`, HALT and break out of the loop
    - see if the command will do any modifications to the contract. If so, set `TOTALFEE <- TOTALFEE + DATAFEE`
    - see if the command will fill up a previously zero memory field. If so, set `TOTALFEE <- TOTALFEE + MEMORYFEE`
    - see if the commend will zero a previously used memory field. If so, set `TOTALFEE <- TOTALFEE - MEMORYFEE`
    - see if the command is `EXTRO` or `BALANCE`. If so, set `TOTALFEE <- TOTALFEE + EXTROFEE`
    - see if the command is `MKTX` or `RAWTX`. If so, set `TOTALFEE <- TOTALFEE + (transaction's value plus transaction's fee)`
    - if `TOTALFEE > contract's endowment`, HALT and break out of the loop
    - else, subtract `TOTALFEE` from contract's endowment. Note that `TOTALFEE` may be negative in some cases, in which case the endowment would actually increase
    - run the command

At this point, ether literally was gas; after every single computational step, the balance of the contract that a transaction was calling would drop a little bit, and if the contract ran out of money execution would halt. Note that this “receiver pays” mechanism meant that the contract itself had to require the sender to pay the contract a fee, and immediately exit if this fee is not present; the protocol allocated an allowance of 16 free execution steps to allow contracts to reject non-fee-paying transactions.

This was the time when the Ethereum protocol was entirely my own creation. From here on, however, new participants started to join the fold. By far the most prominent on the protocol side was Gavin Wood, who reached out to me in an about.me message in December 2013:

Gav Wood sent you a message on about.me
1 message

i@gavwood.com <i@gavwood.com> Thu, Dec 19, 2013 at 11:53 AM
Reply-To: i@gavwood.com
To: vbuterin@gmail.com

me

Hi **Vitalik**!
View Dashboard

Gav Wood sent you a message

"Johnny gave me the heads up - I can do C++ (e.g. github/gavofyork). How far are you with ethereum?

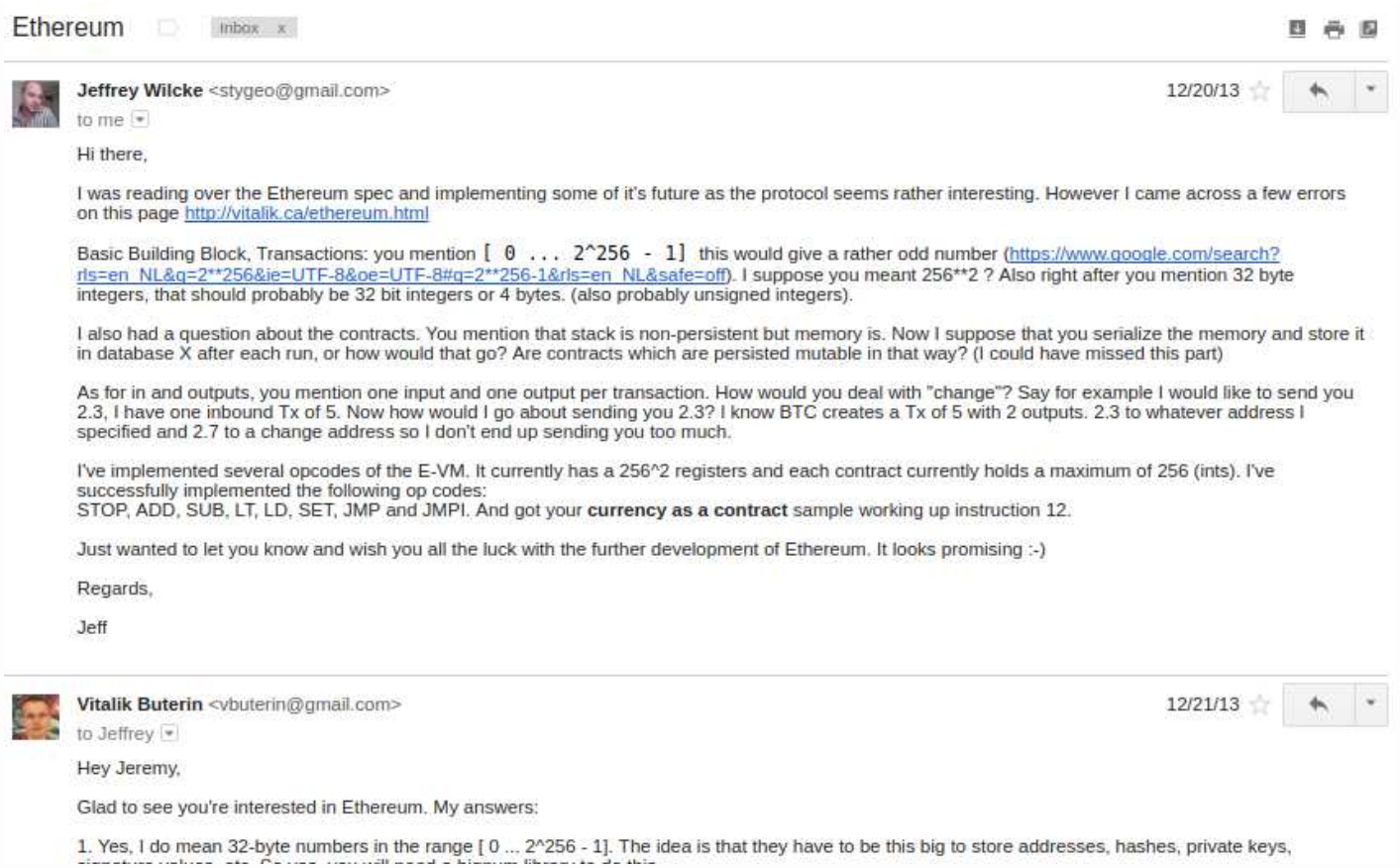
REPLY TO GAV

This email was sent to you by about.me/gavwood, and is not an official communication from about.me.

Cheers,
The about.me team

Don't want these emails? One Click Unsubscribe
Terms of Service | Privacy Policy
about.me 2601 Mission St San Francisco, CA 94110

Jeffrey Wilcke, lead developer of the Go client (back then called “ethereal”) also reached out and started coding around the same time, though his contributions were much more on the side of client development rather than protocol research.



Ethereum Inbox x

Jeffrey Wilcke <stygeo@gmail.com> 12/20/13

to me

Hi there,

I was reading over the Ethereum spec and implementing some of it's future as the protocol seems rather interesting. However I came across a few errors on this page http://vitalik.ca/ethereum.html

Basic Building Block, Transactions: you mention `[ 0 ... 2^256 - 1]` this would give a rather odd number (https://www.google.com/search?rls=en_NL&q=2**256&ie=UTF-8&oe=UTF-8#q=2**256-1&rls=en_NL&safe=off). I suppose you meant 256**2 ? Also right after you mention 32 byte integers, that should probably be 32 bit integers or 4 bytes. (also probably unsigned integers).

I also had a question about the contracts. You mention that stack is non-persistent but memory is. Now I suppose that you serialize the memory and store it in database X after each run, or how would that go? Are contracts which are persisted mutable in that way? (I could have missed this part)

As for in and outputs, you mention one input and one output per transaction. How would you deal with "change"? Say for example I would like to send you 2.3, I have one inbound Tx of 5. Now how would I go about sending you 2.3? I know BTC creates a Tx of 5 with 2 outputs. 2.3 to whatever address I specified and 2.7 to a change address so I don't end up sending you too much.

I've implemented several opcodes of the E-VM. It currently has a 256^2 registers and each contract currently holds a maximum of 256 (ints). I've successfully implemented the following op codes:
STOP, ADD, SUB, LT, LD, SET, JMP and JMPI. And got your **currency as a contract** sample working up instruction 12.

Just wanted to let you know and wish you all the luck with the further development of Ethereum. It looks promising :-)

Regards,

Jeff

Vitalik Buterin <vbuterin@gmail.com> 12/21/13

to Jeffrey

Hey Jeremy,

Glad to see you're interested in Ethereum. My answers:

1. Yes, I do mean 32-byte numbers in the range [0 ... 2^256 - 1]. The idea is that they have to be this big to store addresses, hashes, private keys,

"Hey Jeremy, glad to see you're interested in Ethereum..."

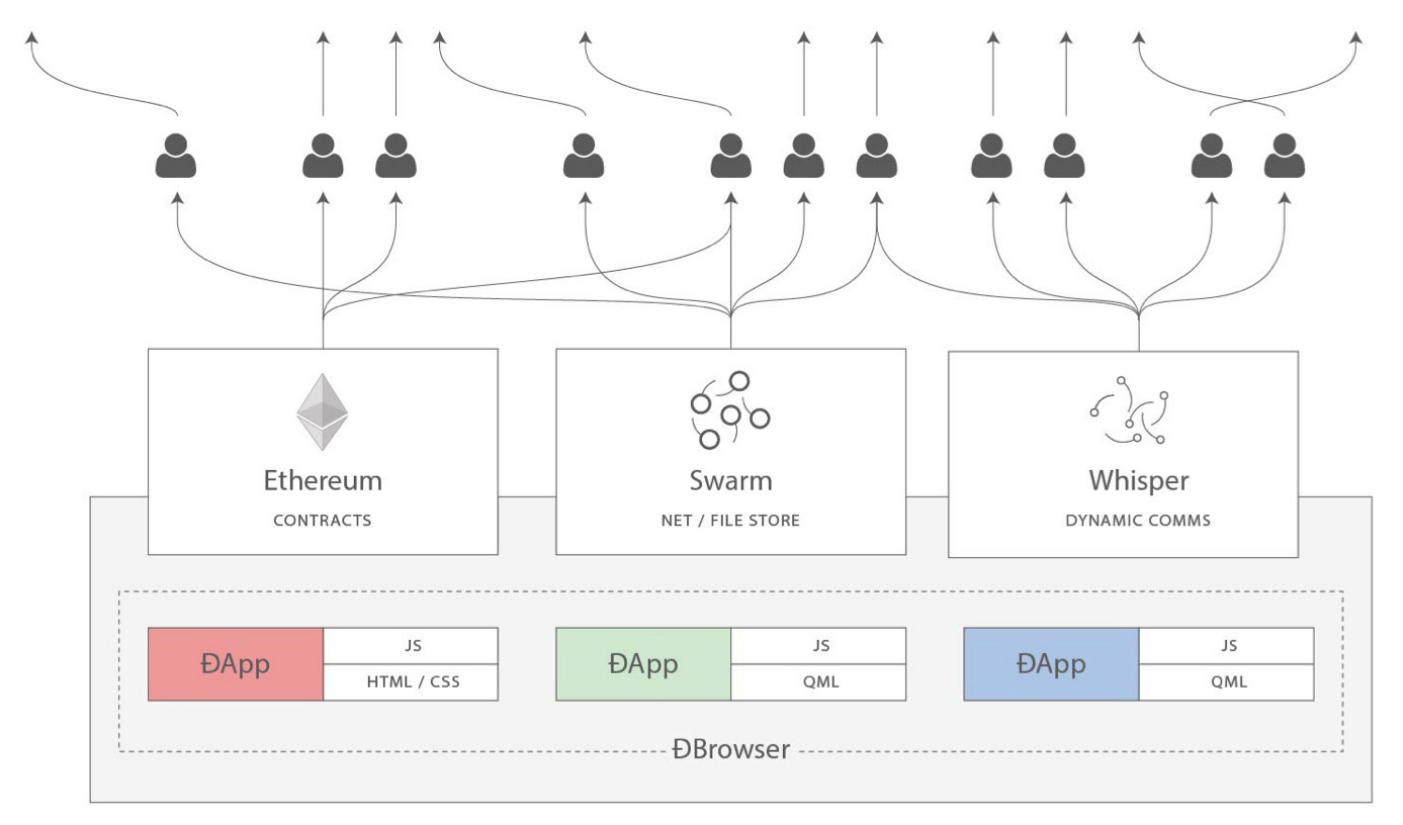
Gavin's initial contributions were two-fold. First, you might notice that the contract calling model in the initial design was an asynchronous one: although contract A could create an "internal transaction" to contract B ("internal transaction" is Etherscan's lingo; initially they were just called "transactions" and then later "message calls" or "calls"), the internal transaction's execution would not start until the execution of the first transaction completely finished. This meant that transactions could not use internal transactions as a way of getting information from other contracts; the only way to do that was the EXTRO opcode (kind of like an SLOAD that you could use to read other contracts' storage), and this too was later removed with the support of Gavin and others.

When implementing my initial spec, Gavin naturally implemented internal transactions synchronously without even realizing that the intent was different - that is to say, in Gavin's implementation, when a contract calls another contract, the internal transaction gets executed immediately, and once that execution finishes, the VM returns back to the contract that created the internal transaction and proceeds to the next opcode. This approach seemed to both of us to be superior, so we decided to make it part of the spec.

Second, a discussion between him and myself (during a walk in San Francisco, so the exact details will be forever lost to the winds of history and possibly a copy or two in the deep archives of the NSA) led to a re-factoring of the transaction fee model, moving away from the "contract pays" approach to a "sender pays" approach, and also switching to the "gas" architecture. Instead of each individual transaction step immediately taking away a bit of ether, the transaction sender pays for and is allocated some "gas" (roughly, a counter of computational steps), and

computational steps drew from this allowance of gas. If a transaction runs out of gas, the gas would still be forfeit, but the entire execution would be reverted; this seemed like the safest thing to do, as it removed an entire class of “partial execution” attacks that contracts previously had to worry about. When a transaction execution finishes, the fee for any unused gas is refunded.

Gavin can also be largely credited for the subtle change in vision from viewing Ethereum as a platform for building programmable money, with blockchain-based contracts that can hold digital assets and transfer them according to pre-set rules, to a general-purpose computing platform. This started with subtle changes in emphasis and terminology, and later this influence became stronger with the increasing emphasis on the “Web 3” ensemble, which saw Ethereum as being one piece of a suite of decentralized technologies, the other two being Whisper and Swarm.



There were also changes made around the start of 2014 that were suggested by others. We ended up moving back to a stack-based architecture after the idea was suggested by Andrew Miller and others.

On 12/19/2013 03:40 PM, Andrew Miller wrote:
> Hi Vitalik,
> I'd really like to talk with you more about this. I'm really
> interested in extending the functionality of Bitcoin beyond trivial
> money-shoving financial transactions and up to user-customizable
> contracts, and I'm pretty stoked that you're taking a shot at this as
> a serious project.
>
> Here are some specific concerns/questions about your transaction language:
>
> 1. (Note: this is my most superficial criticism) Why did you design
> your own register language? What's wrong with a stack based language
> similar to Bitcoin? You can have a turing-complete and higher order
> stack language (look at Joy, Factor or Forth). If anything I'd
> recommend a lambda-calculus based language. From Stack-based to
> Register-based is such a superficial change and there's absolutely no
> motivation for it, yet most of your document is about minutiae related
> to this. When you present your contract examples, you're writing in
> pseudocode that isn't really any closer to ASM than to stack-based or
> functional anyway. You might also look at E, a language basd on
> javascript that was explicitly designed for the purpose of writing
> smart contracts. http://www.erights.org/elang/

Charles Hoskinson suggested the switch from Bitcoin's SHA256 to the newer SHA3 (or, more accurately, keccak256). Although there was some controversy for a while, discussions with Gavin, Andrew and others led to establishing that the size of values on the stack should be limited to 32 bytes; the other alternative being considered, unlimited-size integers, had the problem that it was too difficult to figure out how much gas to charge for additions, multiplications and other operations.

The initial mining algorithm that we had in mind, back in January 2014, was a contraption called Dagger:

https://github.com/ethereum/wiki/blob/master/Dagger.md

Algorithm specification:

Essentially, the Dagger algorithm works by creating a directed acyclic graph (the technical term for a tree where each node is allowed to have multiple parents) with a total of 2^{23} - 1 nodes in sequence. Each node depends on 3-15 randomly selected nodes before it. If the miner finds a node between index 2^{22} and 2^{23} such that this resulting hash is below 2^{256} divided by the difficulty parameter, the result is a valid proof of work.

Let `D` be the underlying data (eg. in Bitcoin's case the block header), `N` be the nonce and `||` be the string concatenation operator (ie. `'foo' || 'bar' == 'foobar'`). The entire code for the algorithm is as follows:

```
D(data,xn,0) = sha3(data)
D(data,xn,n) =
    with v = sha3(data + xn + n)
         L = 2 if n < 2^21 else 11 if n < 2^22 else 3
         a[k] = floor(v/n^k) mod n for 0 <= k < 2
         a[k] = floor(v/n^k) mod 2^22 for 2 <= k < L
    sha3(v ++ D(data,xn,a[0]) ++ D(data,xn,a[1]) ++ ... ++ D(data,xn,a[L-1]))
```

Properties:

Objective: find `xn`, `n` such that `n > 2^22` and `D(data,xn,n) < 2^256 / diff`

Dagger was named after the "directed acyclic graph" (DAG), the mathematical structure that is used in the algorithm. The idea is that every N blocks, a new DAG would be pseudorandomly generated from a seed, and the bottom layer of the DAG would be a collection of nodes that takes several gigabytes to store. However, generating any individual value in the DAG would require calculating only a few thousand entries. A "Dagger computation" involved getting some number of values in random positions in this bottom-level dataset and hashing them together. This meant that there was a fast way to make a Dagger calculation - already having the data in memory, and a slow, but not memory intensive way - regenerating each value from the DAG that you need to get from scratch.

The intention of this algorithm was to have the same "memory-hardness" properties as algorithms that were popular at the time, like Scrypt, but still be light-client friendly. Miners would

use the fast way, and so their mining would be constrained by memory bandwidth (the theory is that consumer-grade RAM is already very heavily optimized, and so it would be hard to further optimize it with ASICs), but light clients could use the memory-free but slower version for verification. The fast way might take a few microseconds and the slow but memory-free way a few milliseconds, so it would still be very viable for light clients.

From here, the algorithm would change several times over the course of Ethereum development. The next idea that we went through is “adaptive proof of work”; here, the proof of work would involve executing randomly selected Ethereum contracts, and there is a clever reason why this is expected to be ASIC-resistant: if an ASIC was developed, competing miners would have the incentive to create and publish many contracts that that ASIC was not good at executing. There is no such thing as an ASIC for general computation, the story goes, as that is just a CPU, so we could instead use this kind of adversarial incentive mechanism to make a proof of work that essentially was executing general computation.

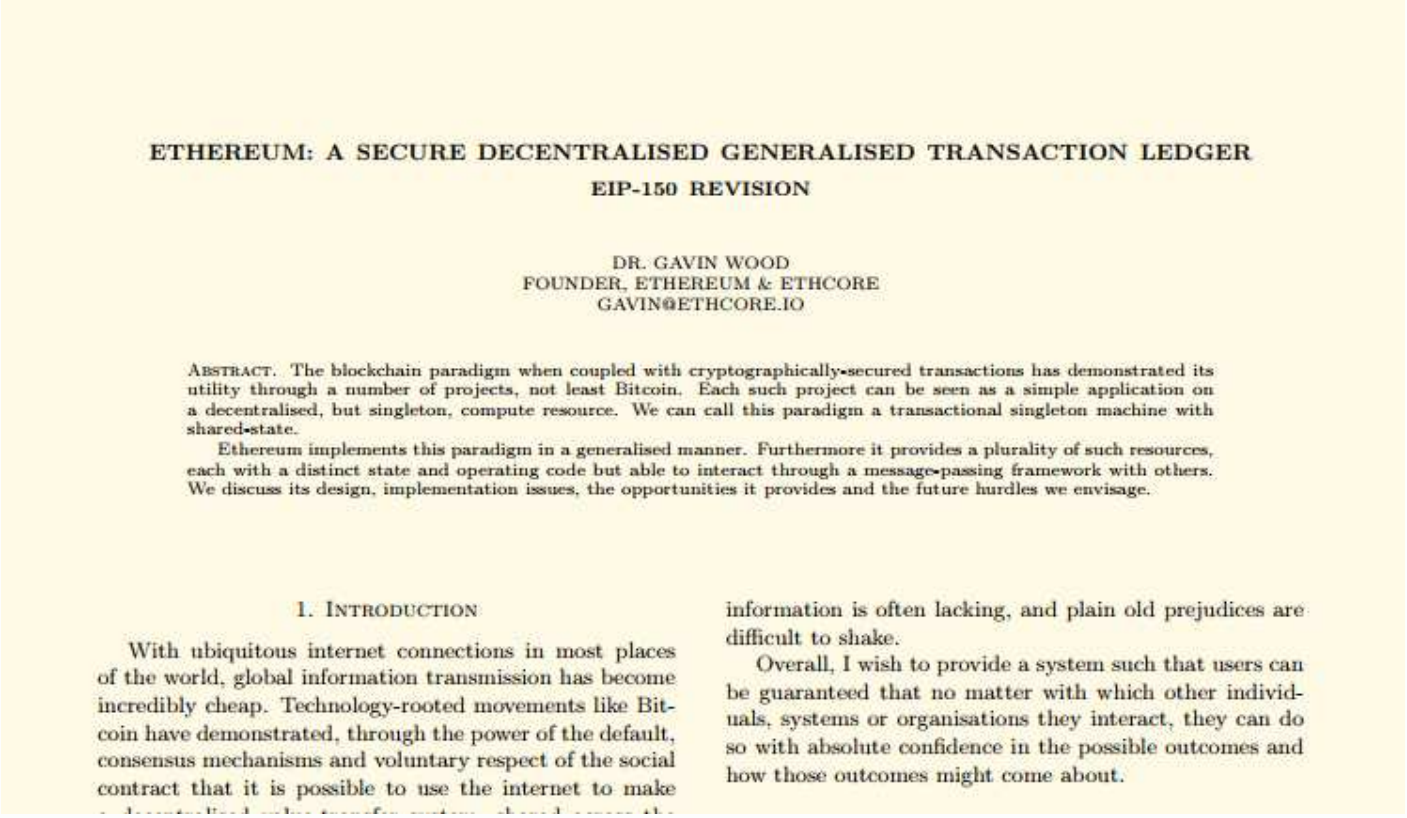
This fell apart for one simple reason:long-range attacks. An attacker could start a chain from block 1, fill it up with only simple contracts that they can create specialized hardware for, and rapidly overtake the main chain. So… back to the drawing board.

The next algorithm was something called Random Circuit, described in this google dochere, proposed by myself and Vlad Zamfir, and analyzed by Matthew Wampler-Doty and others. The idea here was also to simulate general-purpose computation inside a mining algorithm, this time by executing randomly generated circuits. There’s no hard proof that something based on these principles could not work, but the computer hardware experts that we reached out to in 2014 tended to be fairly pessimistic on it. Matthew Wampler-Doty himself suggested a proof of work based on SAT solving, but this too was ultimately rejected.

Finally, we came full circle with an algorithm called “Dagger Hashimoto”. “Dashimoto”, as it was sometimes called in short, borrowed many ideas from Hashimoto, a proof of work algorithm by Thaddeus Dryja that pioneered the notion of “I/O bound proof of work”, where the dominant limiting factor in mining speed was not hashes per second, but rather megabytes per second of RAM access. However, it combined this with Dagger’s notion of light-client-friendly DAG-generated datasets. After many rounds of tweaking by myself, Matthew, Tim and others, the ideas finally converged into the algorithm we now call Ethash.

```
def hashimoto(header, nonce, full_size, dataset_lookup):
    n = full_size / HASH_BYTES
    w = MIX_BYTES // WORD_BYTES
    mixhashes = MIX_BYTES / HASH_BYTES
    # combine header+nonce into a 64 byte seed
    s = sha3_512(header + nonce[::-1])
    # start the mix with replicated s
    mix = []
    for _ in range(MIX_BYTES / HASH_BYTES):
        mix.extend(s)
    # mix in random dataset nodes
    for i in range(ACCESSES):
        p = fnv(i ^ s[0], mix[i % w]) % (n // mixhashes) * mixhashes
        newdata = []
        for j in range(MIX_BYTES / HASH_BYTES):
            newdata.extend(dataset_lookup(p + j))
        mix = map(fnv, mix, newdata)
    # compress mix
    cmix = []
    for i in range(0, len(mix), 4):
        cmix.append(fnv(fnv(fnv(mix[i], mix[i+1]), mix[i+2]), mix[i+3]))
    return {
        "mix digest": serialize_hash(cmix),
        "result": serialize_hash(sha3_256(s+cmix))
    }

def hashimoto_light(full_size, cache, header, nonce):
    return hashimoto(header, nonce, full_size, lambda x: calc_dataset_item(cache, x)

def hashimoto_full(full_size, dataset, header, nonce):
    return hashimoto(header, nonce, full_size, lambda x: dataset[x])
```

By the summer of 2014, the protocol had considerably stabilized, with the major exception of the proof of work algorithm which would not reach the Ethash phase until around the beginning of 2015, and a semi-formal specification existed in the form of Gavin's yellow paper.



ETHEREUM: A SECURE DECENTRALISED GENERALISED TRANSACTION LEDGER

EIP-150 REVISION

DR. GAVIN WOOD
FOUNDER, ETHEREUM & ETHCORE
GAVIN@ETHCORE.IO

Abstract. The blockchain paradigm when coupled with cryptographically-secured transactions has demonstrated its utility through a number of projects, not least Bitcoin. Each such project can be seen as a simple application on a decentralised, but singleton, compute resource. We can call this paradigm a transactional singleton machine with shared-state.

Ethereum implements this paradigm in a generalised manner. Furthermore it provides a plurality of such resources, each with a distinct state and operating code but able to interact through a message-passing framework with others. We discuss its design, implementation issues, the opportunities it provides and the future hurdles we envisage.

1. Introduction

With ubiquitous internet connections in most places of the world, global information transmission has become incredibly cheap. Technology-rooted movements like Bitcoin have demonstrated, through the power of the default, consensus mechanisms and voluntary respect of the social contract that it is possible to use the internet to make

information is often lacking, and plain old prejudices are difficult to shake.

Overall, I wish to provide a system such that users can be guaranteed that no matter with which other individuals, systems or organisations they interact, they can do so with absolute confidence in the possible outcomes and how those outcomes might come about.

In August 2014, I developed and introduced the uncle mechanism, which allows Ethereum's blockchain to have a shorter block time and higher capacity while mitigating centralization risks. This was introduced as part of PoC6.

Discussions with the Bitshares team led us to consider adding heaps as a first-class data structure, though we ended up not doing this due to lack of time, and later security audits and DoS attacks will show that it is actually much harder than we had thought at the time to do this safely.

In September, Gavin and I planned out the next two major changes to the protocol design. First, alongside the state tree and transaction tree, every block would also contain a "receipt tree". The receipt tree would include hashes of the logs created by a transaction, along with intermediate state roots. Logs would allow transactions to create "outputs" that are saved in the blockchain, and are accessible to light clients, but that are not accessible to future state calculations. This could be used to allow decentralized applications to easily query for events, such as token transfers, purchases, exchange orders being created and filled, auctions being started, and so forth.

There were other ideas that were considered, like making a Merkle tree out of the entire execution trace of a transaction to allow anything to be proven; logs were chosen because they were a compromise between simplicity and completeness.

The second was the idea of "precompiles", solving the problem of allowing complex cryptographic computations to be usable in the EVM without having to deal with EVM overhead. We had also gone through many more ambitious ideas about "native contracts", where if miners have an optimized implementation of some contracts they could "vote" the gasprice of those contracts down, so contracts that most miners could execute much more quickly would naturally

have a lower gas price; however, all of these ideas were rejected because we could not come up with a cryptoeconomically safe way to implement such a thing. An attacker could always create a contract which executes some trapdoored cryptographic operation, distribute the trapdoor to themselves and their friends to allow them to execute this contract much faster, then vote the gasprice down and use this to DoS the network. Instead we opted for the much less ambitious approach of having a smaller number of precompiles that are simply specified in the protocol, for common operations such as hashes and signature schemes.

Gavin was also a key initial voice in developing the idea of "protocol abstraction" - moving as many parts of the protocol such as ether balances, transaction signing algorithms, nonces, etc into the protocol itself as contracts, with a theoretical final goal of reaching a situation where the entire ethereum protocol could be described as making a function call into a virtual machine that has some pre-initialized state. There was not enough time for these ideas to get into the initial Frontier release, but the principles are expected to start slowly getting integrated through some of the Constantinople changes, the Casper contract and the sharding specification.

This was all implemented in PoC7; after PoC7, the protocol did not really change much, with the exception of minor, though in some cases important, details that would come out through security audits…

In early 2015, came the pre-launch security audits organized by Jutta Steiner and others, which included both software code audits and academic audits. The software audits were primarily on the C++ and Go implementations, which were led by Gavin Wood and Jeffrey Wilcke, respectively, though there was also a smaller audit on my pyethereum implementation. Of the two academic audits, one was performed by Ittay Eyal (of "selfish mining" fame), and the other by Andrew Miller and others from Least Authority. The Eyal audit led to a minor protocol change: the total difficulty of a chain would not include uncles. The Least Authority audit was more focused on smart contract and gas economics, as well as the Patricia tree. This audit led to several protocol changes. One small one is the use of sha3(addr) and sha3(key) as trie keys instead of the address and key directly; this would make it harder to perform a worst-case attack on the trie.

There are useful parallels between this refund loop and the publish-subscribe function illustrated in Miller's thesis. He demonstrates several hazards that are present when the `publish` callbacks are run synchronously:

- exceptions raised during the callback would prevent execution of later callbacks
- reentrancy hazards if the callback itself executes publish(), subscribe(), or unsubscribe(): repeated actions, missing actions, and inconsistent delivery of messages

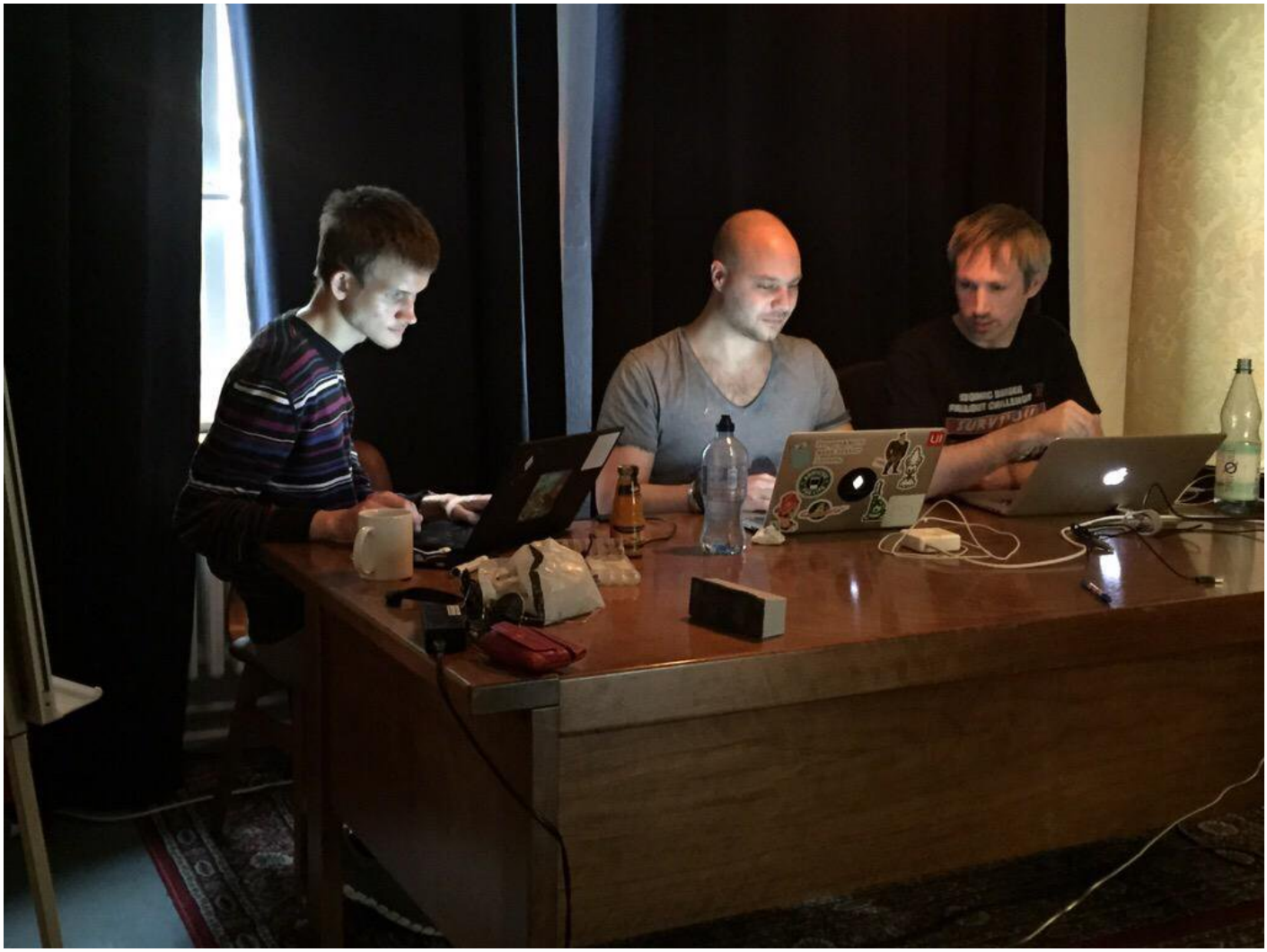
Some analogous issues in the crowdfund example are:

- delivering a contribution, after the funding deadline, with just enough gas to allow some refunds to go through, but not all: the contract could be left in a state where it was unable to refund the remaining contributions
- if the refund was triggered by a contract at the end of a long call stack, the `send` instructions will fail. However the example appears to ignore the return value of the `send`, so execution will continue. All records will be cleared, and the funds can never be recovered.
- the refund callback could make a new donation, triggering another refund cycle, potentially double-refunding the earlier contributions, or failing to refund later ones

And a warning that was perhaps a bit too far ahead of its time...

Another significant thing that we discussed was the gas limit voting mechanism. At the time, we were already concerned by perceived lack of progress in the bitcoin block size debate, and wanted to have a more flexible design in Ethereum that could adjust over time as needed. But the challenge is: what is the optimal limit? My initial thought had been to make a dynamic limit, targeting 1.5 times the long-term exponential moving average of the actual gas usage, so that in the long run on average blocks would be 2/3 full. However, Andrew showed that this was exploitable in some ways - specifically, miners who wanted to raise the limit would simply include transactions in their own blocks that consume a very large amount of gas, but take very little time to process, and thereby always create full blocks at no cost to themselves. The security model was thus, at least in the upward direction, equivalent to simply having miners vote on the gas limit.

We did not manage to come up with a gas limit strategy that was less likely to break, and so Andrew's recommended solution was to simply have miners vote on the gas limit explicitly, and have the default strategy for voting be the 1.5x EMA rule. The reasoning was that we were still very far from knowing the right approach for setting maximum gas limits, and the risk of any specific approach failing seemed greater than the risk of miners abusing their voting power. Hence, we might as well simply let miners vote on the gas limit, and accept the risk that the limit will go too high or too low, in exchange for the benefit of flexibility, and the ability for miners to work together to very quickly adjust the limit upwards or downwards as needed.



After a mini-hackathon between Gavin, Jeff and myself, PoC9 was launched in March, and was intended to be the final proof of concept release. A testnet, Olympic, ran for four months, using the protocol that was intended to be used in the livenet, and Ethereum's long-term plan was established. Vinay Gupta wrote a blog post, "The Ethereum Launch Process", that described the four expected stages of Ethereum livenet development, and gave them their current names: Frontier, Homestead, Metropolis and Serenity.

Olympic ran for four months. In the first two months, many bugs were found in the various implementations, consensus failures happened, among other issues, but around June the network noticeably stabilized. In July a decision was made to make a code-freeze, followed by a release, and on July 30 the release took place.

Vitalik Buterin's website

Vitalik Buterin's website

vbuterin
VitalikButerin

Analyzing Ethereum Classic with Google BigQuery

Yaz Khoury

Feb 6 · 14 min read

I'm happy to announce, through collaboration with Allen Day and Evgeny Medvedev of Google, Ethereum Classic is now part of the Google BigQuery dataset. There's even a CoinDesk article about it.

This means that now, it's more easier than ever to query the Ethereum Classic network using regular SQL which allows for more seamless data analysis. You can also download the datasets directly in Kaggle to use in your notebooks for analysis.

Why is this a Big Deal?

Blockchains are most accessible to cryptography and blockchain engineers, who are most familiar with the inner workings of the client and viewing the data. On the finance side, analysts mostly observe market data. For your average data scientist

or entrepreneur who wants to do quick analysis of block data, they're stuck with running their own Geth or Parity node and trying to parse it. Even if that's successful, they need to continue doing so to keep up to date with more recent Ethereum Classic data.

With the Ethereum Classic dataset being constantly available on Google BigQuery and continuously updating daily, researchers, entrepreneurs and stakeholders can quickly analyze Ethereum Classic's network and blocks without having to worry about the data engineering aspects or their cloud infrastructure or node setups. They can just focus on the data science and let us do all the rest!

How Did This Project Come About?

We at the ETC Cooperative always believed the most important stories can be told with data, and Ethereum Classic is no exception. We were planning on quantifying Ethereum Classic's decentralization for a while now, along with many other analysis we want to explore. For your average data scientist, getting blockchain data can be tricky, if not daunting.

It immediately seemed clear to us there was no easy way to query Ethereum Classic's blockchain history, so we set about looking for solutions.

Apache Airflow is used to update the dataset daily

I've stumbled upon the Ethereum-ETL library developed by Evgeny Medvedev to parse EVM based data, and quickly worked with him on adding more features to allow it to parse Ethereum Classic nodes. We also used Apache Airflow, a powerful workflow library, to update the Ethereum Classic dataset daily. It was all adapted from the original project for Ethereum dataset. If you would like to know how it was built or you'd like to build your own, check out this post.

Analyzing The Ethereum Classic Dataset

The Ethereum Classic dataset contains several tables, like `blocks`, `transactions` and `traces` which contains lots of interesting information about the blockchain activity. Furthermore, you can even analyze traces and smart contracts (who wants to analyze the DAO smart contract before and after the hack?). For more ideas on how what you can analyze with smart contracts, check out this post.

In this Medium post, we will show our analysis of a few interesting things we found in Ethereum Classic.

We set out to quantify decentralization in Ethereum Classic. For that, we will measure the Gini Coefficient of Ethereum Classic using BigQuery. The Gini coefficient is a measure of the income or wealth distribution of a population.

We will use it in two instances here:
1) Daily Top 10K Account Balances
2) Daily Mining Rewards.

Furthermore, we will be using Balaji Srinivasan's "Nakamoto Coefficient" for further analysis of Ethereum Classic, as discussed in his blog post *Quantifying Decentralization*. Nakamoto Coefficient is a proposed measure by Balaji regarding a blockchain's subsystem. It measures what is the minimum number of entities that can influence more than 51% of a subsystem. To check out that, head on over to ***Analyzing ETC With Nakamoto Coefficient*** section below. Over there, we also introduce the `nakamoto` Python library I've built for data analysis.

Running SQL on BigQuery

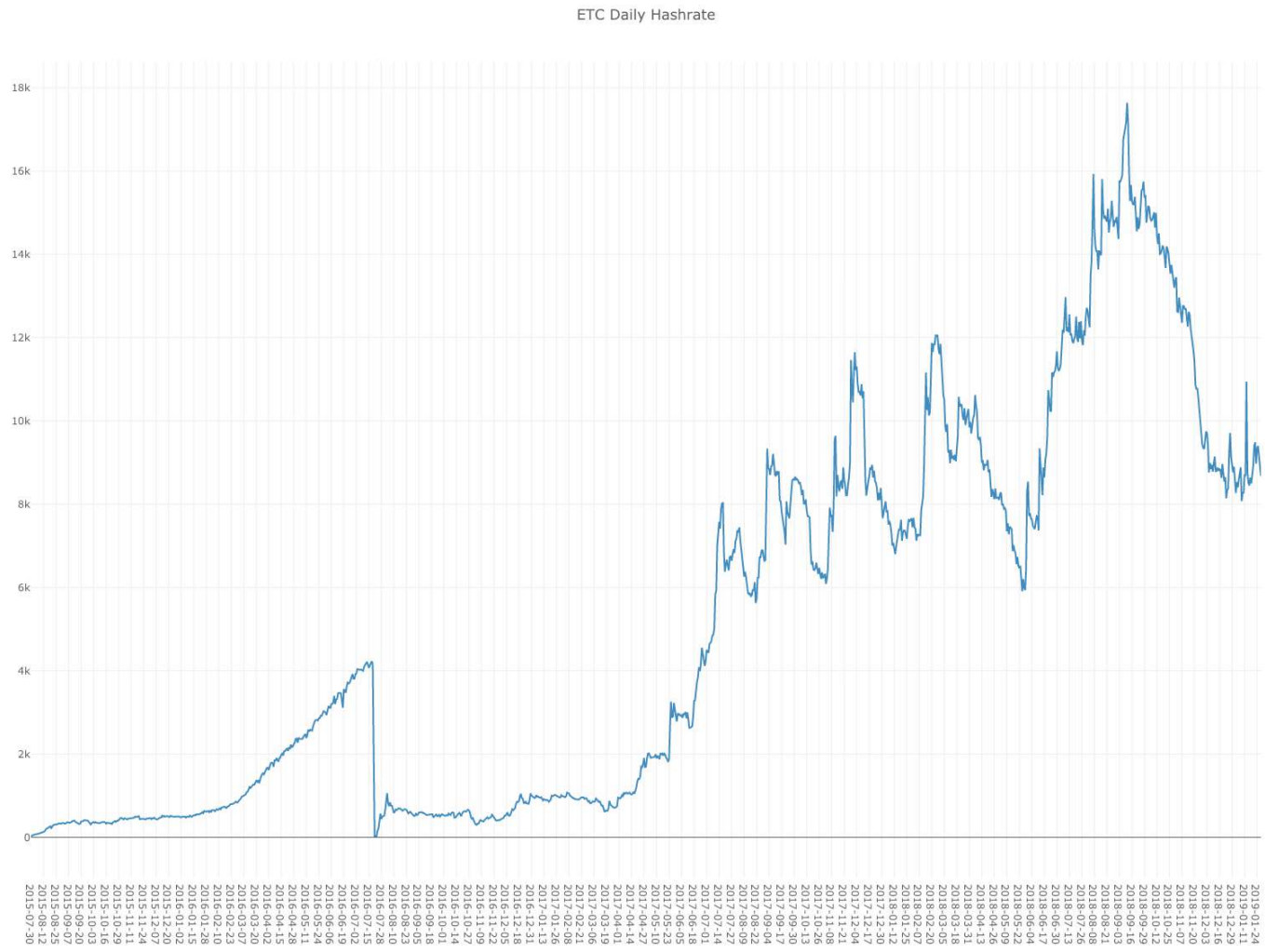
The following queries and plots have full source code in this Kaggle notebook that you can clone and run on your own.

With BigQuery, we can run a query to get the average daily hash rate as shown in the following plot.

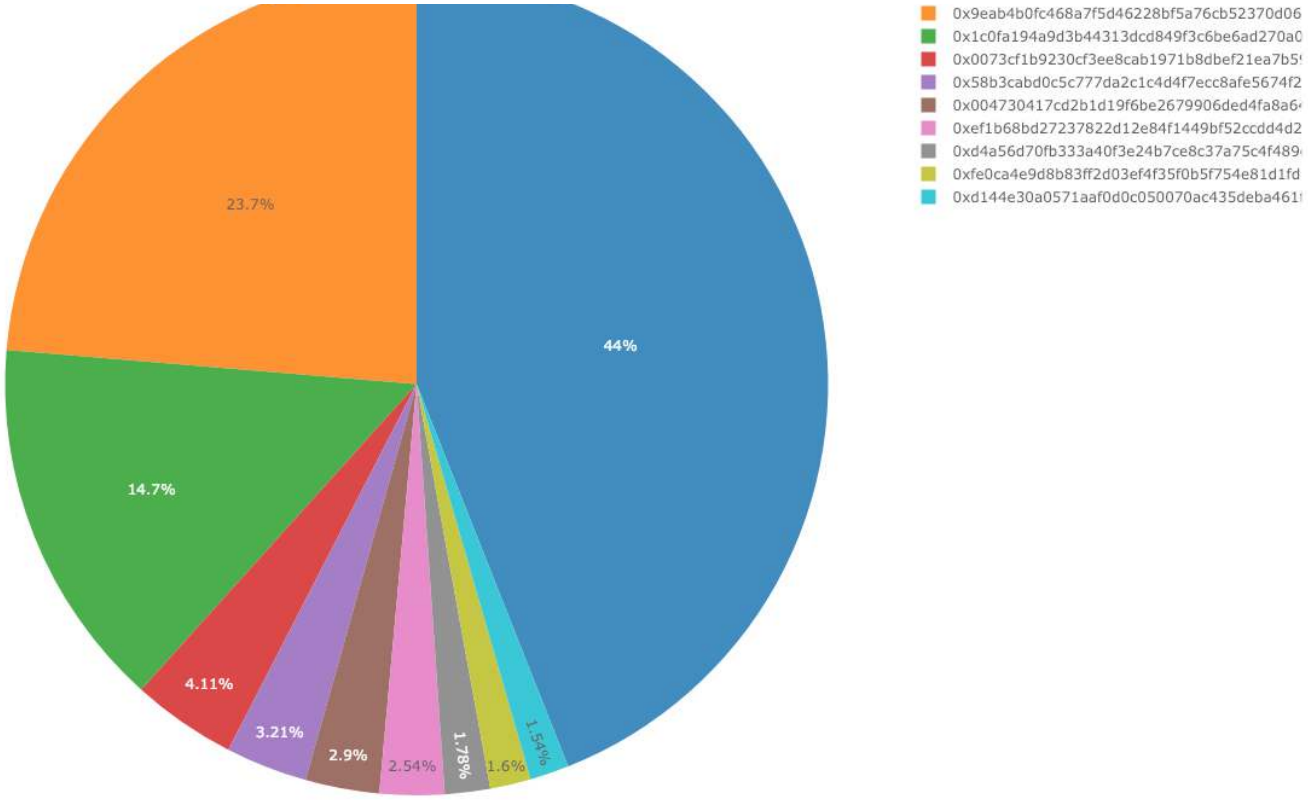
```
#standardSQL
-- MIT License
-- Copyright (c) 2019 Yaz Khoury, yaz.khoury@gmail.com

WITH block_rows AS (
```

```
    SELECT *, ROW_NUMBER() OVER (ORDER BY timestamp) AS rn
    FROM `bigquery-public-data.crypto_ethereum_classic.blocks`
  ),
  delta_time AS (
    SELECT
    mp.timestamp AS block_time,
```

We can plot the output of the following query for the hash rate using Plotly with the following graph shown here, measured in Giga hash.



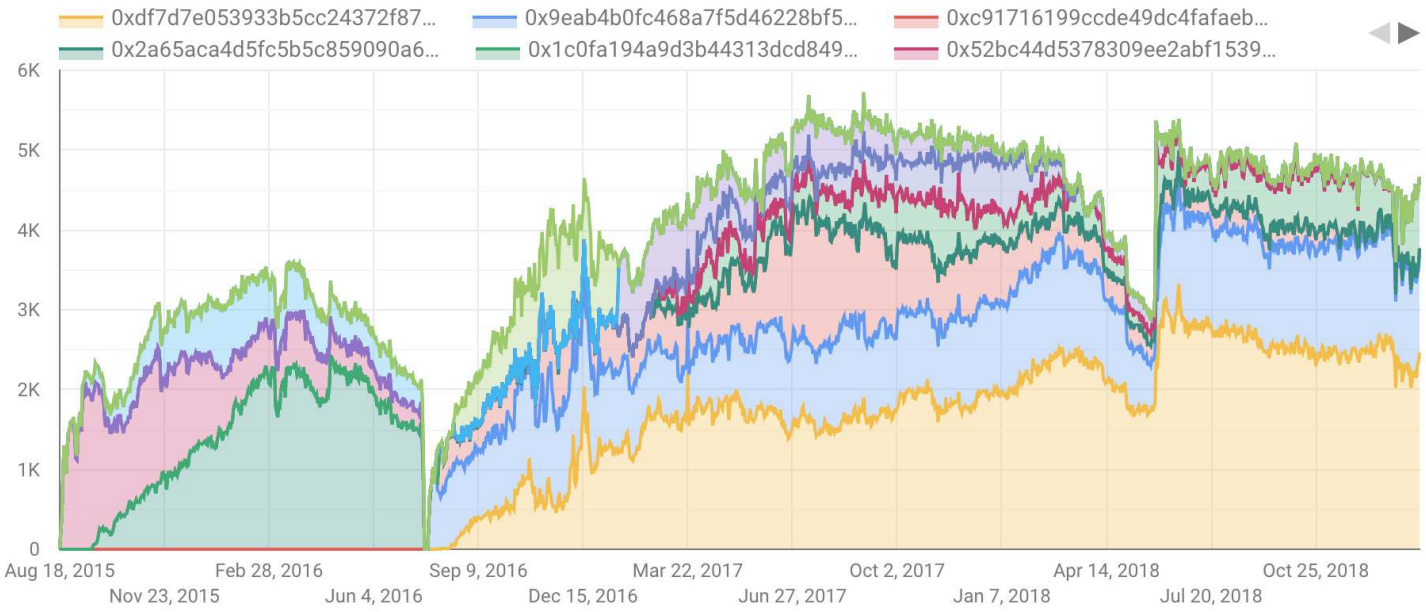
Now, let's run an analysis of the top mining addresses by the number of block rewards they received in the past 30 days. The SQL query is found here. The plot for it is shown below. I've limited the plot to top 10 miners to show it much clearly.



What about if we try to combine the total daily mining blocks found for the miners and see the change in miner accumulation of blocks found over time since genesis?

BigQuery to the rescue! With the ETC Dataset, (SQL Query is found here), you can.

The result of the query can be plotted like shown here with Google DataStudio.



Daily Miner Rewards on Ethereum Classic

As can be seen here in the Google Data Studio chart, there was a sharp drop in mining rewards around the DAO Hard fork.

Now, let's do some deeper analysis.

Given our daily block rewards are distributed to different addresses, we can make a few assumptions. We can first assume that each mining address belongs to a single entity. This helps us in our analysis by simplifying things. We will also not try to make any guesses on which addresses belong to a pool. Here, 1 address is equal to 1 entity.

Also, for simplification, we will only limit our analysis to miners who have mined more than 100 blocks a day, so that we can ignore small time individual miners. Sorry, fellas.

Now, we have the perfect parameters to measure an inequality distribution.

We can measure the daily Gini Coefficient of the total mined blocks of each miner to see if there's a centralization or inequality around a few certain miners.

The Gini coefficient, as mentioned previously, is a statistical measure of distribution used to measure income or wealth distribution among a population.

From the Investopedia article:

> *A country in which every resident has the same income would have an income Gini coefficient of 0. A country in which one resident earned all the income, while everyone else earned nothing, would have an income Gini coefficient of 1.*

The formula for the Gini is shown here:

$$G = \frac{\sum_{i=1}^{n} (2i - n - 1) x_i}{n \sum_{i=1}^{n} x_i}$$

The SQL for calculating the Gini is borrowed from Evgeny Medvedev and Allen Day of Google. What I have focused on here is to write the SQL necessary to generate the daily mining reward and how many each miner received. Then, I applied the Gini formula to measure the Gini index for each day.

```
#standardSQL
WITH total_reward_book AS (
  SELECT miner,
    DATE(timestamp) as date,
    COUNT(miner) as total_block_reward
  FROM `bigquery-public-data.crypto_ethereum_classic.blocks`
  GROUP BY miner, date
),
total_reward_book_by_date AS (
 SELECT date,
        miner AS address,
```

Let’s run this query and plot it using Plotly.

For fun, we will also compare this query to the one generated for Ethereum and plot both together.

The plotly link is shown here. I have attached a screenshot below.

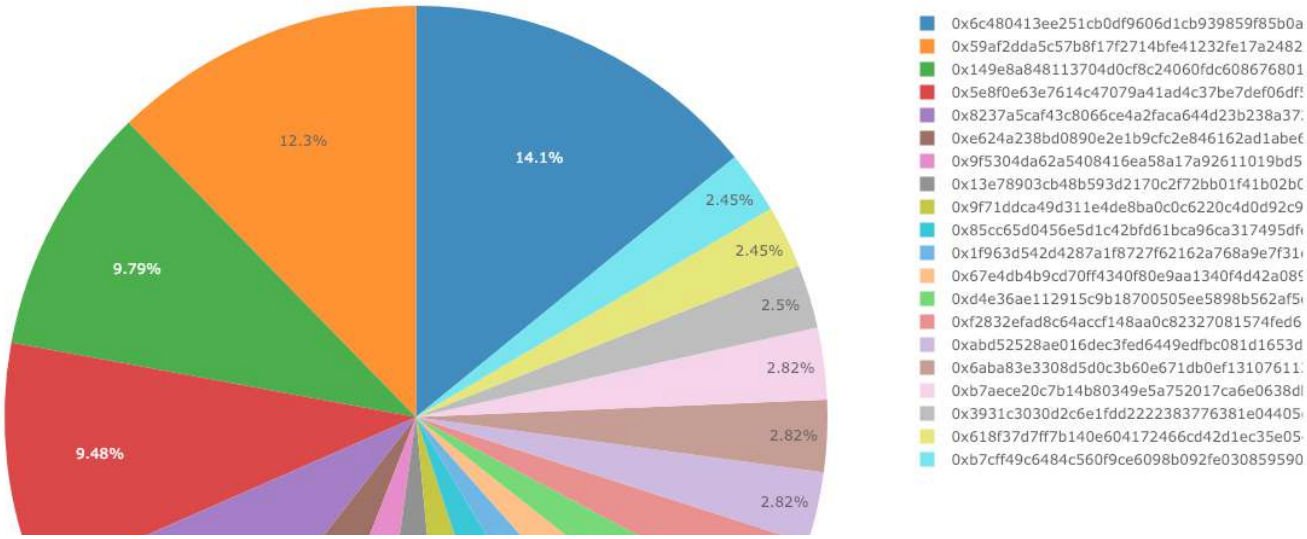
Where to even begin!?

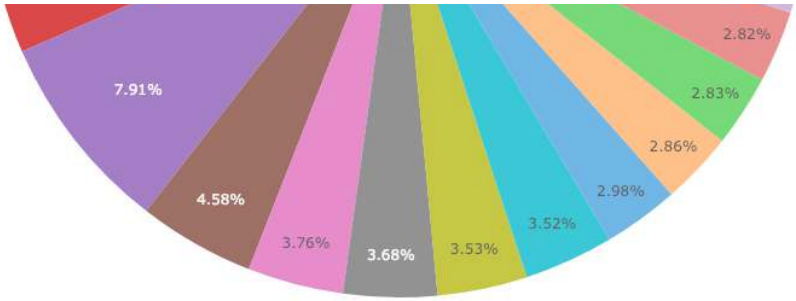
What's interesting here is that after the DAO Hard Fork, the centralization of block rewards among certain miners dropped for ETC for about a good year and a half until come early 2018 where what I call the "flippening" of Gini coefficients happen to both ETH and ETC.

I am not quite sure what happened around the early 2018 period to account for the Gini coefficient of block rewards by miners to increase on ETC. My main hypothesis here is, it must be a miner or two shifting more hash power to ETC and concentrating the mining rewards daily for themselves. It could also hint at less major mining operations happening around ETH due to fears of Proof of Stake, so the lesser Gini for ETH might just mean miners have a more equal opportunity of dividing the daily block rewards among themselves.

Let's look at another analysis.

For here, we will get the rich list of the top 10k accounts. The query to do this can be found in this post by Evgeny Medvedev. If we plot the top 20 balances, we will get this pie chart.

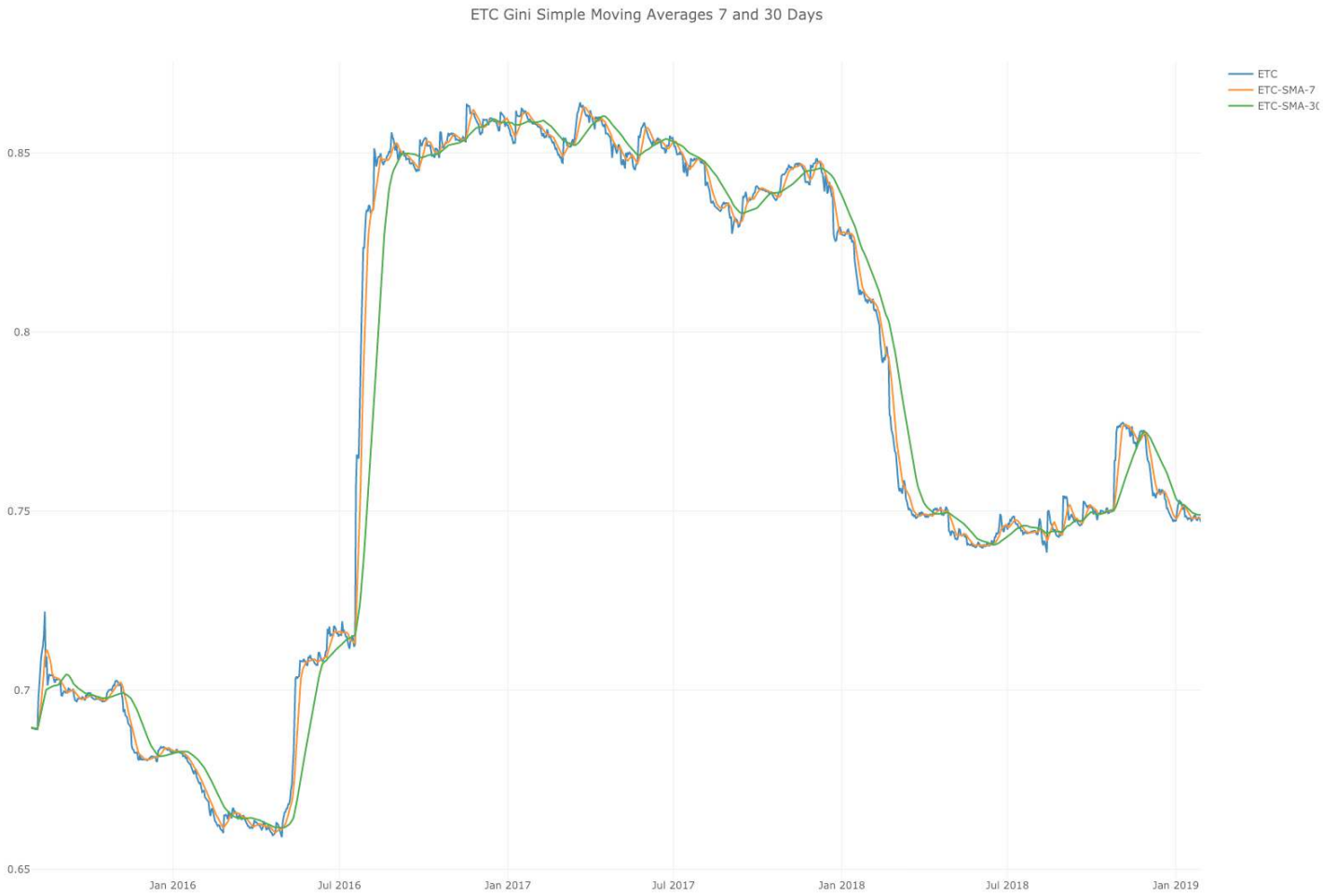




Now, let's try to think about the other Gini study we can do.

We can measure the Gini coefficient of a rich list. It's basically taking into account the assumption that one address belongs to a single entity. It also is ignoring the fact that bigger addresses belong to exchanges and just look at top 10k balances.

The query for the Gini index for daily rich list balances is written by Evgeny Medvedev and Allen Day of Google, which I adapted it to include the Simple Moving Average of the Gini index for the 7 days and 30 days window. Link to the query is here.



For the top 10k addresses, there seems to be a major rise in the Gini coefficient around the DAO Hard fork, where it goes up by about 13 percent! We don't know yet what caused this, but a few hypotheses are that, major movement of Ethereum Classic on exchanges post the DAO hard fork. It's possible it was major buys of ethereum classic when the price was cheap post the fork and this was a movement of ether to whale accounts. One other thing might be it's the DAO hacker moving funds. We will be investigating this further in future Medium posts.

The Gini remains around 0.85 from the DAO Hard fork until early 2018 where it starts dropping for wealth distribution of ethereum classic by wallet addresses.

> *The time periods of DAO Fork to Early 2018 are very interesting for daily top balance Gini because they form a similar behavior to the Gini plot of daily block reward for miners. The daily reward Gini in that time period has dropped, while in the case for Gini daily balances, it rises. There is a clear negative correlation happening here.*

This reverse pattern in Gini coefficient movement between mining rewards and Ethereum Classic balance centralization/decentralization does warrant further investigation into what's causing this.

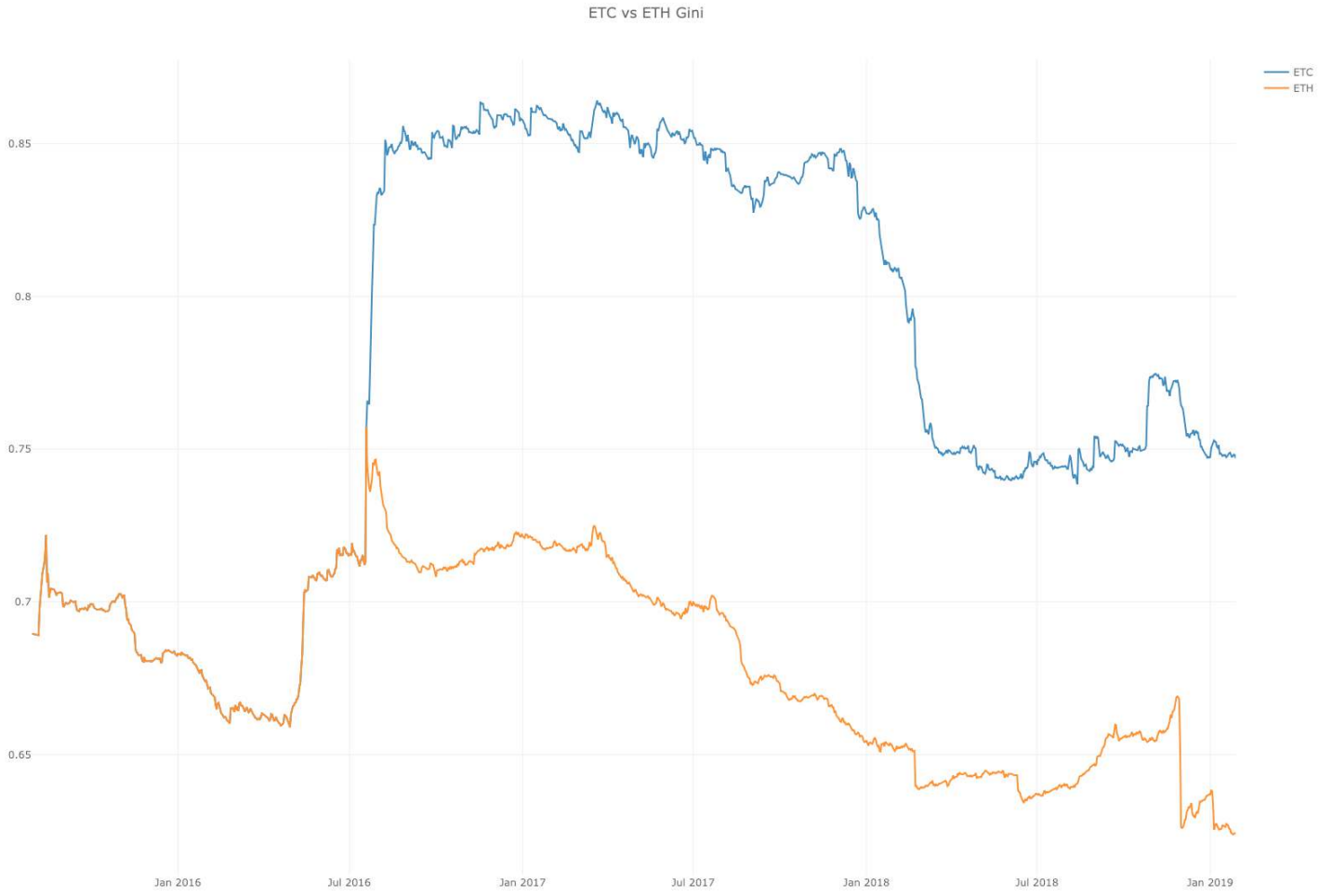
What makes a blockchain's Gini coefficient rise up after it becomes a minority chain due to the majority chain hard forking away? Is it being heavily manipulated by others as the distribution of wealth points to inequality?

What about the drop in the Gini coefficient for mining rewards per miner right after the fork? Clearly, the DAO Hard Fork of Ethereum does tell an interesting story about the behavior of chains before and after community splits. We need to investigate this much deeper, and luckily, with BigQuery, we have all the tools needed to do just that.

Now, let's take Ethereum into account and compare the daily Gini coefficient of both of them.

It’s the same query but you target the Ethereum blockchain dataset on BigQuery to compare.

Here’s the plot for it.

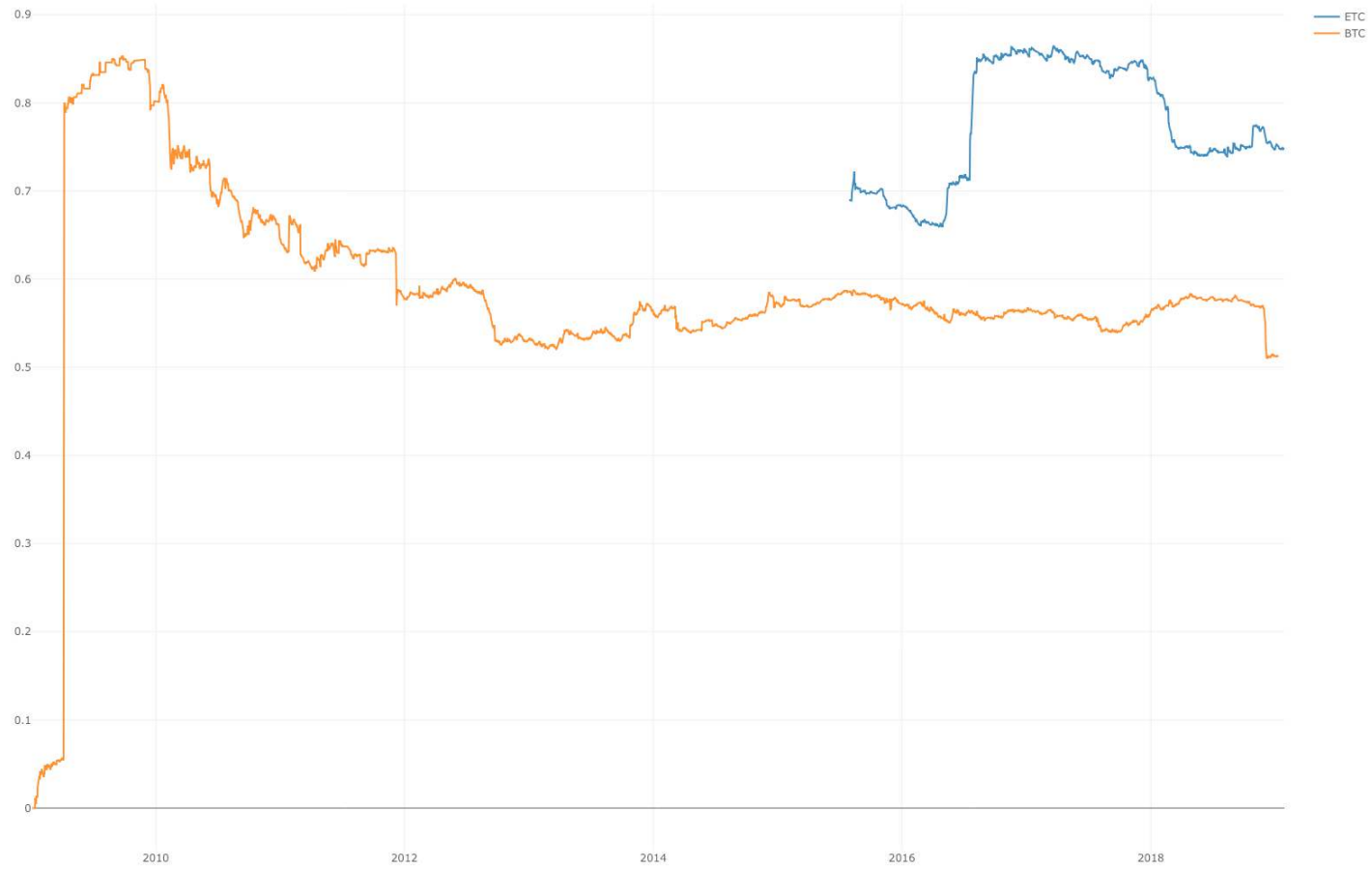


Interesting results! Not only is Ethereum Classic’s Gini rising by 13%, but Ethereum’s actually drops over time.

My only explanation for this is Ethereum’s relative stability in the hype market post-DAO Hard fork followed by the ICO season and further distribution of Ethereum to smart contract addresses in exchange for tokens. ETC stabilizes later around the same point as the highest Gini point for ETH.

We can also compare with ETC with Bitcoin in Gini of daily balances.

Gini ETC and BTC Top 10K Accounts



It’s worth noting that the UTXO record keeping model of Bitcoin would result in more accounts than needed because many transactions are actually tied into a wallet. In the account-balancing model of ETC and ETH, it’s more like a bank so you get a more accurate picture of the balance per account. Therefore, this might actually push the Gini up or down depending on where there’s more transactions tied to a wallet in the Bitcoin case.

Here, we see how clearly distributed Bitcoin is, hovering evenly around 0.55 before reaching 0.5 during the market crash. Bitcoin has the best Gini by far.

Analyzing ETC with Nakamoto Coefficient

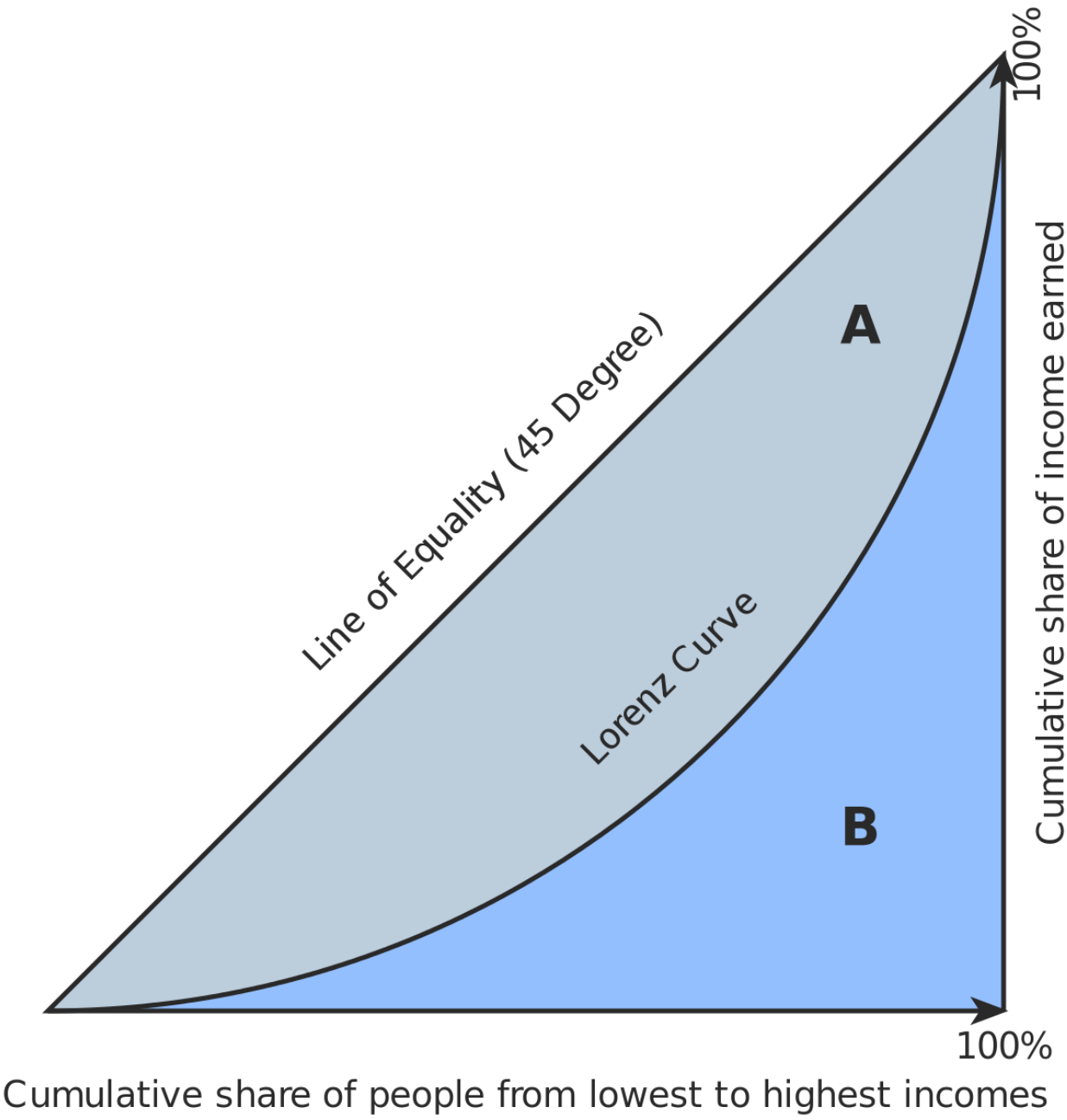
We wanted to make things a little bit interesting before you took off, so we added one final set of analyses you can do with the BigQuery ETC dataset.

The Nakamoto Coefficient was proposed by Balaji Srinivasan as a measurement to compliment the Gini Coefficient as a way of quantifying decentralization in his post “Quantifying Decentralization”.

The Nakamoto coefficient is taken from the Lorenz curve and counts the minimum

The Nakamoto coefficient is taken from the Lorenz curve and counts the minimum number of entities required to gain more than 51% influence in a sector of a blockchain.

The Lorenz Curve is a graphical representation of the inequality distribution.



Nakamoto coefficient measures the minimum number of individuals or entities you need to compromise or control more than half of the network's subsystem. The following is a mathematical formula taken from Balaji's Medium post for the Minimum Nakamoto Coefficient.

Given a subsystem s with K entities, let $p_1 > \ldots > p_K$ be the proportions of the subsystem controlled by each of the K participants such that $\sum_i^K p_i = 1$. Then we define the Nakamoto coefficient as:

$$N_s := \min \left\{ k \in [1, ..., K] : \sum_{i=1}^{k} p_i \geq 0.51 \right\}$$

In other words, the Nakamoto coefficient of a subsystem N_s is the minimum number of entities whose proportions one can sum to get to 51% control. If we assume a decentralized system is composed of S such subsystems, where N_s denotes the Nakamoto coefficient of subsystem s, the minimum Nakamoto coefficient $N_{\min}$ is defined as:

$$N_{\min} := \min \{N_1, ..., N_S\}$$

So the minimum Nakamoto coefficient of a decentralized system is the *minimum* number of entities to compromise to get to 51% control of at least one subsystem.

Formula for Minimum Nakamoto by Balaji Srinivasan

The higher the Nakamoto Coefficient, the more decentralized the sector or subsystem is.

6 Sectors or subsystems were identified in the article that must be measured to quantify the decentralization of the blockchain.

It’s not necessarily only applied to network hash rate, but can be applied to:

- Daily Balances: How many entities own more than 51% of currency.
- Mining Rewards: How many miners discover more than 51% of the blocks.
- Codebase Repository: How many developers contribute more than 51% of code commits for the blockchain client.
- Market: How many exchanges control more than 51% of the volume of the currency.
- Client Usage: How many clients are used by more than 51% of the miners.
- Miner Geography: How many countries have more than 51% of all miners.

Nakamoto: A Python Library for Quantifying Decentralization

New Nakamoto Library We Built

For that, I felt it's best to create a Python library specific for the analysis, so I went ahead and built `nakamoto` a tool that helps one analyze the Gini and Nakamoto coefficient of a blockchain. It can also be used to plot Lorenz Curves. The Github link to `nakamoto` is found here if you're interested.

You can easily install it with:

```
pip install nakamoto
```

Furthermore, I've provided a Kaggle notebook that goes over all the analysis and plotting with fully open-sourced code in more details, which you can check out.

The `nakamoto` Python module can analyze all 6 sectors for you.

To demonstrate the library, we will do 2 analyses, one using BigQuery SQL, and another by analyzing a Github repository.

For this analysis, we will measure the decentralization of Ethereum Classic's top rich list and codebase.

For the top rich list, we will measure the minimum amount of entities that have more than 51% supply of Ethereum Classic. We will also plot the Lorenz Curve.

For top rich list, we run the query for daily rich balance here. We then use nakamoto as the following:

```
from nakamoto.sector import CustomSector


rich_list = CustomSector(rich_list_data,
                         currency,
                         sector_type,
                         **nakamoto_config)
```

```
rich_list.get_gini_coefficient()
```

This would result in:

```
0.90683
```

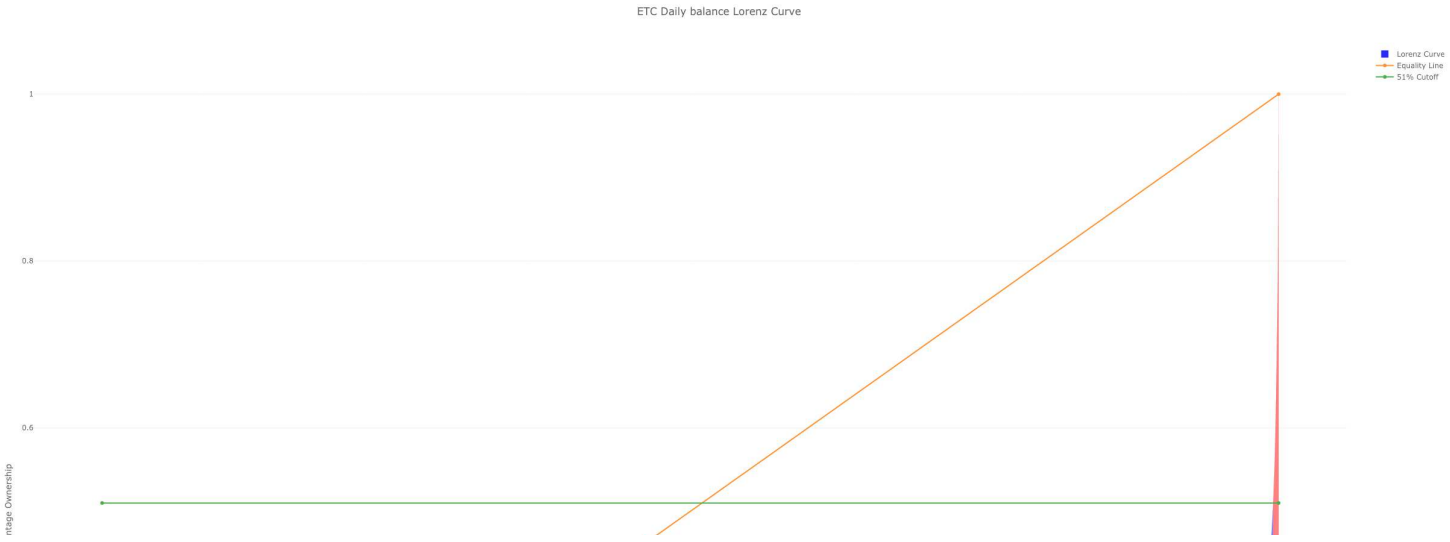
That's a fairly high number, meaning more inequality of ETC as it's mostly in bigger pockets or it could be because it's a smaller network. Also, over time, it'll probably improve as the network grows.

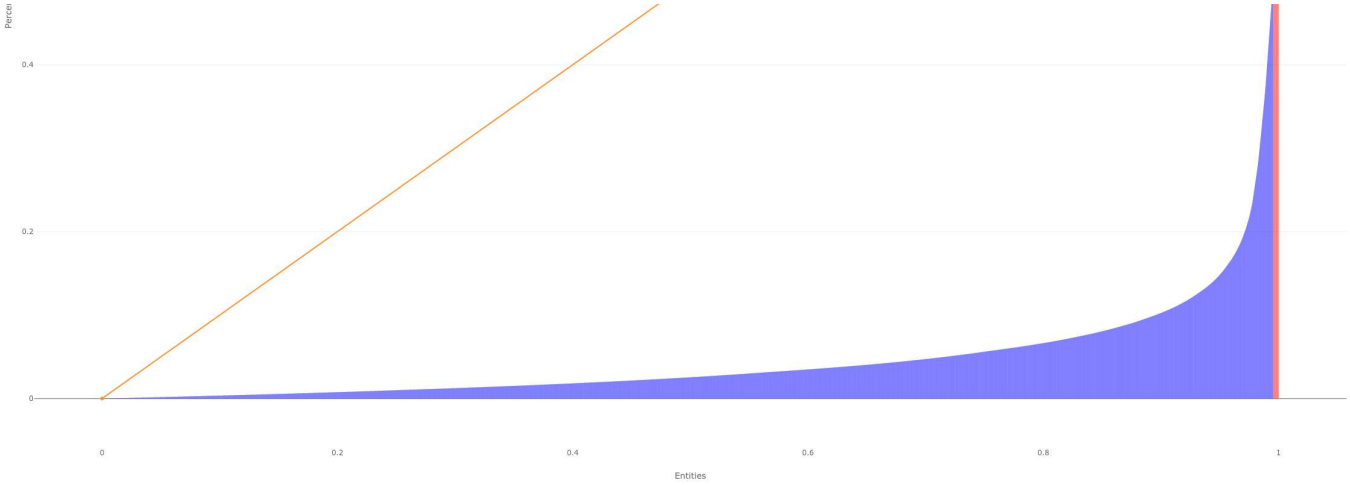
If we run `rich_list.get_nakamoto_coefficient()`

The Nakamoto coefficient here would return `48` which is the number of entities with more than 51% supply of all of ethereum classic circulating.

Now, let's plot the Lorenz curve like this:

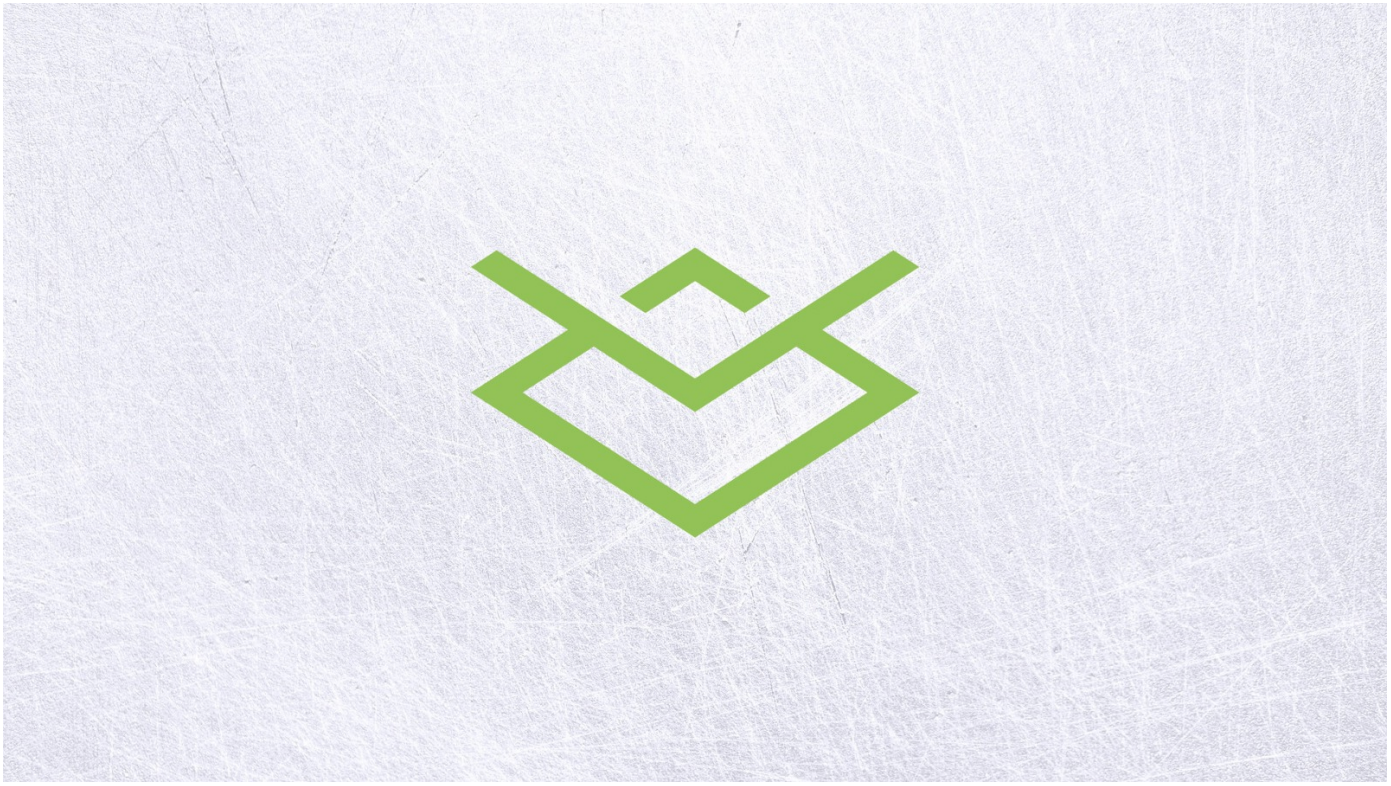
```
import plotly.tools as tls
from IPython.core.display import HTML

plot_url = rich_list.get_plot_url()
plot_html = tls.get_embed(plot_url)

HTML(plot_html)
```





The entities marked in red are the ones with collectively more than 51% influence on the daily balance. The red mark is the upper 51% bound of the Lorenz curve and the lower blue marks what's lower.

Measuring Decentralization of IOHK's Mantis Client



Mantis, the Ethereum Classic client built by IOHK

For the codebase, we will be analyzing IOHK's Mantis Client. More specifically, we will measure the code contributions by each developer calculated by number of commits. This will give us an indication of how decentralized the IOHK Mantis Client

is and what is the minimum amount of developers you need to compromise the system. We realize it’s not always a practical take, but the idea behind this was inspired by the 51% attack needed to control a network. In reality, you’d just need to comprise a few people to compromise a codebase due them injecting harmful codes that affect miners and network.

You can do codebase analysis using the special sector class `Repository` found in `nakamoto`

```
from nakamoto.sector import Repository

github_url = 'https://github.com/input-output-hk/mantis'
currency = 'ETC'

repository = Repository(github_url,
                        github_api,
                        currency,
                        **nakamoto_config)

repository.get_gini_coefficient()
```

The Gini coefficient of Mantis will be:

```
$ 0.381
```

This means that the IOHK repository distribution leans heavily towards the side of equality and decentralization. That’s good to hear!

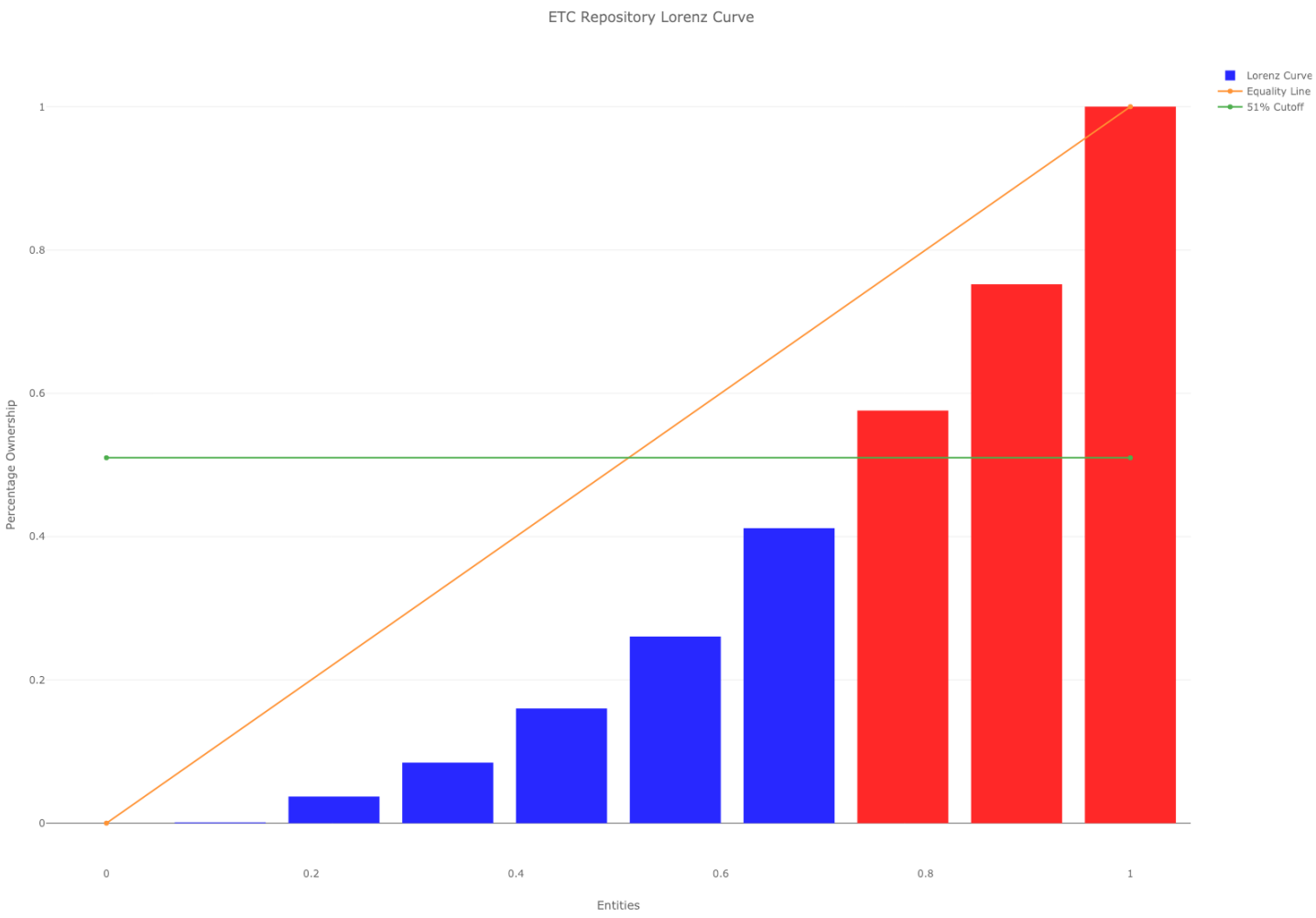
Let’s get the Nakamoto coefficient by calling:

```
repository.get_nakamoto_coefficient()
```

This will give us: `$ 3`

3 developers are the minimum amount you need to influence 51% of the Mantis Ethereum Classic client Github repository. That’s a good sign of more distribution

among developers, but obviously 4 is better. Still, along with the gini coefficient leaning towards line of equality, it's good enough. If we plot the Lorenz Curve, we get the following graph.



Minimum Nakamoto

One last thing you can do with with the `nakamoto` library is getting the minimum Nakamoto Coefficient of all the sector classes to find the most vulnerable sector. You can also get the maximum Gini, which shows most centralized/most unequal distribution among sectors.

```
from nakamoto.coefficient import Nakamoto


sector_list = [sector_1,
               sector_2,
               sector_3,
               sector_4,
               repository
```

```
            repository,
            custom_sector]

nakamoto = Nakamoto(sector_list)

nakamoto.get_summary()
```

This generates a nice summary of all your sectors as a Pandas Dataframe.

	Gini Coefficient	Nakamoto Coefficient
geography	0.875	2.0
market	0.898	4.0
client	0.930	2.0
daily balance	0.907	48.0
mining_rewards	0.922	2.0

Minimum Nakamoto Breakdown

```
nakamoto.get_minimum_nakamoto()
`2.0`

nakamoto.get_maximum_gini()
`0.930`
```

Wrapping Up

Well, I hope you enjoyed this guide into Google BigQuery and the Ethereum Classic Dataset! It would be awesome to see what sort of stories the data tells us. The Gini signals around the DAO Hardfork and its aftermath indicate it’s worth analyzing what happened around the DAO. With the Google BigQuery Ethereum Classic Dataset, you can do just that. You can also analyze the 51% attack in more details.

If you want more code examples, I've written two Kaggle notebook kernels to accompany this Medium Post.

One Kaggle notebook is the general BigQuery analysis queries and plotting.

The other Kaggle notebook goes over the Nakamoto library and BigQuery in more details.

The Nakamoto library is fully open sourced and I welcome all contributions and PR. For a Github repository on all queries I've run for Ethereum Classic SQL on BigQuery, check it out here. Please provide any feedback and I hope you enjoyed this data analysis guide.

Thanks to Anthony Lusardi.

Blockchain | Data Science | Decentralization | Ethereum Classic | Bigquery

Yaz Khoury
Writer, Hardware and Software Hacker, New York City Dweller, Hell Raiser and Dreamer.

Qi (state)

From Wikipedia, the free encyclopedia

Coordinates: 36.8167°N 118.3000°E

This article is about the major state of Qí (□). For the minor state of Qǐ (□), see Qi (Henan).
See also: Qi (Li Maozhen's state)

Qi was a state of the Zhou dynasty-era in ancient China, variously reckoned as a march, duchy, and independent kingdom. Its capital was Yingqiu, located within present-day Linzi in Shandong.

Qi was founded shortly after the Zhou overthrow of Shang in the 11th century BC. Its first marquis was Jiang Ziya, minister of King Wen and a legendary figure in Chinese culture. His family ruled Qi for several centuries before it was replaced by the Tian family in 386 BC.[1] In 221 BC, Qi was the final major state annexed by Qin during its unification of China.

Contents [hide]

1 History
1.1 Foundation
1.2 Spring and Autumn period
1.3 Warring States period
2 Culture of Qi
3 Qi architecture
4 Qi in astronomy
5 Rulers
5.1 House of Jiang
5.2 House of Tian
6 Famous people
7 References
8 Further reading

Qi □ *Dzəj	
1046 BC–221 BC	
 Qi in 260 BC	
Status	Duchy (1046–323 BC) Kingdom (323–221 BC)
Capital	Yingqiu (Zibo) Bogu (Binzhou)
Religion	Chinese folk religion ancestor worship
Government	Monarchy
King of Qi	
Chancellor	
• 685–645 BC	Guan Zhong
History	
• Enfeoffment of Duke Tai	1046 BC
• Conquered by Qin	221 BC
Currency	Knife money
Preceded by	**Succeeded by**
Pugu	Qin dynasty

History [edit]

This section **needs additional citations**

Qi

Nederlands
Norsk
Norsk nynorsk
Occitan
Polski
Português
Русский
Srpskohrvatski / српскохрватски
Svenska
Українська
Tiếng Việt
□□
Edit links

"Qi" in seal script (top), Traditional (middle), and Simplified (bottom) Chinese characters

Traditional Chinese □

Simplified Chinese □

Transcriptions	
Standard Mandarin	
Hanyu Pinyin	Qí
Gwoyeu Romatzyh	Chyi
Wade–Giles	Ch'i^{2}
IPA	[tɕʰǐ]
Wu	
Suzhounese	Zí
Yue: Cantonese	
Yale Romanization	Chàih
Jyutping	Cai^{4}
Southern Min	
Hokkien POJ	Chê
Tâi-lô	Tsê
Eastern Min	
Fuzhou BUC	Cạ̀
Old Chinese	
Baxter–Sagart (2014)	*[dz]ˤəj

Foundation [edit]

During the Zhou conquest of Shang, Jiang Ziya served as the chief minister to King Wu. After Wu's death, Jiang remained loyal to the Duke of Zhou during the Three Guards' failed rebellion against his regency. The Shang prince Wu Geng had joined the revolt along with the Dongyi states of Yan, Xu, and Pugu. These were suppressed by 1039 BC and Jiang was given the Pugu lands in what is now western Shandong as the march of Qi. Little information survives from this period, but the *Bamboo Annals* suggest that the native people of Pugu continued to revolt for about another decade before being destroyed a second time c. 1026.

In the mid-9th century BC, King Yi (r. 865–58 BC) attacked Qi and boiled Duke Ai to death. Under the reign of King Xuan (r. 827–782), there was a local succession struggle. During this time, many of the native Dongyi peoples were absorbed into the Qi state.

The Great Wall of Qi on Dafeng Mountain

Spring and Autumn period [edit]

In 706 BC, Qi was attacked by the Shan Rong. Qi rose to prominence under Duke

Bronze knife-shaped coins of State of Qi, collected in Shandong Museum

Sacrificial horses discovered in the tomb of Duke Jing of Qi

Huan of Qi (685–43 BC). He and his minister Guan Zhong strengthened the state by centralizing it. He annexed 35 neighboring states including Tan and brought others into submission. In 667 BC, Duke Huan met with the rulers of Lu, Song, Chen and Zheng and was elected leader. Subsequently, King Hui of Zhou made him the first Hegemon. He attacked Wei for supporting a rival of the Zhou king and intervened in the affairs of Lu. In 664 BC, he protected Yan from the Rong. In 659 BC, he protected Xing and in 660, Wei, from the Red Di. In 656 he blocked the northward expansion of Chu. After his death, a war of succession broke out among his sons, greatly weakening Qi. The hegemony consequently passed to Jin.

In 632 BC, Qi helped Jin defeat Chu at the Battle of Chengpu. In 589 BC, Qi was defeated by Jin. In 579 BC, the four great powers of Qin (west), Jin (center), Chu (south) and Qi (east) met to declare a truce and limit their military strength. In 546 BC, a similar four-power conference recognized several smaller states as satellites of Qi, Jin and Qin.

Warring States period [edit]

Early in the period, Qi annexed a number of smaller states. Qi was one of the first states to patronize scholars. In 532 BC, the Tian clan destroyed several rival families and came to dominate the state. In 485 BC, the Tian killed the ducal heir and fought several rival clans. In 481 BC, the Tian chief killed a puppet duke, most of the ruler's family, and a number of rival chiefs. He took control of most of the state and left the Duke with only the capital of Linzi and the area around Mount Tai. In 386 BC, the House of Tian fully replaced the House of Jiang as rulers of Qi. In 221 BC, Qi was the last of the warring states to be conquered by Qin, thereby putting an end to the wars and uniting China under the Qin Dynasty.

Culture of Qi [edit]

Before Qin unified China, each state had its own customs and culture. According to the *Yu Gong* or *Tribute of Yu*, composed in the 4th or 5th century BC and included in the *Book of Documents*, there were nine distinct cultural regions of China, which are described in detail in this book. The work focuses on the travels of the titular sage, Yu the Great, throughout each of the regions. Other texts, predominantly military, also discussed these cultural variations.

One of these texts was *The Book of Master Wu*, written in response to a query by Marquis Wu of Wei on how to cope with the other states. Wu Qi, the author of the

work, declared that the government and nature of the people were reflective of the terrain of the environment in which they inhabited. Of Qi, he said:

> Although Qi's troops are numerous, their organization is unstable.
>
> — Wuzi, *Master Wu*

> The people of Qi are by nature unyielding and their country prosperous, but the ruler and officials are arrogant and care nothing for the people. The state's policies are not uniform and not strictly enforced. Salaries and wages are unfair and unevenly distributed, causing disharmony and disunity. Qi's army is arrayed with their heaviest hitters at the front while the rest follow behind, so that even when their forces appear mighty, they are in reality fragile. To defeat them, we should divide our army into three columns and have two attack the left and right flanks of Qi's army. Once their battle formations are thrown into disarray, the central column should be in position to attack and victory will follow.
>
> — Wuzi, *Master Wu*

While visiting Qi, Confucius was deeply impressed with perfection of performance of Shao music □ therein.[2]

During the Warring States period, Qi was famous for its capital's academy Jixia, renowned scholars of the era from all over China visited the academy.

Qi architecture [edit]

Remains of Ancient Linzi city sewer passing underneath the former city wall of the Qi kingdom.

The state of Qi was known for having well organized cities that were nearly rectangular in shape, with roads that were neatly knit into a grid-like pattern. The palace was strategically positioned facing the south. To the left (eastwardly direction) of the palace resided the ancestral temple, to its right (westward) the temple of the gods, both one hundred paces away. This ensured that balance was achieved. In front of the palace was the court also one hundred paces away and to the back of the palace was the city. This type of layout influenced greatly the way cities were designed in subsequent generations.

Smaller cities known as *chengyi* (□□) were abundant throughout Qi. They typically stretched 450 meters from south to north and 395 meters from east to west. The perimeter was usually surrounded by a wall with the living headquarters situated within and a nearly perfect square-shaped courtyard occupying the center.[3]

Qi in astronomy [edit]

Main article: Chinese constellations

Qi is represented by the star **Chi Capricorni** in the "Twelve States" asterism in the "Girl" lunar mansion in the "Black Turtle" symbol. Qi is also represented by the star **112 Herculis** in the "Left Wall" asterism in the "Heavenly Market" enclosure.[*citation needed*]

Rulers [edit]

House of Jiang [edit]

See also: House of Jiang family tree

Title	Name	Reign (BC)	Relationship	Notes
Duke Tai □□□	Lü Shang □□	11th century		Enfeoffed by King Wu of Zhou, with capital at Yingqiu
Duke Ding □□□	Lü Ji □□	10th century	5th-generation descendant of Duke Tai	Traditionally believed to be son of Duke Tai
Duke Yǐ □□□	De □	10th century	Son of Duke Ding	
Duke Gui □□□	Cimu □□	c. 10th century	Son of Duke Yǐ	
Duke Ai □□□	Buchen □□	9th century	Son of Duke Gui	Boiled to death by King Yi of Zhou
Duke Hu □□□	Jing □	9th century	Son of Duke Gui	Moved capital to Bogu, killed by Duke Xian
Duke Xian □□□	Shan □	859?–851	Son of Duke Gui	Moved capital back to Linzi
Duke Wu □□□	Shou □	850–825	Son of Duke Xian	
Duke Li □□□	Wuji □□	824–816	Son of Duke Wu	Killed by supporters of Duke Hu's son.
Duke Wen □□□	Chi □	815–804	Son of Duke Li	
Duke Cheng □□□	Yue □	803–795	Son of Duke Wen	
Duke Zhuang I □□□□	Gou □	794–731	Son of Duke Cheng	Reigned for 64 years
Duke Xi	Lufu	730–698	Son of Duke	

□□□	□□		Zhuang I	
Duke Xiang □□□	Zhu'er □□	697–686	Son of Duke Xi	Committed incest with sister Wen Jiang, murdered her husband Duke Huan of Lu, conquered the state of Ji, murdered by cousin Wuzhi
none	Wuzhi □□	686	Cousin of Duke Xiang, grandson of Duke Zhuang I	Killed by Yong Lin.
Duke Huan □□□	Xiaobai □□	685–643	Younger brother of Duke Xiang	First of the Five Hegemons, when Qi reached zenith of its power. Starved to death by ministers
none	Wukui or Wugui □□ or □□	643	Son of Duke Huan	Killed by supporters of Duke Xiao
Duke Xiao □□□	Zhao □	642–633	Son of Duke Huan	Crown prince of Qi
Duke Zhao □□□	Pan □	632–613	Son of Duke Huan	His supporters murdered the son of Duke Xiao
none	She □	613	Son of Duke Zhao	Murdered by uncle Shangren
Duke Yì □□□	Shangren □□	612–609	Uncle of She, son of Duke Huan	Killed by two ministers
Duke Hui □□□	Yuan □	608–599	Son of Duke Huan	Defeated Long Di invaders
Duke Qing □□□	Wuye □□	598–582	Son of Duke Hui	Defeated by Jin at the Battle of An
Duke Ling □□□	Huan □	581–554	Son of Duke Qing	Annexed the State of Lai; defeated by Jin at the Battle of Pingyin, capital Linzi burned
Duke Zhuang II □□□□	Guang □	553–548	Son of Duke Ling	Ascended throne by killing Prince Ya with the help of Cui Zhu; committed adultery with Cui's wife, killed by Cui

Duke Jing □□□	Chujiu □□	547–490	Half brother of Duke Zhuang II	Killed Cui Zhu. Had famous statesman Yan Ying as prime minister
An Ruzi □□□	Tu □	489	Youngest son of Duke Jing	Deposed by Tian Qi and killed by Duke Dao. Also called Yan Ruzi
Duke Dao □□□	Yangsheng □□	488–485	Son of Duke Jing	Killed by a minister, possibly Tian Heng
Duke Jian □□□	Ren □	484–481	Son of Duke Dao	Killed by Tian Heng
Duke Ping □□□	Ao □	480–456	Brother of Duke Jian	
Duke Xuan □□□	Ji □	455–405	Son of Duke Ping	
Duke Kang □□□	Dai □	404–386	Son of Duke Xuan	Deposed by Duke Tai of Tian Qi, died in 379

House of Tian [edit]

See also: House of Tian family tree

"Tian Qi" redirects here. For the Chinese cricketer, see Tian Qi (cricketer).

Subject to the House of Jiang

Posthumous name	Personal name	Leadership (BC)	Relationship	Notes
Tian Jingzhong □□□	Chen Wan □□		Son of Duke Li of Chen	Exiled to Qi from the State of Chen
Tian Mengyi □□□	Tian Zhi □□		Son of Chen Wan	
Tian Mengzhuang □□□	Tian Min □□		Son of Mengyi	
Tian Wenzi □□□	Tian Xuwu □□□		Son of Mengzhuang	
Tian Huanzi □□□	Tian Wuyu □□□		Son of Wenzi	
Tian Wuzi □□□	Tian Kai □□	?–516	Son of Huanzi	

Tian Xizi □□□	Tian Qi □□		Brother of Wuzi	Deposed An Ruzi
Tian Chengzi □□□	Tian Heng □□		Son of Xizi	Killed Duke Jian, became *de facto* ruler of Qi
Tian Xiangzi □□□	Tian Pan □□		Son of Chengzi	
Tian Zhuangzi □□□	Tian Bai □□	?–411	Son of Xiangzi	
Tian Daozi □□□	*unknown*	410–405	Son of Zhuangzi	

As rulers of Qi

Title	Name	Reign (BC)	Relationship	Notes
Duke Tai □□□	Tian He □□	404–384	Son of Tian Bai	Officially recognized as Qi ruler in 386 BC
none	Tian Yan □□	383–375	Son of Duke Tai	Killed by Duke Huan.
Duke Huan □□□	Tian Wu □□	374–357	Brother of Tian Yan	
King Wei □□□	Tian Yinqi □□□	356–320	Son of Duke Huan	Most powerful Qi ruler of the Warring States.
King Xuan □□□	Tian Bijiang □□□	319–300	Son of King Wei	
King Min □□□	Tian Di □□	300–283	Son of King Xuan	Temporarily declared himself "Emperor of the East".
King Xiang □□□	Tian Fazhang □□□	283–265	Son of King Min	
none	Tian Jian □□	264–221	Son of King Xiang	Qi conquered by Qin

Famous people [edit]

- Guan Zhong (720-645 BC), prime minister to Duke Huan of Qi and known for making the state of Qi one of the most power Hegemons at the time.

- Yan Ying (578-500 BC), prime minister to Duke Jing, known for *Yanzi Chunqiu*.
- Sun Bin (??-316 BC), military strategist known for *Sun Bin's Art of War*.
- Chunyu Kun (386-310 BC), official and master scholar at the Jixia Academy.
- Mencius (372-289 BC), official and one of the most renowned Confucian philosophers.
- Xun Kuang (313-238 BC), philosopher who joined the Jixia Academy when he was 50 years old, known for the *Xunzi*.

References [edit]

1. ^ Burton Watson 2003 p.1. Xunzi: Basic Writings. https://books.google.com/books?id=0SE2AAAAQBAJ&pg=PA1
2. ^ Analects, 17 ("Shu er"):14.
3. ^ http://baike.baidu.com/view/2101263.htm, retrieved on July 5, 2016.

Further reading [edit]

- Michael Loewe, ed. (2006). *The Cambridge history of ancient China: from the origins of civilization to 221 BC*. Cambridge: Cambridge Univ. Press. ISBN 978-0-521-47030-8.
- Glessner Creel, Herrlee (1979). *The birth of China: a study of the formative period of Chinese civilization*. New York: Ungar Publ. ISBN 0-8044-6093-0.

V · T · E	Zhou dynasty states	
Spring and Autumn	Major states	Cai · Cao · Chen · Chu · Jin · Lu · **Qi** · Qin · Song · Wey · Wu · Yan · Yue · Zheng
	Minor states	Ba · Bei [zh] · Chao · Dao · Dai · Deng · E · Eastern Guo · Western Guo · Gumie · Guzhu · Han · Hua · Huang · Huo · Ji · Jia [zh] · Ju · Lai · Liang · Liao · Lü · Luo [zh] · Pi · Qǐ · Quan · Rui · Ruo · Shēn · Shěn · Sui · Tan · Tang · Xi · Xian · Xing · Xu · Yang · Yiqu · Yu · Zhongshan · Zhoulai · Zou
Warring States	Seven states	Chu · Han · **Qi** · Qin · Wei · Yan · Zhao
	Minor states	Ba · Cai · Dai · Lu · Shu · Song · Teng · Wey · Yiqu · Yue · Zheng · Zhongshan · Zou

Categories: Ancient Chinese states | Qi (state) | States and territories established in the 11th century BC | 11th-century BC establishments in China | 3rd-century BC disestablishments | States and territories disestablished in the 3rd century BC | 221 BC

Qi (disambiguation)

From Wikipedia, the free encyclopedia

For the Portal Quick Index, see WP:QI

Qi, in traditional Chinese culture, is an active principle forming part of any living thing.

Look up *qi* or *QI* in Wiktionary, the free dictionary.

Qi, **QI** or **Q.I.** may also refer to:

Contents [hide]

1 Arts and media
- 1.1 Television
- 1.2 Other media

2 People

3 Places
- 3.1 Former states
- 3.2 Modern places

4 Science and technology

5 Other uses

6 See also

Arts and media [edit]

Television [edit]

- *QI* (*Quite Interesting*), a British BBC television programme
  - Quite Interesting Limited, a company that researches for the *QI* television series
  - *QI* (Czech TV series), a Czech remake of the British BBC television programme
  - *QI* (Dutch TV series), a Dutch remake of the British BBC television programme
  - *Intresseklubben*, a Swedish remake of the British BBC television programme

Other media [edit]

- "Q.I" (song), a song by Mylène Farmer from *Avant que l'ombre...*
- *QI: The Quest for Intelligence*, a book by Kevin Warwick

People [edit]

- Qi of Xia, the second king (reigned 2146–2117 BC) of the Xia Dynasty
- Hou Ji, or Qi, an ancestor of the Chinese Zhou dynasty
- Qi (surname), several Chinese surnames

Places [edit]

Former states [edit]

- Qi (Henan) (□; 16th century–445 BC) in Henan, the rump state of the Xia dynasty in Henan under the Shang and Zhou
- Qi (state) (□; 1046–221 BC) in Shandong during the Zhou dynasty
- Southern Qi Dynasty (□; 479–502) during the Southern and Northern Dynasties period

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
Wikispecies

Languages
Български
Català
Čeština
Deutsch
Español
Français
Galego
Italiano
Lietuvių
Bahasa Melayu

- Northern Qi Dynasty (□; 550–577) during the Southern and Northern Dynasties period
- Qi (881-884) (□; 881–884), the short-lived realm of the agrarian rebel Huang Chao during the late Tang
- Qi (Five Dynasties) (□; 907–924) during the Five Dynasties and Ten Kingdoms period
- Qi Dynasty (937-939) (□; 937–939), the predecessor of the Southern Tang (937–976) during the Five Dynasties and Ten Kingdoms period
- Qi (1130–1137), a puppet state of the Jin dynasty (1115–1234) in Central China

Modern places [edit]

- Qi County, Kaifeng, in Henan, China
- Qi County, Hebi, in Henan, China
- Qi County, Shanxi, in Jinzhong, Shanxi, China

Science and technology [edit]

- Qi (standard), an interface specification published by the Wireless Power Consortium, used for charging batteries with electricity
- Qi hardware, an open-hardware project
- ATCvet code QI *Immunologicals*, a section of the Anatomical Therapeutic Chemical Classification System for veterinary medicinal products
- QueryInterface, in Microsoft's COM software
- Quote Investigator, a website dedicated to tracking down the origins of common quotations
- Quality Improvement, a formal approach to the analysis of performance and to systematic efforts to improve performance; see Quality Management

Other uses [edit]

- Qi Card, an Iraqi national credit card
- Cimber Air (IATA designator QI)
- Qimonda (NYSE stock symbol QI)

See also [edit]

- KI (disambiguation)
- Key (disambiguation)
- Chi (disambiguation)
- Qizhou (disambiguation)

*This disambiguation page lists articles associated with the title **Qi**.*
If an internal link led you here, you may wish to change the link to point directly to the intended article.

Qi hardware

From Wikipedia, the free encyclopedia

Qi hardware is a project which produces copyleft hardware, in an attempt to apply the Free Software Foundation's GNU GPL concept of copylefting software to the hardware layer. The project is both a community of popular open hardware websites and a company, co-founded by Wolfgang Spraul and Yi Zhang, that makes hardware products. Formed from the now defunct Openmoko project,[1] key members went on to form Qi Hardware Inc. and Sharism At Work Ltd. Thus far, the project has released the Ben Nanonote,[2][3][4][5] the Milkymist One,[6] and the Ben WPAN wireless project[7][8][9][10][11] to create a copyleft wireless platform.

Qi Hardware Inc.

Type	Public
Industry	Computer hardware Computer software Consumer electronics Digital distribution
Headquarters	San Francisco, California, U.S.
Number of locations	Beijing, Hong Kong, San Francisco, Taipei
Area served	Worldwide
Products	**Products list** Ben Nanonote Milkymist

Copyleft hardware is essentially requiring that all plans for hardware design (i.e. schematics, bill of materials and PCB layout data) are released under the Creative Commons license Attribution-ShareAlike (CC BY-SA) and that the software needed to both manufacture the device and at least some software, including device drivers, necessary to use the hardware is released under the GNU General Public License. Technology for copyleft hardware are to be patent-free, and hence, all hardware which is Qi hardware is to be released early, often and publicly on the Internet.

The primary examples of Qi hardware projects are the Ben NanoNote pocket computer, Elphel 353 video camera and Milkymist One video synthesizer.

Contents [hide]

1 Products
2 See also
3 References
4 External links

Products [edit]

- Ben Nanonote, a Linux/OpenWrt based pocket computer
- Milkymist, a device for interactive visual effects for video performance artists (VJ)

See also [edit]

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
Русский
Edit links

- List of open source hardware projects
- Amateur radio and Amateur television
- Do it yourself (DIY)
- Electronic design automation
- Engineers Without Borders
- FreeCAD (software)
- Free content
- Free software
- Homebrew Computer Club
- Graphics hardware and FOSS
- Open CASCADE - software development platform freely available in open source.
- Open content
- Open design - Open-source physical design with a wider focus
- Open source
- Open-source software
- Open-source robotics

- Open Hardware and Design Alliance (OHANDA)

Wikimedia Commons has media related to ***Open hardware***.

Free and open-source software portal

References [edit]

1. ^ Pam Derringer (2009-07-01). "Openomoko Layoffs Lead to New Open Hardware Venture". linux.com. Retrieved 2011-07-18.
2. ^ Gareth Halfacree (2010-03-16). "Qi Hardware launches NanoNote". bit-tech.com. Retrieved 2011-07-18.
3. ^ Donald Melanson (2010-03-15). "Qi Hardware's tiny, hackable Ben NanoNote now shipping". bit-tech.com. Retrieved 2011-07-18.
4. ^ David Murphy (2010-06-05). "Qi Hardware Launches Open-Source Computer". pcmag.com. Retrieved 2011-07-18.
5. ^ rg (2010-03-17). "Qi Hardware Ben NanoNote". linux.com. Retrieved 2011-07-18.
6. ^ Ray, Bill. "Open-source hardware group puts out vid system-on-a-chip". *The Register*. Retrieved 23 June 2017.
7. ^ Terrence O'Brien (2011-06-17). "Qi-Hardware debuts free, open source wireless solution, not a threat to WiFi". engadget.com. Retrieved 2011-07-18.
8. ^ "Qi Hardware Releases Free Wireless Hardware". rejon.org. 2011-06-15. Archived from the original on 2011-07-08. Retrieved 2011-07-18.
9. ^ Jake (2011-06-16). "Phillips: Qi Hardware Releases Free Wireless Hardware". lwn.net. Retrieved 2011-07-18.
10. ^ Electronista Staff (2011-06-17). "Qi Hardware makes open-source wireless networking tech". electronista.com. Retrieved 2011-07-18.
11. ^ Fabricatorz Staff (2011-06-17). "Qi Hardware Releases First Batch of 6LoWPAN Wireless Devices". fabricatorz.com. Archived from the original on 2011-07-24. Retrieved 2011-07-18.

External links [edit]

- Official website
- Nanonote
- Milkymist One VJ workstation
- Ben WPAN
- Identi.ca

V · T · E	Linux-powered devices		
Computers Components	Nettops	Aleutia · Eee Box · fit-PC · Lemote · Linutop · ThinCan · Zonbu	
	Netbooks	Acer Aspire One · Averatec Buddy · Classmate PC · CloudBook · ECS G10IL · Eee PC · Elonex ONE/ONEt · Gigabyte M912 · HP Mini 1000/2133 · Inspiron Mini · Doel · MSI Wind · NanoBook · Noahpad · OLPC · One A110 · Pinebook · OpenBook · Skytone Alpha-400 · Tianhua GX-1C	
	Tablets	Aakash · Adam · JooJoo · Librem · WeTab	
	Networking	Asus Routers · BT Home Hub · Buffalo AirStation · Junxion Box · Linksys WRT54G series · Netgear DG834G · Picotux · Killer NIC	
	Storage	Buffalo LinkStation / TeraStation · Drobo · Linksys NSLU2 · Synology Inc. · WD My Book · QNAP	
	Other	BeagleBoard · Chumby · DragonBox Pyra · Gumstix · Librem · Nvidia Drive · Nvidia Jetson · Palm Foleo · Pandora · Raspberry Pi · SheevaPlug · Stanley · Asus Tinker Board	
	Multimedia	DBox2 · Dreambox · Hauppauge MediaMVP · Neuros OSD · TiVo · Vu+ · Roku Digital Video Player · Sonos	
		Amazon Kindle · Archos PMA400 ·	

Accessories	**Handhelds**	ILiad · Leapfrog Didj · Nokia 770 / N800 / N810 / N900 · Pepper Pad · Zaurus · Sony Reader · Zipit · Ben NanoNote
	Phones†	Jolla · Motorola A1200 / A1210 / A1600 / A760 / E680i / MOTO VE66 / PEBL U9 / RAZR2 V8 / ROKR E2 / E6 / E8 / EM30 / EM35 / Z6 / ZINE ZN5 / ZN200 · Neo 1973 / FreeRunner · Nokia N9 / N900 · Palm Pixi / Pre / Pre 2 / HP Pre 3 / Veer · Samsung Z1 / Z2 / Z3 / Z4
	Consoles	DragonBox Pyra · GP2X (Wiz · CAANOO) · mylo · Pandora · Dingoo A320 · Ouya · GCW Zero
Defunct/Historical	Cherrypal · Simputer	

† Excluding Android devices.

v · t · e	**Intellectual property activism**	
Issues	Artificial scarcity · Copyright infringement · Digital rights management · Gripe site · Legal aspects of file sharing · Mashup (digital · music · videos) · Monopolies of knowledge · Music piracy · Orphan works · Patents (biological · software · software patent debate · trolling) · Public domain	
Concepts	All rights reversed · Alternative compensation system · Anti-copyright notice · Business models for open-source software · Copyleft · Commercial use of copyleft works · Commons-based peer production · Free content · Free software license · Libertarian positions · Open content · Open-design movement · Open Music Model · Open patent · Open-source hardware · Open-source software · Prize system (contests) · Share-alike · Video on demand	
Movements	Access to Knowledge movement · Anti-copyright · Cultural environmentalism · Free-culture movement · Free software movement	
Organizations	**Pro-copyright**	Copyright Alliance
	Pro-copyleft	Creative Commons · Electronic Frontier Foundation · Free Software Foundation · Open Rights Group · Organization for Transformative Works · The Pirate Bay · Piratbyrån · Pirate Party · Sci-Hub · Students for Free Culture
People	Alexandra Elbakyan · Rick Falkvinge · Lawrence Lessig · Richard Stallman · Peter Sunde · Peter Suber · Aaron Swartz	
Documentaries	*Steal This Film* (2006, 2007) · *Good Copy Bad Copy* (2007) · *RiP!: A Remix Manifesto* (2008) · *TPB AFK: The Pirate Bay Away From Keyboard* (2013) · *The Internet's Own Boy* (2014)	

Categories: Open hardware organizations and companies | Open-source hardware | Computer companies of the United States | Computer hardware companies | Electronics companies of the United States | Home computer hardware companies | Mobile phone manufacturers | Multinational companies headquartered in the United States | Networking hardware companies | Portable audio player manufacturers | Electronics companies | Software companies based in California

Computer Science > Hardware Architecture

Enabling the Adoption of Processing-in-Memory: Challenges, Mechanisms, Future Research Directions

Saugata Ghose, Kevin Hsieh, Amirali Boroumand, Rachata Ausavarungnirun, Onur Mutlu

(Submitted on 1 Feb 2018)

Poor DRAM technology scaling over the course of many years has caused DRAM-based main memory to increasingly become a larger system bottleneck. A major reason for the bottleneck is that data stored within DRAM must be moved across a pin-limited memory channel to the CPU before any computation can take place. This requires a high latency and energy overhead, and the data often cannot benefit from caching in the CPU, making it difficult to amortize the overhead.

Modern 3D-stacked DRAM architectures include a logic layer, where compute logic can be integrated underneath multiple layers of DRAM cell arrays within the same chip. Architects can take advantage of the logic layer to perform processing-in-memory (PIM), or near-data processing. In a PIM architecture, the logic layer within DRAM has access to the high internal bandwidth available within 3D-stacked DRAM (which is much greater than the bandwidth available between DRAM and the CPU). Thus, PIM architectures can effectively free up valuable memory channel bandwidth while reducing system energy consumption.

A number of important issues arise when we add compute logic to DRAM. In particular, the logic does not have low-latency access to common CPU structures that are essential for modern application execution, such as the virtual memory and cache coherence mechanisms. To ease the widespread adoption of PIM, we ideally would like to maintain traditional virtual memory abstractions and the shared memory programming model. This requires efficient mechanisms that can provide logic in DRAM with access to CPU structures without having to communicate frequently with the CPU. To this end, we propose and evaluate two general-purpose solutions that minimize unnecessary off-chip communication for PIM architectures. We show that both mechanisms improve the performance and energy consumption of many important memory-intensive applications.

Subjects: **Hardware Architecture (cs.AR)**

Submission history

From: Saugata Ghose [view email]

[v1] Thu, 1 Feb 2018 15:00:38 UTC (2,413 KB)

Musicoin—The World's First Free Streaming Blockchain App Now Available

Musicoin
Jan 30 · 3 min read

FOR IMMEDIATE RELEASE January 30, 2019
HONG KONG

MUSICOIN OFFICIALLY RELEASES ITS MOBILE APP (V1), UNLOCKING THE TRUE POWER OF BLOCKCHAIN FOR LISTENERS AND MUSICIANS.

What if musicians could be compensated fairly and automatically on a world-class streaming platform? What if fans and listeners could play their favorite tunes for free? Musicoin is a pioneering example today of what blockchain could do for the entire music streaming business tomorrow. Version 1 of the app is now free to download on the App and Google Play stores.

Musicoin conceived a **new form of shared economy** in which every contributor gets paid for their contribution. Universal Basic Income (UBI), Musicoin's fair revenue model for musicians and fans, stems from the platform's forward-thinking development powered by the blockchain.

The promise Musicoin has made is twofold: to compensate musicians fairly on the Musicoin blockchain, allowing direct automatic payment in **$MUSIC**—Musicoin's own cash transferable cryptocurrency. At the same time, fans can browse, play, and share music for free, no subscription fees or ads while supporting artists directly.

"The Musicoin Project started from a simple philosophy, to remunerate creators because they shared valuable creations. The philosophy, dubbed as Sharism, is leading our products design, development, and delivery to all stakeholders." **Isaac Mao, *Founder.***

Enticing numbers reveal how Musicoin plans to shake the global USD 17 billion music business. Today, 5,500 musicians, 77,000 tracks, 7,500,000 streams and

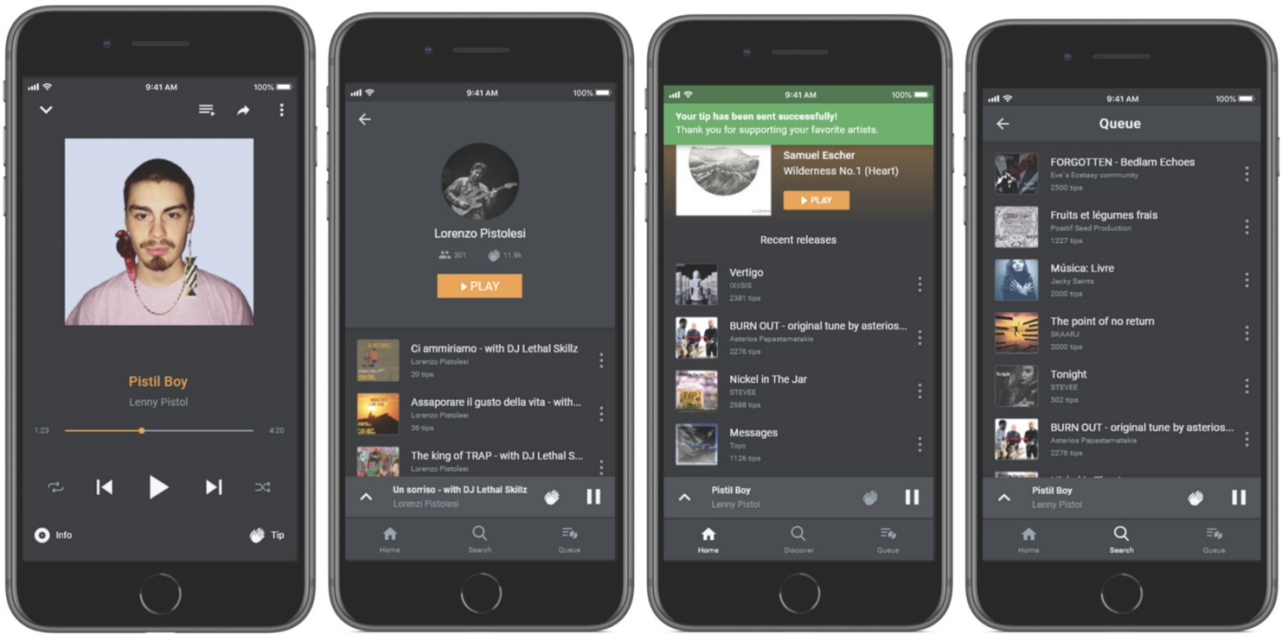
10,200,000 tips (an exclusive feature available on the app that shows support from fans to a track or artist) have made Musicoin an early success.

Founded by innovative leaders in both the music and the blockchain worlds, the Musicoin project is the first of its kind to have launched a solid and beautifully designed app, which fans and musicians can start enjoying.

"Finally we have a platform which allows musicians to be paid fairly. This was long overdue, maybe even 50 years." **Ben Gyles, *Mobile App Developer***.

The app, combining a top-notch blockchain service with a traditional streaming platform, allows fans and musicians to participate together, without intermediaries. It features:

- **Player**—play, pause, rewind, fast forward a track
- **Search**—search a track or artist
- **Browse by genre**—browse music from a genre list
- **Artwork**—add image/visual representation for a track
- **Queue**—play music from a queue/local playlist
- **Artist of the week**—Features the new Artist of the Week
- **Tipping/UBI**—Tip track with UBI



“Musicoin (app) is not merely designed to compete with another streaming platform, it’s designed to revolutionize our mindset of fairness.” **Gibran Septya, *Designer.***

Musicoin is the only streaming app emerging from blockchain technology with a scalable, sustainable vision. The team will continuously refine the product along the year, adding more features (speed enhancements, personal login, playlists…) as well as building up a global community and empowering artists.

Fair Play!

About Musicoin
Musicoin (MUSIC) is a smart cryptocurrency ($MUSIC) and music streaming platform built upon the Musicoin blockchain. Musicians and listeners worldwide are encouraged to visit Musicoin’s official website at musicoin.org .
Musicoin Mobile App can be downloaded on Google Store and App Store.

For press inquiries please contact : press@musicoin.org

Music | Blockchain | Crypto | Mobile App Development | Streaming

Civic Liker + Creators Fund: Double reward

LikeCoin Foundation will start the “Reinventing the Like” campaign from Feb 1 to Feb 22. 30,000 LIKE will be gifted to creators daily. We wish you all the best in Lunar New Year!

Edmond Yu
Jan 30 · 3 min read

There are two reward sources during the campaign: reward from each Civic Liker’s own budget and that from the creator’s fund. Yes, the two sources of reward will be released in parallel.

Civic Likers give more valuable Likes

Civic Likers are those who are willing to pay for additional USD 5 to support online content. Each Like from a Civic Liker distributes their own budget and influencing the

distribution of the daily 30,000 budget from the Creators Fund as well. If you want to be the prevelidged Civic Liker as well, click here to join, limited seat.

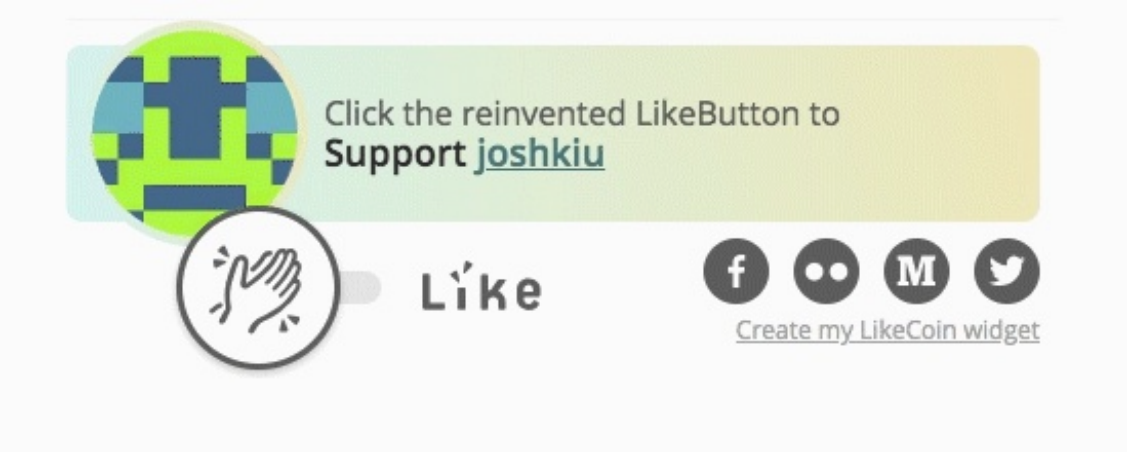
General readers can contribute too

For those readers who are not Civic Likers but have a LikeCoin ID, they can also reward creators by Liking. Their Likes can influence the daily Creators Fund's distribution.

Campaign Enrollment

Enrollment is easy:

- Writers can start adding the new **LikeButton** to their articles on Medium or WordPress now. Click here to learn how to install the LikeButton.
- Publish and promote the articles in any communities and channels to attract Likes; then you are eligible for the LIKE reward in this campaign.



LikeButton—Readers click Like, Creators mine LIKE

LIKE Distribution

- The LIKE bonus distribution will start from Feb 1 to Feb 22, 30,000 LIKE will be distributed daily according to the Like count of each article get in the previous day.

  The reward given by Civic Likers will NOT be affected by the campaign

- The reward given by Civic Likers will NOT be affected by the campaign.
- **Only Likes given by the readers with a LikeCoin ID will be counted for creators' LikeCoin reward.**
- There is no limit on the number of articles by each writer to participate the campaign each day. Let's post more articles to get more Like!
- LikeCoin Foundation reserves all rights to interpret the terms of this campaign. If someone is found to abuse the system, the foundation may disqualify the user.

Tips for Earning More LIKE

The amount of LIKE earned is proportional to the number of Likes that you can get from the readers who with LikeCoin ID registered. The promotion and exposure of your article is hence very important. You cannot earn any LIKE without exposure even with the best content.

Tips for earning more LIKE:

- `Personalised LikeButton Thumbnail` Your brand is important. Let's upload your picture and customised your display name on like.co immediately so that your portrait can show up in the LikeButton.
- `Proper Featured Graphics` Choose an attractive banner for your article can surely help the click rate especially when sharing on social media.
- `Call Out` Feel free to call out your readers to register and give you Likes
- `Enhanced Search` Adding the tag `Proof of Creativity` in your Medium articles to help the community discover your works.
- `Cross Promotion` Bind your contacts such as Facebook page to your LikeCoin ID at like.co so that your fans can more likely be notified by your news.
- `Keep on Sharing` Share your works in whatever channels that you can think of. LikeCoin's telegram group is a good choice of course.

About Civic Liker

Trade a coffee for a better world

Have you ever read a great story, detailed news coverage or beautiful picture on the web, wanted to micro reward it but couldn’t?

Have you realized creativity on the web brings no direct income, creators and civil reporters can only rely on ads, outsource projects and most importantly, enthusiasm?

Civic Liker is a movement to reward open contents. For the cost of a cup of coffee, you become a Civic Liker. Whatever you Like will then be turned into a tangible reward to creators.

Don’t be missed out. Stay informed on LikeCoin.

- Website like.co
- Medium medium.com/likecoin
- Telegram t.me/likecoin
- Facebook fb.com/LikeCoin.Foundation
- Twitter twitter.com/likecoin_fdn
- YouTube youtube.com/c/LikeCoin
- Github github.com/likecoin
- Meetup meetup.com/likecoin

Releated links: Reinventing the Like Progress Review | Civic Liker Trial | □□□

Civic Liker | Reinventing The Like | English | Likecoin | Cryptocurrency

89 claps

Edmond Yu

Medium member since Sep 2017

co-founder of oice □□□□□□

Follow

LikeCoin

Reinventing the Like | □□□□

Follow

Never miss a story from LikeCoin

GET UPDATES

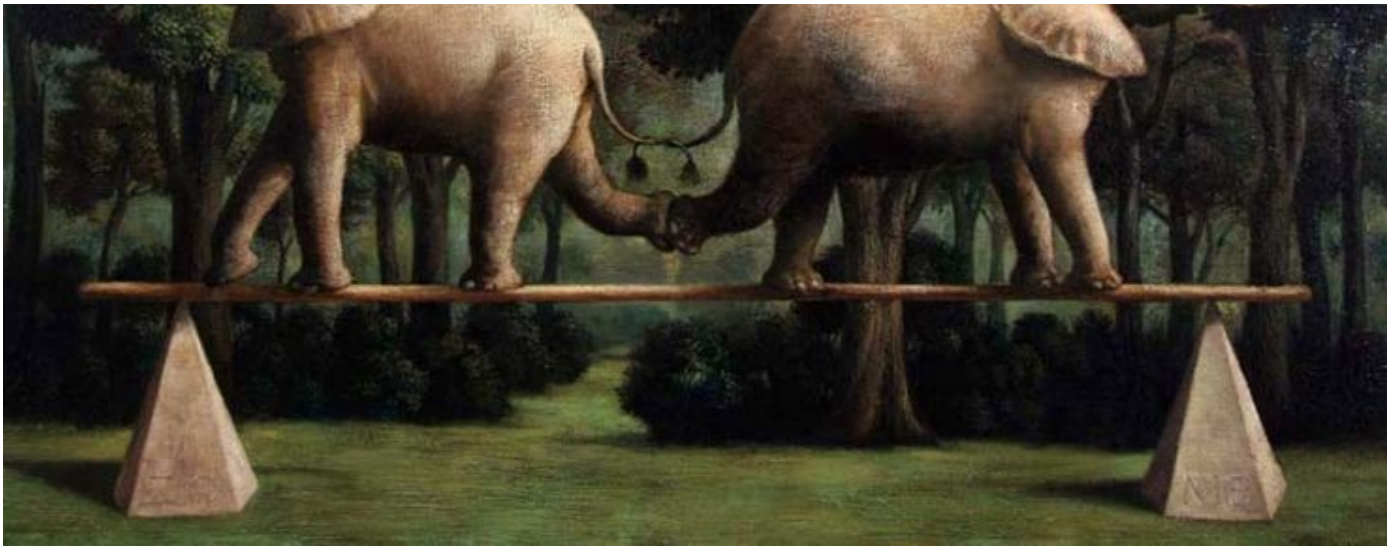
Blockchain is About Not Being Important: Distributing our Community

Anthony Lusardi
Nov 5, 2018

If Cryptocurrency is to survive then it needs to not only be decentralized but distributed. One issue we faced in our early days is a small group controlled all of the major forms of communication.

Although I believe this was entirely unintentional, it did make disagreement very one-sided after the split. Platforms and funding disappeared overnight and we had to fight to build and find new ones. This is a topic I covered extensively in an article I published earlier this year.

In this same spirit I'm going to be reducing the control I have over our various communication channels. This will further diversify control in the ETC community; making us more distributed. We'll start with removing my admin status on Discord, and promoting phyro and OmniEdge to admins.



It takes effort to be properly balanced. Ilya Zomb, Metamorphoses Of Stillness

By the very nature of our community there can’t be a central plan here but my own personal plan for this is to:

- Prefer long term independent community members over organizations.
- Have a fair balance of known and pseudonymous identities; for accountability and resilience respectively.
- Trend overlap between platforms towards zero.

Onwards and upwards towards a more resilient and distributed Ethereum Classic community!

Blockchain Ethereum Cryptocurrency Bitcoin ICO

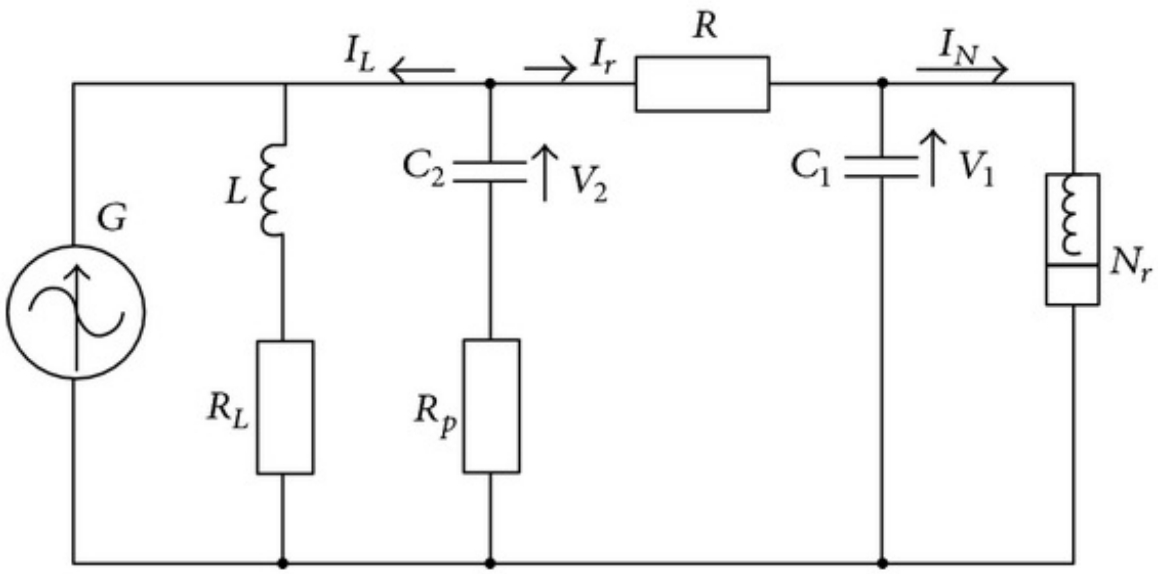
Building a Better, Unified, Testnet

The Ethereum Classic Cooperative's Grant to Project Goerli

Anthony Lusardi

Nov 20, 2018

If you've ever tried to use a testnet on the various Ethereums you've likely encountered issues including the need to mine your own blocks, client incompatibility, and difficulty getting transactions included in blocks. These issues vary depending on which chain you're using but ultimately it means that developers, especially new ones, experience substantial friction testing their applications in a live environment.



A unified circuit. I have no idea what this is. Source.

Enter Goerli, a project led by Afri Schoedon & Aidan Hyman, with a broad base of contributors that will unify PoA testnets on most major clients including parity, geth-etc/eth, and mantis*. Ultimately Goerli will make deploying and using PoA testnets easy so we all may have reliable developer experiences.

Görli testnet is a full success so far: Three clients, three different chain heads □□😄□♀ https://t.co/vmhH1yYXvu

—@5chdn

Eventually it'll be 10 clients and 1 chain head :)

Afri Schoedon has long supported the Ethereum Classic chain through his efforts at Parity Tech and we are happy to provide his Goerli team a grant of $125,000 towards their efforts. We should see a new PoA testnet that works on most major clients ~6 months from now!

And special thanks to Yaz Khoury for helping to develop this relationship!

*Mantis will get a separate grant as we don't have enough talented Scala developers available at the moment.

Thanks to Afri Schoedon.

Blockchain Ethereum Classic Development Ethereum

Anthony Lusardi
Coder, Project Manager, Director @ ETC Cooperative

Follow

Ethereum Classic

Follow

Cryptocurrency

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

Languages

Afrikaans
العربية
Azərbaycanca
বাংলা
Bân-lâm-gú
Башҡортса
Беларуская
Беларуская (тарашкевіца)
Български
Bosanski

A **cryptocurrency** (or **crypto currency**) is a digital asset designed to work as a medium of exchange that uses strong cryptography to secure financial transactions, control the creation of additional units, and verify the transfer of assets.[1][2][3] Cryptocurrencies use decentralized control as opposed to centralized digital currency and central banking systems.[4]

Various cryptocurrency logos.

The decentralized control of each cryptocurrency works through distributed ledger technology, typically a blockchain, that serves as a public financial transaction database.[5]

Bitcoin, first released as open-source software in 2009, is generally considered the first decentralized cryptocurrency.[6] Since the release of bitcoin, over 4,000 *altcoins* (alternative variants of bitcoin, or other cryptocurrencies) have been created.

Contents [hide]

1 History
2 Formal definition
  2.1 Altcoin
  2.2 Crypto token
3 Architecture
  3.1 Blockchain
    3.1.1 Timestamping
  3.2 Mining
    3.2.1 GPU price rise
  3.3 Wallets
  3.4 Anonymity
  3.5 Fungibility
4 Economics
  4.1 Transaction fees
  4.2 Exchanges
  4.3 Atomic swaps
  4.4 ATMs
  4.5 Initial coin offerings
5 Legality
  5.1 Advertising bans
  5.2 U.S. tax status
  5.3 The legal concern of an unregulated global economy
  5.4 Loss, theft, and fraud

5.5 Darknet markets
5.6 Legality in Indonesia
6 Reception
6.1 Academic studies
7 See also
8 References
9 Further reading
10 External links

History

See also: History of bitcoin

In 1983, the American cryptographer David Chaum conceived an anonymous cryptographic electronic money called ecash.[7][8] Later, in 1995, he implemented it through Digicash,[9] an early form of cryptographic electronic payments which required user software in order to withdraw notes from a bank and designate specific encrypted keys before it can be sent to a recipient. This allowed the digital currency to be untraceable by the issuing bank, the government, or any third party.

In 1996, the NSA published a paper entitled *How to Make a Mint: the Cryptography of Anonymous Electronic Cash*, describing a Cryptocurrency system first publishing it in a MIT mailing list[10] and later in 1997, in *The American Law Review* (Vol. 46, Issue 4).[11]

In 1998, Wei Dai published a description of "b-money", characterized as an anonymous, distributed electronic cash system.[12] Shortly thereafter, Nick Szabo described bit gold.[13] Like bitcoin and other cryptocurrencies that would follow it, bit gold (not to be confused with the later gold-based exchange, BitGold) was described as an electronic currency system which required users to complete a proof of work function with solutions being cryptographically put together and published. A currency system based on a reusable proof of work was later created by Hal Finney who followed the work of Dai and Szabo.

The first decentralized cryptocurrency, bitcoin, was created in 2009 by pseudonymous developer Satoshi Nakamoto. It used SHA-256, a cryptographic hash function, as its proof-of-work scheme.[14][15] In April 2011, Namecoin was created as an attempt at forming a decentralized DNS, which would make internet censorship very difficult. Soon after, in October 2011, Litecoin was released. It was the first successful cryptocurrency to use scrypt as its hash function instead of SHA-256. Another notable cryptocurrency, Peercoin was the first to use a proof-of-work/proof-of-stake hybrid.[16]

On 6 August 2014, the UK announced its Treasury had been commissioned to do a study of cryptocurrencies, and what role, if any, they can play in the UK economy. The study was also to report on whether regulation should be considered.[17]

Formal definition

According to Jan Lansky, a cryptocurrency is a system that meets six conditions:[18]

1. The system does not require a central authority, its state is maintained

through distributed consensus.
2. The system keeps an overview of cryptocurrency units and their ownership.
3. The system defines whether new cryptocurrency units can be created. If new cryptocurrency units can be created, the system defines the circumstances of their origin and how to determine the ownership of these new units.
4. Ownership of cryptocurrency units can be proved exclusively cryptographically.
5. The system allows transactions to be performed in which ownership of the cryptographic units is changed. A transaction statement can only be issued by an entity proving the current ownership of these units.
6. If two different instructions for changing the ownership of the same cryptographic units are simultaneously entered, the system performs at most one of them.

In March 2018, the word *cryptocurrency* was added to the *Merriam-Webster Dictionary*.[19]

Altcoin

The term altcoin has various similar definitions. Stephanie Yang of *The Wall Street Journal* defined altcoins as "alternative digital currencies,"[20] while Paul Vigna, also of *The Wall Street Journal*, described altcoins as alternative versions of bitcoin.[21] Aaron Hankins of the *MarketWatch* refers to any cryptocurrencies other than bitcoin as altcoins.[22]

Crypto token

A blockchain account can provide functions other than making payments, for example in decentralized applications or smart contracts. In this case, the units or coins are sometimes referred to as crypto tokens (or cryptotokens).

Architecture

Decentralized cryptocurrency is produced by the entire cryptocurrency system collectively, at a rate which is defined when the system is created and which is publicly known. In centralized banking and economic systems such as the Federal Reserve System, corporate boards or governments control the supply of currency by printing units of fiat money or demanding additions to digital banking ledgers. In case of decentralized cryptocurrency, companies or governments cannot produce new units, and have not so far provided backing for other firms, banks or corporate entities which hold asset value measured in it. The underlying technical system upon which decentralized cryptocurrencies are based was created by the group or individual known as Satoshi Nakamoto.[23]

As of May 2018, over 1,800 cryptocurrency specifications existed.[24] Within a cryptocurrency system, the safety, integrity and balance of ledgers is maintained by a community of mutually distrustful parties referred to as miners: who use their computers to help validate and timestamp transactions, adding them to the ledger in accordance with a particular timestamping scheme.[14]

Most cryptocurrencies are designed to gradually decrease production of that

currency, placing a cap on the total amount of that currency that will ever be in circulation.[25] Compared with ordinary currencies held by financial institutions or kept as cash on hand, cryptocurrencies can be more difficult for seizure by law enforcement.[1] This difficulty is derived from leveraging cryptographic technologies.

Blockchain

Main article: Blockchain

The validity of each cryptocurrency's coins is provided by a blockchain. A blockchain is a continuously growing list of records, called *blocks*, which are linked and secured using cryptography.[23][26] Each block typically contains a hash pointer as a link to a previous block,[26] a timestamp and transaction data.[27] By design, blockchains are inherently resistant to modification of the data. It is "an open, distributed ledger that can record transactions between two parties efficiently and in a verifiable and permanent way".[28] For use as a distributed ledger, a blockchain is typically managed by a peer-to-peer network collectively adhering to a protocol for validating new blocks. Once recorded, the data in any given block cannot be altered retroactively without the alteration of all subsequent blocks, which requires collusion of the network majority.

Blockchains are secure by design and are an example of a distributed computing system with high Byzantine fault tolerance. Decentralized consensus has therefore been achieved with a blockchain.[29] Blockchains solve the double-spending problem without the need of a trusted authority or central server, assuming no 51% attack (that has worked against several cryptocurrencies).

Timestamping

Cryptocurrencies use various timestamping schemes to "prove" the validity of transactions added to the blockchain ledger without the need for a trusted third party.

The first timestamping scheme invented was the proof-of-work scheme. The most widely used proof-of-work schemes are based on SHA-256 and scrypt.[16]

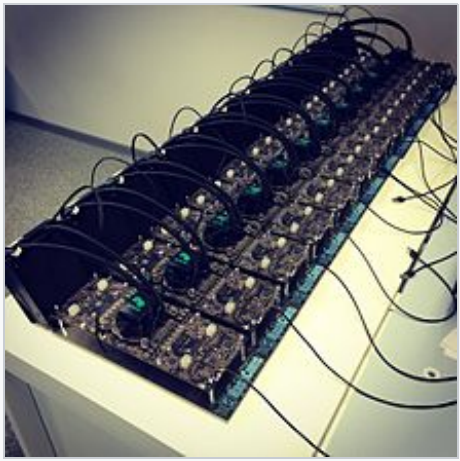
Some other hashing algorithms that are used for proof-of-work include CryptoNight, Blake, SHA-3, and X11.

The proof-of-stake is a method of securing a cryptocurrency network and achieving distributed consensus through requesting users to show ownership of a certain amount of currency. It is different from proof-of-work systems that run difficult hashing algorithms to validate electronic transactions. The scheme is largely dependent on the coin, and there's currently no standard form of it. Some cryptocurrencies use a combined proof-of-work/proof-of-stake scheme.[16]

Mining

In cryptocurrency networks, *mining* is a validation of transactions. For this effort, successful miners obtain new cryptocurrency as a reward. The reward decreases transaction fees by creating a complementary incentive to contribute to the processing power of the network. The rate of generating hashes, which validate any transaction, has been increased by the use of specialized machines such as FPGAs

and ASICs running complex hashing algorithms like SHA-256 and Scrypt.[30] This arms race for cheaper-yet-efficient machines has been on since the day the first cryptocurrency, bitcoin, was introduced in 2009.[30] With more people venturing into the world of virtual currency, generating hashes for this validation has become far more complex over the years, with miners having to invest large sums of money on employing multiple high performance ASICs. Thus the value of the currency obtained for finding a hash often does not justify the amount of money spent on setting up the machines, the cooling facilities to overcome the enormous amount of heat they produce, and the electricity required to run them.[30][31]



Hashcoin mine

Some miners pool resources, sharing their processing power over a network to split the reward equally, according to the amount of work they contributed to the probability of finding a block. A "share" is awarded to members of the mining pool who present a valid partial proof-of-work.

As of February 2018, the Chinese Government halted trading of virtual currency, banned initial coin offerings and shut down mining. Some Chinese miners have since relocated to Canada.[32] One company is operating data centers for mining operations at Canadian oil and gas field sites, due to low gas prices.[33] In June 2018, Hydro Quebec proposed to the provincial government to allocate 500 MW to crypto companies for mining.[34] According to a February 2018 report from *Fortune*,[35] Iceland has become a haven for cryptocurrency miners in part because of its cheap electricity. Prices are contained because nearly all of the country's energy comes from renewable sources, prompting more mining companies to consider opening operations in Iceland. The region's energy company says bitcoin mining is becoming so popular that the country will likely use more electricity to mine coins than power homes in 2018. In October 2018 Russia was to become home to one of the largest legal mining operations in the world, located in Siberia.[*citation needed*]

In March 2018, a town in Upstate New York put an 18-month moratorium on all cryptocurrency mining in an effort to preserve natural resources and the "character and direction" of the city.[36]

GPU price rise

An increase in cryptocurrency mining increased the demand of graphics cards (GPU) in 2017.[37] Popular favorites of cryptocurrency miners such as Nvidia's GTX 1060 and GTX 1070 graphics cards, as well as AMD's RX 570 and RX 580 GPUs, doubled or tripled in price – or were out of stock.[38] A GTX 1070 Ti which was released at a price of $450 sold for as much as $1100. Another popular card GTX 1060's 6 GB model was released at an MSRP of $250, sold for almost $500. RX 570 and RX 580 cards from AMD were out of stock for almost a year. Miners

regularly buy up the entire stock of new GPU's as soon as they are available.[39]

Nvidia has asked retailers to do what they can when it comes to selling GPUs to gamers instead of miners. "Gamers come first for Nvidia," said Boris Böhles, PR manager for Nvidia in the German region.[40]

Wallets

Main article: Cryptocurrency wallet

An example paper printable bitcoin wallet consisting of one bitcoin address for receiving and the corresponding private key for spending

A cryptocurrency wallet stores the public and private "keys" or "addresses" which can be used to receive or spend the cryptocurrency. With the private key, it is possible to write in the public ledger, effectively spending the associated cryptocurrency. With the public key, it is possible for others to send currency to the wallet.

Anonymity

Bitcoin is pseudonymous rather than anonymous in that the cryptocurrency within a wallet is not tied to people, but rather to one or more specific keys (or "addresses").[41] Thereby, bitcoin owners are not identifiable, but all transactions are publicly available in the blockchain. Still, cryptocurrency exchanges are often required by law to collect the personal information of their users.

Additions such as Zerocoin, Zerocash and CryptoNote have been suggested, which would allow for additional anonymity and fungibility.[42][43]

Fungibility

Main articles: Fungibility and Non-fungible token

Most cryptocurrency tokens are fungible and interchangeable. However, unique non-fungible tokens also exist. Such tokens can serve as assets in games like CryptoKitties.

Economics

Cryptocurrencies are used primarily outside existing banking and governmental institutions and are exchanged over the Internet.

Transaction fees

Transaction fees for cryptocurrency depend mainly on the supply of network capacity at the time, versus the demand from the currency holder for a faster transaction. The currency holder can choose a specific transaction fee, while network entities process transactions in order of highest offered fee to lowest. Cryptocurrency exchanges can simplify the process for currency holders by offering priority alternatives and thereby determine which fee will likely cause the transaction to be processed in the requested time.

For ether, transaction fees differ by computational complexity, bandwidth use, and

storage needs, while bitcoin transaction fees differ by transaction size and whether the transaction uses SegWit. In September 2018, the median transaction fee for ether corresponded to $0.017,[44] while for bitcoin it corresponded to $0.55.[45]

Exchanges

Main article: Cryptocurrency exchange

Cryptocurrency exchanges allow customers to trade cryptocurrencies for other assets, such as conventional fiat money, or to trade between different digital currencies.

Atomic swaps

Atomic swaps are a mechanism where one cryptocurrency can be exchanged directly for another cryptocurrency, without the need for a trusted third party such as an exchange.

ATMs

Jordan Kelley, founder of Robocoin, launched the first bitcoin ATM in the United States on 20 February 2014. The kiosk installed in Austin, Texas is similar to bank ATMs but has scanners to read government-issued identification such as a driver's license or a passport to confirm users' identities.[46]

Bitcoin ATM

Initial coin offerings

An initial coin offering (ICO) is a controversial means of raising funds for a new cryptocurrency venture. An ICO may be used by startups with the intention of avoiding regulation. However, securities regulators in many jurisdictions, including in the U.S., and Canada have indicated that if a coin or token is an "investment contract" (e.g., under the Howey test, i.e., an investment of money with a reasonable expectation of profit based significantly on the entrepreneurial or managerial efforts of others), it is a security and is subject to securities regulation. In an ICO campaign, a percentage of the cryptocurrency (usually in the form of "tokens") is sold to early backers of the project in exchange for legal tender or other cryptocurrencies, often bitcoin or ether.[47][48][49]

According to PricewaterhouseCoopers, four of the 10 biggest proposed initial coin offerings have used Switzerland as a base, where they are frequently registered as non-profit foundations. The Swiss regulatory agency FINMA stated that it would take a "balanced approach" to ICO projects and would allow "legitimate innovators to navigate the regulatory landscape and so launch their projects in a way consistent with national laws protecting investors and the integrity of the financial system." In response to numerous requests by industry representatives, a legislative ICO working group began to issue legal guidelines in 2018, which are intended to remove uncertainty from cryptocurrency offerings and to establish sustainable business practices.[50]

Legality

Main article: Legality of bitcoin by country or territory

The legal status of cryptocurrencies varies substantially from country to country and is still undefined or changing in many of them. While some countries have explicitly allowed their use and trade,[51] others have banned or restricted it. According to the Library of Congress, an "absolute ban" on trading or using cryptocurrencies applies in eight countries: Algeria, Bolivia, Egypt, Iraq, Morocco, Nepal, Pakistan, and the United Arab Emirates. An "implicit ban" applies in another 15 countries, which include Bahrain, Bangladesh, China, Colombia, the Dominican Republic, Indonesia, Iran, Kuwait, Lesotho, Lithuania, Macau, Oman, Qatar, Saudi Arabia and Taiwan.[52] In the United States and Canada, state and provincial securities regulators, coordinated through the North American Securities Administrators Association, are investigating "bitcoin scams" and ICOs in 40 jurisdictions.[53]

Various government agencies, departments, and courts have classified bitcoin differently. China Central Bank banned the handling of bitcoins by financial institutions in China in early 2014.

In Russia, though cryptocurrencies are legal, it is illegal to actually purchase goods with any currency other than the Russian ruble.[54] Regulations and bans that apply to bitcoin probably extend to similar cryptocurrency systems.[55]

Cryptocurrencies are a potential tool to evade economic sanctions for example against Russia, Iran, or Venezuela. In April 2018, Russian and Iranian economic representatives met to discuss how to bypass the global SWIFT system through decentralized blockchain technology.[56] Russia also secretly supported Venezuela with the creation of the petro (El Petro), a national cryptocurrency initiated by the Maduro government to obtain valuable oil revenues by circumventing US sanctions.

In August 2018, the Bank of Thailand announced its plans to create its own cryptocurrency, the Central Bank Digital Currency (CBDC).[57]

Advertising bans

Bitcoin and other cryptocurrency advertisements were temporarily banned on Facebook,[58] Google, Twitter,[59] Bing,[60] Snapchat, LinkedIn and MailChimp.[61] Chinese internet platforms Baidu, Tencent, and Weibo have also prohibited bitcoin advertisements. The Japanese platform Line and the Russian platform Yandex have similar prohibitions.[62]

U.S. tax status

On 25 March 2014, the United States Internal Revenue Service (IRS) ruled that bitcoin will be treated as property for tax purposes. This means bitcoin will be subject to capital gains tax.[63] In a paper published by researchers from Oxford and Warwick, it was shown that bitcoin has some characteristics more like the precious metals market than traditional currencies, hence in agreement with the IRS decision even if based on different reasons.[64]

The legal concern of an unregulated global economy

As the popularity of and demand for online currencies has increased since the inception of bitcoin in 2009,[65] so have concerns that such an unregulated person to person global economy that cryptocurrencies offer may become a threat to society. Concerns abound that altcoins may become tools for anonymous web criminals.[66]

Cryptocurrency networks display a lack of regulation that has been criticized as enabling criminals who seek to evade taxes and launder money.

Transactions that occur through the use and exchange of these altcoins are independent from formal banking systems, and therefore can make tax evasion simpler for individuals. Since charting taxable income is based upon what a recipient reports to the revenue service, it becomes extremely difficult to account for transactions made using existing cryptocurrencies, a mode of exchange that is complex and difficult to track.[66]

Systems of anonymity that most cryptocurrencies offer can also serve as a simpler means to launder money. Rather than laundering money through an intricate net of financial actors and offshore bank accounts, laundering money through altcoins can be achieved through anonymous transactions.[66]

Loss, theft, and fraud

Main article: Cryptocurrency and security

In February 2014 the world's largest bitcoin exchange, Mt. Gox, declared bankruptcy. The company stated that it had lost nearly $473 million of their customers' bitcoins likely due to theft. This was equivalent to approximately 750,000 bitcoins, or about 7% of all the bitcoins in existence. The price of a bitcoin fell from a high of about $1,160 in December to under $400 in February.[67]

Two members of the Silk Road Task Force—a multi-agency federal task force that carried out the U.S. investigation of Silk Road—seized bitcoins for their own use in the course of the investigation.[68] DEA agent Carl Mark Force IV, who attempted to extort Silk Road founder Ross Ulbricht ("Dread Pirate Roberts"), pleaded guilty to money laundering, obstruction of justice, and extortion under color of official right, and was sentenced to 6.5 years in federal prison.[68] U.S. Secret Service agent Shaun Bridges pleaded guilty to crimes relating to his diversion of $800,000 worth of bitcoins to his personal account during the investigation, and also separately pleaded guilty to money laundering in connection with another cryptocurrency theft; he was sentenced to nearly eight years in federal prison.[69]

Homero Josh Garza, who founded the cryptocurrency startups GAW Miners and ZenMiner in 2014, acknowledged in a plea agreement that the companies were part of a pyramid scheme, and pleaded guilty to wire fraud in 2015. The U.S. Securities and Exchange Commission separately brought a civil enforcement action against Garza, who was eventually ordered to pay a judgment of $9.1 million plus $700,000 in interest. The SEC's complaint stated that Garza, through his companies, had fraudulently sold "investment contracts representing shares in the profits they claimed would be generated" from mining.[70]

On 21 November 2017, the Tether cryptocurrency announced they were hacked, losing $31 million in USDT from their primary wallet.[71] The company has 'tagged' the stolen currency, hoping to 'lock' them in the hacker's wallet (making them

unspendable). Tether indicates that it is building a new core for its primary wallet in response to the attack in order to prevent the stolen coins from being used.

In May 2018, Bitcoin Gold (and two other cryptocurrencies) were hit by a successful 51% hashing attack by an unknown actor, in which exchanges lost estimated $18m.[72] In June 2018, Korean exchange Coinrail was hacked, losing US$37 million worth of altcoin. Fear surrounding the hack was blamed for a $42 billion cryptocurrency market selloff.[73] On 9 July 2018 the exchange Bancor had $23.5 million in cryptocurrency stolen.[74]

The French regulator Autorité des marchés financiers (AMF) lists 15 websites of companies that solicit investment in cryptocurrency without being authorised to do so in France.[75]

Darknet markets

Main article: Darknet market

Properties of cryptocurrencies gave them popularity in applications such as a safe haven in banking crises and means of payment, which also led to the cryptocurrency use in controversial settings in the form of online black markets, such as Silk Road.[66] The original Silk Road was shut down in October 2013 and there have been two more versions in use since then. In the year following the initial shutdown of Silk Road, the number of prominent dark markets increased from four to twelve, while the amount of drug listings increased from 18,000 to 32,000.[66]

Darknet markets present challenges in regard to legality. Bitcoins and other forms of cryptocurrency used in dark markets are not clearly or legally classified in almost all parts of the world. In the U.S., bitcoins are labelled as "virtual assets". This type of ambiguous classification puts pressure on law enforcement agencies around the world to adapt to the shifting drug trade of dark markets.[76]

Legality in Indonesia

Indonesia law No. 7 of 2011 about currency in Indonesia only allows Rupiah as a medium of exchange in Indonesia[77]. The law effectively prohibits the use of commodities such as cryptocurrencies and gold as currencies. Bank Indonesia has emphasized the prohibition on using cryptocurrency assets as a medium of exchange in Indonesia.[78].

Reception

Cryptocurrencies have been compared to Ponzi schemes, pyramid schemes[79] and economic bubbles,[80] such as housing market bubbles.[81] Howard Marks of Oaktree Capital Management stated in 2017 that digital currencies were "nothing but an unfounded fad (or perhaps even a pyramid scheme), based on a willingness to ascribe value to something that has little or none beyond what people will pay for it", and compared them to the tulip mania (1637), South Sea Bubble (1720), and dot-com bubble (1999).[82]

While cryptocurrencies are digital currencies that are managed through advanced encryption techniques, many governments have taken a cautious approach toward

them, fearing their lack of central control and the effects they could have on financial security.[83] Regulators in several countries have warned against cryptocurrency and some have taken concrete regulatory measures to dissuade users.[84] Additionally, many banks do not offer services for cryptocurrencies and can refuse to offer services to virtual-currency companies.[85] Gareth Murphy, a senior central banking officer has stated "widespread use [of cryptocurrency] would also make it more difficult for statistical agencies to gather data on economic activity, which are used by governments to steer the economy". He cautioned that virtual currencies pose a new challenge to central banks' control over the important functions of monetary and exchange rate policy.[86] While traditional financial products have strong consumer protections in place, there is no intermediary with the power to limit consumer losses if bitcoins are lost or stolen.[87] One of the features cryptocurrency lacks in comparison to credit cards, for example, is consumer protection against fraud, such as chargebacks.

An enormous amount of energy goes into proof-of-work cryptocurrency mining, although cryptocurrency proponents claim it is important to compare it to the consumption of the traditional financial system.[88]

There are also purely technical elements to consider. For example, technological advancement in cryptocurrencies such as bitcoin result in high up-front costs to miners in the form of specialized hardware and software.[89] Cryptocurrency transactions are normally irreversible after a number of blocks confirm the transaction. Additionally, cryptocurrency private keys can be permanently lost from local storage due to malware, data loss or the destruction of the physical media. This prevents the cryptocurrency from being spent, resulting in its effective removal from the markets.[90]

The cryptocurrency community refers to pre-mining, hidden launches, ICO or extreme rewards for the altcoin founders as a deceptive practice.[91] It can also be used as an inherent part of a cryptocurrency's design.[92] Pre-mining means currency is generated by the currency's founders prior to being released to the public.[93]

Paul Krugman, Nobel Memorial Prize in Economic Sciences winner does not like bitcoin, has repeated numerous times that it is a bubble that will not last[94] and links it to Tulip mania.[95] American business magnate Warren Buffett thinks that cryptocurrency will come to a bad ending.[96] In October 2017, BlackRock CEO Laurence D. Fink called bitcoin an 'index of money laundering'.[97] "Bitcoin just shows you how much demand for money laundering there is in the world," he said.

Academic studies

Main article: Ledger (journal)

In September 2015, the establishment of the peer-reviewed academic journal *Ledger* (ISSN 2379-5980) was announced. It covers studies of cryptocurrencies and related technologies, and is published by the University of Pittsburgh.[98]

The journal encourages authors to digitally sign a file hash of submitted papers, which will then be timestamped into the bitcoin blockchain. Authors are also asked to include a personal bitcoin address in the first page of their papers.[99][100]

See also

- 2018 crypto crash
- Crypto-anarchism
- Cryptocurrency bubble
- Cryptocurrency exchange
- Cryptographic protocol
- List of cryptocurrencies
- Virtual currency law in the United States

Information technology portal

Business and economics portal

References

1. ^ [a] [b] Andy Greenberg (20 April 2011). "Crypto Currency". Forbes.com. Archived from the original on 31 August 2014. Retrieved 8 August 2014.
2. ^ Cryptocurrencies: A Brief Thematic Review Archived 25 December 2017 at the Wayback Machine. *Economics of Networks Journal.* Social Science Research Network (SSRN). Date accessed 28 August 2017.
3. ^ Schueffel, Patrick (2017). *The Concise Fintech Compendium*. Fribourg: School of Management Fribourg/Switzerland. Archived from the original on 24 October 2017.
4. ^ Allison, Ian (8 September 2015). "If Banks Want Benefits of Blockchains, They Must Go Permissionless". International Business Times. Archived from the original on 12 September 2015. Retrieved 15 September 2015.
5. ^ Matteo D'Agnolo. "All you need to know about Bitcoin". *timesofindia-economictimes*. Archived from the original on 26 October 2015.
6. ^ Sagona-Stophel, Katherine. "Bitcoin 101 white paper" (PDF). Thomson Reuters. Archived from the original (PDF) on 13 August 2016. Retrieved 11 July 2016.
7. ^ "Archived copy" (PDF). Archived (PDF) from the original on 18 December 2014. Retrieved 26 October 2014.
8. ^ "Archived copy" (PDF). Archived (PDF) from the original on 3 September 2011. Retrieved 10 October 2012.
9. ^ Pitta, Julie. "Requiem for a Bright Idea". Archived from the original on 30 August 2017. Retrieved 11 January 2018.
10. ^ "How To Make A Mint: The Cryptography of Anonymous Electronic Cash". *groups.csail.mit.edu*. Archived from the original on 26 October 2017. Retrieved 11 January 2018.
11. ^ Laurie, Law; Susan, Sabett; Jerry, Solinas (11 January 1997). "How to Make a Mint: The Cryptography of Anonymous Electronic Cash". *American University Law Review*. **46** (4). Archived from the original on 12 January 2018. Retrieved 11 January 2018.
12. ^ Wei Dai (1998). "B-Money". Archived from the original on 4 October 2011.
13. ^ "Bitcoin: The Cryptoanarchists' Answer to Cash". IEEE Spectrum. Archived from the original on 4 June 2012. "Around the same time, Nick Szabo, a computer scientist who now blogs about law and the history of money, was one of the first to imagine a new digital currency from the ground up. Although many consider his scheme, which he calls "bit gold", to be a precursor to Bitcoin"
14. ^ [a] [b] Jerry Brito and Andrea Castillo (2013). "Bitcoin: A Primer for Policymakers" (PDF). *Mercatus Center*. George Mason University. Archived (PDF) from the original on 21 September 2013. Retrieved 22 October 2013.
15. ^ Bitcoin developer chats about regulation, open source, and the elusive Satoshi

Nakamoto Archived 3 October 2014 at the Wayback Machine, PCWorld, 26 May 2013

16. ^ [a] [b] [c] Wary of Bitcoin? A guide to some other cryptocurrencies Archived 16 January 2014 at the Wayback Machine, ars technica, 26 May 2013
17. ^ "UK launches initiative to explore potential of virtual currencies". *The UK News*. Archived from the original on 10 November 2014. Retrieved 8 August 2014.
18. ^ Lansky, Jan (January 2018). "Possible State Approaches to Cryptocurrencies". *Journal of Systems Integration*. **9/1**: 19–31. doi:10.20470/jsi.v9i1.335.
19. ^ "The Dictionary Just Got a Whole Lot Bigger". *Merriam-Webster*. March 2018. Retrieved 5 March 2018.
20. ^ Yang, Stephanie (31 January 2018). "Want to Keep Up With Bitcoin Enthusiasts? Learn the Lingo". *WSJ*. Retrieved 8 June 2018.
21. ^ Vigna, Paul (19 December 2017). "Which Digital Currency Will Be the Next Bitcoin?". *WSJ*. Retrieved 8 June 2018.
22. ^ Hankin, Aaron (4 June 2018). "Bitcoin begins the week with a stumble; SEC announces adviser for digital assets". *MarketWatch*. Retrieved 6 June 2018.
23. ^ [a] [b] Economist Staff (31 October 2015). "Blockchains: The great chain of being sure about things". *The Economist*. Archived from the original on 3 July 2016. Retrieved 18 June 2016.
24. ^ Badkar, Mamta (14 May 2018). "Fed's Bullard: Cryptocurrencies creating 'non-uniform' currency in US". Financial Times. Retrieved 14 May 2018.
25. ^ "How Cryptocurrencies Could Upend Banks' Monetary Role". Archived 27 September 2013 at the Wayback Machine, *American Banker*. 26 May 2013
26. ^ [a] [b] Narayanan, Arvind; Bonneau, Joseph; Felten, Edward; Miller, Andrew; Goldfeder, Steven (2016). *Bitcoin and cryptocurrency technologies: a comprehensive introduction*. Princeton: Princeton University Press. ISBN 978-0-691-17169-2.
27. ^ "Blockchain". *Investopedia*. Archived from the original on 23 March 2016. Retrieved 19 March 2016. "Based on the Bitcoin protocol, the blockchain database is shared by all nodes participating in a system."
28. ^ Iansiti, Marco; Lakhani, Karim R. (January 2017). "The Truth About Blockchain". *Harvard Business Review*. Harvard University. Archived from the original on 18 January 2017. Retrieved 17 January 2017. "The technology at the heart of bitcoin and other virtual currencies, blockchain is an open, distributed ledger that can record transactions between two parties efficiently and in a verifiable and permanent way."
29. ^ Raval, Siraj (2016). "What Is a Decentralized Application?". *Decentralized Applications: Harnessing Bitcoin's Blockchain Technology*. O'Reilly Media, Inc. pp. 1–2. ISBN 978-1-4919-2452-5. OCLC 968277125. Retrieved 6 November 2016 – via Google Books.
30. ^ [a] [b] [c] Krishnan, Hari; Saketh, Sai; Tej, Venkata (2015). "Cryptocurrency Mining – Transition to Cloud". *International Journal of Advanced Computer Science and Applications*. **6** (9). doi:10.14569/IJACSA.2015.060915. ISSN 2156-5570.
31. ^ Hern, Alex (17 January 2018). "Bitcoin's energy usage is huge – we can't afford to ignore it". The Guardian. Archived from the original on 23 January 2018. Retrieved 23 January 2018.
32. ^ "China's Crypto Crackdown Sends Miners Scurrying to Chilly Canada". 2 February 2018 – via www.bloomberg.com.
33. ^ "Cryptocurrency mining operation launched by Iron Bridge Resources". *World Oil*. 26 January 2018. Archived from the original on 30 January 2018.
34. ^ "Bitcoin and crypto currencies trending up today - Crypto Currency Daily Roundup

34. ^ "Bitcoin and crypto currencies trending up today - Crypto Currency Daily Roundup June 25 - Market Exclusive". *marketexclusive.com*. Retrieved 27 June 2018.
35. ^ "Iceland Expects to Use More Electricity Mining Bitcoin Than Powering Homes This Year". *Fortune*. Retrieved 25 March 2018.
36. ^ "Bitcoin Mining Banned for First Time in Upstate New York Town". 16 March 2018 – via www.bloomberg.com.
37. ^ "Bitcoin mania is hurting PC gamers by pushing up GPU prices". Archived from the original on 2 February 2018. Retrieved 2 February 2018.
38. ^ "Graphics card shortage leads retailers to take unusual measures". Archived from the original on 2 February 2018. Retrieved 2 February 2018.
39. ^ "AMD, Nvidia must do more to stop cryptominers from causing PC gaming card shortages, price gouging". Archived from the original on 2 February 2018. Retrieved 2 February 2018.
40. ^ "Nvidia suggests retailers put gamers over cryptocurrency miners in graphics card craze". Archived from the original on 2 February 2018. Retrieved 2 February 2018.
41. ^ Lee, Justina (13 September 2018). "Mystery of the $2 Billion Bitcoin Whale That Fueled a Selloff". *Bloomberg*.
42. ^ "What You Need To Know About Zero Knowledge". *TechCrunch*. Retrieved 2018-12-19.
43. ^ Greenberg, Andy (2017-01-25). "Monero, the Drug Dealer's Cryptocurrency of Choice, Is on Fire". *Wired*. ISSN 1059-1028. Retrieved 2018-12-19.
44. ^ https://ethgasstation.info/. Missing or empty |title= (help)
45. ^ https://bitinfocharts.com/comparison/bitcoin-transactionfees.html. Missing or empty |title= (help)
46. ^ First U.S. Bitcoin ATMs to open soon in Seattle, Austin Archived 19 October 2015 at the Wayback Machine, Reuters, 18 February 2014
47. ^ Commission, Ontario Securities. "CSA Staff Notice 46-307 Cryptocurrency Offerings". *Ontario Securities Commission*. Archived from the original on 29 September 2017. Retrieved 20 January 2018.
48. ^ "SEC Issues Investigative Report Concluding DAO Tokens, a Digital Asset, Were Securities". *www.sec.gov*. Archived from the original on 10 October 2017. Retrieved 20 January 2018.
49. ^ "Company Halts ICO After SEC Raises Registration Concerns". *www.sec.gov*. Archived from the original on 19 January 2018. Retrieved 20 January 2018.
50. ^ R Atkins (Feb. 2018). Switzerland sets out guidelines to support initial coin offerings. *Financial Times*. Retrieved 26 May 2018.
51. ^ Kharpal, Arjun (12 April 2017). "Bitcoin value rises over $1 billion as Japan, Russia move to legitimize cryptocurrency". *CNBC*. Retrieved 19 March 2018.
52. ^ "Regulation of Cryptocurrency Around the World" (PDF). *Library of Congress*. The Law Library of Congress, Global Legal Research Center. June 2018. pp. 4–5. Retrieved 15 August 2018.
53. ^ Fung, Brian (21 May 2018). "State regulators unveil nationwide crackdown on suspicious cryptocurrency investment schemes". Washington Post. Archived from the original on 27 May 2018. Retrieved 27 May 2018.
54. ^ Bitcoin's Legality Around The World Archived 16 September 2017 at the Wayback Machine, Forbes, 31 January 2014
55. ^ Tasca, Paolo (7 September 2015). "Digital Currencies: Principles, Trends, Opportunities, and Risks". Social Science Research Network. SSRN 2657598.
56. ^ Samburaj Das (May 2018) Iran and Russia Consider Using Cryptocurrency to Evade US Sanctions: Report *CCN-Altcoin News*. Retrieved 23 May 2018.

57. ^ Thompson, Luke (2018-08-24). "Bank of Thailand to launch its own crypto-currency". *Asia Times*. Retrieved 2018-08-27.
58. ^ Matsakis, Louise (30 January 2018). "Cryptocurrency scams are just straight-up trolling at this point". Wired. Archived from the original on 1 April 2018. Retrieved 2 April 2018.
59. ^ Weinglass, Simona (28 March 2018). "European Union bans binary options, strictly regulates CFDs". Times of Israel. Archived from the original on 1 April 2018. Retrieved 2 April 2018.
60. ^ Alsoszatai-Petheo, Melissa (14 May 2018). "Bing Ads to disallow cryptocurrency advertising". Microsoft. Archived from the original on 17 May 2018. Retrieved 16 May 2018.
61. ^ French, Jordan (2 April 2018). "3 Key Factors Behind Bitcoin's Current Slide". theStreet.com. Archived from the original on 3 April 2018. Retrieved 2 April 2018.
62. ^ Wilson, Thomas (28 March 2018). "Twitter and LinkedIn ban cryptocurrency adverts – leaving regulators behind". Independent. Reuters. Archived from the original on 4 April 2018. Retrieved 3 April 2018.
63. ^ Rushe, Dominic (25 March 2014). "Bitcoin to be treated as property instead of currency by IRS". *The Guardian*. Archived from the original on 1 June 2016. Retrieved 8 February 2018.
64. ^ On the Complexity and Behaviour of Cryptocurrencies Compared to Other Markets Archived 8 May 2017 at the Wayback Machine, 7 November 2014
65. ^ Iwamura, Mitsuru; Kitamura, Yukinobu; Matsumoto, Tsutomu (28 February 2014). "Is Bitcoin the Only Cryptocurrency in the Town? Economics of Cryptocurrency and Friedrich A. Hayek". doi:10.2139/ssrn.2405790. hdl:10086/26493. SSRN 2405790 .
66. ^ [a] [b] [c] [d] [e] ALI, S, T; CLARKE, D; MCCORRY, P; Bitcoin: Perils of an Unregulated Global P2P Currency [By S. T Ali, D. Clarke, P. McCorry Newcastle upon Tyne: Newcastle University: Computing Science, 2015. (Newcastle University, Computing Science, Technical Report Series, No. CS-TR-1470)
67. ^ Mt. Gox Seeks Bankruptcy After $480 Million Bitcoin Loss Archived 12 January 2015 at the Wayback Machine, Carter Dougherty and Grace Huang, Bloomberg News, 28 February 2014
68. ^ [a] [b] Sarah Jeong, DEA Agent Who Faked a Murder and Took Bitcoins from Silk Road Explains Himself Archived 29 December 2017 at the Wayback Machine, *Motherboard*, Vice (25 October 2015).
69. ^ Nate Raymond, Ex-agent in Silk Road probe gets more prison time for bitcoin theft Archived 29 December 2017 at the Wayback Machine, Reuters (7 November 2017).
70. ^ Cyris Farivar, GAW Miners founder owes nearly $10 million to SEC over Bitcoin fraud Archived 29 December 2017 at the Wayback Machine, *Ars Technica* (5 October 2017).
71. ^ Russell, Jon. "Tether, a startup that works with bitcoin exchanges, claims a hacker stole $31M". *TechCrunch*. Archived from the original on 21 November 2017. Retrieved 22 November 2017.
72. ^ "Bitcoin Gold Hit by Double Spend Attack, Exchanges Lose Millions". *CCN*. 23 May 2018. Retrieved 24 May 2018.
73. ^ Eric Lam, Jiyeun Lee, and Jordan Robertson (10 June 2018), *Cryptocurrencies Lose $42 Billion After South Korean Bourse Hack*, Bloomberg News
74. ^ Roberts, Jeff John (9 July 2018). "Another Crypto Fail: Hackers Steal $23.5 Million from Token Service Bancor". Fortune. Retrieved 10 July 2018.
75. ^ "News releases AMF: 2018". *The Autorité des marchés financiers (AMF)*. 15

March 2018. Retrieved 10 May 2018.

76. ^ Raeesi, Reza (23 April 2015). "The Silk Road, Bitcoins and the Global Prohibition Regime on the International Trade in Illicit Drugs: Can this Storm Be Weathered?". *Glendon Journal of International Studies / Revue d'Études Internationales de Glendon*. **8** (1–2). ISSN 2291-3920. Archived from the original on 22 December 2015.
77. ^ "UU No. 7 Tahun 2011" (PDF). *Bank Indonesia*. Retrieved 21 January 2019.
78. ^ Jacobs, Peter. "Pernyataan Bank Indonesia Terkait Bitcoin dan Virtual Currency Lainnya". *bank Indonesia*. Retrieved 21 January 2019.
79. ^ Polgar, David. "Cryptocurrency is a giant multi-level marketing scheme". *QZ.com*. Quartz Media LLC. Retrieved 2 March 2018.
80. ^ Analysis of Cryptocurrency Bubbles Archived 24 January 2018 at the Wayback Machine. *Bitcoins and Bank Runs: Analysis of Market Imperfections and Investor Hysterics.* Social Science Research Network (SSRN). Accessed 24 December 2017.
81. ^ McCrum, Dan (10 November 2015), "Bitcoin's place in the long history of pyramid schemes", *www.ft.com*, archived from the original on 23 March 2017
82. ^ Kim, Tae (27 July 2017), "Billionaire investor Marks, who called the dotcom bubble, says bitcoin is a 'pyramid scheme'", *www.cnbc.com*, archived from the original on 5 September 2017
83. ^ Cryptocurrency and Global Financial Security Panel at Georgetown Diplomacy Conf Archived 15 August 2014 at the Wayback Machine, MeetUp, 11 April 2014
84. ^ Schwartzkopff, Frances (17 December 2013). "Bitcoins Spark Regulatory Crackdown as Denmark Drafts Rules". Bloomberg. Archived from the original on 29 December 2013. Retrieved 29 December 2013.
85. ^ Sidel, Robin (22 December 2013). "Banks Mostly Avoid Providing Bitcoin Services. Lenders Don't Share Investors' Enthusiasm for the Virtual-Currency Craze". Online.wsj.com. Archived from the original on 19 November 2015. Retrieved 29 December 2013.
86. ^ decentralized currencies impact on central banks Archived 4 March 2016 at the Wayback Machine, rte News, 3 April 2014
87. ^ Four Reasons You Shouldn't Buy Bitcoins Archived 23 August 2017 at the Wayback Machine, Forbes, 3 April 2013
88. ^ Experiments in Cryptocurrency Sustainability Archived 11 March 2014 at the Wayback Machine, Let's Talk Bitcoin, March 2014
89. ^ Want to make money off Bitcoin mining? Hint: Don't mine Archived 5 May 2014 at the Wayback Machine, *The Week,* 15 April 2013
90. ^ Keeping Your Cryptocurrency Safe Archived 12 July 2014 at the Wayback Machine, Center for a Stateless Society, 1 April 2014
91. ^ "Scamcoins". August 2013. Archived from the original on 1 February 2014.
92. ^ Bradbury, Danny (25 June 2013). "Bitcoin's successors: from Litecoin to Freicoin and onwards". *The Guardian*. Guardian News and Media Limited. Archived from the original on 10 January 2014. Retrieved 11 January 2014.
93. ^ Morris, David Z (24 December 2013). "Beyond bitcoin: Inside the cryptocurrency ecosystem". *Fortune*. Archived from the original on 27 January 2018. Retrieved 27 January 2018.
94. ^ "PAUL KRUGMAN: Bitcoin is a more obvious bubble than housing was".
95. ^ Krugman, Paul (26 March 2018). "Opinion - Bubble, Bubble, Fraud and Trouble" – via NYTimes.com.
96. ^ "Warren Buffett: Cryptocurrency will come to a bad ending". *CNBC*.

97. ^ Imbert, Fred (13 October 2017). "BlackRock CEO Larry Fink calls bitcoin an 'index of money laundering'". Archived from the original on 30 October 2017. Retrieved 19 November 2017.
98. ^ "Introducing Ledger, the First Bitcoin-Only Academic Journal". *Motherboard*. Archived from the original on 10 January 2017.
99. ^ "Editorial Policies". *ledgerjournal.org*. Archived from the original on 23 December 2016.
100. ^ "How to Write and Format an Article for Ledger" (PDF). *Ledger*. 2015. doi:10.5195/LEDGER.2015.1 (inactive 2019-02-10). Archived (PDF) from the original on 22 September 2015.

Further reading

- Chayka, Kyle (2 July 2013). "What Comes After Bitcoin?". Pacific Standard. Retrieved 18 January 2014.

- Guadamuz, Andres; Marsden, Chris (2015). "Blockchains and Bitcoin: Regulatory responses to cryptocurrencies". *First Monday*. **20** (12). doi:10.5210/fm.v20i12.6198.

External links

- Media related to Cryptocurrency at Wikimedia Commons

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		

V · T · E	**Bitcoin**
History · Economics · Legal status	
People	Gavin Andresen · Andreas Antonopoulos · Wences Casares · Tim Draper · Hal Finney · Mark Karpelès · Satoshi Nakamoto · Charlie Shrem · Nick Szabo · Amir Taaki · Ross Ulbricht · Roger Ver · Erik Voorhees · Cody Wilson · Winklevoss twins · Craig Wright
Groups	List of bitcoin companies · List of bitcoin organizations · List of people in blockchain technology
Technologies	Base58 · Bitcoin network · Blockchain · Colored coins · **Cryptocurrency** · Bitcoin ATM · ECDSA · Lightning Network · P2P · POW ·

	Segregated Witness · SHA-2	
Software client	Bitcoin Core	
Forks	**Client**	Bitcoin XT · Bitcoin Classic · Bitcoin Unlimited
	Currency	Bitcoin Cash · Bitcoin Gold
Exchanges	ANX · Binance · Bitcoin Center NYC · Bitfinex · bitFlyer · Bithumb · BitMEX · Bitstamp · Bittrex · BTCC · BTC Markets · CEX.IO · Coinbase · Coincheck · Coinfloor · Coinrail · Coins.ph · Cryptopia · Gatecoin · Gemini · Huobi · Kraken · LocalBitcoins · OKEx · ShapeShift · Upbit	
	Defunct	BitInstant · BTC-e · Mt. Gox · QuadrigaCX
Book · Category · Commons · Portal		

V · T · E	**Cryptography**
History of cryptography · Cryptanalysis · Outline of cryptography	
Symmetric-key algorithm · Block cipher · Stream cipher · Public-key cryptography · Cryptographic hash function · Message authentication code · Random numbers · Steganography	
Category · Portal · WikiProject	

V · T · E	**Medium of exchange**	
Commodity money	Precious metals · Salt (Roman world) · Koku (rice) · Shells · Shekel (barley) · Cocoa bean (PreHispanic) · Rai stones (Micronesia) · Manilla (W. Africa) · Trade bead	
	Domestic animals	Water buffalo (SE Asia) · Cow (Hindu) · Camel (Arabia) · Yak (Tibet, China)
Money	Currency (Local) · Coinage · Paper money · Representative money (Fiat money · Gold certificates)	
General	List of historical currencies · Barter	

Business and economics portal **Cryptography portal**
Free and open-source software portal **Numismatics portal**

Categories: Cryptocurrencies | Financial technology | Decentralization | Uberisation | Applications of cryptography

https://scale.qihardware.org