Zcash 2.0

misconceptions about unstoppable private money

Frank Braun

2025-10-04

@thefrankbraun

Introduction

about me

> “I believe that, for a free society, the ability to communicate and *transact privately* is essential.”

- cypherpunk
- cryptoanarchist
- I want *freedom money*
- which got me into Bitcoin

However…

what's the biggest problem with Bitcoin?

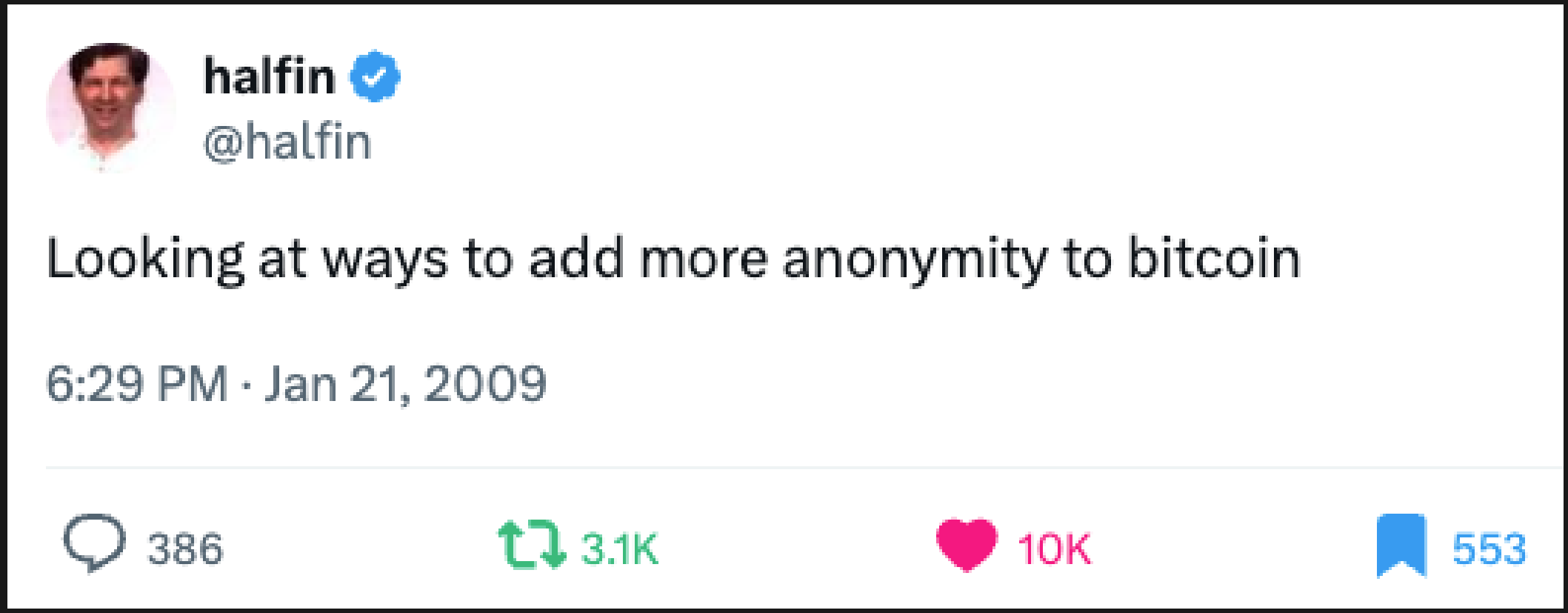
A: blocks too small

B: only 21M coins

C: lack of privacy

D: unknown founder

lack of privacy



x.com/halfin/status/1136749815

Bitcoin Talk, August 11, 2010

> As some might have noticed, one of the things that bugs me about bitcoin is that the entire history of transactions is completely public.

> Although I was recently reading about …

> “This is a very interesting topic. If a solution was found, a much better, easier, more convenient implementation of Bitcoin would be possible.”

(Satoshi)

Money

what is money?

definition:

- medium of exchange (7 Euro exchanged for Döner)
- unit of account (your total balance is 2.56 Euro)
- store of value (Krugerrand under mattress)

what is money?

features:

1. portability (cattle are not portable)
2. divisibility (cattle are not divisible)
3. durability (tea is not durable)
4. rarity (sand is not rare)
5. fungibility (diamonds are not fungible)

Gold

property	
portable	❌
divisible	❌
durable	✅
rare	⚠️
fungible	✅

- good analog money
- ~1-2% anual inflation

fiat money

property	
portable	✅
divisible	✅
durable	⚠️
rare	❌
fungible	⚠️

- cash is good (medium of exhange, unit of account)
- cash is trash (store of value)

comparison

property	Gold	Fiat
portable	❌	✅
divisible	❌	✅
durable	✅	⚠️
rare	⚠️	❌
fungible	✅	⚠️

what is digital cash?

- **anonymous** electronic money
- aka "*unstoppable private money*"
- aka "*freedom money*"

Early incarnations:

- David Chaums' DigiCash (1982 paper, 1990s implementation)
- E-gold (1996, shut down in 2009)

Main problem: centralization

what is unstoppable private money?

1. unstoppable
    - decentralized
    - censorship resistant
    - cannot be switched off
2. private
    - sender & receiver anonymity
    - hidden amounts
    - no metadata leakage
3. money
    - has money properties
    - integrated & exchangeable
    - number go up (NgU) tech 🚀

Bitcoin

2009: modern digital cash (genesis)

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.

bitcoin.org/bitcoin.pdf

Bitcoin

property	
portable	✅
divisible	✅
durable	✅
rare	✅
fungible	⚠️

- digital gold
- solved double-spending problem without a trusted party
- “tainted” coins can be blacklisted

comparison

property	Gold	Fiat	Bitcoin
portable	❌	✅	✅
divisible	❌	✅	✅
durable	✅	⚠️	✅
rare	⚠️	❌	✅
fungible	✅	⚠️	⚠️

- made gold digital
- but less fungible

Satoshi on zero-knowledge proofs

> “This is a very interesting topic. If a solution was found, a much better, easier, more convenient implementation of Bitcoin would be possible.”

(Bitcoin Forum, August 11, 2010)

- Q: What solution?
- A: How to apply zero-knowledge proofs to Bitcoin

what are zero-knowledge proofs?

in cryptography, a zero-knowledge, is a protocol in which:

- one party (the prover)
- can convince another party (the verifier)
- that some given statement is true,
- without conveying to the verifier any information beyond the mere fact of that statement's truth.

Bitcoin with ZKPs: what to prove?

1. ownership (authorization)
2. existence (membership)
3. **no double-spends** (uniqueness)
4. conservation of value (no inflation)
5. amounts are valid (range)
6. outputs are well formed
7. consensus rules are respected

Satoshi’s doubt of ZK proofs

> “It’s the need to check for the absence of double-spends that requires global knowledge of all transactions.”

> “It’s hard to think of how to apply zero-knowledge-proofs in this case.”

> “We’re trying to prove the absence of something, which seems to require knowing about all and checking that the something isn’t included.”

a solution was found!

Zcash talk overview

- 🏛️ Zcash history
- 📍 Zcash present
- 🔮 Zcash future
- 🤔 Zcash misconceptions
- 🚀 Zcash investing

Zcash: common misconceptions

1. had premine
2. contains inflation bug
3. requires trusted setup
4. bad UX / not practical
5. shielded pools not used
6. centralized ecosystem
7. bad investment

Zcash history

2013: Zerocoin

2013 IEEE Symposium on Security and Privacy

Zerocoin: Anonymous Distributed E-Cash from Bitcoin

Ian Miers, Christina Garman, Matthew Green, Aviel D. Rubin
The Johns Hopkins University Department of Computer Science, Baltimore, USA
{*imiers, cgarman, mgreen, rubin*}*@cs.jhu.edu*

***Abstract*—Bitcoin is the first e-cash system to see widespread adoption. While Bitcoin offers the potential for new types of financial interaction, it has significant limitations regarding privacy. Specifically, because the Bitcoin transaction log is completely public, users' privacy is protected only through the use of pseudonyms. In this paper we propose Zerocoin, a cryptographic extension to Bitcoin that augments the protocol to allow for fully anonymous currency transactions. Our system uses standard cryptographic assumptions and does not introduce new trusted parties or otherwise change the security model of Bitcoin. We detail Zerocoin's cryptographic construction, its integration into Bitcoin, and examine its performance both in terms of computation and impact on the Bitcoin protocol.**

I. Introduction

Digital currencies have a long academic pedigree. As of yet, however, no system from the academic literature has

typically associated with e-cash schemes. On top of such transactions, one could build mechanisms to partially or explicitly identify participants to authorized parties (e.g., law enforcement). However, to limit this information to authorized parties, we must first anonymize the underlying public transactions.

The Bitcoin community generally acknowledges the privacy weaknesses of the currency. Unfortunately, the available mitigations are quite limited. The most common recommendation is to employ a *laundry service* which exchanges different users' bitcoins. Several of these are in commercial operation today [6, 7]. These services, however, have severe limitations: operators can steal funds, track coins, or simply go out of business, taking users' funds with them. Perhaps in recognition of these risks, many services offer short laundering periods, which lead to minimal transaction

doi.org/10.1109/SP.2013.34

2014: Zerocash

2014 IEEE Symposium on Security and Privacy

Zerocash: Decentralized Anonymous Payments from Bitcoin

Eli Ben-Sasson*, Alessandro Chiesa†, Christina Garman‡, Matthew Green‡, Ian Miers‡, Eran Tromer§, Madars Virza†
*Technion, eli@cs.technion.ac.il
†MIT, {alexch, madars}@mit.edu
‡Johns Hopkins University, {cgarman, imiers, mgreen}@cs.jhu.edu
§Tel Aviv University, tromer@cs.tau.ac.il

***Abstract*—Bitcoin is the first digital currency to see widespread adoption. While payments are conducted between pseudonyms, Bitcoin cannot offer strong privacy guarantees: payment transactions are recorded in a public decentralized ledger, from which much information can be deduced. Zerocoin (Miers et al., IEEE S&P 2013) tackles some of these privacy issues by unlinking transactions from the payment's origin. Yet, it still reveals payments' destinations and amounts, and is limited in functionality.**

In this paper, we construct a full-fledged ledger-based digital currency with strong privacy guarantees. Our results leverage recent advances in *zero-knowledge Succinct Non-interactive ARguments of Knowledge* (zk-SNARKs).

First, we formulate and construct *decentralized anonymous payment schemes* (DAP schemes). A DAP scheme enables users to directly pay each other privately: the corresponding transaction hides the payment's origin, destination, and transferred amount. We provide formal definitions and proofs of the construction's

party and then, after some interval, retrieve different coins (with the same total value) from the pool. Yet, mixes suffer from three limitations: (i) the delay to reclaim coins must be large to allow enough coins to be mixed in; (ii) the mix can trace coins; and (iii) the mix may steal coins.[1] For users with "something to hide," these risks may be acceptable. But typical legitimate users (1) wish to keep their spending habits private from their peers, (2) are risk-averse and do not wish to expend continual effort in protecting their privacy, and (3) are often not sufficiently aware of their compromised privacy.

To protect their *privacy*, users thus need an instant, risk-free, and, most importantly, automatic guarantee that data revealing their spending habits and account balances is not publicly accessible by their neighbors, co-workers, and merchants. Anonymous transactions also guarantee that the market value

zerocash-project.org/media/pdf/zerocash-oakland2014.pdf

2016: Zcash (genesis block)

Zcash Protocol Specification

Version 2025.6.0-79-g7d61ca [NU6.1 proposal]

Daira-Emma Hopwood†
Sean Bowe† — Taylor Hornby† — Nathan Wilcox†

September 17, 2025

zips.z.cash/protocol/protocol.pdf

2016: Zcash design

“Fork” of Bitcoin:

- total supply: 21M ZEC
- same halving schedule
- block time: 2.5m (reduced to 75s in 2019)
- proof-of-work (PoW): Equihash algorithm
- difficulty adjustment every block
- transparent addresses (t-addr)
- 20% “founders reward”

2016: Sprout (production release)

Privacy improvement over Bitcoin:

- shielded addresses (z-addr)
- Sprout pool
- trusted setup: 6 participants
- at least 1 honest participant needs to destroy toxic waste
- Edward Snowden participated
- not practical on mobile

2018: Sapling (practical release)

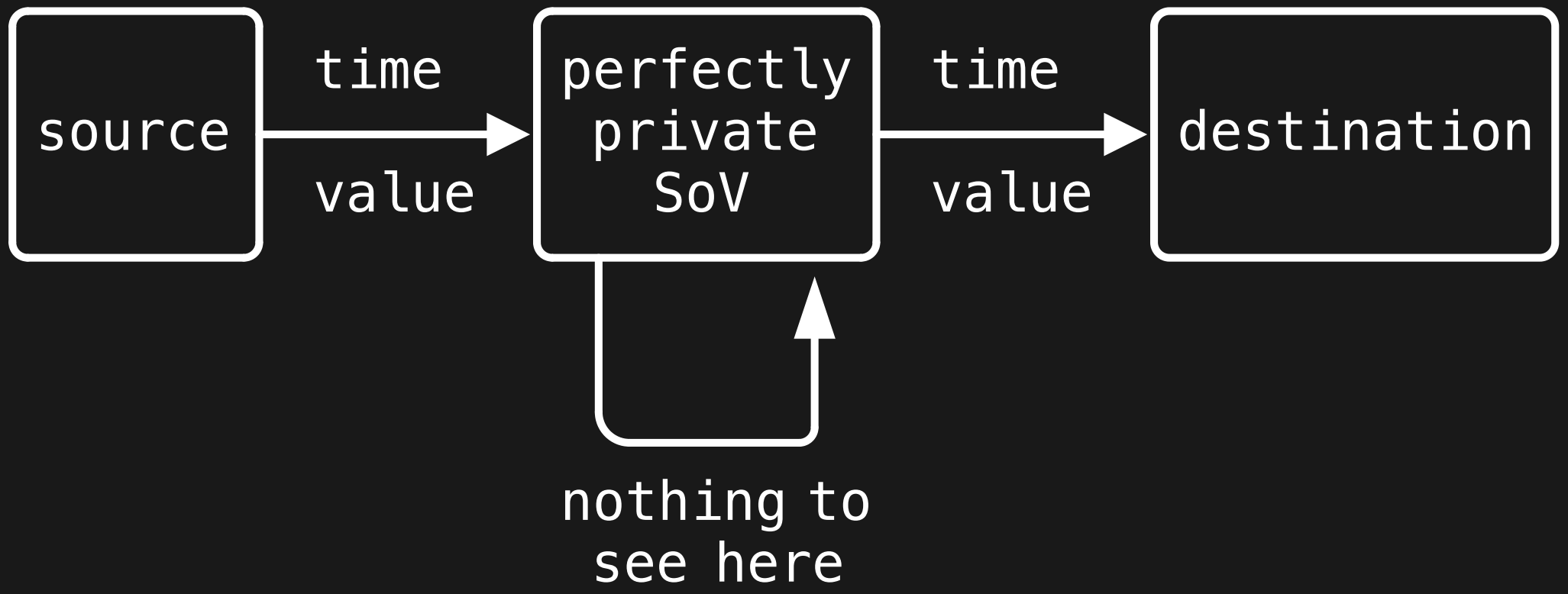
- Sapling pool
- trusted setup: two phases
- Powers of Tau (phase 1): 87 contributions
- Sapling MPS (phase 2): “over 90” contributions
- at least 1 honest participant needs to destroy toxic waste
- fixed inflation bug in Sprout (error in zk-SNARK construction)
- turnstiles also introduced
- practical on mobile

2022: Orchard (trustless release)

- Halo 2 proving system (**no** trusted setup)
- simpler transaction design
- modern crypto primitives:
- allows FROST-style multisig compatiblity
- unified addresses became the default UX
- today Orchard is the most common default
- Sapling still used, Sprout is being phased out

Zcash present

privacy comes from value at rest



frankbraun.org/layer1

why I changed my mind on t-addr

until all transactions are private, using a privacy coin means:

1. moving funds into the privacy coin
2. transacting within the privacy coin
3. moving funds out of the privacy coin

what really counts:

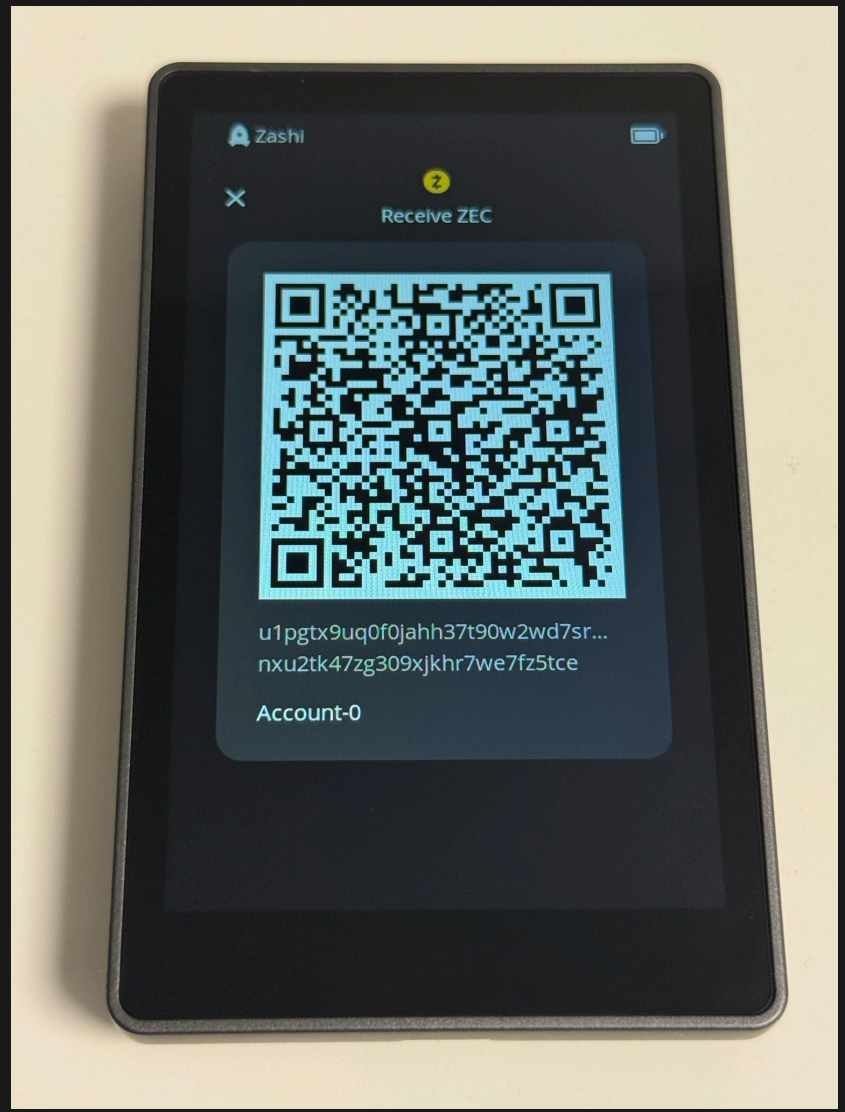
- the privacy of shielded transactions
- the integration into the wider crypto ecosystem

More details: frankbraun.org/t-addr

Zashi

- user friendly mobile wallet (iOS & Android)
- *iPhone moment for Zcash*
- designed exclusively for shielded ZEC payments
- forces shielding
- Swap ZEC with NEAR Intents (a DEX; no KYC)
- Pay with ZEC (exact amount of destination cryptocurrency)
- Pay with Flexa

hardware wallet support



frankbraun.org/keystone

the “Zashi effect”

zechub.wiki/dashboard

DEXs

- NEAR Intents → RHEA Finance (high volume)
- Maya Protocol → LeoDex / THORSwap

the market loves competition

multi-coin:

- Unstoppable Wallet supports shielded Zcash (Sapling)
- Unstoppable Wallet is adding swaps (Maya Protocol)
- Cake Wallet is adding Zcash (details TBD)

Zcash only:

- Ywallet
- Zingo!

ecocsystem decentralization

organizationally:

- Zcash Foundation (ZF) 🇺🇸
- Electric Coin Company (ECC) 🇺🇸
- Shielded Labs (donation-funded) 🇨🇭

funding wise:

- Zcash Community Grants (ZCG): 8%
- Coinholder-Directed Retroactive Grants Program: 12%

Zcash

property	
portable	✅
divisible	✅
durable	✅
rare	✅
fungible	✅

comparison

property	Gold	Fiat	Bitcoin	Zcash
portable	❌	✅	✅	✅
divisible	❌	✅	✅	✅
durable	✅	⚠️	✅	✅
rare	⚠️	❌	✅	✅
fungible	✅	⚠️	⚠️	✅

- Zcash made Bitcoin fungible
- ⇒ *unstoppable private money*

Zcash future

Money is technology — technology evolves.

more coinholder voting

- coinholder poll to ratify the retroactive grants program
- quarterly coinholder polls on retroactive grants (November)
- good governance is necessary but not sufficient for success
- examples: Decred and Tezos
- counter-example: Bitcoin?

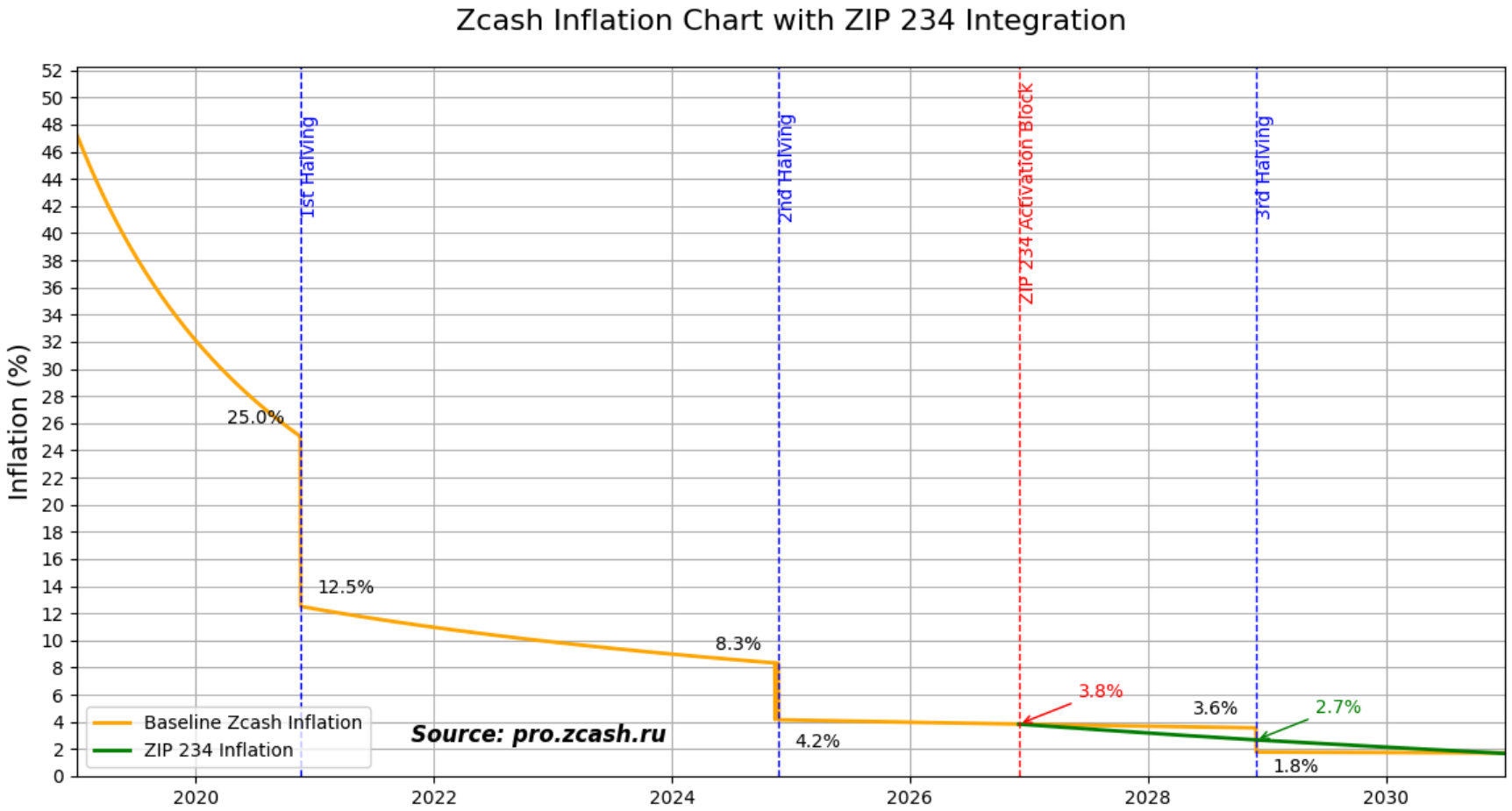
rewrite in Rust

- huge, risky undertaking (a rewrite killed Netscape)
- node: C++ node `zcashd` is being replaced by `zebrad`
- including proof system & circuits (Halo 2 & Orchard)
- wallets/services: `librustzcash`
- almost done; left: ecosystem migration, RPC parity
- benefits: higher velocity & security, better integration

NSM

- problem: future security budget (tx fees not enough?)
- constraint: 21M hard cap (like in Bitcoin)
- proposal: Network Sustainability Mechanism (NSM)
- ZIP 233: establishes a voluntary burn mechanism
- ZIP 234: smoothes the issuance curve (adds burned coins)
- ZIP 235: proposes to burn 60% of transaction fees
- no urgency: do it sooner rather than later

More details: shieldedlabs.net/nsm/



github.com/ruzcash/ZIP234-Inflation-Visualizer

ZSAs (Zcash Shielded Assets)

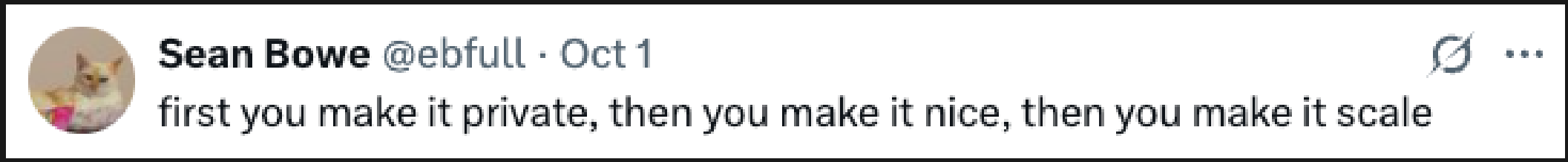
- Orchard extension enabling the creation, transfer, and burn of custom assets (like ERC-20)
- also allows for NFTs
- assets can be wrapped assets (with bridging)
- same anonymity as shielded ZEC transactions, same pool
- no freeze function
- *not* smart contracts

Crosslink proposal

- adds assured finality to Zcash by introducing PoS finalizers
- hybrid PoS/PoW (“defence in depth”)
- rooster of 100 stake weighted finalizers (they take fee)
- yield for stakers (40% stakers, 40% miners, 20% dev fund)
- staking from Orchard pool
- 21M cap unchanged

See forum discussion: forum.zcashcommunity.com/t/crosslink-early-tokenomics-design/52154

Project Tachyon



- current bottleneck: global nullifier set (no pruning)
- wallets need to try to decrypt all notes
- Project Tachyon delivers a *believable* scalability story
- compromises neither privacy nor self-custody
- UX challenge: wallets need to adopt out-of-band payments

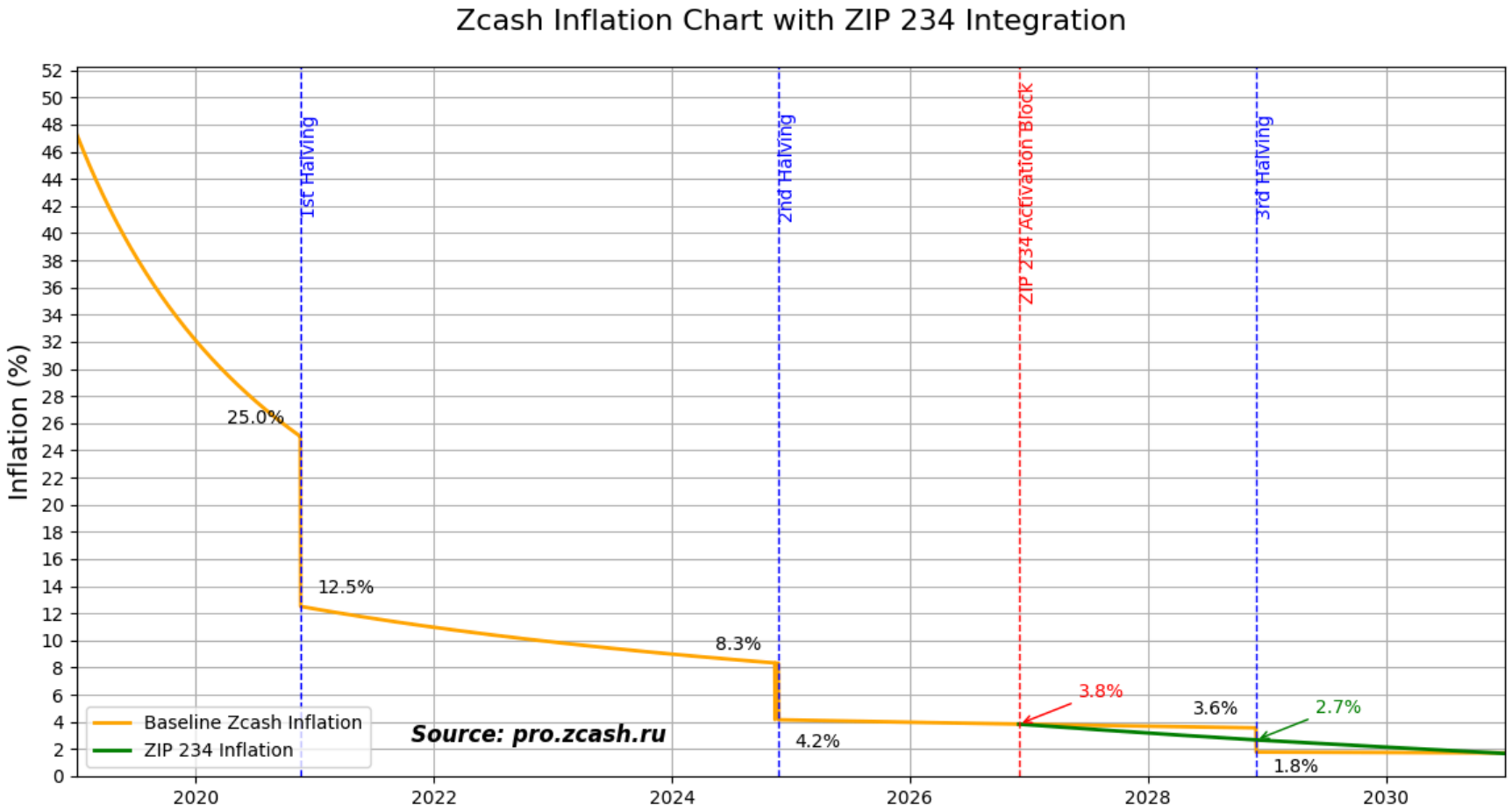
More details: seanbowe.com/blog

Zcash investing

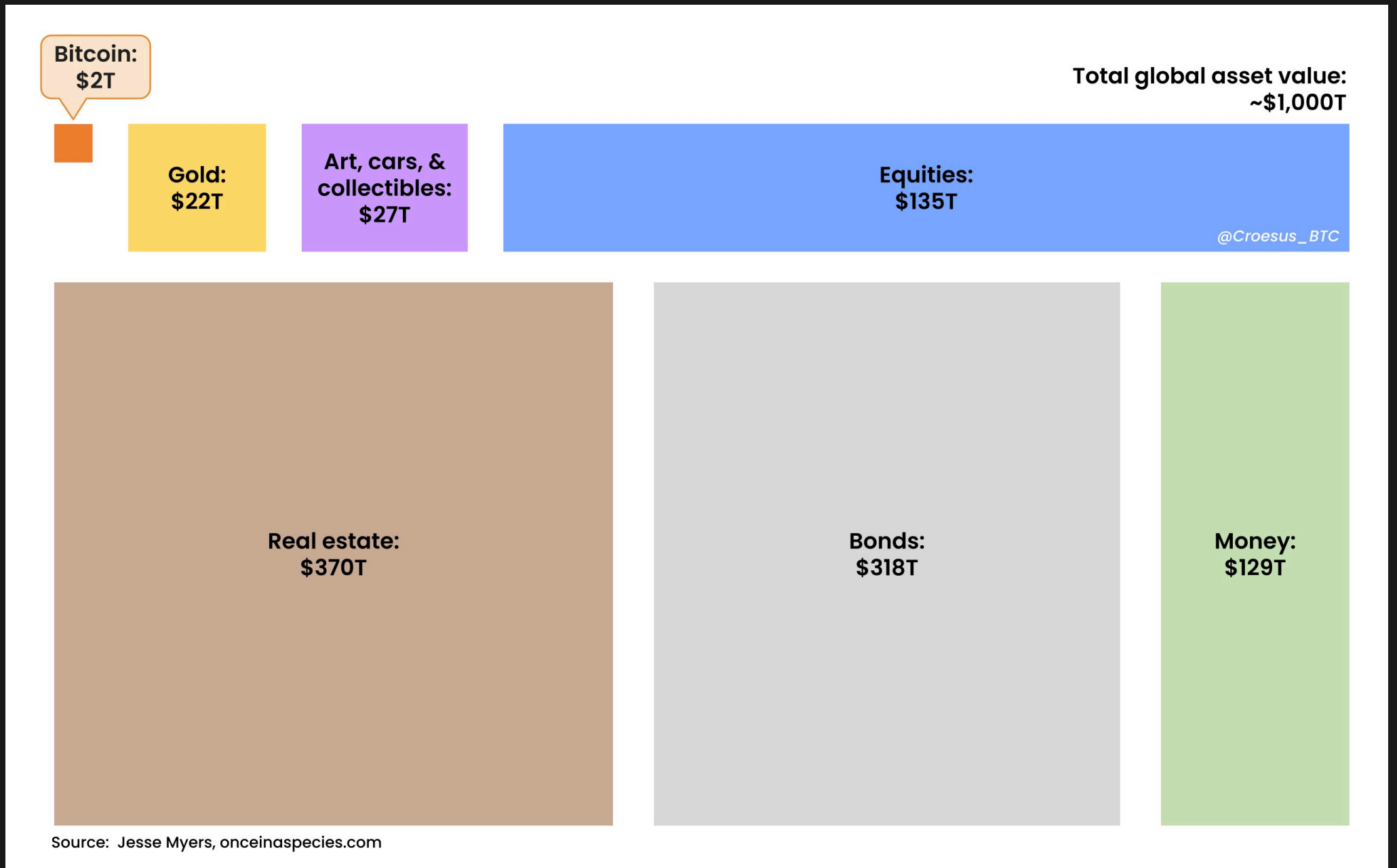
For something to work as money, in the “competition of monies”, it has to work as an investment.


Price
Market Cap
TradingView
24H
7D
1M
3M
1Y
Max
LOG
$3.5K
$3K
$2.5K
$2K
$1.5K
$1K
$500.00
$0
coingecko
6
Jul '17
Jul '18
Jul '19
Jul '20
Jul '21
Jul '22
Jul '23
Jul '24
Jul '25

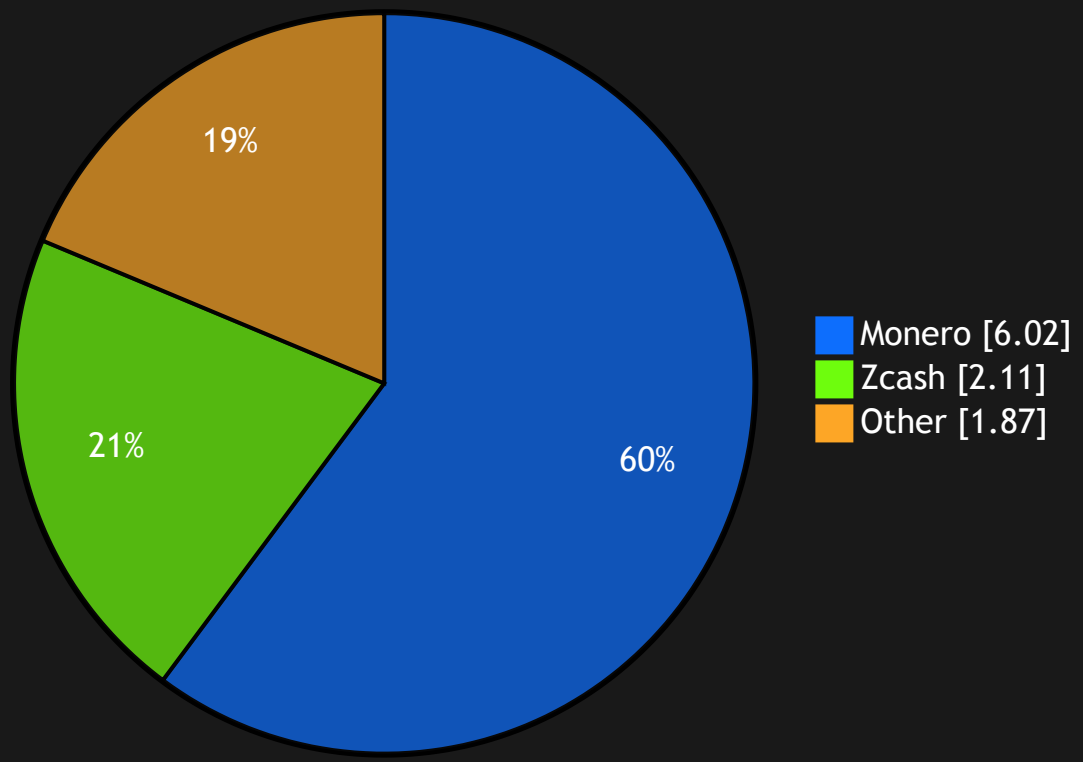
@thefrankbraun



github.com/ruzcash/ZIP234-Inflation-Visualizer

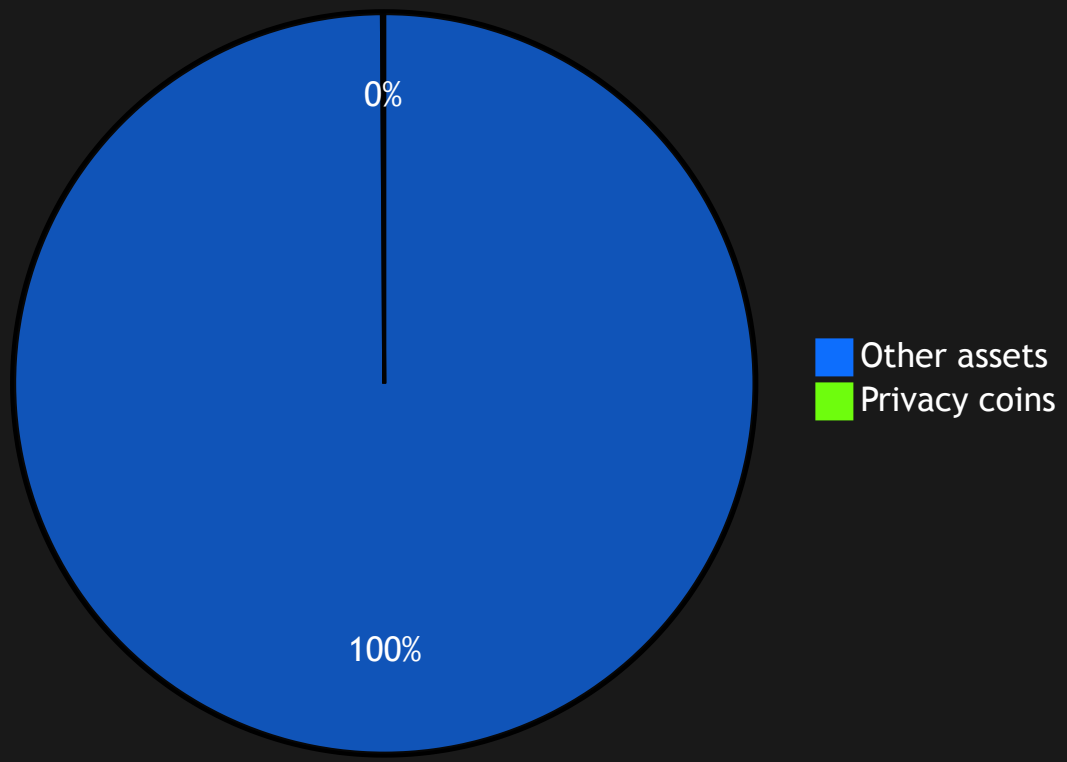

Bitcoin:
$2T
Total global asset value:
~$1,000T
Gold:
$22T
Art, cars, &
collectibles:
$27T
Equities:
$135T
@Croesus_BTC
Real estate:
$370T
Bonds:
$318T
Money:
$129T
Source: Jesse Myers, onceinaspecies.com

market cap of all privacy coins is $10B



0.5% of Bitcoin’s market cap…

offshore wealth is at least $10T



MC of all privacy coins is less than 0.1% of offshore wealth…

alpha?

- total global assets (TGA) value: $1,000T
- market cap of gold: $22T (2.2% of TGA)
- market cap of Bitcoin: $2T (~10% of gold, 0.2% of TGA)
- undeclared offshore wealth: $10T+ (1%+ of TGA)
- privacy coins: $10B (<0.1% of offshore wealth, 0.5% of Bitcoin)
- Zcash: ~$2.2B (21% of privacy coins, 0.02% offshore wealth)

global environment

- more surveillance (digital IDs, age verification, etc.)
- more reporting requirements
- higher taxes (“tax the rich”)
- more mobility (“millionaire migration”)

questions:

- % of offshore wealth relative to TGA: up or down?
- % of privacy coins relative to offshore wealth: up or down?

Zcash's position

- Zcash has best in class privacy
- Zcash less "shady" than Monero
- Zashi has best in class UX
- Zashi has deep integration into crypto ecosystem (no KYC)

questions:

- % of privacy coins relative to Bitcoin: up or down?
- % of Zcash market cap relative to privacy coins: up or down?

Zcash investment thesis in a nutshell

Using Zcash as a mixer doesn't work — transactions going in and out can be correlated by time and value.

The only way to break this link is to use it as a store of value.

If the market demands more financial privacy and understands this dynamic, value will accrue to Zcash.

$\Longrightarrow$ ZEC is a very interesting privacy play (mid- to long-term)

More details: frankbraun.org/zecbag

too early to tell?

2025-10-04 (compared to 2025-07-16):

- BTC: 3.00% (122408.15 USD)
- XMR: -3.17% (324.10 USD)
- ZEC: 200.95% (133.11 USD)

@thefrankbraun

	#	Coin		Price	1h	24h	▾ 7d	24h Volume	Market Cap	Last 7 Days
☆	70	Zcash ZEC	Buy	$134.99	▲ 1.5%	▼ 8.0%	▲ 142.0%	$567,979,580	$2,216,581,583	
☆	65	Pump.fun PUMP		$0.007011	▲ 2.6%	▼ 0.4%	▲ 40.0%	$579,259,931	$2,482,637,575	
☆	48	Aptos APT	Buy	$5.35	▼ 0.4%	▲ 4.5%	▲ 30.6%	$981,269,779	$3,777,414,883	
☆	41	OKB OKB	Buy	$231.88	▼ 1.2%	▲ 21.2%	▲ 21.9%	$547,817,778	$4,845,099,234	
☆	5	BNB BNB	Buy	$1,159.43	▼ 0.2%	▲ 4.4%	▲ 19.1%	$4,481,415,807	$161,416,108,983	
☆	53	Story IP		$9.83	▼ 1.3%	▲ 3.0%	▲ 19.1%	$128,282,539	$3,081,565,910	
☆	31	Cronos CRO	Buy	$0.2147	▲ 0.7%	▲ 1.1%	▲ 14.5%	$48,816,441	$7,488,552,888	
☆	26	Litecoin LTC	Buy	$118.58	▲ 0.1%	▲ 1.4%	▲ 14.4%	$984,294,079	$9,056,068,701	
☆	57	Binance Staked SOL BNSOL		$246.48	▲ 0.1%	▼ 0.6%	▲ 14.1%	$5,233,251	$2,809,431,733	
☆	51	Jito Staked SOL JITOSOL		$283.19	▲ 0.0%	▼ 0.8%	▲ 14.0%	$24,071,370	$3,498,620,681	

Conclusion

The future of money is private.

the future of money is private

> “This is a very interesting topic. If a solution was found, a much better, easier, more convenient implementation of Bitcoin would be possible.”

(Satoshi)

- a solution *was* found (and implemented in Zcash)
- ⇒ *unstoppable private money*
- money is a technology — technology evolves

Zcash 2.0

- Zcash has best in class privacy
- Zashi has best in class UX and integrations
- ZEC is a very interesting privacy play

Zcash: common misconceptions

1. ~~had premine~~
2. ~~contains inflation bug~~
3. ~~requires trusted setup~~
4. ~~bad UX / not practical~~
5. ~~shielded pools not used~~
6. ~~centralized ecosystem~~
7. ~~bad investment~~

Zcash is unstoppable private money

1. unstoppable ✅
    - decentralized ⬆️
    - censorship resistant ✅
    - cannot be switched off ⬆️
2. private ✅
    - sender & receiver anonymity ✅
    - hidden amounts ✅
    - no metadata leakage ⬆️
3. money ✅
    - has money properties ✅
    - integrated & exchangeable ⬆️
    - number go up (NgU) tech ⬆️

thank you!

@thefrankbraun