ON CONCEPTUAL RESPONSE TO SOME OF THE BLOCKCHAIN PROBLEMS

A.V. Bogdanov [1,a], A.B. Degtyarev [1], V.V. Korkhov [1], O.O. Iakushkin [1], V. Khvatov [2]

[1] *Saint Petersburg State University, 7/9 Universitetskaya nab., St. Petersburg, 199034, Russia*

[2] *BGX, Toronto, Canada*

E-mail: [a] a.v.bogdanov@spbu.ru

We discuss some of the main solutions we see fit for the future of Blockchain 4.0, look at how with broader spread of blockchain-related economic interaction such networks as DEC and platforms alike BGX would change businesses, developers, and market relations. We discuss the current problems and conceptual solutions for them that include new generation of efficient distributed consensus algorithms and new technological platform. Our primary focus is on business needs and potential approaches that a new distributed software paradigm can provide for them.

Keywords: blockchain, consensus, distributed ledger

1. Introduction

The major change in the business world today is digital transformation. The needs and expectations of a business undergoing digital technological transformation can be divided into several key areas:

- Exchange of a wide range of digital assets, not just cryptocurrency: formation of ecosystems based on such assets as loyalty (for example, a telecommunications company, a chain of coffee shops, an airline company, a taxi - due to synergy, they need their own token that changes miles into minutes and kilometers);
- Tasks of the supply chain: equipment supply, cargo delivery with the participation of many intermediaries;
- A speculative market that brings the problem of distributed suppliers to a new level by adding an element of risk associated with active fluctuations in the price of a resource, its predictions and expectations;
- Loan and co-financing organizations: from large interbank corporations to local credit unions supporting home enterprises and forms of financial support in exchange for a share in the business;
- Services provided virtually: digitalization of database services and access to digital information.

The reasons for such needs are several main factors: globalization of the spread of digital technologies, the alternation of generations, the increase in cyber threats, virtualization of the world. As a result, today traditional systems work poorly, businesses grow only with innovations, and competition itself has changed. If yesterday a business was based on a linear value chain, creating added value based on products from the supplier, today platforms such as AirBnb, Uber, Amazon came to the fore, the main idea of which is to turn suppliers and consumers into their regular customers. In our opinion, the logical development of such systems will be realized in multi-platforms, the objective function of which is not just the elimination of intermediaries, but the creation of a new communication environment that supports the whole ecosystem. An example of such a multiplatform is BGX, a decentralized processing platform aimed at digital assets [1].

Distributed platforms are not new, but the new wave of solutions also requires a decentralized approach, in which the system is used by different actors with opposing interests who generally do not trust each other. The answer to this need is Blockchain and Blockchain-like solutions.

The first generation Blockchain solutions, such as Bitcoin and Ethereum, showed the fundamental possibility of forming distributed solutions, but they operate at low speed and, despite the high reliability of the Blockchain networks themselves, are subject to fraud, mainly due to the attacks on end nodes and smart contracts. For business, a set of private Blockchain networks were developed, for example, Hyperledger, Corda, etc. However, these systems also have relatively low performance and do not support tokenization enough, which is an important aspect that facilitates the exchange of digital assets.

Recently, fundamentally new solutions have appeared e.g. IOTA, Hashgraph, Stellar, COTI, EOS. Three new core innovations are present in these new solutions: focus on the applied market; using its own consensus algorithm; targeting a specific market segment (e.g. IOTA uses the Internet Of Things: small devices, free transactions, weak processors; Stellar is used for interbank transfers; EOS targets fulfilling smart contracts). Most of the presented examples dropped the original chain of blocks structure of data storage in favor of the DAG - Directed Acyclic Graph.

2. BGX platform paradigm

In our opinion, the answer to the above business needs is the creation of a new paradigm of a distributed decentralized system. This paradigm is currently developed by our team on the basis of the BGX platform.

The BGX platform is based on a distributed decentralized network, focused on use in two modifications: a) a public network; b) the so-called *boxed solutions* for use by closed organizations that do not require the introduction of tokens in an explicit form.

The public network is focused on ecosystems consisting of several distributed organizations (consortium-based). Each such system uses BGX platform as a transport infrastructure, but is capable of releasing its own token for exchange. In BGX, a node is a group of virtual computers. The model can be called Business-Business-Consumer or BBC (as opposed to B2B and B2C, focused on connecting only two sides).

Any node can join the network, but under certain conditions. The node must have: an account in an external, public network, e.g. in Ethereum, and KYC (know your customer) permission against money laundering and organized crime. Thus, the fundamental requirement for conducting operations with a network is that the nodes must have some cryptocurrency on their accounts. This approach allows users to get the "anchor" of the network with PoW or other consensus algorithms.

Nodes can issue their own exchange currency with a “hard” smart contract. The essence of this issue is the release of currency not subject to volatility. Volatility is a characteristic of all cryptocurrencies. To combat it, two token systems are introduced. One token - *system token* - is issued by the BGX network during the initial emission process. The BGX network token is called DEC (Digital Economy Coin), as the network itself is called. The node produces secondary emission, choosing to bind to some stable exchange rate (for example, to the dollar). Then DEC can fluctuate, but at a specific point in time a node can release its own token based on recalculation. This stabilizes the exchange rate of the token for digital assets and makes it possible to pay for books, music, loans, etc.

3. Approach to implementation of BGX technological platform

The Virtual Supercomputer paradigm that has been developed by the scientific group of professor Bogdanov for last 10 years to speed up computations on hybrid systems, provides a reliable technological platform for solving the problems of efficient acceleration of computations [2,3] and is used as the technological core of BGX. The idea is not only to virtualize all major components of the system, but also to form a mandatory entry point, an API for each node. This allows, on the one hand, to manage the entire virtual ecosystem, and, on the other, to provide reliable isolation of transactions within a selected set of nodes, preventing third-party users from entering there.

Using virtual processors instead of real processors is a key element in accelerating distributed systems, since different processors are used in different nodes of a distributed system, and load balancing of different processors in a distributed system is very complicated. Moreover, in modern computing systems based on GPGPU, virtualization is the only way to efficiently use a large number of cores.

Network virtualization is a necessary element in creating secure connections, and VPN technology is a necessary element in organizing user access to confidential data. But it is important to go further and use network virtualization to create a completely isolated system of nodes, which should ensure the security of the transaction and reduce the time required for interfacing data on the nodes, which is key to speeding up transactions.

In all modern data processing systems, the availability of a distributed file system is a necessary element for processing data in real time. However, as soon as we are talking about working with data located on different nodes, standard tools drastically slow down their performance, and to such an extent that data loss is sometimes possible. Therefore, the most important step in our approach is the creation of virtual shared memory based on a virtual network of transaction nodes. This step slows down the exchange rate inside the physical memory of the hypernode, but it significantly increases the exchange rate between the remote nodes.

4. Consensus on the BGX platform

Distributed consensus is a collective agreement by various computers in a network that allows the network to work in a decentralized, P2P manner without the need of central authority to deter dishonest network participants. Consensus is used to make decisions about accepting received transactions into the common ledger. With the help of consensus mechanism, malicious transactions are warned, compromised nodes are detected.

As part of the DEC network, a modification of the FBA (Federated Byzantine Agreement) algorithm, in turn based on PBFT, is implemented on the BGX platform. The essence of the consensus algorithm is that the cluster votes for each new transaction, it is necessary to collect 2/3 of votes are to consider it successful, then the transaction goes beyond the cluster and is finally packaged in a DAG. The number of votes can be reduced if the owner of the transaction has a good reputation.

Transaction data is stored in the DAG. Transactions in the network may have differences thus forming a family of transactions. Most of its life cycle, the transaction is packed into a byte array (except for the header and signatures), the transaction families are decrypted in the process by special handlers, transaction processors. The following terminology is used:

- The client is the one who sent the transaction;
- Initiator node (*Initiator*): the node to which the transaction arrived;
- Leading node (*Leader*): the node that communicates between the cluster nodes and calculates the votes per transaction;
- *Cluster* nodes: the nodes included in the cluster that support the processing of transactions of the same family as the *Leader*;
- *Parent* node: a node located one level above the cluster.

A cluster is formed according to the nodes supported by the transaction family. All network nodes are aware of the topology of each of the nodes. Communication between nodes is carried out through the leading node using permalinks. The cluster is unstable, that is, the number of its nodes is not constant and can vary over time, and their availability is not equal to 100%

4.1. Requirements to the consensus algorithm

According to the CAP theorem, it is necessary to take into account that the operation of a distributed transactional system cannot provide full support for the ACID properties (atomicity, consistency, isolation, stability). It is possible to provide support for only two of the three properties: consistency, availability and partition tolerance.

It is important that the consensus algorithm is resistant to the main attack vectors:

1. Double Spending: the possibility of a user spending a single amount twice or, in a more general version, of the amount that he does not have in the accounts. A special case is the Finney attack: double spending with the participation of the node;
2. 51% attack: the majority of nodes join and validate transactions at the expense of a minority;
3. Sybil attack: substitution of a node (Byzantine node);
4. DDOS attack targeting the failure of one or more nodes to vote;
5. Packet sniffing / Middle Man: packet capture and its replacement.

In addition, the consensus algorithm must meet the following additional requirements:

1. Provide robust cryptographic solution;
2. Solve the problem of scaling and data segmentation;
3. Ensure all transactions are completed.

4.2. Consensus algorithm concept

The algorithm is based on the idea of *voting* for a transaction by all connected nodes of the cluster (i.e., the decision about the transaction must be made not only by one node, the initiator (if it supports this family of the received transaction), or the leader (if the initiator does not support the received transaction family), but by all the nodes in the cluster). The leading node should be responsible for counting votes for a transaction.

Within the framework of the consensus algorithm being developed, a two-stage verification is used: separation of the voting into two stages, verification and validation within the cluster and validation by the Parent node. The essence of this separation is to prevent the likelihood that the cluster and / or its nodes (including the Leader) are compromised.

The first stage of transaction processing begins at the moment when the Client sends it to the Initiating node. The milestones of this phase are:

1. Receipt of a transaction from the Client (for its verification and approval);

2. Verification of the transaction by the Initiating node;
3. Verification of the transaction by the Leading node;
4. Transaction verification by cluster nodes;
5. Transaction validation by cluster nodes.

To validate a transaction on the second stage, the transaction needs to go outside the cluster in which it arrived, to be validated by the Parent node. The Parent node operates reliably with respect to the remaining nodes and is trustworthy. However, if the Parent node fails, then it should be replaced almost imperceptibly. In addition to the validation of the transaction, the Parent node must check all the participants of the voting.

5. Conclusion

The proposed approach can be a solution to the three main problems of the development of distributed ledgers in the BGX platform:

- LOW PERFORMANCE PROBLEM: BGX abandons PoW consensus, proposes new efficient and fast consensus algorithm, admits only professional (business) node operators, and establishes node competition according to real-life market without simulated difficulty of transaction validation.
- HIGH ENTRY BARRIER PROBLEM: A normal business has significant difficulty joining the blockchain and lacks a convenient and accessible interface. Creating their own crypto processing is expensive. BGX is highly integrative through API, easy for opening nodes.
- VOLATILITY PROBLEM: Speculative pressure makes cryptocurrencies unstable and the resulting hyperinflation (or hyperdeflation) cripples underlying economies. BGX introduces a stable second coin for the consumer, while keeping the original token high-growth focused to appease its investors.

Acknowledgement

This work was partially supported by the grant of Saint Petersburg State University no. 26520170.

References

[1] BGX Blue paper, 2018, URL: https://bgx.ai/documents/en/BGX_BLUEPAPER_1.0.pdf

[2] A. Bogdanov, A. Degtyarev, V. Korkhov. Desktop supercomputer: what can it do? Physics of Particles and Nuclei Letters, 2017, Volume 14, Issue 7, pp 985–992, DOI: 10.1134/S1547477117070032

[3] Alexander Bogdanov, Alexander Degtyarev, Vladimir Korkhov, Vladimir Gaiduchok, Ivan Gankevich. Virtual Supercomputer as basis of Scientific Computing, in series: Horizons in Computer Science Research, vol. 11, eds.: Thomas S. Clary, pp. 159-198, Nova Science Publishers, 2015, ISBN: 978-1-63482-499-6