Blockchains:
What They Are and What They Can Do

Summit on Cyber Risks
ETH-Zurich
26 June 2017

Ari Juels

Professor,
Jacobs Institute, Cornell Tech
Co-Director,
Initiative for CryptoCcurrencies and Contracts (IC3)

What is the / ( ) blockchain?

Ethereum Charts

results using bitcoin tech

INNOVATION

Torrent of technical terms

Mining

Hard fork

Proof of work

Bitcoin

Permissionless

ethereum

Permissioned

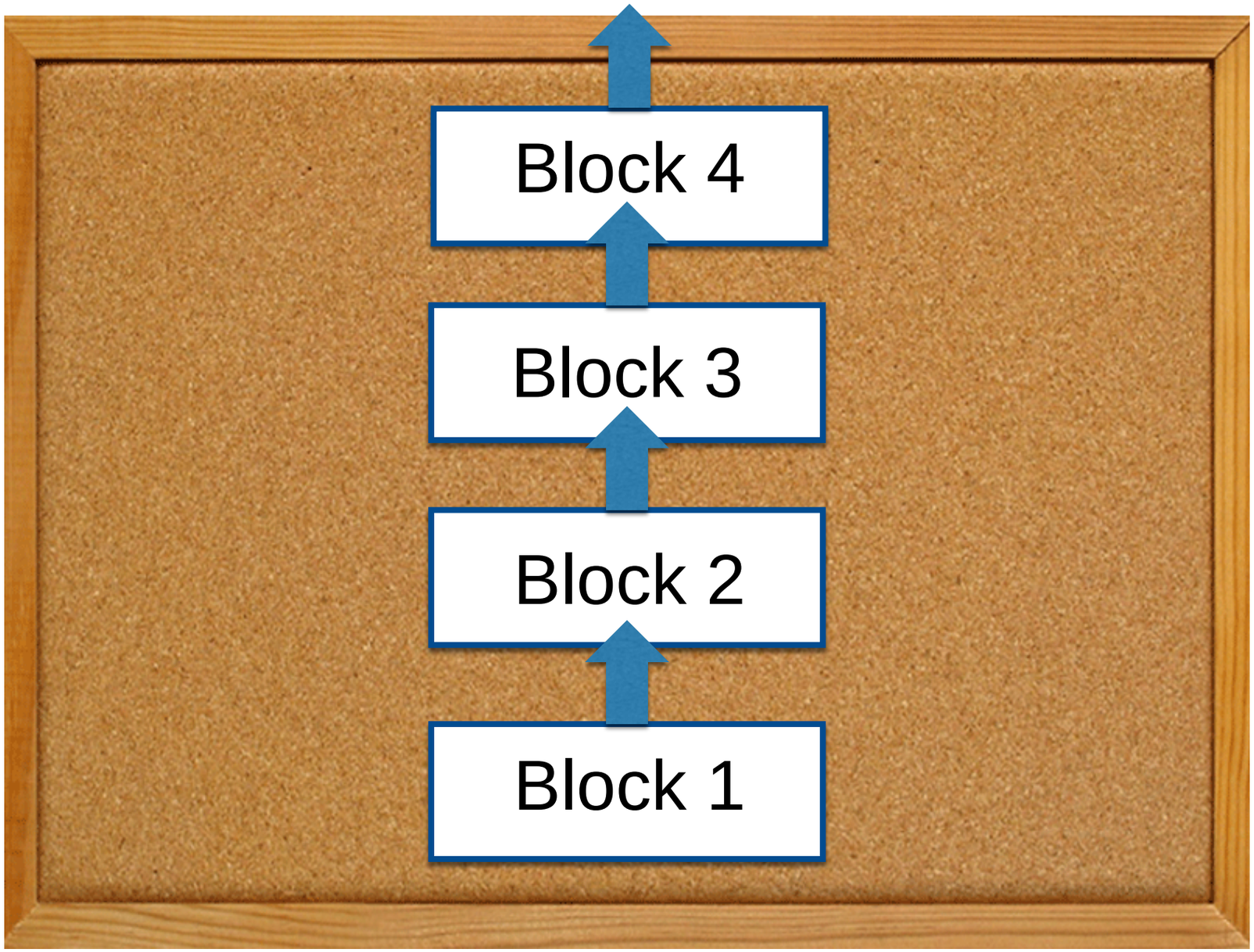
Byzantine Fault Tolerance

Hyperledger

Distributed Ledger Technology

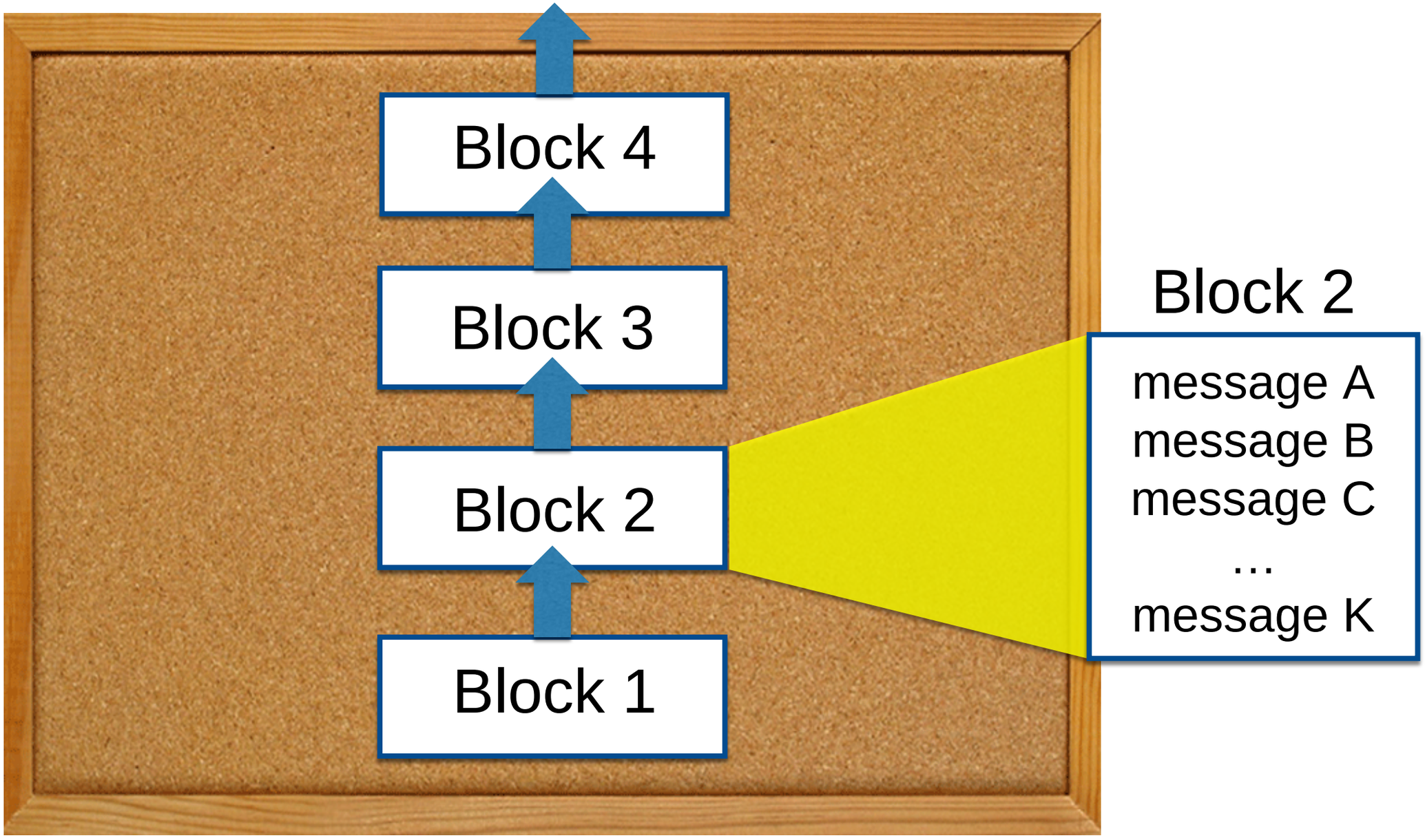
Blockchains: Abstraction

Blockchains: Abstraction



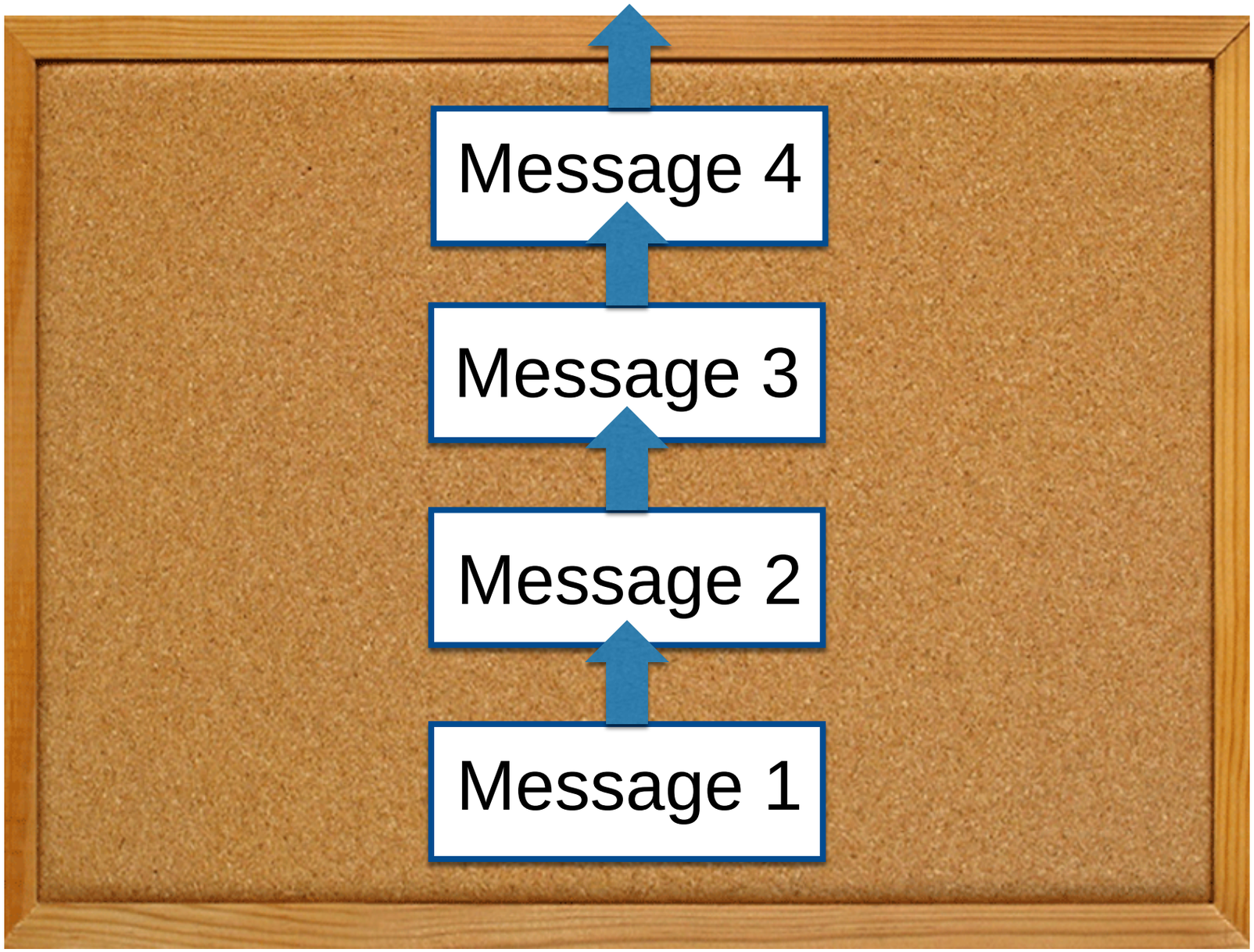
Blockchains: Abstraction

#1 Strict ordering of messages



Blockchains: Abstraction

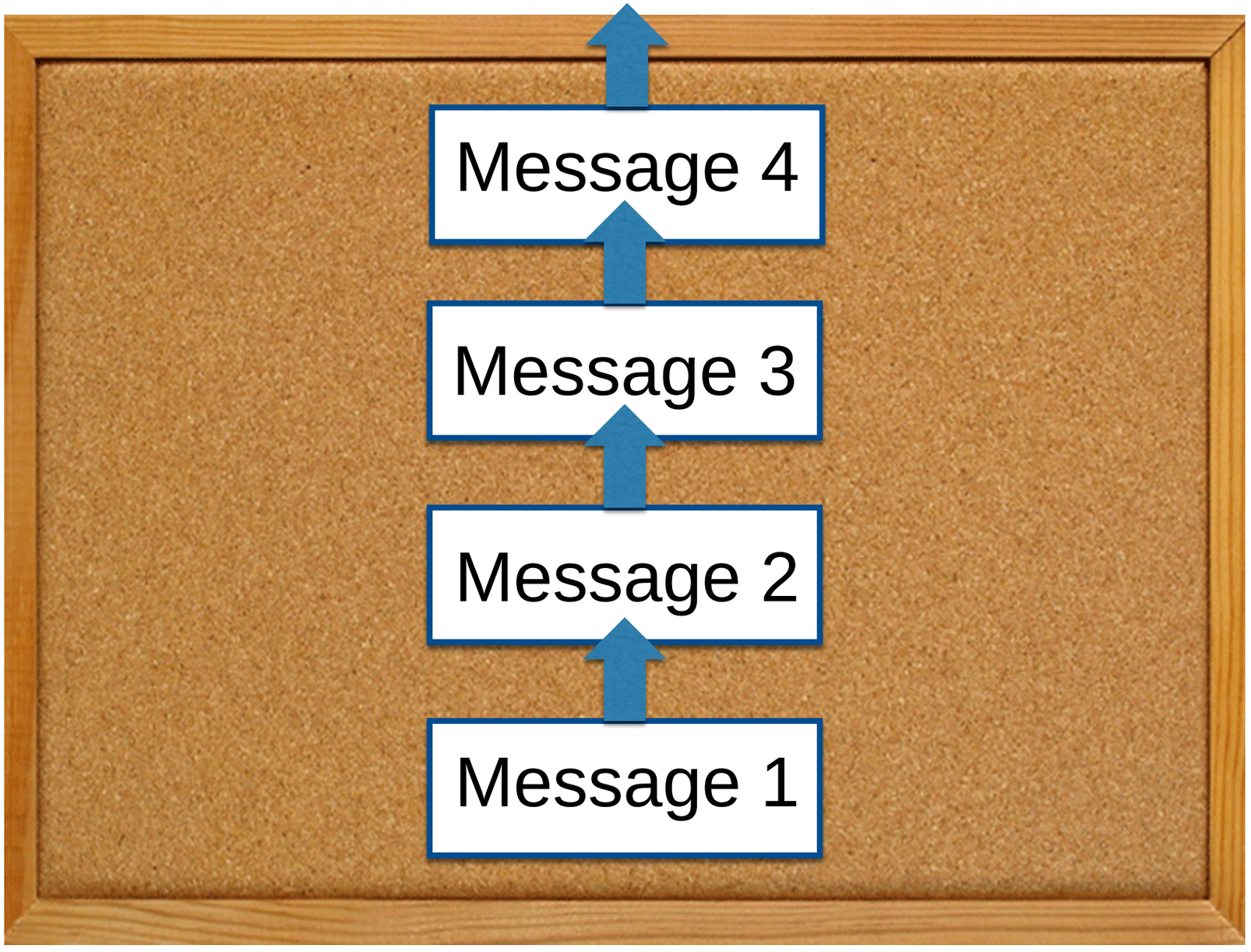
#1 Strict ordering of messages



Blockchains: Abstraction

#2 Rule-based write, global read

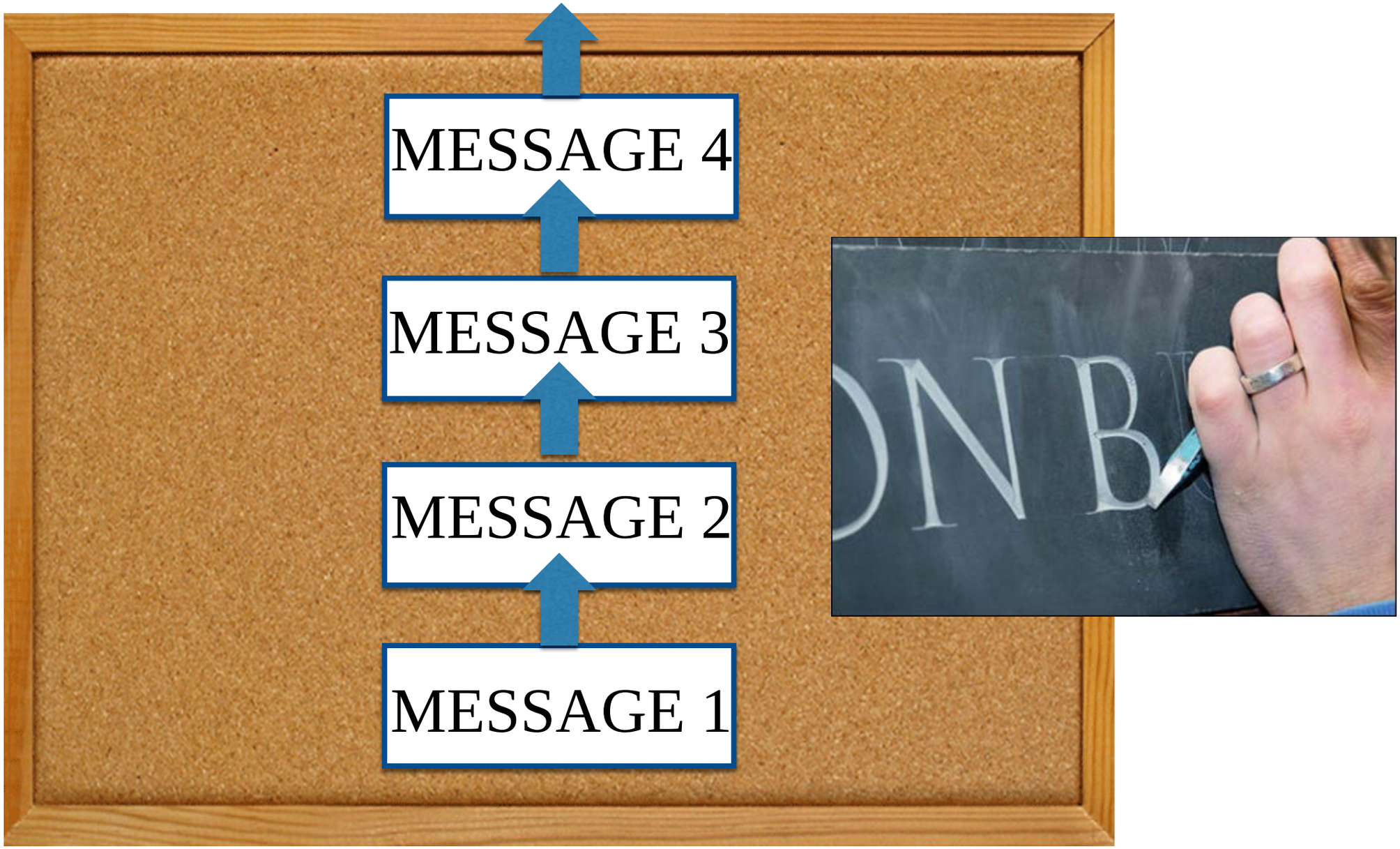
Write Permission: Rule-based



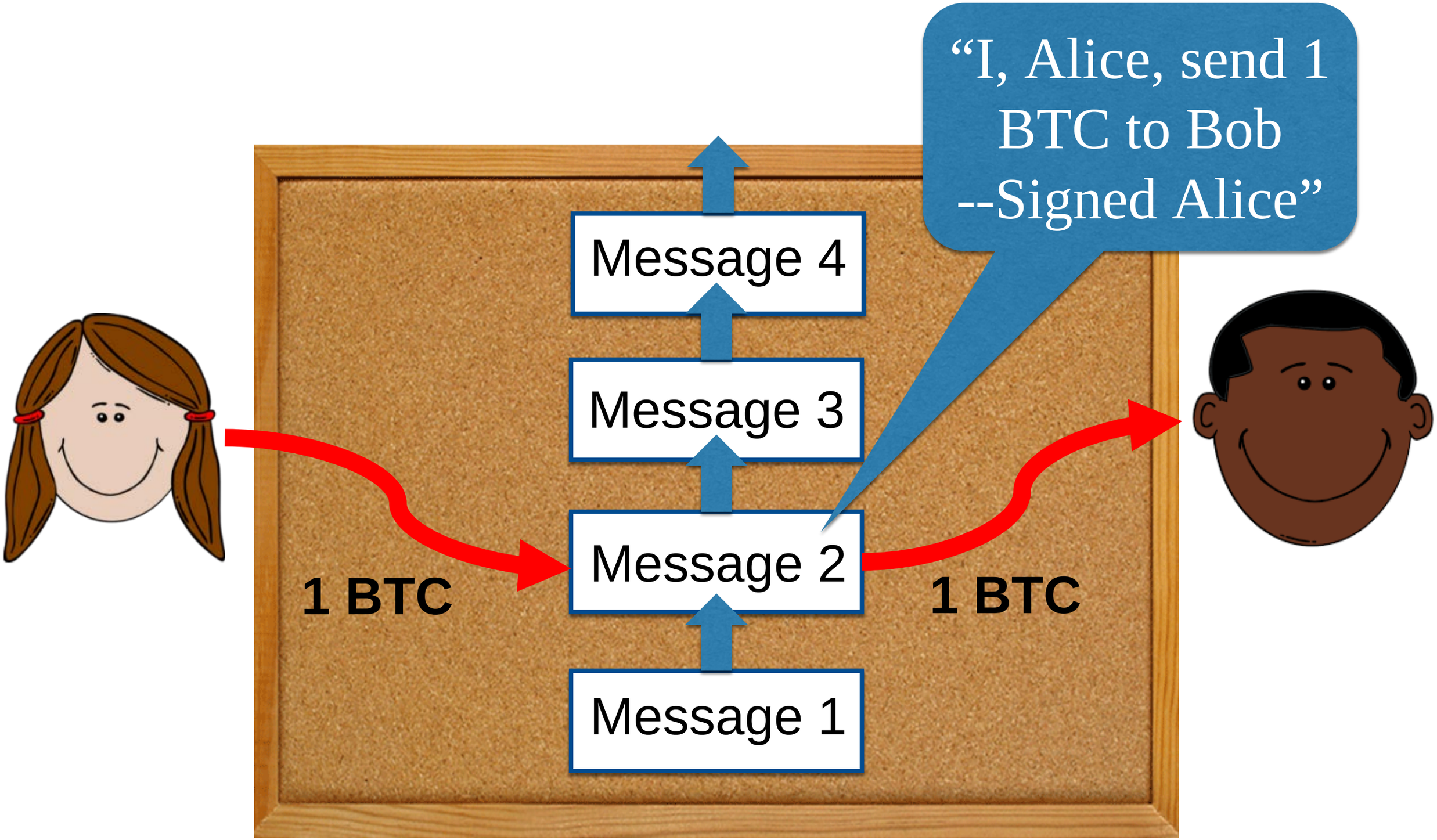
Read Permission:

Blockchains: Abstraction

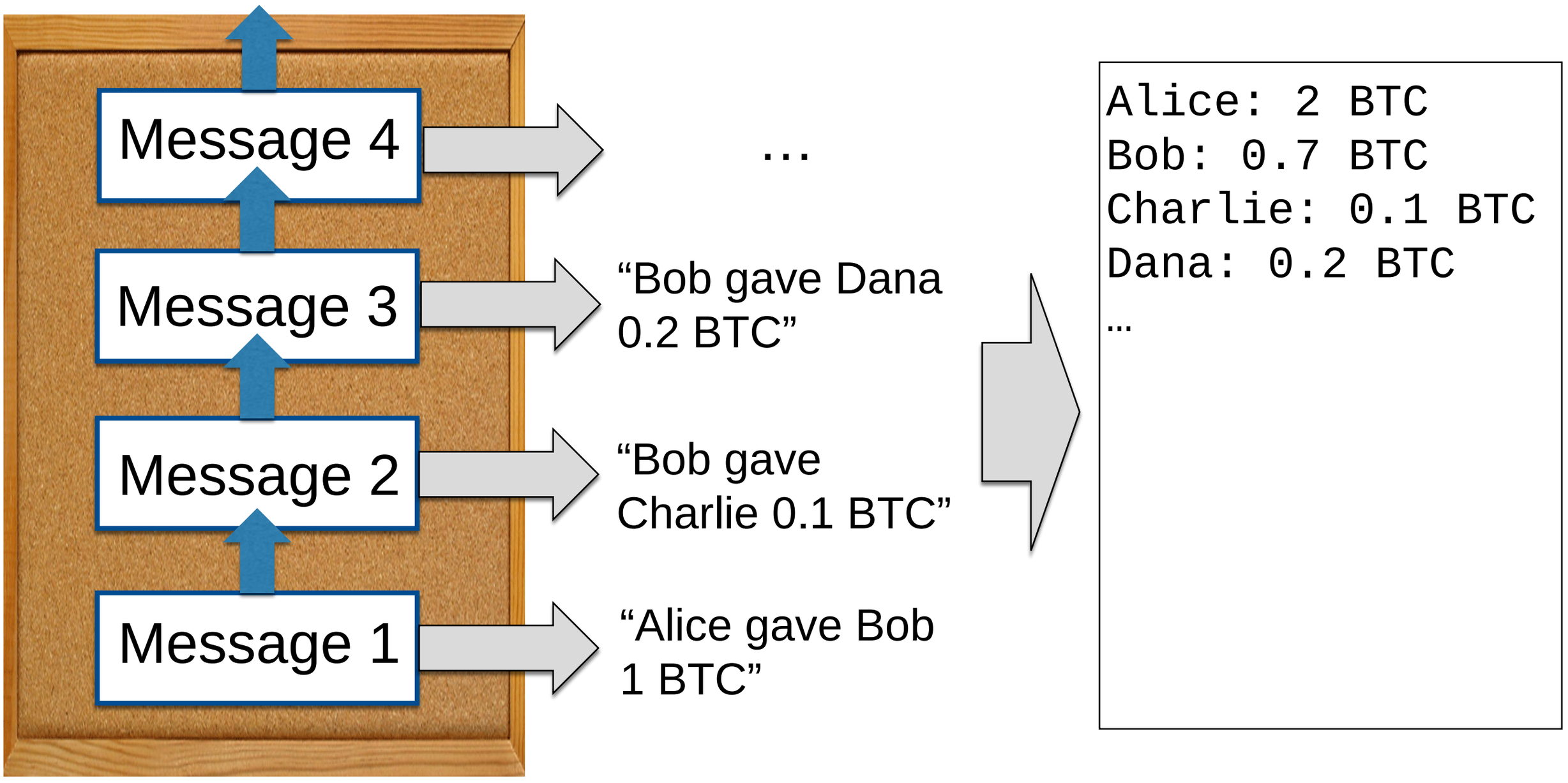
#3 No message modification



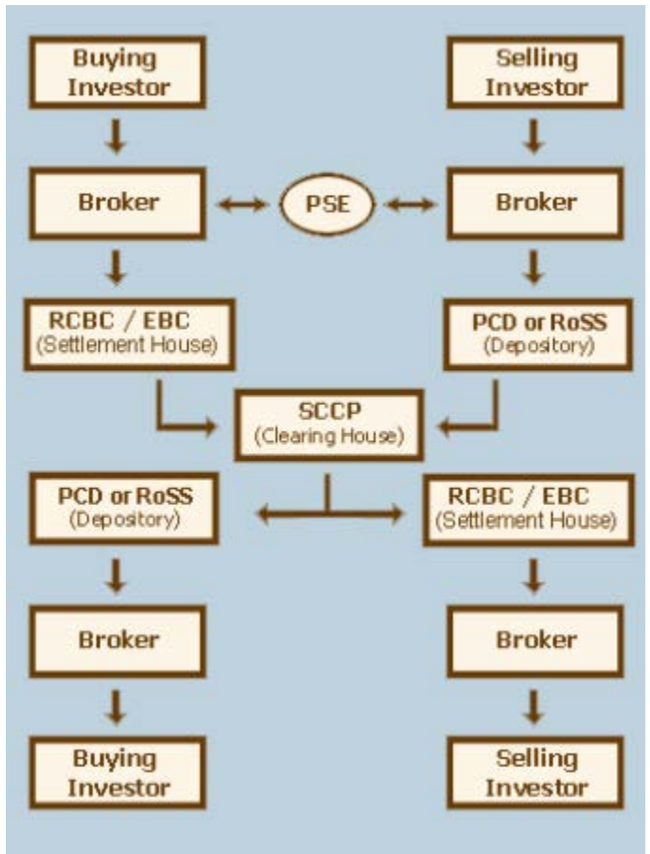
Power of the Abstraction

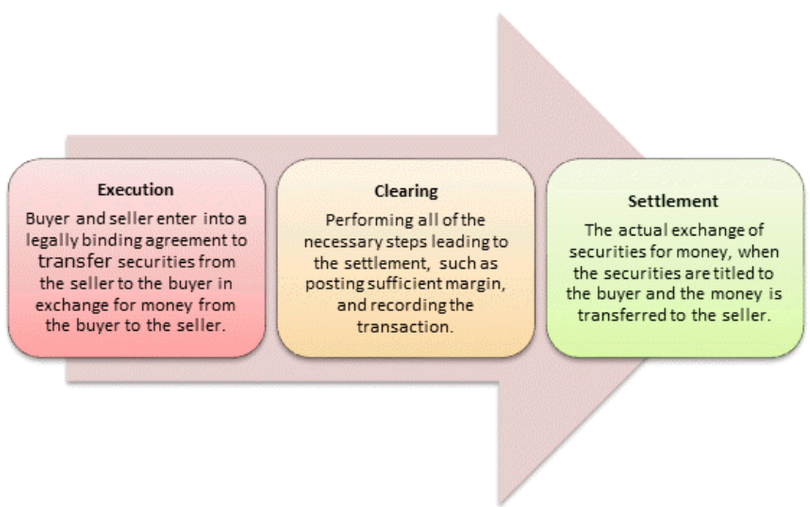


Power of the Abstraction



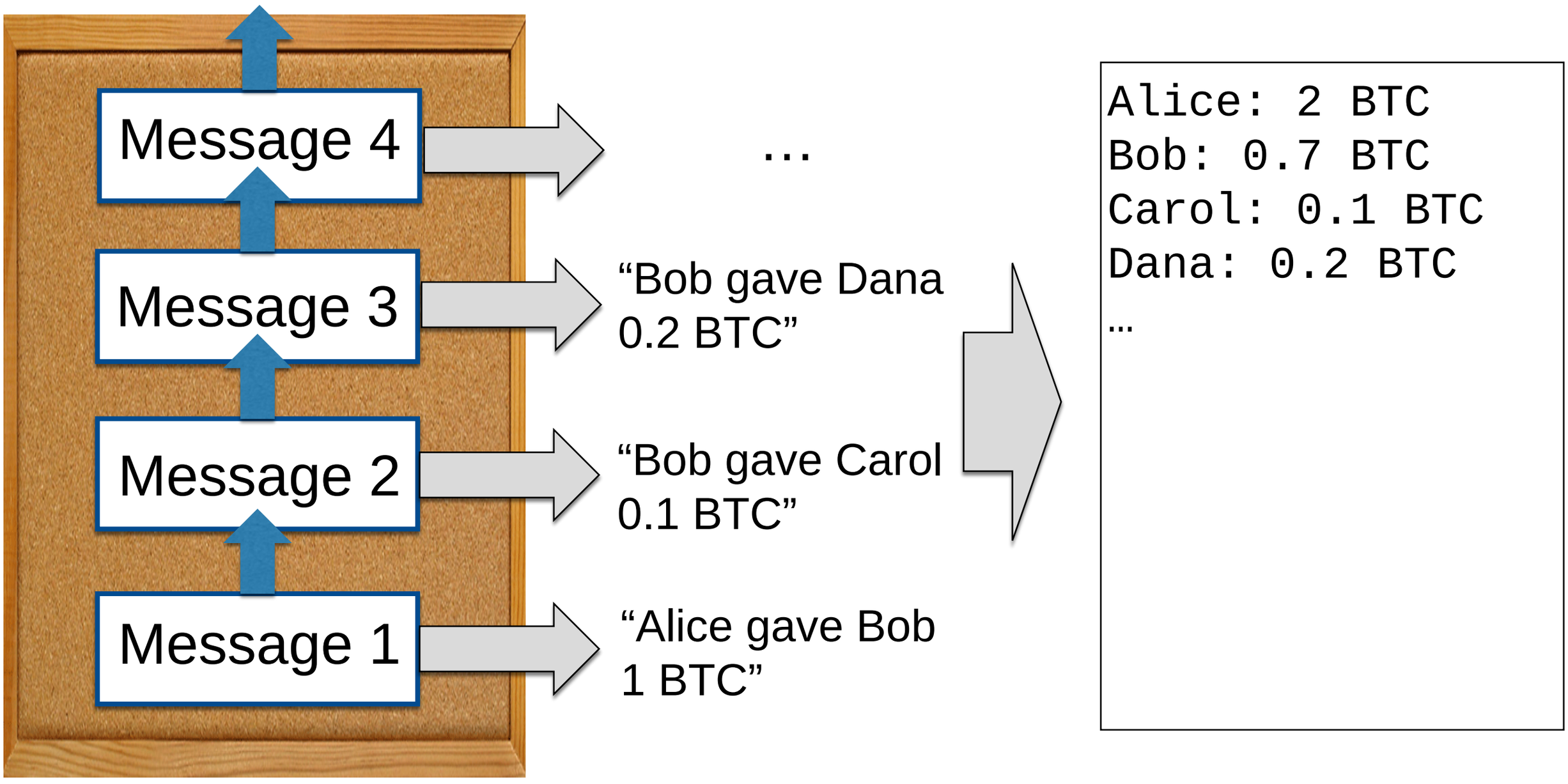
Compare: Execution, clearing, and settlement



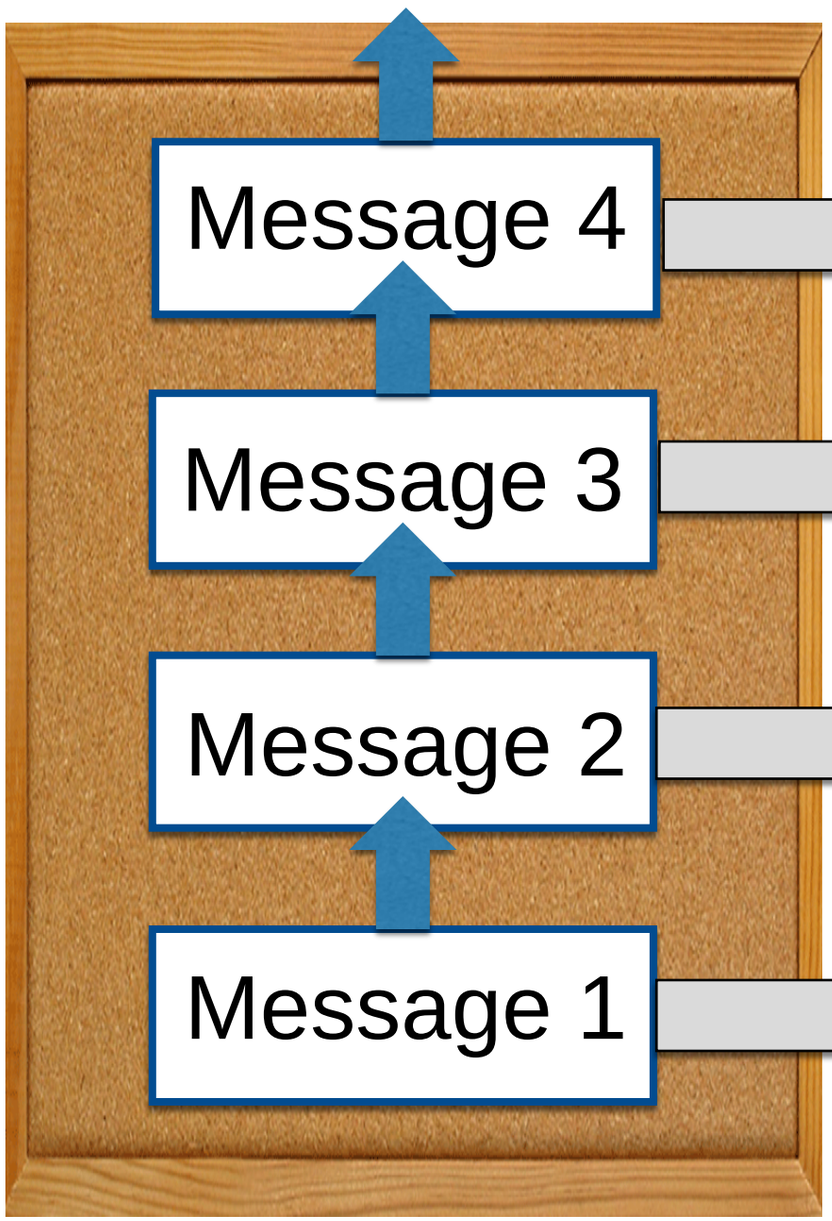


- For transfer of financial instruments
- Up to three days to complete (T+3)
- Many middlemen
- Fragmented records
- Difficult to audit

Blockchains are much faster…



and more transparent…



…

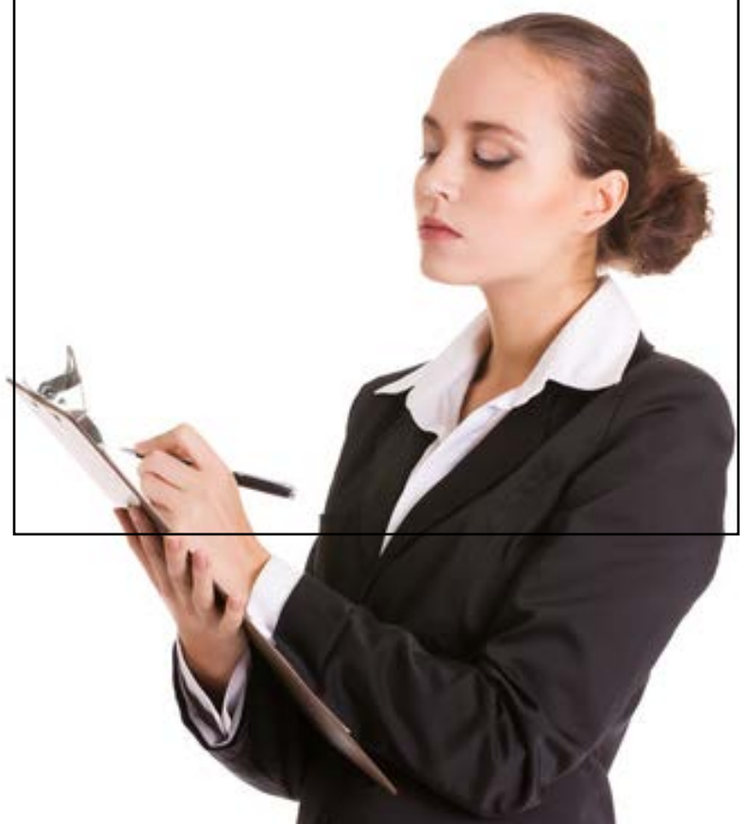
“Bob gave Dana 0.2 BTC”

“Bob gave Carol 0.1 BTC”

“Alice gave Bob 1 BTC”

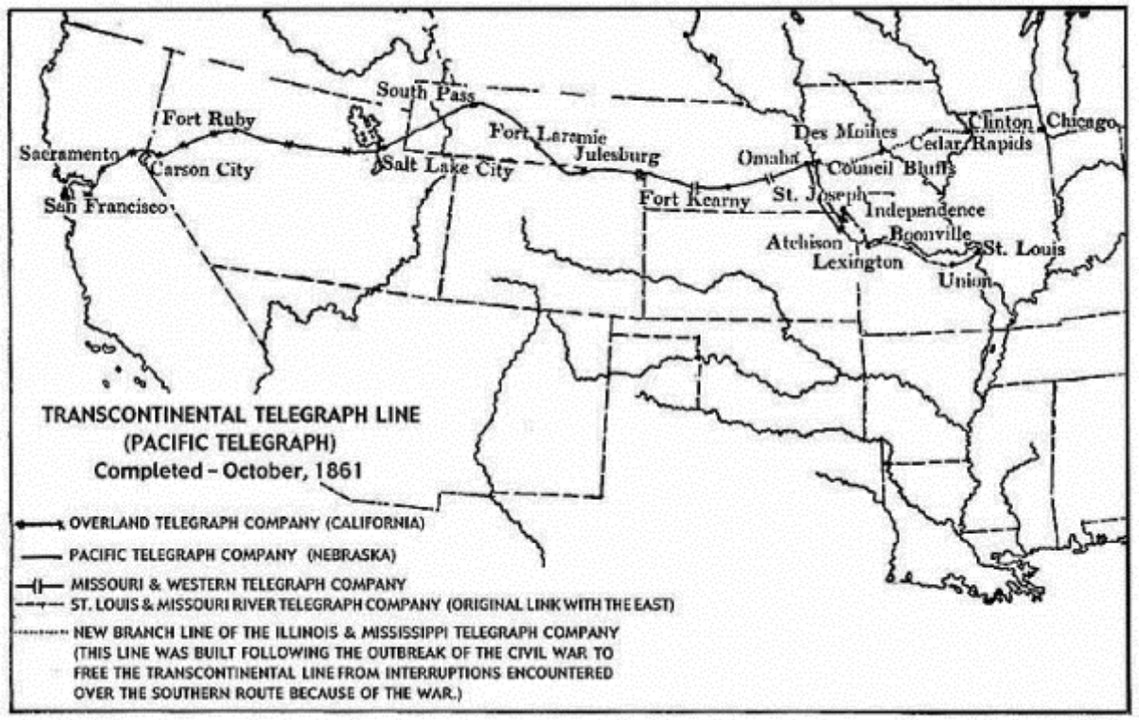
```
Alice: 2 BTC
Bob: 0.7 BTC
Carol: 0.1 BTC
Dana: 0.2 BTC

...
```



Mail delivery in 19th-century United States

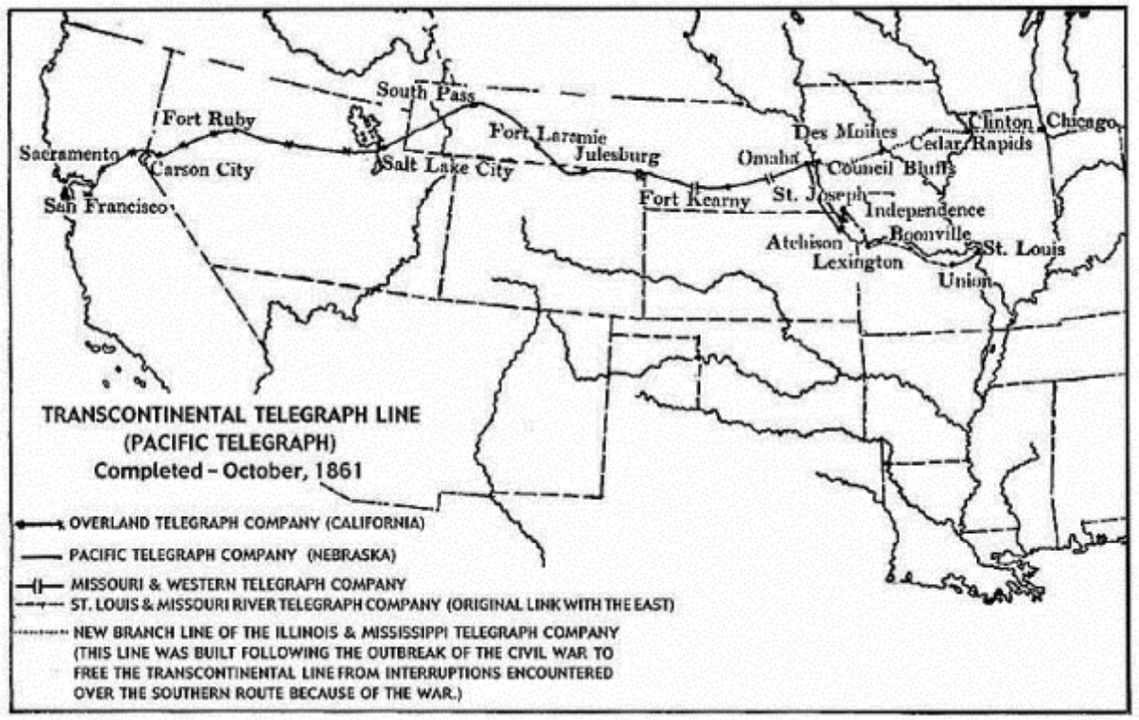
28 Oct. 1861



26 Oct. 1861

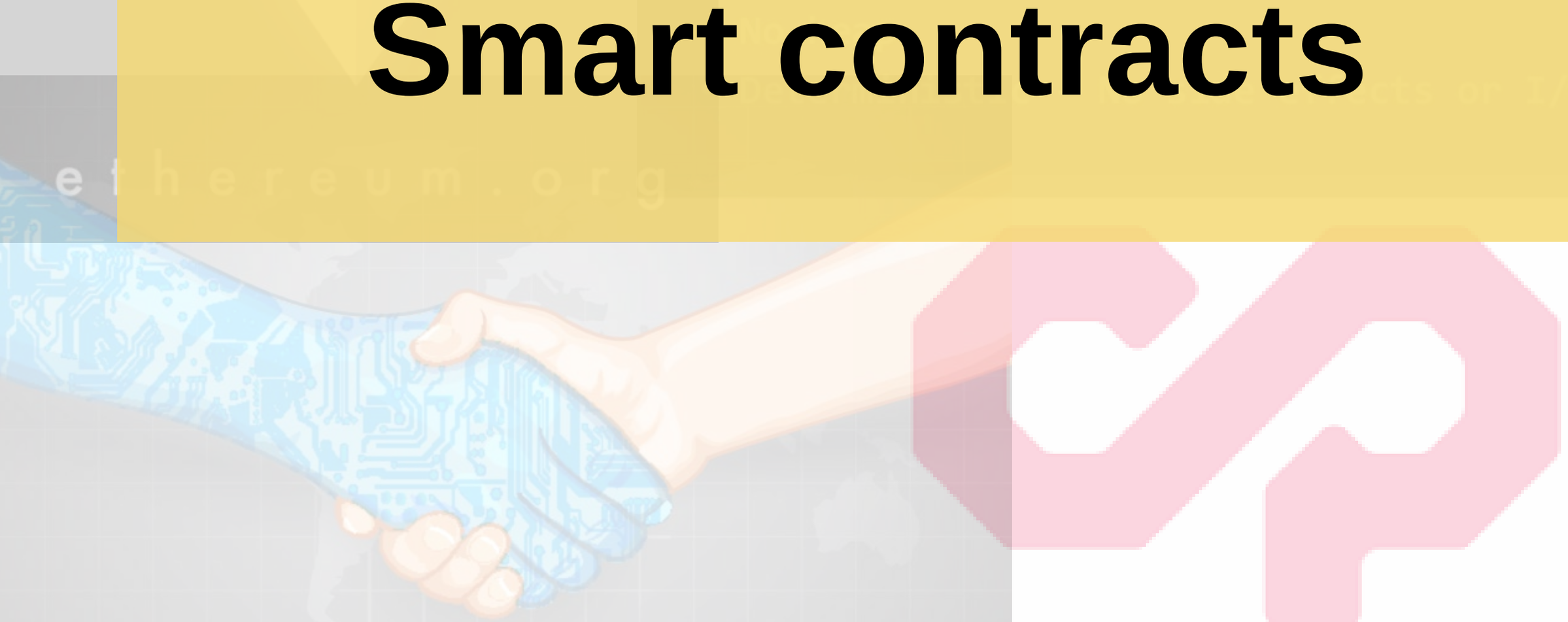
Shouldn’t blockchains just kill existing settlement systems?

28 Oct. 1861



26 Oct. 1861

Smart contracts



What is Bitcoin Script?

- Forth-like, stack-based VM, RPN
- 1 byte opcodes
- All values are variable length byte arrays
- Type interpreted by operations
- Only stack & alt-stack
- No return stack (no calls)

What's a smart contract?

- Code executed on blockchain

…in "Turing-complete" language

- Can operate on blockchain data + currency
- Code defines contract, e.g.,
  - Financial instrument
    - If GOOGL rises to $1,500 by 30 Aug. 2018, assign 10 shares from Alice to Bob and have Bob pay Alice $15,000
- Behavior and data are *publicly visible*

Simple smart contract: Lottery

Contract Lottery

Lottery

What’s a smart contract?

- Best known system: Ethereum
  - $25 Billion market cap
- Decentralized → autonomous: Correct *execution enforced by network*

What's a smart contract?

Abstraction: Smart contract simulates *trusted third party with public state*

- Decentralized →
- Self-enforcing →
- Expressive →

execution enforced by network

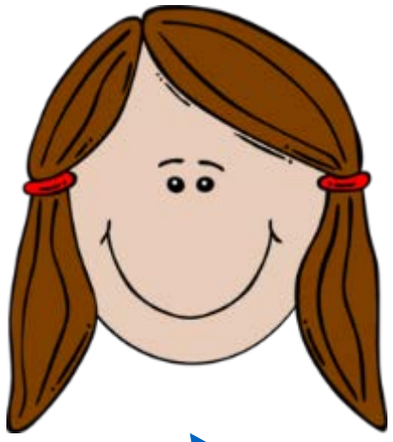
Virtual trusted third-party

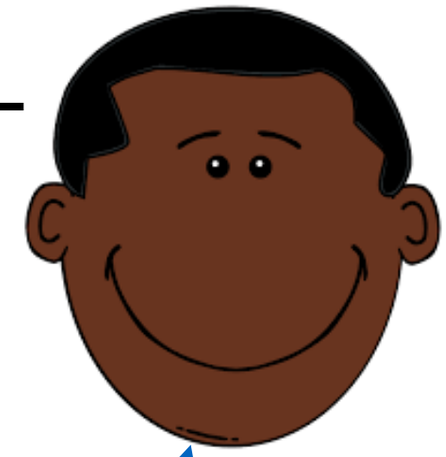
Stock ticker:
GOOGL = $1500

$15,000

Contract

10
shares
GOOGL



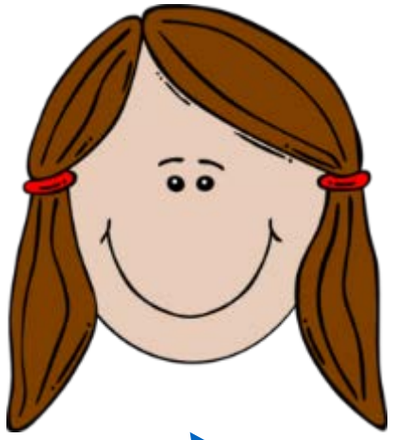


10 shares
GOOGL

$15,000

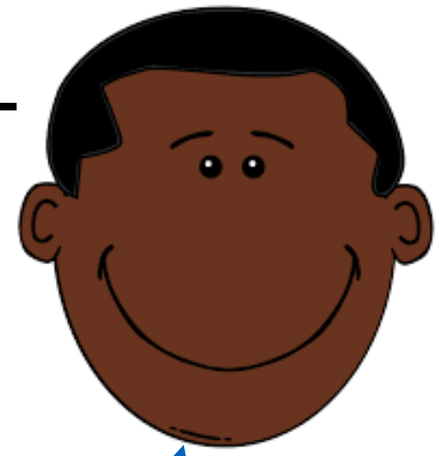
A simplified view

Stock ticker:
GOOGL = $1500



$15,000

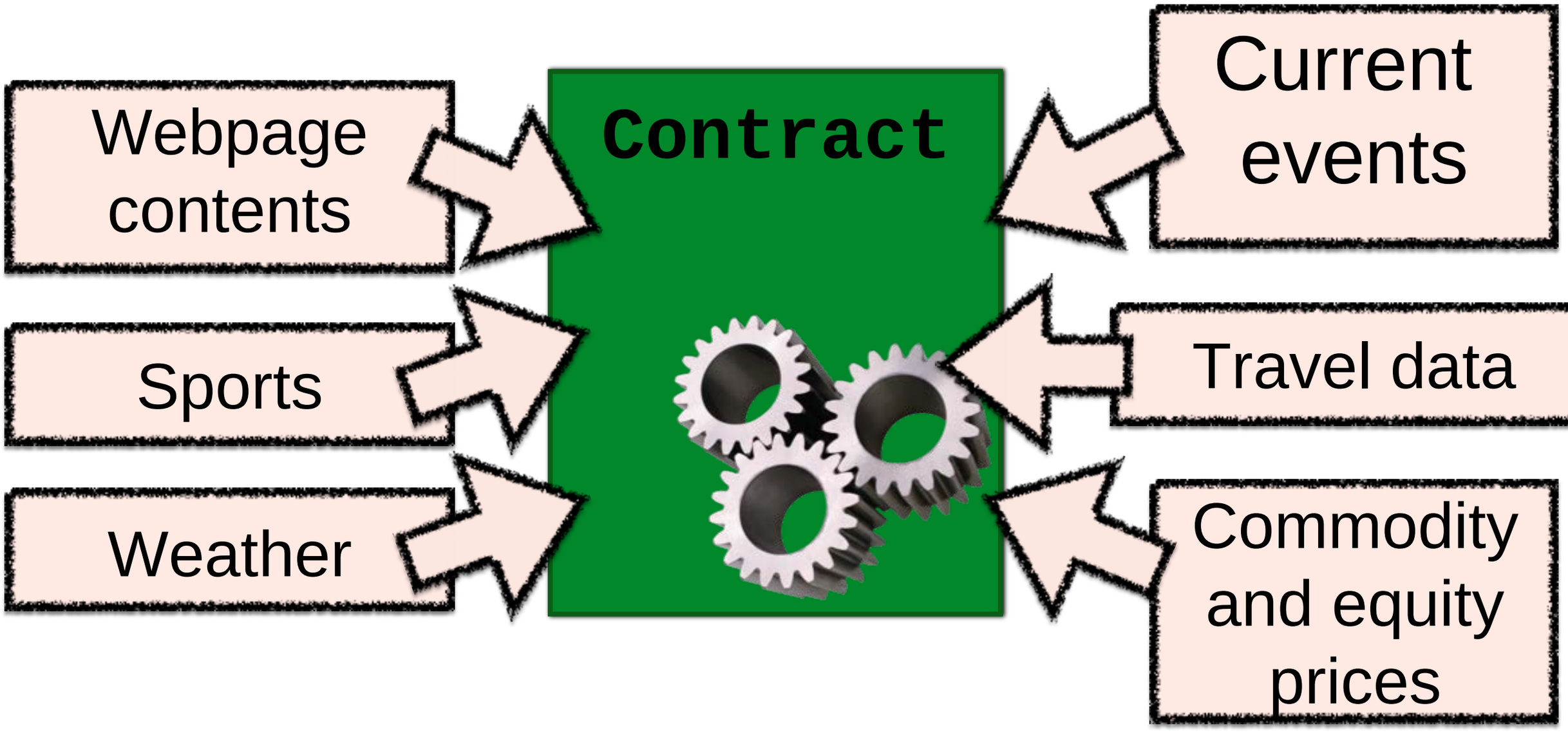
10 shares GOOGL



GOOGL

$15,000

Smart contract systems rely on data feeds…



…digitally signed by (trustworthy) sources.

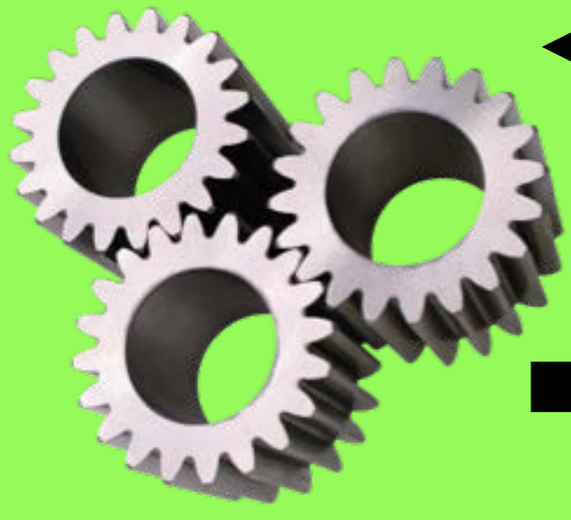
What can blockchains do?

Self-enforcing insurance policies

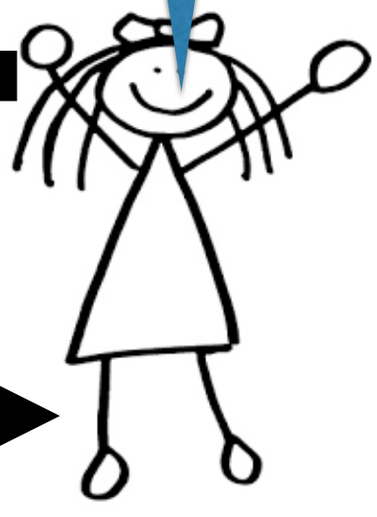
Flight Insurance

Gimme a $100 policy

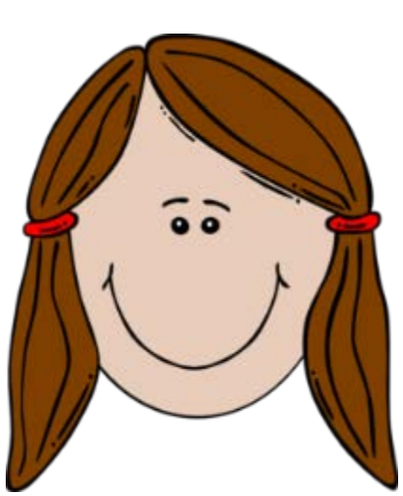
(Flight #1215, 27 June 2017,
Policy price: $1)



$100



New digital-goods marketplaces

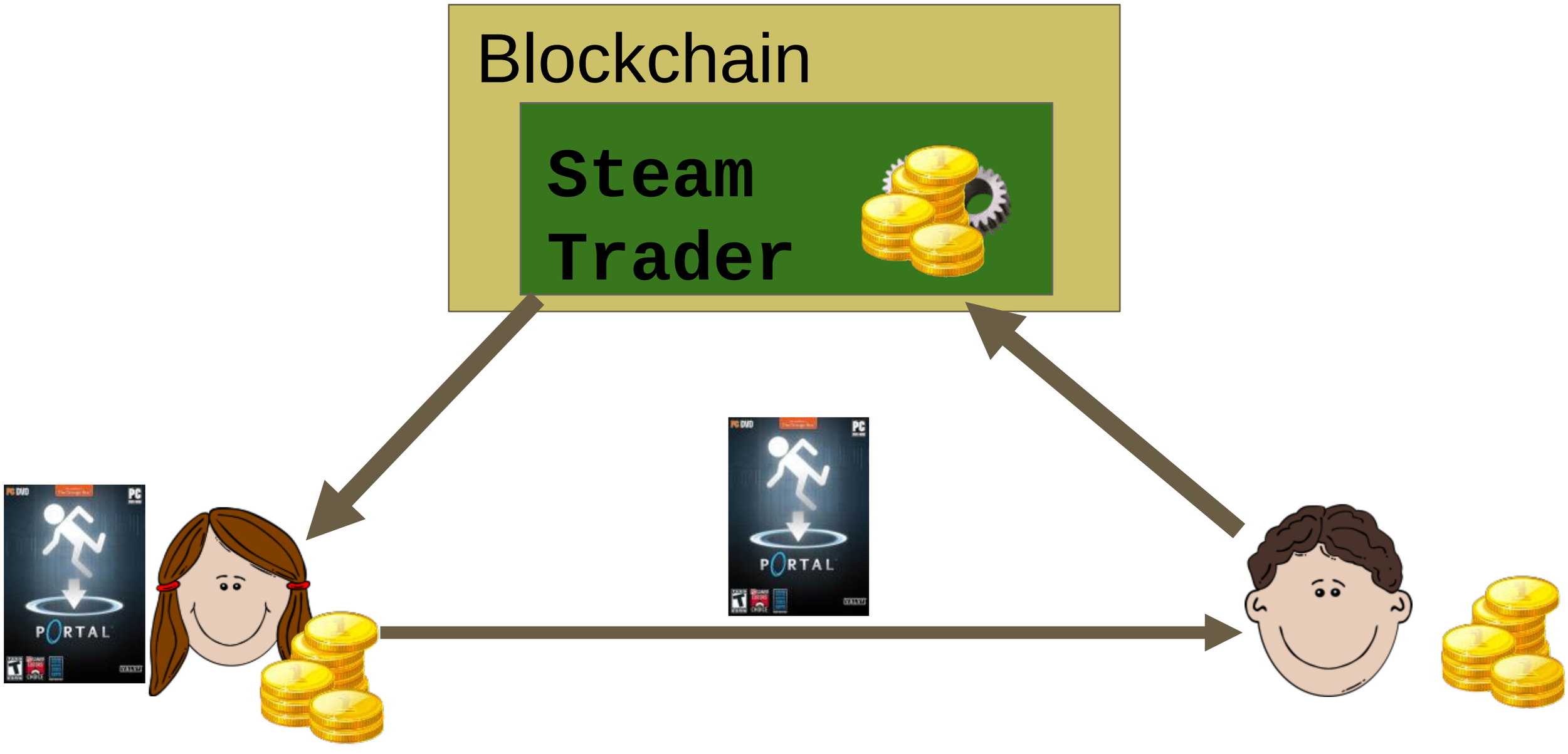


Online game license

Ether

Steam Community Marketplace

…via sophisticated fair exchange



Other things blockchains can do

- Blockchain + IoT
  - Szabo (1997): Smart contract locks you out of car if you miss auto loan payment
- Digital rights management
  - Automated, transparent royalty payments
- Supply-chain management
  - Tamperproof provenance tracking
  - + cryptocurrency → anti-corruption tool?

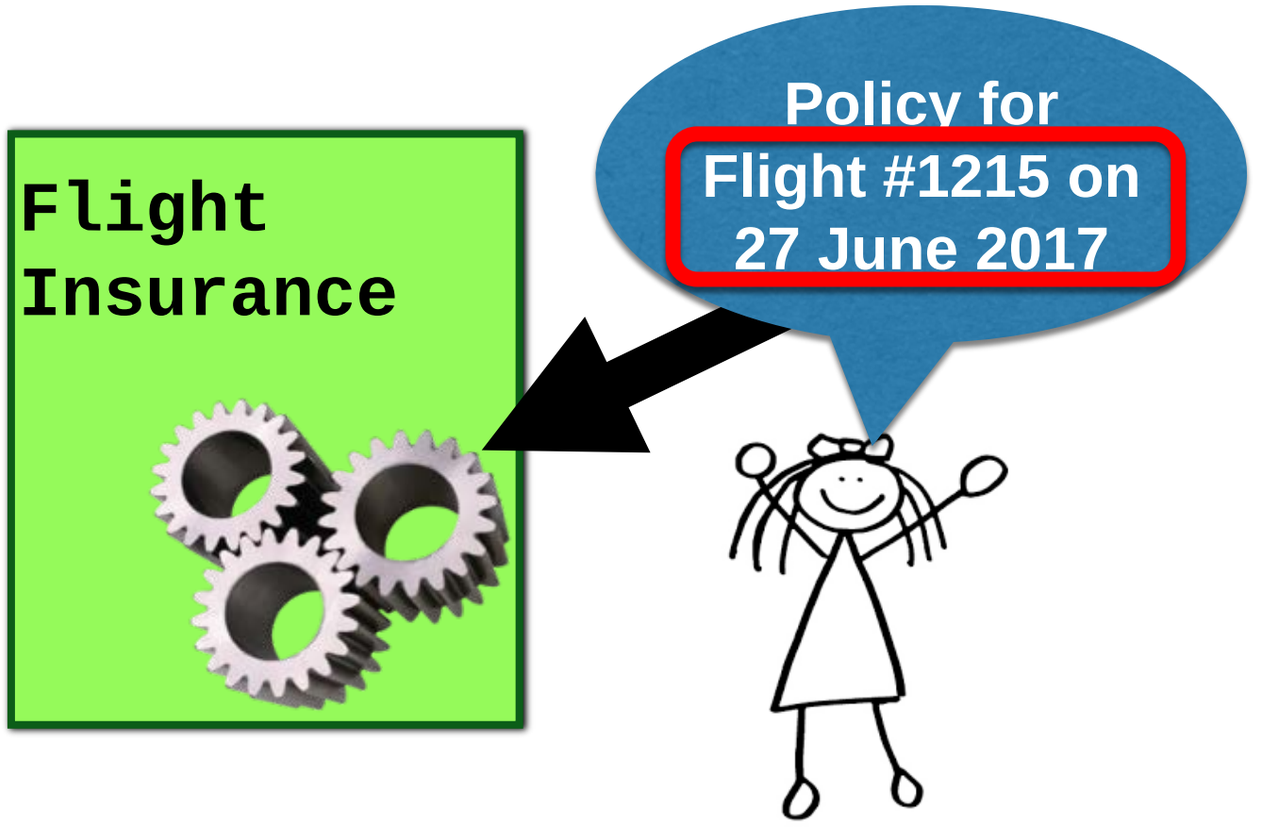
What *can't* blockchains do?

IC3 Grand Challenges

- #1 Scaling
- #2 Correctness
- #3 Confidentiality
- #4 Strongly authenticated data
- #5 Safety and compliance

IC3 Grand Challenges

- #1 Scaling
- #2 Correctness
- #3 Confidentiality
- #4 Strongly authenticated data
- #5 Safety and compliance



High promise, but early days

- Main application of Ethereum?

  …launching other cryptocurrencies
  - E.g., Bancor
    - Cryptocurrency executed within a cryptocurrency for launching cryptocurrencies
  - J. K. Galbraith: All financial innovation is leverage in a new disguise.
    - “The world of finance hails the invention of the wheel over and over again, often in a slightly more unstable version.”
- Tools for “private” (permissioned) blockchains
  - Caveat emptor!

Summary

- Blockchains will have a transformative effect on many industries, but…
- Scientific advances (e.g., in Grand Challenges) needed to fully unleash their power
- Today, careful scoping needed to reap blockchain benefits

IC3 The Initiative For CryptoCurrencies & Contracts

To learn more:

www.initc3.org