IOHK | SCOREX BLOG

Centralized cryptocurrencies

MARCH 06, 2017 DMITRY MESHKOV 2 MIN READ COMMENTS

This article is inspired by recently visited blockchain technology (http://www.osp.ru/iz/blockchain) conference which I attended and my discussions with colleagues about ideas to improve blockchain. Most of the conference speakers were from big Russian banks and their talks were about blockchain use cases, mainly as databases or smart contract platforms. However, none of the speakers were able to answer the question, 'why did they really need blockchain?'. The correct answer for this question recently came from the R3 CEV consortium: "no blockchain because we don't need one". Blockchain is not needed for banks, it is needed instead of banks. It is required for decentralized systems only, applications with a trusted party will always be more efficient, simple, etc.

The meaning of decentralization was widely discussed earlier (see, for example, this post from Vitalik Buterin) and it is the only real purpose of blockchains. In this blog post I'm going to discuss the degree of centralization of existing cryptocurrencies and reasons leading to it.

Governance and development centralization

Let's start with a non-technical topic. It is nice to think that **no-one controls blockchain**, ie that network participants (miners) act as a decentralized community and chose the direction of development. In fact, everything is much worse.

The first source of centralization here, is the source of the protocol for improvement. Only a small group of **core developers** is able to accept changes to the source code or even understand some protocol improvement proposals (https://en.bitcoin.it/wiki/Bitcoin_Improvement_Proposals). No-one works for free and the organization that pays money to the core team in fact controls the cryptocurrency's source code. For example, Bitcoin development is controlled by Blockstream, and this organization has its own interests. A **Treasury system** like the one for Dash (https://iohk.io/research/papers/dash-governance-system-analysis-and-suggestions-for-improvement/) or the one proposed for Ethereum Classic may be the solution here. However, a lot of questions are still open (for example, the 78 pages of ETC treasury proposal are quite complicated, while the Dash treasury system was developed without any documentation).

The next centralization risk in governance is the **cult of personality**. While Vitalik us tells in his post, that no-one controls cryptocurrencies, his opinion is so important for the Ethereum community, that most of them

accepted the bailout of the DAO, which breaks the basic immutability principle of cryptocurrencies.

Finally, there are a lot of interested parties behind cryptocurrencies, and the opinion of some of them (for example the end users of the currency) is usually **ignored**. Anyway, the development of cryptocurrencies is a social consensus, and it is good to have a manifesto, declaring its purpose from start.

Services centralization

One of the biggest problems with existing cryptocurrencies is the centralization of services. Blockchain **processing is heavy** (e.g. Ethereum processing from the genesis block may take weeks) and regular users that just want to send some coins have to **trust centralized services**. Most of Bitcoin users trust blockchain.info, Ethereum users trust myetherwallet and so on. If these popular wallets are compromised, users' funds could be lost.

Moreover, most users trust in blockchain explorers and never check that the blocks in it are correct. What is the meaning of the "decentralized" social network Steemit, if almost none of its users ever downloaded a blockchain and believe that the data on steemit.com is correct? Or imagine that blockchain.info was compromised: an attacker could steal all the users' money from their wallets, hide the criminal transactions and show user-created transactions in blockchain explorer, and the attack would be unnoticed for a long time.

Thus, trust in centralized services produce **single point of failure**, allows **censorship** and put user coins in **jeopardy**.

Mining centralization

With popular cryptocurrencies, **hardware requirements are high** even just for blockchain validation. Even if you own modern hardware able to process blocks fast, your network channel may not be wide enough to download the created blocks fast enough. This leads to a situation where only a few high-end computers are able to create new blocks, which leads to mining centralization. Being open by design, Bitcoin mining power is now concentrated in a limited group of miners, which could easily meet and agree to perform a 51% attack (or just censor selected transactions or blocks). Mining pools worsen the situation, for example, in Bitcoin just five mining pools control more than 50% of the hash rate (at least if you believe blockchain.info). Another option for miners is to skip transaction processing and produce empty blocks, which would also make blockchain meaningless.

Proof-of-Stake is usually regarded as more hardware friendly, however, a really popular blockchain requires a wide network channel to synchronize the network anyway. Also, it is usually unprofitable to keep a mining node in PoS and just a small percentage of coins is online that makes the network valuable. This is usually fixed by delegating mining power to someone else, that also leads to a **small amount of mining nodes**.

Centralization as a solution

The most scary point of all this is that more and more often, centralization is regarded as a solution for some problems for cryptocurrencies. To fix scalability issues, cryptocurrencies propose to use a limited number of trusted "masternodes", "witnesses", "delegates", "federations" and so on to "fix" the too large amount of mining nodes in network. The number of these trusted nodes may vary, but using this method to fix scalability issues developers also **destroy the decentralized nature of currency**. Eventually this would lead to a cryptocurrency

with only one performing node, that processes transactions very efficiently, without confirmation delays and forks, but suddenly a blockchain is not needed, as in R3's case.

Unfortunately, most users are not able to determine the lie in cryptocurrencies and like these centralized blockchains more and more, because for sure, the centralized way is (and will always be) more simple and user-friendly.

Conclusion

We are going to see more and more centralized cryptocurrencies, that will inevitably lead to mass disappointment in blockchain technology, because it is not needed for centralized solutions. It is still a user choice, whether to believe a beautiful and fast web interface or to use trustless, but harmful software, requiring you to download blockchain data and process it.

Most centralization risks may be fixed, if trustless full-nodes, wallets, explorers will be cheap to launch and easy to use. I'm not going to propose a solution in this paper, but I hope it is coming soon!

March 06, 2017 by dmitry.meshkov@iohk.io

Centralized cryptocurrencies

This article is inspired by recently visited blockchain technology (http://www.osp.ru/iz/blockchain) conference which I attended and my discussions with colleagues about ideas to improve blockchain. Most of the conference speakers were from big Russian banks and their talks were about blockchain use cases, mainly as databases or smart contract platforms. However, none of the speakers were able to answer the question, 'why did they really need blockchain?'. The correct answer for this question recently came from the R3 CEV consortium: "no blockchain because we don't need one". Blockchain is not needed for banks, it is needed instead of banks. It is required for decentralized systems only, applications with a trusted party will always be more efficient, simple, etc.

February 20, 2017 by alex.chepurnoy@iohk.io

Authenticated Dynamic Dictionaries, with Applications to Cryptocurrencies

Our paper "Improving Authenticated Dynamic Dictionaries, with Applications to Cryptocurrencies" will appear at the Financial Cryptography 2017 conference in Malta in April. It was also presented at the Real World Crypto 2017 conference in New York and I highly recommend watching the impressive presentation from Leonid Reyzin, professor of computer science at Boston University and one of the four authors of the paper.

October 11, 2016 by jan.kotek@iohk.io

IODB storage engine

Log-Structured-Merge trees (LSMT) are a good fit for modern SSD storage and offer good performance and reliability. LSMT are also a good fit for blockchain storage requirements (snapshots, consistency, proof of existence). This blog post describes a database designed specifically for blockchain storage, inspired by existing LSMT implementations (RocksDB, COLA tree).

May 17, 2016 by alex.chepurnoy@iohk.io

Announcing Ergaki - A performant, public bulletin board for voting and auctions

The first Scorex-based testnet, Lagonaki, combines the Permacoin consensus protocol implementation with a simple, Nxt-like payments

module. After Lagonaki, the next Scorex-based testnet will be *Ergaki*, a block chain system that will be used as a public and performant bulletin board for various protocols including voting and auctions.

May 17, 2016 by alex.chepurnoy@iohk.io

Ergaki, the Next Scorex Testnet

A Scorex application is comprised if core, and Scorex itself is the core functions and module interfaces, and modules. The current testnet, Lagonaki, is made of Permacoin consensus protocol implementation and a simplest Nxt-like payments module.