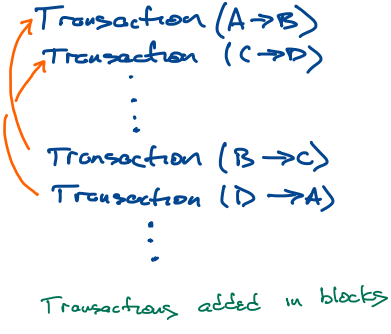
Announcements

- Exams are finished, just need to double-check current averages
  Will return tonight
- Final Problem Set due Friday
- Goal is to have Exam 3 ready next Monday (11/23)
  Due 12/3
- *Please fill out course evaluation when you get the email!*

High-level idea behind Bitcoin

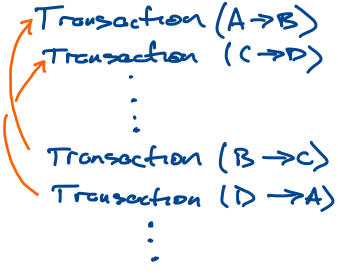
Ledger of Transactions



Transactions added in blocks

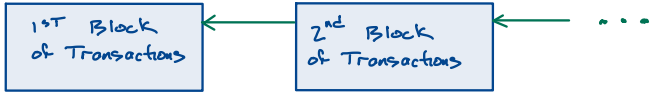
High-level idea behind Bitcoin

Ledger of Transactions



Transactions added in blocks

Blockchain



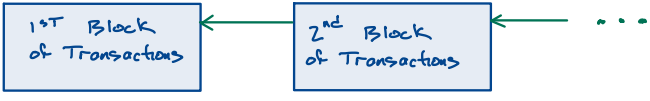
High-level idea behind Bitcoin

Ledger of Transactions

Transaction (A → B)
Transaction (C → D)
⋮
Transaction (B → C)
Transaction (D → A)
⋮

Transactions added in blocks

Blockchain



Node maintainers keep set of

Unconfirmed Transactions

Miners form blocks
If added to blockchain, miner gets paid
Requires "proof of work"

Cryptographic protocols used in Bitcoin

- **Hashes**: SHA256( ) and RIPEMD160( )
  Several places combined: hash160(x) = RIPEMD160(SHA256(x))

- **Signatures:** ECDSA using curve secp256k1
  - 256-bit key gives security level of 128 bits
  - RSA, DSA would require 3072-bit keys for equivalent security level
    (See October 26 files for reference)

Structure of a Bitcoin transaction

Alice Bitcoin Wallet
Public Key
Private Key

Bob Bitcoin Wallet
Public Key
Private Key

How does Bob transfer 1 BTC to Alice?

PREVIOUS TRANSACTION
Bob receives 1 BTC

Structure of a Bitcoin transaction

Alice Bitcoin Wallet
Public Key
Private Key

Bob Bitcoin Wallet
Public Key
Private Key

How does Bob transfer 1 BTC to Alice?

PREVIOUS TRANSACTION
Bob receives 1 BTC

Transaction Bob $\xrightarrow{1\ \text{BTC}}$ Alice

Input: PrTx hash = SHA256(Previous Transaction)
Acts as identifier/pointer

ECDSA(PrTx hash)
Bob's Public Key

Output: Value in Satoshi's (1 BTC = 100 000 000 Satoshis)

hash160(Alice's Public Key)

Structure of a Bitcoin transaction

Alice Bitcoin Wallet
Public Key
Private Key

Bob Bitcoin Wallet
Public Key
Private Key

How does Bob transfer 1 BTC to Alice?

PREVIOUS TRANSACTION
Bob receives 1 BTC

Transaction Bob $\xrightarrow{1\ \text{BTC}}$ Alice

Input: PrTx hash = SHA256(Previous Transaction)
Acts as identifier/pointer

ECDSA(PrTx hash)
Bob's Public Key

Hash must match output of prev transaction

Output: Value in Satoshi's (1 BTC = 100 000 000 Satoshis)

hash160(Alice's Public Key)

Some interesting (?) references

- Bitcoin protocol documentation:
  https://en.bitcoin.it/wiki/Protocol_documentation
- Bitcoin explorer: https://bitaps.com
- Bitcoin difficulty: https://btc.com/stats/diff
- The DAO on Ethereum:
  https://en.wikipedia.org/wiki/The_DAO_(organization)
- CryptoKitties (really):
  https://www.vox.com/videos/2018/5/24/17390778/cryptokitties-blockchain-explainer