# Economic Applications of Cryptography

## Past, Present, and Future of Blockchain Technology and the Cryptocurrency Asset Class

Quantitative & Computational Finance Summer Bootcamp

Joseph Hall

Georgia Institute of Technology

August 19, 2026

josephphall.com

# Roadmap

# Roadmap

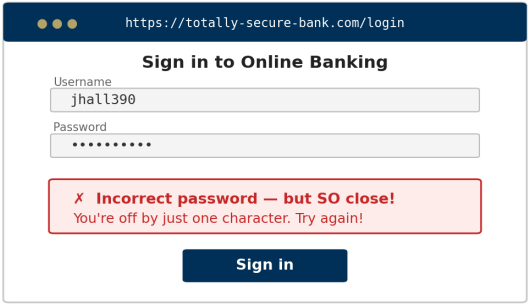
# Hash Functions

- A **hash function** takes some input string, and "chaotically" spits out an output string. Demo
- Servers (to which you log in) store hashes, not passwords!

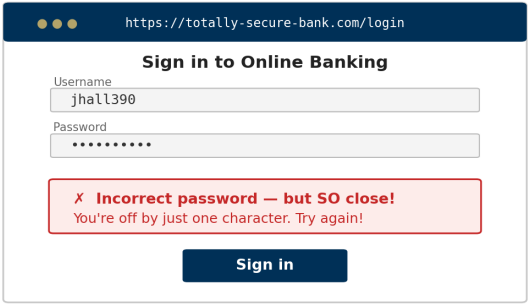
# Hash Functions

- A **hash function** takes some input string, and "chaotically" spits out an output string. Demo
- Servers (to which you log in) store hashes, not passwords!
- "Chaotic" means deterministic but unpredictable. The hash of a number never changes, yet knowing the hash of $N$ reveals nothing about the hash of $N + 1$.
  - **One-way**. You can calculate outcomes but cannot back out initial conditions
  - **Collision resistant**. So many outcomes are possible that two initial conditions rarely produce the same one (a "collision")

# Pop Quiz. Why Is This a Red Flag?



# Pop Quiz. Why Is This a Red Flag?




If the server can tell you are close, it is comparing your guess to your actual password – stored in plain text. A server storing only $H(\text{password})$ cannot know you were off by one character: the hash of $N$ reveals nothing about the hash of $N \pm 1$.

# Hash Functions

Hash functions are the basis for **Proof of Work**

- By publishing $y = H(x)$, anyone can check that they know the real $x$ without $x$ ever becoming public information

# Hash Functions

Hash functions are the basis for **Proof of Work**

- By publishing $y = H(x)$, anyone can check that they know the real $x$ without $x$ ever becoming public information
  - Easy to compute $H(x)$ given $H(\cdot)$ and $x$

# Hash Functions

Hash functions are the basis for **Proof of Work**

- By publishing $y = H(x)$, anyone can check that they know the real $x$ without $x$ ever becoming public information
  - Easy to compute $H(x)$ given $H(\cdot)$ and $x$
  - If someone changes $x$ to $\tilde{x}$, even by one letter, $H(\tilde{x})$ will be very different!
  - Used in checksums for file downloading
- The application we care about is **mining and proof-of-work**
  - No way to discover $x$ given $H(x)$ beside **brute force**!
  - The Secure Hash Algorithm 1 ("**SHA1**") takes between $2^{63}$ - $2^{80}$ evaluations to find a collision ($x, y$ such that $H(x) = H(y)$) (depending on how clever you are)
  - Bitcoins are mined by brute-forcing hashes to find $x$s that produce $H(x)$ with leading zeroes.

# Digital Signature Schemes

The requirements are

- JPH has a public key everyone knows
- JPH has a private key only JPH knows
  - **Non-invertability** means the public key doesn't reveal the private key

# Digital Signature Schemes

The requirements are

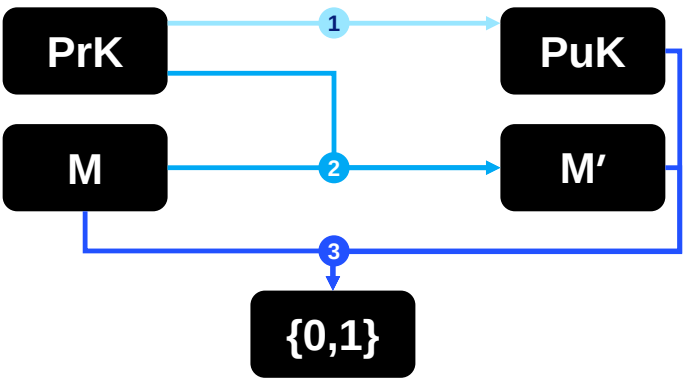
- JPH has a public key everyone knows
- JPH has a private key only JPH knows
  - **Non-invertability** means the public key doesn't reveal the private key
- JPH can "sign" messages, using the private key to alter the message in a way that proves JPH created his public key
- Public key allows **verification**, but not **signature production**

# Digital Signature Schemes

The requirements are

- JPH has a public key everyone knows
- JPH has a private key only JPH knows
  - **Non-invertability** means the public key doesn't reveal the private key
- JPH can "sign" messages, using the private key to alter the message in a way that proves JPH created his public key
- Public key allows **verification**, but not **signature production**
  - Using the public key, anyone can verify that JPH used his private key to sign the message
  - But, using the public key, can't generate new valid signatures

# Digital Signature Schemes, Visually



# Clock Arithmetic Is a One-Way Street

"mod $p$" means wrap around a clock of size $p$. On a 12-hour clock, $9 + 4 = 1$.

# Clock Arithmetic Is a One-Way Street

"mod $p$" means wrap around a clock of size $p$. On a 12-hour clock, $9 + 4 = 1$.

- Do it with powers, on a 17-hour clock ...

| | | | | | | |
|---|---|---|---|---|---|---|
| $3^1, 3^2, 3^3, 3^4, 3^5$ | = | 3, | 9, | 27, | 81, 243 |
| same, mod 17 | = | 3, | 9, | **10**, | **13**, **5** |

# Clock Arithmetic Is a One-Way Street

"mod $p$" means wrap around a clock of size $p$. On a 12-hour clock, $9 + 4 = 1$.

- Do it with powers, on a 17-hour clock …

| | | | | | | |
|---|---|---|---|---|---|---|
| $3^1, 3^2, 3^3, 3^4, 3^5$ | = | 3, | 9, | 27, | 81, 243 |
| same, mod 17 | = | 3, | 9, | **10**, | **13**, **5** |

- Without the clock, powers grow in an obvious pattern – easy to reverse. With the clock, they jump around like random numbers.
- One color rule holds for everything that follows. **Red** = private; **blue** = public.
- Forward is easy. Computing $3^d \bmod 17$ from $d$ is fast, even for enormous $d$.
- Backward is hopeless. Asked "which $d$ gave me 5?", you can do no better than trying $d$'s one by one. On a 600-digit clock, that outlasts the universe.
- This is the **discrete logarithm problem** – the one-way street everything below drives on.

# ElGamal, Start to Finish

- **Setup**: everyone agrees on a clock size $p$ and base $\alpha$. You pick a secret number $d$ and publish $\beta = \alpha^d \bmod p$. Extracting $d$ from $\beta$ is the discrete log problem, so it is infeasible.

# ElGamal, Start to Finish

- **Setup**: everyone agrees on a clock size $p$ and base $\alpha$. You pick a secret number $d$ and publish $\beta = \alpha^d \bmod p$. Extracting $d$ from $\beta$ is the discrete log problem, so it is infeasible.
- **Sign** a number $x$: draw a fresh random $k$ and publish $r = \alpha^k$; then solve $x = d \cdot r + k \cdot s$ for $s$ – the one unknown left – and publish it. Only someone who knows $d$ can solve it.

# ElGamal, Start to Finish

- **Setup**: everyone agrees on a clock size $p$ and base $\alpha$. You pick a secret number $d$ and publish $\beta = \alpha^d \bmod p$. Extracting $d$ from $\beta$ is the discrete log problem, so it is infeasible.
- **Sign** a number $x$: draw a fresh random $k$ and publish $r = \alpha^k$; then solve $x = d \cdot r + k \cdot s$ for $s$ – the one unknown left – and publish it. Only someone who knows $d$ can solve it.
- **Verify**: anyone checks, using only blue quantities,

$$\beta^r \cdot r^s \stackrel{?}{=} \alpha^x \pmod{p}$$

- **Why it balances**: $\beta^r = \alpha^{dr}$, and the rule $\alpha^a \alpha^b = \alpha^{a+b}$ still holds on the clock, so the left side is $\alpha^{dr+ks} = \alpha^x$.

# ElGamal, Start to Finish

- **Setup**: everyone agrees on a clock size $p$ and base $\alpha$. You pick a secret number $d$ and publish $\beta = \alpha^d \bmod p$. Extracting $d$ from $\beta$ is the discrete log problem, so it is infeasible.
- **Sign** a number $x$: draw a fresh random $k$ and publish $r = \alpha^k$; then solve $x = d \cdot r + k \cdot s$ for $s$ – the one unknown left – and publish it. Only someone who knows $d$ can solve it.
- **Verify**: anyone checks, using only blue quantities,

$$\beta^r \cdot r^s \stackrel{?}{=} \alpha^x \pmod{p}$$

- **Why it balances**: $\beta^r = \alpha^{dr}$, and the rule $\alpha^a \alpha^b = \alpha^{a+b}$ still holds on the clock, so the left side is $\alpha^{dr+ks} = \alpha^x$.
- **Why it's secure**: forging $(r, s)$ for a new $x$ requires knowing $d$ – which is locked behind the one-way street.

# Pop Quiz. What Does This Have to Do With Cryptography?

# This Wall Helps Encrypt the Internet

- This is the lobby of **Cloudflare** in San Francisco

# This Wall Helps Encrypt the Internet

- This is the lobby of **Cloudflare** in San Francisco
- Every signature needs a fresh, unpredictable $k$ – and computers are terrible at being unpredictable

# This Wall Helps Encrypt the Internet

- This is the lobby of **Cloudflare** in San Francisco
- Every signature needs a fresh, unpredictable $k$ – and computers are terrible at being unpredictable
- Lava flow is **chaotic**, deterministic but unpredictable – the same property we prize in hash functions
- A camera films the wall; the pixels help seed the encryption behind https connections at Cloudflare, which fronts **24.7% of all websites** (W3Techs, Aug 2026) – one in four encrypted connections traces randomness to this wall

# From ElGamal to Digital Signatures

- Never reuse $k$. Each signature is one equation with two secrets, $d$ and $k$ – safely unsolvable. Reuse hands the world two equations in two unknowns, and it solves for $d$: Sony's PlayStation 3 signing key fell exactly this way in 2010.

# From ElGamal to Digital Signatures

- Never reuse $k$. Each signature is one equation with two secrets, $d$ and $k$ – safely unsolvable. Reuse hands the world two equations in two unknowns, and it solves for $d$: Sony's PlayStation 3 signing key fell exactly this way in 2010.
- $\beta$ is the public key everyone knows; $d$ is the private key only you know; $(r, s)$ is a signature anyone can verify from blue quantities alone, but only $d$ can produce.

# From ElGamal to Digital Signatures

- Never reuse $k$. Each signature is one equation with two secrets, $d$ and $k$ – safely unsolvable. Reuse hands the world two equations in two unknowns, and it solves for $d$: Sony's PlayStation 3 signing key fell exactly this way in 2010.
- $\beta$ is the public key everyone knows; $d$ is the private key only you know; $(r, s)$ is a signature anyone can verify from blue quantities alone, but only $d$ can produce.
- ElGamal ("The Beauty" in Arabic) fits in ten lines of Python – see the worked code – and ECE 6280 goes deeper. Bitcoin uses a cousin (ECDSA) built on the same one-way street.

The treatment of ElGamal on these slides is adapted from Anthony Lee Zhang's course notes.

# Uses of Merkle Trees

A Merkle Tree is a way of efficiently storing the required information to ensure that a set of documents or messages have not been tampered with or corrupted.

# Uses of Merkle Trees

A Merkle Tree is a way of efficiently storing the required information to ensure that a set of documents or messages have not been tampered with or corrupted.

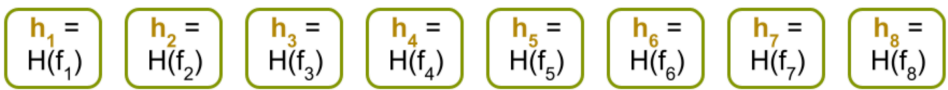
Merkle Trees are used in many applications to solve problems such as these.

- Maintaining integrity of files stored on Dropbox.com, or *file outsourcing*
- Proving a transaction between Alice and Bob occurred, or *set membership*
- Transmitting files over unreliable channels, or *anti-entropy*

# Construction of Merkle Trees

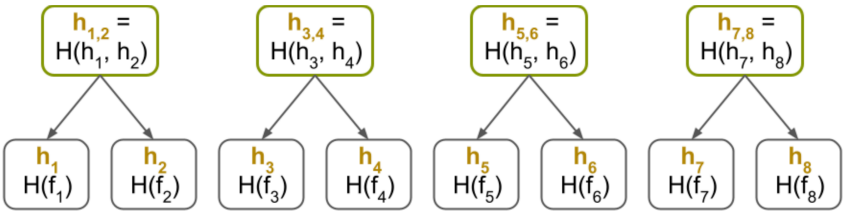
Start with, say, 8 files $(f_1 ... f_8)$, and a hash function $H(.)$

Start by hashing each file, $H(f_i)$



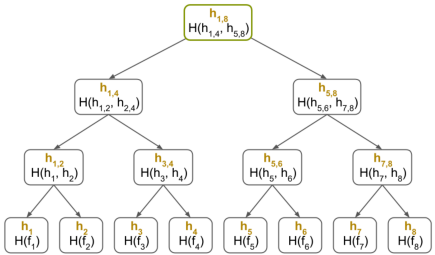
# Construction of Merkle Trees

Next, hash each pair of hashes



# Construction of Merkle Trees

Repeat until one hash remains — the **Merkle Root** $h_{1,8}$




This building block predates Bitcoin by three decades.

# Ralph Merkle

Invented the Merkle tree in 1979 — and was later a **Georgia Tech professor of computing**.
Photo: Wikimedia Commons.

# Verification with Merkle Trees

Upload your files $(f_1 ... f_8)$ **and** your Merkle Tree to Dropbox, storing only the **Merkle Root** $h_{1,8}$ locally.

# Verification with Merkle Trees

Upload your files $(f_1 ... f_8)$ **and** your Merkle Tree to Dropbox, storing only the **Merkle Root** $h_{1,8}$ locally.

Later, ask for the file you want, say $f_3$, but make sure to also ask for the **Merkle Proof**: the hashes needed to compute $h_{1,8}$ from the desired **Merkle Leaf** $(f_3)$

# Verification with Merkle Trees

Upload your files $(f_1 ... f_8)$ **and** your Merkle Tree to Dropbox, storing only the **Merkle Root** $h_{1,8}$ locally.

Later, ask for the file you want, say $f_3$, but make sure to also ask for the **Merkle Proof**: the hashes needed to compute $h_{1,8}$ from the desired **Merkle Leaf** $(f_3)$

The proof needs only **one hash per level**, so it scales with $\log_2 n$

- 8 files $\rightarrow$ 3 hashes
- 1,024 files $\rightarrow$ 10 hashes
- one billion files $\rightarrow$ 30 hashes ($\sim$1 KB)

# Advantages of Merkle Trees

**Question**: Why not just store the hash of every file? Wouldn't that be simpler?

# Advantages of Merkle Trees

**Question**: Why not just store the hash of every file? Wouldn't that be simpler?
**Answer**: That would require storing 1 hash per document, so your local storage would scale linearly with number of files. The Merkle Tree requires storing **only** the Merkle Root, a single hash, **for any number of files**!

# Advantages of Merkle Trees

**Question**: Why not just store the hash of every file? Wouldn't that be simpler?
**Answer**: That would require storing 1 hash per document, so your local storage would scale linearly with number of files. The Merkle Tree requires storing **only** the Merkle Root, a single hash, **for any number of files**!

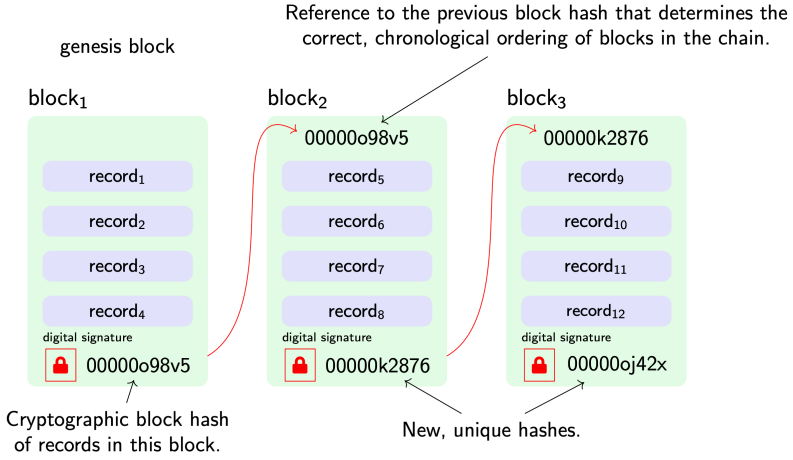
**Question**: The server stores ($h_4$, $h_{1,2}$, and $h_{5,8}$) for you. Can't the server modify these to make the Merkle Proof appear true, even if $f_3$ is changed to $\tilde{f}_3$?
**Answer**: The cryptographic property of **Non-Invertability** ensures that it is prohibitively difficult to create a false Merkle proof.

For other (analogous) uses of Merkle Trees including Transaction Verification and Transmitting files robustly over error-prone communication channels, see Tomescu (2020)

# Roadmap

# What is a Blockchain?

A **Blockchain** is a list of records that are linked together by hash functions



# A Centralized Blockchain

Say that I, JPH, own and operate a private server which records a Blockchain. I don't know the users' private keys, but I control everything that is written on the blockchain. What can I do?

# A Centralized Blockchain

Say that I, JPH, own and operate a private server which records a Blockchain. I don't know the users' private keys, but I control everything that is written on the blockchain. What can I do?

- Create false messages?

# A Centralized Blockchain

Say that I, JPH, own and operate a private server which records a Blockchain. I don't know the users' private keys, but I control everything that is written on the blockchain. What can I do?

- Create false messages?
  - No – I don't have the private keys to create messages that can be verified as true.
- Cancel or revert messages?
  - Yes – I can refuse to include a new block or roll back the blockchain to a previous state.
- Selectively cancel three messages ago, but not the last two?
  - No – the hashes of the last two messages would be wrong if the middle hash is missing.

# A Centralized Blockchain

Centralized Blockchains are in fact widely-used.

- Binance Smart Chain
- Coinbase Base
- Ripple XRP
- "Permissioned" or "Private" Blockchains use **Proof of Authority**, where the admin's public key *per se* is hard-coded into the protocol.

# A Centralized Blockchain

Centralized Blockchains are in fact widely-used.

- Binance Smart Chain
- Coinbase Base
- Ripple XRP
- "Permissioned" or "Private" Blockchains use **Proof of Authority**, where the admin's public key *per se* is hard-coded into the protocol.

When are these better than just a spreadsheet?

# A Centralized Blockchain

Centralized Blockchains are in fact widely-used.

- Binance Smart Chain
- Coinbase Base
- Ripple XRP
- "Permissioned" or "Private" Blockchains use **Proof of Authority**, where the admin's public key *per se* is hard-coded into the protocol.

When are these better than just a spreadsheet?

- Often they aren't. Chase, VISA, Zelle, and Federal Reserves are all just spreadsheets at the end of the day
- A Centralized Blockchain adds one extra level of security – a transaction history that can't be arbitrarily tampered with, only censored or rewound
- That's still a lot of power in the admin's hands!

# A Decentralized Blockchain

**Can we take away even more power from the admin – agree on a shared history without trusting anybody?**

# A Decentralized Blockchain

**Can we take away even more power from the admin – agree on a shared history without trusting anybody?**

- A natural, "democratic" rule would be to have multiple admins taking turns adding transactions to the chain

# A Decentralized Blockchain

**Can we take away even more power from the admin – agree on a shared history without trusting anybody?**

- A natural, "democratic" rule would be to have multiple admins taking turns adding transactions to the chain
- How do we prevent one admin from just pretending to be multiple admins?
- Needs to be some "cost"/"barrier" to becoming an admin
- Bitcoin solves this through **proof of work**
- Ethereum solves this through **proof of stake**

# Hash Puzzles

- The amount of computational power in the world is finite!
- Let's try to find a number whose SHA256 hash has a 0 at the beginning...

# Hash Puzzles

- The amount of computational power in the world is finite!
- Let's try to find a number whose SHA256 hash has a 0 at the beginning...
- Why is this a nice puzzle? Like a PhD
  1. Hard to do
  2. Proves that you did something hard to do

# Hash Puzzles

- The amount of computational power in the world is finite!
- Let's try to find a number whose SHA256 hash has a 0 at the beginning...
- Why is this a nice puzzle? Like a PhD
  1. Hard to do
  2. Proves that you did something hard to do
- With puzzle solution in hand, you become the admin!
- **Incentives**. Solving the puzzle earns you BTC, the block reward
- **Consensus**. Everyone works on the longest chain
  - Cooperating beats defecting to a chain of your own, because when compute is power you want to be on the side with the most compute

# Roadmap

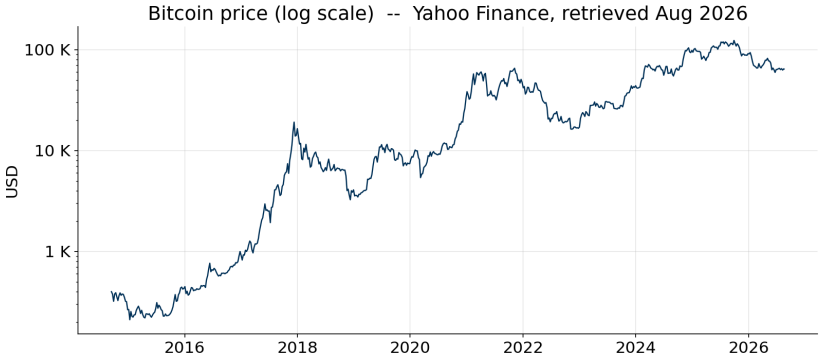
# Satoshi Nakamoto

- Started sending emails about Bitcoin August 2008
- The Bitcoin white paper and code appeared in October 2008
- The first block was mined on January 9!
  - "The Times 03/Jan/2009 Chancellor on brink of second bailout for banks"
- On May 22, 2010, Laszlo Hanyecz bought two Papa John's pizzas for 10,000 BTC, now worth $600mil USD!
- Quickly became popular among black markets, Silk Road...
  - Founder Ross Ulbricht was recently pardoned by Trump

# Prizes for a Starcraft Tournament in 2011

**Prizes:**
**1st Place: *$500***
**2nd Place: *$250***
**3rd Place: *$150***
**4th Place: *$100***
**5th-8th Place: *25 BitCoins***

# Bitcoin Prices




Yahoo Finance, retrieved Aug 2026 (chart is clickable – live version)

# Each BTC Block is a Merkle Tree of Transactions!

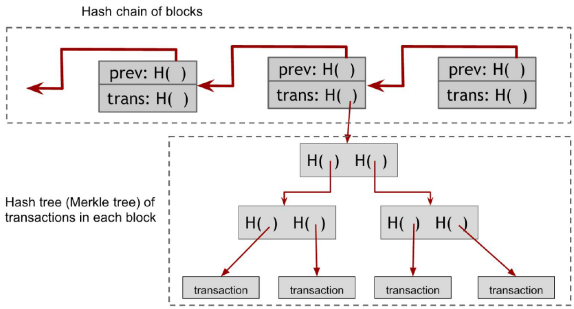



***Figure 3.8.*** The Bitcoin block chain contains two different hash structures. The first is a hash chain of blocks that links the different blocks to one another. The second is internal to each block and is a Merkle Tree of transactions within the blocks.

- Valid block headers' hashes start with a big number of 0's (mining puzzle)

NBFMG, fig. 3.8

# BTC mining

- Suppose mining a block pays 0.001 BTC
- Suppose mining block costs $60 in electricity
  - If BTC price $> \$60k$, everyone mines; blocks produced quickly
  - If BTC price $< \$60k$, nobody mines; tx's aren't included and the blockchain stops working!
- The fact that mining rate depends on BTC vs electricity price is not desirable...
- The fix is difficulty adjustment, which maintains a constant block production rate

# BTC Difficulty Adjustment

- Blocks should be produced every 10 minutes
- Every 2016 blocks (approx 14 days), Bitcoin considers average block production rate, and...
  - Increases/decreases hash problem difficulty, if block production is too fast/slow
- What determines how fast blocks are produced, fixing hash rate?

# BTC Difficulty Adjustment

- Blocks should be produced every 10 minutes
- Every 2016 blocks (approx 14 days), Bitcoin considers average block production rate, and...
  - Increases/decreases hash problem difficulty, if block production is too fast/slow
- What determines how fast blocks are produced, fixing hash rate?
  - How many people (that is, how much electricity) is devoted to mining

# BTC Difficulty Adjustment

- Blocks should be produced every 10 minutes
- Every 2016 blocks (approx 14 days), Bitcoin considers average block production rate, and...
  - Increases/decreases hash problem difficulty, if block production is too fast/slow
- What determines how fast blocks are produced, fixing hash rate?
  - How many people (that is, how much electricity) is devoted to mining
- What determines how many people mine?
  - How profitable mining is, that is, how high BTC price is, vs electricity price

# The Money Pot Game

- You have two options.
  1. Get $1 for sure
  2. Fight for a $10 pot, which is equally divided between everyone who picks this option

# The Money Pot Game

- You have two options.
  1. Get $1 for sure
  2. Fight for a $10 pot, which is equally divided between everyone who picks this option
- Which do you pick?

# The Money Pot Game

- What is going on?
  - Everyone wants the money pot
  - But the more people take the money pot, the less money there is for everyone
  - In "Nash equilibrium", the money pot becomes no better than the "outside option"

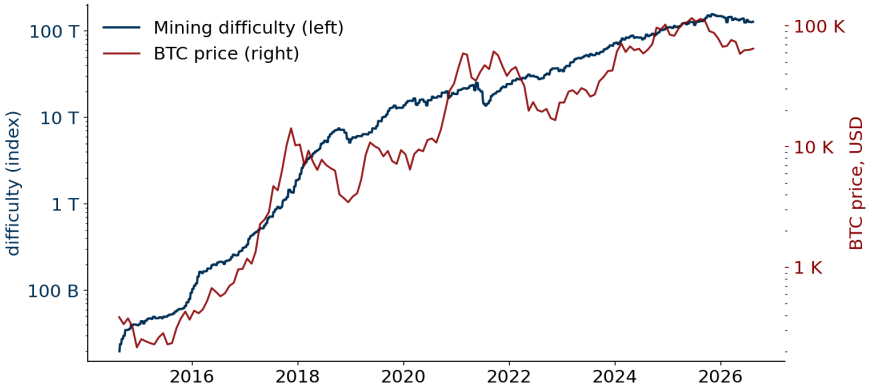
# The Money Pot Game

- What is going on?
  - Everyone wants the money pot
  - But the more people take the money pot, the less money there is for everyone
  - In "Nash equilibrium", the money pot becomes no better than the "outside option"
- What's the equilibrium condition in similar settings?
  - Firms competing for profits?

# The Money Pot Game

- What is going on?
  - Everyone wants the money pot
  - But the more people take the money pot, the less money there is for everyone
  - In "Nash equilibrium", the money pot becomes no better than the "outside option"
- What's the equilibrium condition in similar settings?
  - Firms competing for profits?
  - Going to the beach on a sunny day?
  - Getting a table for Brunch on Sunday at 12pm?
- "Equilibrium" behavior is easy to predict in such settings
  - In equilibrium, the "good" deal is so crowded that it becomes just as bad as the "bad" deal
- Game theory calls these congestion games, or wars of attrition, or tragedy of the commons

# Difficulty vs BTC price




Difficulty is an index, where 1 = the first block (January 2009) and today ∼127 trillion. Blockchain.com, Aug 2026 (chart is clickable – live version)

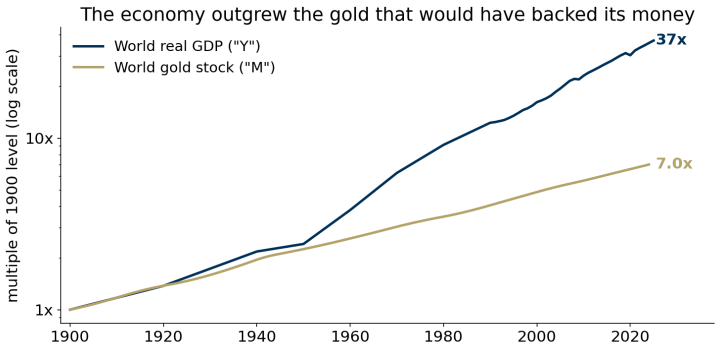
# BTC Halving

- Approximately every 4 years, issuance of BTC drops by half
- The last halving was April 2024, leaving 3.125 BTC per block
- Does this affect block production rate?
  - No! Difficulty adjustment always ensure a constant block production rate.

# BTC Halving

- Approximately every 4 years, issuance of BTC drops by half
- The last halving was April 2024, leaving 3.125 BTC per block
- Does this affect block production rate?
  - No! Difficulty adjustment always ensure a constant block production rate.
- Also implies there will only ever be 21 million BTC in existence!
  - By approximately 2140, the block reward will drop to less than the smallest unit of bitcoin ($1/10^8$) and become equal to zero.
  - Difficulty adjustment ensures that block production rate is approximately constant

# Bitcoin Is Digital Gold – Which Is the Problem




A hard-capped money supply in an exponentially growing economy forces **deflation** – gold's fatal flaw as a currency. Bitcoin's 21M cap is stricter still – past 2140, its supply stops growing entirely. A plausible store of value; a poor medium of exchange and unit of account.

# Two Meanings of "Inflation"

- Crypto engineers use "inflation" for growth in the **money supply** – Ethereum's issuance schedule, Bitcoin's halvings

# Two Meanings of "Inflation"

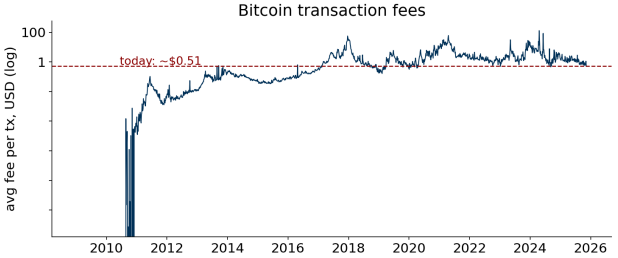
- Crypto engineers use "inflation" for growth in the **money supply** – Ethereum's issuance schedule, Bitcoin's halvings
- Economists use it for growth in the **price level**

# Two Meanings of "Inflation"

- Crypto engineers use "inflation" for growth in the **money supply** – Ethereum's issuance schedule, Bitcoin's halvings
- Economists use it for growth in the **price level**
- Zero supply inflation in a growing economy is not zero price inflation – it is **deflation** – which punishes borrowers and depresses investment, and with it, growth

# Transaction Fees

- Block rewards are not the only incentive – miners also collect transaction fees, quoted in Satoshis ($10^{-8}$ BTC) per byte; the **mempool** is the pool of transactions waiting to be included
- Fees are also Bitcoin's exit ramp from 2140. When the block reward halves to zero, **100% of miner revenue will be fees** – and maybe that's enough to keep the chain secure




Today an average transaction clears for ~$0.51. Explore it live at mempool.space

# Incentives

- A centralized authority can "censor", i.e. not include tx's
- Decentralization and competition "ensure" performance
  - If you don't include my tx, the next miner will
  - Even if the US bans US miners from including tx's, someone else will include them

# Further Reading on Mining Industry

- Galaxy digital 2023 and 2024
- Cool paper on mining pools

# Roadmap

# Smart Contracts

- A smart contract is three things.
  - A wallet, which can hold Ether (ETH),
  - Functions it can call when requested as determined by its code,
  - (optionally) a source of data to which it can read and write

# Smart Contracts

- A smart contract is three things.
  - A wallet, which can hold Ether (ETH),
  - Functions it can call when requested as determined by its code,
  - (optionally) a source of data to which it can read and write
- If you've heard of object oriented programming, smart contracts are a bundle of functions (code), data, as well as ETH balances

# Smart Contracts

- A smart contract is three things.
  - A wallet, which can hold Ether (ETH),
  - Functions it can call when requested as determined by its code,
  - (optionally) a source of data to which it can read and write
- If you've heard of object oriented programming, smart contracts are a bundle of functions (code), data, as well as ETH balances
- The most popular coding language which compiles Ethereum script code (a minimal Turing-complete language akin to assembly) is called **Solidity**

Deploying a smart contract or calling its functions requires a **gas fee** – ETH must be paid to the network to run the code.

# Smart Contracts Make Tokens

- An ETH address, "technically", only "holds" Ether ("ETH") natively – no other tokens!
- An ETH address can be assigned non-ETH tokens through smart contracts
- A smart contract can define tokens using the **ERC-20** standard
  - So-called because it was originally the 20th submission to "Ethereum Requests for Comments"

# Unlike BTC, ETH has native gas fees

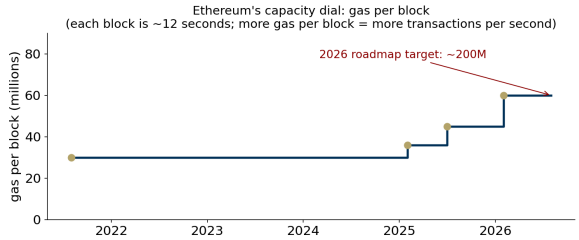
"In Bitcoin, there are no mandatory transaction fees. Transactions can optionally include fees which are paid to miners, and it is up to the miners to decide what fees they are willing to accept. In Bitcoin, such a mechanism is already imperfect...In Ethereum, because of its Turing-completeness, a purely voluntary fee system would be catastrophic. Instead, Ethereum will have a system of mandatory fees, including a transaction fee and six fees for contract computations."
-Ethereum Whitepaper, Vitalik Buterin (2014)

# Proof of Stake

- Originally, ETH mining proof-of-work, similar to BTC
- On Sept 15 2022, ETH switched to proof of stake – called **"The Merge"**
- Reduced energy consumption by **over 99%**!
- Users deposit ("stake") 32 ETH into a special smart contract
- Stakers randomly selected (prop. to stake) to propose new blocks
- If a staker is caught trying to do "bad things" (e.g. propose 2 inconsistent blocks), they are "slashed" – staked ETH is removed by smart contract
- Most newer blockchains (SOL, LUNA, AVAX) use proof-of-stake

# Capacity of Ethereum

- Ethereum L1 processed ∼15 transactions per second (tps) for years; staged gas-limit raises have pushed it to ∼25 tps today




- This is pretty bad! Visa is 24,000 tps!
  - Every ETH staker has to run every transaction, and keep a copy of all data!
- Decentralization very expensive, in terms of computational efficiency!
- Proof-of-stake doesn't help throughput
  - Rollups do, which we will cover

# Roadmap

# Rollups or "L2's"

ETH is getting expensive! One set of solutions is rollups, also called L2's. The idea is this.

- Put our ETH, tokens, etc. in a "smart contract pot" (L2 bridge)
- People do transactions (smart contract, etc.) using funds in the pot, without doing anything on "main chain"
- Transactions are periodically batch settled

# Rollups or "L2's"

ETH is getting expensive! One set of solutions is rollups, also called L2's. The idea is this.

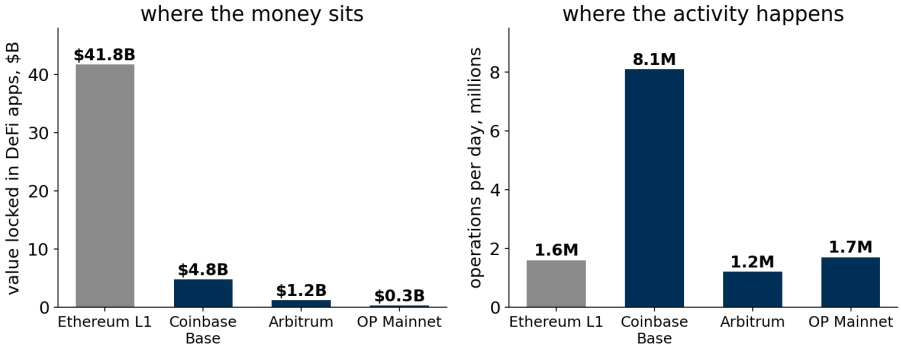
- Put our ETH, tokens, etc. in a "smart contract pot" (L2 bridge)
- People do transactions (smart contract, etc.) using funds in the pot, without doing anything on "main chain"
- Transactions are periodically batch settled
- Need to guarantee whatever happens on the rollup is exactly what would happen on ETH main chain! There are two methods

# Rollups or "L2's"

ETH is getting expensive! One set of solutions is rollups, also called L2's. The idea is this.

- Put our ETH, tokens, etc. in a "smart contract pot" (L2 bridge)
- People do transactions (smart contract, etc.) using funds in the pot, without doing anything on "main chain"
- Transactions are periodically batch settled
- Need to guarantee whatever happens on the rollup is exactly what would happen on ETH main chain! There are two methods
  - An **optimistic rollup** (Optimism, Arbitrum, Coinbase Base) lets anyone "challenge" L2 transactions, will (essentially) run on L1 if challenged
  - In a **ZK-rollup** (zkSync, StarkWare, Polygon), zero-knowledge cryptographic proofs ensure security, but at a high computing cost
- Optimistic rollups hold the larger market share; ZKs are growing

# L2s Today

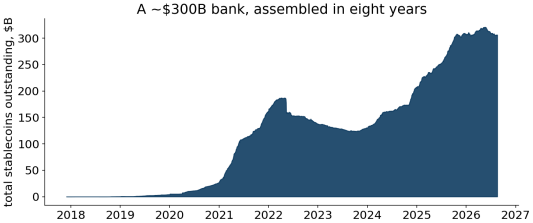



DefiLlama and L2BEAT APIs, Aug 2026; L1 activity approximate (Etherscan).

# Roadmap

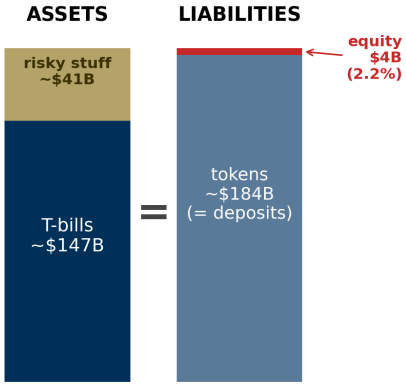
# What Is a Stablecoin?

- A token defined by its peg – a claim to a dollar, intended to always trade at a dollar
- So it is **not an asset class** – appreciation is ruled out by construction. It is a transaction technology for payments, savings, and smart-contract interoperability. (The cryptography is a mechanical design choice, **not** the source of value – the peg is.)
- To an economist, a stablecoin is nothing new. **It is a bank deposit** – but the issuer may or may not be a bank



# The Issuer Runs a Bank's Balance Sheet

- A pot of assets; tokens issued against it – the holder is an uninsured depositor
- Competition pushes for yield, meaning riskier collateral and thinner equity
- None of these economics will confuse anyone who knows leverage and macroprudential regulation, deposit insurance, or banking crises




*To scale: Tether, Q2 2026.*
*Risky assets = 10x the equity behind them.*

# And Bank-Like Liabilities Invite Bank-Like Runs

- A depositor who doubts the pot's value has one dominant move – redeem first

# And Bank-Like Liabilities Invite Bank-Like Runs

- A depositor who doubts the pot's value has one dominant move – redeem first
- That is a **bank run** – the same one that has stalked finance since the wildcat banking era

# And Bank-Like Liabilities Invite Bank-Like Runs

- A depositor who doubts the pot's value has one dominant move – redeem first
- That is a **bank run** – the same one that has stalked finance since the wildcat banking era
- We have already watched it happen. Terra/Luna (2022) collapsed in days; USDC broke its peg in the March 2023 SVB weekend before deposit insurance intervened
- Terra's $50B collapse in three days was a classic run led by large sophisticated holders (Liu, Makarov & Schoar, NBER 2023); stablecoins behave like uninsured money-market funds under stress (Anadu et al. 2023; Luck, "Historical Perspective on Stablecoins," 2025)

# The GENIUS Act

- The 2025 GENIUS Act gives US stablecoins a banking-style rulebook of licensed issuers, reserve requirements, and disclosure

# The GENIUS Act

- The 2025 GENIUS Act gives US stablecoins a banking-style rulebook of licensed issuers, reserve requirements, and disclosure
- One provision stands out. Issuers are **prohibited from paying interest** to holders

# The GENIUS Act

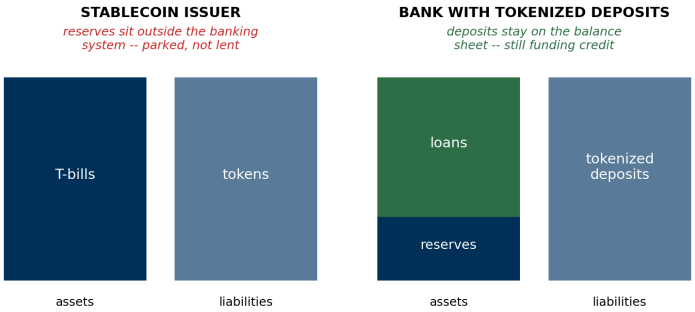
- The 2025 GENIUS Act gives US stablecoins a banking-style rulebook of licensed issuers, reserve requirements, and disclosure
- One provision stands out. Issuers are **prohibited from paying interest** to holders
- So the product is a bank deposit that pays no interest – but with extra interoperability, because smart contracts can natively hold and accept it
- Demystified this way, the payments scorecard coming in Part II should not surprise you – a zero-interest deposit competing against Treasuries, banks, and fast-payment rails has to win on convenience alone

# Stablecoins vs. Tokenized Deposits

- On the surface these are the same product – a dollar claim that lives on a blockchain. The difference is where the money sits

# Stablecoins vs. Tokenized Deposits

- On the surface these are the same product – a dollar claim that lives on a blockchain. The difference is where the money sits




A dollar that migrates from a bank deposit into a stablecoin stops funding loans. At scale, that is **bank disintermediation** – the policy fight underneath the stablecoin rulebook.

# Roadmap

# Part II. Where Does Crypto Actually Stand?

- Everything so far has been the technology – elegant, functional, mature

# Part II. Where Does Crypto Actually Stand?

- Everything so far has been the technology – elegant, functional, mature
- Now the harder question. How is crypto doing as an industry?

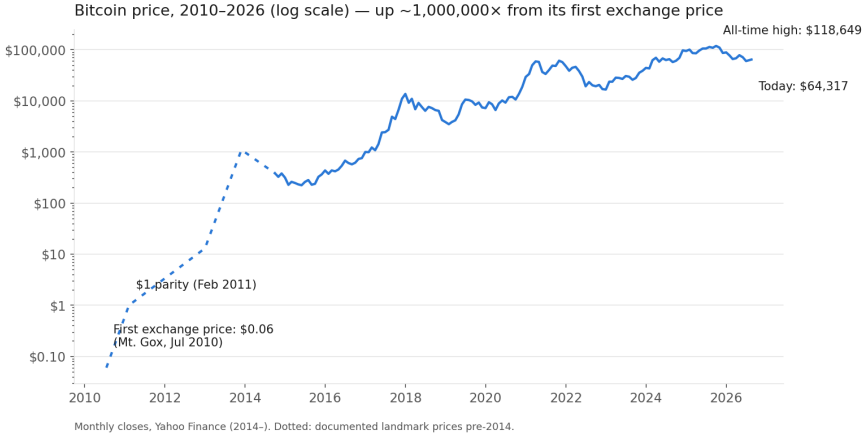
# Part II. Where Does Crypto Actually Stand?

- Everything so far has been the technology – elegant, functional, mature
- Now the harder question. How is crypto doing as an industry?
- My assessment:

**Crypto has failed – so far – to mature into a product development platform for finance and software.**

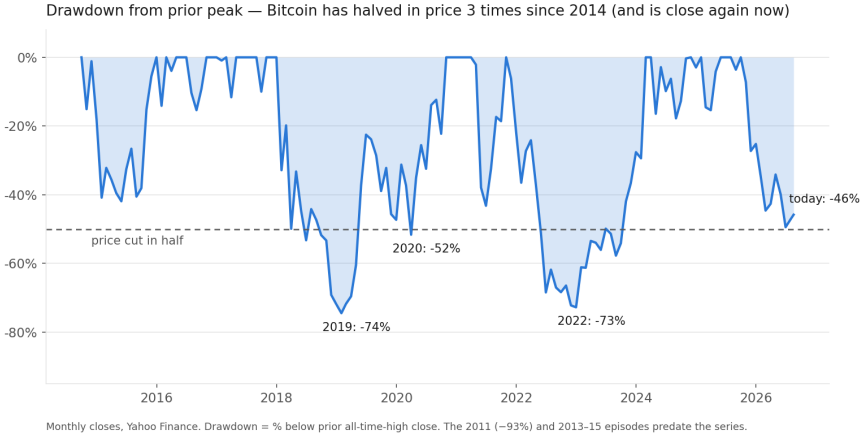
- The next 30 minutes cover the evidence, five structural reasons, and what is thriving instead

# First, the Asset Everyone Asks About



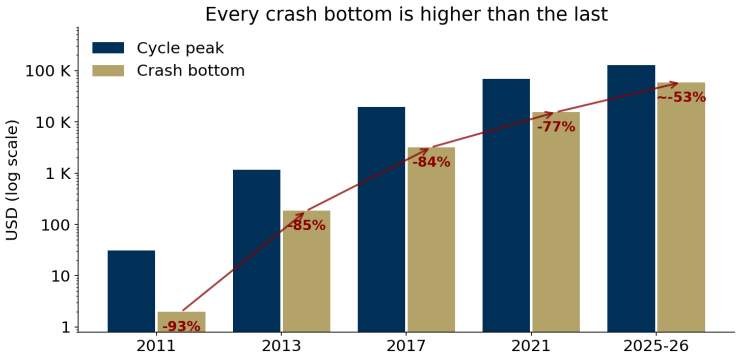

Both things are true at once. The greatest price appreciation of any asset in recorded history...

# ...and Traders' "Price Halving" Is a Regular Event



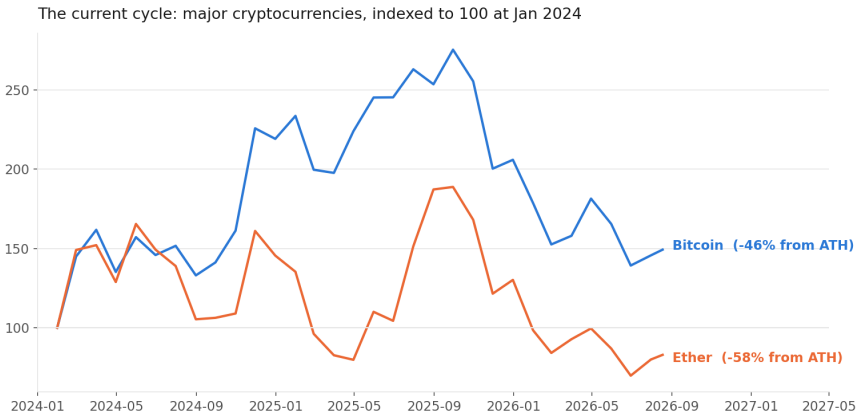

Roughly every 2–4 years, Bitcoin loses half its value. Any portfolio thesis must survive this.

# ...but Each Halving Happens at a Higher Floor



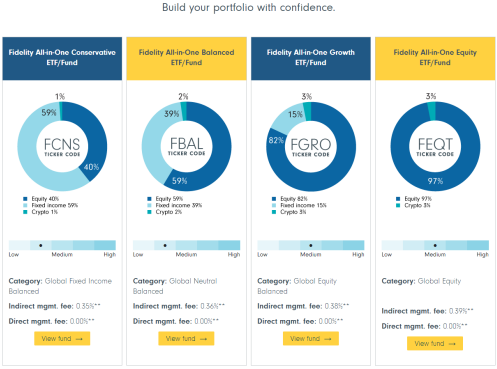

The floor rises and the drawdowns shrink – marked in red.

# The Current Cycle



# "Buy the Market"

The CAPM says buy the market – and BTC's market cap (∼$1.3T) is now roughly 2.5% of the S&P 500's ∼$55T




Fidelity Canada; market caps as of August 2026 (CoinGecko; S&P DJI).

# The "Market Cap" Illusion

**Market Capitalization** is just units outstanding times unit price

- Say everyone tried to sell their BTC tomorrow. Would they get that price for it?

# The "Market Cap" Illusion

**Market Capitalization** is just units outstanding times unit price

- Say everyone tried to sell their BTC tomorrow. Would they get that price for it?
- Traditional assets (stocks, bonds) generate **dividends** or **coupons**
  - If a major owner of a stock worth 2% of the S&P500 sold, the supply would be absorbed relatively quickly
  - Investors are willing to substitute frictionlessly between stocks if one is temporarily undervalued

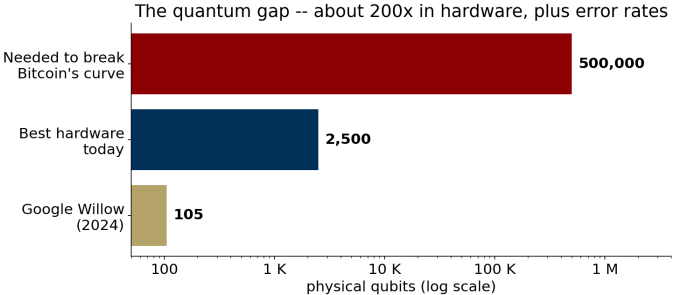
# The "Market Cap" Illusion

**Market Capitalization** is just units outstanding times unit price

- Say everyone tried to sell their BTC tomorrow. Would they get that price for it?
- Traditional assets (stocks, bonds) generate **dividends** or **coupons**
  - If a major owner of a stock worth 2% of the S&P500 sold, the supply would be absorbed relatively quickly
  - Investors are willing to substitute frictionlessly between stocks if one is temporarily undervalued
- Reports of $TRUMP being worth $10 billion+ assume unit price would survive a large selloff (a bad assumption in my opinion)

# The Long-Run Quantum Risk

- Bitcoin's signatures rest on the discrete-log problem (recall ElGamal) – and quantum computers solve discrete logs efficiently in theory (Shor's algorithm)

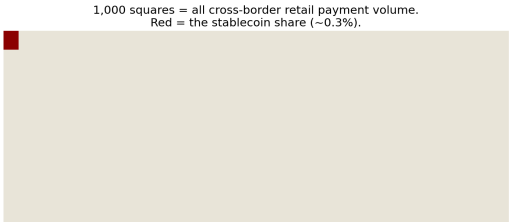



Expert projections (not facts) put cryptographically relevant machines in the **2030s**. Quantum-resistant cryptography already exists – but migrating the chain to it is a massive coordination problem.

# The Payments Scorecard

After 17 years, here is crypto's share of the job it was invented for.

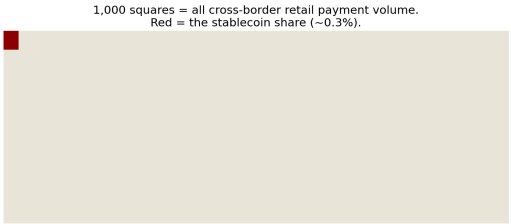
- The stablecoin share, drawn to scale (and essentially **0%** of wholesale) ...



# The Payments Scorecard

After 17 years, here is crypto's share of the job it was invented for.

- The stablecoin share, drawn to scale (and essentially **0%** of wholesale) ...

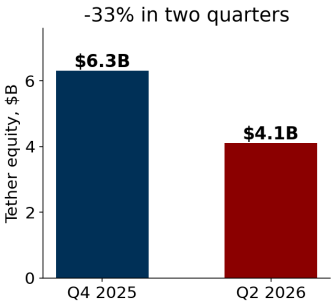



- Banca d'Italia ran actual $200 remittances (USDC vs. traditional corridors) and found **no systematic cost or speed advantage** once on/off-ramps are counted. Growth continues – from a base that rounds to zero

FXC Intelligence–Allium (July 2026); Banca d'Italia stablecoin-remittance study (August 2026).

# The Flagship Issuer

- Tether (USDT), the largest issuer, saw equity fall **a third** in two quarters
- The cushion sits under the risky slice of the Part I balance sheet
- Where usage is growing fastest – emerging markets – the IMF warns of dollarization (residents abandoning the local currency for dollar claims) and illegal-payment channels (Nigeria note, July 2026)
- The largest exchange, Binance, pled guilty (2023) to Bank Secrecy Act and sanctions violations, paying **$4.3B** and exiting the US market
  - Since the settlement, >$1B in Iran-linked flows, under active DOJ monitorship




Tether attestation, Q2 2026; IMF Note on Nigeria's cross-border crypto flows (July 2026); Fortune, Senate HSGAC letter (Feb–Apr 2026).

# In Their Own Words

From the unsealed CFTC and SEC complaints against Binance (2023):

# In Their Own Words

From the unsealed CFTC and SEC complaints against Binance (2023):

- Binance's Chief Compliance Officer, on certain customers:
  *"Like come on. They are here for crime."*

# In Their Own Words

From the unsealed CFTC and SEC complaints against Binance (2023):

- Binance's Chief Compliance Officer, on certain customers:
  *"Like come on. They are here for crime."*
- Binance's Money Laundering Reporting Officer, in reply:
  *"we see the bad, but we close 2 eyes"*
- The CCO again, December 2018:
  *"we are operating as a fking unlicensed securities exchange in the USA bro"*

CFTC v. Zhao, Binance & Lim, complaint filed Mar 27, 2023 (N.D. Ill.); SEC v. Binance, complaint filed June 5, 2023. Quotes verbatim from the complaints.

# The Platform Thesis (As Designed)

How crypto was supposed to become a product platform ...

- The **utility-token thesis** says a token's value grows in proportion to the use cases built on its platform
  - Monegro's "Fat Protocols" (2016) argued that, unlike the internet (where value went to apps, not TCP/IP), blockchain value would concentrate in the protocol layer – so hold the token

# The Platform Thesis (As Designed)

How crypto was supposed to become a product platform ...

- The **utility-token thesis** says a token's value grows in proportion to the use cases built on its platform
  - Monegro's "Fat Protocols" (2016) argued that, unlike the internet (where value went to apps, not TCP/IP), blockchain value would concentrate in the protocol layer – so hold the token
  - Burniske's MV=PQ valuation says a token's price should scale with the transaction volume its platform hosts

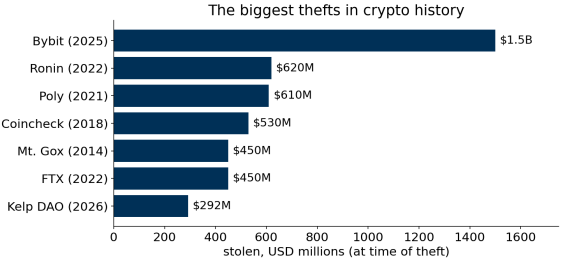
# The Platform Thesis (As Designed)

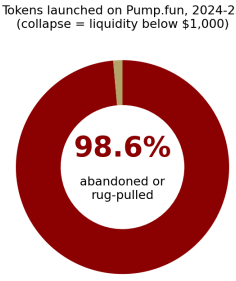
How crypto was supposed to become a product platform ...

- The **utility-token thesis** says a token's value grows in proportion to the use cases built on its platform
  - Monegro's "Fat Protocols" (2016) argued that, unlike the internet (where value went to apps, not TCP/IP), blockchain value would concentrate in the protocol layer – so hold the token
  - Burniske's MV=PQ valuation says a token's price should scale with the transaction volume its platform hosts
  - Cong, Li & Wang's *Tokenomics* (RFS 2021) formalized it, deriving token prices from platform adoption
- This thesis is exactly why DAO treasuries look the way they do ...
  - Hold billions in native tokens → write grants to developers → developers build DApps → usage raises token value → treasury appreciates
- A flywheel, on paper. **The flywheel never spun.** Five reasons why →

# Reason 1. Open Design Invites Predators

- Permissionless + irreversible + pseudonymous means no chargebacks, no deposit insurance, no intermediary with a duty to you
- The retail-scale version is the **rug pull** – launch a token, attract buyers, drain the liquidity, vanish




Even on Arbitrum – the most trusted L2 – protocols were drained in 2026 (Kelp DAO, above). The openness that makes the technology beautiful makes the industry adversarial.

# Reason 2. A Tragedy of the Commons

- The developer who builds a great DApp creates value for every token holder – but captures almost none of it

# Reason 2. A Tragedy of the Commons

- The developer who builds a great DApp creates value for every token holder – but captures almost none of it
- Under equity, building a great product inside a firm means the shareholders (including you, via options) capture it

# Reason 2. A Tragedy of the Commons

- The developer who builds a great DApp creates value for every token holder – but captures almost none of it
- Under equity, building a great product inside a firm means the shareholders (including you, via options) capture it
- Token grants $\neq$ equity; they are one-time payments with no claim on the value your app creates going forward
- The prediction is **persistent underinvestment** in the ecosystem – exactly what we observe
- (This is the subject of an ongoing Harvard Business School case study I'm coauthoring.)

# Reason 3. Nobody Touches the Chain

- Most people will never manage keys, gas, or slippage – they interface through a polished app that abstracts many layers over the blockchain

# Reason 3. Nobody Touches the Chain

- Most people will never manage keys, gas, or slippage – they interface through a polished app that abstracts many layers over the blockchain
- So the app layer owns the customer relationship, the data, and the margin

# Reason 3. Nobody Touches the Chain

- Most people will never manage keys, gas, or slippage – they interface through a polished app that abstracts many layers over the blockchain
- So the app layer owns the customer relationship, the data, and the margin
- In practice Monegro's "fat protocols" thesis inverted. The value accrued to Coinbase – the app layer – not to the protocols
- A platform whose end users can't touch it directly is a platform whose token can't capture their value

# Reason 4. The Talent Sorted

- **My own assessment**:

# Reason 4. The Talent Sorted

- **My own assessment**:
- The best and most trustworthy developers have been content to pay the regulation-and-taxation toll to build inside Uncle Sam's dollar-denominated, SEC-regulated ecosystem

# Reason 4. The Talent Sorted

- **My own assessment**:
- The best and most trustworthy developers have been content to pay the regulation-and-taxation toll to build inside Uncle Sam's dollar-denominated, SEC-regulated ecosystem
- Bad actors find the unregulated setup optimal for scamming – so they stayed
- A sorting equilibrium set in. Over time, "crypto-native" became a negative quality signal for talent and users alike
- Once sorting sets in, it self-reinforces, as users learn to distrust, honest builders leave faster

# Reason 5. Anonymity Meets AI

- From my research with Victor Huang on the Arbitrum DAO, whose treasury holds billions of dollars

# Reason 5. Anonymity Meets AI

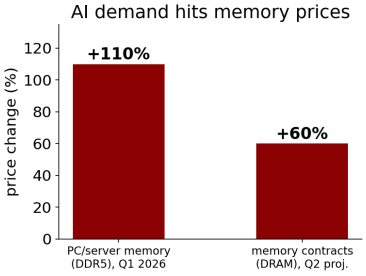
- From my research with Victor Huang on the Arbitrum DAO, whose treasury holds billions of dollars
- Forum deliberation predicted vote outcomes – until early 2024, when LLMs could produce indistinguishable governance prose

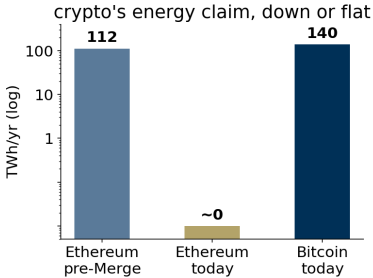
# Reason 5. Anonymity Meets AI

- From my research with Victor Huang on the Arbitrum DAO, whose treasury holds billions of dollars
- Forum deliberation predicted vote outcomes – until early 2024, when LLMs could produce indistinguishable governance prose
- After that, the correlation is **gone** – even though few posts were actually AI-written
- The theory is that when identity is anonymous and text is cheap to fake, the signal value of all text can collapse at a discrete tipping point
- Anonymity – a design pillar of crypto – is precisely the vulnerability AI exploits

Hall & Huang, "The Effect of AI Writing on Governance: Evidence from a $3.5 Billion DAO" (working paper) – josephphall.com.

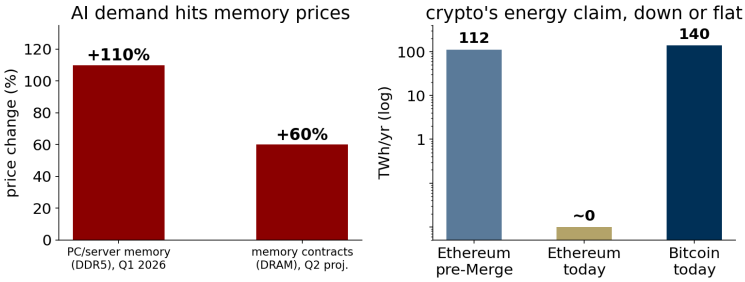
# AI's Second Squeeze Is in Hardware




- Miners are converting. IREN, a large listed bitcoin miner, raised $3B to turn mining sites into AI data centers

# AI's Second Squeeze Is in Hardware




- Miners are converting. IREN, a large listed bitcoin miner, raised $3B to turn mining sites into AI data centers
- The energy decline is by design – mining burn is socially wasteful; ending it was the point of The Merge and of L2s. Mining secured the chain because it was the best use of that hardware. It no longer is.

TrendForce DRAM contract data Q1–Q2 2026; ethereum.org (Merge); Cambridge CBECI; IREN convertible notes (May 2026).

# Meanwhile, TradFi Is Adopting the Technology

The blockchain applications are thriving – inside the regulated system.

- **Robinhood moved its backend onto a blockchain**. Robinhood Chain (mainnet July 2026), built on Arbitrum's stack – tokenized U.S. stocks trading 24/7 in 120+ countries

# Meanwhile, TradFi Is Adopting the Technology

The blockchain applications are thriving – inside the regulated system.

- **Robinhood moved its backend onto a blockchain**. Robinhood Chain (mainnet July 2026), built on Arbitrum's stack – tokenized U.S. stocks trading 24/7 in 120+ countries
  - Caveat: the "stock tokens" are debt claims on Robinhood, not equity

# Meanwhile, TradFi Is Adopting the Technology

The blockchain applications are thriving – inside the regulated system.

- **Robinhood moved its backend onto a blockchain**. Robinhood Chain (mainnet July 2026), built on Arbitrum's stack – tokenized U.S. stocks trading 24/7 in 120+ countries
  - Caveat: the "stock tokens" are debt claims on Robinhood, not equity
- **Native tokenized securities**. JPMorgan, BlackRock & Goldman tokenizing stocks and Treasuries – the actual asset, not a wrapper; BNY pushing 24/7 Treasury settlement
- **Tokenized deposits**. Wells Fargo and other major banks, for corporate treasury
- Note what they kept (the ledger, atomic settlement, programmability) and what they dropped (permissionlessness, anonymity, the native token)

Robinhood newsroom (Jun 2025); Forbes, CoinDesk (Feb–Jul 2026); WSJ (Jul–Aug 2026).

# ...and Sovereigns Are Building the Rails

- **Tokenized sovereign debt**. UK digital gilt pilot (HSBC/LSEG), first digital bond by 2027

# ...and Sovereigns Are Building the Rails

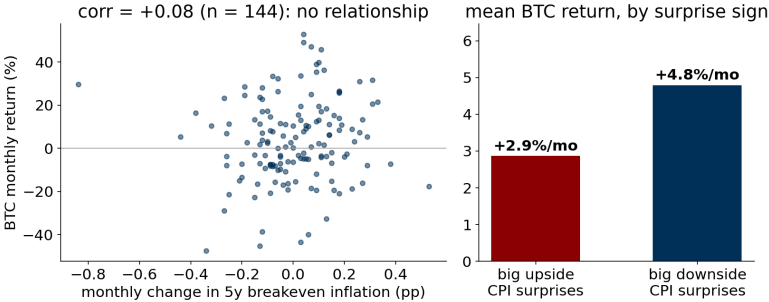
- **Tokenized sovereign debt**. UK digital gilt pilot (HSBC/LSEG), first digital bond by 2027
- **Central-bank digital currency (CBDC) pilots**. ECB digital-euro pilot (36 payment firms); Korea's two-layer CBDC; BIS Project Agorá for programmable cross-border payments

# ...and Sovereigns Are Building the Rails

- **Tokenized sovereign debt**. UK digital gilt pilot (HSBC/LSEG), first digital bond by 2027
- **Central-bank digital currency (CBDC) pilots**. ECB digital-euro pilot (36 payment firms); Korea's two-layer CBDC; BIS Project Agorá for programmable cross-border payments
- **Public fast payments winning at scale**. Brazil's Pix so dominant it triggered a US trade dispute; BRICS cross-border linkage; e-CNY settling cross-border trades in 30 minutes
- Across all of these, the state and the banks took what worked and put it behind identity, regulation, and the sovereign's monetary fiat

# Testing "Bitcoin Is a Bet Against Fiat"

- If BTC hedges sovereign money-printing, it should rise on inflation surprises. Monthly data, 2014–2026.




And in the one real test – the 2021–22 CPI shock, the largest inflation surprise in four decades – BTC returned −59%. Where fiat does fail (Nigeria, Argentina), the flight is into dollar stablecoins. The debasement hedge exists, and it is the dollar.

# Faster Horses

# Prognosis. Augmentation, Not Replacement

- The libertarian wild-west utopia – money and finance without states, banks, or identity – has not come to pass, and looks less like a forecast and more like science fiction every year

# Prognosis. Augmentation, Not Replacement

- The libertarian wild-west utopia – money and finance without states, banks, or identity – has not come to pass, and looks less like a forecast and more like science fiction every year
- **That is not a doomer take on the technology.** The blockchain toolkit – shared ledgers, atomic settlement, programmable assets, 24/7 markets – is proving genuinely transformative in TradFi's hands

# Prognosis. Augmentation, Not Replacement

- The libertarian wild-west utopia – money and finance without states, banks, or identity – has not come to pass, and looks less like a forecast and more like science fiction every year
- **That is not a doomer take on the technology.** The blockchain toolkit – shared ledgers, atomic settlement, programmable assets, 24/7 markets – is proving genuinely transformative in TradFi's hands
- Crypto will not replace the traditional financial system; on current evidence it will augment and support it – the rails beneath tokenized Treasuries, stock tokens, and instant settlement
- The five structural problems explain why the value migrated. They are design features of permissionless anonymity, and TradFi adopted everything else
- As a steelman, crypto has been declared dead before, and EM stablecoin demand is real. What would change my mind? A DApp ecosystem that grows without grant subsidies.

# Discussion

## Questions to argue about

- If the utility-token flywheel can't spin, what should a DAO do with a multi-billion-dollar treasury? Is there a mechanism design that lets DApp developers capture the value they create?

# Discussion

## Questions to argue about

- If the utility-token flywheel can't spin, what should a DAO do with a multi-billion-dollar treasury? Is there a mechanism design that lets DApp developers capture the value they create?
- Is there a market for proof of computing power in the long run? Is Bitcoin that market?

# Discussion

## Questions to argue about

- If the utility-token flywheel can't spin, what should a DAO do with a multi-billion-dollar treasury? Is there a mechanism design that lets DApp developers capture the value they create?
- Is there a market for proof of computing power in the long run? Is Bitcoin that market?
- How long will the U.S. dollar stay the world's dominant currency? Will it be replaced by another sovereign or by something else?

# Credits & Sources

- Part I is adapted in part from teaching materials by **Anthony Lee Zhang**, used with permission – thank you, Anthony
- Much of the market evidence in Part II was surfaced through **Darrell Duffie**'s fast-digital-payments seminar list
- Research cited includes Hall & Huang (2026); Cong, Li & Wang (RFS 2021); Monegro (2016); reports by FXC Intelligence–Allium, Banca d'Italia, the BIS, and the IMF (2026)
- Price data from Yahoo Finance. Errors and opinions are mine alone.

josephphall.com