About cryptocurrencies and blockchains – part 4

Jyväskylä 25th of April 2018

Henri Heinonen (henri.t.heinonen@jyu.fi)

What is needed from bitcoin/cryptocurrency in order to be a useful paying system?

- Reducing the volatility
- Changing the consensus algorithm
- Making it more scalable
- Sharding the blockchain
- Atomic swaps
- Updating to quantum computer safe algorithms
- Making the anonymity better

Reducing the volatility

Reducing the volatility

- The changing of the bitcoin exchange rate is called the volatility.
- Within the half a year (October 2017...April 2018) the price of bitcoin has been in the range of 4602 EUR/BTC...16457 EUR/BTC on the Bitstamp exchange.
- The maximum value has been 3,5 times the minimum at most within the half a year.
- The bitcoin volatility is explained as regulatory uncertainty, low liquidity, low marketcap, limited market value, low adoption, etc.
- The huge volatility makes bitcoin an interesting investment target, but less appealing as a medium of exchange: ”If a flatscreen TV costs now half a bitcoin, what if I can buy three of them if I just wait half a year?”

Reducing the volatility

- There have been suggestions that the Bitcoin protocol should be changed so that there would be more bitcoin generated when the bitcoin price is high, and less bitcoin generated when the bitcoin price is low. It would be difficult to get the honest bitcoin price from the external world and set it into the blockchain.
- There have been suggestions that the amount of bitcoin in one’s wallet should change with the price of bitcoin. Here, too, it is difficult to get and set the honest price information.
- There have been suggestions that there could a central bank of some sort to manage the fiscal policy of bitcoin.

Changing the consensus algorithm

- The consensus algorithm of Bitcoin is Proof-of-Work using SHA256 hash function works, so that the block fork with the most of work (the heaviest chain) is the one that the miners will keep on working with.
- Mining has been done initially with computer central processing units (CPU), then with graphics cards (GPU), and eventually with special FPGA and ASIC chips. In a way ASIC chips are the most energy efficient way to minne bitcoin, because they have been designed to do only SHA-256 calculations.
- Mining has become very centralized with FPGA and ASIC, because it is better to buy lots of ASIC machines and bring them to a place with cheap electricity and possibly natural cooling mechanism (sea water, cold climate). A regular user might not purchase ASIC, because it can only be used for SHA-256 calculations. For comparison: CPU and GPU, which are suitable for general calculations.
- Ethereum’s Ethash algorithm is PoW, which is puroposefully designed to be ASIC resistant, so it is difficult to build ASIC chip for calculating Ethash calculations. Yet another example is Litecoin’s Scrypt algorithm, though it already has ASIC chips.

Changing the consensus algorithm

- The mining of bitcoin is using as much electricity as a small country.
- (One example of) A consensus algorithm that needs less energy is Proof-of-Stake. Here one is able to form consensus by owning some tokens and holding them a certain amount of time.
- Ethereum is moving to Casper Proof-of-Stake algorithm.
- Peercoin is using the Proof-of-Stake.

Making it more scalable

- There is enough room for several thousand of transactions in the Bitcoin’s one megabyte block.
- New blocks will be generated every 10 minutes in average.
- So, there can only be a few transactions per second, globally.
- In order to be useful for billions of people, bitcoin must be able to handle thousands of transactions per second.
- This would mean that blockchain would grow by several gigabytes an hour. For comparison: During the 9 years the Bitcoin blockchain has grown from zero to about 150 gigabytes.

Making it more scalable

- Raising the block size fron one megabyte to e.g. eight megabytes is only a temporary solution.
- In a same way reducing the time between blocks from 10 minutes to e.g. 2.5 minutes (like Litecoin) or to about 15 seconds (like Ethereum) would be only a partial solution to the scalability problem.
- How about not storing all the transactions to the blockchain? Lightning Network has already been successfully tested.
- In Lightning Network a payment channel is opened between the buyer and the seller, tens or hundreds of payments are made within a month or so (say, buy a cup of coffee every morning), and then, finally, the payment channel is closed. Only the opening and closing transactions of the payment channel will be stored on the blockchain. The system is designed so that there is no cheating possibility, and also, the network can find the best route itself (minimizing the transactions fees) for the transactions.

Sharding the blockchain

- Sharding a database or horizontal partitioning is a design principle, in which the rows of the database are stored separately.
- This means that not every shard needs to hold all the data of the database.
- Bitcoin blockchain is about 150 gigabytes. This amount of data must every full-node download from the Bitcoin peer-to-peer network.
- Bitcoin applications make it possible to prune the blockchain, but full-node must still download the whole blockchain before pruning.
- It would be important to shard the blockchain, so that a smartphone could download a gigabyte worth of sharded blockchain.

Atomic swaps

- What if I own bitcoin, but I want to exchange some of them to litecoin? Litecoin (and most of cryptocurrencies) is difficult to buy with fiat money.
- Almost the only way is to exchange bitcoin into the desired cryptocurrency using a third party exchange service. This is highly centralized solution, where the middleman takes a small fee of the exchange operation. Also, many of the exchange services are operating in the grey area of law.

Atomic swaps

- Atomic swaps are technology in the development phase, which make it possible to swap tokens of different blockchains without third parties. The swaps are atomic, so they will either happen completely (100%) or not at all. For comparison: In the third party exchange one must first send bitcoin to their wallet, and after a long waiting period (minutes/hours) one is able to start doing buying and selling with other users of the exchange site.

Updating to quantum computer safe algorithms

- The Shor algorithm developed for quantum computers is useful for integer factorization in polynomial time.
- Few years ago the Shor algorithm was used to factor the number 21. (21 = 7 * 3.)
- An another algorithm developed for quantum computer is the Grover algorithm, which is more general purpose so it could be used in breaking also SHA-256 and RIPEMD-160 hash functions.
- The Grover algorithm does not give so dramatic speedup in breaking attempts compared to the Shor algorithm.
- A spent bitcoin address (which has been used to send bitcoin) has revealed the public key. The elliptic curve cryptography might be a target for Shor algorithm breaking attempts.
- An unspent bitcoin address (which has not been used to send bitcoin) is more safe, because RIPEMD-160 would still be quite safe despite the Grover algorithm.

Updating to quantum computer safe algorithms

- Lamport signature scheme from 1979 could make Bitcoin quantum computer safe.
- https://en.wikipedia.org/wiki/Lamport_signature
- https://web.archive.org/web/20160116115057/https://bitcoinmagazine.com/articles/bitcoin-is-not-quantum-safe-and-how-we-can-fix-1375242150/
- http://www.bitcoinnotbombs.com/bitcoin-vs-the-nsas-quantum-computer/