UDC 004.056.5 DOI:10.30837/rt.2019.3.198.07

KATERYNA ISIROVA, OLEKSANDR POTII, Dr. Sc.(Tecnology),
JENS CHRISTIAN CLAUSSEN, Dr. Sc.

ESTABLISHING TRUST PROTOCOLS IN MUTUAL DISTRUST NETWORK BY CONSENSUS FORMATION

Introduction

TRUST formation in computer networks by means of verification protocols has become an important subject in computer science and impacts the architecture and design of networked applications in a wide range. This issue is particularly relevant in the face of future increasing threats from quantum computing, when it will become impossible to rely only on the cryptographic strength of key system parameters.

In this paper, we draw attention to the analogy between consensus formation in social networks and trust formation in verification computer protocols. In both application domains, trust could be built within different possible topological architectures. It is interesting that consensus formation, in both disciplines, could be reached, among other topologies, both for a hierarchical and for a distributed architecture. However, the computational efficiency, in this context quantified by the time to consensus, can be quite different and depends both on the number of nodes and on the network topology.

The paper is organized as follows. In section 2 we introduce the paradigmatic voter model and present the results of simulation with two types of different architectures. In section 3 we generalize the main principles of the most widespread infrastructure and describe how it could be implemented with different architectures. Finally, in section 4 we compare and discuss the results of consensus formation time simulations, and discuss practical implications.

1. Consensus formation in social networks

1.1. The paradigmatic voter model

In this work, we are primarily concerned with the consensus formation in hierarchical versus distributed consensus protocols, highlighting the network topology dependence of the system size scaling. In complementing perspective, topology-dependence of consensus formation has been extensively studied in the context of consensus or political opinion formation both in homogeneous populations [1, 2] and in social networks [3]. Besides the formal mathematical analogy, we intend to convey the transdisciplinary viewpoint, to view (a) the protocol handshake between two computer nodes as an interaction between agents within an (artificial) society, and (b) social individuals within a population, when exchanging and agreeing on opinions, implicitely perform a formal protocol that is (observing some transmission uncertainties frameable in an information- theoretical treatment) prescribed by a logical set of social rules.

To arrive at a mathematically or computationally tractable model, it appears necessary to razor down the model to the bare necessities of the mechanism. The voter model [4] casts opinion transmission from one agent to annother into only one possible elementary interaction: in each time step, one agent is selected at random, and thereafter persuades annother agent, that is randomly chosen among the next neighbours. We observe that the interaction topology, defined by a graph adjacency matrix, will influence the dynamics of the opinion formation process.

Although it has been prominetly questioned whether the voter model itself serves as a precise model for voters [5] it is acknowledged that statistical scaling features of opinion formation processes are covered even from this simplified model.

1.2. Definition of the Voter Model

The voter model mathematically is defined as a discrete stochastic process [4]. In its standard version, the system is comprised of N nodes forming a connected graph with adjacency matrix (a_{ij}), and the system state is defined by the state of all nodes, which can assume the values 0 or 1, respectively. These binary states can reflect opinions, an activated gene, an infection status in a contagion system, or the certification status of a node in a computer network. In the case of all nodes being in a homogeneous initial condition, i.e., all 0 or all 1, due to the absence of mutations or spontaneous opinion changes, no further change takes place, hence these states are absorbing states of the dynamics. In each step in discrete time, the following dynamics (algorithm) is executed:

1) One node is chosen at random.
2) One of the nodes *j* is connected to *i* (i.e., a_{ij} = chosen at random.
3) Node *j* assumes the state (opinion) of node *i*.

The last step can be interpreted in the way that node *i* convinces node *j*. If all nodes reach the same state, all 0, or all 1, consensus is reached, and the number of iterations is called time to consensus. It is common to perform Monte-Carlo simulations averaging over a sufficiently large number of initial conditions, to obtain reliable estimates for the expected average time to consensus. As the average time to consensus is largest when the number of 0 states and 1 states in the initial configuration equals N/2|, we∫have chosen such a symmetric configuration of maximal dissensus as initial configuration for all our simulations of the voter model.

1.3. Consensus Formation in the Voter Model in Different Topologies

To address systematically the average time to consensus, we have performed extensive Monte Carlo simulations of the voter models on different network architectures. These include an all-to-all coupled network (also known as complete graph in graph theory), a ring network as a one-dimensional structure with periodic boundary conditions, and specific hierarchical tree structures that resemble hierarchical both social and computer architectures.

Fig. 1 displays the average time to consensus depending on the total number of nodes N , in double logarithmic plot, for the different architectures.

2. Trust formation in computer networks

The concept of consensus formation takes place not only in the context of social networks, but also in the context of computer protocols. For almost 20 years, the society has been introducing electronic technologies into its life.

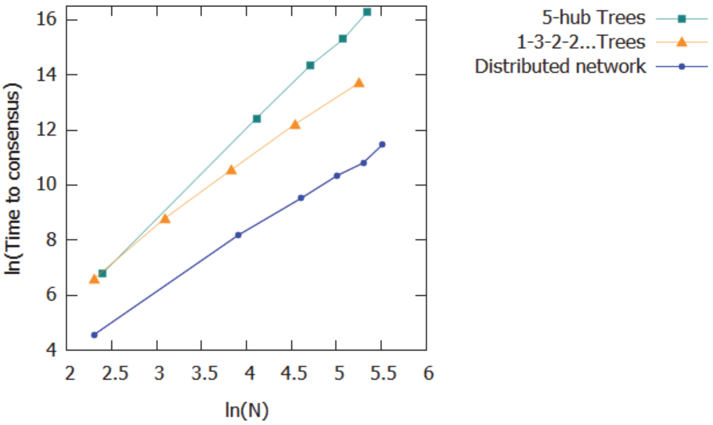

Fig. 1. Simulation results for the voter model on different network topologies. Distribution of different opinions on initial stage is 50/50. Probability of acceptance neighbor's opinion is equal to 0.5. (Results are averaged over 100 experiments)

Building trust in the online environment is a key to economic and social development. Lack of trust makes stakeholders hesitate to carry out transactions electronically and to adopt new services. The critical issue is to ensure trust in an environment of mutual distrust: a network where none of the participants trust the other. Let us mention that not only people can act as participants in the network, but also artificial intelligence agents. For instance, when building a network using the Internet of Things. As we can see, successful implementation of modern technologies of electronic management, electronic trusted services are not possible without the creation of an appropriate infrastructure. The infrastructure for implementing the above mentioned technologies is the public key infrastructure (PKI).

PKI is a set of tools (technical, material, human, etc.), distributed services and components, which are collectively used to support crypto tasks based on private and public keys [8]. It does not matter whether it is a national PKI to support electronic signature tasks or a private PKI for an individual organization to support employee authentication processes, or PKI deployed on a smart home base, the principles for ensuring security remain unchanged.

In fact, PKI are based on several basic principles:

1. Private Key is known only to its owner.

2. Certification Authority (CA) creates an electronic document – a public key certificate, thus certifying the fact that the private key is known exclusively to the owner of the certificate, the public key is freely transferred in the certificate.

3. Nobody trusts each other, but everyone trusts to CA.

4. CA confirms or refutes the belonging of the public key to the given person who owns the corresponding private key.

As we can see CA acts the role of security guarantor. Although, the presence of the guarantor itself cannot ensure the security of iterations between network users. Additionally, to ensure the trust between participants reliable implementation of actual trust model should be done.

According to [7] there are verities of possible trust models:

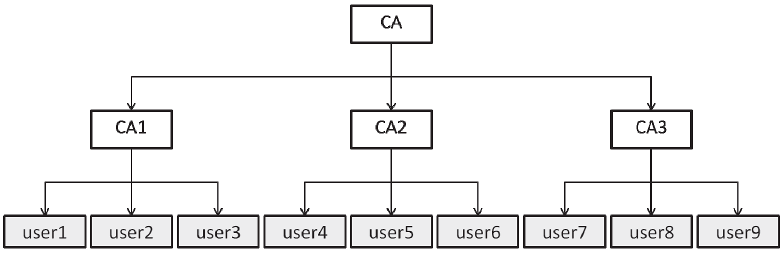

Fig. 2. Strict hierarchy of CA

- strict hierarchy of CA;
- not a strict hierarchy of CA;
- policy based hierarchy;
- distributed trust model;
- quadrilateral trust model;
- trust model around the user;
- web trust model.

In current paper we will consider two of them (a) Strict hierarchy of CA and (b) Trust model around the user, since the first one is the most widespread nowadays and the second is very convenient for developing distributed PKI.

2.1. Hierarchical PKI developing principles

The hierarchical structure is easy to imagine as a tree with a root at the top and leaves at the bottom (as shown in Fig. 2). The end point of trust is the root of the tree. The number of intermediate levels can be different, including zero. Classically, in a hierarchical architecture, security is ensured by the trust of all participants to a third trusted party, certification authorities, based on the fact that they are subject to a certification procedure.

A user requiring knowledge of a public key generally needs to obtain and validate a certificate containing the required public key. If the public key user does not already hold an assured copy of the public key of the CA that signed the certificate, the CA's name, and related information (such as the validity period or name constraints), then it might need an additional certificate to obtain that public key. Certification paths start with a public key of a CA in a user's own domain, or with the public key of the top of a hierarchy. In both cases, it is impossible to verify the validity of the user's public key certificate without building a complete certificates chain. Such a chain links current user and a tree top. This structure allows reliably implement iterations between users, since CA is considered as trust anchor. On the other hand, that means that in the network there are a number of critical and potentially vulnerable points. Usually, these points should be subject to regular audit and strict control. In order to reduce the risk of data loss, it is necessary to store a large amount of backups, which significantly increases the cost of maintaining the system.

We can conclude that such structure has a number of other drawbacks [11], [12]:

- security of the hole system depends on CA root certificate. In case of its compromise, all certificates in the system are compromised;
- users do not actually dispose of their identity. If necessary, make any adjustments user need to contact CA;
- lack of interoperability, since certificates issued by different CA not always could be used in one system;
- there is no one-to-one correspondence between the user and the certificate, by how many certificates can be issued for one user.

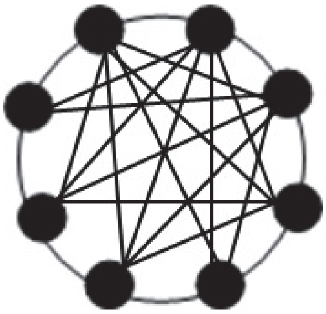

Fig. 3. Example of distributed PKI

2.2. Decentralized PKI developing principles

Another way for developing PKI without building tree structure was proposed by authors in paper [11]. The main idea was to exclude the central point of trust and ensure security using blockchain technology.

The blockchain technology [9] was introduced in 2008, its first implementation, i.e. Bitcoin, was introduced a year later, in 2009, published in the paper "Bircoin: a Peer-to-Peer Electronic Cash System" under alias Satoshi Nakamoto [10]. Since then, this technology has only gained its spread, cryptocurrencies and e-commerce market remain the main areas of application [15 – 17]. However, besides its use in electronic commerce, the blockchain technology can be implemented in other aspects. In particular, in order to avoid the disadvantages associated with the construction of a hierarchical structure. The main idea of using blockchain technology for building a decentralized PKI is that we place the register of the public key certificate status into blocks, thus, ensuring its safe storage. At the same time, the special structure of the distributed database allows users to reliably verify the certificate of the public key of another user with- out referring to a third trusted party. The main difference from the hierarchical structure is that users independently store their key pair, so that a user's public key certificate can be obtained only from himself. Special procedure was introduced only for the new user primary identification process. For this purpose, trusted nodes (analogs of CA) still exist, but their functions are sharply reduced compared with the hierarchical structure. After a new user goes through the primary identification procedure at a trusted site, he will no longer be contacted.

Such a structure can be a variation of distributed graphs (in this paper we will consider only a fully connected graph) as shown in Fig. 3.

According to [12] the main advantages of such propose are:

- considerable reduction in the cost of maintaining a cumbersome hierarchical structure of CA;
- users are able independently control their identification data and is able to immediately report about the need for their correction (compromise);
- leveling ”man in the middle” threat. The intruder will need to attack the entire system;
- the directed attack target disappeared. In contrast to hierarchical structure, when the main targets for the attackers were CA, in this case there is no clear target for the attack, because the information is stored in a distributed manner and in fact the attacker is forced to attack the whole network but not a specific node;
- the proposed system coulb be used not only for the electronic signature service, but also for ensuring the electronic identification;
- collapse of one or more nodes does not result in system shutdown;
- no need to make and store backups;
- system interoperability relies on the fact that certificates issued by various CA can easily be used in a single system;
- easy scalability, because adding a new user (a new node) occurs without changing the basic principles of the architecture.

3. The analogy between opinion formation in social network and trust formation in PKI

By consensus in PKI, we mean the state of the network, in which each node is confident in the legitimacy of all other participants. This is possible after the “network authorization” procedure. The essence of which is to initiate the interaction of each user with all others according to the laws of the certification chain in a hierarchical structure and according to the blockchain laws in a distributed one.

In this section, we present the results of simulations that were carried out using the developed software. Note that we did not integrate the digital signature algorithms directly. For the comparison procedure, it is sufficient for us to state that a uniform digital signature algorithm is applicable in all topologies.

To perform simulations regarding “network authorization” procedure on different topologies, the following initial conditions should be specified:

1. The network is given by a graph (fully connected or hierarchical one).
2. Nodes store the field ”opinion” (boolean values 1 – user is legitimate, 0 – intruder).
3. Participants do not know in advance which of the nodes are controlled by intruders. They can figure it out only in process of pairwise interaction. That means (a) passing through the certification path in the hierarchical architecture or (b) by interacting with each other participant in a distributed one.
4. We assume that at the initial stage, 50 percent of the nodes are controlled by attackers.
5. If an intruder is detected, he (and the nodes that depend on him in the tree) should be excluded from the network and consensus formation should be completed without it. In this way a network of legitimate participants will be formed and they will be able to interact seamlessly and securely.
6. Nodes that have been excluded from the network have to be regenerated (again with a probability of 50 percent) and added to the network.
7. By consensus time, we will mean the time spent on the full authorization of the network (including the time for regeneration and re-connection of nodes)

The following assumptions are necessary to describe the “network authorization” procedure:

- the considered topologies are in a closed / protected space (thus, we consider a private PKI or a private blockchain);

- the time of mutual/cross verification (verification of the public key certificate) takes one iteration;
- the node regeneration time takes two iterations (since it is necessary to regenerate the private key and create a new public key certificate).

3.1. Hierarchical network protocol

For the correct work of the protocol, prerequisite is to follow the requirements that are enshrined in X.509 [7]. Current paper considers only the protocol for a strict hierarchical structure, which means the need to build a certification path up to the root node when initializing the interaction of any two users.

”Network authorization” procedure for hierarchical net- work topology should consist of following.

1. The interaction begins with the leaves of the tree and has a direction to the root.
2. The route is determined by the rules of the certification path in accordance with X.509 [7].
3. When an intruder node is detected, it and all of its child nodes must be excluded and subjected to a regenerating procedure.
4. The interaction procedure should continue for all legitimate sites.
5. After all the legitimate nodes have interacted; the procedure for regenerating the offending nodes should be be started.

Moreover,

- if the node-intruder had no children (acted as an end user), during the procedure of its replenishment there is a probability (we will set it equal to 50 percent) that it will again appear to be intruder.
- if not (acted as a certificate authority), then it should be directly regenerated with the value “1-legitimate”, and all its child nodes, with a probability of 50 percent can again become intruders.

Corresponding simulations were performed for two hierarchical topologies types : for (a.1) tree where every node has a degree of three (Fig. 4) and (a.2) tree with five hubs (Fig. 5).

The tree with every node degree is three is a classic symmetrical PKI, which is well suited for structuring an indepth organizational structure. The limited number of child nodes does not allow the system to expand rapidly in the horizontal direction. An example of the use of such a PKI can be the union of small but clearly structured units.

From the opposite side, it is worth noting that tree with five hubs looks typical for a “wide” company PKI organization. With this topology, we have several (in this case, five) large subtrees (divisions) within which a large number of equal users can interact.

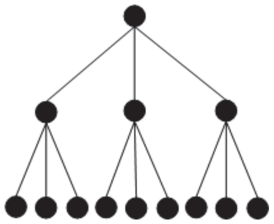

Fig. 4. Tree where every node has a degree of three

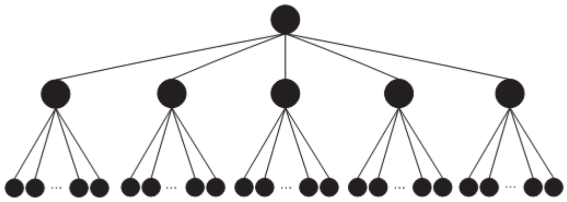

Fig. 5. Five-hubs Tree

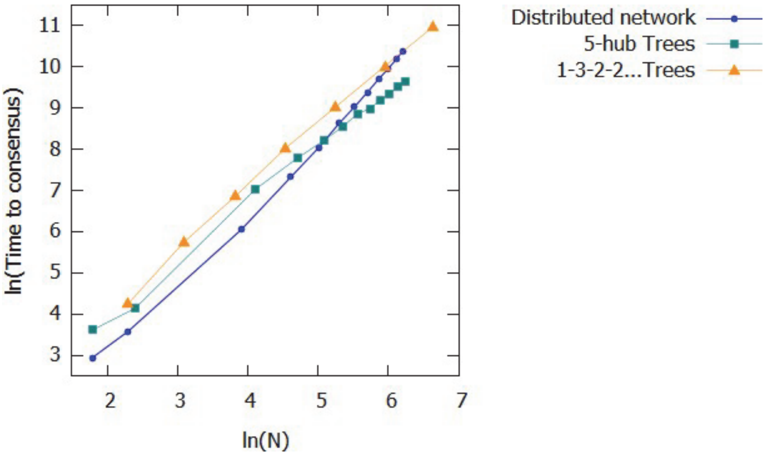

Fig. 6. Simulation results for different topology types. Distribution of legit users/intruders on initial stage is 50/50. Probability of regeneration for node is equal to 0.5. Results are averaged over 100 experiments

3.2. Distributed network protocol

”Network authorization” procedure for hierarchical net- work topology should consist of following.

1. Interaction could be started from any node in the network.
2. It is required to perform pairwise certification (ex- change key certificates) between every nodes
3. When an intruder node is detected, it must be excluded and subjected to a regenerating procedure.
4. The interaction procedure should continue for all legitimate sites.
5. After all the legitimate nodes have interacted, the procedure for regenerating the offending nodes must be launched (taking into account the probability of regeneration equal to 50 percent)

The protocol continues its operation until all nodes are legitimate and do not interrelate with each other.

3.3. Simulation results

Fig. 6 presents results of simulations.

We can conclude that for smaller networks distributed networks shows much better time to consensus and with an increasing number of nodes the advantage ceases to be so noticeable.

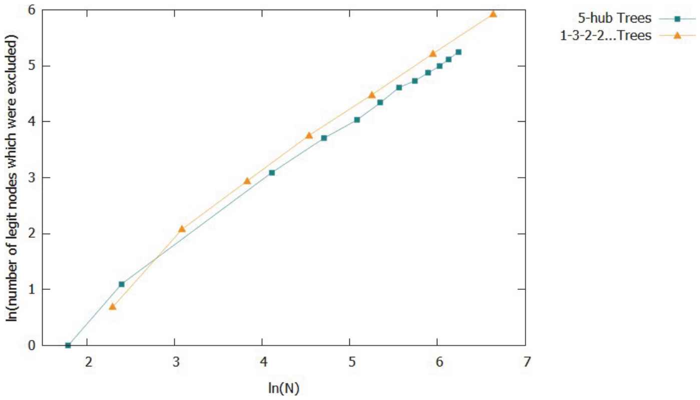

Fig. 7. Simulation results for Tree topologies. Dependence of the number of legitimate nodes that have been excluded from the size of the network. Distribution of legit users/intruders on initial stage is 50/50. Probability of regeneration for node is equal to 0.5

This tendency can be explained by the fact that to establish all links to a node in a distributed structure, it is necessary to perform a greater number of “handshakes” (cross-certification procedures) with a larger system size. At the same time for tree structures, this number grows at a slower rate.

However, another parameter should be taken into ac- count too. The number of legit users, which were excluded from the network. Obviously, such a situation is possible only in tree structures (Fig. 7), and for a distributed net- work, this value will be zero for any size of the network.

Based on the plot it is clear that with the growth of the network, the number of legitimate users who have been excluded and regenerated is growing and can reach 50 percent (and in some cases 100 percent) of the number of all users on the network. This is easy to imagine if the root node of the tree system is compromised. This situation causes network redundancy and leads to inefficient use of resources.

Discussion and conclusions

Nowadays progress in the field of electronic technologies allows providing more efficient electronic trusted services. Building trust is an important task for the reliable critical infrastructures functioning at any level. Moreover, to conduct completely secure interactions, not only the trust among the users (human or artificial intelligence) is required, but also confidence in the technology itself. Distributed trust models and public key infrastructures will become information technologies of increasing importance, especially in the context of information security when quantum computing technologies become available. Industries, trafic and trade networks as well as the public services sector are increasingly relying on secure networks [13], [14], which often operate internationally and on scales of large number of nodes. This imposes challenges on the architecture of the verification protocols, such that these can be managed with computational and network resources scaling with system size in a feasible way. Besides optimizing the protocols themselves, the network topology of each verification concept will have a significant impact on its efficiency. PKI looks like a very promising instrument to ensure trust in a mutual distrust network, however, zero-day threats, such as the active development of quantum computing, should be taken into account. And if we do so, then it should be understood that the security of the whole system cannot rely only on the key parameters cryptographic security, but additional measures are also required to ensure the resilience of the system. Such measures can be distributed technologies, in particular, those based on the blockchain technology. Here, we have investigated distributed PKI in comparison with hierarchical CA architecture. The time (in units of protocol verification steps) for verification of all nodes in the whole network has, as we argue, an important analogy to the time to consensus formation in a social network. Consequently, we investigate this time to consensus on different topologies, both for computer verification protocols, and for consensus formation in social networks as described by the well-established voter model. We have performed Monte-Carlo simulations for all-to-all coupled networks, or complete graphs, resembling a fully distributed PKI, or a maximally connected social network in which information may reach out to any node. This is not unrealistic in some social subnetworks, like a school class, or the scientific com- munity where all university lecturers and active researchers can be reached electronically through their departmental email documented in the web. For representative hierarchical architectures, we have focused on a tree where all top and middle layer nodes have a node degree of three, and a hub-tree akin of a company with 5 departments and flat hierarchy therein. These two trees represent a many- layer structure and a few-layer structure, respectively. We find that, in the social opinion formation by the voter model, the distributed network, by large margin, provides fastest consensus. This result holds over the whole range of investigated network sizes. While both tree architectures perform similarly on small networks, for large networks the 5-hub trees converge slower, even with a different scaling, to consensus. For medium-size networks, the results for the verification protocols are similar, although the 5-hub trees outperform the many-layer trees for medium and large net- works. Counterintuitively, the largest networks investigated (around $N = 200$) show a decaying performance for the distributed networks.

This may be related to our assumption, originally motivated from the opinion formation analogy, of 50 of 100 nodes being not trusted, which puts the system in a dynamical regime where recovery to a fully certified net- work may take long. Further, our investigation confirms our hypothesis that the network topology has a significant role in the time to consensus. However, the network architecture which is optimal may still depend on the type of protocol (where we made some generic assumptions), and on the system size. This aspect, together with addressing resilience to targetet attacks, should be subject of further investigation.

Acknowledgments

Kateryna Isirova acknowledges funding through the Erasmus programme during her research visit to Aston University, Birmingham (UK).

References:

1. Jan Lorenz. Continuous Opinion Dynamics Under Bounded Confidence: a Survey // J. Mod. Phys. C 18, 1819-1838 (2007).

2. Claudio Castellano, Santo Fortunato and Vittorio Loreto. Statistical physics of social dynamics // Rev. Mod. Phys. 81, 591 (2009).

3. Petter Holme and M. E. J. Newman. Nonequilibrium phase transition in the coevolution of networks and opinions // Phys. Rev. E 74, 056108 (2006).

4. Thomas M. Liggett. Interacting Particle Systems. Springer, Berlin (2012).

5. Juan Fern a´ndez-Gracia, Krzysztof Suchecki, Jose´ J. Ramasco, Maxi San Miguel, and V´ıctor M. Egu´ıluz, Is the Voter Model a Model for Voters? // JPhys. Rev. Lett. 112, 158701 (2014).

6. Quantum Safe Cryptography and Security; An introduction, benefits, enablers and challenges. Quantum Safe Cryptography // ETSI White paper, 2015

7. ISO / IEC 9594-8 ITU – T Rec. The X.509 ”The Basic s e PROVISIONS certification key and certificate attributes”.

8. PKI: technology, architecture, construction and implementation: a tutorial / Potiy A.V., Lenshin A.V., Soroka L.S., Esin V.I., Moroz B.I. Dnepropetrovsk : Akadimiya border service of Ukraine 2011. 202 pp.

9. Draft NISTIR 8202 : Blockchain Technology Overview.

10. Satoshi Nakamoto. Bitcoin: A Peer-to-Peer Electronic Cash System. Technical report.

11. Isirova Kateryna. Decentralized Public Key Infrastructure Development Principles / Kateryna Isirova, Oleksandr Potii // The 9th IEEE International Conference on Dependable Systems, Services and Technologies, DESSERT’2018, 24-27 May, 2018, Kyiv, Ukraine. P. 320-326.

12. K. Isirova, Blockchain technology as the perspective instrument for ensuring electronic trusted services in conditions of cyberthreats // European Cybersecurity Journal. Volume 5 (2019), Issue 1, pp. 34-42.

13. Stefan L a¨mmer, Hiroshi Kori, Karsten Peters and Dirk Helbing. Decentralised control of material or traffic flows in networks using phase-synchronisation // Physica A 363, 39-47 (2006).

14. Laura Alessandretti, Abeer ElBahrawy, Luca Maria Aiello and Andrea Baronchelli. Anticipating Cryptocurrency Prices Using Machine Learning // Complexity 2018, 8983590 (2016).

15. Deepak Puthal, Nisha Malik, Saraju P. Mohanty, Elias Kougianos and Chi Yang. The Blockchain as a Decentralized Security Framework // IEEE Consumer Electronics Magazine 7, 18 (2018).

16. Zibin Zheng, Shaoan Xie, Hongning Dai, Xiangping Chen and Huaimin Wang. An Overview of Blockchain Technology: Architecture, Consensus, and Future Trends // 2017 IEEE 6th International Congress on Big Data, DOI: 10.1109/BigDataCongress.2017.85.

17. Francesco Parino, Mariano G. Beir o´ and Laetitia Gauvin. Analysis of the Bitcoin blockchain: socio-economic factors behind the adoption // EPJ Data Science 7, 38 (2018).

Kharkiv National V.N. Karazin University;
JSC "Institute of Information Technologies";
Mathematics EAS, Aston University, United Kingdom

Received 11.09.2019