Decentralization and Incoordination

Thaddeus Dryja <tdryja@media.mit.edu>

Blockchain Protocol Analysis and Security Engineering
2017-01-26

Decentralize everything

- Are we really talking about decentralization?
- Catch-all phrase - let’s separate meanings
- We do not yet have formally defined attributes like in cryptography (Confidentiality, non-repudability, etc) and this talk won’t provide any (sorry) but we can better define terms

Decentralization

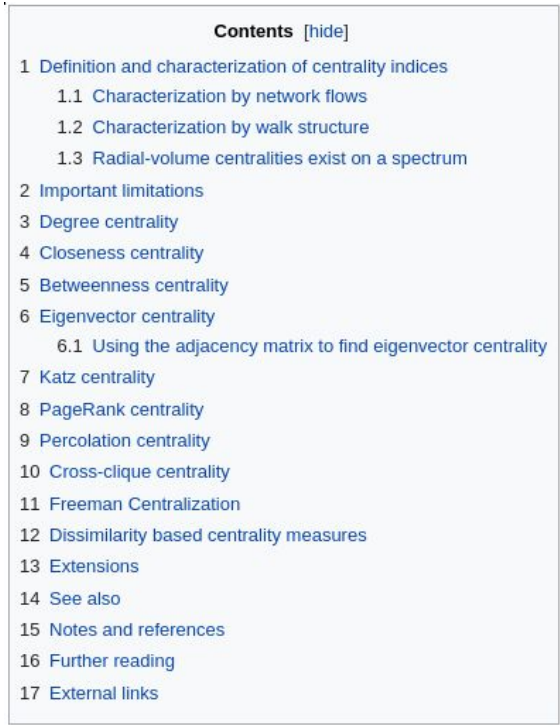
- Not mentioned in the Bitcoin paper
- Frequently cited as a property or goal of blockchains, currencies

In this talk:

- How to quantify (de)centralization?
- Why do we want it?
- How about (in)coordination?

Centrality

- For graphs / networks
- Rigorous, but lots of different definitions!
- These metrics do help
  - Remove single points of failure
  - Add redundant links
  - Help prevent monopolies



Wikipedia “Centrality”

Decentralization is the means

- Not the ends. Ends is uniform access. (censorship resistance), nobody in control
- Decentralization helps - fully centralized means easy to deny access
- Even if decentralized, the network can adapt and censor transactions

Cryptocurrencies and consensus

- With gold, everyone must agree that gold is money; use physics to determine allocation
- With p2p currency, allocation must be agreed upon.
- If people agree that you don’t have gold, you may still have gold
- If the network agrees you don’t have bitcoins, you don’t have bitcoins

Centralization and consensus

- With 1 entity in change, consensus is easy
  - If the bank decides than now you don’t have a balance, sorry for your loss
- Decentralization can impede changes
  - Hard to get 1000s of independent entities to decide you don’t have a balance. Most of them don’t know you and don’t care.

Bitcoin decentralization

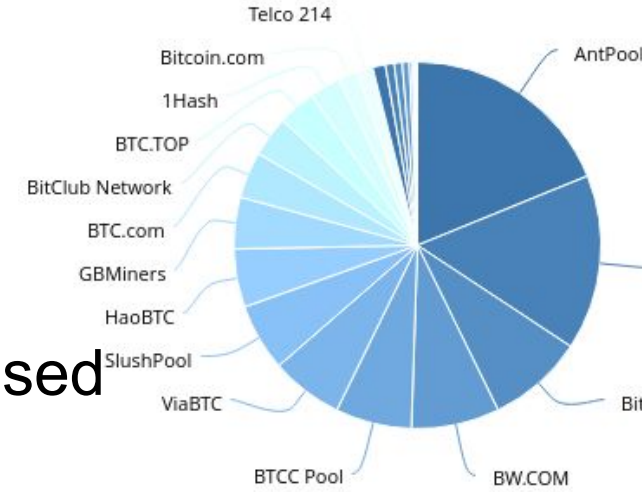
- P2P Network fairly robust (~5K listening, tor)
- Transaction graph somewhat noisy
- Heterogeneous node software
- Mining not very decentralized
  - Wait, how do we know?

Natural tendency to coordinate

- 2nd law of blockchaindynamics:

  Data broadcast is known forever
- 3rd law:

  Any available sequence of bytes will be used for ads, memes, spam, etc
  - Vanitygen, GPU based address brute forcer
  - Coinbase input - supposedly anonymous miners all advertise their names



Why do we know this?

This is normal

- Mechanism design is adversarial to users!
- People want names. Companies want to advertise.
- Vanitygen author doesn’t think they’re hurting the bitcoin network
- Neither do miners branding their coinbase inputs… but they are

Ethereum and decentralization

- Ethereum is in some aspects, more decentralized than Bitcoin
- GPU based mining reduces capex, shorter block times both help smaller miners
- Threat of PoW obsolescence prevents development of ASICs
- Wait… threat?

Ethereum and coordination

- End of proof of work is not in the code; agreement on how the code should change
- Accounts; more state than utxos
- Foundation; known programmers, exchanges, people mostly agree on goals
- Coordinate and ‘fix’ problems with a hard-fork

Ethereum and coordination

- Decentralized, but coordinated
- Influence and hierarchy to follow
- In ethereum’s case, most people wanted this coordination
- Robust against some attacks (DoS)
- Not robust against majority decisions

  (democratic wolves attack)

Stop coordination: are you sure [Y/n]?

- Antagonistic to users; prevent even majority of users from changing the system
  - Prevent majority from recognizing it's a majority
  - Prevent assembly, free speech
  - Undemocratic
- Design a system the designers can't control
  - Scary right? Do you want that?

Impede coordination

- Remove coinbase input, force new output addresses
  - People may brute force signature R values!
- BIP69, canonical sorting of input / outputs
- Link economic rewards to privacy
  - One-time use signatures
  - Lose privacy, immediately lose money

Eliminate signal from data

- From UI, from codebase
- Research directions: eliminate history?
- Obscure interface points
- Eliminate … progress?
  - Many Bitcoin devs want to improve bitcoin; but there may be a limited window of time for improvements
  - Window for hard forks may already be over

Ideal uniform access

- Miners don’t know what they’re mining
- Senders aren’t sure where they’re sending
- Receivers don’t know where it came from
- Nobody knows where exchanges are
- System is auditable but not attributable
  - Impractical now; who verifies? Trust is much faster

Rule-set Heat-Death

- If large scale coordination isn’t possible, modifications can’t happen
- BIP9 doesn’t work if people don’t agree on what the soft-fork bits mean
- Immutable, but also stuck; tradeoff