Richard Darst

2014-02-14

Group meeting outline

- Discussion of how bitcoin works (150% of time)
- Discussion of *Kondor D, Psfai M, Csabai I, Vattay G (2014) Do the Rich Get Richer? An Empirical Analysis of the Bitcoin Transaction Network. PLoS ONE 9(2): e86197. doi:10.1371/journal.pone.0086197* (40% of time)
- Discussion of recent bitcoin news (25% of time)

What do you want to do?

Real money: why is it valuable?

Real money: why is it valuable?

- Others accept it
- It is scarce

Real money: why is it valuable?

- Others accept it
- It is scarce

Bitcoin is an agreement to follow certain rules which:

- Enforce scarcity
- Allow verifiable transaction between entities.

And somehow, people have started accepting it!
There is a delicate balance of technology providing incentive to obeying the rules.

Key cryptographic concepts

- Asymetric cryptography and digital signatures
- Hash functions

Key cryptographic concepts

- Asymetric cryptography and digital signatures
  - *Public key* and *private key*. Public key can be broadcast and anyone can verify a *signature* from the private key.
  - Allows one to prove identity (and in this case, ownership of coins)
- Hash functions

Key cryptographic concepts

- Asymetric cryptography and digital signatures
  - *Public key* and *private key*. Public key can be broadcast and anyone can verify a *signature* from the private key.
  - Allows one to prove identity (and in this case, ownership of coins)
- Hash functions
  - Take a large amount of data and return a small function of that data
  - example: d0a41012d25416be4504e395b34f3b06
  - Small changes in input yield complete changes in output
  - Impossible to get a specific output except by trial and error.

What is a bitcoin?

- Bitcoins do *not exist*
- Value in bitcoin is everyone agreeing that you have a positive balance (sum of all transactions to your key).
- The only thing you own are private keys allowing you to sign a message sending money to someone else.
- Example bitcoin address (public key): 17LgTwEMbLWk6YhQwup3b177HbXqYYb4cb
- "Losing bitcoins": throwing away the private key.

Transactions

- Multiple “in” transactions of a certain value
  - Signed by private key of each input address.
- Multiple “out” transactions of a certain value
  - Designating new owner’s public key
- *transaction fee*
- Identified by another hash

Verification of transactions

When a node wants to add a transaction to the public ledger, they check:

- Every input signature matches
- Every input transaction exists
- Every input transaction has not been spent previously

The Block Chain

- Public ledger of all transactions
- Each block depends on hash of the previous one
- Requires large computation power to “verify”
- Produced at 10 minute intervals.

One block

- Hash of previous block
- Record of all transactions (hashed in)
- Timestamp
- The block hash itself must start with a certain number of zeros, e.g.: 00000000000b4eb057d098453bc6b98c
- Finding this hash is trial and error and takes a lot of CPU power.
- Everyone wants to race to find the next block first

Incentives for block creation

- You get 25BTC for each block mined
- You get sum of all transaction fees you included
- Your block is only accepted if other people use yours as the "next block".
- Everyone agrees that the longest continuous block chain is the correct one.
- Checking that you made the block correctly is easy (hash it, verify all transactions in it) and if you cheated your block won't be accepted by the network.

The network

- Peer to peer network: all transactions and all blocks broadcasted to everyone.
- Local rules allow the network to come to a consensus.
- Tends to be organized in “hash pools”

Possible attacks

- Change the block chain: can't be done without invalidating everything since then
- Replace the block chain
  - Make a longer blockchain than the "real" one.
  - Requires extreme computational power.
- Transaction based attacks:
  - Receiver accepts transaction but it isn't included in the blockchain.
  - Sender sends money and it is included but not seen by sender (*transaction malleability*)

Practical details

- Addresses
- ...

Competing cryptocurrencies

- Litecoin - fork of bitcoin
  - Memory-bound, not CPU-bound, so less advantage to professionals with dedicated hardware
  - Faster block creation - faster confirmation.
- Dogecoin - litecoin derivitive
  - Even faster block creation
  - No maximum limit of coins.
- Zerocoin
  - Bitcoin "add-on" to bitcoin / future independent currency
  - Zero-knowledge proofs providing full anonymity
- Peercoin
  - More equitable, new mining does not go to those with most CPU power but those who have coins.
  - Steady inflation

End part 1.

Questions?

-