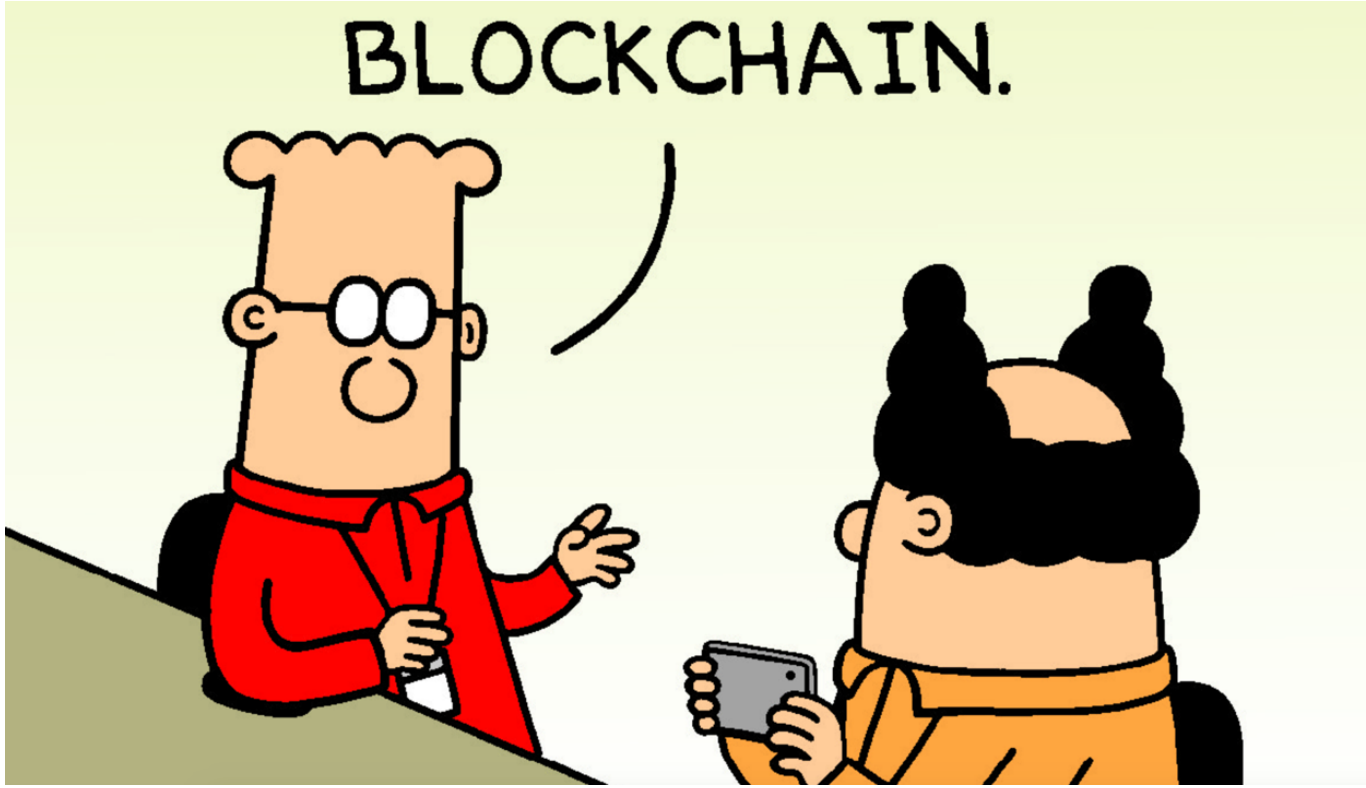
COM-402
Information Security and Privacy

Blockchains
1/3

Credits: Several of the slides borrowed from Ari Juels



© Dilbert.com

Ten Reasons to Care about Blockchains, Cryptocurrency, and Smart Contracts

Reason 1: You like excitement!

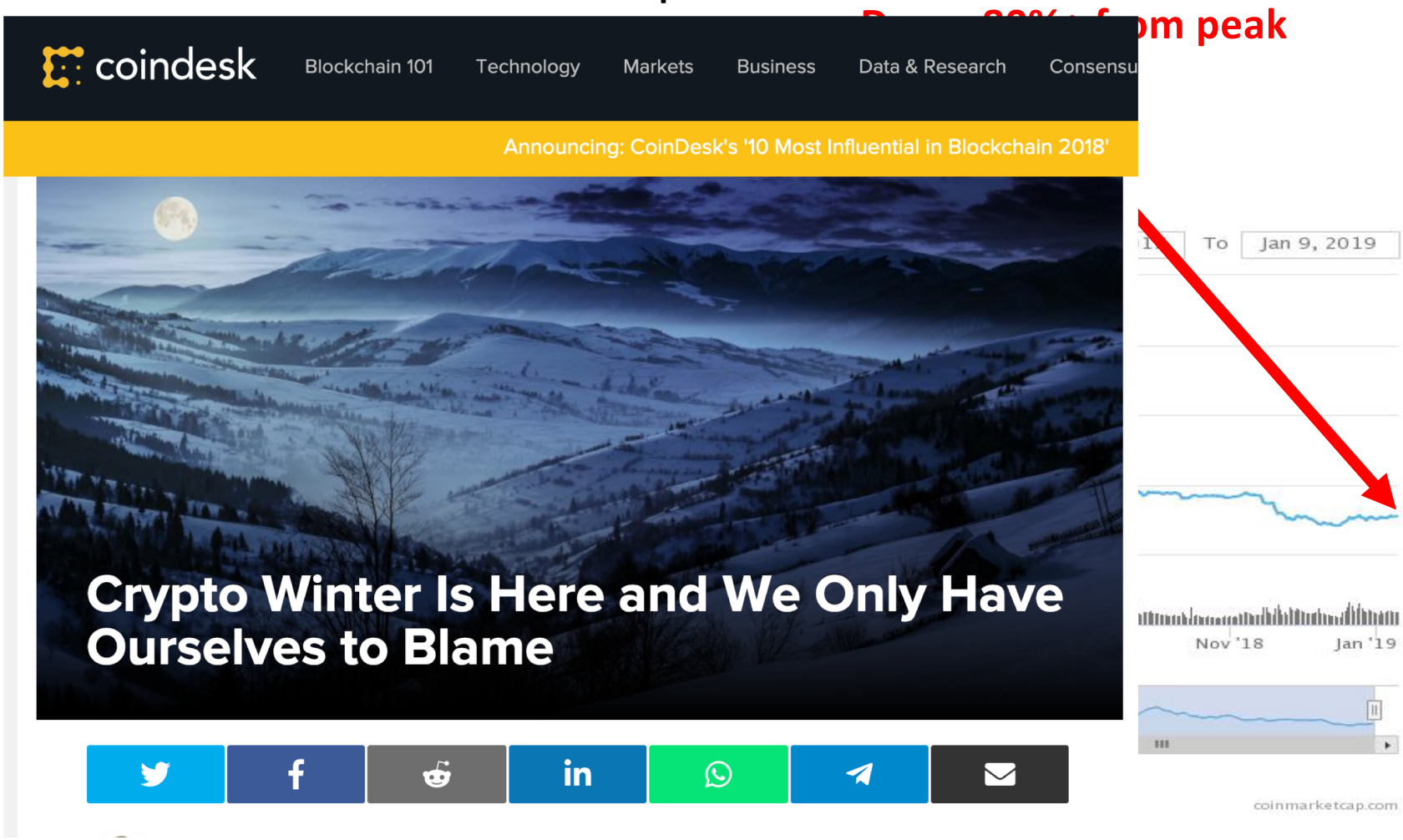
Market capitalization of cryptocurrencies + tokens

Reason 2: You like rollercoasters

Market capitalization of cryptocurrencies + tokens

Reason 3: You like to be depressed

Market capitalization of cryptocurrencies + tokens



Reason 4: You have a sense of the absurd

Down 97% from peak

Reason 5: You like cats…

Dragon, the world's most expensive cat on a blockchain
Cost: about $172,000

Reason 5: You like cats, but not kitty litter

Dragon, the world's most expensive cat on a blockchain
Cost: about $172,000

Cato, the world's most expensive fur-and-Blood Kitty
Cost: about $41,000 (29,000 GBP)

Reason 6: Everyone else cares

Forbes

Insurance Int
Blockchain In
Transforming
Industry

Andrea Tinianow Contrib
Crypto & Blockchain
I am the Blockchain Czarina.

609 views | Dec 21, 2018, 04:04am

Can New Technologies Slow The Progress Of The Sixth Mass Extinction?

Yoav Vilner Contributor
Crypto & Blockchain
A serial startup mentor and CEO. Veteran blockchain advisor.

Forbes audience. What is This?

n Will Usher
optech

tyVoice

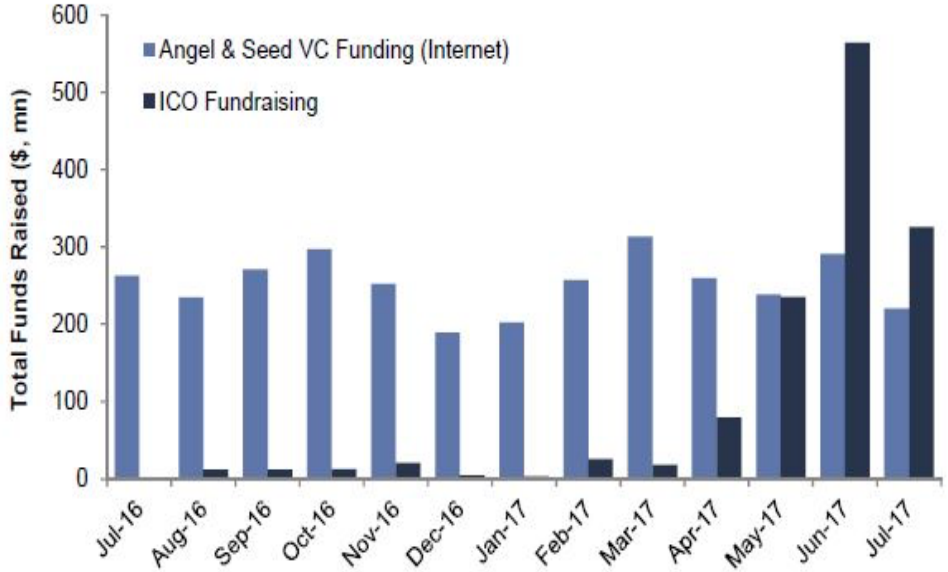
nsparency into residential/commercial real

Reason 6: Everyone else cares

Reason 7: Because they could change the face of venture funding

Exhibit 8: The pace of ICO fundraising has now surpassed Angel & Seed stage Internet VC funding globally

Total Funds Raised by month ($, millions)

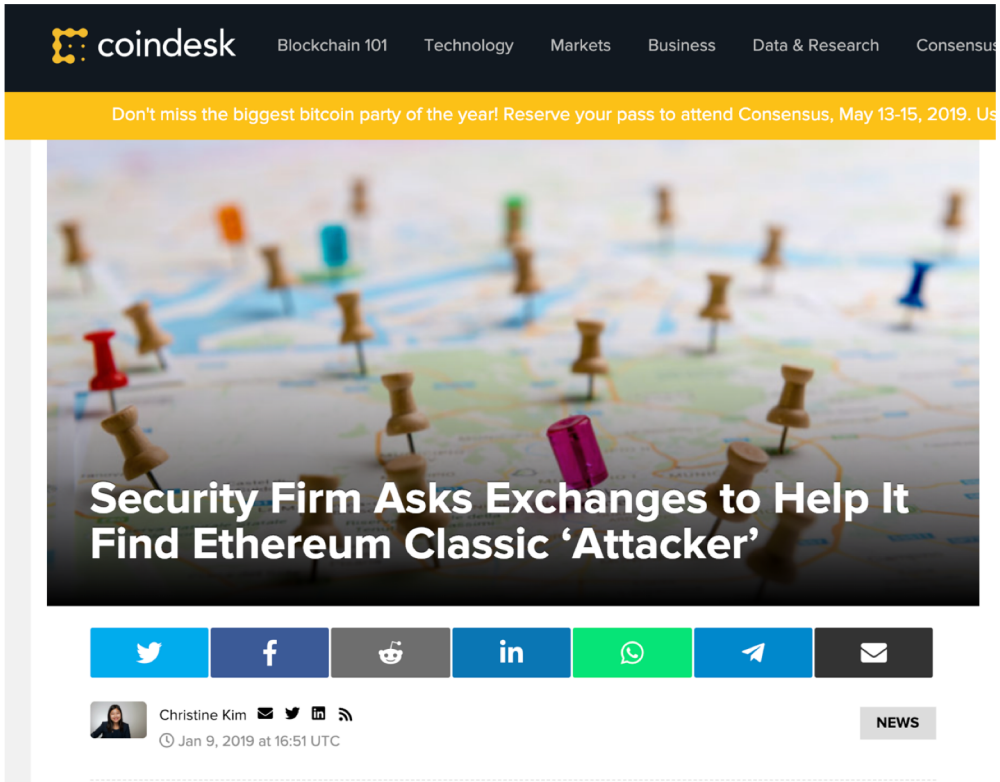


Note: ICO fundraising as of July 18th, 2017, per Coin Schedule. Angel & Seed VC funding data as of July 31st, 2017 and does not include "crowdfunding" rounds.

Source: CoinSchedule, CB Insights, Goldman Sachs Global Investment Research.

ICO: Intial Coin Offering

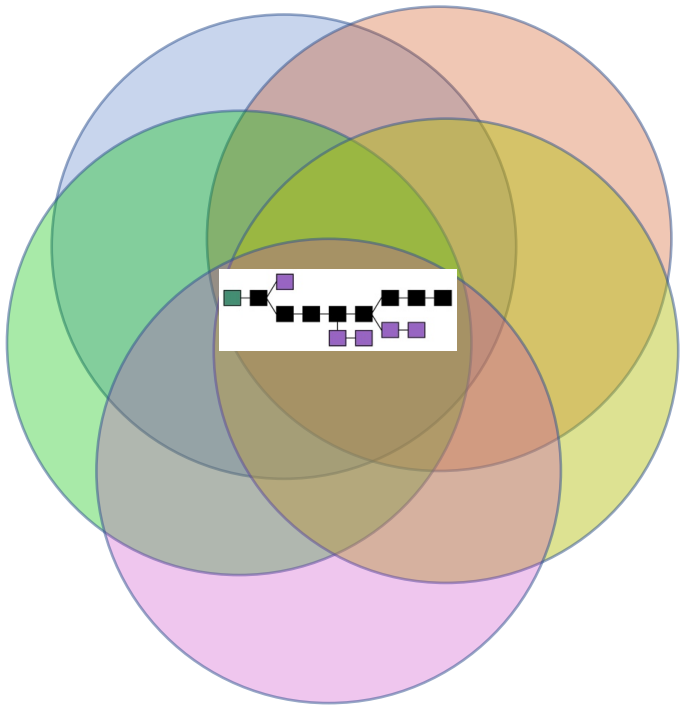
Reason 8: There's always something interesting going on in blockchain land



Reason 9: They are a fascinating technology spanning many areas of computer science–and beyond

For example:

- Distributed systems
- Programming languages
- Formal verification
- Cryptography / security
- Game theory
- Technology law
- Business



Reason 10: Because you believe that trust lies at the root of human prosperity

October 2015

It all began with Bitcoin…

2008: Breakthrough

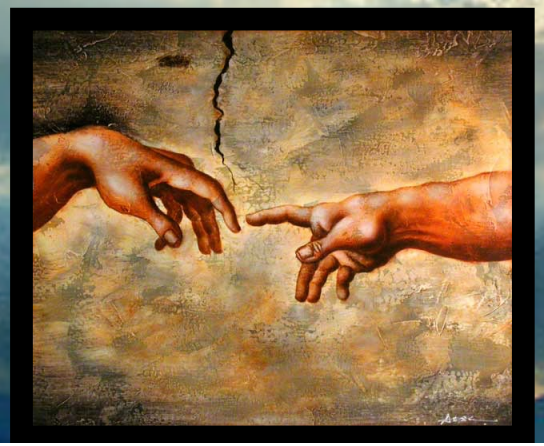
Bitcoin: A Peer-to-Peer Electronic Cash System

Satoshi Nakamoto
satoshin@gmx.com
www.bitcoin.org

Blockchain

In the Beginning, There Was The Coin
The Year 1 A.B. (a.k.a. 2009)

The Genesis Block



2009 : Birth of the Bitcoin

- Mankind discovers that a decentralized piece of software can embody a virtual currency
- That piece of software is the blockchain
- No central bank, no legal person, no regulation

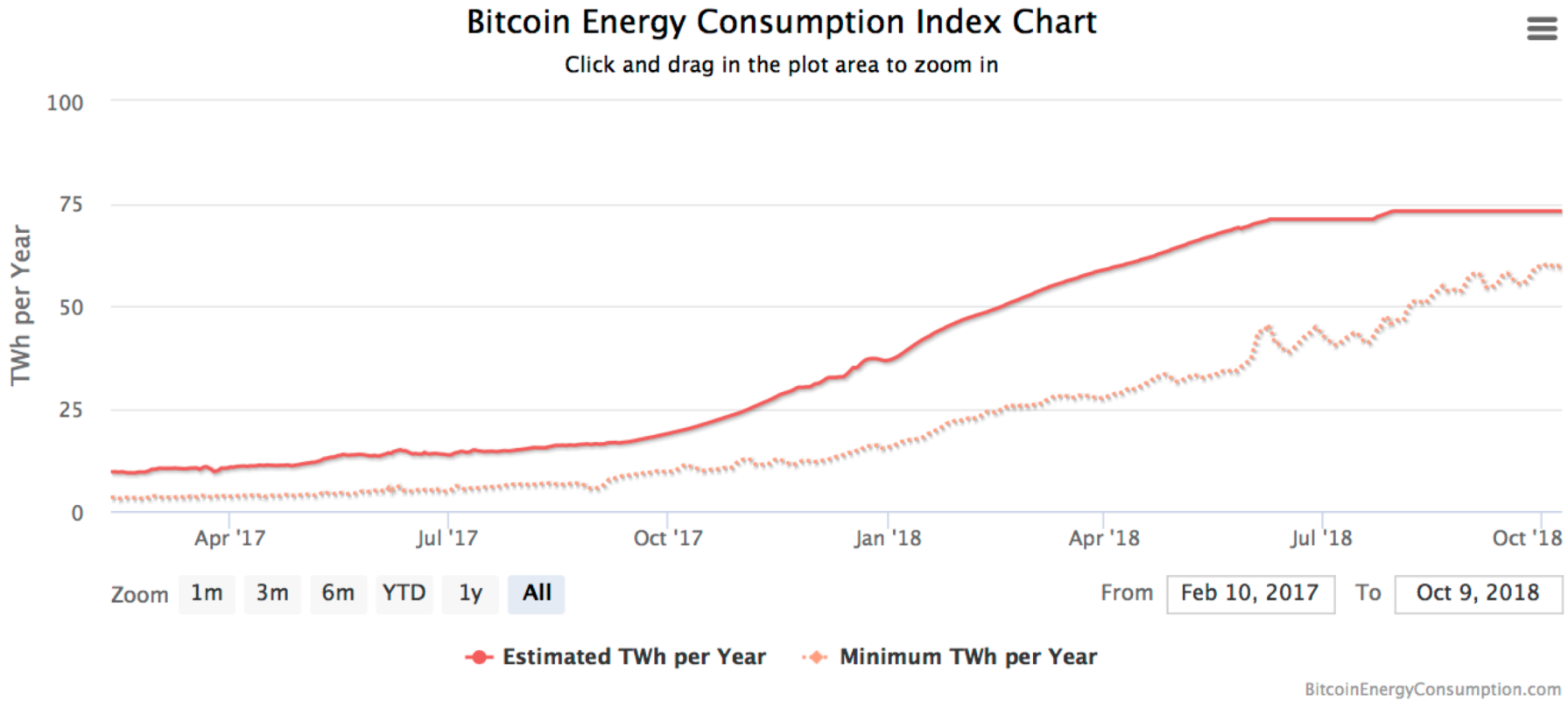
Mining Nodes

- Validate transactions
- Add them to the block they are building
- Broadcast the completed block to other nodes

All these operations (especially the many, many cryptographic computations) have a huge cost

6H
E
4F
G

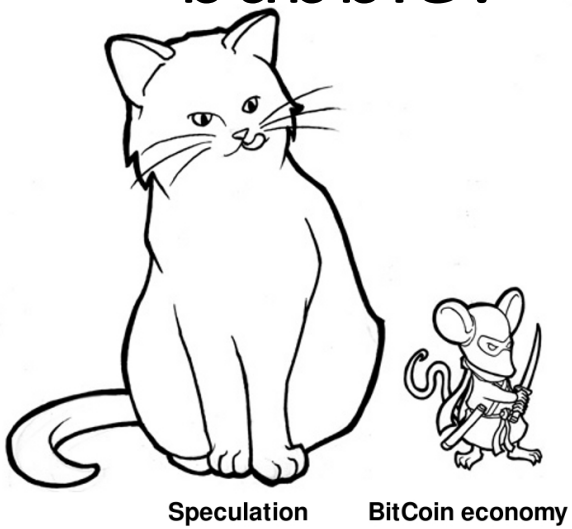
Bitcoin Energy Consumption Index



60 TWh/year: yearly electricity consumption of Switzerland

Currency?

Or speculative bubble?



bitcoin ACCEPTED HERE

Overstock.com®

https://help.overstock.com/help/s/article/Bitcoin

Fostering trust?

Or mistrust?

PHOTO: CREATIVE COMMONS/GEORGE FREY/GETTY IMAGES

It all began with Bitcoin…

Or did it???

Actually…

32 B.B.

1977 1982 1992 1996 1999 1 A.B. 10 A.B.

- Hashcash
- "Proof of Work (PoW)" defined and formalized
- First proof-of-work-based cryptocurrency (Rivest and Shamir)
- Proofs of work introduced (Dwork and Naor)
- Anonymous cryptocurrency introduced (Chaum)
- Lamport paper on Byzantine Generals problem
- RSA invented—digital currency an early proposed application

Bitcoin through the lens of…
money

Two flavors of financial instrument

1. Bearer instrument
   - Physical holder of object (or secret) possesses asset
     - E.g., cash, bearer bond
   - Looser definition includes holder of *secret*
     - E.g., Swiss bank account, once upon a time
   - Pros:
     - Easy to transfer
     - Anonymous
   - Cons:
     - Easy to lose!

Two flavors of financial instrument

2. Registered instrument
   - Asset with centralized record of ownership
     - E.g., most types of shares or bonds
   - Pros:
     - Can’t (physically) lose it!
   - Cons:
     - Not anonymous
     - Hard to transfer… unless register is digital…
- Both types of instrument have a venerable history

What is money?

- Resource with widespread use as medium of exchange
- Four key ingredients for bearer version, mechanisms for:
    1. Creation
    2. Forgery prevention
    3. Verification of validity / ownership
    4. Transfer between parties

Example

What are mechanisms for:

1. Creation
2. Forgery prevention
3. Verification of validity / ownership
4. Transfer between parties

????

Forgery prevention of Swiss banknotes

- 7’ film: https://www.snb.ch/en/iabout/cash/series9/id/cash_series9_security_concept

Money

- In the mid 7th century B.C.E., in Lydia and Ionia (modern Turkey), the first *coins* were struck.
- For forgery prevention, coinage usually relied on three things:

A. Tokens made from scarce resource

- Electrum (gold and silver)

B. Sign / signature that was hard to duplicate

- Initially drew on skills of gem-engravers

C. Death penalty for forgers didn't hurt

- This solution lasted for many centuries…

Alyattes Trite (Lydia 1/3 stater). 6th-5th century B.C.E.
Image Courtesy of CNG: www.cngcoins.com.

Intaglio depicting goddess Demeter. 1st cent. B.C.E. Private collection.

2600+ years later…

Still uses classic principles!

For forgery prevention:

A. Scarce resource: computation
B. Hard-to-forge data: cryptography

Bitcoin

What kind of money is Bitcoin?

- Combines:
  - A ledger: Public record of asset ownership called the *blockchain*
  - Secret keys for control of individual's assets
- So it's got features of bearer instruments *and* registered instruments
- Quasi-anonymous (pseudonymous)
  - Like Swiss bank account (well, once upon a time…)
- Loose comparisons to Yap currency, etc., but no perfect physical analog

"Anyone got change?"

Where did Bitcoin / blockchains come from?

Where did Bitcoin come from?

- Created by “Satoshi Nakamoto”
  - Paper “Bitcoin: A peer-to-peer electronic cash system” [2008]
  - Source code [2009]
- **But who is Nakamoto?**

The face of Bitcoin?

Maybe not!

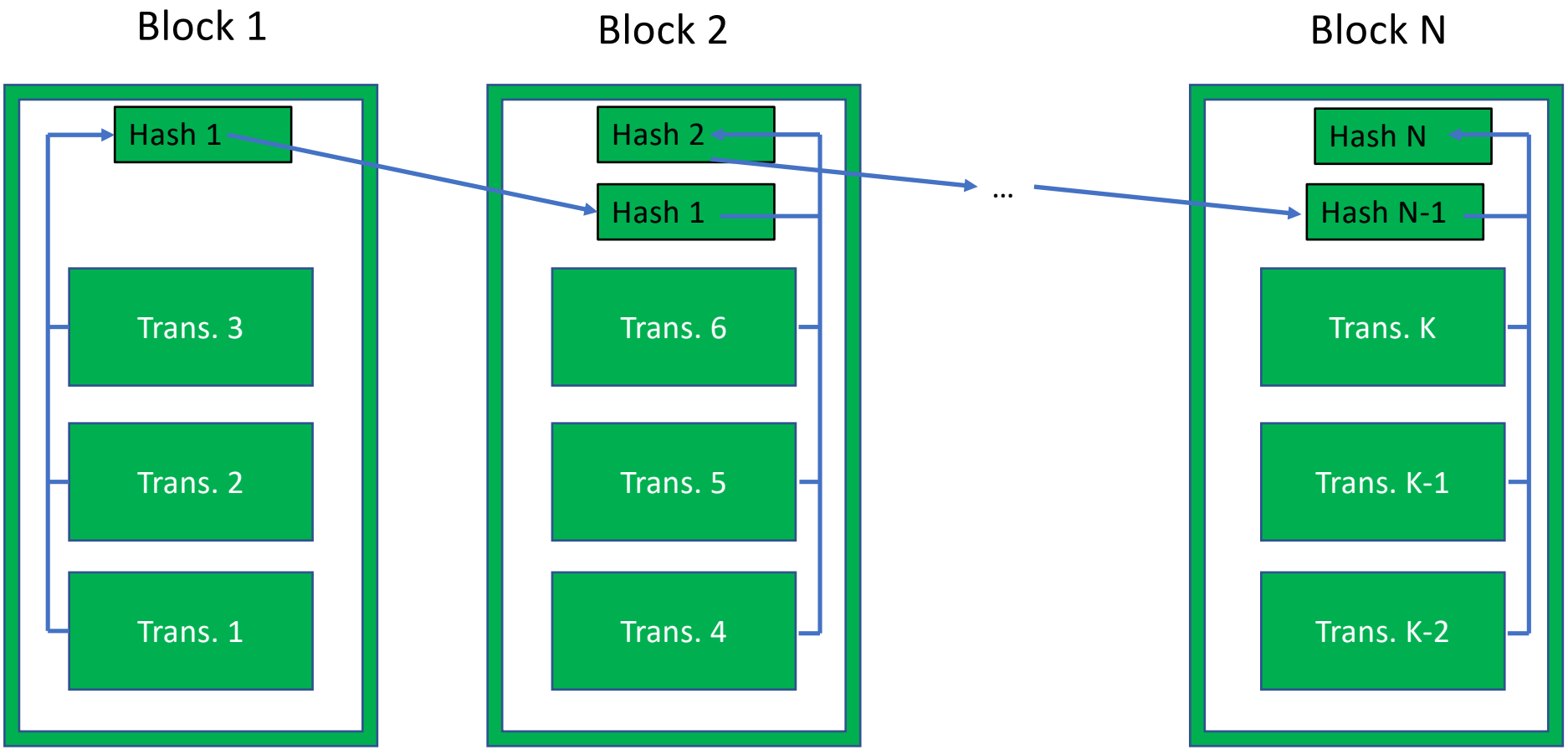
Blockchains and Bitcoin: the Bird’s Eye View

Transactions

	Sender	Receiver	Amount
Trans. 1	Alice	Bob	10 Francs
Trans. 2	Charles	Deborah	25 Francs
Trans. 3	Deborah	Emil	180 Francs
Trans. 4	Alice	Francis	20 Francs

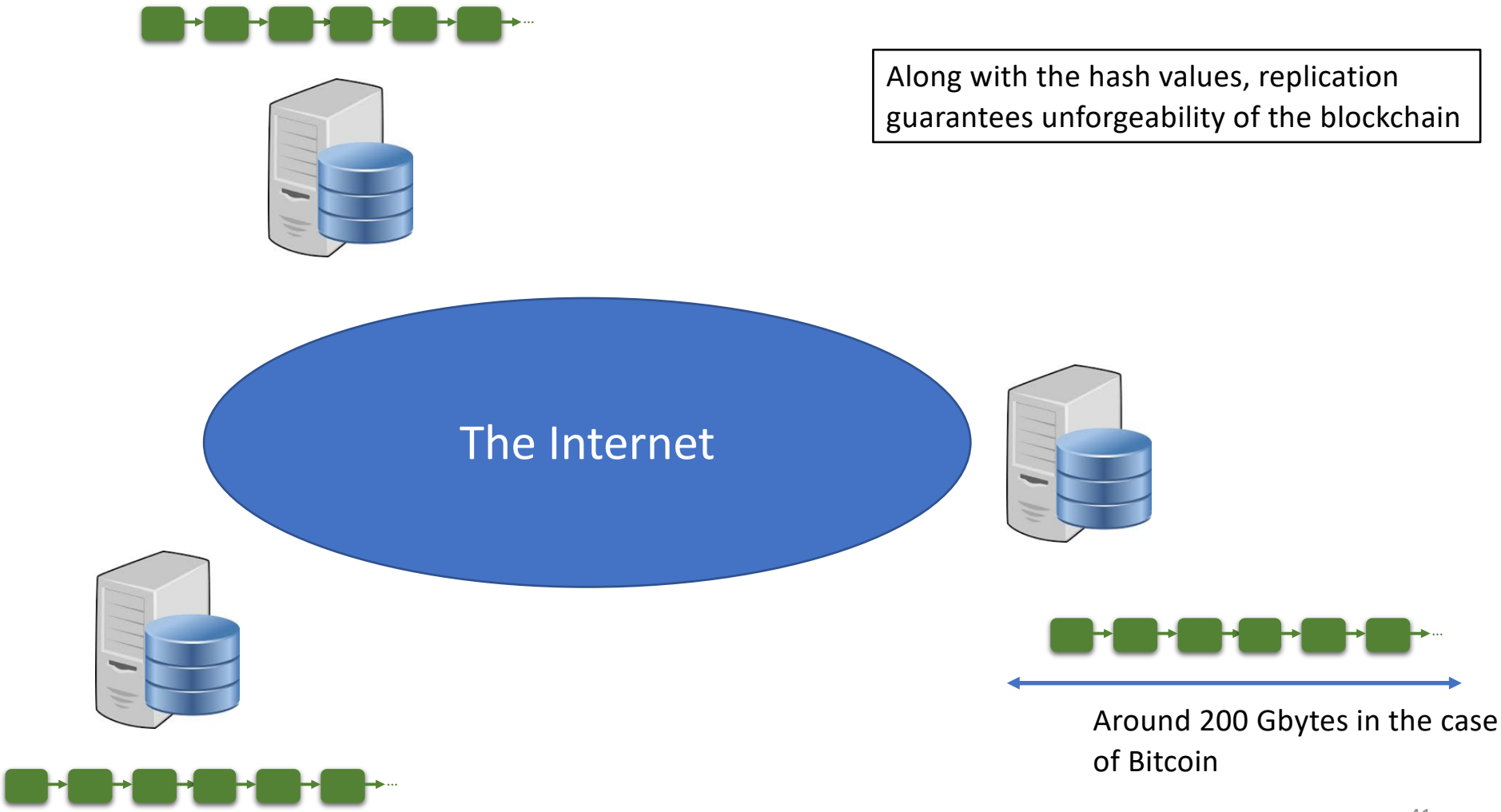
A crucial challenge: prevent double spending!

The Blockchain: Immutable Ledger of Transactions



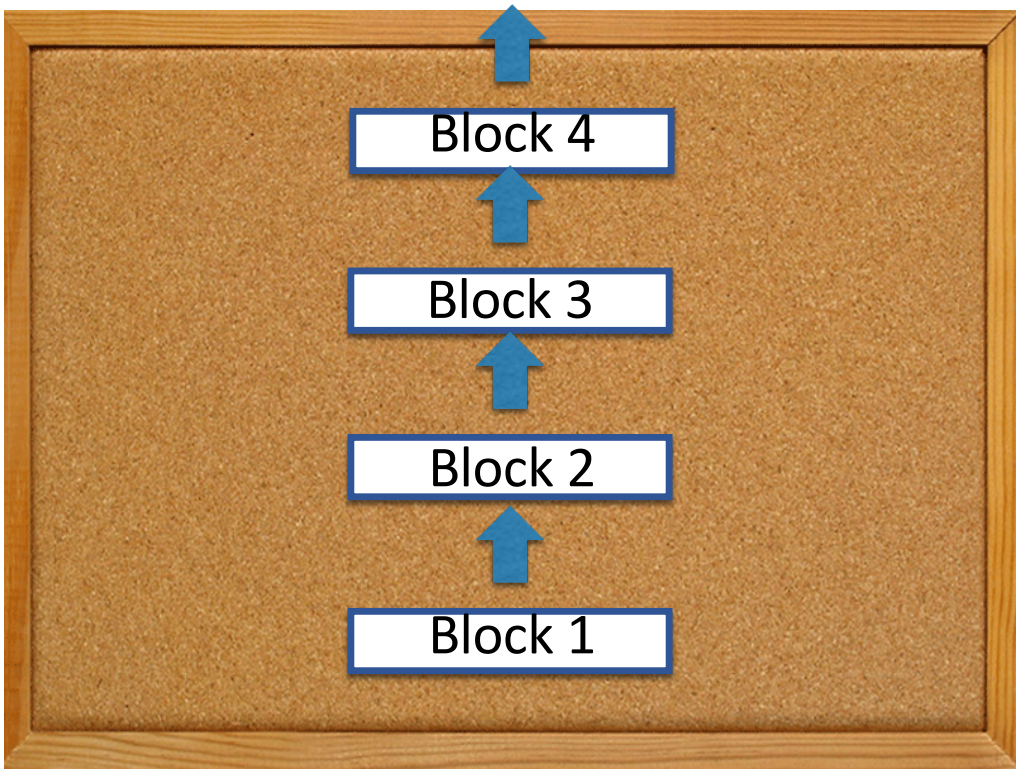
Hash: One-way hash function: Unique fingerprint of its inputs

Decentralization: Replication of the Blockchain



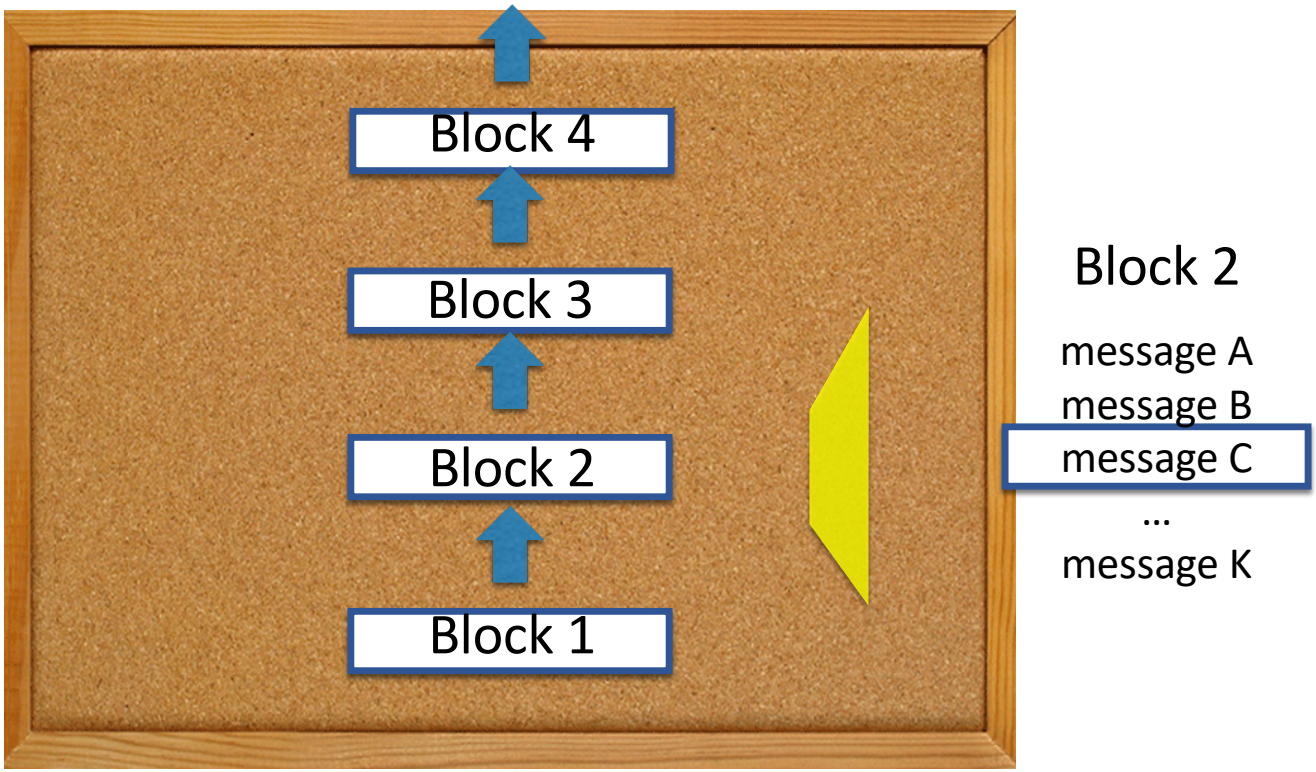
Blockchains: Abstraction

Blockchains: Abstraction



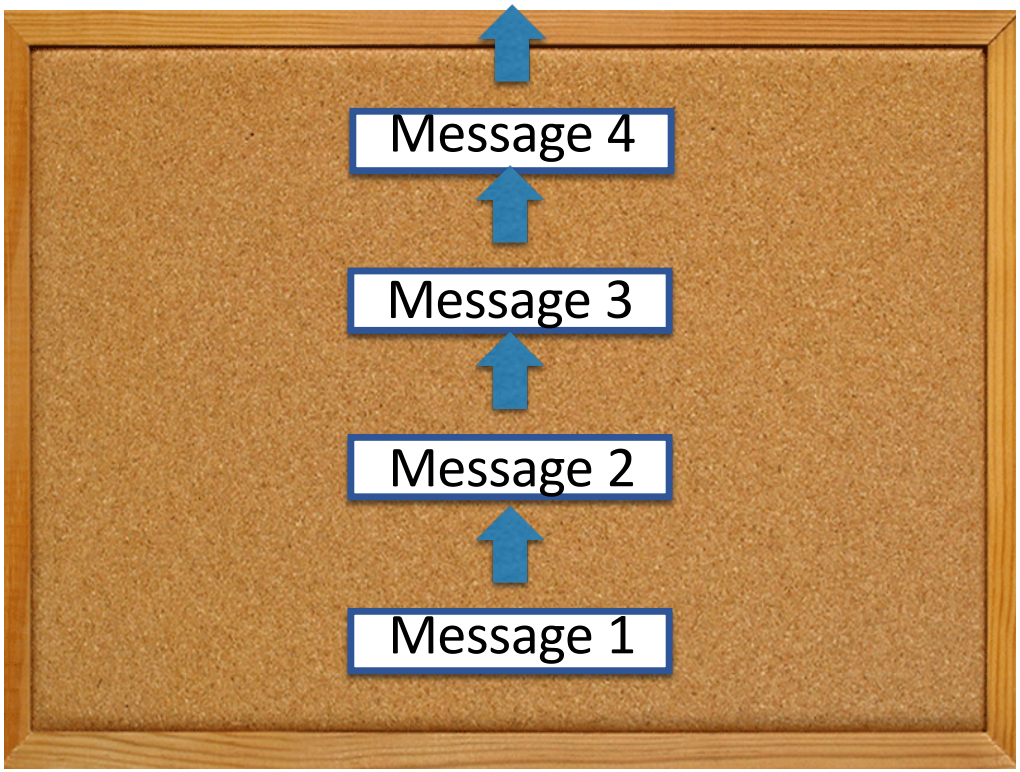
Blockchains: Abstraction

#1 Strict ordering of messages



Blockchains: Abstraction

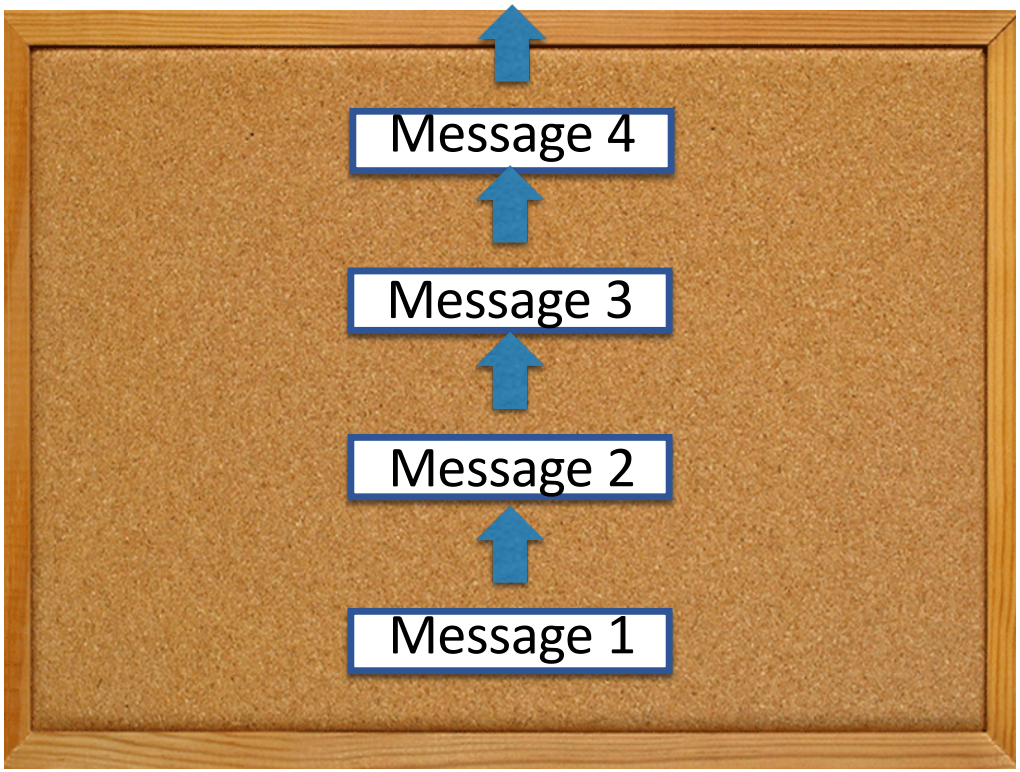
#1 Strict ordering of messages



Blockchains: Abstraction

#2 *Rule-based write, global read*

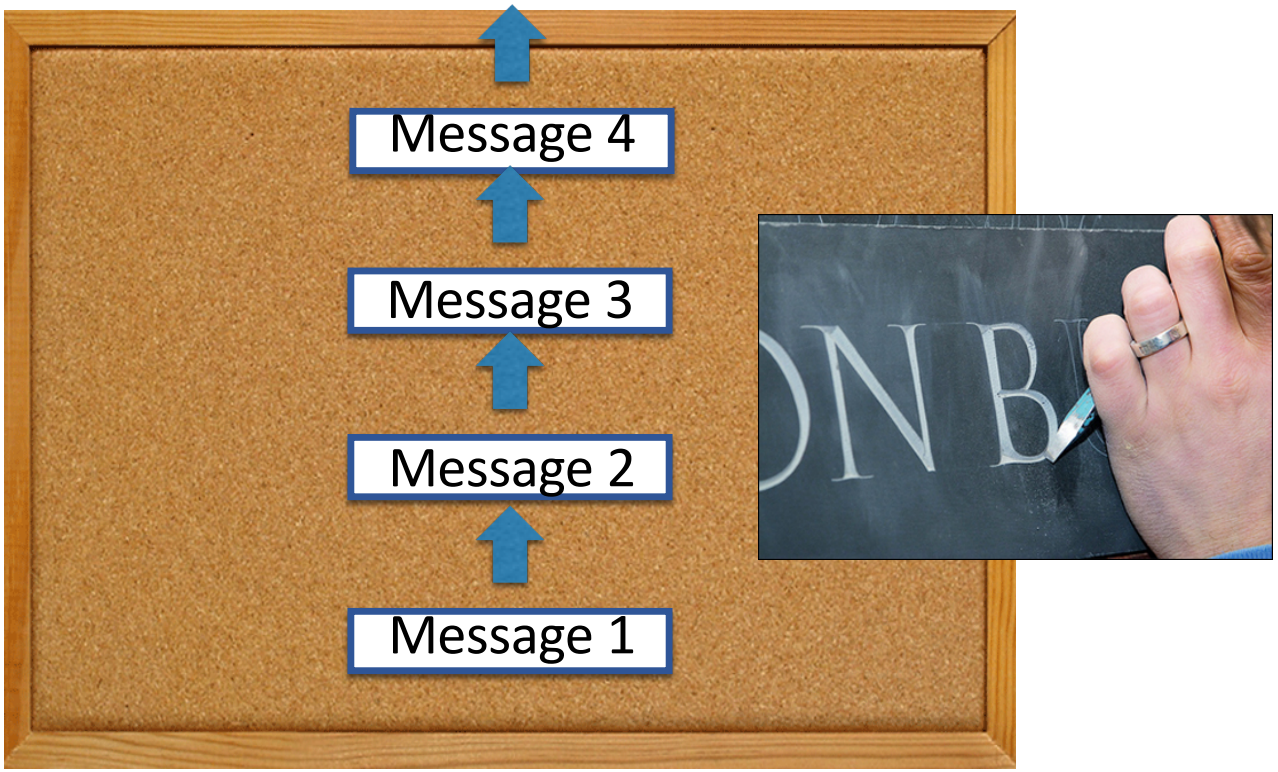
Write Permission: Rule-based



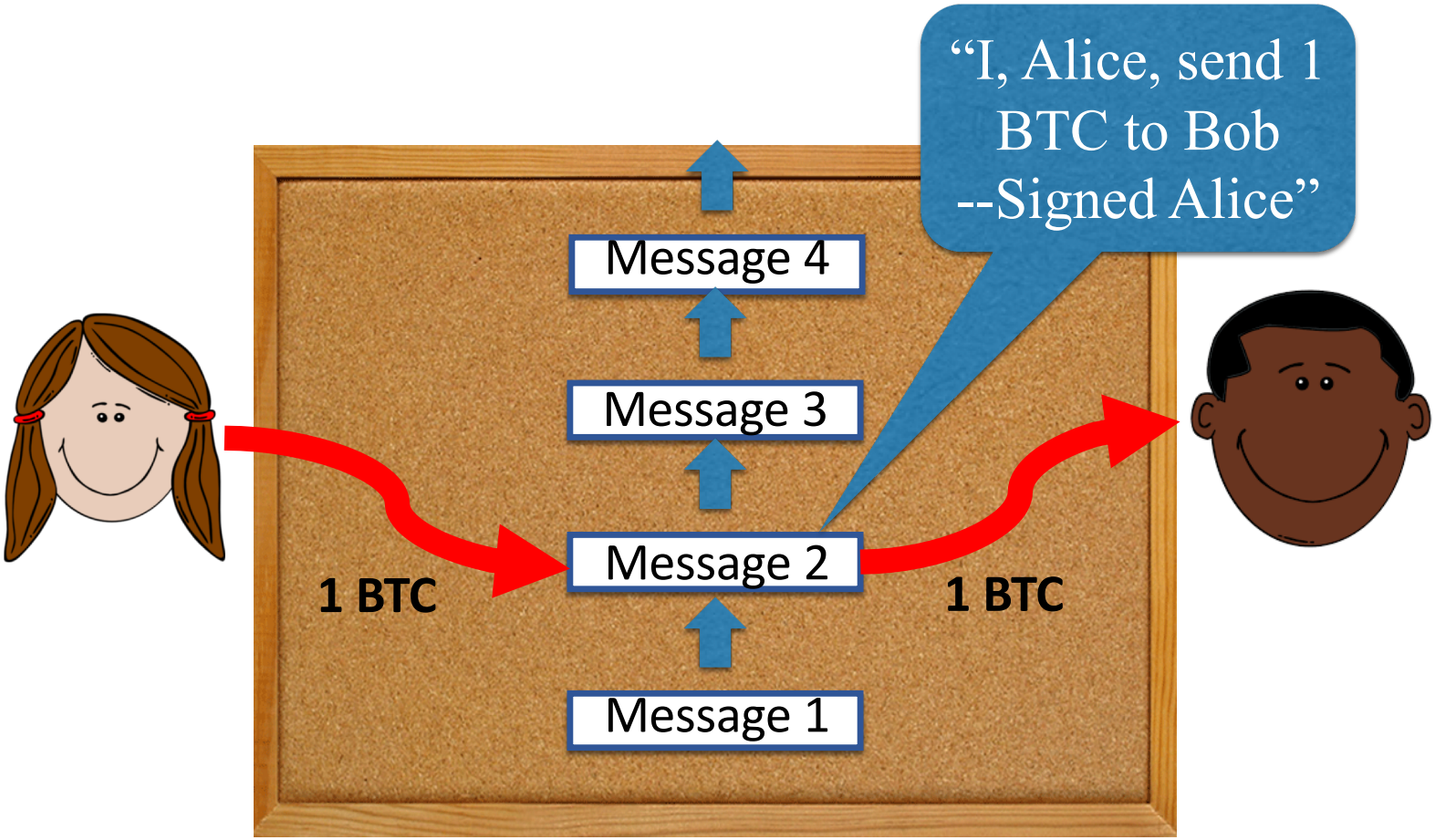
Read Permission:

Blockchains: Abstraction

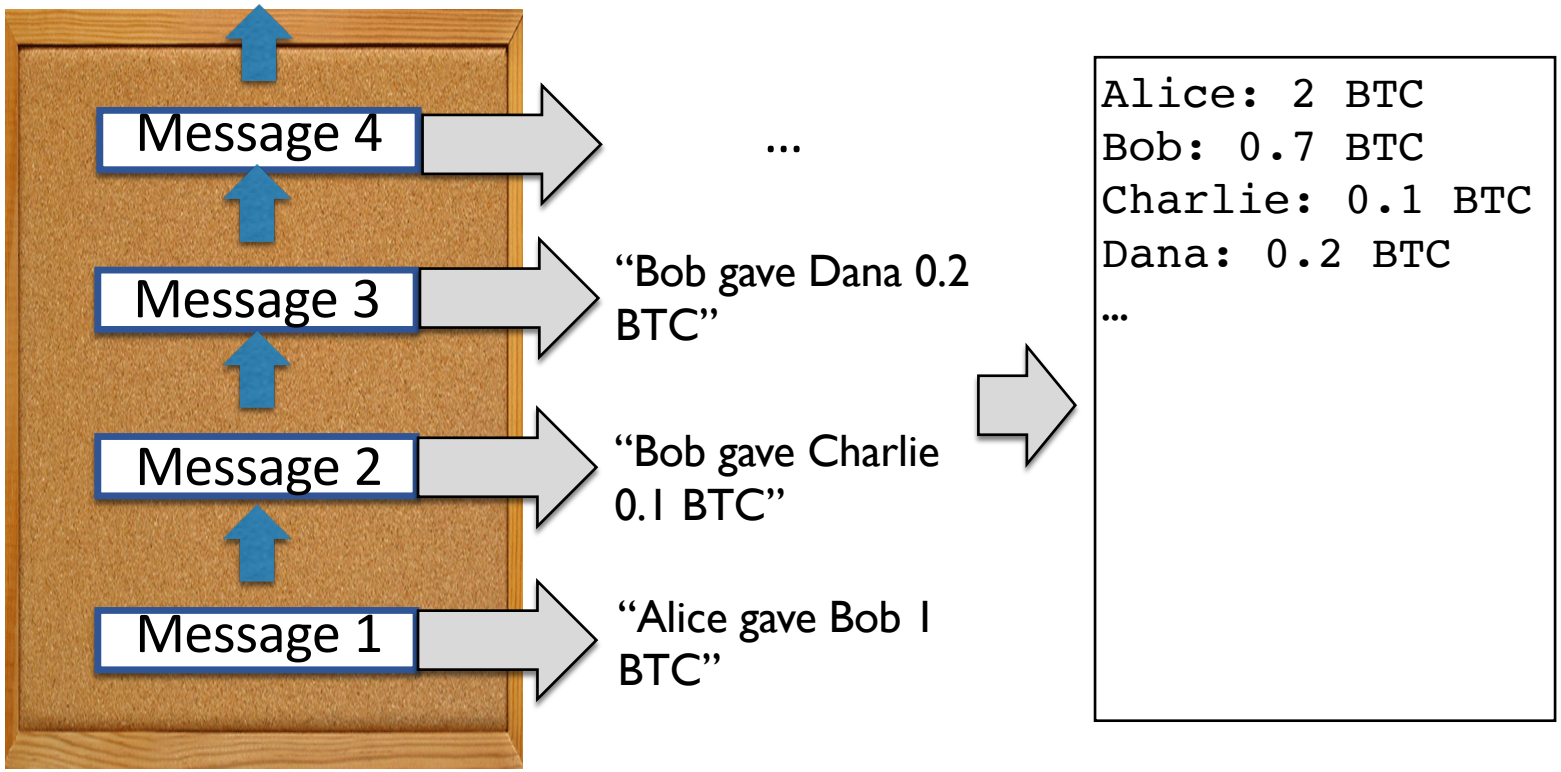
#3 No message modification



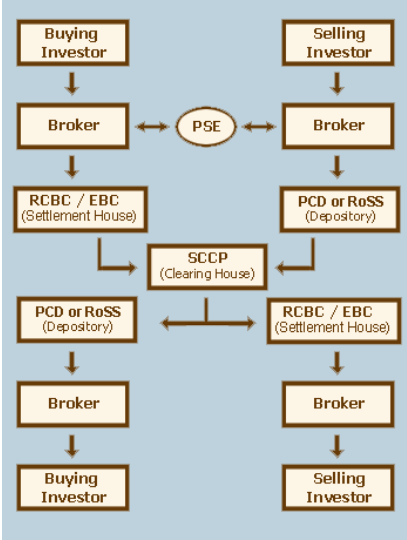
Power of the Abstraction

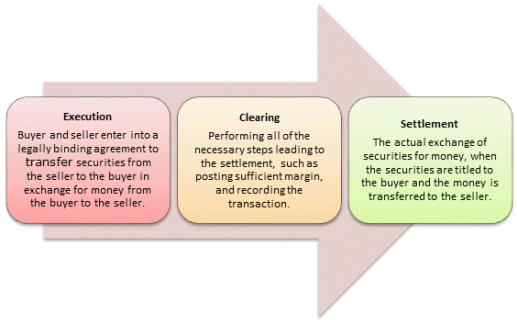


Power of the Abstraction



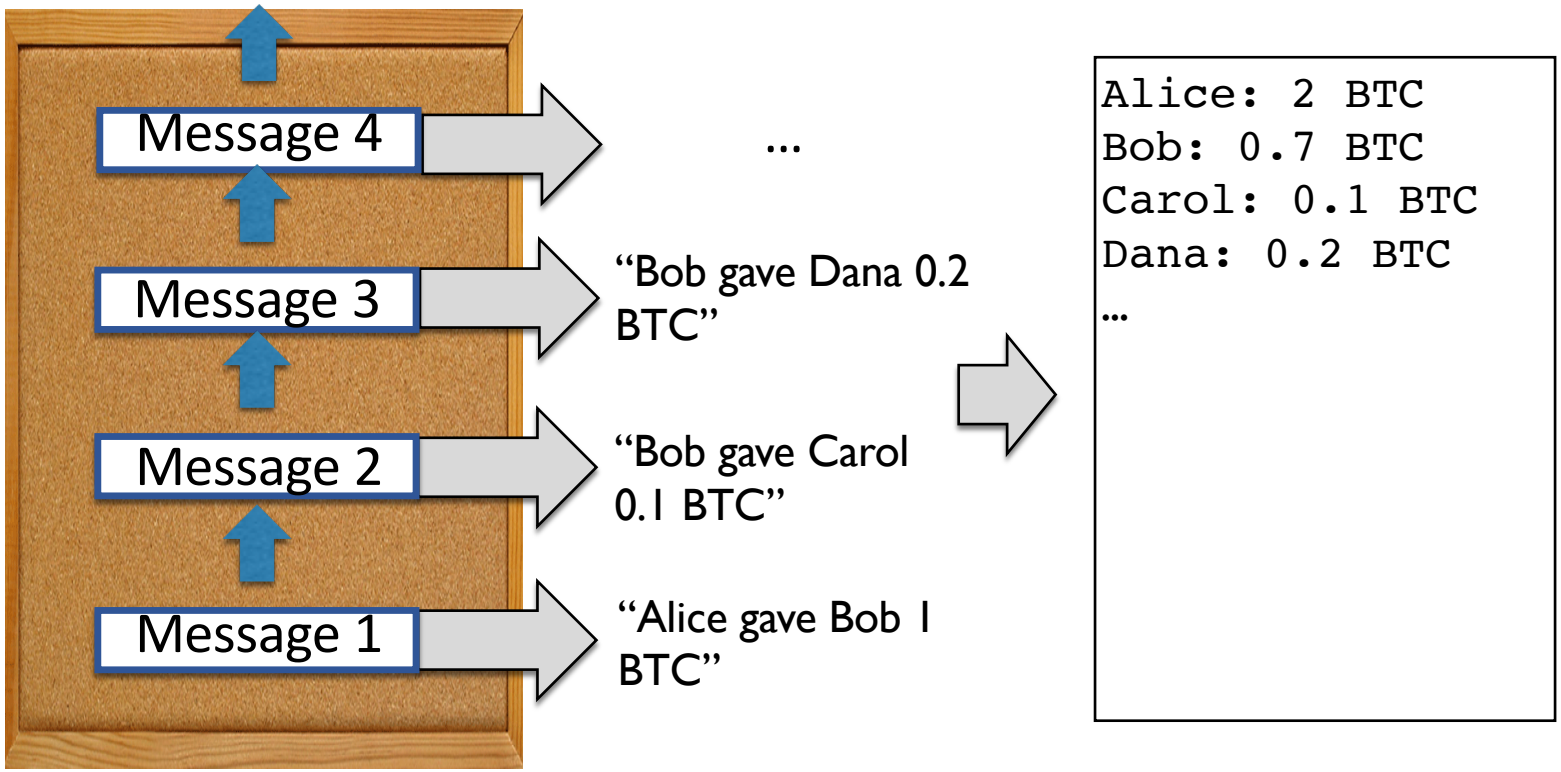
Compare:
Execution, clearing, and settlement



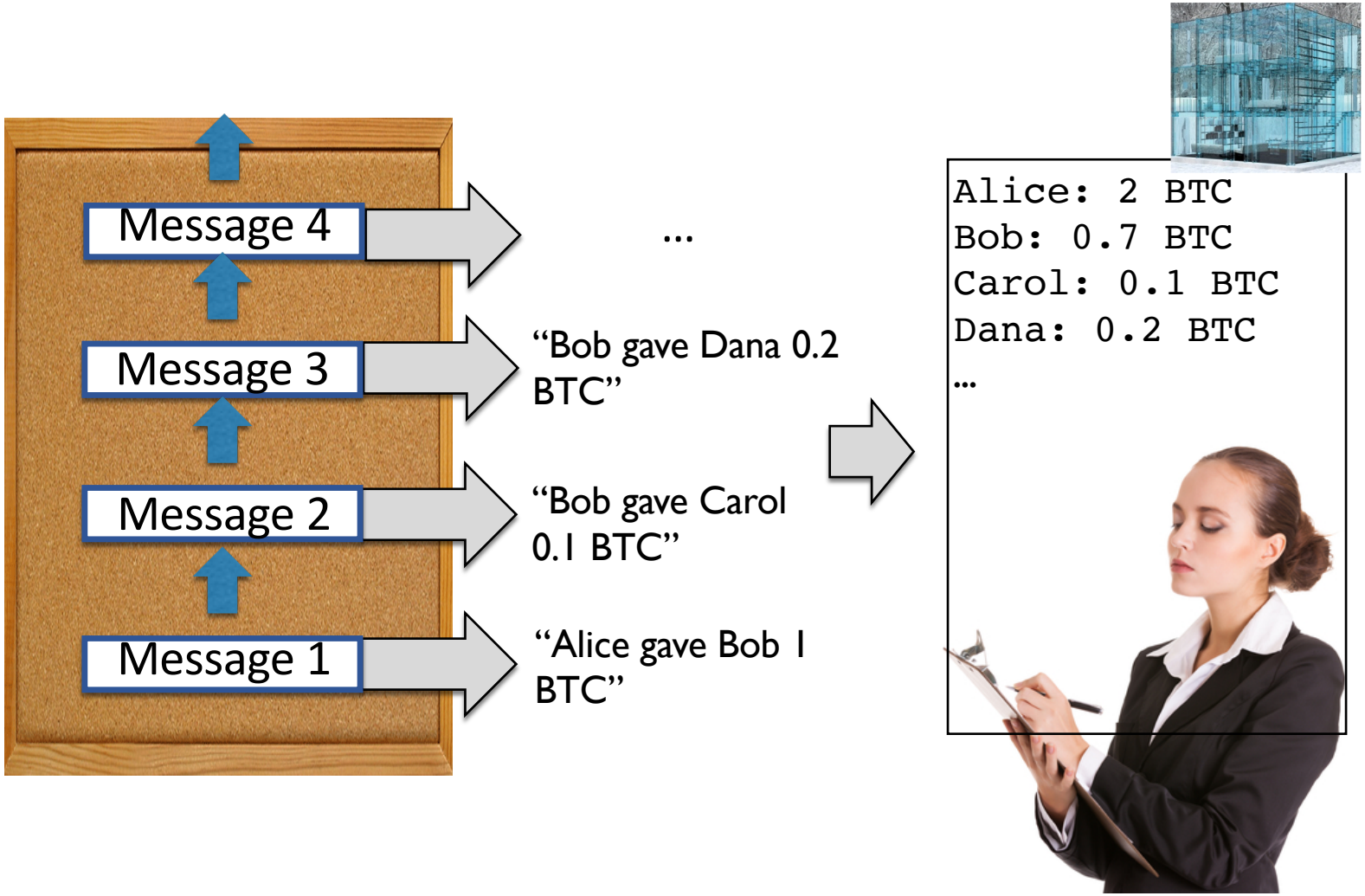


- For transfer of financial instruments
- Up to three days to complete (T+3)
- Many middlemen
- Fragmented records
- Difficult to audit

Blockchains are much faster…

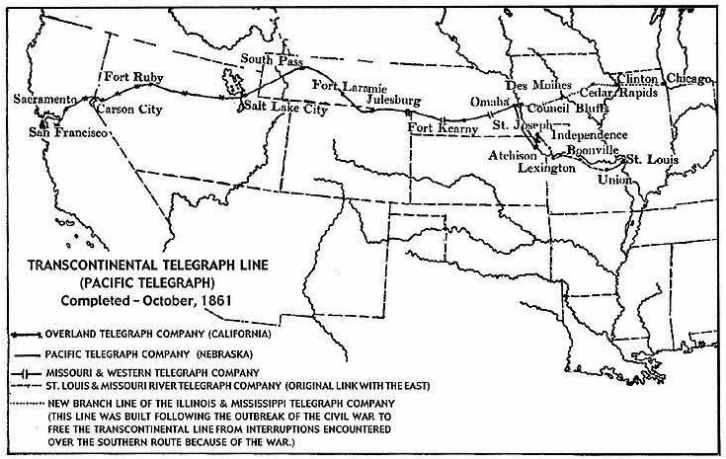


and more transparent…



Mail delivery in 19th-century United States

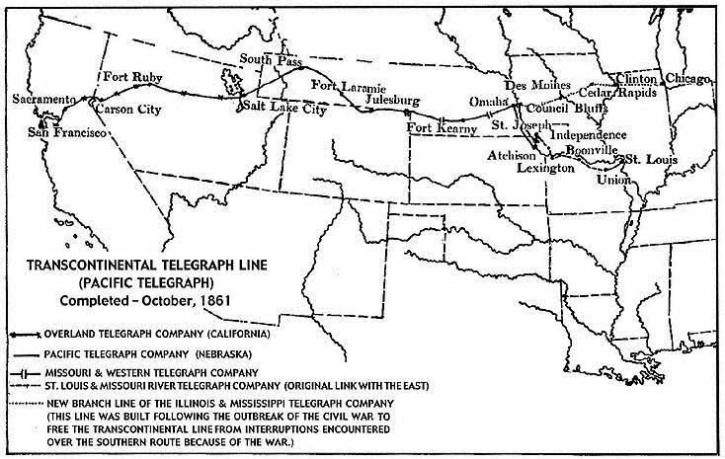
28 Oct. 1861



26 Oct. 1861

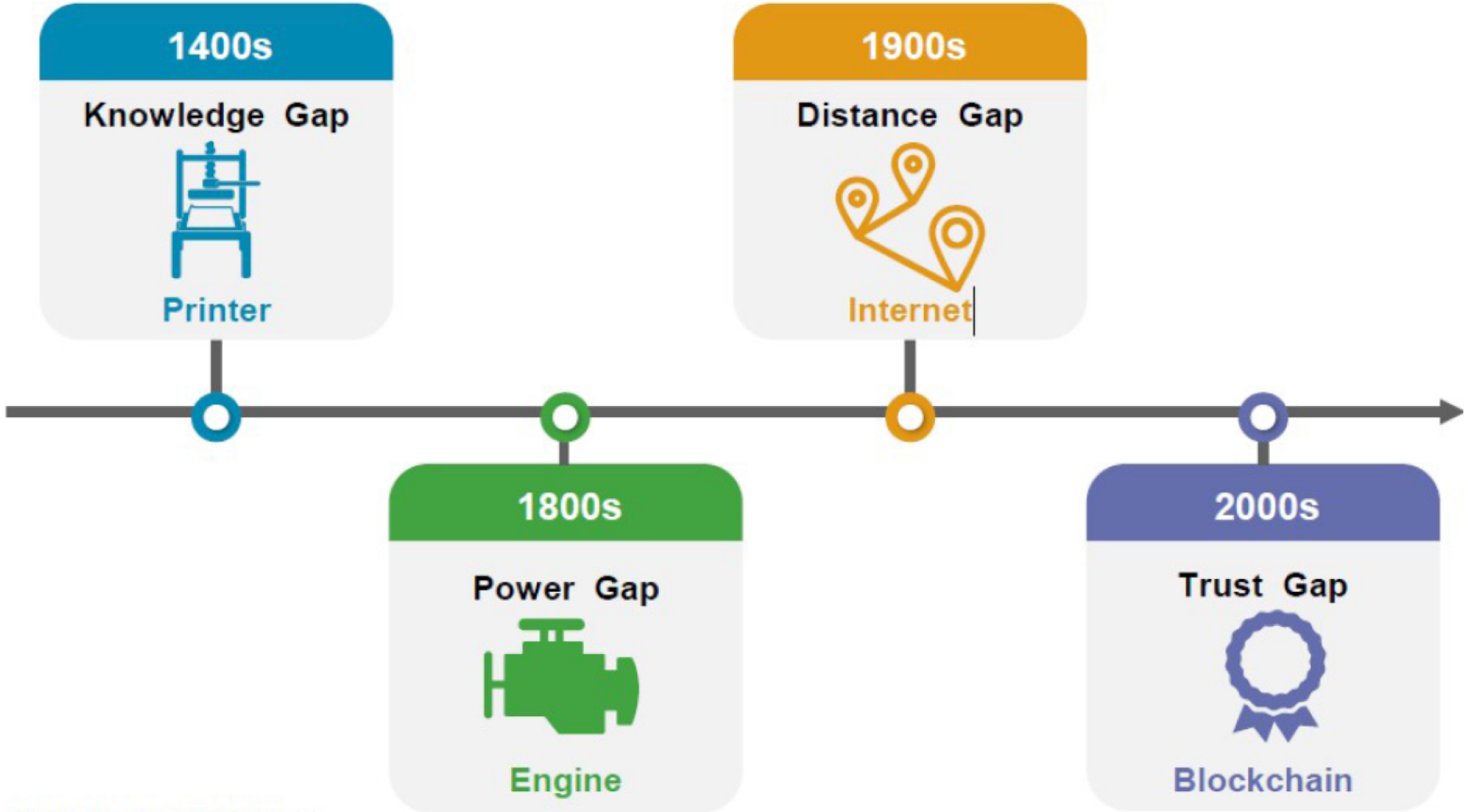
Will blockchains just kill existing settlement systems and take over the world?

28 Oct. 1861



26 Oct. 1861

Will blockchains fix the trust gap?



Source: Richie Etwaru,TEDxMorristown

It’s complicated…
as we’ll see