



Cypherpunk Beginnings and the Case for Proof Of Work

Bob Summerwill

ACT I - The Cypherpunks



Surveillance capitalism

“Surveillance capitalism is a concept in political economics which denotes the widespread collection and commodification of personal data by corporations. This phenomenon is distinct from government surveillance, though the two can reinforce each other.”

“The concept of surveillance capitalism, as described by Shoshana Zuboff, is driven by a profit-making incentive, and arose as advertising companies, led by Google's AdWords, saw the possibilities of using personal data to target consumers more precisely”

“If you are not paying for the product, you are the product”

WIRED

Jaron Lanier Moves On

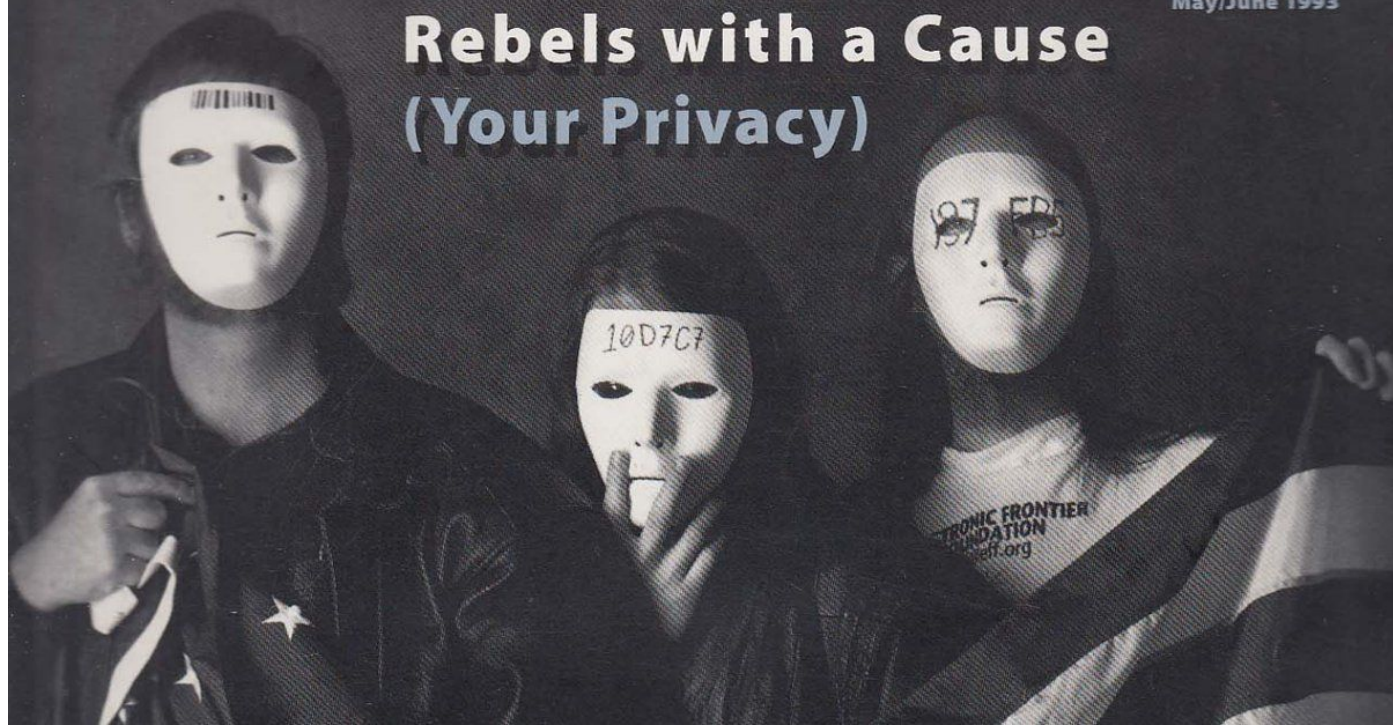
Seymour Papert:

Literacy Is Obsolete

3DO - Hip or Hype?

May/June 1993

Rebels with a Cause (Your Privacy)



Who were the Cypherpunks?

A cypherpunk is any individual advocating widespread use of strong cryptography and privacy-enhancing technologies as a route to social and political change.

Originally communicating through the Cypherpunks electronic mailing list, informal groups aimed to achieve privacy and security through proactive use of cryptography. Cypherpunks have been engaged in an active movement since at least the late 1980s.

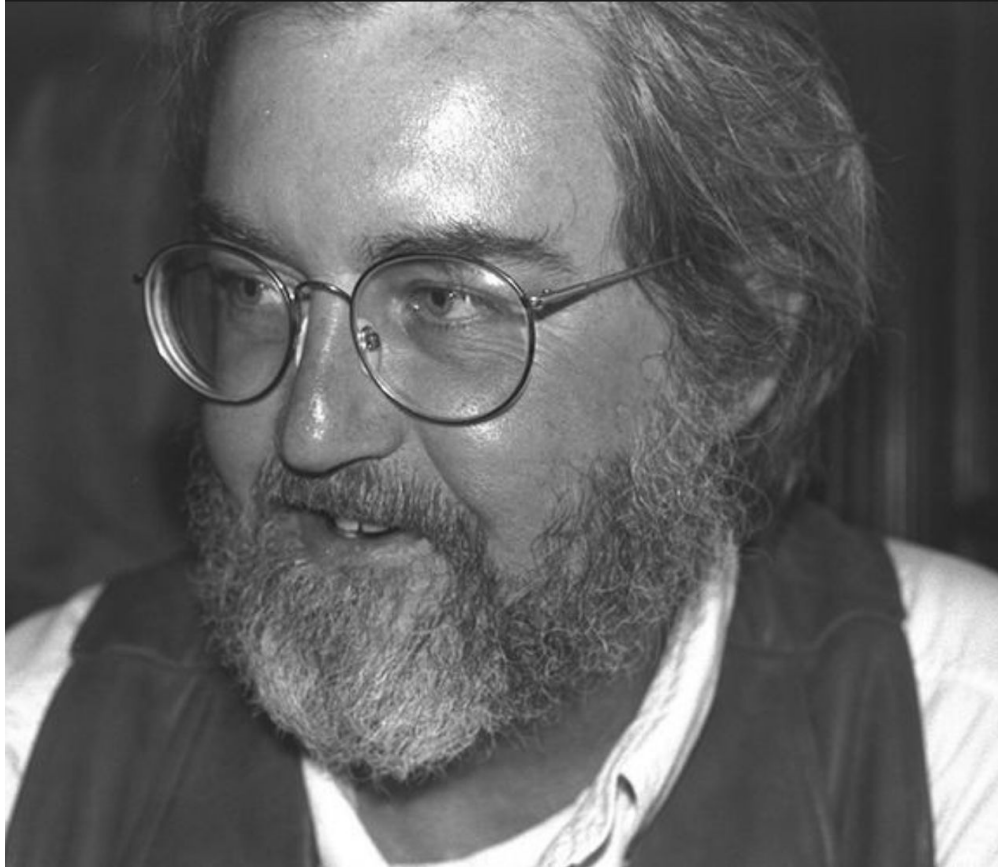
The technical roots of Cypherpunk ideas have been traced back to work by cryptographer David Chaum on topics such as anonymous digital cash and pseudonymous reputation systems, described in his paper "Security without Identification: Transaction Systems to Make Big Brother Obsolete" (1985). In the late 1980s, these ideas coalesced into something like a movement.

Cypherpunks saw the fork in the road

- Flourishing of human freedom?
- Or an Orwellian Big Brother state
- The story of the cypherpunks and of blockchain is one story
- Revolution is not pretty
- The cypherpunks were outlaws
- That fork in the road is still playing out today
- And battle is not over

Goals of the Cypherpunks

- Privacy on the internet (hence encryption)
- Censorship resistance
- Digital currency
- Smart contracts and digital agreements
- **Trust minimization (mentioned 14 times by Satoshi in Bitcoin WP)**
- The history of the cypherpunks demonstrates again and again that any centralization vector or degree of trust in third parties is always abused.
- Cryptographers are often paranoid with very good reason.



Timothy May

Timothy C. May, better known as Tim May (December 21, 1951 – December 13, 2018) was an American technical and political writer, and electronic engineer and senior scientist at Intel.

May was also the founder of the crypto-anarchist movement. He retired from Intel in 1986 at age 35 and died of natural causes at his home on December 13, 2018 at age 66.

Crypto Anarchist Manifesto (1988)

“A specter is haunting the modern world, the specter of crypto anarchy.”

“Computer technology is on the verge of providing the ability for individuals and groups to communicate and interact with each other in a totally anonymous manner. Two persons may exchange messages, conduct business, and negotiate electronic contracts without ever knowing the True Name, or legal identity, of the other.”

Crypto Anarchist Manifesto (1988)

“The technology for this revolution--and it surely will be both a social and economic revolution--has existed in theory for the past decade. **The methods are based upon public-key encryption, zero-knowledge interactive proof systems**, and various software protocols for interaction, authentication, and verification.”

“Just as the technology of printing altered and reduced the power of medieval guilds and the social power structure, so too will cryptologic methods fundamentally alter the nature of corporations and of government interference in economic transactions. Combined with emerging information markets, crypto anarchy will create a liquid market for any and all material which can be put into words and pictures.”

The Cyphernomicon - “What is Crypto Anarchy?” (1994)

“Some of us believe various forms of strong cryptography will cause the power of the state to decline, perhaps even collapse fairly abruptly. We believe the expansion into cyberspace, **with secure communications, digital money, anonymity and pseudonymity, and other crypto-mediated interactions**, will profoundly change the nature of economies and social interactions. Governments will have a hard time collecting taxes, regulating the behavior of individuals and corporations (small ones at least), and generally coercing folks when it can't even tell what continent folks are on!”



David Chaum

His 1982 dissertation "Computer Systems Established, Maintained, and Trusted by Mutually Suspicious Groups" is the first known proposal for a blockchain protocol.

Complete with the code to implement the protocol, Chaum's dissertation proposed all but one element of the blockchain later detailed in the Bitcoin whitepaper. He has been referred to as "the father of online anonymity", and "the godfather of cryptocurrency"



Adam Back

Adam Back (born July 1970) is a British cryptographer and cypherpunk. He is the CEO of Blockstream, which he co-founded in 2014.

Back is a pioneer of early digital asset research similarly as Wei Dai, David Chaum, and Hal Finney.



Nick Szabo - Smart contracts

Nicholas Szabo is a computer scientist, legal scholar, and cryptographer known for his research in digital contracts and digital currency. He graduated from the University of Washington in 1989 with a degree in computer science and received a Juris Doctor degree from George Washington University Law School. He holds an honorary professorship at the Universidad Francisco Marroquín.

The phrase and concept of "smart contracts" was developed by Szabo with the goal of bringing what he calls the "highly evolved" practices of contract law and practice to the design of electronic commerce protocols between strangers on the Internet. In 1994, he wrote an introduction to the concept and, in 1996, an exploration of what smart contracts could do.



Nick Szabo - Bit gold

In 1998, Szabo designed a mechanism for a decentralized digital currency he called "bit gold".

Bit gold was never implemented, but has been called "a direct precursor to the Bitcoin architecture. In Szabo's bit gold structure, a participant would dedicate computer power to solving cryptographic puzzles. In a bit gold network, solved puzzles would be sent to the Byzantine fault-tolerant public registry and assigned to the public key of the solver. Each solution would become part of the next challenge, creating a growing chain of new property. This aspect of the system provided a way for the network to verify and time-stamp new coins, because unless a majority of the parties agreed to accept new solutions, they couldn't start on the next puzzle.

Trusted Third Parties are Security Holes

Nick Szabo

Originally published in 2001

Introduction

Commercial security is a matter of solving the practical problems of business relationships such as privacy, integrity, protecting property, or detecting breach of contract. A security hole is any weakness that increases the risk of violating these goals. In this real world view of security, a problem does not disappear because a designer assumes it away. The invocation or assumption in a security protocol design of a "trusted third party" (TTP) or a "trusted computing base" (TCB) controlled by a third party constitutes the introduction of a security hole into that design. The security hole will then need to be plugged by other means.

Money, blockchains, and social scalability (2017)

“Instead, the secret to Bitcoin’s success is that its prolific resource consumption and poor computational scalability is buying something even more valuable: social scalability. Social scalability is the ability of an institution -- a relationship or shared endeavor, in which multiple people repeatedly participate, and featuring customs, rules, or other features which constrain or motivate participants’ behaviors -- to overcome shortcomings in human minds and in the motivating or constraining aspects of said institution that limit who or how many can successfully participate. Social scalability is about the ways and extents to which participants can think about and respond to institutions and fellow participants as the variety and numbers of participants in those institutions or relationships grow.”



Phil Zimmermann

Philip R. Zimmermann (born 1954) is an American computer scientist and cryptographer. He is the creator of Pretty Good Privacy (PGP), the most widely used email encryption software in the world. He is also known for his work in VoIP encryption protocols, notably ZRTP and Zfone. Zimmermann is co-founder and Chief Scientist of the global encrypted communications firm Silent Circle.



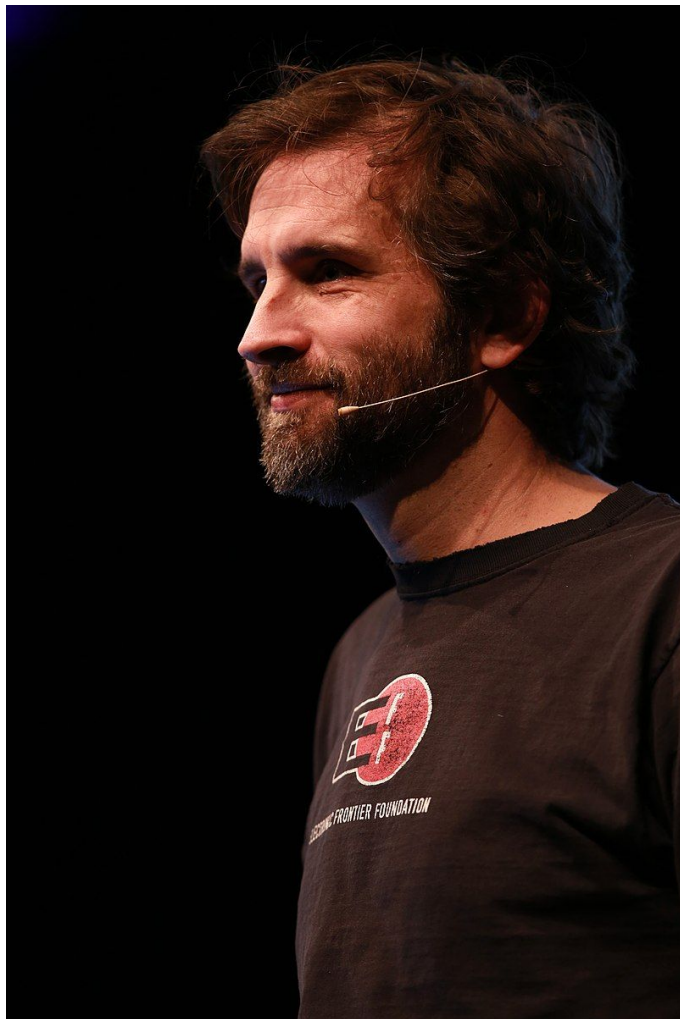
Encryption as a munition

The United States Customs Service started a criminal investigation of Zimmermann (1995), for allegedly violating the Arms Export Control Act. The United States Government had long regarded cryptographic software as a munition, and thus subject to arms trafficking export controls. At that time, PGP was considered to be impermissible ("high-strength") for export from the United States.

The “Clipper chip”

- Developed and promoted by the NSA
- To “secure” voice and data with a backdoor for law enforcement
- Intended to be adopted by telecoms companies.
- Introduced in 1993 and dead by 1996





Zooko Wilcox

Cypherpunk

Worked on DigiCash with David Chaum in 1996. Early Bitcoiner.

First use of ZK-Snarks in production with the launch of ZCash in 2017.

The Outlaws - Heroes or Villains?



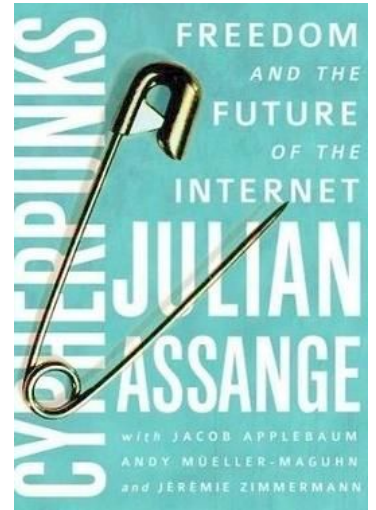
Julian Assange

Author of “Cypherpunks” book.

Wikileaks whistleblowing site exposed multiple instances of government malfeasance, notably for Chelsea Manning.

Wikileaks was one of the first cases of Bitcoin funding to work around sanctions.

Appealing extradition to US facing up to 170 years in prison.





Chelsea Manning

Chelsea Elizabeth Manning (born Bradley Edward Manning; December 17, 1987) is an American activist and whistleblower.

She is a former United States Army soldier who was convicted by court-martial in July 2013 of violations of the Espionage Act and other offenses, after disclosing to WikiLeaks nearly 750,000 classified, or unclassified but sensitive, military and diplomatic documents.

She was imprisoned from 2010 until 2017 when her sentence was commuted by President Barack Obama. A trans woman, Manning stated in 2013 that she had a female gender identity since childhood and wanted to be known as Chelsea Manning.



Edward Snowden

Exposed mass-scale secret surveillance of the US public by the the NSA and other “Five Eyes” powers.

Living in exile in Russia since 2013.

It was recently revealed that he participated in the ZCash Trusted Setup Ceremony, under a pseudonym.



Aaron Swartz

Aaron Hillel Swartz (November 8, 1986 – January 11, 2013) was an American computer programmer, entrepreneur, writer, political organizer, and Internet hacktivist.

As a programmer, Swartz helped develop the web feed format RSS; the technical architecture for Creative Commons, an organization dedicated to creating copyright licenses; the website framework web.py; and Markdown, a lightweight markup language format. Swartz was involved in the development of the social news aggregation website Reddit until he departed from the company in 2007.

He is often credited as a martyr and a prodigy, and his work focused on civic awareness and activism.



Ross Ulbrecht

Ross William Ulbricht (born March 27, 1984) is an American serving life imprisonment for creating and operating the darknet market website Silk Road from 2011 until his arrest in 2013. The site operated as a hidden service on the Tor network and facilitated the sale of narcotics and other illegal products and services. Ulbricht ran the site under the pseudonym "Dread Pirate Roberts", after the fictional character from *The Princess Bride*.



Virgil Griffith

Virgil Griffith (born 1983), also known as Romanpoet, is an American programmer. He worked extensively on the Ethereum cryptocurrency platform, designed the Tor2web proxy along with Aaron Swartz, and created the Wikipedia indexing tool WikiScanner. He has published papers on artificial life and integrated information theory.

Griffith was arrested in 2019, and in 2021 pleaded guilty to conspiring to violate U.S. laws relating to money laundering using cryptocurrency and sanctions related to North Korea. On April 12, 2022, Griffith was sentenced to 63 months imprisonment for assisting North Korea with evading sanctions and is currently in a federal low-security prison in Pennsylvania.

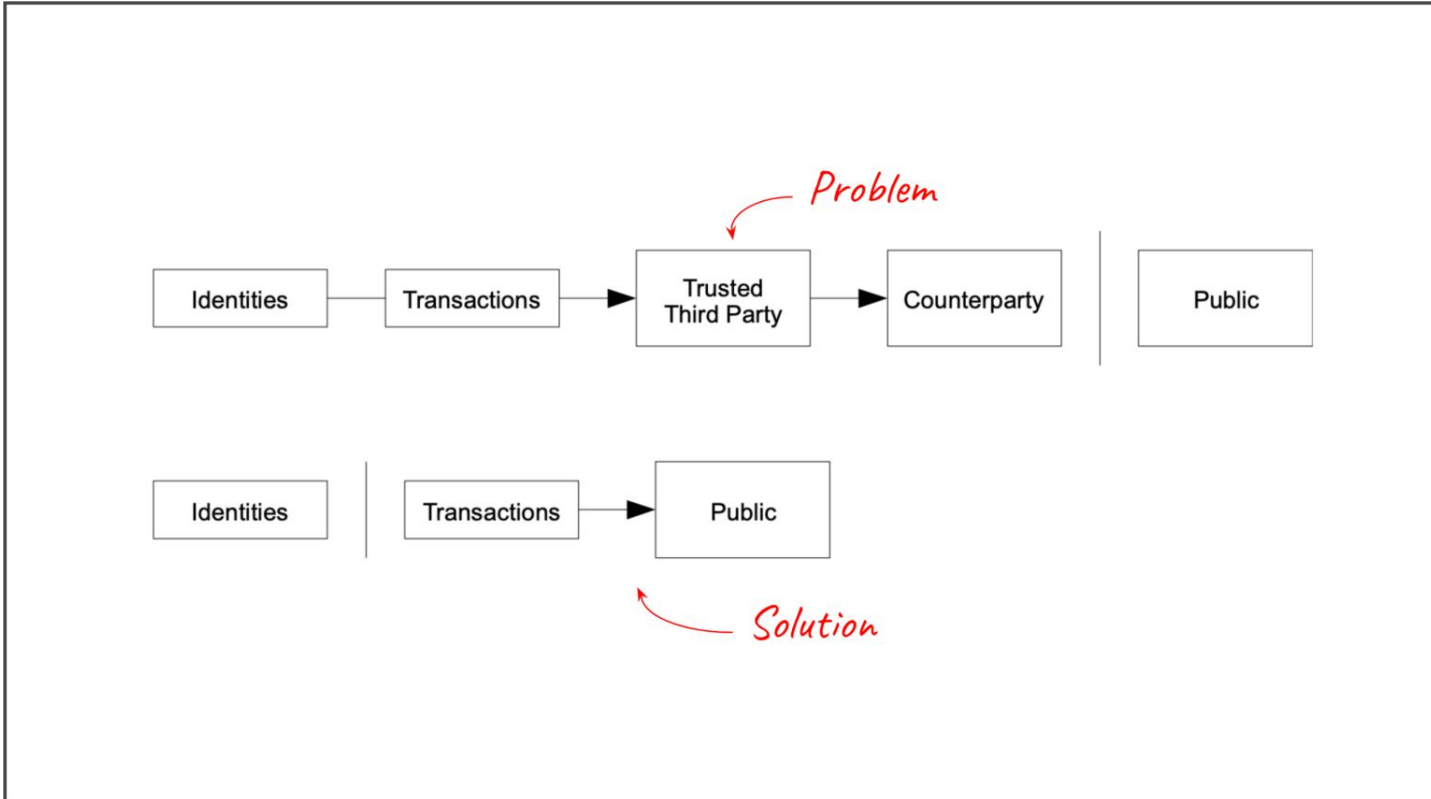
ACT 2 - Bitcoin, Blockchain, Cryptocurrency

Bitcoin: A Peer-to-Peer Electronic Cash System

Satoshi Nakamoto
satoshin@gmx.com
www.bitcoin.org

Abstract. A purely peer-to-peer version of electronic cash would allow online payments to be sent directly from one party to another without going through a financial institution. Digital signatures provide part of the solution, but the main benefits are lost if a trusted third party is still required to prevent double-spending. We propose a solution to the double-spending problem using a peer-to-peer network. The network timestamps transactions by hashing them into an ongoing chain of hash-based proof-of-work, forming a record that cannot be changed without redoing the proof-of-work. The longest chain not only serves as proof of the sequence of events witnessed, but proof that it came from the largest pool of CPU power. As long as a majority of CPU power is controlled by nodes that are not cooperating to attack the network, they'll generate the longest chain and outpace attackers. The network itself requires minimal structure. Messages are broadcast on a best effort basis, and nodes can leave and rejoin the network at will, accepting the longest proof-of-work chain as proof of what happened while they were gone.

Satoshi mentioned trust minimization 14 times!



Bitcoin - Proof of Work

- New block added to chain on average every 10 minutes
- Created by bitcoin miner (ASIC) contributing processing power
- Packing thousands of transactions into the block
- “Random guesses” - the more equipment you have the more likely to solve
- Difficulty adjustment natural rebalancing
- Completely permissionless
- In 2021 China banned crypto, and 50% of the network went offline and moved elsewhere.
- It is unstoppable whack-a-mole.
- Mining pools are NOT custodial
- Nodes can come and go at will, with the most work chain always being correct
 - this is called Nakamoto consensus

Bitcoin - Proof of Work wasteful?

- Waste of energy?
- It is not wasted because it is serving an incredibly valuable purpose - keeping the system maximally decentralized with **no** communication, not manual intervention, no subjectivity.
- Work is the arbitrator of truth and cannot be faked.
- No central authority.
- Global consensus
- The more energy, the more secure the transactions.

Proof of Stake

- Holders of the crypto lock up or stake their coins
- They are used to “vote” on the valid blockchain
- Rewarded for participating in that process
- Not electricity or computing power

Proof of Work is simple, because there is no need to punish bad miners who try to create invalid blocks, or to double-spend. Their punishment is that they spent electricity which was wasted. They self-inflict their own wounds. There is a tangible connection between the blockchain and real world resources.

Ethereum proof of stake transition

- POS was planned from the start for Ethereum, mentioned in white paper
- But it took EIGHT YEARS to implement
- POW is fundamentally simple - maybe 100 lines of code.
- ETH POS clients are hundreds of thousands of lines of code.

There are many more attack vectors from that complexity.

- Slashing mechanisms
- Long range attacks, checkpoints and weak subjectivity

Worst part of POS?

- Prone to centralization
- The more coins you have, the more voting power you have and the more rewards you acquire.
- The billionaires get millions of times more votes
- It has been described as an oligopoly
- More like a corporation and equity in that corporation

POS seems less suited for decentralized and censorship-resistant global money.

Quote

“You see that with other commodity money, like physical gold. It’s a system that works because money has a cost. I think money that doesn’t have a cost ultimately ends up being political in nature. So people closer to the money, the so-called Cantillon Effect, are going to be advantaged”

- Adam Back

Division of powers

- In a POW system (and particularly Bitcoin with its purposely small-nodes), power is distributed between miners, developers and individual nodes.
- Ability to be as miner is based on capital investment and specifically finding cheap (often stranded) electricity. Economies of scale only go so far.
- Ability to run your own node is critical, because ultimately the power rests with the nodes, not the miners, because they reject invalid blocks.
- Similar to the US Constitution with three branches of government to limit each other (Executive, Legislative and Judicial), which by design makes the political system resistant to changing too much.
- Natural state of network is to resist change.

SegWit2X and the New York Agreement

- The Bitcoin “blocksize wars” ran from around 2015-2017
- Disagreement on whether or not and how to scale the L1 chain.
- Over 80% of mining processing power, the biggest ASIC manufacturer, most exchanges and bitcoin companies were all in favor of SegWit2X. Huge corporate support.
- But they failed, because the node operators were not on board.
- UASF hats.
- Not even coin holders. Not correlated with \$\$\$.
- Uprising.
- Bigger blocks, plebs less able to run -> centralization

But POW is obsolete, right?

- POS is just plain superior to POW, right?
- Real world resource cost of POW is a feature, not a bug.
- Maximally secure.
- Simple with minimal attack surface.
- Social defense through division of responsibilities
- POS merges block producers and coin holder “pools”.
- On-chain governance (not in ETH) goes one step further, by tying the hands of the developers to the votes of the oligarchy.
- POW is better for “global money”
- POS is more similar to “tech stocks”, suitable for speculative investment if you are aware of the risks.
- Comes back to “Is ETH money? Or fuel for the decentralized computing platform?”

So you must hate the planet, then? You just don't care? 😲



TECH REVIEW EXPLAINS

Ethereum moved to proof of stake. Why can't Bitcoin?

There is no technical obstacle to making the notoriously energy-hungry cryptocurrency far more efficient—just a social one.

By Amy Castor

February 28, 2023





Home

Issues

Resources

Latest

About Us

Take Action

You've heard Bitcoin fuels the climate crisis,

but did you know a software code change could clean it up?

Our mission is to stop Bitcoin from polluting the planet.



Of course I care, but the story is not so simple

- The energy markets are complex, and very irregular
- You have “base load” fairly constant supply sources (mainly natural gas, coal and nuclear)
- But many renewables deliver very irregular amounts of energy over time (solar panels, wind) - time of year, time of day
- Storage is a big issue
- There is a lot of wastage for renewables because they have to be “over-built” because of how variable their output is.
- Transporting energy over distance is very expensive and lossy
- Decentralizing the grid is very important to minimize wasted energy

A story about the ants

- “Bitcoin uses as much power as small country X”
- Many smaller countries don’t use a lot of energy because most of their heavy duty industry has been outsourced to China and other low-cost centers.
- If you accounted for all of their imports and the energy expended as “input” then the figures would look very different.
- Some large North American cities probably use as much energy as a small country.
- Crypto mining operations are the most price sensitive thing you can imagine, not directly competing with customer energy use.
- They are like ants eating crumbs of food around the world while people are starving. If you sum all that food up you can probably make the ants look bad too.

POW incentivizes renewables

- Crypto mining incentivizes and accelerates the path to renewables
- It is a buyer of last resort - slurping up energy which would otherwise be wasted.
- It stabilizes grids, and can make new renewable energy source builds economical.
- The image of ASIc churning 24/7 is incorrect too, because they are very sensitive to price, and can be and are “abated” during periods of peak demand.
- eWaste? Electric cars are amazing but ASICs are evil?
- So much of this is demonization



FEATURE

BITCOIN 'ENERGY PER TRANSACTION' IS A MISLEADING METRIC

Measuring Bitcoin's environmental impact with "energy per transaction" is misleading and disingenuous.

LEVEL39 • JAN 12, 2022



FEATURE

THE MAJORITY OF BITCOIN MINING IS FUELED BY SUSTAINABLE ENERGY

Contrary to a Cambridge University study, Bitcoin mining leverages 52.6% sustainable energy, making it an appealing ESG investment.

DANIEL BATTEN • FEB 19, 2023



A Climate Change with Matt Matern 

@AClimateChanges



Join Matt and Adam Wright, CEO of Vespene Energy, as they discuss the importance of trapping & utilizing methane from landfills for the betterment of the environment. [#aclimatechange](#) [#adamwright](#) [#vespeneenergy](#)

Full episode: bit.ly/acc89wright



JOIN MATT MATERN AND ADAM WRIGHT FOR A DISCUSSION ABOUT
THE IMPORTANCE OF TRAPPING & UTILIZING METHANE FROM LANDFILLS




Tweet



Daniel Batten 

@DSBatten



Because it is uniquely suited to capture air-bound methane as a power-source, [#Bitcoin](#)  is on course to become carbon negative in 2025. It will achieve this without offsets.

Without offsets, Proof of Stake based cryptocurrency can never become carbon negative.

8:33 PM · Aug 22, 2022

83 Retweets **12** Quote Tweets **458** Likes

POW can be “carbon negative”, without carbon offsets

- Methane is around 30x worse than CO₂ as a greenhouse gas
- This is why you here the stories about cow's farts
- Lots of methane is just vented into the atmosphere (from landfills and other sources)
- Better than venting is flaring the methane, but all of that energy is wasted.
- There are now multiple projects putting that energy to use to with crypto mining at that energy source.
- Funds generated can be shared with the municipalities.
- The outcome is equivalent to carbon negative.

Have questions?



@bobsummerwill

June 26-27, 2023

POW SUMMIT

La Fabrika, Prague | Czech Republic

[Buy Tickets >](#)

