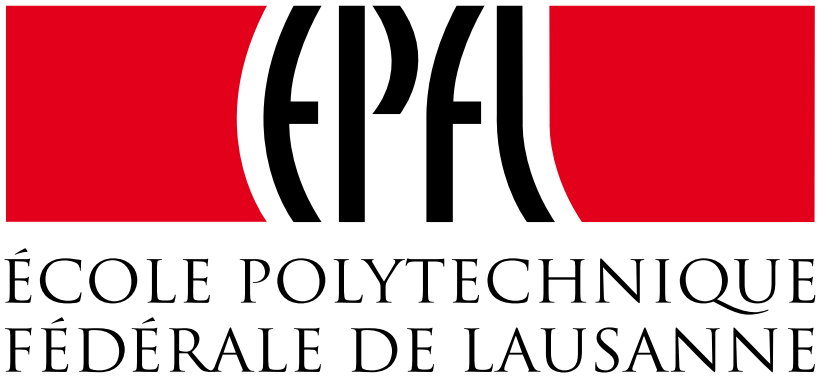
Blockchain for Beginners

Bryan Ford
Decentralized/Distributed Systems (DEDIS)



What is a Blockchain?

In essence, a blockchain is:

- A distributed ledger
- A consensus protocol
- A membership protocol

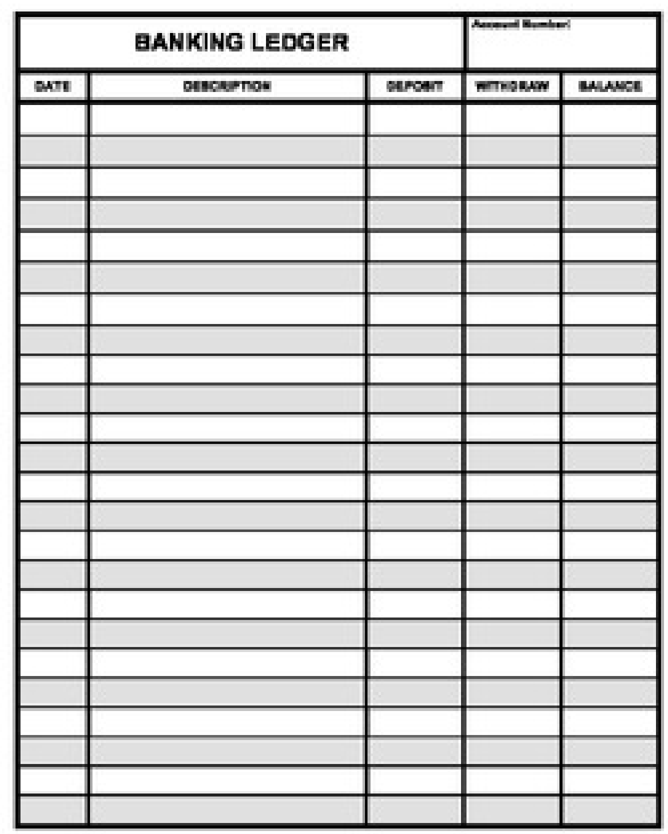
How to track wealth (or anything)?

Things

- Gold, beads, cash...

Ledgers

- Who owns what?



Precedent: the Rai Stones of Yap

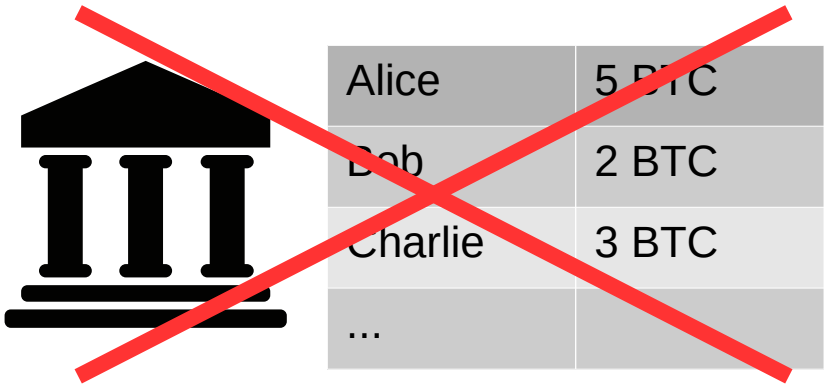
Stone “coins” weighing thousands of kilograms

- Left in place once created (“mined”)
- Ownership transfer by *public proclamation*

(this comparison shamelessly borrowed from Gün Sirer and others)

Distributed Ledgers

Problem: we don't want to trust any designated, centralized authority to maintain the ledger



Alice	5 BTC
Bob	2 BTC
Charlie	3 BTC
...	

Solution: “everyone” keeps a copy of the ledger!

- Everyone checks everyone else's changes to it

Alice's copy

Alice	5 BTC
Bob	2 BTC
Charlie	3 BTC
...	

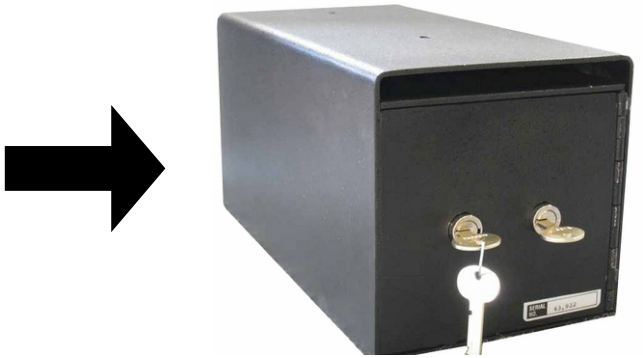
Bob's copy

Alice	5 BTC
Bob	2 BTC
Charlie	3 BTC
...	

Charlie's copy

Alice	5 BTC
Bob	2 BTC
Charlie	3 BTC
...	

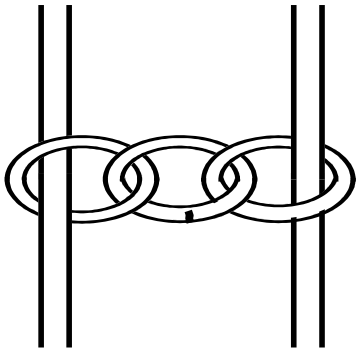
The Basic Goal: to Distribute Trust

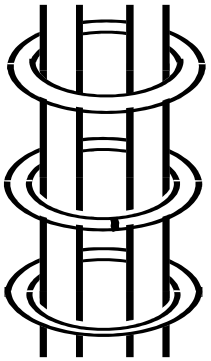


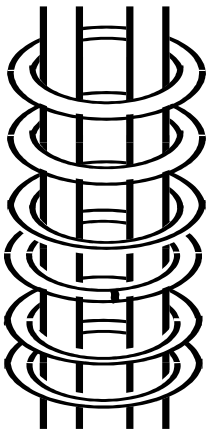
“weakest-link” security

“strongest-link” security in a small group

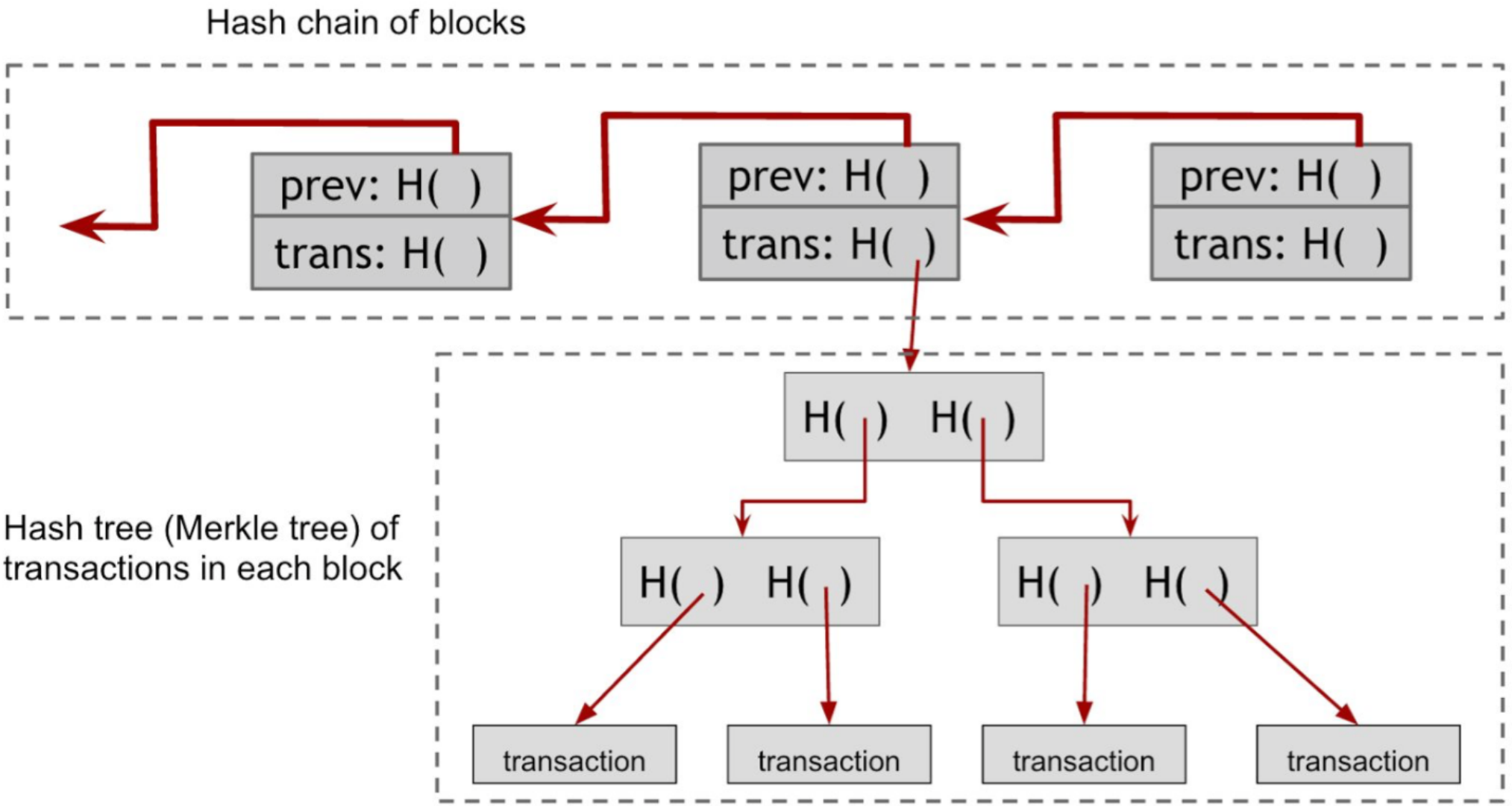
“strongest-link” security in a large group







The Bitcoin Blockchain



The Power of Distributed Ledgers

Can represent a distributed electronic record of:

- Who owns how much **currency**? (Bitcoin) 
- Who owns a name or a digital work of art? 
- What are the terms of a **contract**? (Ethereum) 
- When was a **document** written? (notaries)
- …

What is a Blockchain?

In essence, a blockchain is:

- A distributed ledger
- A consensus protocol
- A membership protocol

Blockchains Require Consensus

Replicating a (fixed) ledger is actually easy…

- Decades-old technology: e.g., **gossip** protocols

But the participants must **agree** somehow on who gets to **extend** the blockchain, and how!

- Must reach a distributed **consensus** on all changes

Nakamoto Consensus

Public blockchains such as Bitcoin, Ethereum use consensus by crypto-lottery

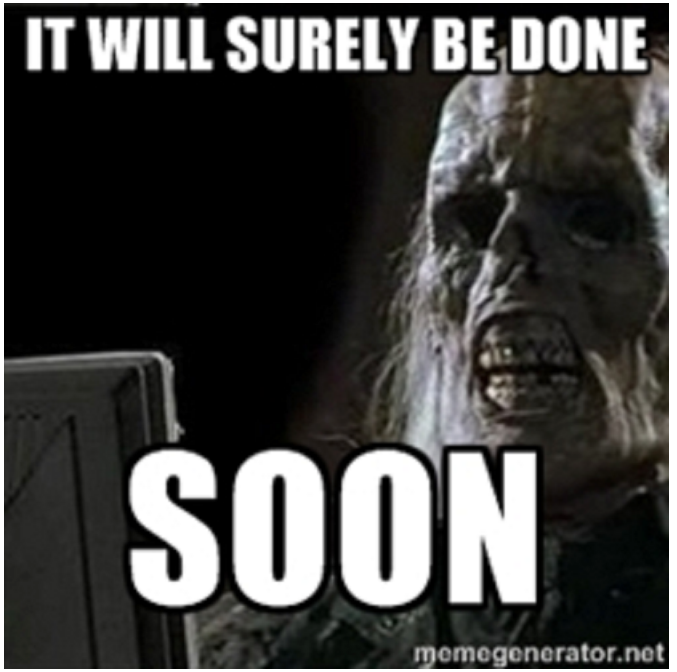
1) **Miners** print their own "lottery tickets" by solving crypto-puzzle (**proof-of-work**)

2) Winner gets to add one **block** to blockchain; typically gets **reward**: e.g., print new money

3) All miners gravitate to **longest chain.** Repeat.

Drawbacks of Nakamoto Consensus

- **Transaction delay**
  - Any transaction takes ~10 mins *minimum* in Bitcoin
- **Weak consistency:**
  - You're not *really* certain your transaction is committed until you wait ~1 hour or more
- **Low throughput:**
  - Bitcoin: ~7 transactions/second
- **Proof-of-work mining:**
  - Wastes huge amount of energy



Scaling Blockchains is Not Easy

Blockchain Scaling Approaches

Avoid the problem:

- Move more work off-blockchain (Bitcoin)
  - Shifts burdens onto users, “trusted” intermediaries
- Tweak tuning parameters (Ethereum)
  - Limited headroom, reduced security margins
- Small, semi-closed groups (Ripple, Stellar)
  - Lose openness, public transparency benefits

Solve the problem:

- Rethink architecture (Bitcoin-NG, ByzCoin)
  - Technically hard but best long-term solution

The Problem with “Off-Blockchain”...

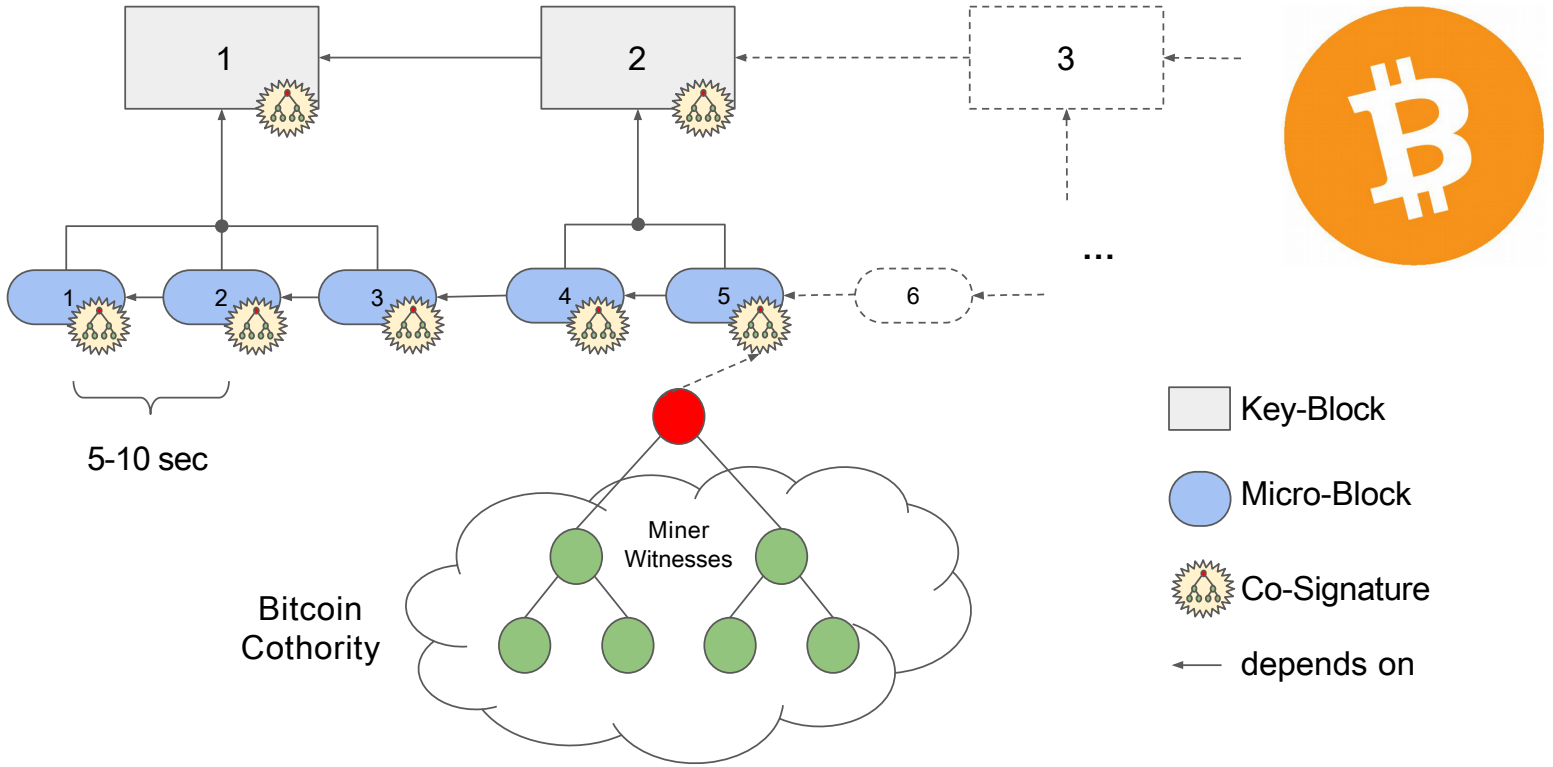
Even if the blockchain is secure, your money isn't!

- The only convenient/feature-rich ways to use are via less-secure Web exchanges, etc.
  - Ask you to “trust them” but frequently compromised

ByzCoin: Fast, Scalable Blockchains

DEDIS lab project presented in [USENIX Security '16]

- **Permanent** transaction commitment in **seconds**
- **700+ TPS** demonstrated (100x Bitcoin, ~PayPal)
- **Low-power** verification on light mobile devices



What is a Blockchain?

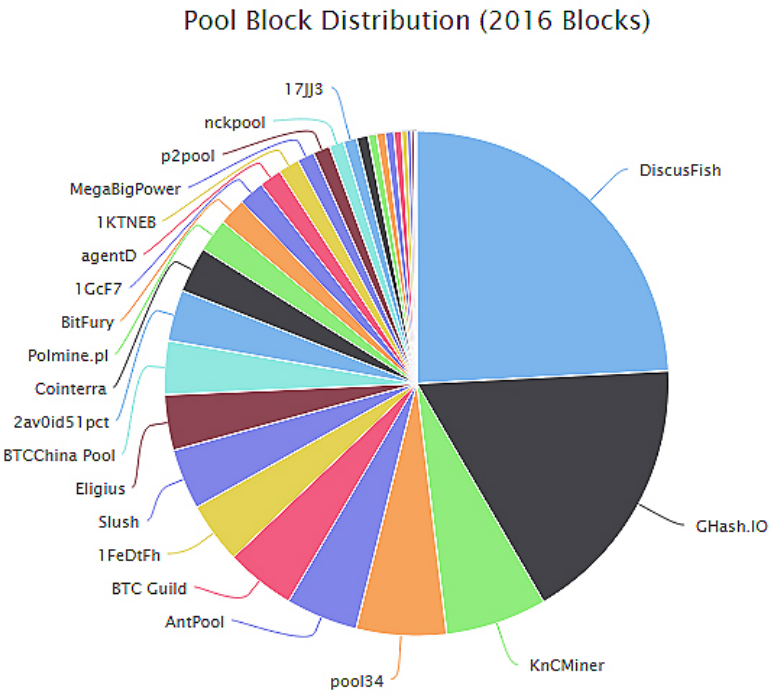
In essence, a blockchain is:

- A distributed ledger
- A consensus protocol
- A membership protocol

Who Participates in Consensus?

Permissionless blockchains (Bitcoin, Ethereum): “anyone” who invests in solving crypto-puzzles.

- Now practical only with ASICs and cheap power
- Re-centralization: e.g., 4 pools now hold >50%



Environmental Costs

Proof-of-work = “scorched-earth” blockchains

- Tremendous energy waste,
  now comparable to all of Ireland
-

Permissioned Blockchains

Just decide **administratively** who participates;
Fixed or manually-changed group of “miners”

- ☺ No proof-of-work needed → low energy cost
- ☺ More mature consensus protocols applicable
- ☹ Higher human organizational costs
- ☹ No longer open for “anyone” to participate

Other Membership Approaches

- **Proof-of-Stake:** assigns consensus shares in proportion to prior capital investment
  - ☺ Could address energy waste problem
  - ☹ Major unsolved security & incentive problems
  - ☹ Just reinvents the shareholder corporation

Open *Democratic* Blockchains?

Proof-of-Personhood: “one person one vote”

- e.g., via Pseudonym Parties [SocialNets ‘08]
- Participants mint new currency at equal rate
  - Decentralized analog to “basic income”?

Blockchains need solid foundations

Conclusion

In essence, a blockchain is:

- A distributed ledger
- A consensus protocol
- A membership protocol

Thank you.

Prof. Bryan Ford, head of DEDIS lab at EPFL.