Admin:  Pset #4 out today. (6.857 coins!)

Today:  E-cash & 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
  =) double spending
  Need "accounts" to prevent/detect double-spending
  accounts may be centralized or decentralized (bitcoin)
  transferable (x 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_u $100, date, serial #")

signed by U

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

Usual problem: overdraft

Privacy: Bank & Merchant know exact details

Bank maintains transaction history & accts
Coins vs Checks

Coin: bit string signed by bank $\equiv$ 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 =

\[
\text{xact 1: } \begin{align*}
\text{from: } & \text{PK}_u \\
\text{to: } & \text{PK}_v \\
\text{amt } & \$100 \\
\text{signed by } & U
\end{align*}
\]

\[
\text{xact 2: } \vdots
\]

ledger = entire state of system!

where do accts get value?

Anyone can check that xact is valid
Public Ledger:

Centralized or decentralized?
Who can read?
write? (create, add to ledger)

Decentralized public ledger is key
Bitcoin contribution

Bitcoin (Nakamoto 2009)

Public ledger records all transactions
Decentralized maintenance of ledger
based on POW to validate blocks
put on the "block chain" (ledger)
Uses bitcoin to incentivize maintenance

\[ B_0 \rightarrow B_1 \rightarrow \ldots \]
blockchain
Block chain

Each block contains:

- hash of previous block (i.e., "chain")
- PK of creator (i.e., "miner") (\text{real} || \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) \geq Value (output)
       - inputs not previously spent
       - Input sigs valid
       - Change \to miner as exact fee
Communications Network

- Anyone (with bitcoins) can propose a transaction for inclusion in public ledger.
- Transaction is only valid if it's on ledger.
- Blocks distributed to other nodes via a "gossip" protocol.
- New blocks posted about 1/ten-minutes.
- 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

\(d \times 74.5\) 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 blockchain

\[ \text{genesis block} \rightarrow \rightarrow \cdots \rightarrow \text{fork in blockchain} \rightarrow \text{longest chain wins} \]
Hash power & 51% attack

Let \( p \) = prob honest node finds next block

\( q = \) "malicious" "" "

\( b_2 = \) "" " miner will overtake main chain if it stays 2 nodes behind

\[
\begin{align*}
\text{if } q &> p \\
\left(\frac{q}{p}\right)^2 &\text{ if } q < p
\end{align*}
\]

e.g., \( \left(\frac{0.49}{0.51}\right)^{144} = 0.003148 \)

"wait 6 blocks" (one hour)ry 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 solutions" 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-hord POW