RESEARCH

A Blockchain-free Approach for a Cryptocurrency

OCTOBER 12, 2016 MARIO LARANGEIRA 3 MIN READ

A major technical challenge of the cryptocurrencies is to find a way to safely increase the throughput of the system in terms of number of transactions. An approach to tackle this limitation is to review the role of the blockchain, or even to take that data structure out of the picture completely.

In this post, we will comment a paper by Boyen, Carr and Haines named Blockchain-Free Cryptocurrencies: A Rational Framework for Truly Decentralized Fast Transactions which proposes the latter approach.

Before describing the idea of the paper, and where the main contribution is, it is helpful to give an overview of how we can generally split the main components of a cryptocurrency protocol, or what is commonly known as the **consensus protocol**. The three main components are:

- the protocol itself, the routine that every node follows;
- the blockchain data structure; and
- the proof-of-work (PoW) paradigm.

Here we are clearly giving the emphasis on the Bitecoin like systems which rely on the PoW idea. The reader should keep in mind that not all systems rely on it (as for example proof-of-stake based protocol).

We start by reviewing the second item above: the blockchain.

The Blockchain

The reader familiar with decentralized cryptocurrencies is aware that the blockchain is a data-structure which is kept by the network players, which are often called *miners* in Bitcoin jargon.

Each smallest part of such structure is called block, hence the name, which is where the transactions are described. There are different ways of building the actual structure (for example, Bitcoin-NG and GHOST, however in the end, the pace of the the block generation (including its addition in the structure) is the heartbeat of the whole system.

That is, with each new added block, containing brand new transactions, we are sure that the system is “alive`` and making progress. However here also lies a problem.

The Scalability of the Blockchain

In the pace of the whole system lies the fundamental constrain of the growth speed of the blockchain. Nakamoto was aware of it as well as its implications, as stated in the Bitcoin seminal Nakamoto’s whitepaper.

A major implication of this limitation is the regulated speed of block generation using the **difficulty level**. That is the hash value that the player needs to find in order to generate a new block in PoW. That value is carefully set within the Bitcoin network to keep just the right balance between the block generation time and the block spread time over the network.

In a different setting, say, with an arbitrarily low difficulty level, there would be a higher block generation rate for sure. However, due to the competitive nature of the PoW and the blockchain addition, the forks will become more frequent, therefore increasing the risk of attacks. One should expect this because the miners are competing against each other, in order to generate new valid blocks.

In other words, the scalability constraints derive from the blockchain centralized setting.

A Blockchain-free Approach

The main idea behind the study of Boyen et al. is to substitute the blockchain by a directed graph of **transactions**, not blocks.

In that setting the system is not required to make progress by the pace of a single data structure like the blockchain. In fact, there is not a notion of block in their idea. The obvious direct consequence is that there is no race among the players of the system to generate the new block. The players are allowed to choose in which point in the graph they want to expand it.

Instead of the previous competitive blockchain environment, the players cooperatively expand the directed graph by adding new nodes, i.e., transactions, to it. We stress that every new node in the graph is a new transaction. And the action of attaching the transaction into the graph validates the transactions where the new one is attached to, i.e., the parent nodes (the new node has two parent nodes in the graph).

In order to incentivize the players to keep the progress of the system, every new transaction specifies a fee, which is decided by the issuer of the transaction. Consequently every new node which is later attached to that transaction (as described earlier) does two actions: (1) validate the transaction represented of its two parents (the number of parents is fixed by their framework) and (2) collects the fee from its parents.

Differently from the blockchain setting, there is not a notion of rounds (or epochs), i.e., the new block generation. However, due to the collection of fees, the players are incentivized to keep adding transactions to the system, therefore making the transaction history evolve. Another advantage is that the issuer of a transaction can increase the speed of the validation by offering a higher fee.

This framework reverses the competitive nature of the miners to a more cooperative approach to validate transactions in the system.

Other papers describing scalability issues within blockchain based protocols can be found here:

- On Scaling Decentralized Blockchains
- Inclusive Block Chain Protocols