Decentralized Electronic Voting System Based on Blockchain Technology Developing Principals

Kateryna Isirova [0000-0002-0250-7636], Anastasiia Kiian [0000-0003-2110-010X], Mariia Rodinko [0000-0003-4692-9811] and Alexandr Kuznetsov [0000-0003-2331-6326]

V. N. Karazin Kharkiv National University, 4 Svobody Sq., Kharkiv, 61022, Ukraine
KaterinaIsirova@gmail.com, nastyaK931@gmail.com, m.rodinko@gmail.com, kuznetsov@karazin.ua

Abstract. Electronic trust services are becoming an integral part of the information space. With the reliable implementation of basic services as an electronic signature and electronic authentication, it is possible to build more complex systems that rely on them, particularly the electronic voting system. In the paper, the new concept for developing a decentralized electronic voting system using blockchain technology is proposed. The two-level architecture provides a secure voting process without redundancy of existing (not based on blockchain) systems. The presented blockchain-based voting protocol has six steps that ensure all requirements that are put forward to such types of protocols including voting transparency and anonymity.

Keywords: Decentralized Electronic Voting System, Decentralized identification, Electronic Voting Protocol, Blockchain Technology.

1 Introduction and Formal Problem Statement

Electronic trust services are becoming an integral part of the information space. Their use is governed by Regulation (EU) No 910/2014 of the European Parliament and of the Council of 23 July 2014 on electronic identification and trust services for electronic transactions in the internal market and repealing Directive 1999/93/EC [1] which establishes terms and conditions. With the reliable implementation of such basic services as an electronic signature and electronic authentication, it is possible to build more complex systems that rely on them, for example, an electronic voting system.

Remote (electronic) voting has many advantages. It is assumed that they are more convenient for end-users because people can vote without leaving home; this increases the activity of voters. Maintenance of electronic voting is cheaper: instead of permanently printing ballots, it's enough to develop a system once. In addition, the assumption that no one can interfere with the program on the voting device implies that electronic voting is less susceptible to corruption, administrative pressure, and human factors. However, this raises a number of specific problems that hinder the integrity of elections. Remotely, it is much more difficult to authorize a voter or make sure that no one has influenced the voting process. On the other hand, the Internet provides more opportunities for checking by ordinary voters whether the voice is correctly taken into account. Currently, electronic voting is fully legal or partially applicable in many countries of the world [2]. Since more and more people are involved in them, the need for safer and more efficient methods for their implementation is increasing, which is what special cryptographic protocols are designed for [3-8].

It should be noted that today the developing process of any system has to take into account the evolution of quantum computers and as a result the growth of computational speed. In the conditional of current cyber threats secure of the system should not base only on key parameters cryptographical secure [9-11]. Important point is to ensure the resilience of the system. From this point of view blockchain technology might be useful.

The main purpose of this paper is to formulate the development principles for a decentralized e-voting system that would prevail over existing e-voting systems without a decentralized structure.

2 Electronic Voting System Principals Structure

The system of electronic voting is a set of interrelated rules, methods, processes, tools, and technologies, as well as legal norms that together provide and regulate the remote legitimate voting of authorized users (voters).

Components (subsystems / levels) of the electronic voting system (see Fig. 1):

- legal level (laws and other regulatory documents);
- organizational level (e-voting system architecture);
- process level (processes for participants);
- technological level (methods, tools, protocols, technologies).

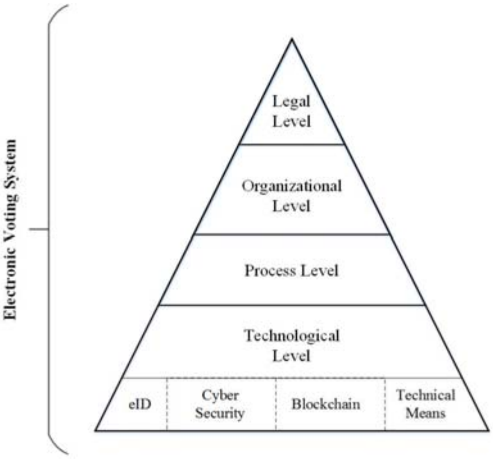

Fig. 1. Levels of electronic voting system

Requirements for secret e-voting systems [12].

Required:

- no one except the voter should know his choice;
- only legitimate members can vote, and moreover only once;
- the decision of the voter cannot be secretly or explicitly changed by anyone (except, perhaps, by himself). In addition, the desired requirements are set out [12]:

Desirable:

- each legitimate participant can check whether his voice is correctly counted;
- each legitimate participant may change his mind and change his choice within a certain period of time;
- the system should be protected from the sale of votes by voters;
- in case the vote is incorrectly counted, each legitimate participant can report this to the system without revealing his anonymity;
- it is impossible to track where the voter remotely voted from;
- operator authentication;
- you can find out who participated in the vote, and who - no;
- maintaining the system should not require a lot of resources;
- the system must be fault tolerant in case of technical malfunctions (loss of power supply), unintended (loss of the key by the voter) and malicious (intentionally disguising itself as another voter, DoS / DDoS) attacks.

The major threats to systems of this type are:

- legitimate voter cannot vote;
- loss of voter anonymity;
- registration of non-existent voters;
- the use of blank ballots that registered but did not participate in the election.

3 The architecture of the decentralized voting system

The architecture of the decentralized e-voting system is two-level and consists of two intersecting blockchain networks, the lower network is a decentralized electronic identification infrastructure (DI eID), and the upper network is a decentralized infrastructure for voting itself and counting the results (DI voting) (see Fig. 2).

3.1 Decentralized Electronic Identification Infrastructure (DI eID)

This infrastructure should provide a procedure for the reliable identification of users and a list of legitimate voters' establishment. It consists of providers of identification services (hereinafter - IdP providers). It is necessary to ensure the implementation of the identification using:

- BankID;
- MobileID;

- e-passport of the citizen;
- electronic signature (including both software and hardware implementation (token))

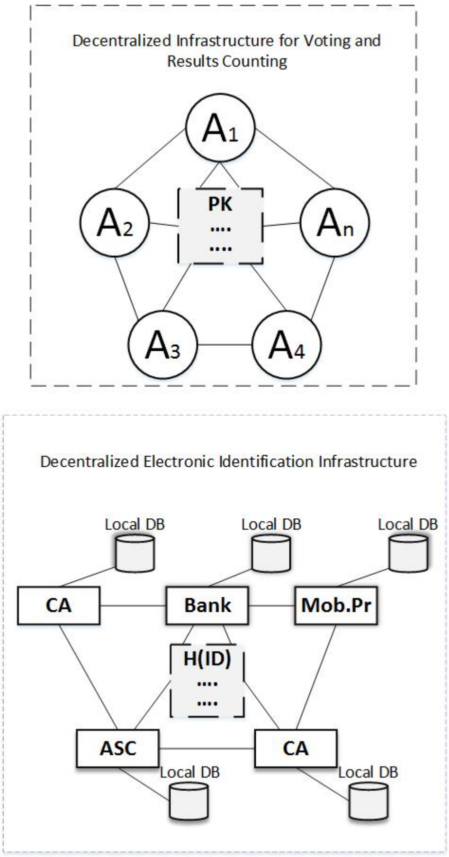
Decentralized Infrastructure for Voting and Results Counting
A_1
A_2
PK
....
....
A_n
A_3
A_4
Decentralized Electronic Identification Infrastructure
Local DB
Local DB
Local DB
CA
Bank
Mob.Pr
H(ID)
....
....
ASC
CA
Local DB
Local DB

Fig. 2. Decentralized Electronic Voting System Architecture

According to the requirements, the following entries may act as identity providers:

- Bank institutions;
- Mobile operators;
- Migration Service Centers (Administrative Service Centers - ASC);
- Certification authorities of the national digital signature system.

Provisions for the operation of providers are established by the Law of Ukraine "On Electronic Trust Services", implemented by the EU Regulation and other international and national normative documents.

Each identity provider has a pre-generated local database of its users, which contains their identities and possibly local IDs. The responsibility for the secure storage and correct use of local databases rests with identity providers.

In order to organize the identification infrastructure within a decentralized electronic voting system, the identity providers are combined into a separate private permissioned blockchain network. In this network, each of the identity provider acts as a validator node. It should be noted that complex and energy-intensive consensus protocols are not required for such a network because the network connects trusted ("honest") nodes.

3.2 Decentralized Infrastructure for Voting and Results Counting

The infrastructure should provide for the process of the remote voting of registered (authorized) legitimate voters and the process of results counting. In addition, generation processes for voters' wallets and candidates' wallets should be organized in this infrastructure. For the organization voting infrastructure under the decentralized electronic voting system, the representative offices responsible for conducting the election process (A1, A2, ..., An), like identification providers, are combined into a separate private blockchain network, in which each of Ai acts as a validator node - collectively they represent a decentralized Agency (A). Similar to the upper blockchain network, the lower one also does not need to use complex and energy-intensive consensus protocols because the network connects trusted ("honest") nodes. Validator nodes form purses for legitimate voters and carry out voter authentication. They are also responsible for the process of wallet generation for alternatives (candidates).

3.3 Voting Protocol in a Decentralized Electronic Voting System

The voting protocol in a decentralized electronic voting system consists of the following steps:

1. Formation of the of legitimate voters' list in a decentralized electronic identification infrastructure;
2. Generation of legitimate voters' wallets in a decentralized infrastructure for remote voting and results counting;
3. Candidates registration in a decentralized infrastructure for remote voting and results counting;
4. Voters' authentication in decentralized infrastructure for remote voting and results counting;
5. Voting in a decentralized infrastructure for voting and results counting;
6. Counting of votes in a decentralized infrastructure for voting and results counting.

The implementation of this protocol using blockchain technology allows depending on the needs of the target system to change the order of some stages (basically the fourth and fifth) without loss of reliability. The direct sequence (fourth to fifth) implies that only authenticated users (legitimate voters) are allowed to vote. The reverse sequence (fifth to fourth) allows participation in the voting process of potential violators (illegitimate voters), but due to the peculiarities of the implementation of the transaction consensus mechanism, and accordingly, the votes of illegitimate users will not be taken into account. This is based on the assertion that in any blockchain network, a transaction is considered validated only if both conditions are fulfilled:

1. the format and signatures of the transaction are verified;
2. validator nodes have reached consensus on including this transaction in the block chain.

The principles of building a decentralized infrastructure for remote voting and counting results do not allow validation nodes to include a transaction from an illegitimate voter in the blockchain since the first condition will not be fulfilled (transaction signature will not be valid).

Stage One (Formation of the of legitimate voters' list in a decentralized electronic identification infrastructure).

Forming lists of legitimate voters occurs in the lower blockchain network. Each potential voter independently generates a key pair (SK; PK). Then he/she sents a request to be included in the voters' list to one of his/her available identity provider, in which he/she provides his/her with his identification information and public key.

The format of the request depends on the available communication channels between the voter and the identity provider. It can be made remotely via the Internet provided there is a reliable communication channel (see Fig. 3b), or such an identification request can be made personally by a potential voter within the identity provider controlled zone. If the request is made remotely, the responsibility for complying with the key pair generation rules rests with the user. If the request is made personally within the controlled zone, the identity provider is responsible for complying with the conditions of the generation of the key pair of the user.

If a potential voter already has generated key pair as required by one of the identification providers, he or she may use it. In this case, the public key certificate must be included in the request to the provider (see Fig. 3a).

If a positional voter does not have a local ID in any of the identity provider database, he or she must undergo a primary identification procedure with one of the identity providers and only then be included in the list of legitimate voters (see Fig. 3c). The initial identification procedure should be conducted in accordance with the rules of a certain identity provider.

Thus, when the time allotted for forming legitimate voters' list has run out, an anonymous (depersonalized) list of potential legitimate voters is created in the lower blockchain, and the Agency receives a list of all registered legitimate voters, but voters remain anonymous. The identification processes for different types of users are shown on the figures 4a-4c.

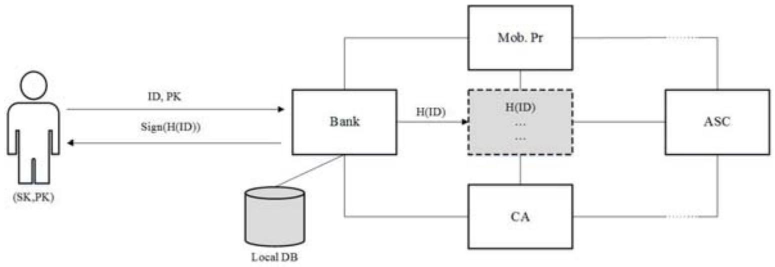

Fig. 3a. Identification procedure based on user's local ID

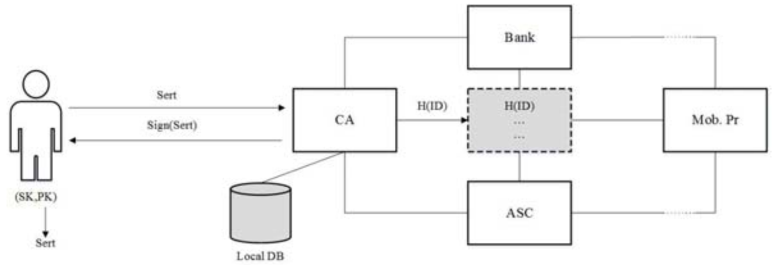

Fig. 3b. Identification procedure based on user's Certificate

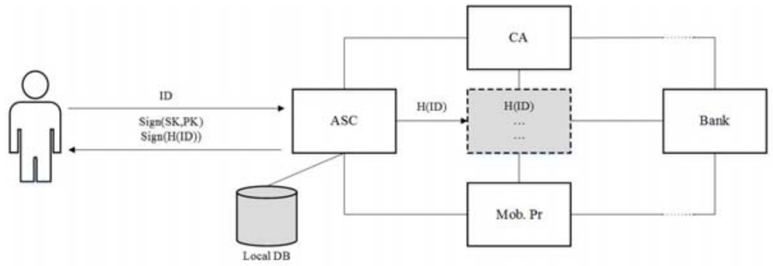

Fig. 3c. Identification procedure based on user's ID

Depersonalized Identity Format should be established in the following form:

$$H(ID),$$

where ID is the user ID in the following sequence: (series and passport number of the citizen); and H is a cryptographic hash function

The ID format must be the same for all identity providers. This condition makes it impossible for voters to re-register with different identity provider.

Stage Two (Generation of legitimate voters' wallets in a decentralized infrastructure for remote voting and results counting).

The process of generating a voter wallet (see Fig. 5) is initiated by the validator node of the upper blockchain network when it receives the public key from any of the identity providers in the form of a transaction. The voter wallet's initial balance is 0.

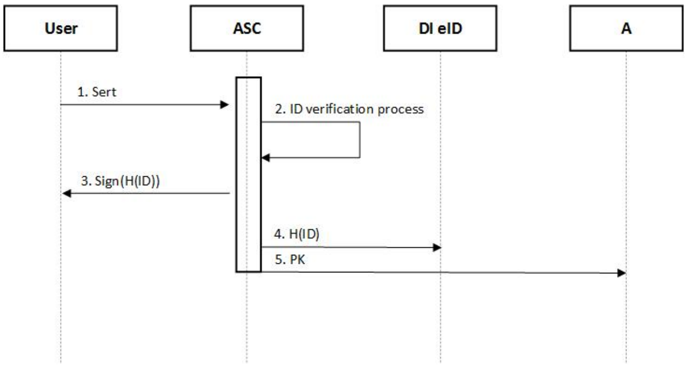

Fig. 4a. Identification process based on user's Certificate

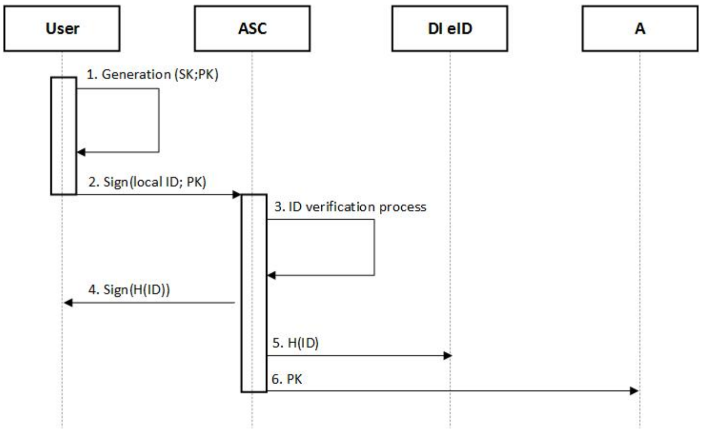

Fig. 4b. Identification process based on user's local ID

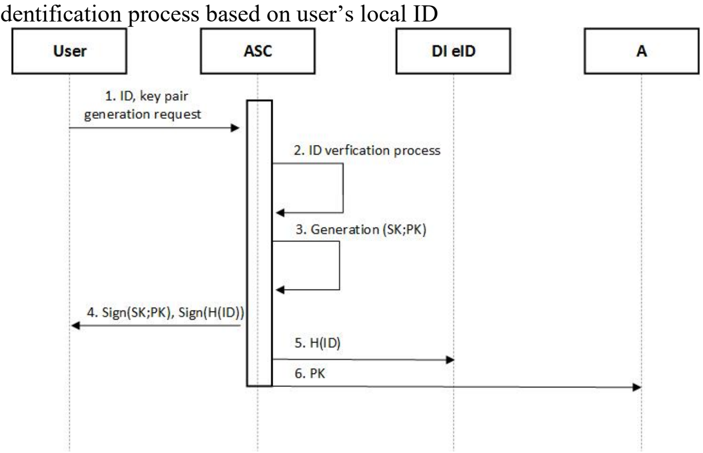

Fig. 4c. Identification process based on user's ID

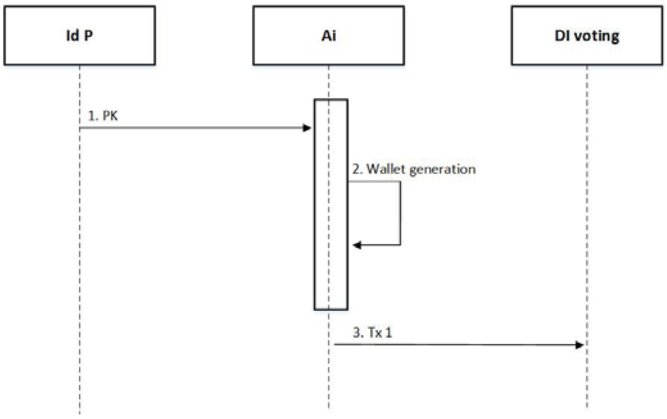

Fig. 3. User's wallet generation process

Stage Three (Candidates registration in a decentralized infrastructure for remote voting and results counting).

Candidates are registered in the top blockchain network. Hereinafter, the Agency will be understood to mean the totality of territorial polling stations combined into a separate private permissioned blockchain.

Responsibility for the candidates' registration rests on the Agency (upper blockchain validators) (see Fig. 6).

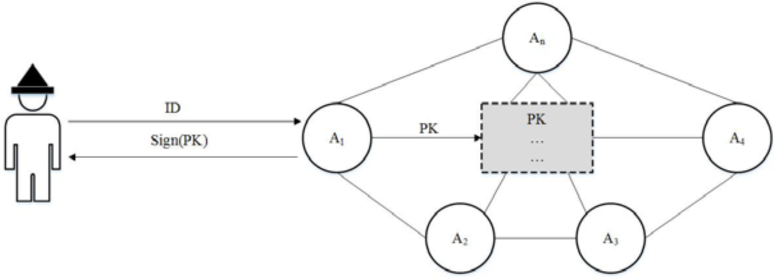

Fig. 4. Candidate registration procedure

Representatives of the Agency are responsible for conducting the initial identification of the candidates and initiate a transaction for the inclusion of the candidate which means the generation of the candidate wallet with zero starting balance (see Fig. 7).

Stage Four (Voters' authentication in decentralized infrastructure for remote voting and results counting).

A voter who has received confirmation from the identity provider for admission to the voting process and wishes to participate in the voting will contact one of the

Agency's nodes for the authentication procedure (see Fig. 8). The user can only authenticate with a private key (SK), provided that there is a corresponding public key (PK) in the Agency's blockchain network.

If the authentication process (see Fig. 9) was successful, the balance of the voter's wallet is increased by 1 token.

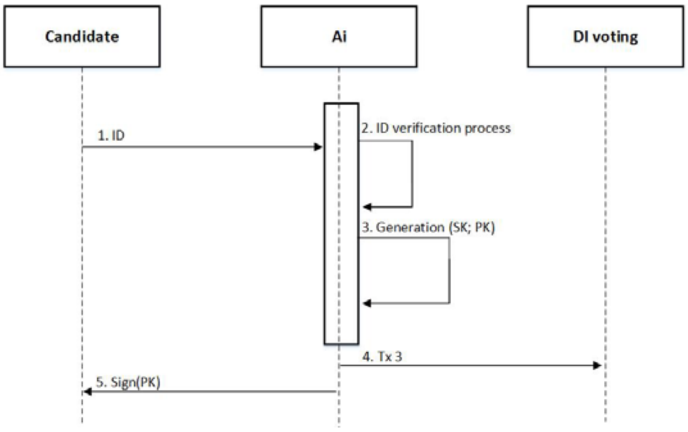

Fig. 5. Candidate wallet generation

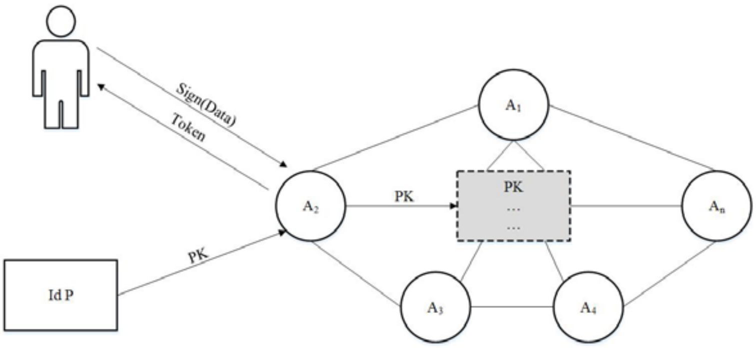

Fig. 6. User's authentication procedure

Stage Five (Voting in a decentralized infrastructure for voting and results counting).

Voters who have undergone an authentication procedure will make a choice by forwarding a token to one of the wallets which corresponds to the registered candidate by forming a corresponding transaction, which they sign with their own private key (see Fig. 10).

Stage Six (Counting of votes in a decentralized infrastructure for voting and results counting).

Vote counting is done automatically. The results will become available to everyone after the voting time has elapsed.

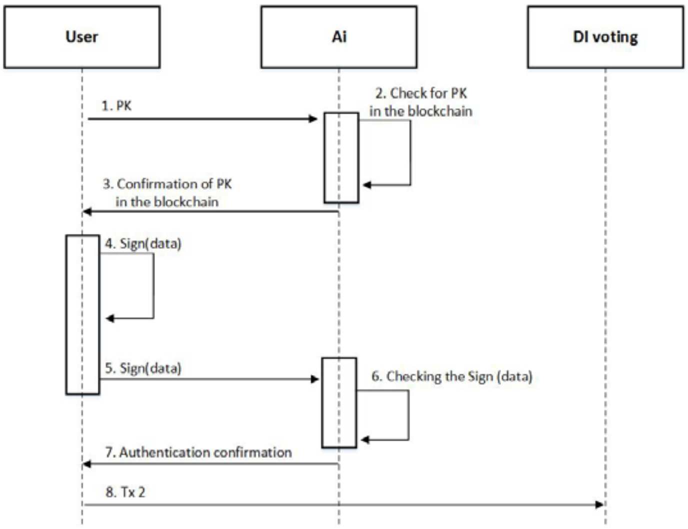
User
Ai
DI voting
1. PK
2. Check for PK in the blockchain
3. Confirmation of PK in the blockchain
4. Sign(data)
5. Sign(data)
6. Checking the Sign (data)
7. Authentication confirmation
8. Tx 2

Fig. 7. User's authentication process

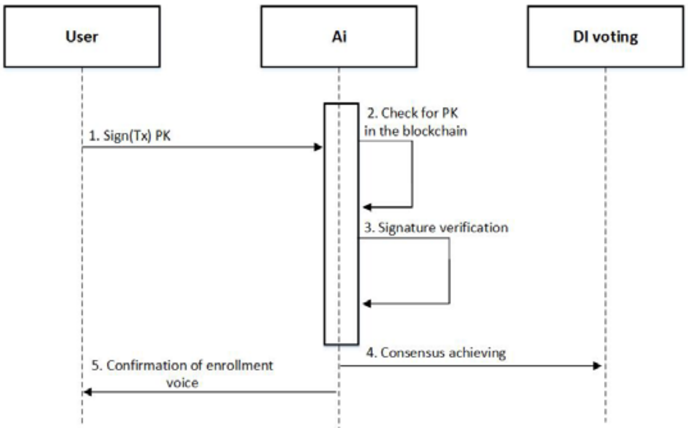
User
Ai
DI voting
1. Sign(Tx) PK
2. Check for PK in the blockchain
3. Signature verification
4. Consensus achieving
5. Confirmation of enrollment voice

Fig. 8. Voting process

4 Conclusions

In the face of cyber threats, the deployment of reliable electronic services systems becomes an important task. The analysis showed that blockchain technology can be useful for this purpose. Particularly, for developing electronic voting systems. Classical systems do not meet all desired requirements for voting systems (for example, a voter cannot check whether his voice is correctly taken into account and, if necessary, inform the authorized bodies about this).

In the paper, the new concept for developing a decentralized electronic voting system using blockchain technology is proposed. The two-level architecture provides a secure voting process without redundancy of existing (not based on blockchain) systems. The presented blockchain-based voting protocol has six steps that ensure all requirements that are put forward to such types of protocols including voting transparency and anonymity. Proposed blockchain-based approach has several advantages: central trust point absence, as a result there is no directed attack aim; reducing material costs for each stage of voting (since there is no need to print ballots, deliver them to polling stations).

Moreover, it should be noted that blockchain technology is more convenient for switching to post-quantum crypto primitives. Such an opportunity is also an important advantage in conditions of rapid evolution of quantum computers. It can also be used in other important applications [13-17].

References

1. Regulation (EU) No 910/2014 of the European Parliament and of the Council of 23 July 2014. https://www.eid.as/Regulation
2. E-voting world map. https://www.e-voting.cc/en/it-elections/world-map/
3. Menezes, A.J., van Oorschot, P.C., Vanstone, S.A.: Handbook of Applied Cryptography (2018). doi: 10.1201/9780429466335
4. Kuznetsov, O., Potii, O., Perepelitsyn, A., Ivanenko, D., Poluyanenko, N.: Lightweight Stream Ciphers for Green IT Engineering. In: Green IT Engineering: Social, Business and Industrial Applications. pp. 113–137. Springer International Publishing (2018). doi: 10.1007/978-3-030-00253-4_6
5. Gorbenko, Yu.I., Isirova, K.V.: Improved mechanism of one-time keys for post-quantum period based on the hashing functions. Telecommunications and Radio Engineering. Volume 77, Issue 14, 1277–1296 (2018)
6. Andrushkevych, A., Gorbenko, Y., Kuznetsov, O., Oliynykov, R., Rodinko, M.: A Prospective Lightweight Block Cipher for Green IT Engineering. In: Green IT Engineering: Social, Business and Industrial Applications. pp. 95–112. Springer International Publishing (2018). doi: 10.1007/978-3-030-00253-4_5
7. Gorbenko, I., Kuznetsov, A., Gorbenko, Y., Vdovenko, S., Tymchenko, V., Lutsenko, M.: Studies on Statistical Analysis and Performance Evaluation for Some Stream Ciphers. International Journal of Computing. 18(1), 82–88 (2019)
8. Bernstein, D.J., Buchmann, J., Dahmen, E. eds: Post-Quantum Cryptography. Springer Berlin Heidelberg (2009)
9. Pass, R., Seeman, L., Shelat, A.: Analysis of the blockchain protocol in asynchronous networks. Annual International Conference on the Theory and Applications of Cryptographic Techniques. 643-673 (2017)
10. Isirova, K., Potii, O.: Decentralized public key infrastructure development principles. In: 2018 IEEE 9th International Conference on Dependable Systems, Services and Technologies (DESSERT). IEEE (2018). doi:10.1109/dessert.2018.8409149
11. Kovalchuk, L., Kaidalov, D., Nastenko, A., Rodinko, M., Shevtsov, O., Oliynykov, R.: Decreasing Security Threshold Against Double Spend Attack in Networks with Slow Syn-

chronization. In: IEEE INFOCOM 2019 - IEEE Conference on Computer Communications Workshops (INFOCOM WKSHPS). IEEE (2019). doi: 10.1109/INFCOMW.2019.8845301

12. Nurmi, H., Salomaa, A.: Conducting secret ballot elections in computer networks: Problems and solutions. Annals of Operations Research. 51, 185–194 (1994). doi:10.1007/bf02032763
13. Bondarenko, S., Liliya, B., Oksana, K., & Inna, G.: Modelling instruments in risk management. International Journal of Civil Engineering and Technology. 10(1), 1561-1568 (2019)
14. Runovski, K., Schmeisser, H.: On the convergence of fourier means and interpolation means. Journal of Computational Analysis and Applications. 6(3), 211-227 (2004)
15. Tkach, B.P., Urmancheva, L.B.: Numerical-analytic method for finding solutions of systems with distributed parameters and integral condition. Nonlinear Oscillations. 12, 113–122 (2009). doi:10.1007/s11072-009-0064-6
16. Chornei, R.K., Daduna V.M., H., Knopov, P.S.: Controlled Markov Fields with Finite State Space on Graphs. Stochastic Models. 21, 847–874 (2005). doi:10.1080/15326340500294520
17. Kuznetsov, A., Shekhanin, K., Kolhatin, A., Kovalchuk, D., Babenko, V., Perevozova, I.: Performance of Hash Algorithms on GPUs for Use in Blockchain. In: 2019 IEEE International Conference on Advanced Trends in Information Theory (ATIT). IEEE (2019). doi: 10.1109/ATIT49449.2019.9030442