Admin:

Quiz - 24 hr extension with no questions asked
Projects - meetings

Today:

Digital Payments

Bitcoin
Representing value: bits vs. atoms

Gold atoms:
- unforgeable & scarce
- "ownable"
- transferable (multiple times one after another)
- decentralized
- divisible & combinable
- anonymous

Bits:
- Easy to generate bits (dig sigs?)
- Easy to copy \[\Rightarrow\] double spending \[\Rightarrow\]
- Need "accounts" to prevent/detect double-spending
- accounts may be centralized or decentralized (bitcoin)
- transferable (\& checks)
- divisible & combinable
- not as anonymous (PK = identity)
Electronic Checks

With TTP (trusted-third party = bank):

Bank has PK_B, SK_B
User has PK_u, SK_u

certificate on PK_u (signed by B)

Check = cert on PK_u, signed by B

("Pay PK_v $100, date, serial #")

signed by U

Bank processes check once. (ser # prevents replay = double spending)

Usual problem: overdraft

Privacy: Bank & Merchant know exact details

Bank maintains transaction history & accounts
Coins vs Checks

Coin: bit string signed by bank = coin "blindly"

bank can recognize coin when deposited

Checks: Replace bank B by "public ledger" (append-only log of xacts)

- IDs are just PKs, not more (-anonymous, pseudonymous)

ledger =

<table>
<thead>
<tr>
<th>xact 1:</th>
<th>$100</th>
<th>from: PKu</th>
<th>to: PKv</th>
<th>serial #</th>
<th>signed by U</th>
</tr>
</thead>
<tbody>
<tr>
<td>xact 2:</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

ledger = entire state of system!

where do accounts get value?

Anyone can check that xact is valid
Public Ledger:

Centralized or decentralized?

Who can read? write? (create, act, add to ledger)

Decentralized public ledger a key Bitcoin contribution

---

Bitcoin (Nakamoto 2009)

Public ledger records all transactions

Decentralized maintenance of ledger based on POW to validate blocks put on the "blockchain" (ledger)

Uses bitcoin to incentivize maintenance

\[
\begin{array}{c}
\text{\textbf{B}_0} \\
\rightarrow \\
\text{\textbf{B}_1} \\
\rightarrow \\
\vdots
\end{array}
\]

= Public ledger

blockchain

"genesis" block
Block-chain

Each block contains:

- hash of previous block (as "chain")
- PK of creator (as "miner") \( \text{null} \| \text{hash}(pk) \)
- nonce (for puzzle - see later)
- Transactions:
  1. coinbase = fee to creator = 12.5 $B$
  2. Merkle tree of transactions
    - Each transaction has
      - inputs: block & output # where created (or coinbase) with sigs
      - outputs: PKs (actually hashes) of recipients, with amounts
      - Value (input) ≠ Value (output)
      - Inputs not previously spent
      - Input sigs valid
      - Change => miner as exact fee
Communications Network

- Anyone (with bitcoins) can propose a transaction for inclusion in public ledger.
- Transaction is only valid if it is on ledger.
- Blocks distributed to other nodes via a "gossip" protocol.
- New blocks posted about 1/10-minute.
- If network partitioned, can be lack of consensus as to what is current state of blockchain.
- Even if no partition, several nodes may propose what should be "next" block on blockchain. Bitcoin provides a distributed consensus protocol (perhaps its biggest contribution)
Consensus Protocol

Consensus via race to solve block puzzle first
"nonce" is solution to puzzle if
\[ H(\text{block}) \leq 2^{256-d} \]
\(d\) includes block header, nonce,
\( H(\text{PK(miner)}) \), Merkle root of txs
\(d \geq 74.5\) now (e.g. start with 74.0 bits)
Takes about \(2^d\) tries to find a good nonce.
\(d\) adjusted so soln found about every 10 minutes
"POW" = proof of work
Prob (good guys find soln first)
= \% of hash power owned by good guys
Once a solution is found, it is broadcast.
All other nodes work to extend longest block chain
Hash power & 51% attack

Let $p = \text{prob honest node finds next block}$

$g = \text{"malicious"}$

$g^2 = \text{"miner will overtake main chain if it stays 2 nodes behind"}$

\[
= \begin{cases} 
1 & \text{if } g \geq p \\
\left(\frac{g}{p}\right)^2 & \text{if } g < p
\end{cases}
\]

E.g. \[\left(\frac{0.99}{0.51}\right)^{144} = 0.003148\]

"wait 6 blocks" (one hour) to "confirm payment received"
Mining Pools

Many miners combine forces to even out variance in payments.

Make "pay to" for coinbase = mining pool operator can show "POW" for "almost solves" to pool operator Reward split among pool miners according to work done
Bitcoin (In)efficiency

- Ledger getting big (197GB)

- Electricity use 500 kWh/transaction
total ≈ Bangladesh
  0.25% of all electricity

- Time to "settle" one hour? (Latency)
  more?

- Throughput
  VISA 5000/sec
  Bitcoin 5/sec
Variations & Extensions

"Side chains"
"Smart contracts"
"Anonymity & Zcash"
Algorand (Micali) - not POW
"Proof of stake" (more generally)
Probabilistic payments?
Memory-hard POW

NFTs - Non-Fungible Tokens