Communication Papers of the Federated Conference on Computer Science and Information Systems pp. 45–48
DOI: 10.15439/2020F190
ISSN 2300-5963 ACSIS, Vol. 23

The general universal model of blockchain technology based on an analysis of some implementations

Polina Sazonova
Novosibirsk State University, JetBrains Research Laboratory
Sobolev Institute of Mathematics
Novosibirsk, Russia
Email: p.sazonova@nsu.ru

***Abstract*—First imlementation of blockchain technology was appeared in 2008, and 12 years later more than 2000 different implementations of it have appeared. After deep analysis we found that approaches for development blockchain technologies is fragmented, there are no common system of concepts and general model of technology. In this article we want to propose the general universal model and system of concepts for the blockchain technology irrespective of differenced of some implementations. Our approach is based on a technical analysis of the popular blockchains. The results of this work can be used by architects of new blockchains implementstions, by researchers to achieve theirs goals and also in educational process.**

I. Introduction

A. Blockchain definition

BLOCKCHAIN technology has become popular due to the its properties such as openness, immutability, inability to delete stored data, decentralization and the ability to make decisions in an untrusted environment between equal participants in this network without the participation of a trusted party (trusted centre). Thus, blockchain uses in a wide variety of subject areas, especially in logistics, banking and public administration.

Blockchain is a type of decentralized system that collects, stores and manages data, in which:

- consensus will be reached in an untrusted environment;
- transactions are stored in a data structure called blocks, and each subsequent block stores the value of the hash function from the contents of the previous one;
- copies of the blockchain are stored at the same time by all its users and are automatically updated.

In this work, under the blockchain is meant a system that uses a chain of blocks as a technology for storing data. It provides ensures the immutability and integrity of the data stored in the blocks. Unlike centralized systems, where consensus can be achieved through a central node, blockchain technology allows to reach consensus in decentralized environment. Moreover, in the blockchain system, consensus can be reached when the network nodes are not authorized. It means that the probability of malicious nodes or Byzantine nodes [1] appearing on the network is increase. In decentralized networks with unauthorized (untrusted) nodes, a Sybil [2] attack may occur. It can happens when the node performing the calculations connects only to nodes controlled by the attacker, which entails incorrect behavior and consensus in making a decision that is beneficial to the attacker. Blockchain technology allows to make the right decisions in a decentralized network with untrusted nodes, provided that 51% of the nodes are not intruders.

This work was supported by Math Centre in Academgorodok by agreement of The Ministry of Science and Higher Education of the Russian Federation number 075-15-2019-1613 and by JetBrains Research Cryptography Laboratory.

B. Introduction to history

The first practical implementation of blockchain technology was done in 2008, it was described in the article by S. Nakomoto about digital monetary system Bitcoin [3]. Bitcoin is a protocol for exchanging digital money in a decentralized untrusted environment that allows to make transactions without the participation of third parties (trusted centre).

But before the publication of this article, it was made lots of reseaches influented over on the blockchain technology appearing. In 1982 D. Chaum proposed the blind signature algorithm and introduced the concept of digital money [4]. S. Haber and S. Shtornetta presented a theoretical description of the system for certifying immutability of documents, built on timestamps in 1991 [5]. The Proof of Work (PoW) mechanism was proposed by A. Back in the Hashcash project to prevent [6] spamming. The idea of smart contracts was proposed by N. Szabo in 1996 [7]. N. Szabo also proposed a protocol for digital money Bit-gold in 1998, which was published in 2005 [8]; it was based on bit-chain computation and used the PoW consensus mechanism. But the system was not implemented in practice and was vulnerable to the Sybil attack.

However, the first implementation of blockchain technology was created only as a part of the Bitcoin cryptocurrency project. Subsequently, new cryptocurrency systems began to appear, similar to Bitcoin. It was added data hiding mechanisms, such as in Zcash [9], transaction acceleration mechanisms, such as in Litecoin [10]. Currencies were created for various purposes, for example, providing a set of alternative

DNS servers as in Namecoin [11]. The first implemented blockchain which was a platform for creating a smart contracts was Ethereum, created by V. Buterin in 2013 [12].

II. Motivation of Creation a Blockchain Technology Model

A. Statement of the Problem

An analysis of several hundred articles in Scopus on the topic of blockchain technologies showed that there are practically no scientific works that describes blockchain technology in general focused on its technical construction, covering all components of technology, regardless of specific implementations. In this direction it is worth highlighting this work [13], an overview of the blockchain technology components from the developers of the "Roadmap for the development of Distributed Ledger Technology (DLT)" in Russian Federation [14], an activity of the Geneva Telecommunication Standardization Sector Assembly (ITU) [15] and an activity of ISO/TC 307 committees [16]. But the results of most researchers work are not yet publicly available or have obvious flaws. This confirms the assumption that knowledge about technology is fragmented and the overall picture is not visible to researchers. This slows down the development of new technology implementations and makes it difficult to analyze new blockchains when we need to find real innovations, in contrast to the result of applying marketing tools.

B. Methods, Purpose and Criteria of the Developed Model

In this article the task of constructing a general universal model was to propose a model that would meet the following criteria: it would make it possible to make a universal description of current blockchain systems, answer questions about the structure of the system, and pose new questions to researchers and industry engineers. To build the model, an experimental-analytical approach was used: based on existing software implementations of the blockchain technology, the components of the technology were analyzed, then the obtained components were generalized, and a system of concepts was formulated for them. Then it was shown that each specific technology implementation corresponded to the proposed model.

To make a general universal model, five popular blockchains were analyzed, which are independent implementations of platforms for developing decentralized applications and cryptocurrencies. Among them: Bitcoin [17], Ethereum [18], NEO [19], DASH [20], EOS [21]. The choice of these technologies is due to their relevance as platforms for the development of decentralized applications, the high level of readiness of the technology for application, its developed by community to support them and the availability of satisfactory documentation. The characteristics of the selected blockchains are presented in the table (cf. table I).

To solve this problem the general model of blockchain technology was developed. This model does not depend on specific implementations. A key components of blockchain technology were defined and their definitions were supposed with the aim of eliminating disagreements of interpretations.

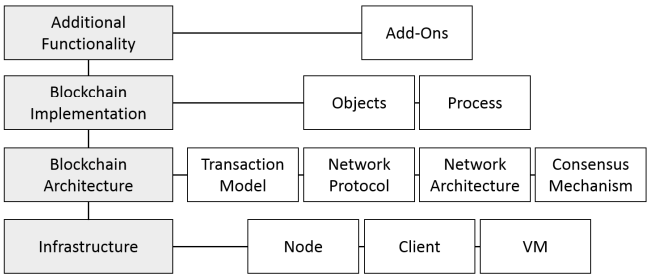

Fig. 1. Proposed blockchain technology model

The developed general model of blockchain technology is presented in the next section.

III. Proposed Blockchain Technology Model

For the five selected blockchains some documents as s technical documentations, technical concepts, «yellow papers» were analyzed. Common components that uniquely determine the blockchain technology were identified. These components are shown in the figure 1 and described in the text below.

At the **first**, basic, level of the model are the infrastructure components that ensure the functioning of the system. This is *node* – a single computer that performs actions on the network; *client* – software that implements the protocol of interaction with the blockchain; and *virtual machine (VM)* – a software system that emulates distributed work of a decentralized blockchain platform and executing decentralized applications and smart contracts.

At the **second** level, components are placed that ensure the functioning of the blockchain network. Depending on how this level is built, implementation features are established.

Network architecture – a combination of network nodes and a set of rules which uses for the the transmission of messages over the network. Blockchain networks can be single-layer or two-layer, public or private; they can have separation of nodes by roles.

Consensus Mechanism is a protocol that allows to reach an agreement between equal participants in a decentralized network. There are many implementations, but the most popular consensus is PoW, PoS, BFT and etc.

Transaction Model is a set of algorithms and features of design of the blockchain implementations that determine the method of conducting transactions and fixing the state of a distributed system. Currently, there are only two models uses in blockchains - UTXO or account model.

Network Protocol - the rules which uses for transmitted data over the network.

At the **third** level, objects and processes are located. This level arrangement depends on the implementation of the previous level. To begin with, we list **objects**, the presence of which is uniquely determined the blockchain technology.

TABLE I
CHARACTERISTICS OF THE INVESTIGATED BLOCKCHAINS

Blockchain	Transaction validation speed	Block size	One block creation speed	Bandwidth
Bitcoin	78 Min.	1 Mb	10 Min.	3 TPS
Ethereum	6 Min.	1 Mb	15 Sec.	20 (PoW), 400 (PoA) TPS
EOS	1,5 Sec.	About 1 Mb	1 Sec.	50000 TPS
NEO	15 Sec.	About 1 Mb	15 Sec.	1000-10000 TPS
DASH	15 Min.	2 Mb	1 Sec.	28-56 TPS

Block is a data structure uses to store data on the blockchain. The block stores transactions, network status, smart contracts, permissions to access data and other information.

Block chain is a data structure constructed by sequentially combining blocks into a chain. By storing the value of the hash function from the previous block, all blocks are strictly sequential, numbered by continuous numbering, the child block always refers to only one parent block.

Transaction is the minimum logically meaningful operation of the transfer or exchange of assets that makes sense and can only be completed in full. A transaction can transfer messages, actions, create a contract, and more.

Address (account, account) is a structure for identifying an active object on the network. Addresses uniquely determine the sender and recipient of the assets transferred to the blockchain network, all actions of the user in the network are associated with the address. Depending on the blockchain, the address can be either a string or a data structure, it can be associated with a user or with a smart contact.

Smart contract is a set of formalized rules implemented in the form of program code, the execution of which entails some events in the real world or digital systems. Smart contracts are not a mandatory component of the blockchain network, however, as practice has shown, contracts have become the main functional element of blockchain technology. Depending on the structure of the blockchain, smart contracts can be implemented either in Turing-complete languages or non-Turing-complete ones.

The objects listed above are part of the processes. The main **processes** taking place in the blockchain network are presented below.

Transactional life cycle: transaction signing process; broadcasting over the network; transaction verification; transaction completion. *Including a transaction in a block*: process of taking a set of transactions for a block; transaction validation; block signing process; sending a block to the network; block fixing in a common chain. *Network Maintenance*: consensus mechanism; network complexity regulation; selecting a chain that continues the block of several branches; payment for computing resources.

The **fourth** level defines additional functionality for blockchain networks that do not affect the internal architecture of the technology, but significantly expand its functionality. For example, mechanisms that provide increased speed and confidentiality of transactions, mechanisms for off-chain transactions, modules that protect blockchain against attacks by quantum computers, and others.

IV. CONCLUSIONS

After analyzing the blockchain implementations and building model as a result, we can offer *a method for considering each new technology being developed*. To analyze the new blockchain implementation, first of all, we should pay attention to the transaction model. Currently, only two models are presented - UTXO and the accounts model. The transaction model affects on: the structure of blockchain blocks, the structure of addresses (accounts), the existence of smart contracts in this blockchain and the principles of their construction, approaches to fixing the state of the system. Next, we should pay attention to the number of layers in the blockchain network, identify the purpose of each of the layers, consider the consensus mechanisms used in each layer. This information will give us an understanding of the transaction validation process – we can assume the bounds of transaction confirmation rate and network bandwidth. Based on this, we can suppose the requirenments to the necessary infrastructure to provide the network. The transactions rate is determined by the consensus mechanism, by the number of nodes involved in the transaction validation process and by the principles of working with orphaned blocks. The more stronger requirenments to network decentralization, the lower the transactions speed. The ability to create smart contracts is determined by the transaction model.

Using the results of this research we can *explain approaches to the implementation of specific blockchain technologies*. After researches we suppose that the majority of blockchain implementations are based on Bitcoin and Ethereum construction, and subsequently they were supplemented by some improvements at different levels. According to data obtained from open sources, it seems that the NEO blockchain consist of configuration of networks based on UTXO models and account models. We suppose that it makes in order to smooth out the limitations of the Bitcoin network, taken as the basis for NEO blockchain. This assumption was also made because the duplicate assets CNEO and CGAS seems artificial in these network. There is an assumption that the EOS and NEO blockchains are not blockchains, since the blockchain operates in an untrusted environment by definition, but for these networks the main transaction validators are authorized nodes, which suggests the centralization of these networks.

The Dash blockchain ensures data confidentiality and transaction speed through mechanisms operating at the fourth level of the blockchain model.

V. Results

As a result of this work, the general model of blockchain technology was proposed. This model allows to make a universal description of current blockchains, answer some questions about components and links between it in the system, and pose new questions to researchers. In this work, it was proved that the proposed model does not depend on specific implementations of the five selected blockchains and suggest methods for considering each new blockchain implementation and explain approaches to the implementation. In the future, it is planned to investigate a larger number of different blockchains in order to confirm the correctness of the model and its quality, also we plan to show connections of blockchain technology to the environment.

References

[1] L. Lamport, M. Pease, R. Shosta. "The Byzantine Generals Problem." *ACM Transactions on Programming Languages and Systems 4*, p. 3, pp. 382-401, 1982.
[2] J. R. Douceur. "The sybil attack." *International workshop on peer-to-peer systems*. Springer, Berlin, Heidelberg, 2002, pp. 251-260.
[3] S. Nakamoto. "Bitcoin: A Peer-to-Peer Electronic Cash System." The Cryptography Mailing List, 2008, https://bitcoin.org/bitcoin.pdf.
[4] D. Chaum. "Blind Signatures for Untraceable Payments." *Advances in Cryptology Proceedings of Crypto 82*, Plenum, 1982, pp. 199-203, 1982.
[5] S.Haber, W.S. Stornetta. "How to time-stamp a digital document." *J. Cryptology 3*. 1991, pp. 99–111.
[6] A. Back. Mail "Hash cash postage implementation". The Cypherpunks Mailing List. https://cypherpunks.venona.com/date/1997/03/msg00774.html.
[7] N. Szabo. "Smart Contracts: Building Blocks for Digital Markets." A partial rewrite of the article which appeared in Extropy No 16, 1996, http://www.alamut.com/subj/economics/nick_szabo/smartContracts.html.
[8] N. Szabo. "Bit gold." Unenumerated: N. Szabo's blog, 2005, https://web.archive.org/web/20060329122942/http://unenumerated.blogspot.com/2005/12/bit-gold.html.
[9] Zcash - a privacy-protecting, digital currency, https://z.cash/.
[10] Litecoin - decentralised money, https://litecoin.com/en/.
[11] Namecoin - a trust anchor for the Internet, https://www.namecoin.org/.
[12] Ethereum - a global, open-source platform for decentralized applications, https://ethereum.org/ru/.
[13] H.Y. Paik, X. Xu, H. M. N. Dilum Bandara, S. U. Lee, S. K. Lo. "Analysis of Data Management in Blockchain-Based Systems: From Arcitecture to Governance." *IEEE Access*, 2019, t.7, pp. 186091-186107, https://ieeexplore.ieee.org/stamp/stamp.jsp?tp=&arnumber=8938787.
[14] Ministry of Digital Development, Communications and Mass Media of the Russian Federation. "Roadmap for the development of Distributed Ledger Technology (DLT)." https://digital.gov.ru/ru/documents/6670/.
[15] ITU's Telecommunication Standardization Sector (ITU-T). "ITU-T Focus Group on Application of Distributed Ledger Technology." https://www.itu.int/en/ITU-T/focusgroups/dlt/Pages/default.aspx#.
[16] Technical cometees ISO/TC 307. "Blockchain and distributed ledger technologies." https://www.iso.org/committee/6266604.html.
[17] Bitcoin developers documentation, https://developer.bitcoin.org/.
[18] G. Wood. Ethereum: a secure decentralized generalized transaction ledger, https://ethereum.github.io/yellowpaper/paper.pdf.
[19] Technical Specification for NEO Blockchain, https://github.com/neoresearch/yellowpaper.
[20] E. Duffield, D. Diaz. Dash: A Payments-Focused Cryptocurrency. https://github.com/dashpay/dash/wiki/Whitepaper.
[21] EOS Developer Portal, https://developers.eos.io/.