Lecture 6 - Flaws

Rylan Schaeffer and Vincent Yang

May 5, 2016

Note: This lecture is based on Princeton University's BTC-Tech: Bitcoin and Cryptocurrency Technologies Spring 2015 course.

Community Failure

- System completely controlled by just a handful of people.
- Investing

  People prefer to sit on the money and not spend
- Block cap - set by Satoshi to be far above what would be hit; prevents network DOS.

  Need hard fork to make changes, which should have been possible.

  Hard fork is a change that has all users upgrade, without the possibility of reverting.

Full Block Chain

- Artificial cap of 1 mb per block has shifted network capacity to near full
- In July, someone did a stress test and flooded the network with transactions. At that level, about 700 kb of transactions were able to go through per second, or about 3 payments per second.

  In theory, it can hit 1000kb but sometimes miners produce small blocks, even empty blocks, despite the existance of transactions that are waiting to be confirmed.

  The large number of txs waiting to confirm seems to largely be caused by the Chinese "Great Firewall" system.

  2mb is twice as big, would mess up their advantage
- The average is currently at the cap - 700kb.
- There are frequent times when Bitcoin can't keep up with the transaction load, even when all blocks are max size.
- Networks are incredibly unreliable when they run out of capacity. (e.g. DDOS)
- Paxos problem - fully possible for a transaction to never be verified. It is impossible to depend on the network because you don't know if the payment will go through since congestion is so bad that even minor spikes drastically change network conditions.

  The average time is 49 minutes, but it is easily possible for it to reach upwards of 14 hours.
- Why not just raise the capacity?
  - Block chain is controlled by two Chinese miners (over 50% of hash power)
  - Miners refuse to switch to a competing product because of loyalty, and causing panic.

    - They (Bitcoin Core developers) won't let it grow because they don't want news to cause panic.
    - Chinese Firewall

      Moving data across the border is so broken by the firewall that it barely works at all.

      Currently, they can just barely maintain connection and claim the reward. If it gets more popular, taking part might be too difficult and they'd lose income.

- Due to severe mismanagement, "Bitcoin Core" project wasn't going to release a version with a higher block size limit.

  Users could cast a vote by using BitcoinXT. If 75% was reached, the bigger blocks would be allowed.

- BitcoinXT
    - Somehow pushed emotional buttons - one was the admin of the bitcoin.org website and top discussion forums
    - In the past, he allowed discussion of criminal activity in the name of 'freedom of speech'. However, he claimed XT did not represent "developer concensus", and was not really bitcoin.
    - Voting was an abomination, because "One of the great things about Bitcoin is its lack of democracy".
    - He worked to kill XT, starting with censoring Bitcoin's primary communication channels - anything that had "Bitcoin XT" was erased, and XT couldn't be linked to or mentioned anywhere on the official site. Anyone trying to do as such was banned.
    - For the first time, investors couldn't get a clear picture of what was happening. Most people have no idea that the system is about to reach capacity.

- Why is Bitcoin Core keeping the limit?
    - Satoshi left program to Gavin Andresen, an early contributor. Gavin was just pushed with the responsibility - he didn't want it. He brought on four other developers.

      Side note - he lost commit access on May 2nd.
    - One such developer was Gregory Maxwell, who claimed he had mathematically proven Bitcoin to be impossible.
    - In the beginning, when asked about questions of overwhelming amounts of data, Satoshi said it never really hits scale ceiling as machines improve.

      Maxwell disagreed - he stated that as volume increases, only companies would be running Bitcoin because of cost.

      "You'd need a lot of bandwidth, on the order of a gigabit connection. It would work. THe problem is that it wouldn't be very decentralized, because who would run a node?"
    - People preferred to kick the can down the road and avoid arguments - no firing policy. Maxwell founded a company that hired other developers
    - Gavin started writing to counter arguments of not raising the limit.
    - Developer responsible for releases refused to get involved.

- Civil War

  Coinbase - the largest/most popular Bitcoin startup in the USA has been erased from the official Bitcoin website for 'picking the wrong side', and banned from forums.

- XT's struggles
    - 15% of nodes were running XT, and one mining pool offered. DDOS attacks started to the extent that they even disconnected large regions of the internet. The mining pool was attacked and threatened to stop.

  - Scaling Bitcoin conferences - hosted by Core

    First conference banned discussion of concrete proposals.

    Extremely effective - people didn't upgrade because they thought they could just wait for Core to raise the limit (supposed to happen in December).

    tl;dr it stalled a block size decision while transaction free priceand block space pressures increase.

- The solution... but not really
  - 60% capacity increase through accounting trick - not counting some bytes in each transaction.

    Huge coordinated effort needed for implementation, rather than upping the limit.

    Temporary solution
  - March 16, 2016: Fees to control congestion: fee might change when you hit front of queue - let people mark payments as changable until they appear in blockchain. However, this lets people point back to themselves, thus reversing it.

    Currently, 0.0001 BTC fee unless otherwise specified. Dynamic fees may let the sender change the fee based on network congestion.

    Makes bitcoin useless for buying
- If the team were swapped out, there are far too few people controlling too much (under 10 people). Source: `https://github.com/bitcoin-dot-org/bitcoin.org/pull/1178`

Storing bitcoin wallets on internet-connected devices

- Criminals used a botnet called Pony to infect a large number of computers Sept 2013-Jan 2014, stealing around 220,000 worth of bitcoins.
- It stole bitcoin wallets stored locally on infected machines.

51%

- GHash.io and Eligius combined have over 51% computing power.
- Most of the problems are less about the protocol and more about people and services handing/storing bitcoin.