Introduction to Cryptocurrency & Blockchain

Dawn Song
Raymond Cheng

Berkeley EECS
ELECTRICAL ENGINEERING & COMPUTER SCIENCES

Slides credits: Andrew Miller & Ari Juels

Bitcoin market cap over $190B

How it all got started (I)

- Aug 18, 2008: bitcoin.org registered at anonymousspeech.com
- Oct 31, 2008: Nakamoto publishes whitepaper on Bitcoin
- Nov 9, 2008: Bitcoin project registered on SourceForge.net as a community open source project

How it all got started (II)

- Jan 3, 2009: Nakamoto generated Bitcoin's first block of transactions (Block #0): Genesis Block
- Jan 12, 2009: First Bitcoin transaction (Block #170), btw Nakamoto and Hal Finney

- May 22, 2010: First real-world Bitcoin transaction: Laszlo Hanyecz paid 10,000 bitcoins for a

Cryptocurrency Explosion

Coindesk.com

Cryptocurrency market cap over $500B

Cryptocurrency Design Bit by Bit

Cryptocurrency v0: SuckerCoin
World of perfect trust

Pros / Cons of SuckerCoin (v0)

Pros:

- Dirt simple!
- Universal access
- Fast transactions

Cons:

- **No privacy**
- **No security**

Cryptocurrency v1: WallCoin Registered digital currency

- Trusted entity maintains *ledger*, i.e., all transactions over history of the system
  - E.g., running example: Facebuck
- Users identify themselves to Facebuck by logging into Facebuck's website
  - E.g., using password-based authentication
- Facebuck can dictate creation of money
  - E.g., users must deposit dollars with Facebuck

facebuck

3 3 4 Search Home Profile Find Friends

Ari: $100

Deborah: $200

facebuck$ wall

Transaction history:

- Ari ➔ Deborah: $50
- 11 Dec. 2015

… (and all other users)

Facebook © 2011 · English (US)

About · Advertising · Create a Page · Developers · Careers · Privacy · T

facebuck

3 3 4 Search Home Profile Find Friends

facebuck$ wall

Ari: $100

Deborah: $200

Ari: $150

Deborah: $150

Transaction history:

- Deborah ➔ Ari: $50
- 31 Jan. 2017

Ari liked this

Pros / Cons of WallCoin (v1)

Pros:

- Dirt simple!
  - (At least simpler than Facebook privacy settings)
- Universal access
- Fast transactions
- Facebuck can fix errors / reverse transactions

Cons:

- No privacy
  - Facebuck could show information selectively, but…
- **Weak security**

Weak security?

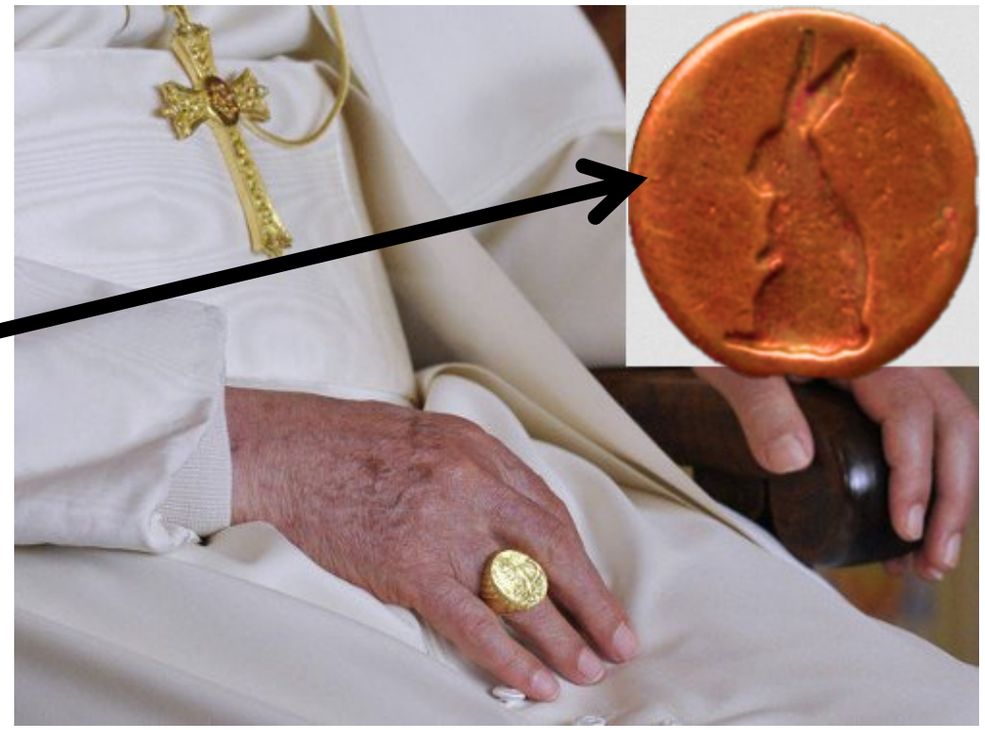
- What if Facebuck cheats?
  - E.g., forges Ari ➔ Deborah: $50
- If Facebuck shows wall selectively for privacy, more opportunity to cheat
- What if passwords are stolen from the system? Unthinkable! Right?

Transaction authentication

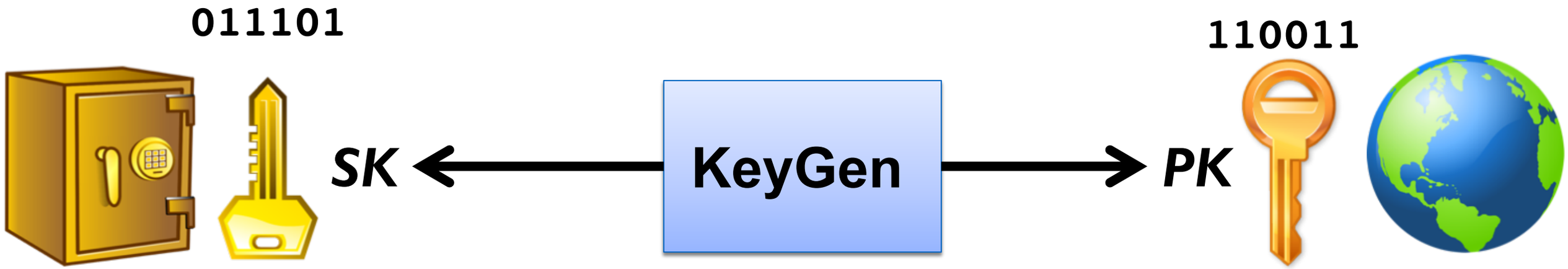
- Passwords represent tradeoff
  - Convenient but vulnerable
  - Require Facebuck to manage them
- Alternative: Digital signatures
  - Much stronger security
  - Facebuck can verify that I authorized a transaction without knowing my secrets!

How digital signatures work: An analogy

- Suppose you had a perfect signet ring
- Everyone knows what your seal looks like
  - "Public key" ***PK***
- But it can only be produced by someone with your ring
  - "Private key" ***SK***
- *Anyone* can verify authenticity of seal ***Sig*** on message ***M***, but *only* holder of rabbit ring can create one



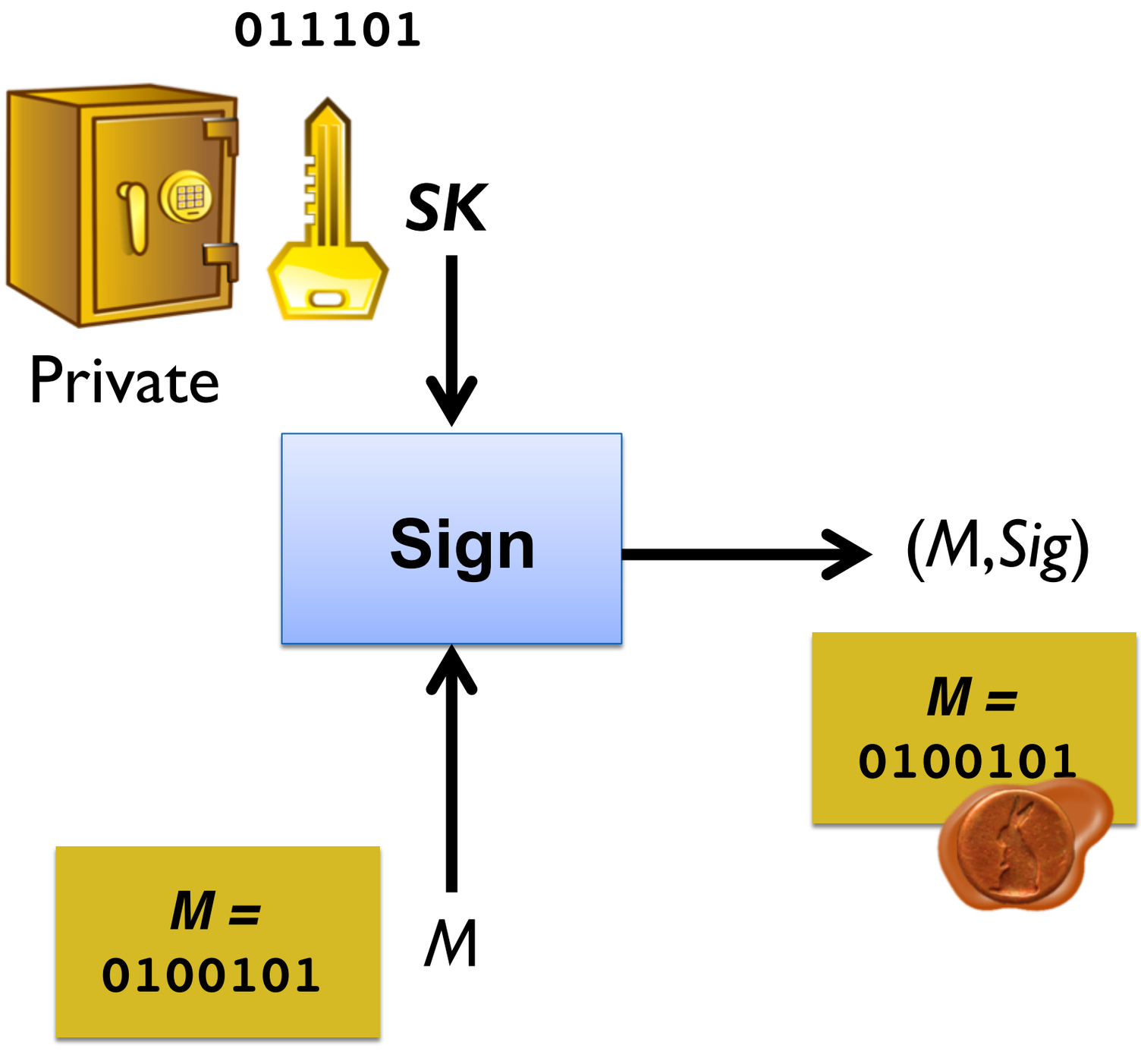
Digital signatures: Technical view



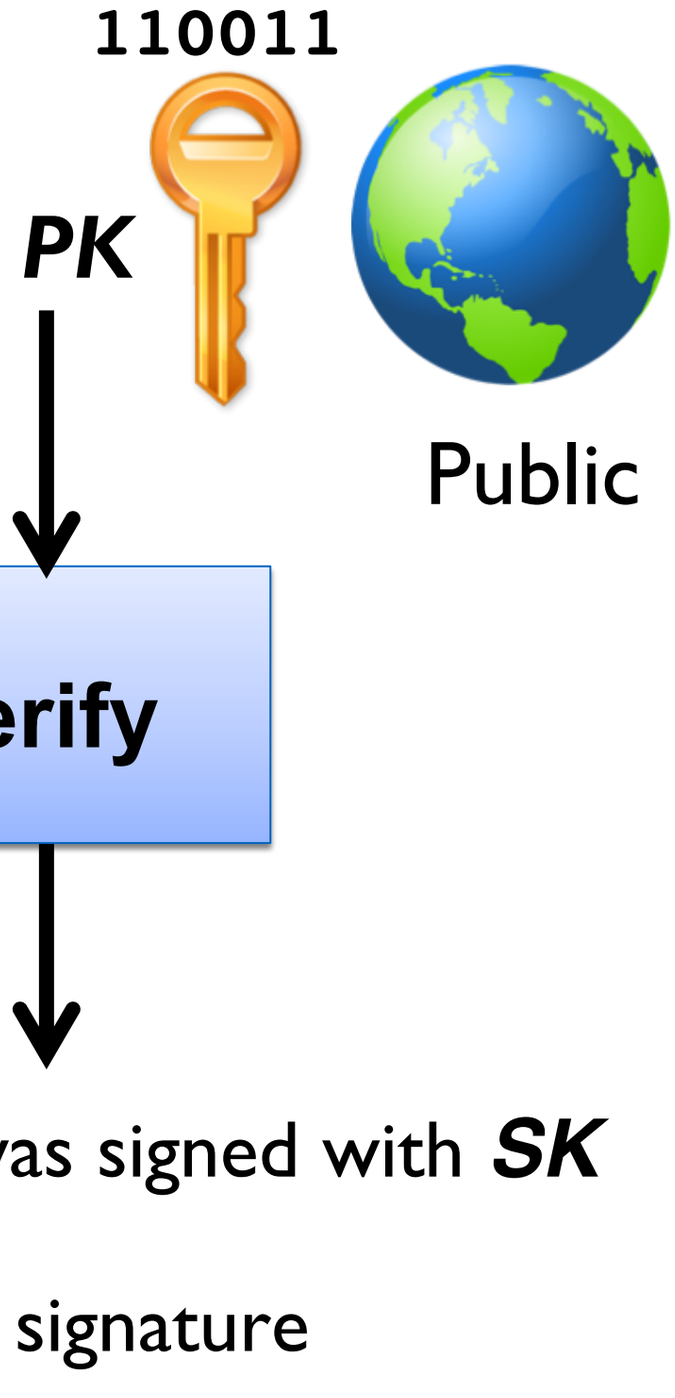
Private

Public

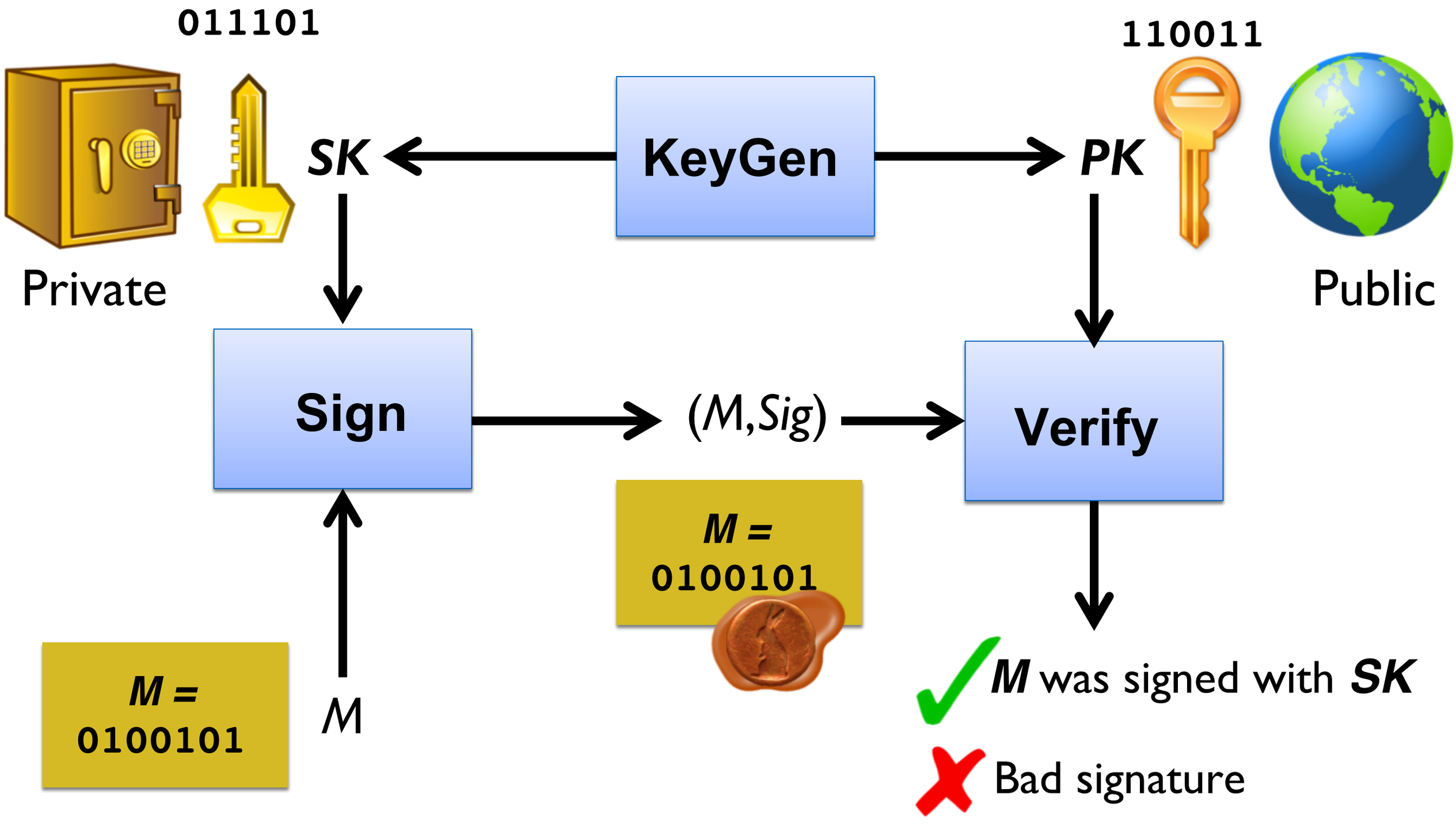
Digital signatures: Technical view



Digital signatures: Technical view



Digital signatures: Technical view



Digital signatures:

Note: Anyone can run software that executes KeyGen, Sign, or Verify, so:

- Any entity *X* can generate unique keypair (SK_X, PK_X)
- *X* can sign using private key SK_X
- Anyone can verify *X*'s signatures against PK_X
- But PK_X does not contain *X*'s real-world identity

Private

Public

K

Bad signature

Bitcoin uses ECDSA

- "Elliptic-Curve Digital Signature Algorithm"
- Private key *SK* is 256 bits; (uncompressed) public key *PK* is 512 bits
- secp256k1 (slightly nonstandard) curve

Digest of *PK*

SK

Bitcoin Paper Wallet

Cryptocurrency v2: SigCoin

- For every account X, sign transactions using private key SK_X
- Assume all public keys PK_X known to the world

facebook 3 3 4 Search Home Profile Find Friends

10 Dec. 2011

Ari: $100

Deborah: $200

facebuck$

11 Dec. 2011

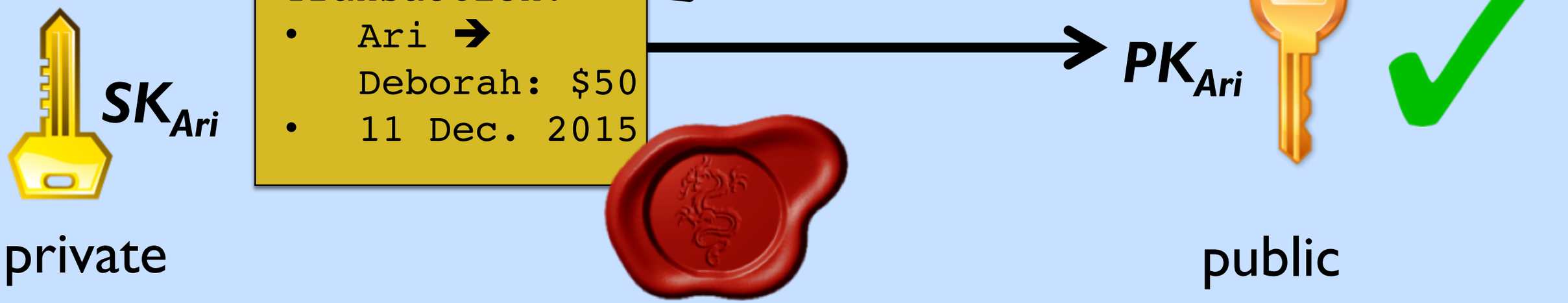
Ari: $50

Deborah: $250

Transaction history:

- Ari → Deborah: $50
- 11 Dec. 2015

Facebook © 2011 · English (US) About · Advertising · Create a Page · Developers · Careers · Privacy · T



Better security!

- Facebuck can't falsify my transactions
- Without $SK_{Ari,}$ no way to generate valid transaction signature
- SK_{Ari} can't be stolen from Facebuck
  - It's not on the Facebuck server!

Adding privacy

- Users can be identified using public keys, not real-world identifiers
  - E.g., Ari is known to Facebuck as PK_{rabbit}
- Users are now *pseudonymous*
  - Transactions linkable, so only partial privacy
    - Rabbit $➔ Frog, Goat
- What are risks of pseudonymity?
  - E.g., if someone learns that PK_{rabbit} is Ari, Ari loses his privacy

Pros / Cons of SigCoin (v2)

Pros:

- No passwords to steal
- Universal access
- Fast transactions
- Facebuck can't falsify transactions

Cons:

- Users need to manage private keys
  - Can't store in head like password!
- Facebuck needs to manage public keys
- Partial privacy: Pseudonymity only
- **Facebuck can still cheat**

Private key *SK* = ownership
leakage = theft

News anchor receives Bitcoin on TV only to have it promptly stolen

75

by Adrianne Jeffries | Dec 23, 2013, 12:33pm EST

SHARE TWEET LINKEDIN

How can Facebuck still cheat?

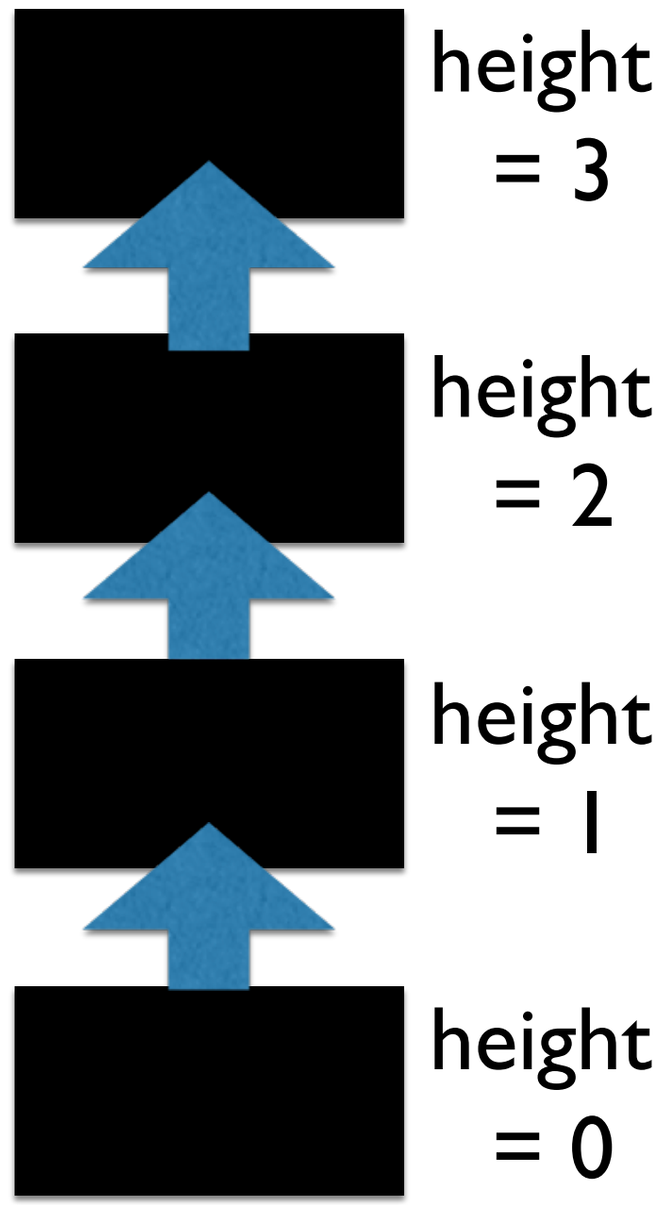
- Can fail to process / post transactions
  - E.g., Facebuck has a put option on an equity—delays or suppresses buy orders by customers
  - E.g., govt. pressures Facebuck to block transactions of suspected criminal
- Can go back and erase transactions!
  - Can take away your money
- Can show different subsets of transactions to different users
- *Rare events, but if they happen, you could lose everything!*

Cryptocurrency v3: ChainCoin

- Facebuck periodically—*every 10 minutes*—applies digital signature to batches of transactions (plus all old batches)
- Now:
  - Batches of transactions signed w.r.t. $PK_{Facebuck}$
  - If Facebuck presents different batches to different users, will be caught
  - If Facebuck tries to delete transaction after the fact, will get caught

Ledger now constructed as a chain of *blocks*

- A *block* is a batch of transactions + a digital signature
- Whole chain contains all transactions over time
- This is a *blockchain*
- Specifies complete system history



Pros / Cons of ChainCoin (v3)

Pros:

- Facebuck can't falsify transactions
- No passwords to steal
- Universal access
- Fast transactions
- If Facebuck deletes transaction, will get caught
- If Facebuck "forks," will get caught

Cons:

- Users need to manage private keys
  - Can't store in head like password!
- Facebuck needs to manage public keys
- Partial privacy: Pseudonymity only
- **Facebuck can suppress transactions**

Transaction suppression

- Facebuck can refuse to process / post transactions
- If Facebuck cheats, there's no recourse
  - You catch Facebuck cheating, not much you can do
- Trust resides in a single entity

Why not trust a central authority?

- E.g., we all trust big banks to manage our money, right?

Why not trust a central authority?

- Hyperinflation, e.g.,
  - Germany in 1919-23
  - Zimbabwe: 624% in 2004
- Frozen assets, e.g.,
  - Greece: banks closed for a week in 2015
  - Argentina: Forbade purchase of dollars from 2011-4

Bitcoin

Bitcoin

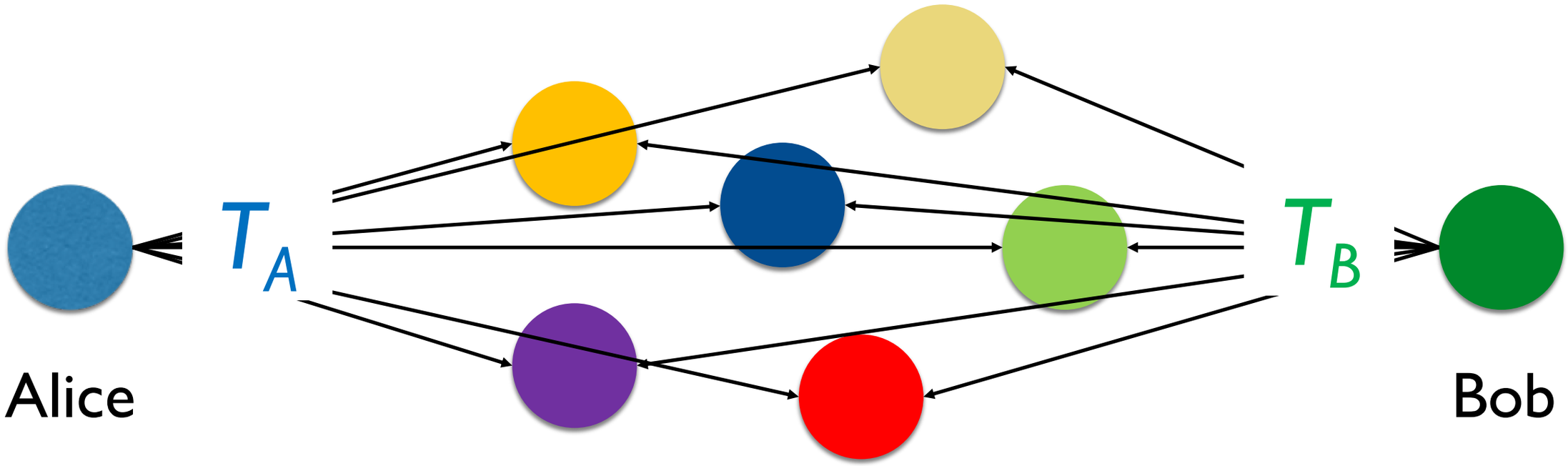
- Just like ChainCoin, i.e.,
  - Pseudonymous: User identities correspond to (*SK*, *PK*) key pairs
  - Users digitally sign transactions to authorize movement of money
  - Transactions recorded in blockchain

Bitcoin

- Except that the blockchain is *fully decentralized*
- Instead of *one* trusted entity like Facebuck, we rely on *whole community*
- Community maintains fully public blockchain / ledger, so that…
- No bank or jurisdiction can suppress transactions

How does community decide what transactions in ledger?

- Idea: Everyone broadcasts to everyone else

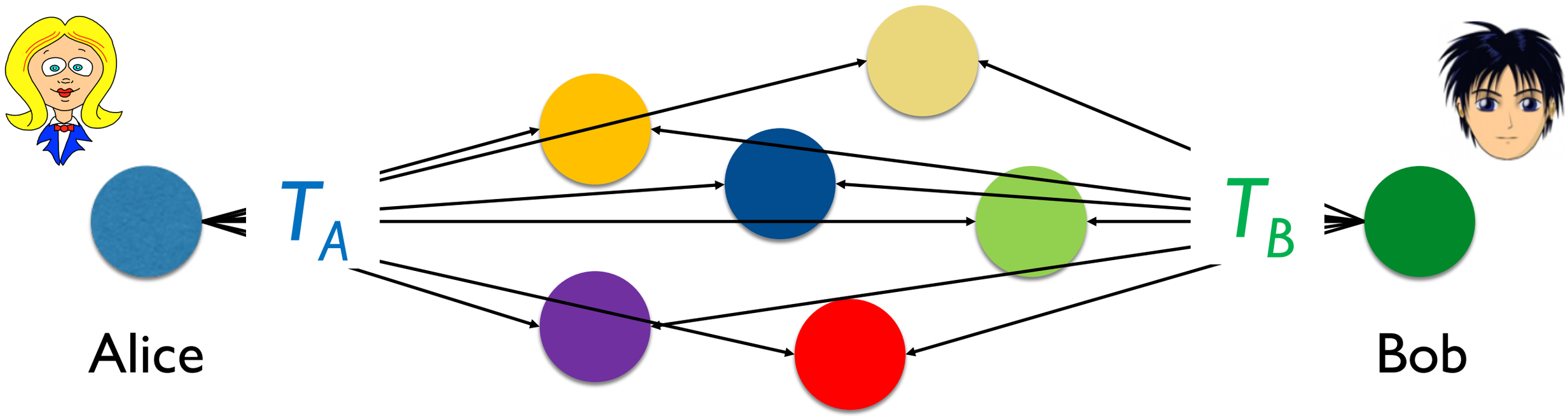


How does community decide what transactions in ledger?

- Idea: Everyone broadcasts to everyone else
- Problems:
  - Won't work with thousands or millions of participants—not always online
  - And even if it did, messages delivery times may vary…

What if messages are delayed?

T_A = *"Pay $5 to Bob"*
T_B = *"Pay $5 to Carol"*



What if messages are delayed?

T_A = *"Pay $5 to Bob"*
T_B = *"Pay $5 to Carol"*

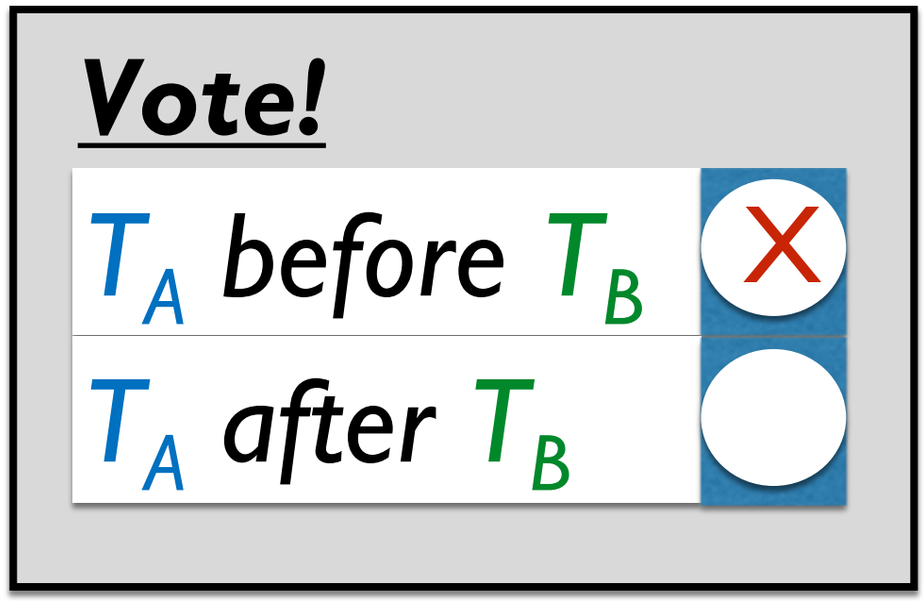
Suppose Bob starts with $0 and then:

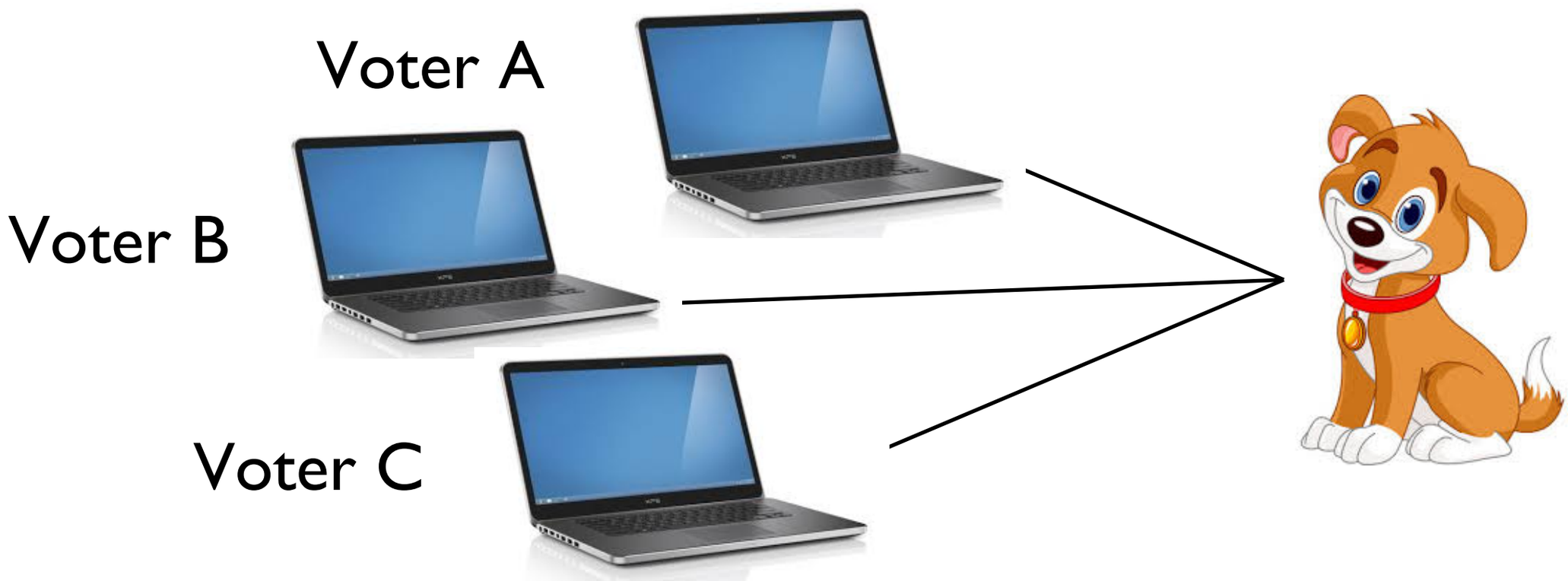
- Case 1: Carol sees T_A *before* T_B
- Case 2: Carol sees T_A *after* T_B

Arguments about transaction order will ensue!

How to decide what transactions are on ledger?

- Another idea: People might vote on what goes in ledger and on order
- Problem: on the Internet, no one knows you're a dog…
- Remember: Bitcoin is pseudonymous

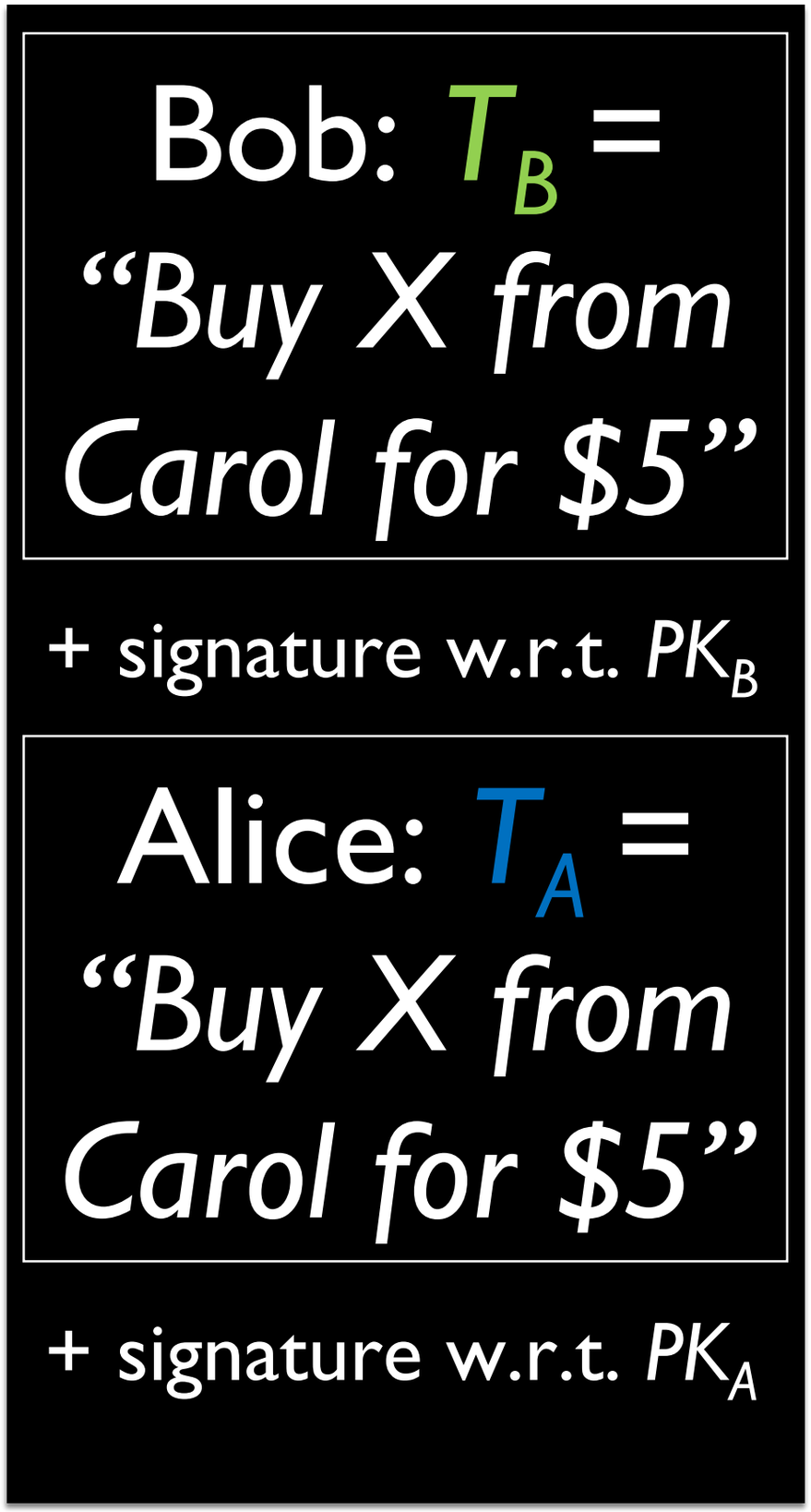




Mining

Key ideas:

- Designate one player to sequence transactions authoritatively in a *block*
  - No dispute about ordering
- Make it hard for same player to be designated many times in succession
  - Prevents denial of transactions
  - Enforces fairness



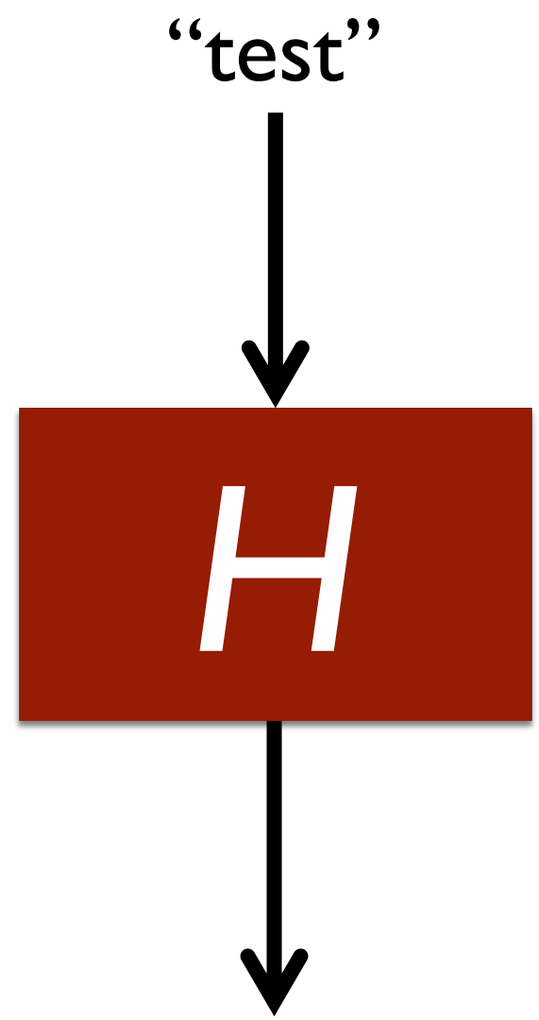
Block

Bitcoin mining

- In Bitcoin, blocks of transactions made authoritative by “mining”
- Anyone in community can be a “miner”
- Idea: "Miners" all race to be the lucky winner (selected leader), who creates the next block on current, ordered batch of transactions

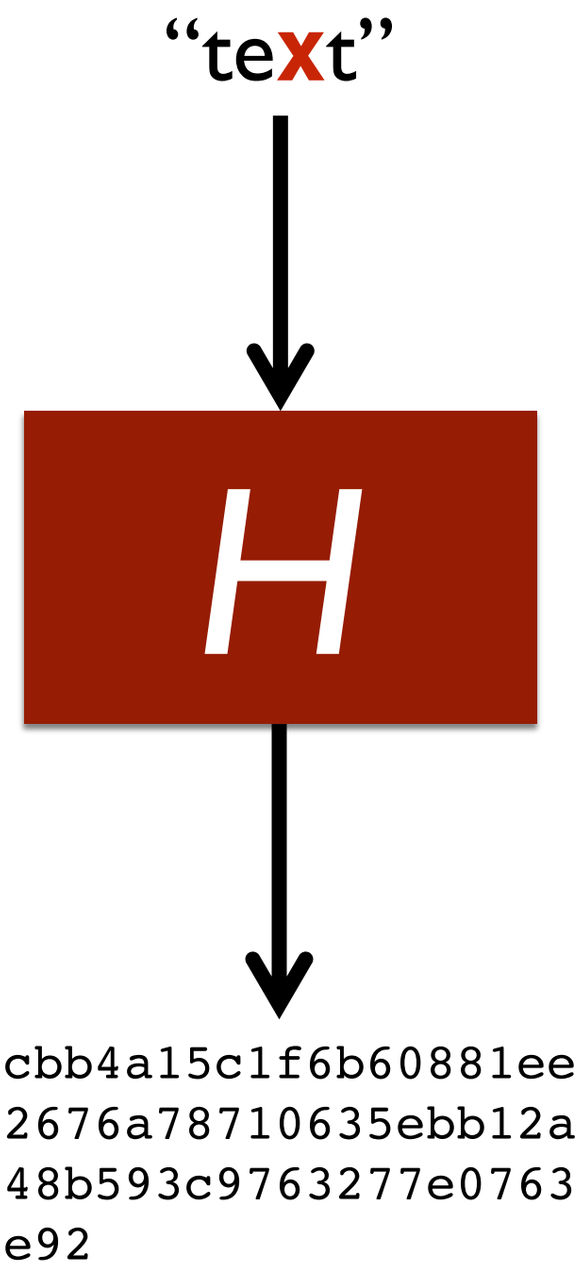
Hash function

- A *hash function H* is a deterministic cryptographic function
- *H* takes as input any desired bitstring / text *B*
- Outputs a *random*(-looking) fixed-size (256-bit) value *H*(*B*)
  - (SHA-256^2 used in Bitcoin)
- Same input ***B* always produces same output**
- Preimage resistance: Given H(x), it is computationally difficult to determine x
- 2nd preimage resistance: Given x, it is computationally difficult to find x' s.t. H(x) == H(x')
- Collision resistance: it is computationally difficult to find x and y s.t. H(x) == H(y)



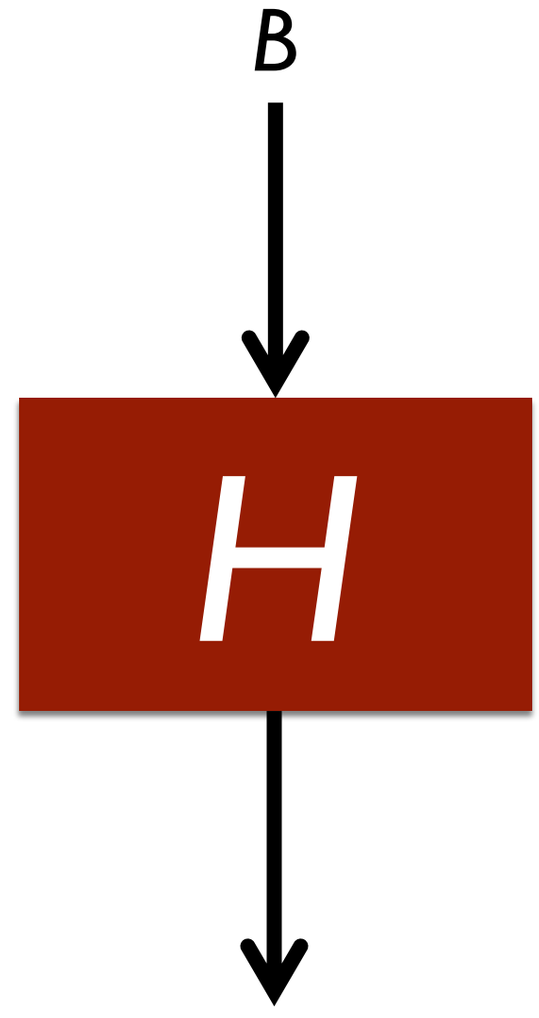
Hash function

- A *hash function H* is a deterministic cryptographic function
- *H* takes as input any desired bitstring / text *B*
- Outputs a *random*(-looking) fixed-size (256-bit) value *H*(*B*)
  - (SHA-256^2 used in Bitcoin)
- Same input ***B* always produces same output**
- Preimage resistance: Given H(x), it is computationally difficult to determine x
- 2nd preimage resistance: Given x, it is computationally difficult to find x' s.t. H(x) == H(x')
- Collision resistance: it is computationally difficult to find x and y s.t. H(x) == H(y)



Mining:
The hashing slot machine

- To mine block, miner keeps trying different values of *B* (varying the nonce value) until H(*B*) has *k* leading zeros
  - *k* is set by system
- Like trying slot machine again and again until row of cherries
- Lots of 0s = lots of work!
- Today, every ten minutes, the whole community pulls slot machine handle more than 100,000,000,000,000,000,000,000 times!
- The faster your machine, the higher the probability that you get lucky and are the first to mine a block
- Called "Proof of work"

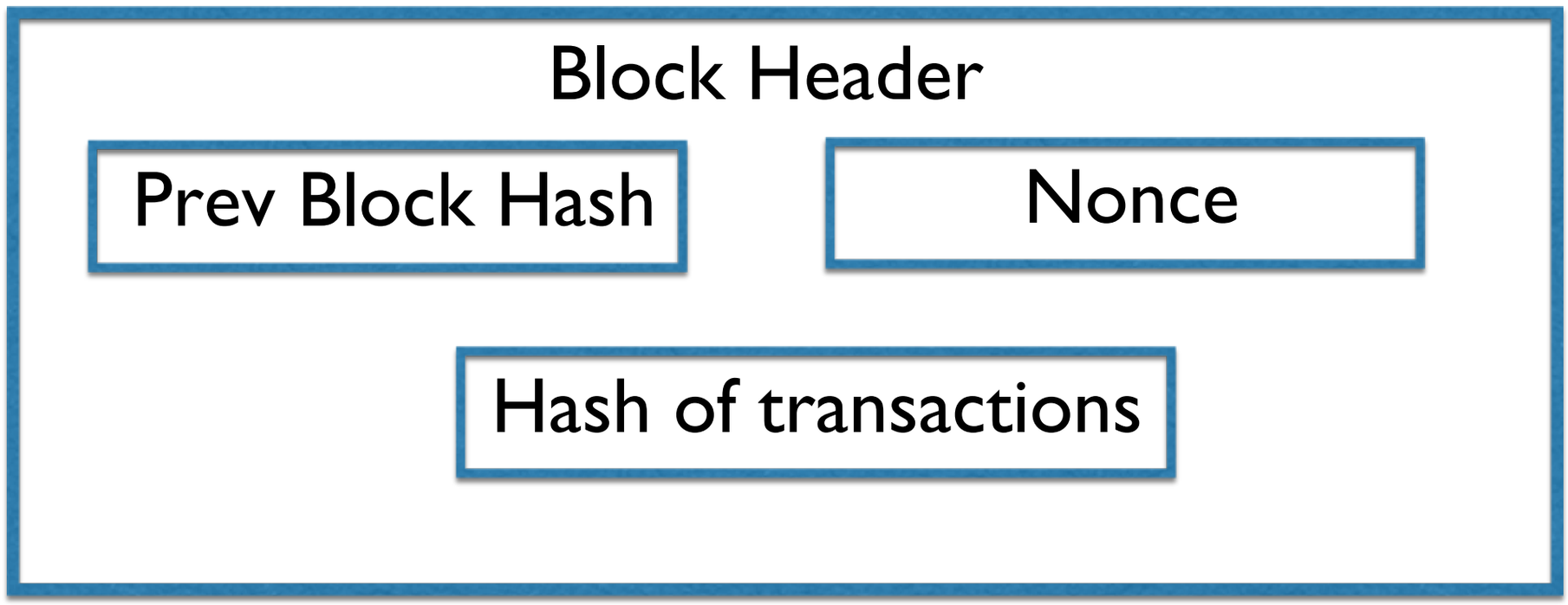


Mining Pseudocode

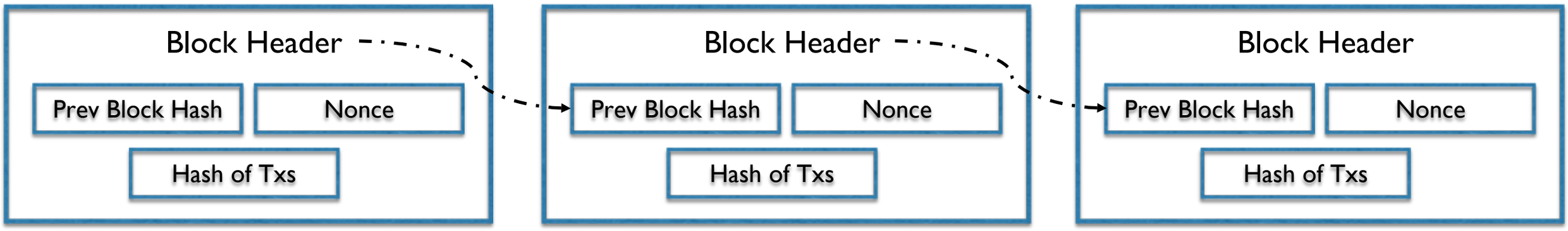
```
TARGET = (65535 << 208) / DIFFICULTY;
coinbase_nonce = 0;
while (1) {
      header = makeBlockHeader(transactions, coinbase_nonce);
      for (header_nonce = 0; header_nonce < (1 << 32); header_nonce++){
            if (SHA256(SHA256(makeBlock(header, header_nonce))) <
      TARGET)
                  break; //block found!
      }
      coinbase_nonce++;
}
```

Figure 5.6 : CPU mining pseudocode.

Block Header

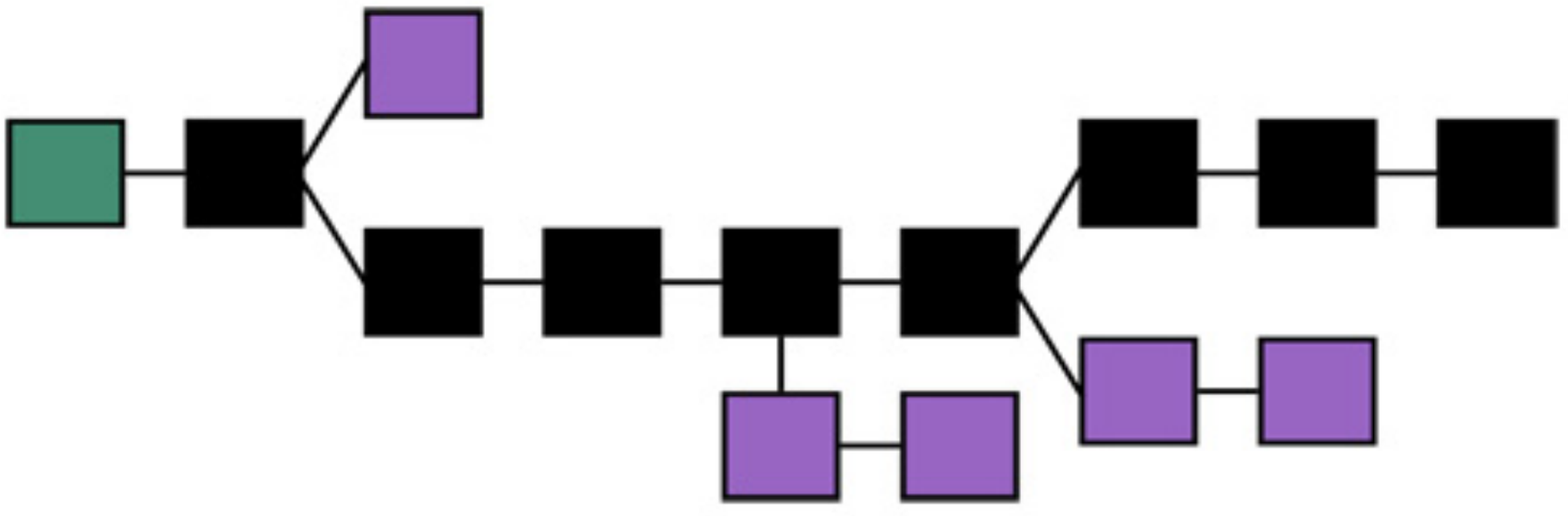


Chain of Blocks



The Longest Chain Wins

- What if there's a fork?
  - The longest chain wins (the chain with the most amount of work)
- Require majority to be honest
  - O.w., can create fork to double spend



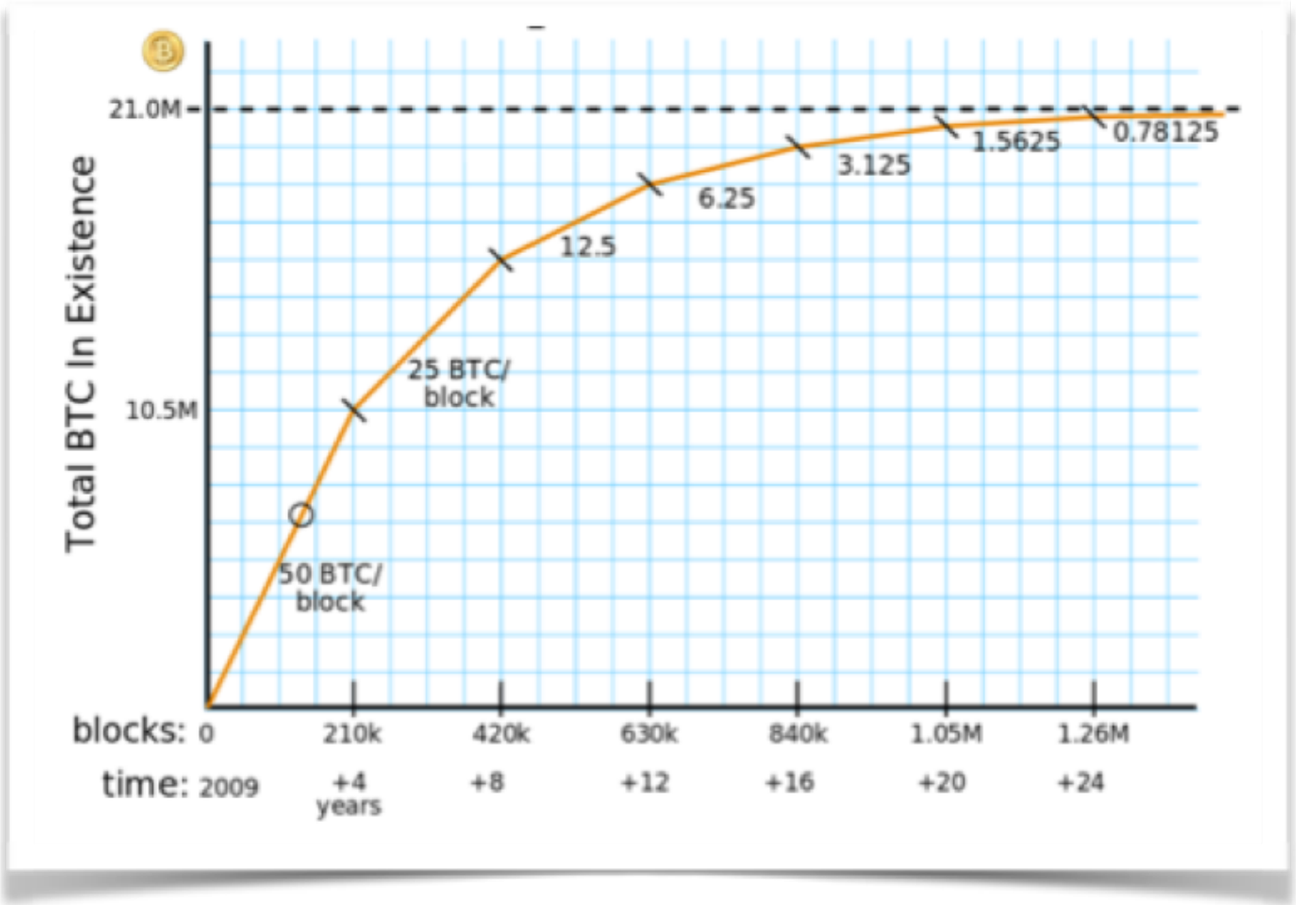
Why should miners mine?

- Bitcoin is a *lottery*!
- Whichever miner solves the hash problem first gets a reward
  - Allowed to assign reward as a special transaction in mined block
  - Today, 12.5 BTC
  - (Miner also gets transaction fees, but these tend to be smaller)

Block reward is how Bitcoin are created!

Bitcoin creation schedule

- Block mined about once every 10 minutes
- 21 million BTC will be produced over system lifetime
- Intentionally *anti-inflationary*



Courtesy:
Brian Warner

Observe

- Massive amount of computing in network
  - Whole community pulls slot machine handle more than 100,000,000,000,000,000,000,000 times per block!
- Only Bitcoin network capable of solving puzzle
  - Massive “proof of work”
  - Not easy for an attacker to compete
- Bitcoin secured by the computational power of its network

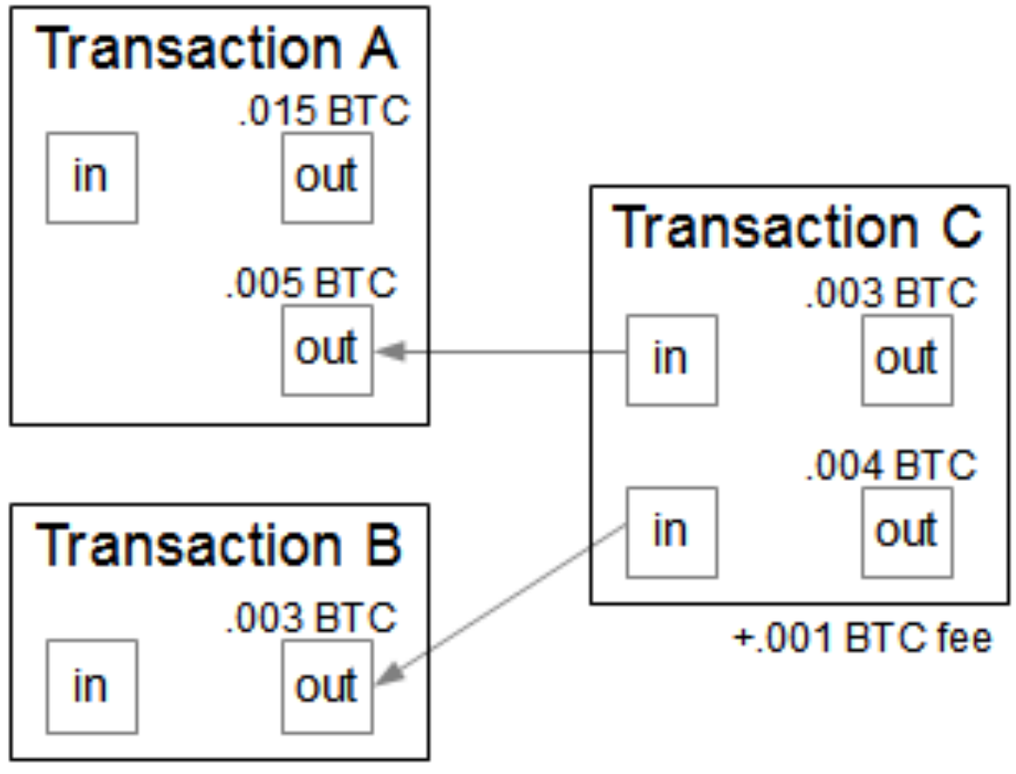
Transaction lifecycle:

What happens when you send money from wallet?

- You scan QR code—get address *R* of receiver.
- You choose transfer amount.
- Your wallet uses your private key (SK) to digitally sign transaction.
- Your wallet broadcasts transaction to Bitcoin network / miners ("I'm sending X BTC to *R*").
- Miners pick up your transaction.
- A successful miner includes your transaction in a block.
- Your transaction is on the blockchain!
- The whole world knows you sent X BTC to address *R*.

Blockchain structure

- Because full chain is a complete ledger / history of *all* transactions…
- Computing over the full block chain reveals the state / ownership of all BTC
- No explicit "account balances"
- Structured in terms of transactions



[Figure source: http://www.righto.com/2014/02/bitcoins-hard-way-using-raw-bitcoin.html; Hi, Ken!]

Bitcoin nodes and network

Bitcoin relies on an underlying network of *full nodes*

GLOBAL BITCOIN NODES DISTRIBUTION

Reachable nodes as of Wed Oct 26 2016 19:44:01 GMT-0400 (EDT).

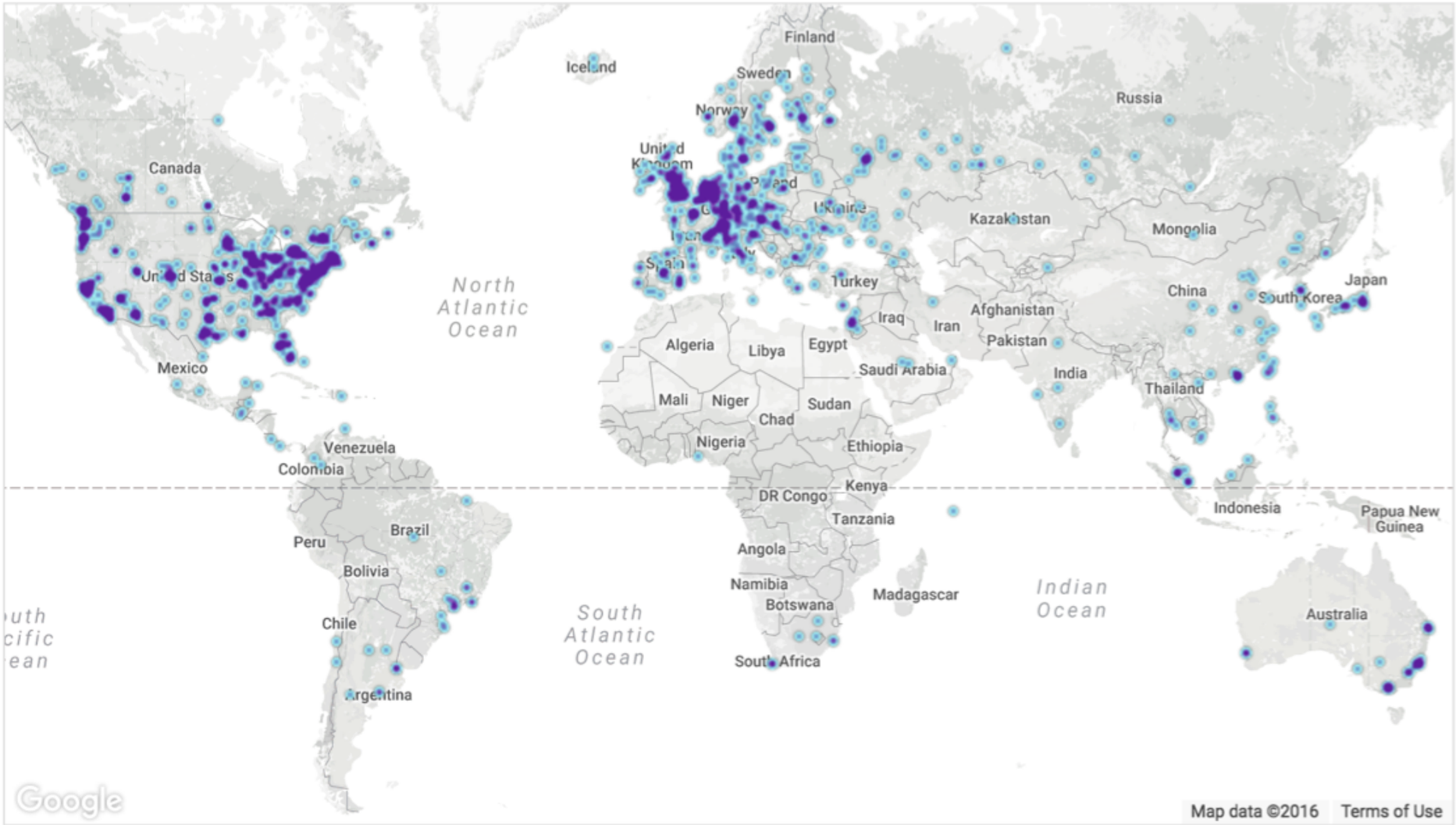
5274 NODES

24-hour charts »

Top 10 countries with their respective number of reachable nodes are as follow.

RANK	COUNTRY	NODES
1	United States	1470 (27.87%)
2	Germany	918 (17.41%)
3	France	447 (8.48%)
4	Netherlands	300 (5.69%)
5	Canada	245 (4.65%)
6	United Kingdom	213 (4.04%)
7	China	182 (3.45%)
8	n/a	155 (2.94%)
9	Russian Federation	125 (2.37%)
10	Switzerland	85 (1.61%)

More (84) »



Map shows concentration of reachable Bitcoin nodes found in countries around the world.

LIVE MAP

Routing functionality

- Transactions and blocks broadcast to *entire network of full nodes*
- Rebroadcast protocol
  - Each node transmits to 8 other (randomly selected) nodes
  - TCP on port 8333

Full nodes

- Store entire blockchain
- Enforce consensus rules, ensuring mined blocks adhere to
  - 12.5 BTC reward
  - Correct signatures on transactions
  - BTC not double-spent
  - Etc., etc.

Bitcoin's nice properties

- Completely portable
  - ☐ Hard asset with qualities like gold—can't be easily confiscated
- Decentralized
  - ☐ Cross-border remittances
- Low transaction fees + no middleman
  - ☐ Low-fee payments

Bitcoin Power Consumption

- Hundreds of millions of dollars in computing hardware in Bitcoin ecosystem
- Power consumption: over 5000MW
- In Oct 2017 alone, Bitcoin mining electricity consumption is estimated to have increased by **29.98%**
- If it keeps increasing at this rate, Bitcoin mining will **consume all the world's electricity by February 2020**.
- Estimated annualised global mining revenues: **$7.2 billion USD (£5.4 billion)**
- Estimated global mining costs: **$1.5 billion USD (£1.1 billion)**
- Number of Americans who could be powered by bitcoin mining: **2.4 million** (more than the population of Houston

Bitcoin Limitations

- Scaling limitations
  - 3.3-7 transactions per second
  - Long confirmation time:
    - Block mined only once every 10 minutes
    - Often need to wait for a number of blocks (e.g., 6) deep to confirm transaction
- Privacy limitations
  - Linkability; transaction amount is known

Cryptocurrency

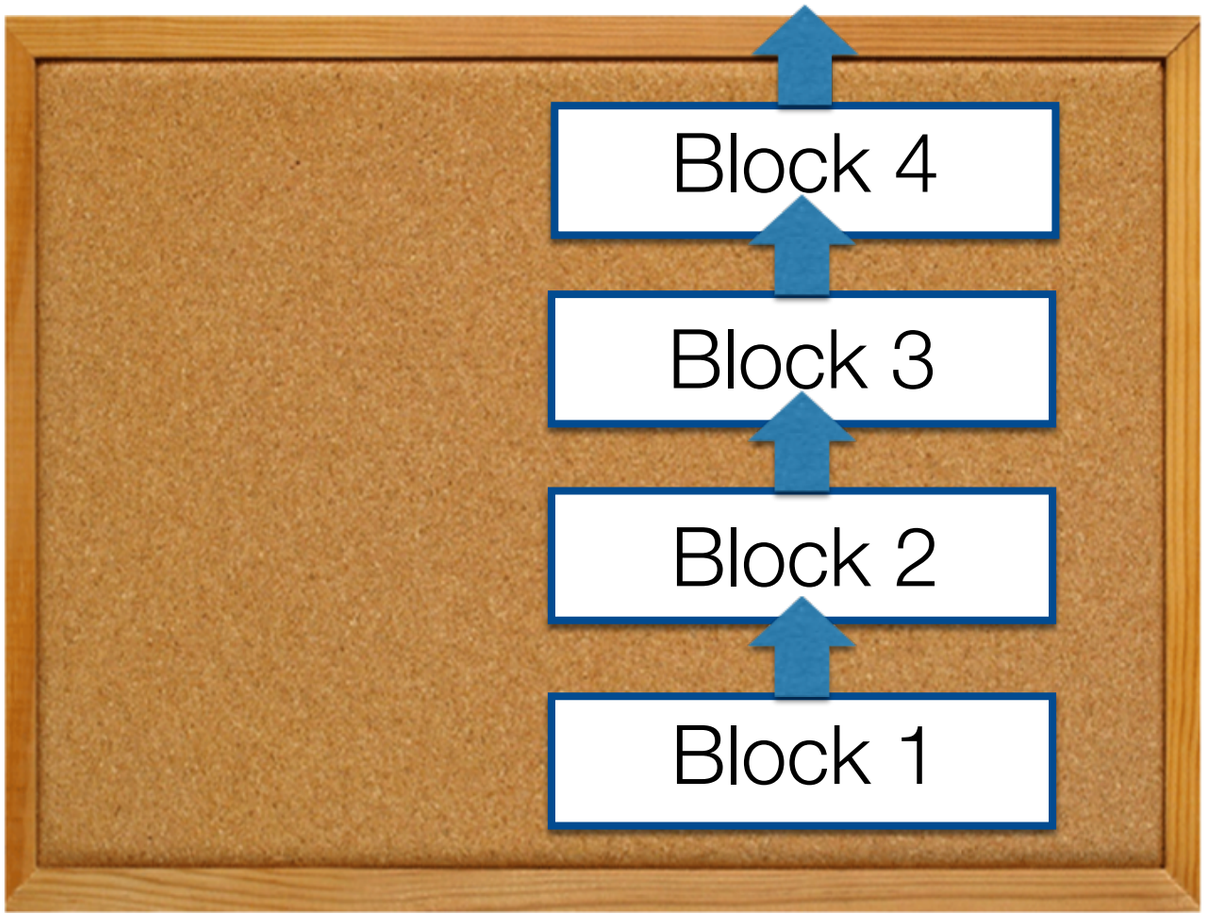
≠

Blockchain

What is a blockchain?

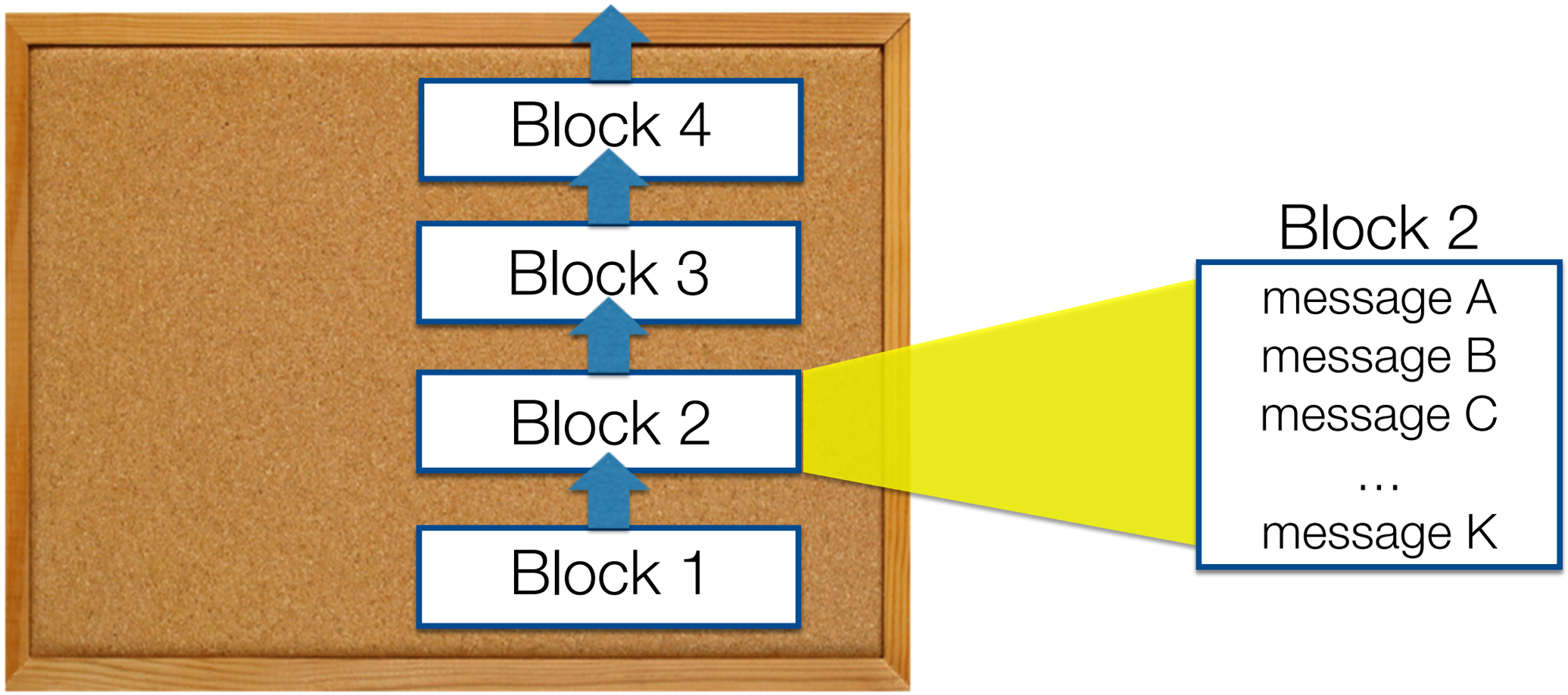
Blockchains: Abstraction

Blockchains: Abstraction



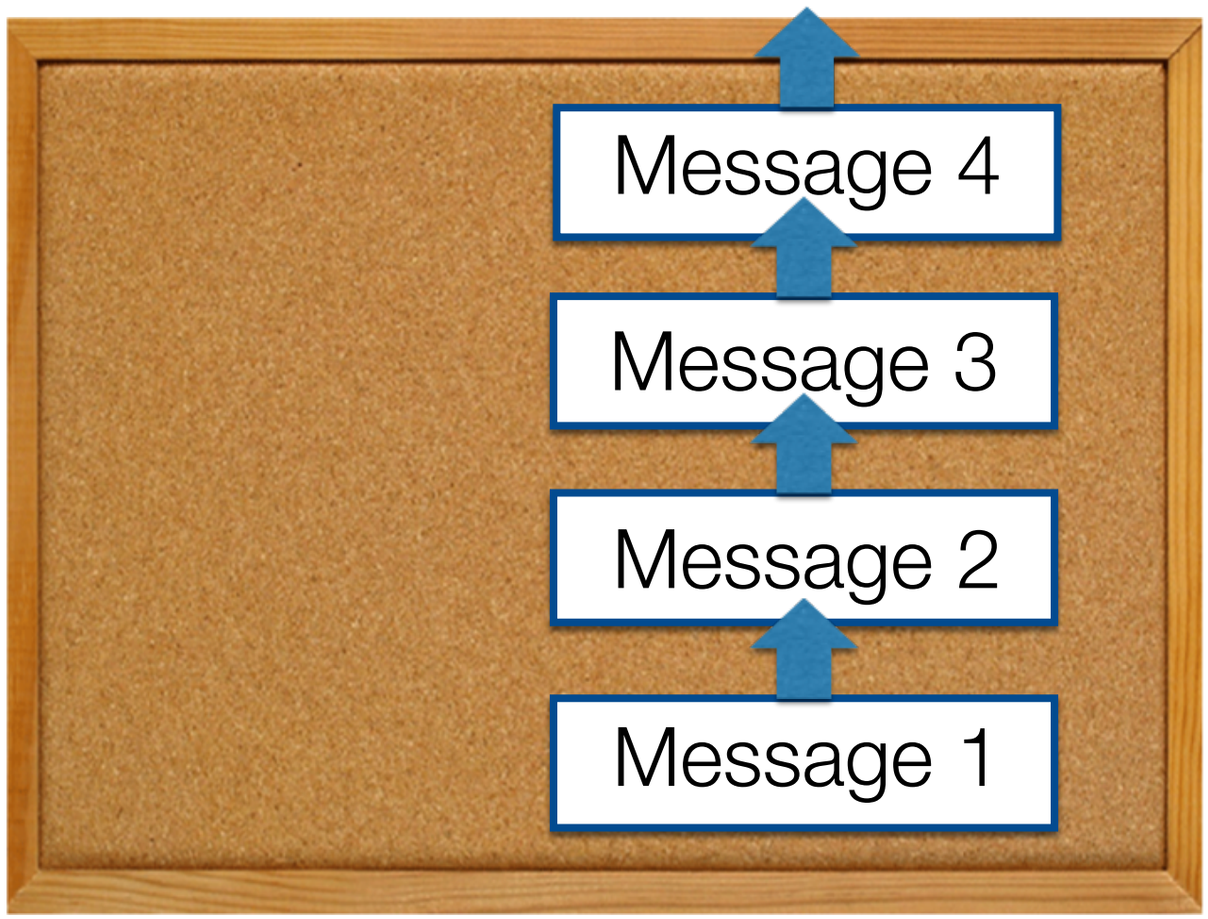
Blockchains: Abstraction

#1 Strict ordering of messages



Blockchains: Abstraction

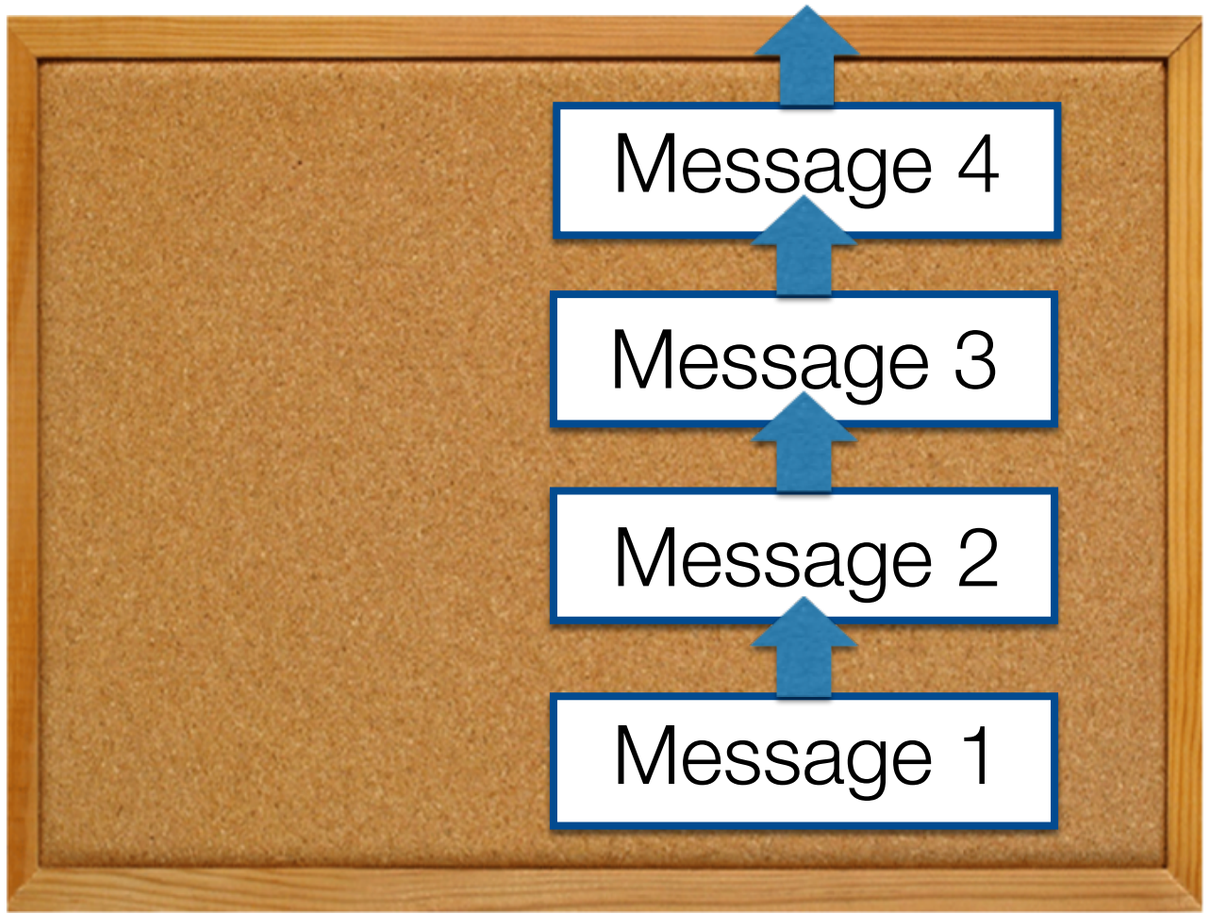
#1 Strict ordering of messages



Blockchains: Abstraction

#2 Rule-based write, global read

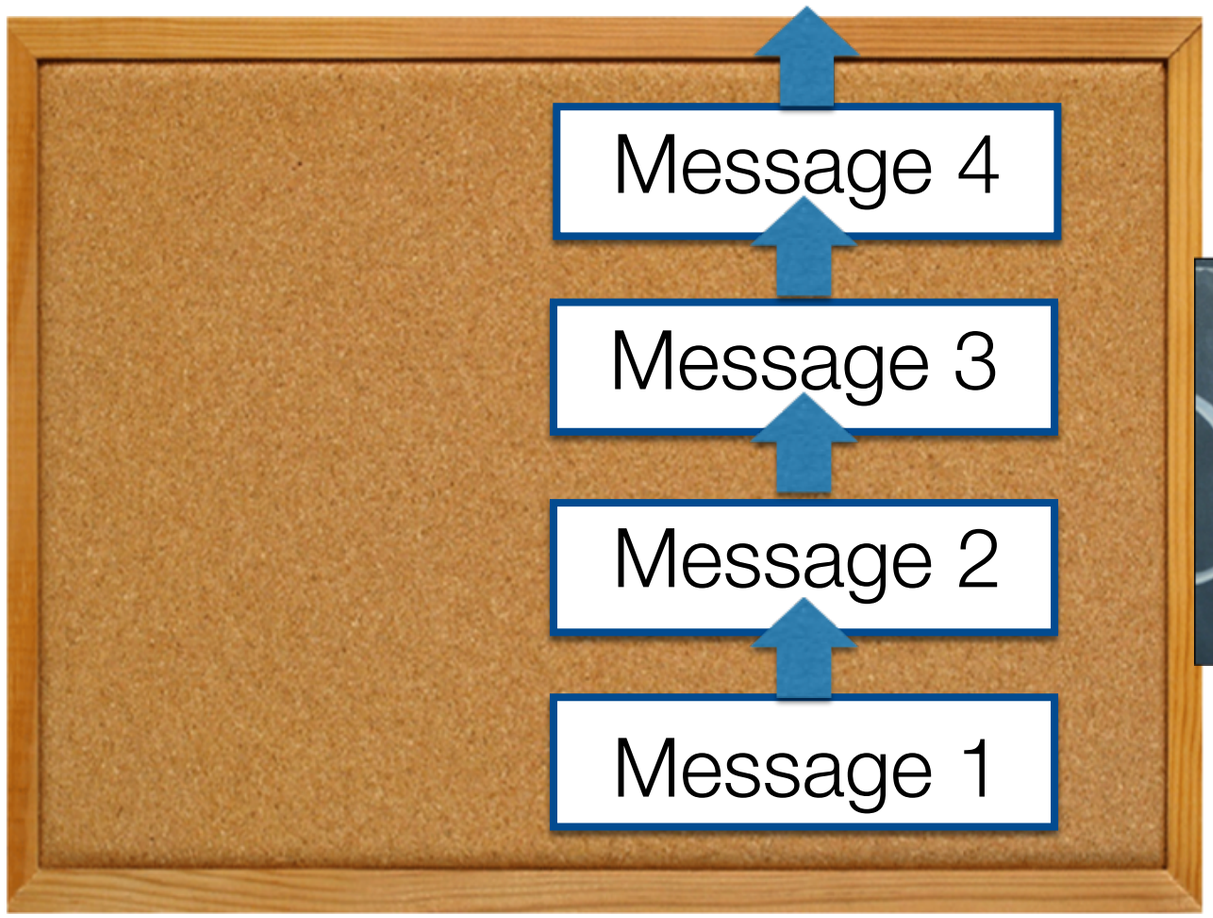
Write Permission: Rule-based



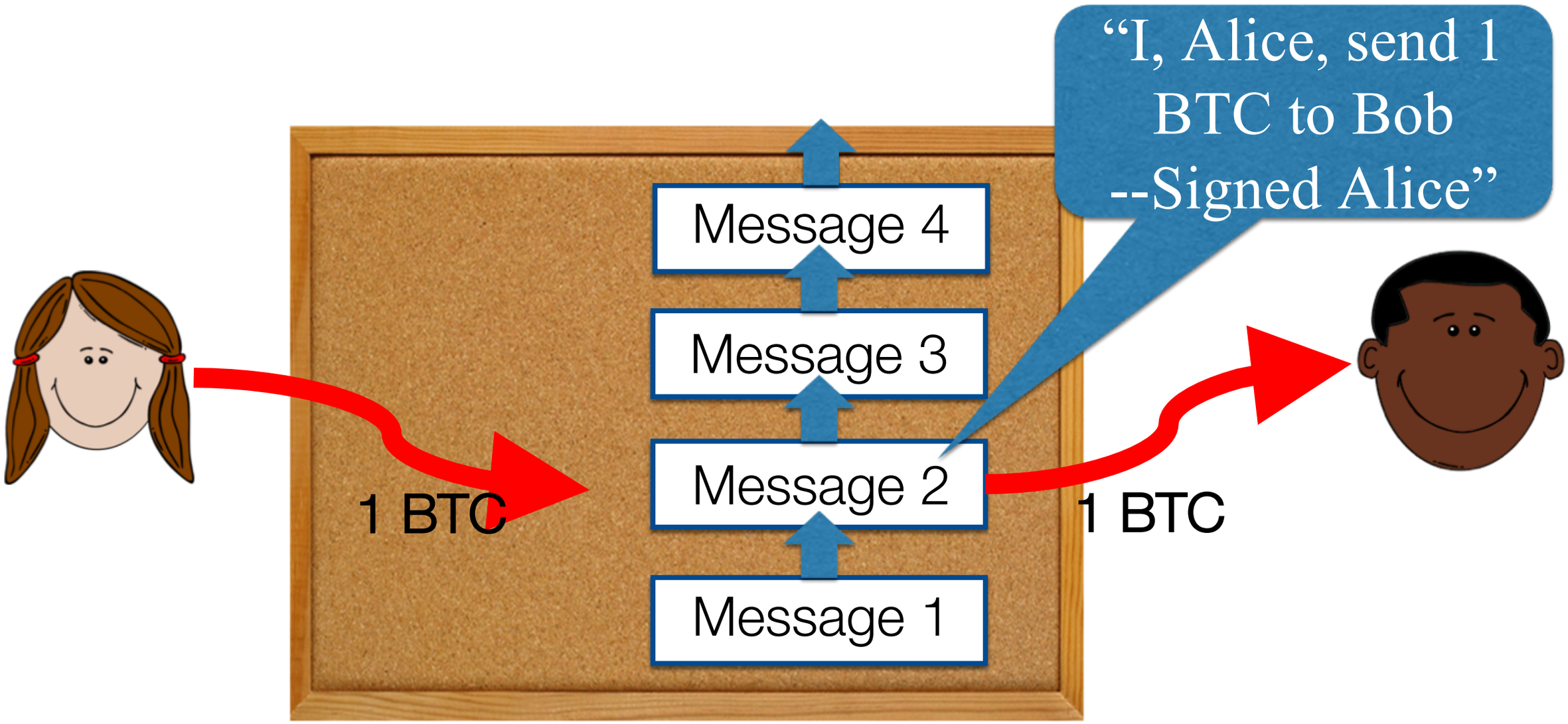
Read Permission:

Blockchains: Abstraction

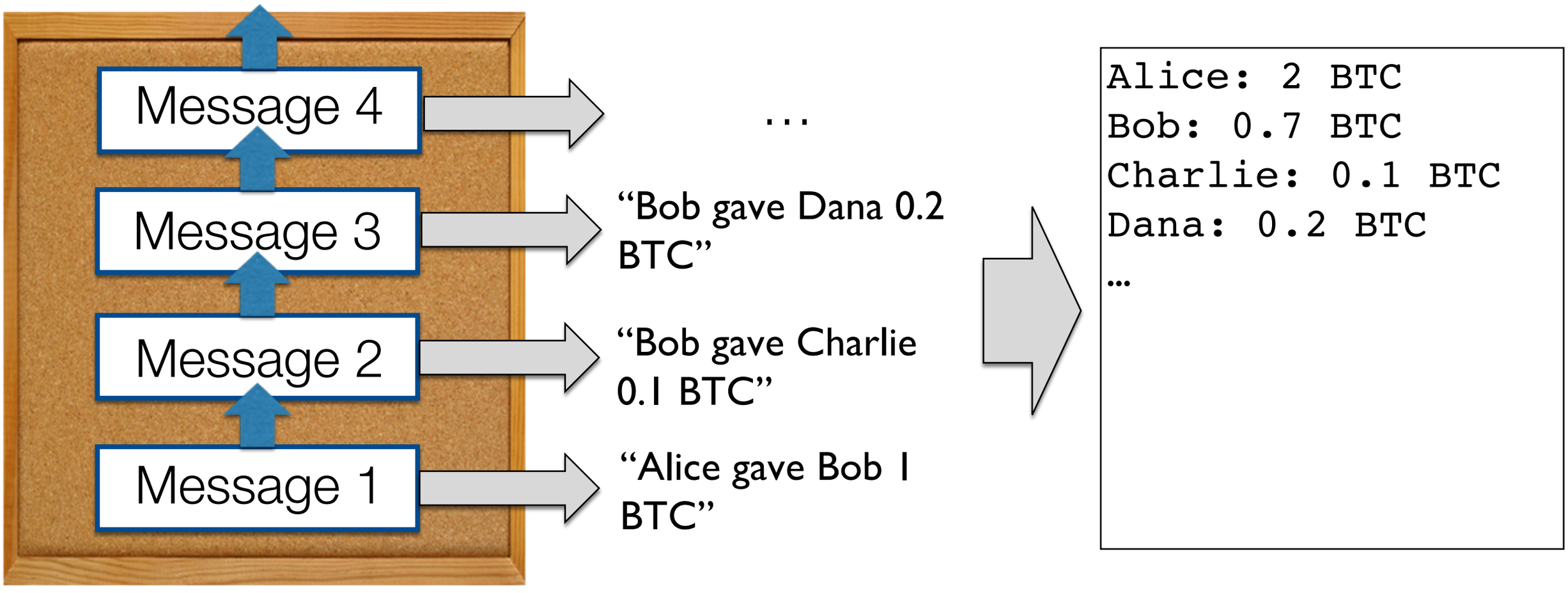
#3 No message modification



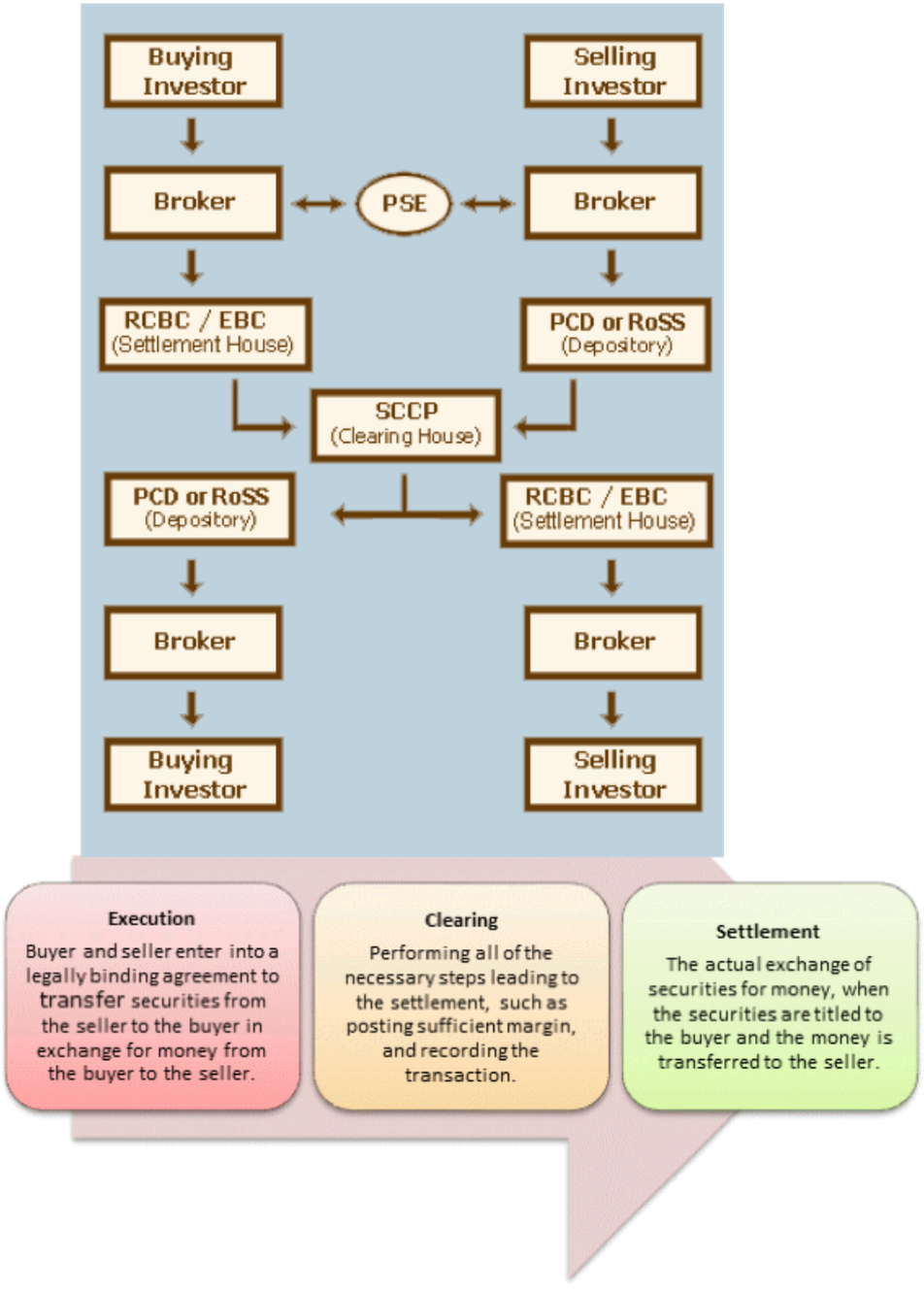
Power of the Abstraction



Power of the Abstraction

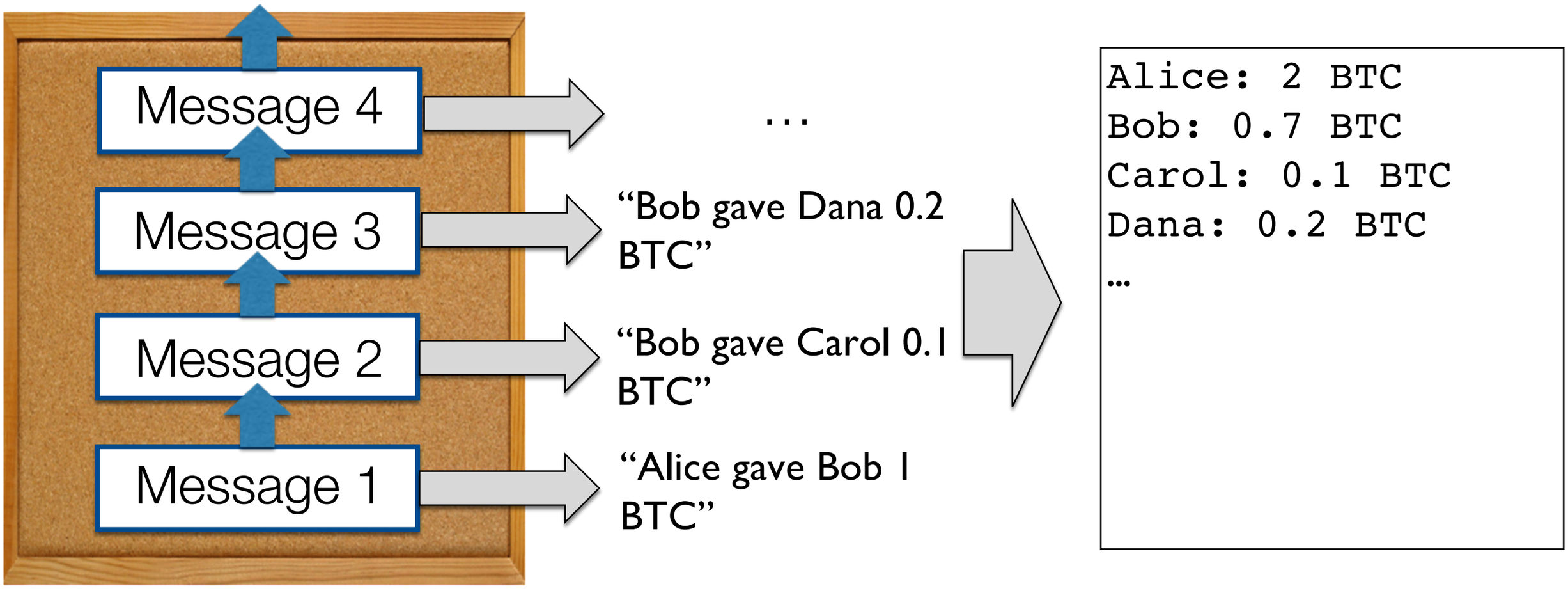


Compare: Execution, clearing, and settlement

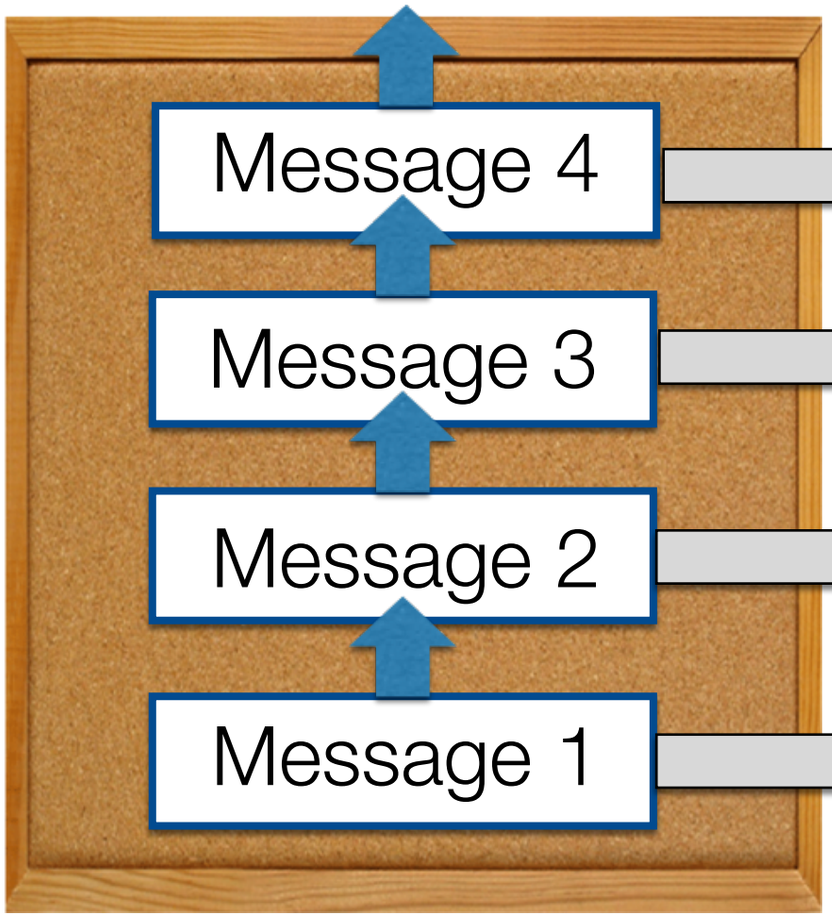


- For transfer of financial instruments
- Up to three days to complete (T+3)
- Many middlemen
- Fragmented records
- Difficult to audit

Blockchains are much faster…



and more transparent…



…

“Bob gave Dana 0.2 BTC”

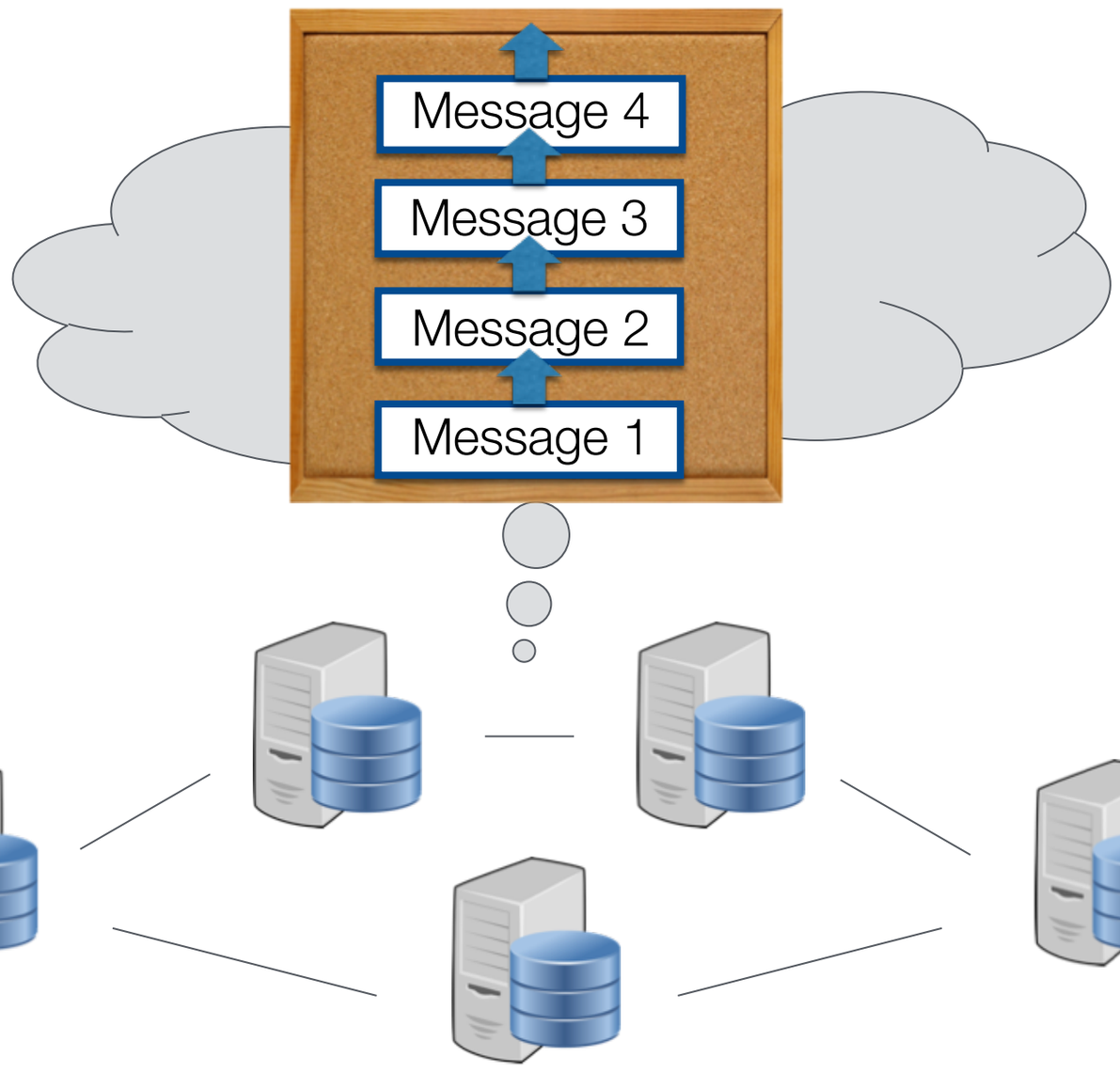
“Bob gave Carol 0.1 BTC”

“Alice gave Bob 1 BTC”

```
Alice: 2 BTC
Bob: 0.7 BTC
Carol: 0.1 BTC
Dana: 0.2 BTC
…
```

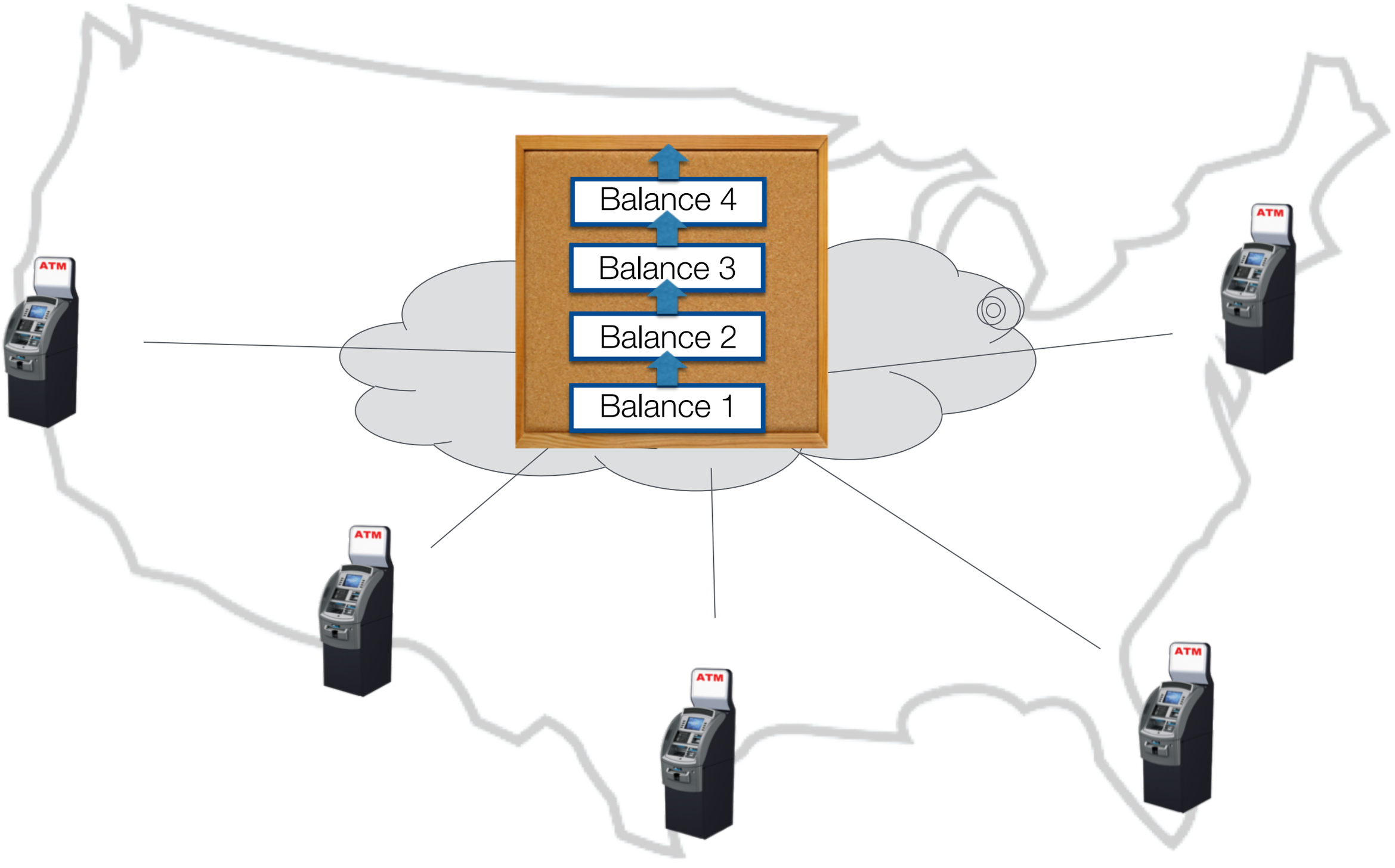
Blockchain is
an opportunity to build
resilient by design
infrastructure

A blockchain is a ***Distributed Bulletin Board***



Consistency - Every server gives the same result

Availability **-** New transactions are processed (quickly)


Balance 4
Balance 3
Balance 2
Balance 1
ATM
ATM
ATM
ATM
ATM

ATM heist clears $1 million exploiting Citigroup e-payment flaw

Scam worked by simultaneously withdrawing funds from ATM kiosks in 11 casinos.

by **Dan Goodin** - Oct 30, 2012 5:05pm EDT

Alice: $300

Alice

Withdraw $500

Does Alice's account have $500?

OK, subtract $500 and dispense cash

ATM heist clears $1 million exploiting Citigroup e-payment flaw

Scam worked by simultaneously withdrawing funds from ATM kiosks in 11 casinos.

by **Dan Goodin** - Oct 30, 2012 5:05pm EDT

Alice: $-200!!!

Harrah's

BELLAGIO

Does Alice's account have $500?

OK, subtract $500 and dispense cash

Does Alice's account have $500?

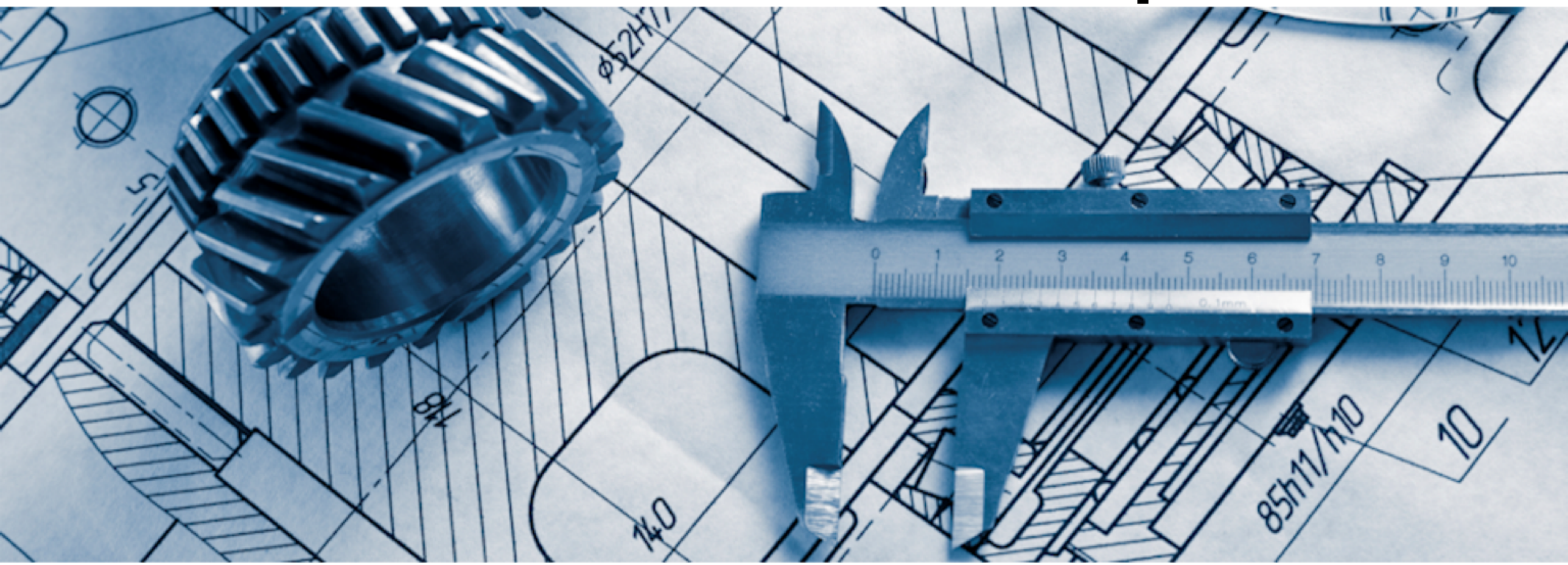
OK, subtract $500 and dispense cash

Distributed systems are notoriously difficult

"A distributed system is one in which the failure of a computer you didn't even know existed can render your own computer unusable."

– Leslie Lamport, 1987

The good news - 30 years of science to draw upon



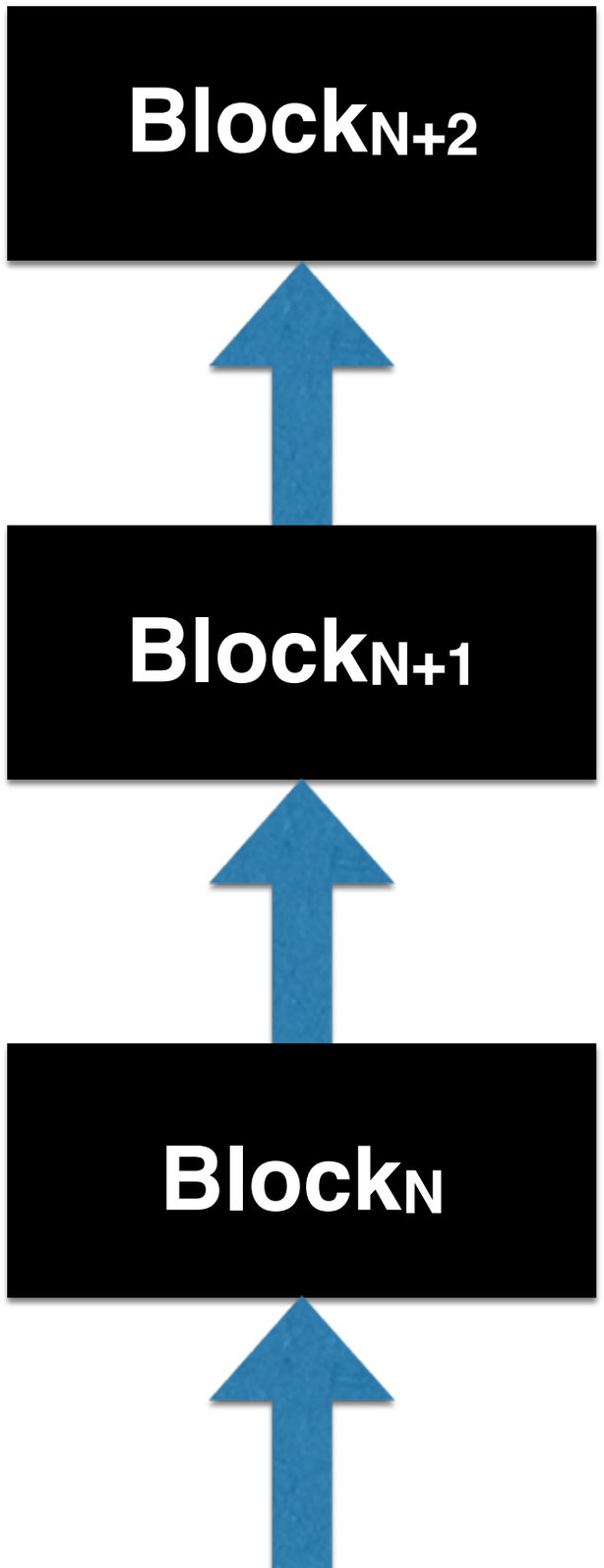
The 5 layers of blockchain architecture

Application:	transactions, smart contract language
View:	cached summary of the transaction log
Consensus:	the agreement-reaching engine
Storage:	bootstrapping new nodes, storing archival data
Network:	broadcasting transactions and blocks

Many Types of Blockchains

- Permissioned vs. Permissionless
- Proof of Work vs. Proof of X
  - Stake
  - Space
  - Elasped time; luck

The **blockchain** means much more than Bitcoin



- Blockchain is nebulous term…
- Generally refers to *ledger*
- Distributed, robust, publicly visible piece of memory
- Abstraction enables
  - Immutability; persistency
  - Transparency; frictionless;
- Good for things other than money!
  - Timestamping documents
  - Audit
  - Etc., etc.

Conclusion: remember the bulletin board abstraction