- Assign 1 marks back later today
- Assign 2 due Monday evening
- Project 1 - find a group, register for repo; out next week
- Blockchain-based
- Today: BitCoin blockchain; background for Project 1

Key ideas:
- proof of work (A.1)
- blockchain
- P2P transactional ledger

Key challenges:
- Double spending
- Trust in network
- Incentives
Alice $\rightarrow$ Bob: trust Alice? Who is Alice? I give Bob 1 BitCoin (BTC), is it Alice who sent me the msg?

Bob knows key for Alice's pub

Mag signed by Alice (A) is easy to verify

Trusted source w/ trials #s for each BT

Bank:
1. Get 1 BTC
2. #544...
3. $S_A (msg)$
4. P: Check #544... is Alice's + it's not spent
5. B: Check

$P2P$: everyone knows what everyone has

- Decentralized
- Nodes are equivalent
- Open
network

\[ C \xrightarrow{\text{ack}} A \]
\[ A \xrightarrow{\text{msg}} B \]
\[ S_A(\text{msg}) \xrightarrow{\text{ack}} B \]
\[ \text{check msg w/ network} \]
\[ \text{ok} \]

\[ \text{Concurrency} \]
\[ \text{Double spending} \]

\[ \text{tx commit} \rightarrow 0 \]
\[ \text{tx commit} \rightarrow 0 \]
\[ \text{tx commit} \rightarrow 0 \]
\[ \text{tx commit} \rightarrow 0 \]

2 PC
2 phase commit
Doesn’t scale
Used DBMS

phase 1

phase 2

proof of work: eliminates byzantine

Raw CPU power
(or GPU)

\[ \text{txn} \]
\[ \text{txn} \]
\[ \text{txn} \]

node N

\[ \text{Block B} \]

\[ \text{txn 1} \]
\[ \text{txn 2} \]
\[ \text{txn 3} \]

subtree N

\[ \text{find nonce} \quad \text{s.t.} \quad h(B) \leq \text{target} \]
\[ h(B) = 3a\times c2a6,000 \]
Only generate blocks on the longest chain in Blockchain.

Win: Observed and accepted by majority of nodes.

Each node validates tens of mining blocks.

Time to follow a block containing a transaction.
Miner

Server

Register
settings

getNodes

M2
M3

hBeat

hBeat

hBeat

Miner-server protocol

Intersecting Shapes = conflict

Black shape + Blue shape conflicting