Cryptocurrency sucks

In excruciating detail

Drew DeVault
SourceHut

April 13, 2022

Who am I?

Drew DeVault
`https://drewdevault.com`

- Prolific FOSS developer & advocate
- Internet privacy advocate
- Digital security expert
- Internet infrastructure security expert
- Some background in traditional cryptography

Cryptocurrency holdings: 0 (today); <$10,000 (prior to 2016)

Scope of this talk

Included:

- Does cryptocurrency meet its stated goals?
- Is cryptocurrency a useful currency?
- Mostly limited to Bitcoin and Ethereum

Mostly excluded:

- Altcoins
- Blockchain utility outside of cryptocurrency
- Internal political structure of cryptocurrency
- Broader social and political consequences
- Cult of cryptocurrency
- Global finance is a pyramid scheme

Essential goals of cryptocurrency

A currency has two fundamental goals:

- Establish value
- Facilitate the exchange of value

We can evaluate currencies based on how well they meet these goals.

How does cryptocurrency establish value?

Establish *scarcity* as the basis of *value*, usually as part of a *consensus algorithm*.

- Proof of work (PoW)
- Proof of stake (PoS)
- Proof of space (also PoS, but less relevant)
- Some others...

One-way functions

One-way functions: easy to compute in one direction, hard to reverse. These functions are the basis of modern cryptography.

For example: what are the prime factors of 104,927?

$104,927 = x \times y$ Solve for x and y

One-way functions

One-way functions: easy to compute in one direction, hard to reverse. These functions are the basis of modern cryptography.

For example: what are the prime factors of 104,927?

$$104,927 = 317 \times 331$$

Hashing algorithms

Hashing algorithms are a kind of one-way function which takes some kind of arbitrary input and produces a unique numeric "hash" of that input.

Input = "hello" $\quad$ a = 0, b = 1, c = 2, ...

$$
\begin{aligned}
X &= 0 \\
X &= X + 7 \bmod 26 && \text{H} \\
X &= X + 4 \bmod 26 && \text{E} \\
X &= X + 11 \bmod 26 && \text{L} \\
X &= X + 11 \bmod 26 && \text{L} \\
X &= X + 14 \bmod 26 && \text{O} \\
X &= 21
\end{aligned}
$$

Properties of cryptographic hashes

Cryptographic hashes have specific properties:

- Easy to compute in one direction, hard to reverse
- Small changes to input = large, unpredictable changes to output
- Output is generally longer, unique

"hello" $\rightarrow$ 2cf24dba5fb0a30e26e83b2ac5b...	Easy
2cf24dba5fb0a30e26e83b2ac5b... $\rightarrow$ "hello"	Very hard (ideally impossible)

How does proof of work work?

Bitcoin uses cryptographic hashes to establish *scarcity* from the fact that starting with a cryptographic hash with desirable traits and finding a suitable input to produce it is very difficult. If I want to find an input which produces a hash starting with 20 zeroes, the only way is to try a bunch of random inputs until I find one that works.

But once I have the answer, anyone can trivially verify my work.

"hello" $\rightarrow$ 2cf24dba5fb0a30e26e83b2ac5b...	Easy
2cf24dba5fb0a30e26e83b2ac5b... $\rightarrow$ "hello"	Very hard (ideally impossible)

How does proof of work work?

The Bitcoin algorithm:

```
SHA256(ledger() + rand()) = bc4e31614f2edd1c52ab0e1f6fcfa53a4e2a90...
SHA256(ledger() + rand()) = d017f0355555ddd27b2936ac95525848d60cca...
SHA256(ledger() + rand()) = 0655fc46bf19ac30b725ad5063daf3c1ed2dca...
SHA256(ledger() + rand()) = cb7e9a76d9e5ae65ece72ff5b9bb15191e8bf2...
SHA256(ledger() + rand()) = ea8813cd9cf3fda9ec751ff780ba7ac56c084b...
SHA256(ledger() + rand()) = 00000000000000000001e280f8fa12d5af3c8...
                            ^ 20 zeroes: 6 BTC get
```

Does scarcity come from hashes?

Important: Cryptographic hashes are a derivative product of other scarce resources, and are a proxy for their value.

- Electricity to power computer hardware
- Computer hardware itself (plus the supply chain: silicon, transistors, etc)
- Real estate to store the computers in
- Others: cooling, staff, costs of business, etc

One Bitcoin has value because it serves as self-evident proof that you wasted valuable resources to produce it.

What is it all for, anyway?

Bitcoin is designed to be a currency. Bitcoin blocks contain:

- The hash of the previous block (forming a *chain* of *blocks*)
- A list of transactions to include in that block
- Random data (to produce the desired hash characteristics)

Miners (people who generate hashes) are incentivized to mine with a *block reward* and the *transaction fees* from each transaction they include. This process establishes a *consensus* on the state of a distributed ledger of transactions, thus facilitating commerce.

Don't we already have currencies?

We already have a global financial system. Does cryptocurrency do it better?

Stated promises:

- Anonymity
- Programmable money
- Decentralization
- Democratization of finance

Unstated promises:

- Lack of regulatory oversight

Further questions

- Is it useful?
- Is it secure?
- Is it efficient?
- Is it scalable?

Is it useful?

Is Bitcoin useful as a currency?

- Average transaction confirmation time: 43 minutes
- Average transaction fees: 10€

Is (for example) Visa useful as a currency?

- Transaction confirmation time: effectively instantaneous
- Transaction fees: 1-3%

Sources:
https://ycharts.com/indicators/bitcoin_average_confirmation_time
https://ycharts.com/indicators/bitcoin_average_transaction_fee
https://www.fool.com/the-ascent/research/
average-credit-card-processing-fees-costs-america/

Volatility

Forex performance against EUR over 1 year

	USD	GBP	CNY	XBT
Max/Min	10.10%	8.00%	12.05%	156.85%
% Change	8.34%	6.99%	11.51%	83.75%

Forex performance against EUR over 10 years

	USD	GBP	CNY	XBT
Max/Min	34.63%	33.54%	32.55%	1,840,444.94%
% Change	14.24%	-0.59%	13.40%	1,095,217.00%

`https://fxtop.com/en/historical-exchange-rates-comparison.php`

“But it’s still early!”

How long does it take a revolutionary technology to change the world?

Product	Release date	Market cap
iPhone introduction	January 2007	$2896B
Facebook (general availability)	September 2006	$642B
Amazon Web Services	August 2006	$1664B
Bitcoin	October 2008	$886B
Ethereum	July 2015	$423B
Dogecoin	December 2013	$20B

Side note: If you don’t think there’s a cryptocurrency bubble, I’ve got a bridge to sell you.

Cryptocurrency is revolutionary actually

Cryptocurrency *has* revolutionized one industry:

Cryptocurrency is revolutionary actually

Cryptocurrency *has* revolutionized one industry: **crime**.

- At least $739M was lost to cryptocurrency-related theft & fraud in March 2022
- $8.6B in money laundering was associated with cryptocurrency in 2021
- "WannaCry" ransomware: North Korea extorted at least $316M in cryptocurrency to fund its nuclear weapons program
- $1M in revenue from sale of child sexual abuse material (CSAM) in 2020

Sources:
Theft & fraud: `https://web3isgoinggreat.com`
Money laundering: `https://www.bbc.com/news/technology-60072195`
North Korea: Edith M. Lederer, Associated Press, summarizing a UN report
CSAM: Chainalysis: The 2021 Crypto Crime Report

Maybe financial regulation is a good idea

The lack of regulation in the cryptocurrency space is fertile ground for scams that are regulated within the traditional financial system:

- Ponzi schemes
- Insider trading
- Pump & dump
- Wash trades
- And more!

The cryptocurrency ecosystem has all of this and more in spades.

Is cryptocurrency useful?

Is cryptocurreny useful as a currency or a market?
For general use: no
For crime: yep!
Next: is it secure?

Security of the cryptography

Is SHA-256 secure?
Yes, probably. So that's a relief.

The best modern attack on SHA-2 was presented by Dmitry Khovratovich, Christian Rechberger, and Alexandra Savelieva in the paper "Bicliques for Preimages: Attacks on Skein-512 and the SHA-2 family" in 2011, which breaks pre-image resistance for SHA-256 up to 52/64 rounds in 2^{255} operations.

We are probably still many years (10+) away from practical attacks on SHA-256.

However, a cryptographic system is only as good as its side-channels...

Security of the blockchain

Proof-of-work cryptocurrencies are vulnerable to a **51% attack**, which is possible when a malicious actor controls a majority of the hashing power in a blockchain.

For large cryptocurrencies like Buttcoin and Ethereum, such attacks are probably out of reach for all but nation states. However, for smaller blockchains, these attacks are practical.

Successful 51% attacks:

- Krypton & Shift: August 2016
- Bitcoin Gold: May 2018, January 2020
- Bitcoin SV: August 2021

Attacking other side channels

Blockchain security is also threatened by other kinds of attacks:

- Cyberattacks on exchanges and wallet providers
- Real-world theft (e.g. threats of violence, B&E, ransoms, etc)
- Denial of service attacks
- Software vulnerabilities (see CVE database for examples)

Many of these attacks are possible with traditional finance (e.g. bank robberies), but mitigations exist (e.g. FDIC insurance). Transaction permanence makes it much more difficult to mitigate these incidents on the blockchain.

End-user security

What are some problems end-users face with cryptocurrencies?

- Between 2.78M and 3.79M BTC ($124B-$174B) is permanently lost as of 2017
- Consumers need technical knowledge to use cryptocurrency safely
- Security of your money relies on the security of your laptop (or wallet provider)
- No consumer protections or recourse when defrauded

Source for lost BTC: Chainanalysis

Is cryptocurrency secure?

The fundamentals are mostly secure, but...

- Small blockchains are more vulnerable to attacks
- Hundreds of billions of dollars have been lost forever
- Security is left in the hands of consumers and lay people
- No consumer protections or recourse from fraud

In short, while some (but not all) cryptocurrencies can be used securely, traditional financial systems provide a much greater level of security and consumer protections for end-users.

Next: Is cryptocurrency efficient?

The short answer is "hell no".

"*One Bitcoin has value because it serves as self-evident proof that you wasted valuable resources to produce it.*"

Is cryptocurrency efficient?

Proof-of-work cryptocurrencies directly monetize the use of electricty. It fundamentally derives value from of energy waste.

Traditional financial systems use energy to maintain the ledger, but the ledger itself is an abstraction for value that exists independently of the energy use. This is inherently a much more efficient design.

CO_2 emissions

Yep, we're going to talk about this.

Emission source	**CO_2 emissions**
Average US household consumption, weekly	102 kg
Flight from London $\rightarrow$ New York, per passenger	670 kg

CO_2 emissions

Emission source	**CO_2 emissions**
Average US household consumption, weekly	102 kg
Flight from London $\rightarrow$ New York, per passenger	670 kg
One Bitcoin transaction	402 kg
One Ethereum transaction	102 kg

CO_2 emissions

Emissions source	**CO_2**
Average US household consumption, weekly	102 kg
Flight from London $\rightarrow$ New York, per passenger	670 kg
One Bitcoin transaction	402 kg
One Ethereum transaction	102 kg
One Visa transaction	0.00045 kg

Sources:
Statista: Bitcoin average energy consumption per transaction
BBC: Climate change: Should you fly, drive or take the train?
University of Michigan: Carbon Footprint Factsheet

CO_2 emissions

Emissions source	**CO_2**	**Energy use**
Average US household consumption, weekly	102 kg	
Flight from London $\rightarrow$ New York, per passenger	670 kg	
One Bitcoin transaction	402 kg	2,258 kWh
One Ethereum transaction	102 kg	238 kWh
One Visa transaction	0.00045 kg	0.0014 kWh

Sources:
Statista: Bitcoin average energy consumption per transaction
BBC: Climate change: Should you fly, drive or take the train?
University of Michigan: Carbon Footprint Factsheet

Electronic waste

Most proof-of-work miners use *Application-specific integrated circuits* (ASICs).

- Thrown out as soon as faster hardware is available
- Once obsolete, not useful for anything else
- Pollution of heavy metals, production chemicals
- Disruption of the global electronics supply chain

Bitcoin alone produces 30.7 kT of e-waste per year, similar to the Netherlands.

272g of waste per transaction on average (about one or two iPhones in terms of weight).

Source: `https://doi.org/10.1016/j.resconrec.2021.105901`

Example: NFT sales

Everyone here (should) already understand that NFTs are horseshit. But it is horseshit with harmful consequences.

If party A buys ETH, then party B buys ETH, then party A mints and sells an NFT to party A, a total of at least 408kg of CO_2 is released.

If an artist mints and sells 33 NFTs, they will have doubled their household's carbon emissions for the year.

The big picture

Emissions source	Annual megatons CO_2
Sweden	44 Mt
Bitcoin	**37 Mt**
New Zealand	33 Mt
Nepal	8 Mt
Ethereum	**7 Mt**
El Salvador	7 Mt

Lifetime Bitcoin emissions have completely offset the global emissions reduction from the deployment of electric vehicles.

Sources:
`https://doi.org/10.1016/j.erss.2020.101721`
`https://doi.org/10.1016/j.oneear.2021.05.009`

Will Proof of Stake save us?

University of London Centre for Blockchain Technologies estimates an improvement of one third; the Ethereum developers expect a factor of ten. Both answers still leave Ethereum less efficient than traditional finance by a factor of 10,000.

Will talk more about proof of stake later in the talk!

Is cryptocurrency scalable?

Depending on which blockchain you're talking about, the answer is various ways of saying "no". We'll focus on Bitcoin, because it is the largest cryptocurrency and therefore operates at the largest scale. Ethereum scales similarly to Bitcoin, at least until Ethereum 2.0, which is now 3 years late and counting.

The theoretical scalability of other blockchains is based on speculation and modeling, as none of them have been proven at scale.

How far can cryptocurrency scale?

Can cryptocurrency scale to the global market? Let's characterize the world's payment systems in terms of transactions per second (TPS).

Product	Peak TPS
Visa	65,000
Ethereum	15
Bitcoin	7

So the answer is obviously "no", though this raises some questions.

Sources:
visa.co.uk: Visa Fact Sheet
CoinBase: Scaling Ethereum & crypto for a billion users
https://doi.org/10.1007/978-3-662-53357-4_8

Consequences of congestion

Essentially: high transaction fees and waits.

- Average Bitcoin confirmation time: 43 minutes
- Average Bitcoin transaction fees: 10€

- Average Ethereum confirmation time: 2 minutes – much better! Not great!
- Average Ethereum transaction fees: 2€

In times of high demand these numbers go up. In May 2022, Ethereum fees averaged over 70€ on two days and was consistently over 20€ throughout May. As ETH becomes more popular, this problem will worsen.

Why can't Bitcoin scale?

Recall how a Bitcoin block is made:

1. Concatenate the hash of the previous block, some random data, and a list of transactions to include in the block
2. Compute SHA-256 over this data, updating the random data until you get a hash with twenty leading zeroes

The following factors govern transaction throughput:

- Block size (governs transactions per block)
- Rate of block production

Both of these values are fixed: 10 minutes and 1 MiB.
Can they be changed?

Scalability solutions

Option 1: Increase the block size
Problem: The blockchain is already 398 GiB and can only grow: a bigger block size means greater storage requirements for every node.

Option 2: Reduce the block time (aka the *difficulty*)
The implications of this are very complicated, and I'm not going to get into it.

Changing either number requires a "fork" (and this has been tried, see e.g. Bitcoin Gold, famous for its inclusion on the list of successful 51% attacks on slide 22 of this presentation).

Important: Both approaches increase throughput *linearly*.

Lightning

Option 3: "Layer 2" protocols, e.g. the Lightning network.
Lightning was designed in 2015 and was rolled out for Bitcoin in 2019. Did it fix the problem?

Promise:	1,000,000 transactions per second
Reality:	5 transactions per second

Lightning did not make Bitcoin scalable. The reality is that there is no demand for a solution to make Bitcoin scale for payment processing because there is no demand for processing payments with Bitcoin. It is not a currency: it is a vehicle for speculative investments.

Buttcoin's promises

Recall from earlier:

- Anonymity
- Programmable money
- Decentralization
- Democratization of finance

Does Bitcoin achieve any of its stated goals?

Is cryptocurrency anonymous?

Bitcoin, Ethereum, and many other cryptocurrencies are non-anonymous by design. All transactions are publically recorded in the blockchain.

Several "Bitcoin washers" exist on the dark web, but they are very illegal: (1) it's literally money laundering; (2) you're probably violating sanctions by using them; and (3) a lot of people lose their money to fraudulent landerers.

Monero

Monero is a cryptocurrency that attempts to be actually anonymous, and largely succeeds.

It is very popular for crime:

- Currency of choice for many dark web black markets
- Common in non-consentual mining operations*
- Used for 44% of all cryptocurrency ransomware attacks
- Used by white nationalists who were deplatformed by traditional finance
- The IRS has posted a $625,000 bounty on tools to trace Monero (and others)

Monero is anonymous (for now). It still suffers from all of the other problems addressed in this talk.

Is cryptocurrency anonymous?

- Most of them are not
- Some of them are
- Their killer use-case is even more crime

But again: side-channel attacks...

Programmable money

This claim is true: it is (arguably) money, and you can program it.

Problem: Programs have bugs. Traditional finance works around this with human judgement; computers do not posess judgement.

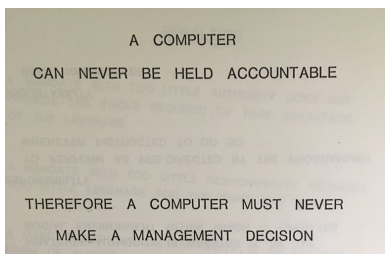


Figure: Slide from a 1979 IBM presentation, credit @bumblebike

Smart contracts

Smart contracts are essentially programmable scripts that "run" alongside Ethereum transactions, and can be used to build self-enforcing financial contracts and other complex systems on top of blockchain.

Setting aside the fact that every use of a smart contract costs as much as 70€ in fees and emits 100kg+ of CO_2 into the atmosphere...

Distribution of wealth

Let's examine cryptocurrency's promise of decentralization. I'll start with this one: is the ownership of wealth in Bitcion decentralized?

Balance in USD	Number of addresses	Percentage of wealth
$\geq \$10,000,000$	6,952	58.21%
$\geq \$1,000,000$ & $< \$10,000,000$	79,883	24.65%
$\geq \$100,000$ & $< \$1,000,000$	347,822	9.26%
$\geq \$10,000$ & $< \$100,000$	1,777,558	4.43%
$\geq \$1,000$ & $< \$10,000$	5,709,181	2.76%
$\geq \$100$ & $< \$1,000$	14,169,869	0.68%

Source: Ashish Rajendra Sai, Jim Buckley, and Andrew Le Gear; Characterizing Wealth Inequality in Cryptocurrencies

Distribution of wealth

Let's examine cryptocurrency's promise of decentralization. I'll start with this one: is the ownership of wealth in Bitcion decentralized?

Balance in USD	Number of addresses	Percentage of wealth
$\geq \$10,000,000$	6,952	58.21%
$\geq \$1,000,000$ & $< \$10,000,000$	79,883	24.65%
$\geq \$100,000$ & $< \$1,000,000$	347,822	9.26%
$\geq \$10,000$ & $< \$100,000$	1,777,558	4.43%
$\geq \$1,000$ & $< \$10,000$	5,709,181	2.76%
$\geq \$100$ & $< \$1,000$	14,169,869	0.68%

Source: Ashish Rajendra Sai, Jim Buckley, and Andrew Le Gear; Characterizing Wealth Inequality in Cryptocurrencies

Distribution of wealth

Let's examine cryptocurrency's promise of decentralization. I'll start with this one: is the ownership of wealth in Bitcion decentralized?

Balance in USD	Number of addresses	Percentage of wealth
$\geq \$10,000,000$	6,952	58.21%
$\geq \$1,000,000$ & $< \$10,000,000$	79,883	24.65%
$\geq \$100,000$ & $< \$1,000,000$	347,822	9.26%
$\geq \$10,000$ & $< \$100,000$	1,777,558	4.43%
$\geq \$1,000$ & $< \$10,000$	5,709,181	2.76%
$\geq \$100$ & $< \$1,000$	14,169,869	0.68%

Source: Ashish Rajendra Sai, Jim Buckley, and Andrew Le Gear; Characterizing Wealth Inequality in Cryptocurrencies

Distribution of power

"Over 50% of the mining power has exclusively been shared by eight miners in Bitcoin and five miners in Ethereum throughout the observed period. Even 90% of the mining power seems to be controlled by only 16 miners in Bitcoin and only 11 miners in Ethereum. Hence, both platforms rely heavily on very few distinct mining entities to maintain the blockchain."

Gencer, Adem Efe & Basu, Soumya & Eyal, Ittay & Van Renesse, Robbert & Sirer, Emin. (2018). Decentralization in Bitcoin and Ethereum Networks.

But anyone can mine crypto, right?

Mining cryptocurrency is competitive. The outcomes are predictable: those with more mining power earn more block rewards.

More mining power $\rightarrow$ More block rewards $\rightarrow$ More funds to invest in more mining power

Anyone can run a miner, but the rewards are proportaional to your ~~downline~~ investment: the wealthy take more money from a finite pool.

The part where he says Bitcoin is a pyramid scheme

It is a mathematical certainty that any cryptocurrency based on PoW will become centralized. In fact, the system will adopt a particular shape...

Cryptocurrency is a pyramid scheme. The block reward system is explicitly designed such that wealth moves from the suckers at the bottom to the miners at the top, giving them even more resources to invest in better mining equipment. Their access to mining hardware far outstrips the resources of new miners, especially anyone lacking millions to invest upfront.

Is global finance also a pyramid scheme?

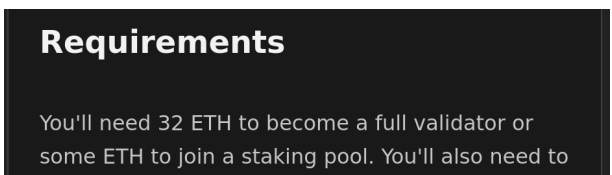
This is the only part of the talk where I am going to acknowledge this argument, which is a "whataboutism".

- Global finance, in addition to being a pyramid scheme, facilitates a productive global economy in a way that cryptocurrency does not.
- Global finance being a pyramid scheme does not make it okay for cryptocurrency to also be a pyramid scheme.
- Making new pyramid schemes does not solve the problem.

Will proof of stake save us?

Proof of stake is an even more transparent pyramid scheme.

Ethereum 2.0's block rewards are proportional to your *stake* (i.e. the amount of wealth you have in the system), so the wealthy get more block rewards simply as a function of how wealthy they are.



Bonus: The minimum investment is $111,256 USD.

Proof of Stake bonus fact

Proof-of-work currencies derive value from the waste of valuable resources, e.g. electricity.

Proof-of-stake currencies attribute value to the consensus of the stakeholders.

Ethereum 2.0 is a fiat currency!

Is cryptocurrency distributed?

So, is cryptocurrency distributed?

- 58% of the wealth owned by 0.01% of the users
- 90% of Bitcoin and Ethereum mining power held by 16 and 11 entities respectively
- New miners disadvantaged against incumbents by several orders of magnitude
- Strenuous and constantly increasing requirements for nodes
- The system centralizes wealth by design

No, cryptocurrency is not distributed. Next question: is it democratic?

Democratization of finance

Is cryptocurrency democratic?

- How are decisions made in cryptocurrencies?
- Who gets to make those decisions?
- Do end-users have any influence in these decisions?

How are decisions made?

Case study: 2013 block size controversey

Two possible outcomes:

- Consensus among all "economically active" full nodes to adopt a proposal
- Hard fork (forming N new blockchains for each of N possible outcomes)

Segregated Witness

The solution eventually adopted was “Segregated Witness”, which, among other things effectively raised the block size limit to 1 MiB.

The deployment was marred by miners blocking the change as it disfavored their interests, which delayed the rollout by almost a year. Required coordinated, large-scale, and near unanimous action among users to overcome.

Understanding the problem required either a substantial technical, political, and economic background; or choosing entities to trust amid a flurry of large-scale disinformation campaigns.

The DAO

Case study: Ethereum's DAO hard fork

Promise: Smart contracts mediate commerce entirely automatically and independently of social or political concerns.

Reality: When the chips were down and money was walking out of the door, the powers that be resorted to social and political solutions to recover their money.

Is cryptocurrency democratic?

The answer is a highly qualified "I don't really know".

- Difficult to resolve conflicts of interest
- Miners have disparate access to capital and propaganda tools
- "Core developers" have weird, difficult to characterize power
- Large-scale and well-coordinated grassroots action can work
- Informed political action requires technical, political, and economic background
- Also: smart contracts and DAOs are dumb and their promise is a lie

The scorecard so far

Is cryptocurrency:

- ~~Anonymous~~
- Programmable money: yes, but
- ~~Decentralized~~
- Democratic: I don't know and neither do you
- Useful for ~~general commerce~~ and criminal commerce
- Secure for ~~lay people~~ and experts
- ~~Efficient~~
- ~~Scalable~~

Other cryptocurrencies?

There are cryptocurrencies which claim to be looking into these problems. Here are some things to watch out for while evaluating them:

- Solving one problem but not the others
- A design that centralizes wealth & power
- Small enough to be vulnerable to attacks

Almost all cryptocurrencies are a scam. Don't be a victim. Do not victimize others. Do not treat it as an investment.

Scope of this talk

Included:

- Does cryptocurrency meet its stated goals?
- Is cryptocurrency a useful currency?
- Mostly limited to Bitcoin and Ethereum

Mostly excluded:

- Altcoins
- Blockchain utility outside of cryptocurrency
- Internal political structure of cryptocurrency
- Broader social and political consequences
- Cult of cryptocurrency
- Global finance is a pyramid scheme

Questions?

Thanks for listening! Any questions?

Slidedeck and other resources
`https://drewdevault.com/talks/cryptocurrency.html`