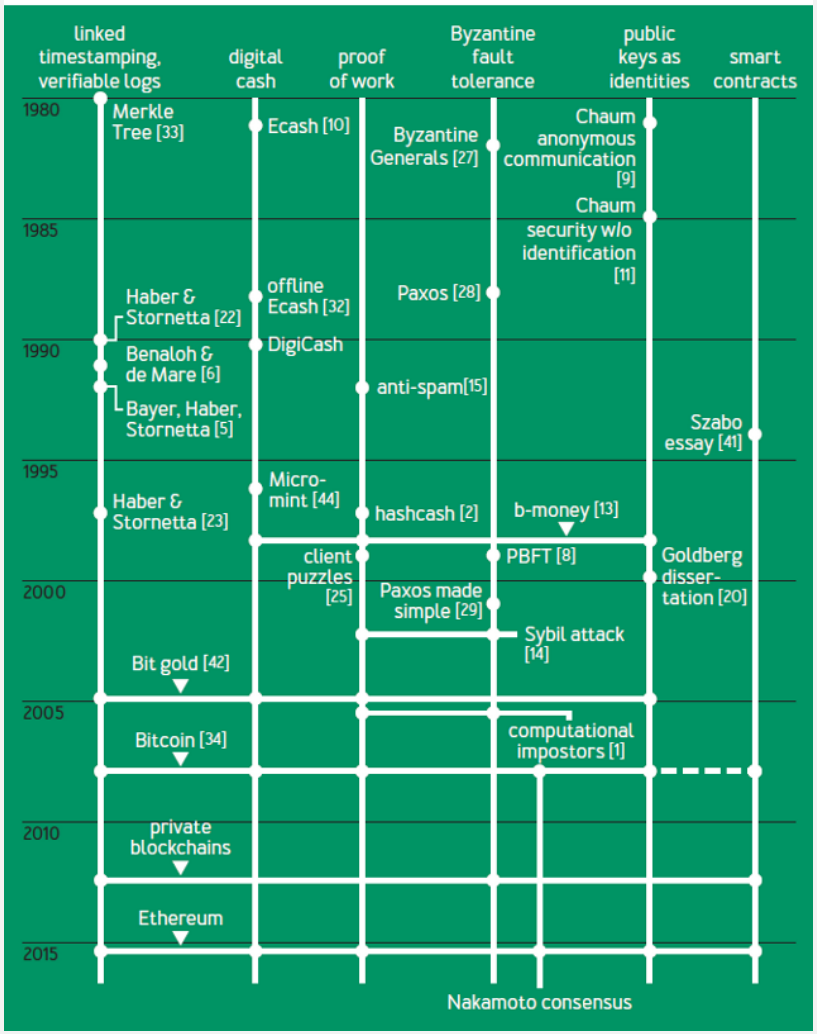
TRANSACTIONS

EJ Jung

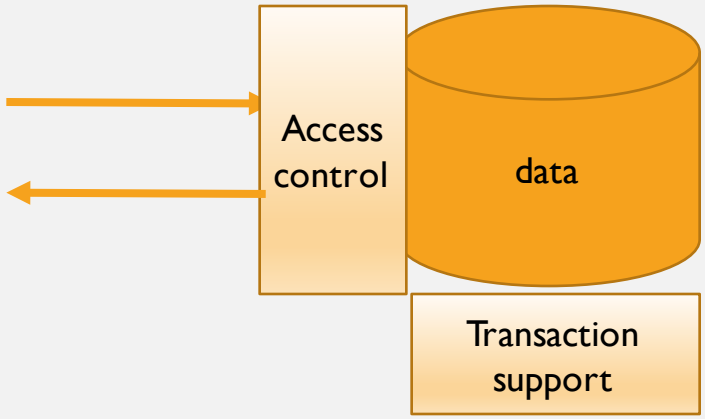
FIGURE 1: CHRONOLOGY OF KEY IDEAS FOUND IN BITCOIN



[image src]

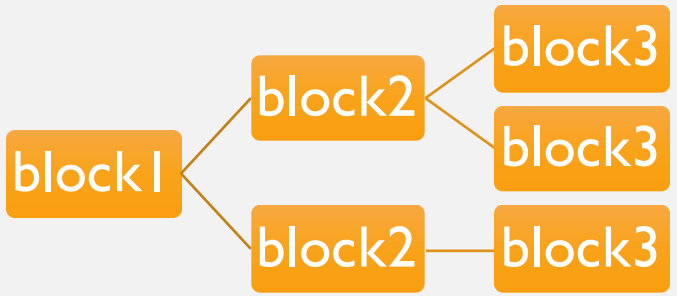
WE NEED TO SHARE DATA

- Example: payment info in *database*
- ACID properties
  - Atomicity – debit/credit happen together or not
  - Consistency - everyone sees the same data
  - Isolation – parallel transaction support
  - Durability – once written, forever written
- Access Control - only authorized user adds data
- Traditionally centralized
  - e.g. Oracle server



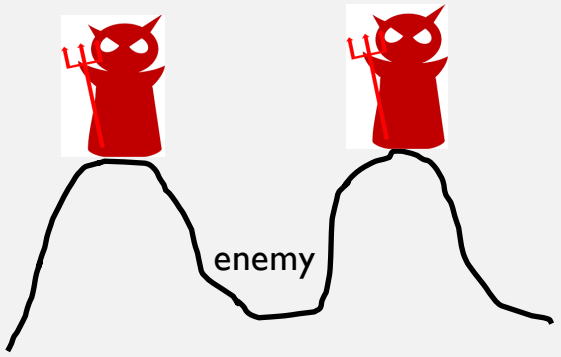
INGREDIENTS FOR DECENTRALIZATION

1. Merkle tree (hash chain)
   - One-way hash functions (mixing colors)
   - Irreversible (Duration)
2. Consensus on hash chain
   - Consistency and Isolation
3. No Centralized Access Control
   - Every user submits its own transaction



HOW HARD CAN CONSENSUS BE?

- Byzantine-faulty users
  - Act maliciously even when there is no gain
  - Replay attack on Bitcoin fork
- Impossibility of consensus (FLP proof)
  - Asynchronous network – one faulty node
  - Synchronous network – 1/3 faulty nodes
  - Alice pays Bob 1 BTC vs. Alice pays Charlie 1 BTC
- System has to have at least 3f+1 nodes
- Sybil attack



Two Generals' Problem

I'M NOT BAD. I'M SMART.

- Altruistic users
- Rational users
  - Act differently from the specification for their own benefit
  - Free-riders
  - Incentive-Compatible
- Byzantine-fault tolerant + Incentive-Compatible = BAR tolerant
- Any cryptocurrency system has to be BAR-tolerant

WHY DO WE NEED PROOF?

- Blockchain = Merkle Tree + consensus on each block
- Cryptocurrency on Blockchain = consensus on transactions + coin generation
- How to achieve BAR-tolerant consensus
  - Leader election - agree on who decides the content of the next block
  - Consensus - agree on the content of the next block

Prove this!!

	Proof of Work	Proof of Stake
Leader election	Bitcoin, Litecoin, Zcash, Monero	Cardano
Consensus		Ethereum/Casper, EOS*

- More proof of consensus: Ripple, Dfinity, Stellar
- Neither: Dash, Filecoin

PROOF OF WORK

- Bitcoin, Litecoin, Monero, Zcash, etc
- There are keys buried *x* feet under. Any key will open this treasure box. Go and dig!

```
while (key not found) {
    grab a spot and dig x feet
}
```

- Why BAR tolerant?
  - Incentives (tx fee and new coin)
  - Fake answers are easily verifiable and rejected

Image src

PROBLEMS OF POW

- More/better resource = more keys faster
  - The richer get richer
- Wasted resources
  - *x* gets bigger over time!
- Blocks are not finalized for a long time
  - Multiple leaders can be elected at the same time
  - (Temporary) forks are not preventable
  - No real-time transaction processing

Image src

PROOF OF STAKE

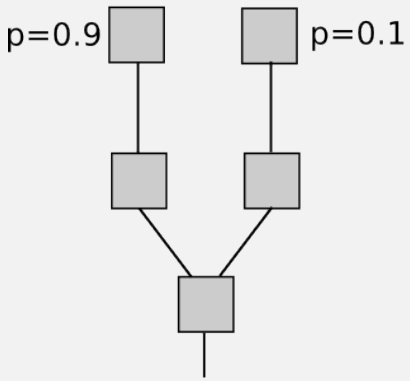
- Ethereum/Casper
  - Users vote on the new block
- Cardano/Ouroboros
  - Users vote on the slot leader
- Direct democracy*
  - (Almost) every node with “stakes(shares)” can vote
- No mining
- Pooling?

ETHEREUM/CASPER/CHAIN

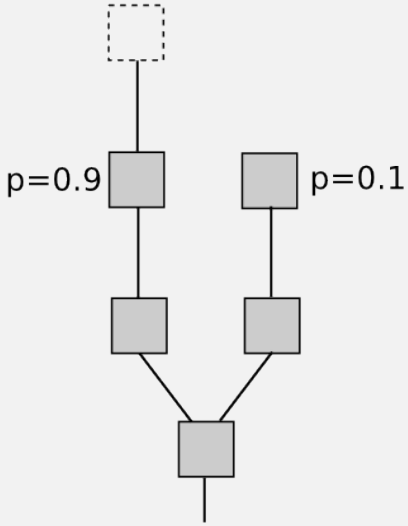
- Chain-based proof of stake
- Each node puts a "stake" in a new block candidate
  - Think of it as a campaign money for election
- Rewards to stakeholders of the winning block (tx fee)
- Penalty to stakeholders of the losing block (slash partial deposit)

ETHEREUM/CASPER/CHAIN

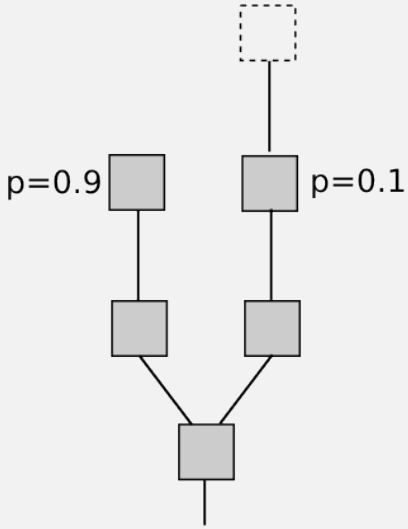
Vote on neither
EV = 0



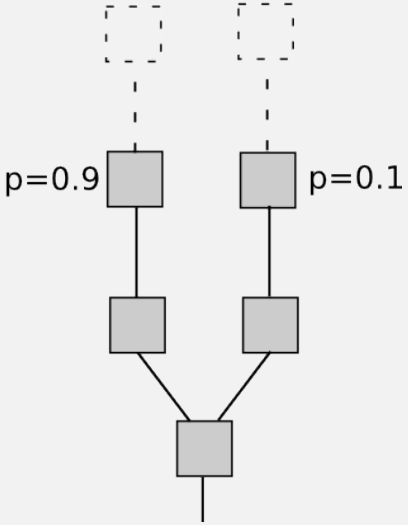
Vote on A
EV = 0.9



Vote on B
EV = 0.1 - 0.9 * 5 = -4.4



Vote on both
EV = 0.1 + 0.9 - 5 = -4



[image source]