Emerging Technologies and Law

The Blockchain

In this video…

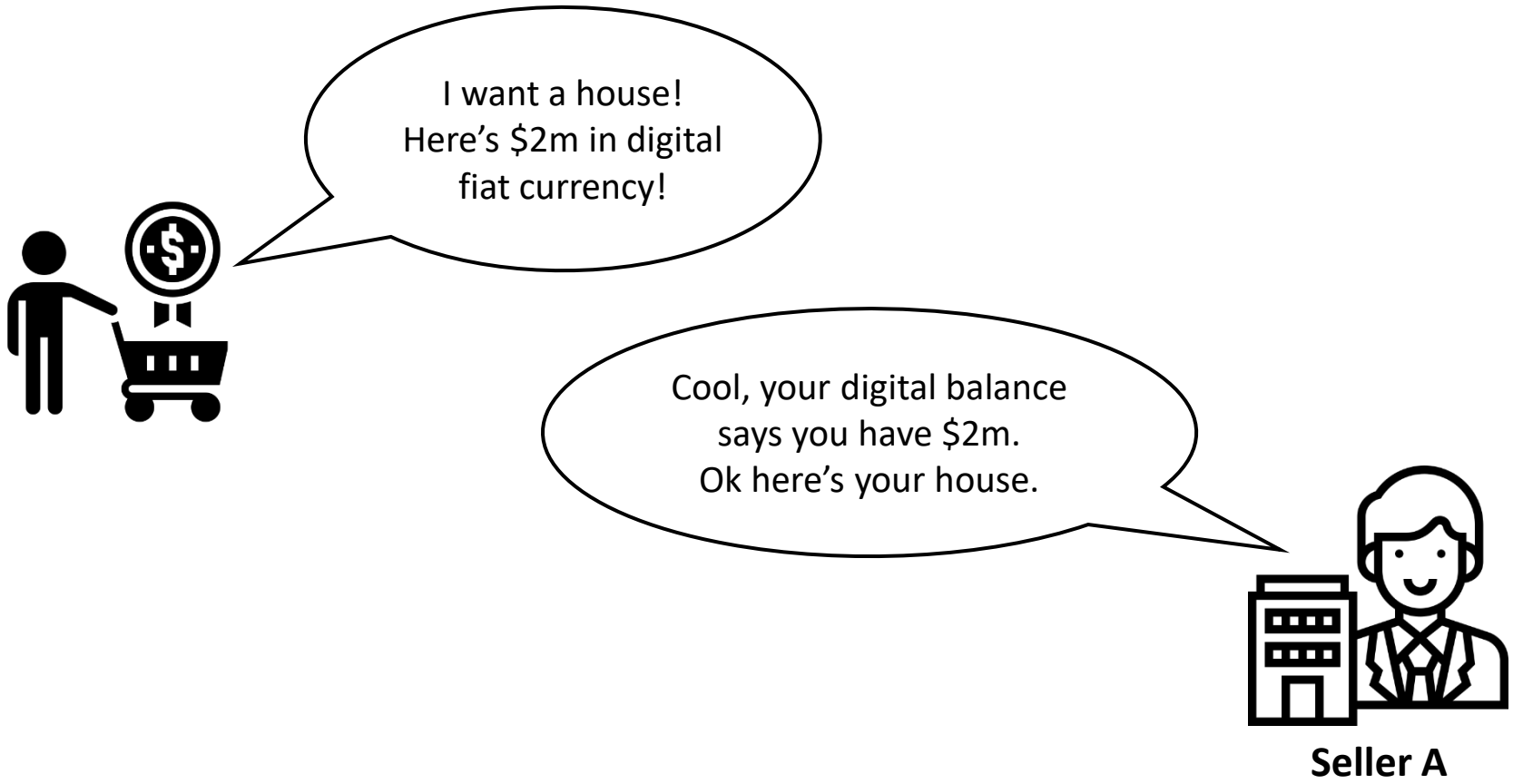
- The next big thing (banks HATE this)
- Understanding the blockchain and its implications

What is Blockchain?

The OG Definition

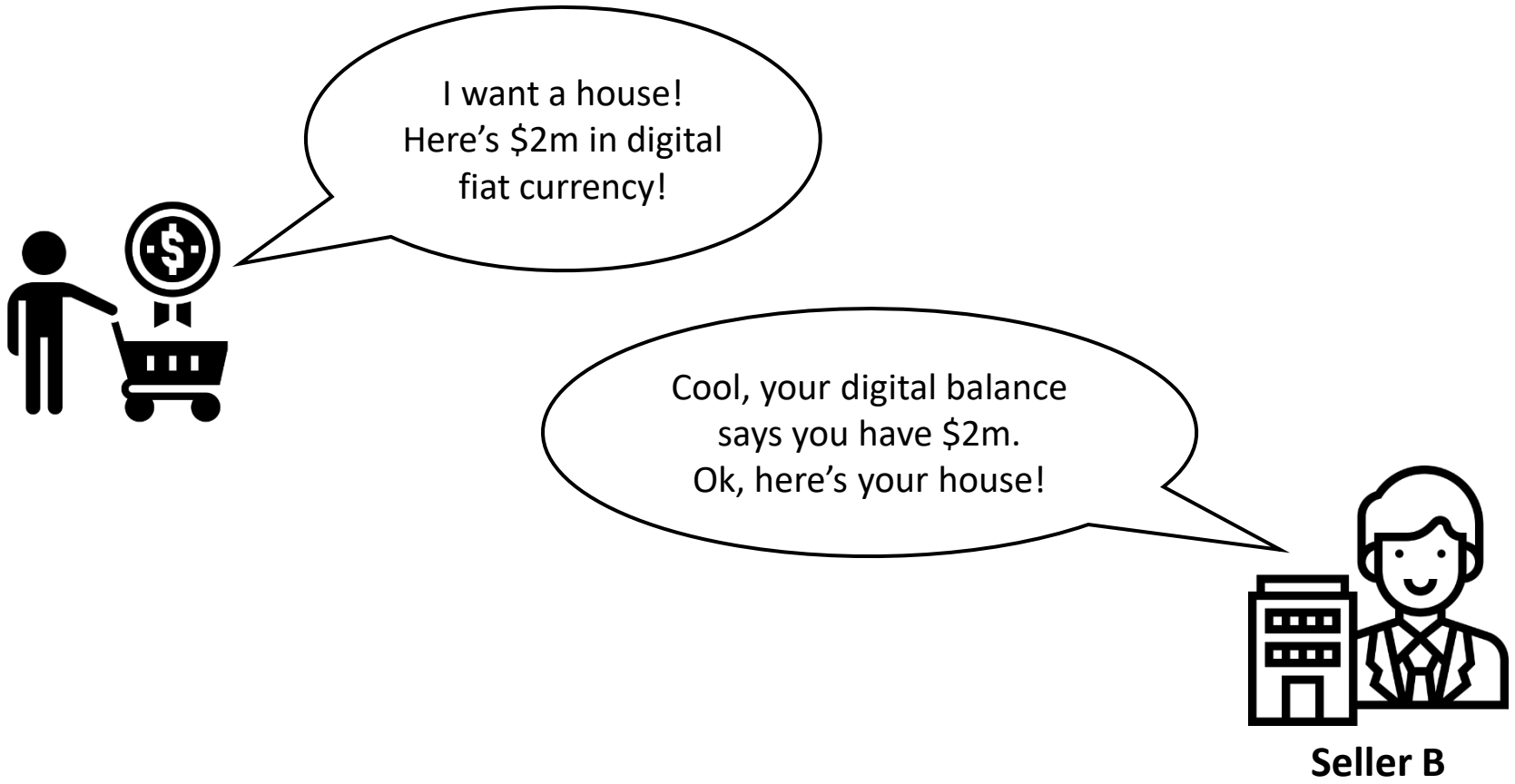
"a solution to the **double-spending problem** using a **peer-to-peer distributed timestamp server** to generate **computational proof** of the chronological order of transactions"

Double Spend Problem




A FEW
MOMENTS LATER

Double Spend Problem



The Solution

- How do sellers know you have what you purport to give?
- Physical cash: proof is in **possession**

- Digital currency?

The Solution

DigiBank

Buyer has $2m with me on escrow

I want a house!
Here's $2m in digital fiat currency!

Cool, DigiBank says you have $2m.
Ok here's your house.

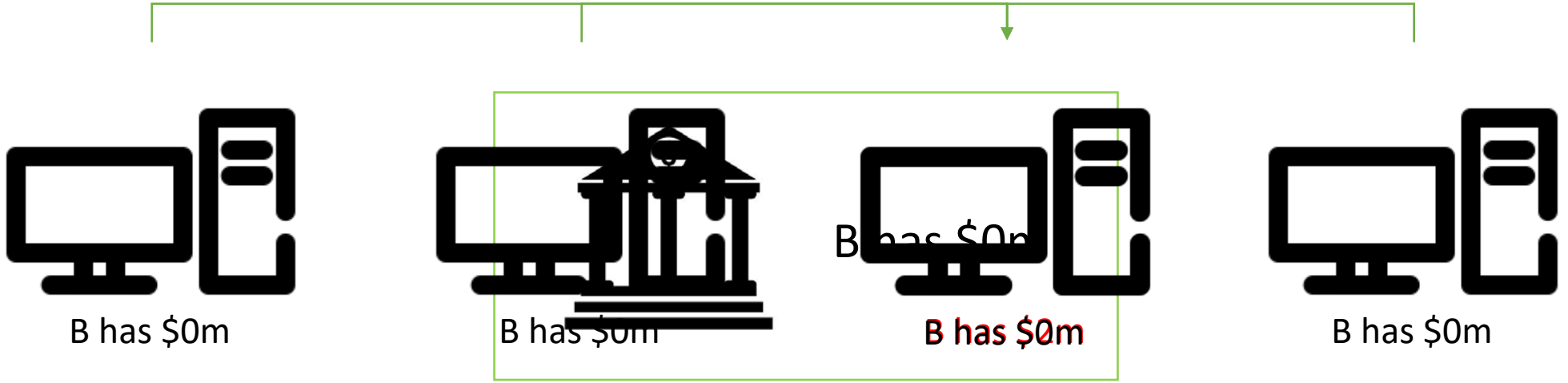
Seller B

The Solution

- Problem unique to **online** transactions (and other transactions based on **records**, even if not electronic)

- Traditional solution is **trusted intermediaries (aka platforms)**
- *Why do we trust banks?*
- Laws, enforcement → trust in government
- Business reputation, profitability → trust in markets
- Social capital → trust in norms
- **Now enter blockchain → trust in code**

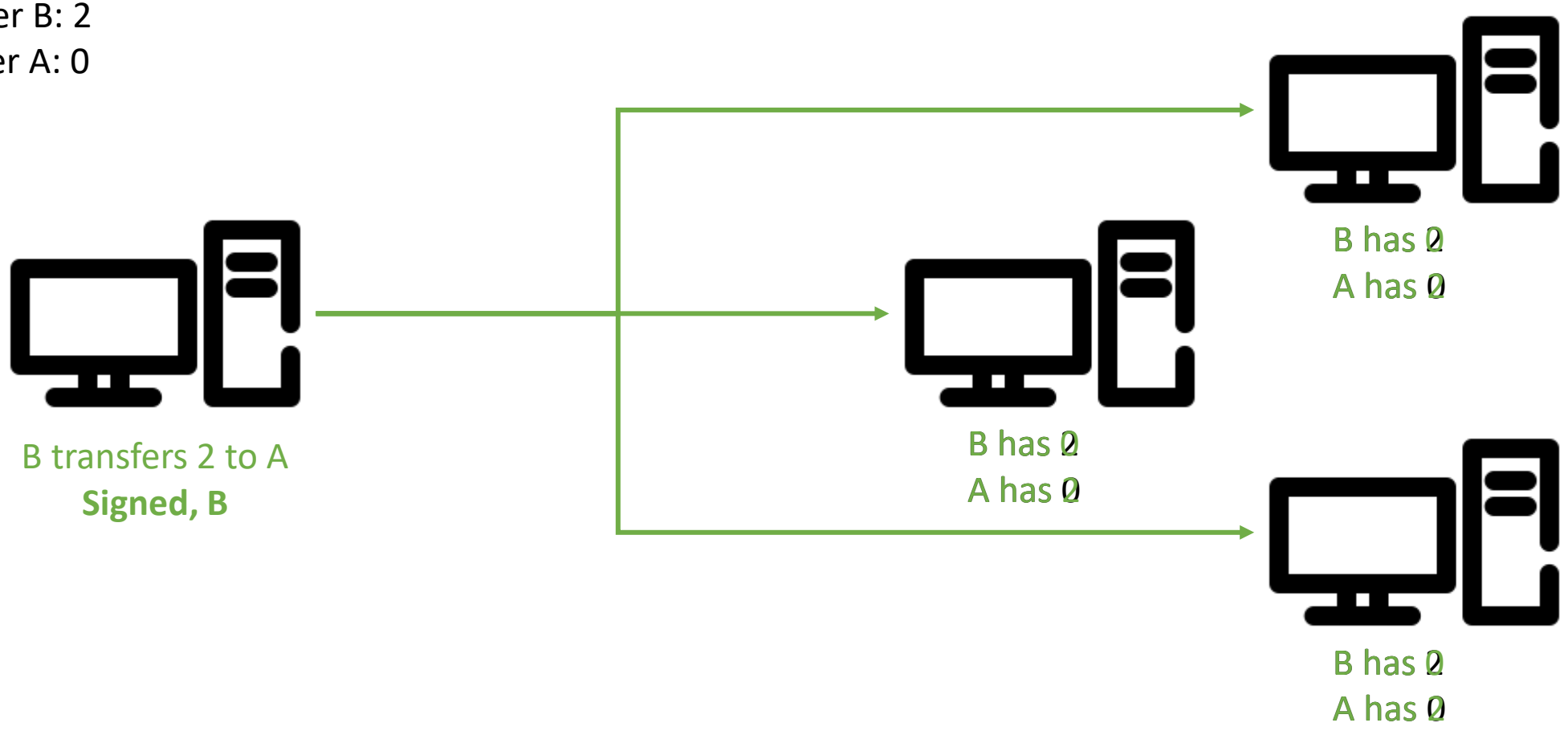
“Peer-to-peer distributed timestamp server”



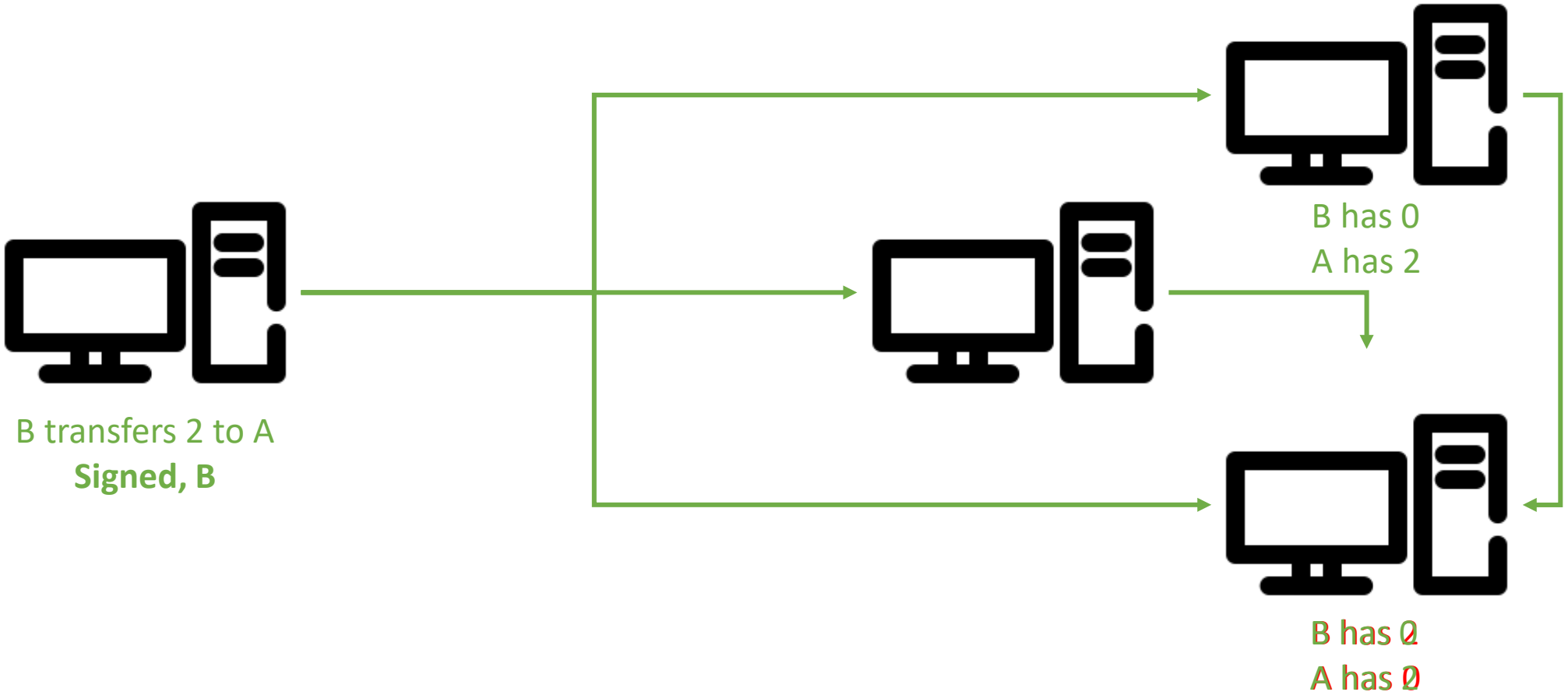
B has $0m

"Computational Proof of Transactions"

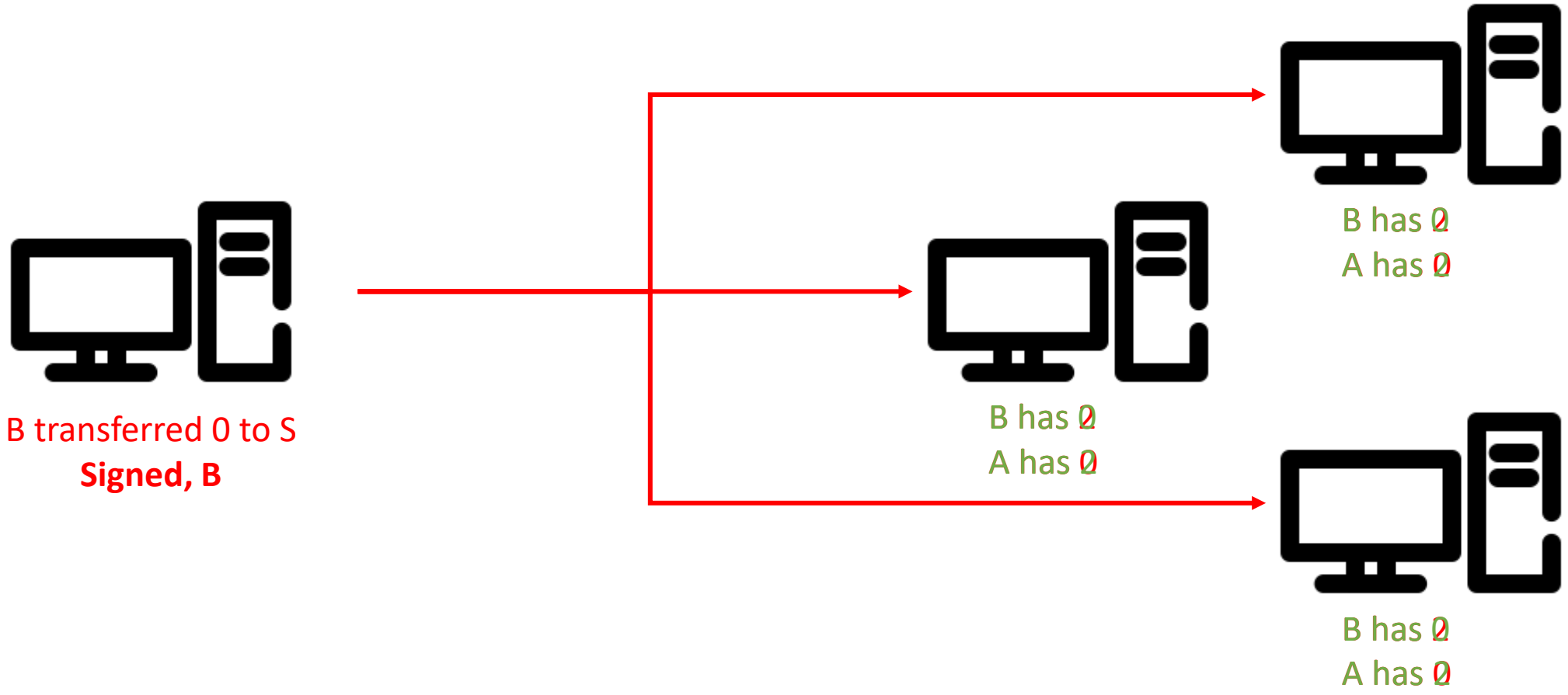
Current balances:
Buyer B: 2
Seller A: 0



Tampering Attempt 1: Mis-repeating



Tampering Attempt 2: Re-writing Records



How to Overcome?

- Attack vectors: assume the most dangerous situation (where the attacker is the original transactee)
- **Markets won't work**: B has every **incentive** to 'undo' transaction after spending money
- **Law** not efficient, too slow
- No clear **social norms**
- So back to code: **consensus mechanisms that enforce majority agreement at the point of accepting transactions**

Cryptographic Hash (#) Functions

- **SHA (or Secure Hash Function) 256** is one (of many) algorithms available for encrypting information
- Encryption is achieved by converting or ("hashing") *human readable information*, like plain English, to some gibberish. For instance:

  SHA256("blockchain") → ef7797e13d3a75526946a3bcf00daec9fc9c9c4d51ddc7cc5df888f74dd434d1

- For the encryption to be **secure**, it is essential that given the RHS output, you **cannot easily figure out the what the original LHS output was**
- However, you can guess what the LHS was, and see if SHA([your guess]) produces the same output. If so, you have "decrypted" the info.
- As we will see later, however, the blockchain does not rely on this bit to encrypt data, because **all the inputs are transactions that should be on public record**

- For SHA**256** specifically, the output is always 256 characters regardless of input length

POW Consensus and Tamper-Proofing

B transfer 2 to S
Signed, B

Block ID 1233

…

Block ID 1234
Date: 28-09-2021
Time: 1600:30:30
Transactions:
- **B-2, S+2**
- Y-3, Z+3
- …

Previous block #:
abc4032
~~**X?**~~ **X: 123**

Block ID 1235
Date: 28-09-2021
Time: 1605:00:00
Transactions:
- …

Previous block #:
cdef1234
X?

Proof-of-work: Find X so that SHA256("280920211600303O—B-2,S+2…abc4032—X") starts with "00000"
E.G. SHA256("blockchain") = ef7797e13d3a75526946a3bcf00daec9fc9c9c4d51ddc7cc5df888f74dd434d1

All blocks are publicly-distributed, so anyone can try to solve (or "mine"). **Suppose X is found to be 123. Block 1234's # = SHA256("…123"). Say this is cdef1234 for simplicity.**

POW Consensus and Tamper-Proofing

B transferred 0 to S
Signed, B

Block ID 1233

…

Block ID 1234
Date: 28-09-2021
Time: 1600:30:30
Transactions:
- **B-0, S+0**
- Y-3, Z+3
- …

Previous block #:
abc4032
X?

Block ID 1235
Date: 28-09-2021
Time: 1605:00:00
Transactions:
- …

Previous block #:
Not cdef1234
X?

Suppose attacker wants to re-write block 1234 as such. They must:

1. Find **new X** for block 1234 so that SHA("…B-0,S+0…") starts with "00000".
2. If they succeed (say new X is 321), SHA("…321") is different too.
3. **So must find new X for block 1235 also**

POW Consensus and Tamper-Proofing

B transferred 0 to S
Signed, B

Block ID 1234
Date: 28-09-2021
Time: 1600:30:30
Transactions:
- **B-0, S+0**
- Y-3, Z+3
- …

Previous block #:
abc4032
X?

Block ID 1235
Date: 28-09-2021
Time: 1605:00:00
Transactions:
- …

Previous block #:
Not cdef1234
X?

Block ID 1236
Date: 28-09-2021
Time: 1610:00:00
Transactions:
- …

Previous block #:

X?

Block ID 1237
Date: 28-09-2021
Time: 1620:00:00
Transactions:
- …

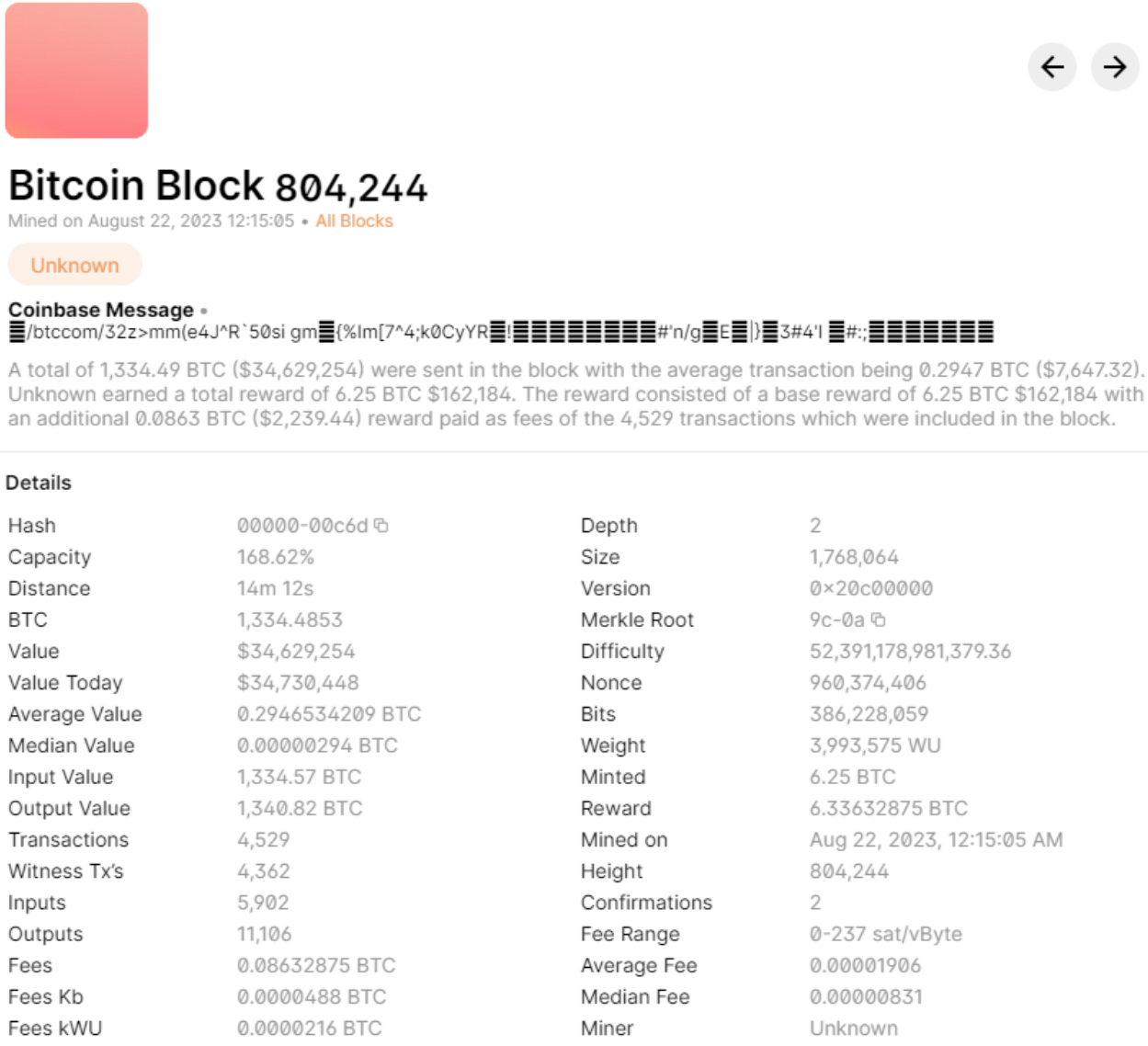
Previous block #:

X?

- While solving 1235, network adds 1236, 1237, etc,
- Attacker **must present *longest* blockchain** to win consensus
- Sets up a **race between honest and dishonest nodes**
- By naïve (Poisson) probability model, can show that chance of attacker winning diminishes exponentially as (a) more nodes added, (b) honest/attacker nodes compute faster/slower

The Actual Bitcoin Chain

Try and spot some of the terms and concepts just covered. Of course, we haven't covered everything.



Bitcoin Block 804,244

Mined on August 22, 2023 12:15:05 • All Blocks

Unknown

Coinbase Message •
/btccom/32z>mm(e4J^R`50si gm{%lm[7^4;k0CyYR#'n/g{%|}3#4'l #:;

A total of 1,334.49 BTC ($34,629,254) were sent in the block with the average transaction being 0.2947 BTC ($7,647.32). Unknown earned a total reward of 6.25 BTC $162,184. The reward consisted of a base reward of 6.25 BTC $162,184 with an additional 0.0863 BTC ($2,239.44) reward paid as fees of the 4,529 transactions which were included in the block.

Details

Hash	00000-00c6d	Depth	2
Capacity	168.62%	Size	1,768,064
Distance	14m 12s	Version	0×20c00000
BTC	1,334.4853	Merkle Root	9c-0a
Value	$34,629,254	Difficulty	52,391,178,981,379.36
Value Today	$34,730,448	Nonce	960,374,406
Average Value	0.2946534209 BTC	Bits	386,228,059
Median Value	0.00000294 BTC	Weight	3,993,575 WU
Input Value	1,334.57 BTC	Minted	6.25 BTC
Output Value	1,340.82 BTC	Reward	6.33632875 BTC
Transactions	4,529	Mined on	Aug 22, 2023, 12:15:05 AM
Witness Tx's	4,362	Height	804,244
Inputs	5,902	Confirmations	2
Outputs	11,106	Fee Range	0-237 sat/vByte
Fees	0.08632875 BTC	Average Fee	0.00001906
Fees Kb	0.0000488 BTC	Median Fee	0.00000831
Fees kWU	0.0000216 BTC	Miner	Unknown

https://www.blockchain.com/explorer/blocks/btc/804244

Other Consensus Mechanisms (optional)

- Proof-of-stake
  - To mine, must put up deposit
  - The more deposit, the more ‘compute’ in a POW-like sense
  - Slashing conditions (deposit forfeiture) activate if you try to be funny
  - Code-enforced economic disincentives for security
- BFT, Hashgraphs
  - Complicated structure of broadcasts/re-broadcasts to ensure ‘right’ record is found despite attackers
  - Relies on attacker not controlling too many nodes
- See Computer Law & Security Review article

Other Blockchain Features

- Efficient ways of identification/authentication/retrieval, etc
  - Through private/public key cryptography that's a **separate** system from Proof-of-Work and which exists for lots of non-blockchain tech
- Private vs Public blockchains
- No theoretical limit

Takeaways

- Blocks are nothing special. Just **packets of data**
- **Hash chaining** **essential** to tamper-resistance
- Only **probabilistic** resistance. Attacker can still win if:
  - Very few blocks added (slow bit rate)
  - Puzzle too easy to solve
  - Honest nodes have less compute (**50+% attack**)
  - Dumb luck
- POW, POS, etc are necessary for so-called **computational proof of transactions,** but are not entirely bulletproof
- Horrendous waste but good alternative means elusive (like capitalism)
  - Bitcoin's blockchain has **not yet been hacked**
  - Other blockchains have (e.g. Ethereum classic's 50% attack)
  - Ethereum classic was a POW system, though it was thin)

Larger Uses of ~~Blockchain~~ Databases

- Bitcoin blockchain used to record only **transactions** of bitcoin
- **But idea of blockchain as a way to store data securely without trusted 3P is more general**
- What else might be stored on a blockchain?
- Text describing legal or economic rights → ICOs, "tokens"
- Links to real world assets → Off-chain assets/"tokenisation"
- Property records → Land register
- Links to (digital) art → NFT
- Computer code itself → smart contracts
  - Thousands of sub-cryptocurrencies are implemented as code on Ethereum blockchain

Legal Characterisations of Cryptoassets

- Is Bitcoin (and other cryptocurrencies and derivative assets property)?
  - **Note**: Bitcoin is just one 'app' built using a (not *the*) blockchain
- *Bybit v Ho Kai Xin and others [2023] SGHC 199*
  - [31] Cryptoassets are "not classed as physical assets" but "do manifest themselves in the physical world, albeit in a way that humans are unable to perceive".
  - Private/public key locking/unlock system appears to be said "physical manifestation at the level of digital bits and bytes".
  - While not permanent, we can "give a name to a river even though the water contained within its banks is constantly changing"
  - [33] "This description of crypto assets shows that they can be defined and identified by modern humans, such that they can be traded and valued as holdings." They meet the Ainsworth formula.

Bybit v Ho Kai Xin and others [2023] SGHC 199

- [34-35] Are cryptoassets things in possession or in action (given that all personal property are either one or the other)?
- [36] My conclusion is therefore that **the holder of a crypto asset has in principle an incorporeal right of property recognisable by the common law as a thing in action and so enforceable in court.** While it might be said that **this conclusion has an element of circularity in that it could also be said that the right to enforce in court is what makes it a thing in action**, this type of reasoning is not strikingly different from how the law approaches other social constructs, such as money. It is only because people generally accept the exchange value of shells or beads or differently printed paper notes that they become currency. **Money is accepted by virtue of a collective act of mutual faith.**
- What is the court's role here? Is it recognizing the broader societal act of mutual faith in crypto? Or, is it creating one? **Is this an issue with law, tech, or both?**

In this video…

- The next big thing (banks HATE this)
- Understanding the blockchain and its implications