ISSN 0005-1055, Automatic Documentation and Mathematical Linguistics, 2017, Vol. 51, No. 6, pp. 235–238. © Allerton Press, Inc., 2017.
Original Russian Text © M.R. Biktimirov, A.V. Domashev, P.A. Cherkashin, A.Yu. Shcherbakov, 2017, published in Nauchno-Tekhnicheskaya Informatsiya, Seriya 2: Informatsionnye Protsessy i Sistemy, 2017, No. 00000, pp. 00000–00000.

Blockchain Technology: Universal Structure and Requirements

M. R. Biktimirov[a], *, A. V. Domashev[b], **, P. A. Cherkashin[c], *, and A. Yu. Shcherbakov[d], ******

[a]All-Russian Institute for Scientific and Technical Information, Russian Academy of Sciences, Moscow, 125190 Russia
[b]Scientific and Technical Center Atlas, Moscow, 127018 Russia
[c]Granit Company, Moscow, 119019 Russia
[d]Computer Science and Control Federal Research Center, Russian Academy of Sciences, Moscow, 119333 Russia
**e-mail: marat@ras.ru*
***e-mail: domix@stcnet.ru*
****e-mail: cherkashin@granit-concern.ru*
*****e-mail: x509@ras.ru*

Received September 21, 2017

Abstract—The project elaboration of the configuration and mathematical model of distributed blockchain data storage, blockchain applications for implementing various information technologies, and blockchain requirements that stem from its analytical and structural features are considered.

Keywords: blockchain, distributed data storage, information security, e-voting, auction, encryption, electronic signature

DOI: 10.3103/S0005105517060036

INTRODUCTION

The advanced and trending model of distributed blockchain data storage [1] has become an object of broad scientific and practical discussion. Unfortunately, this issue involves misunderstandings and speculation. This work is written to clarify the basic blockchain features for making balanced decisions on choosing and applying this technology in corporate and governmental information systems.

The word *blockchain* indicates a chain or string of blocks; first of all, the technology is designed to maintain such typical chain features as continuity and reliability that form the paraphrase of integrity.

Continuity is defined as blocks (links in a chain) that follow one another in a sequence specified in the course of formation of a blockchain; reliability is defined as the impossibility of replacing or removing a link from the chain.

If we consider a blockchain as a kind of system-level integrity it must consist of individual elements (links). In its respect, each of the elements is divided in basic components (we will refer to them as blockchain atoms). Atoms as elements associated or integrated with the computer system can be active or passive.

The Blockchain Structure As System-Level Integrity

Atoms have characteristic identifiers (names) and certain features.

There are several types of blockchain atoms.

Type one includes blockchain border atoms (initial and final atoms) with references either to the end of the previous link or to the beginning of the next link.

Type two includes structural atoms. They define and describe the vector of identifiers of atoms found in the link and form the logical continuation of initial—final atoms.

Type three includes data atoms with description of data interpreted as the passive link component. Data atoms are classified in the following varieties:

- an open data atom is characterized by its length and contains unprocessed data;
- an integral data atom is characterized by the length of fixed-integrity data and the identifier of or reference to the data integrity control procedure;
- a signed data atom is characterized by the length of signed data, the identifier of or reference to the data signature check procedure, and the reference to the signature check key; the signature check procedure can be externally specified relative to blockchain or be a subject atom;
- an encrypted data atom is characterized by the length of the encrypted data, the identifier of or reference to the data encryption or decryption procedure and to the encryption or decryption key;
- a signature atom contains the signature of one or several signed data atoms with (a) preset identifier (-s);

Table 1

Identifier	Atom name	Contents	Note
1	Initial border atom	Reference to link Zi – 1	
2	Structural atom		
3	Open data atoms	Ui	
4	Encrypted data atoms	E(Gi,Xi)	Encrypted vote of a participant who can decrypt it by himself only
5	Encrypted data atoms	E(Gi,[Xi])	Encrypted vote of a participant, the voting organizer can disclose by sorting with a target complexity
6	Hash atom	H([Xi])	Information for the correct choice of a sorted key
7	Signature atom	Electronic signature of the voting organizer under fields 1–6 and 8	Information for fixing a link's unalterability
8	Ending border atom	Reference to the link Zi + 1	

- a hash atom contains the integrity control standard for one or several integral data atoms with (a) preset identifier (-s).

Type four includes subject atoms with descriptions of data interpreted as the active link component.

Subject atoms are divided into

- scenario atoms with an interpretable code for data atom processing,
- executor atoms with a compiled code for a real processor, a computer system hypervisor, or an atom machine where a blockchain is processed;
- machine atoms with the environment for the executing scenario or executor atoms.

Examples of Block Applications in Modern Technologies

We will consider an example of a blockchain link for registration procedures (voting included).

We assume that voting occurs featuring N participants ($N = 1, 2, ..., i, ... N$). The voting can be complex and its possible results include not only *yes* or *no* but also a random line, e.g., a candidate's full name (strictly speaking, *yes*, *no*, and *abstain* are text lines, as well).

Thus, Ui is a participant in the voting, Gi is his voice (generally, a text line), Xi is the secret identifier created by Ui in person with the aid of a random number sensor and unknown to anyone else, and [Xi] is the secret identifier reduced to provide the target length of sorting (e.g., at least for 1 day).

Ui forms a blockchain link Zi (Table 1).

In the vote reception phase the voting organizer forms and puts his own signature under the Zi blockchain links; in the summing up phase he performs the sequential sorting of [Xi] keys with regard to the contents of fields (atoms) four and five and fixes the votes of the participants as the results of decrypting atom four.

As a result, it becomes impossible to falsify the voting results and put pressure on real-time voters because their votes remain unknown until the summing-up phase; in addition, the vote giving sequence is kept unaltered and the voting minutes are reliably archived in the form of blockchain links.

To develop the described procedure, the reduction of the long-time modifier Xi can be made unnecessary by using the independent random number Ri such that |Ri| = |[Xi]|.

In terms of cryptography, this replacement is aimed at reducing the load on Xi when the voting is held more than once for a given participant. The definition of [Xi] that is then made to recover the vote will not affect the reduction in the set of sorting the entire Xi.

To expand the functional capabilities of a universal blockchain by adding the possibility of performing a job of a given complexity and receiving the respective remuneration, we will add a template atom or a future data atom to the data atoms. The added atom can be both a subject and an object.

A template atom contains the indication for a place in the link that a participant in the system is offered to fill in order to receive the target remuneration.

We will consider the registration procedure, where Ui is a participant in the system (the object owner) that registers the object Mi which generally includes binary data, such as an electronic document or a graphic file;

Xi is a secret identifier elaborated personally by Ui using a random number sensor and is unknown to anyone else;

Table 2

Identifier	Atom name	Contents	Notes
1	Initial border atom	Reference to link Zi – 1	
2	Structural atom		
3	Open data atom	Ui	
4	Encrypted data atom	E(Mi,Xi)	Encrypted registration object that can be decrypted only by its owner
5	Encrypted data atom	E(Mi,[Ri])	Encrypted registration object that can be decrypted by another participant in the sorting of a given complexity
6	Hash atom	H([Ri])	Information for the correct choice of a sorted key
7	Hash atom	H(Mi)	Information for the ultimate verification of object decryption
8	Template atom	Space for including Mi (when document disclosure is planned) or indicating the atom's functionality when no disclosure is planned	
9		Data or instructions (object or subject) followed in data disclosure, including the procedure for receiving remuneration	
10	Signature atom	Owner's electronic signature under fields 1–7, 9, and 12	Information for fixing the unalterability of a link while data remain undisclosed
11	Signature atom	Owner's electronic signature under fields 1–9 and 12	Information for fixing the unalterability of a link when data are disclosed and included in the template (the owner can do this because he owns Mi)
12	Final border atom	Reference to link Zi + 1	

[Ri] is the secret identifier created to achieve the complexity of target sorting.

We will consider the case where a second participant can discover and confirm the registration and physical existence of Mi and receive the respective remuneration.

The Zi blockchain link formed by Ui is described in the table below.

This technology is applicable when it is necessary to keep data confidential for a given period of time and then publish them in open access.

Blockchain Requirements

The blockchain requirements can be divided in the following groups:

(1) Structural requirements on the availability of particular types of atoms (data) in blockchain links to ensure the operation of the specified technologies. Additionally, these requirements may include the requirement for global blockchain cohesion: there must be one or several links to describe the general structure or a particular subset of blockchain.

(2) Organizational requirements related to national or international cryptography regulations that stipulate the application of national, recommended, or certified cryptographic tools to form and process blockchain atoms. In addition, this group may include requirements related to national or institutional standards in application fields: taxation area, voting technologies, in-house document workflow, etc.

(3) Technological requirements on the reliability of block link storage (using, e.g., the technology from [2]), which must help to maintain the storage reliability and availability parameters of these links. The parameters are set by regulatory bodies of blockchain application industries. Additionally, the technological requirements must describe the requirements on the capacity of operations with links and extreme volumes of their accumulation and storage.

(4) Confidence requirements with a clear blockchain structure, regulated link processing technologies, and an interface for link operations. All applied

interfaces must be available with source codes to ensure a high level of confidence. Additionally, the technology can be formally verified by mathematical modeling.

CONCLUSIONS

The considered features of the blockchain technology, typical data structures, and its requirements can be the basis for elaborating corporate blockchain requirements and solutions and can be utilized to make balanced decisions on choosing and utilizing this technology in corporate and governmental information systems.

ACKNOWLEDGMENTS

This work was written as part of the research carried out by the Cybersecurity Problems task group of the Federal Agency for Scientific Organizations of Russia and also as part of the *Algebraic and Combinatory Techniques of Mathematic Cybernetics and New-Generation Information Systems* basic research program of the Department of Mathematical Sciences of the Russian Academy of Sciences, supported by the Russian Foundation for Basic Research, project no. 15-07-08522.

REFERENCES

1. Centralized crypto-currencies. http://www.geektimes.ru/company/waves/blog/289379/.
2. Zaitsev, A.V., Gostev, S.S., Cherkashin, P.A., and Shcherbakov, A.Yu., Regarding the technology of distributed storage of confidential information in centers of general-purpose data processing, *Autom. Doc. Math. Linguist.,* 2017, vol. 5, no. 3, pp. 117–119.

Translated by S. Kuznetsov

SPELL: 1. ok