Towards the Blockchain Technology for System Voting Process

Michał Pawlak, Jakub Guziur, and Aneta Poniszewska-Marańda(✉)

Institute of Information Technology, Lodz University of Technology,
Lodz, Poland
{michal.pawlak,jakub.guziur}@edu.p.lodz.pl,
aneta.poniszewska-maranda@p.lodz.pl

Abstract. There are many existing voting solutions which have different benefits and issues. The most significant ones are lack of transparency and auditability. Recently developed blockchain technology may be a solution to these issues. This paper describes Auditable Blockchain Voting System (ABVS), which integrates e-voting process with blockchain technology into one supervised non-remote internet voting system which is end-to-end verifiable. In addition to the description of components and overall voting process, the paper contains presentation of the results of the initial tests conducted on the prototype of the system.

Keywords: E-voting · Blockchain · E-voting system
Audit · Verification

1 Introduction

An individual (or a group) under a pseudonym Nakamoto introduced a new digital currency in 2008 [1]. It was called Bitcoin and was based on blockchain technology. Since then both became considered by many to be revolutionary not only in the financial field [2]. In simple terms, blockchain technology is a distributed system of ledgers stored in a chain-like structure of connected blocks, which content is collectively negotiated and validated in a peer-to-peer network via dedicated algorithm [3,4]. Blockchain technology gained a lot of attention and its various possible applications are researched [2,5]. One such application lies in a field of electronic voting (e-voting).

The ability to vote is a foundation of a democracy. However, despite its importance and complex security measures, it is not free from frauds and manipulations [6,7]. In general, most modern voting systems are slow and prone to manipulations. This is the result of their dependence on ballots collected and counted by a single central institution. Furthermore, results obtained this way are not verifiable because voters do not have the ability to ensure that their votes were correctly and fairly handled.

E-voting systems were created to solve all of these problems [8]. Unfortunately, the systems used today are still not ideal and have many different

A. Castiglione et al. (Eds.): CSS 2018, LNCS 11161, pp. 209–223, 2018.
https://doi.org/10.1007/978-3-030-01689-0_17

issues with authentication, privacy, data integrity and transparency [6]. However, blockchain technology may be a solution to e-voting problems. Blockchain can be used for a creation of platforms allowing for public verification of the data stored inside, which in turn would allow the voters to audit and verify the results without dedicated institutions and officials. Some countries already started researching and implementing e-voting systems based on blockchain technology [9,10]. In 2017 South Korea conducted a successful community voting and in 2018 Sierra Leone conducted a nationwide election using Agora blockchain system [11].

The existing electronic voting systems based on blockchain technology have many advantages. The most important one is the ability to securely and anonymously cast vote via the Internet, which can be verified. However, these systems still have issues with identification and authentication. In fact, most of them leave this process to the election officials or depend only on cryptography, which removes the benefits of remote voting and creates a possibility of voter impersonation.

The goal of this paper is to describe an end-to-end verifiable blockchain-based electronic voting system, which is intended as an enhancement of the existing voting process in Poland. The system is intended to provide the voters with the ability to follow and verify votes and election results.

The paper is organised in the following way: Sect. 2 describes the theoretical and technical aspects of blockchain technology and e-voting, Sect. 3 presents an overview of works related to this field. Section 4 deals with the original e-voting systems and results of its testing, while Sect. 5 contains the conclusion drawn from this stage of the research.

2 Background

In this section theoretical background of blockchain technology and electronic voting is described in detail. Each of these topics is presented in a dedicated subsection.

2.1 E-voting

Electronic voting, also known as e-voting, is defined as any type of election or referendum that utilizes electronic means facilitating voting procedures (at minimum for casting votes) [21]. E-voting systems provide many benefits, for example, due to reduction of human factor in tallying process they can increase results accuracy and minimize potential of frauds. Furthermore, they can improve voting accessibility with multilingual interfaces or with dedicated interfaces for disabled people. Finally, e-voting can reduce time and costs of the voting procedure due to reduction of spoiled ballots and removal of distribution and shipment of ballots [18].

On the other hand, electronic voting is connected with many significant challenges. One of the most important ones is lack of trust in such systems. This is the result of inadequate transparency and poor understanding of e-voting solutions by non-experts. Despite reduction of human factor, electronic voting is not free from frauds as privileged insiders or hackers may be able to manipulate votes. This is a severe flaw as e-voting systems are centralized, which means a single entity controls a code base, databases and voting equipment. Furthermore, devices used for the voting process mostly come from third parties and full verification of them all is impossible. Another important problem of e-voting is lack of widely accepted standards and certifications, which can further decrease trust which is crucial for democratic voting [18,33].

Similarly to traditional voting systems, electronic voting consists of six phases: (i) voter registration, done personally or by an authority; (ii) authentication, that is confirming voter identity; (iii) authorization, that is allowing identified voters to vote; (iv) vote casting; (v) vote counting; (vi) vote verification, which is checking if the vote was conducted correctly and without frauds. In addition, all electronic voting solutions must have the following properties [6,19,22,23]:

- voter authentication and authorization,
- voter privacy,
- correctness,
- transparency,
- verifiability,
- integrity,
- availability,
- fairness.

Voter authentication and authorization property means that only eligible people are allowed to cast votes. *Voter privacy* property ensures that only voters themselves know the value of their votes. *Correctness* means that all valid votes are included in the final tally. *Transparency* property means that the procedures of the voting system are open to scrutiny and are understandable for non-experts. *Verifiability* property ensures that the system can be inspected by an independent entity to check whether the voting was conducted correctly. *Integrity* property refers to immutability of any cast votes. *Availability* property means that all eligible voters can cast their votes in the election time-frame. Finally, *fairness* property ensures that participants have equal chances and have no advantage from the system itself.

Electronic voting systems can be classified in many different ways. In the most general way they can be differentiated by two key characteristics [24]:

- remoteness,
- supervision.

Remoteness refers to whether the ballots are transmitted through some communication channel to some central location (remote voting) or are just recorded locally on some medium (non-remote voting). *Supervision* describes if the voting process is conducted from a location controlled by some authority (e.g. polling station) or is conducted remotely from a location outside any control.

Furthermore, electronic voting solution can be divided into four types depending on the usage of information and communication technologies (ICT). The first type is *voting by dedicated voting machines*, which uses electronic devices for recording, storing or transmitting user votes. Sometimes, they are accompanied by voter-verified audit paper trail, which are printed copies of the recorded votes. They provide fast data collection, fast vote counting and prevent ballot spoiling. However, they are expensive to deploy and maintain. Furthermore, they are vulnerable to manipulation as it is impossible to inspect every single device [18,24,25].

The second type is *voting with optical scanning machines*, which record votes by scanning machine-readable paper ballots. They are easy to implement because they do not change the voting process from the point of view of the voters. Like most electronic voting solutions they provide fast and accurate results. On the other hand, they depend on paper ballots and suffer from the same lack of auditability as the previously described dedicated voting machines [18,24,25].

The third type consists of *voting with electronic ballot printers*, which are similar to dedicated voting machine but they produce machine-readable ballot or token which is used in another device to record votes instead of recording them on the machine itself. They leave a physical trail in a form of a printed ballot which can be verified before being cast. However, this solution is expensive due to a need of maintaining separate devices for printing and counting [18,24,25].

The fourth type is *voting by the Internet*, in which votes are cast on devices connected to the Internet and then transmitted to the central counting server. This type of voting provides fast and accurate results. It allows remote and non-supervised voting which seems to be currently the most desirable method of voting. Unfortunately, it also has the most security concerns, for example, hacker attacks, potential lack of anonymity and privacy, "creation" of votes, third parties influencing voters [18,24,25].

Finally, electronic voting systems can be classified depending on cryptographic primitives and schemes they are utilizing. The most common cryptographic primitives used in electronic voting are: (i) *zero knowledge proofs*, which allow one party to prove to the other that it knows some value without revealing any additional information; (ii) *secret sharing*, in which a secret information is shared among a group in such a way that each participant obtains only a part of the whole information; (iii) *homorfic encryption*, which allows to perform operations on encrypted data and obtain valid results; (iv) *blind signatures* that allow authorities to sign an encrypted data without decrypting it; (v) *mix-net* which create difficult to trace communications by sending messages through a network of authorities which shuffle received messages before sending them forward [19,23].

As can be seen, there are many different ways to analyse electronic voting systems. Each type has its own advantages and disadvantages, which cannot be overlooked. Some are connected to the whole concept of e-voting, while others come directly from the specific implementation.

2.2 Blockchain Technology

Blockchain technology is composed of two elements [3,34]:

- blockchain data structure,
- blockchain system or network.

Blockchain data structure is an ordered list of connected data units called blocks. Each block is composed of block header and transaction data. The block header contains block metadata, which contains information about block itself, for example, index and creation timestamp. Most important field in the header is hash representation of the previous block. This value is generated from the contents of the previous block and is used to connect block to each other. The transaction data contains a list of transaction and their respective data. Figure 1 presents a model of the blockchain data structure. The two main components of each block are represented by rectangle with thicker lines, standard rectangles represent component subelements and arrows illustrate connections between blocks.

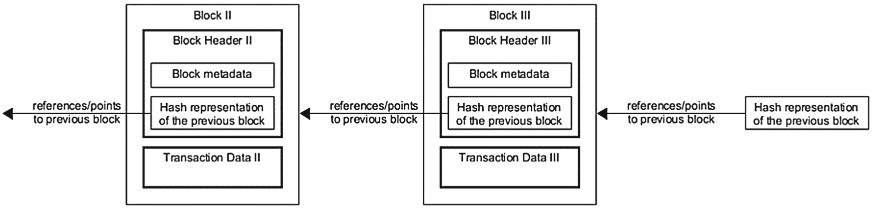
Block II
Block Header II
Block metadata
Hash representation of the previous block
Transaction Data II
references/points to previous block
Block III
Block Header III
Block metadata
Hash representation of the previous block
Transaction Data III
references/points to previous block
references/points to previous block
Hash representation of the previous block

Fig. 1. Model of a blockchain, adapted from [3]

The hash representations are result of application of one of cryptographic one-way hash functions to the contents of each block. It maps data of arbitrary size to a unique bit string of a fixed size called hash value (or reference). Due to the properties of these functions, the value is easy to calculate but difficult to invert from the point of view of computational theory. Another important property of the cryptographic hash functions is sensitivity to change of input data. Even a small modification of the input will result in a different hash value [12]. This ensures immutability of the ordered list of blocks because a change of a single block would force modification of all subsequent blocks. Furthermore, due to hash value uniqueness, each block can be identified and tracked allowing verification of their correctness. There exist many cryptographic hash functions used in various blockchain implementations, the most popular include SHA256, RIPEMD160, Merkle trees and the Elliptic Curve Digital Signature Algorithm [13,15].

On the other hand, *blockchain system* is a distributed peer-to-peer network of connected nodes which store and negotiate the information content of the blockchain. Each node validates incoming transactions and, if they are valid, propagates them to other nodes which continue this process until all nodes of the system are aware of the new transactions. Nodes maintain their own copies of the blockchain and add new blocks to it in a process called *mining*, in which transactions are validated and aggregated into blocks and appended to the chain. Each new block is broadcasted to the other nodes so they can modify their copies of the blockchain. In order to maintain consistency the system attempts to reach a consensus about which blocks must be added. This is done via *consensus algorithms*, which there are many types. The most common are [14,15,34]:

- proof-of-work,
- proof-of-stake,
- delegated-proof-of-stake,
- practical-byzantine-fault-tolerance.

In *proof-of-work* nodes compete in solving mathematical problem, which is computationally expensive. The node which first solves the puzzle is allowed to append a new block to the blockchain and gets a reward. The new block is validated by the other nodes and appended to their chains. The algorithm assumes that the longest chain is the most authoritative due to the amount of total work. *Proof-of-stake* is based on ownership of a digital currency. It assumes that the owner of large amount of currency would not have incentive to tamper with the network. Various methods of authoritative node are proposed to prevent centralisation, for example, random selection or age and size of a coin set. *Delegate-proof-of-stake* is based on proof-of-stake but the nodes responsible for block validation are selected by other nodes. Finally, in *practical-byzantine-fault-tolerance* new blocks are selected in three phase round. In order to advance between phases, nodes must obtain votes of more than 2/3 of all nodes.

In order to provide authentication and authorization, the blockchain systems use asymmetric cryptography. This approach utilizes public and private keys, which can be used to encrypt and decrypt messages. It is important to note that a messages encrypted with one key can only be decrypted with the other (Fig. 2).

Public-to-private is a method of encryption, in which messages are encrypted with the available to everyone public key and then decrypted with the private key. This is similar to a mailbox which can receive mail from anyone but only the owner can open it. In blockchain systems accounts are identified by addresses, which are also cryptographic public keys. This allows the transactions to be encrypted, so only the receiver can decrypt them. Private-to-public is a method, in which messages are encrypted with the private key and are decrypted with the public key. This is a method of proving ownership as only the owner of the private key could create a message, which can be decrypted with the corresponding public key. Blockchain systems use this method for transaction authorization [3,4].

Blockchain technology is constantly developed and there exist many different implementations and applications. In general, blockchain-based systems can be divided by two characteristics [3]:

1. read rights,
2. write rights.

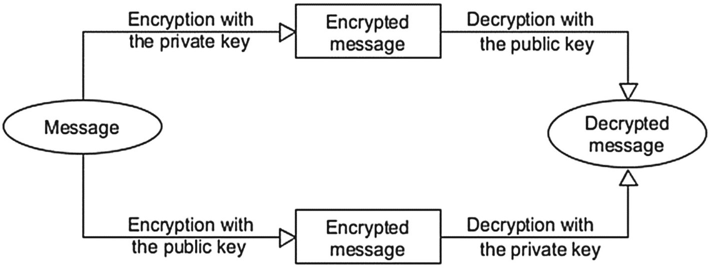
Encryption with the private key
Encrypted message
Decryption with the public key
Message
Decrypted message
Encryption with the public key
Encrypted message
Decryption with the private key

Fig. 2. Illustration of asymmetric cryptography, adapted from [3]

Read rights divide the blockchain-based systems into two classes: (i) *public* where users and nodes all have access to the contents of the blockchain and transactions; (ii) *private* where rights to access the blockchain is restricted to only a selected group. On the other hand, write rights groups blockchain-base systems into: (i) *permissionless* which allow every user and node to participate in the consensus algorithm; (ii) *permissioned* in which only a selected group of users and nodes can verify transactions and add new blocks to the chain.

As mentioned previously, many implementations of the technology exist. The best-known is Bitcoin virtual currency, from which the technology originates. It is fully distributed, public and permissionless system using proof-of-work algorithm. Second popular system is Ethereum Platform created by Ethereum Foundation [16]. It is blockchain platform which uses both proof-of-work and smart contracts. It provides a platform for creation of blockchain-based applications. Lastly, Multichain platform allows creation of private blockchain systems utilizing consensus protocol similar to practical-byzantine-fault-tolerance algorithm [17].

From the point of view of electronic voting, blockchain technology provides many potential benefits. It is censorship-proof because it is distributed among a peer-to-peer network of nodes without central authority. It is very secure on transaction and system level. Finally, because each node not only stores the blockchain but supervises transactions anyone with access to node can view the blockchain data. This can potentially provide a solution to problems with transparency from which most of the e-voting systems suffer.

3 Related Works

There are numerous publications concerning electronic voting. The authors of [23] provide a thorough overview of electronic voting schemas. The paper starts with a review of security properties of e-voting systems and the most used cryptographic primitives used in a construction of the schemes. Finally, the paper describes sixteen electronic voting schemes and their comparison.

Similarly, in [22] the authors describe the current state of electronic voting. The work presents various methods of attacking e-voting systems and different design schemas divided with respect to utilized cryptographic primitives. The authors also present chosen existing e-voting systems and discuss still open problems form which electronic voting suffer.

As discussed previously, there are no official and widely accepted standards for electronic voting systems. However, a few documents, which support development and implementation of e-voting solutions, were released by various organisations. The Council of Europe created two documents. [31] describes recommendations for conducting elections with electronic means in a form of a checklist. [32] is an explanation for the previous document and contains detailed technical recommendations. Finally, [21] was developed as a mean of providing assistance and guidelines for introducing e-voting.

Another standard was developed by The International Institute for Democracy and Electoral Assistance (International IDEA). This intergovernmental organisation created [18], which contains guidelines, recommendations and considerations for implementing electronic voting systems.

Despite being relatively new technology, there is ongoing research of blockchain application in various fields. In [9] the authors present research on possible applications of the technology in e-governance conducted by the Digital5 (D5) countries. This includes research of its usage in electronic voting. The two most active countries in this field are Estonia and South Korea. The latter was able to conduct a successful community vote using blockchain technology in 2017.

In [20] the authors present system SAVE, which is a supervised e-voting system for medium and large scale voting, for instance, elections on university. The paper describes all components and processes of the system. SAVE utilizes commonly available personal computers and smartphones as voting machines for supervised voting. Furthermore, the system uses symmetric encryption for signing its software components, asymmetric encryption (RSA with 2048 bit key length) for data encryption and HMAC-SHA256 for message authentication. Finally, it is worth noting that SAVE utilizes VVPATs generated by printers for vote verification.

It is important to mention the most successful electronic voting system. Estonian i-voting was introduced in 2005 and it is being in constant use since [29]. It provides a remote unsupervised internet voting based on "envelope scheme" [30]. Before casting votes, the voters are required to authenticate with ID-cards or mobile phones with special SIM cards containing an encrypted ID of the owner. Multiple votes can be cast but only the most recent one is considered. The votes can be verified by the common voters using a dedicated application. Furthermore, the system is being constantly upgraded and improved.

There exist some working blockchain-based e-voting solutions. The main example is Agora [26], which is customizable multi-layer system. It allows supervised and unsupervised internet voting with a hybrid of permissionless and permissioned public blockchain. The system was successfully implemented in elections in Sierra Leone in 2018 [11]. It is worth noting that Agora leaves authentication and authorization to the election officials. However, it also offers a system based on digital signatures for facilitating this process.

Another solution is Ethereum-based FollowMyVote [28] voting platform. It is designed for remote and unsupervised internet voting. The system uses elliptic curve cryptography for security and webcams for identification and authorization by ID scanning. FollowMyVote provides the users with an ability to supervise the election process in real time and to switch their votes during the election.

In [27] an end-to-end verifiable, Bitcoin-based system is presented. The solution conducts authentication and transactions using a protocol called Anonymus Kerberos. The system represents votes as "tokens", which are the smallest transferable amount of bitcoins (including fees). The system assumes that the voters must register with election officials before they can participate in the voting process. The authors note that the system fulfils most of the e-voting requirements with the exception of voter's privacy, which can be violated dude to possibility of linking the voters to their transactions.

4 Auditable Blockchain Voting System

In this section Auditable Blockchain Voting System (ABVS) is presented. It is designed as a non-remote and supervised voting system that uses blockchain system to store and verify the voting procedure. ABVS is intended to enhance the existing critical voting processes in Poland. The system is in a development stage, in which prototypes are developed and tested. In the following subsections ABVS components, process overview and result of initial testing are presented.

4.1 Auditable Blockchain Voting System Components

Auditable Blockchain Voting System is a public and permissioned blockchain-based electronic voting system. It is made of six components:

1. client applications (polling stations),
2. system of trusted nodes,
3. Vote Identification Tokens,
4. voter-verified paper audit trail (VVPAT),
5. vote error notification module,
6. counting application.

Figure 3 illustrates relations between the components of ABVS. Ovals represent components and relations are shown as labelled arrows.

Client applications are lightweight programs installed on computers located at polling stations used for casting votes in a form of blockchain transactions. Each transaction contains information about transaction creation, voter's choice (vote value), vote identification token and polling station identifier. The transactions are broadcasted to the nodes in accordance with the blockchain technology

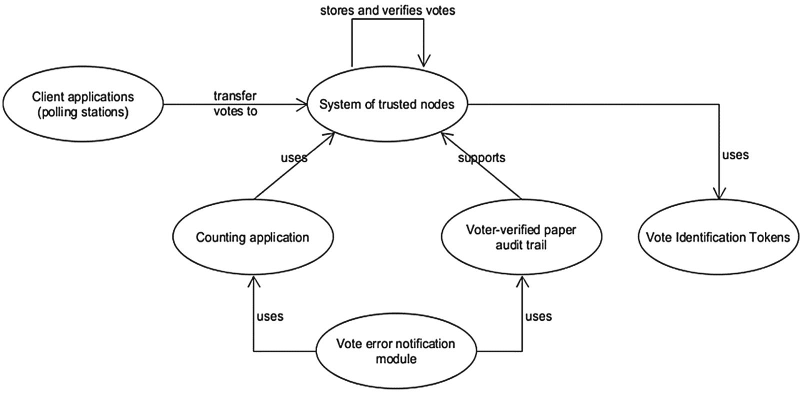
stores and verifies votes
Client applications (polling stations)
transfer votes to
System of trusted nodes
uses
supports
uses
Counting application
Voter-verified paper audit trail
Vote Identification Tokens
uses
uses
Vote error notification module

Fig. 3. Model of relations between Auditable Blockchain Voting System components

paradigm. For security purposes, each application should be signed during election preparation in order to prevent unauthorized participation.

System of trusted nodes is a set of blockchain nodes which store the chain containing blocks with votes and mine new ones. One node, called super-node, represents central national electoral authorities (National Electoral Commission in case of Poland). It is responsible for creation of the initial block (*genesis block*) aggregating all information about the voting in its transaction. The block is then broadcasted to other trusted blockchain nodes, which are pre-selected and verified public institutions (e.g. universities). Figure 4 illustrates interactions between the nodes and the client applications.

Vote Identification Tokens (VITs) are alphanumerical codes used for authentication and authorization of the voters. Furthermore, they allow vote following and vote identification during and after the election. They may be contained on paper sheets hidden in envelopes or any other medium which can be randomly selected by voters without showing their contents in advance. VITs must be generated and distributed during the election preparation stage. Each node stores a list of VIT-polling station pairs for vote verification.

Voter-verified paper audit trails (VVPATs) are paper representations of votes. Each VVPAT contains the same vote information as ABVS transaction. They are printed by standard printers after voters cast their votes and are disposed into traditional ballot boxes. This is implemented to provide additional audit and verification capabilities.

Vote error notification module is a service for reporting inconsistencies in the recorded votes. In order to send notification to the service, the voters have to provide a valid VIT and error explanation. The inconsistencies are resolved by comparison of the given block with the corresponding VVPAT.

Counting application is a certified and signed program for iterating over blockchains and producing results of the voting. Each node is equipped with its own instance of the application in order to created multiple comparable results for verification purposes.

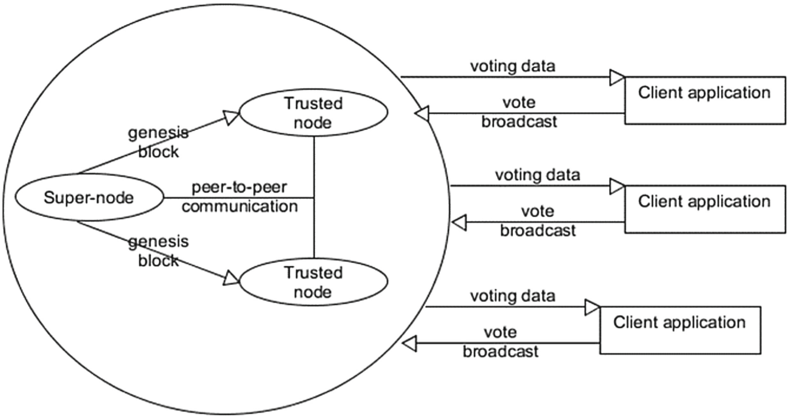

Fig. 4. Schema of the Auditable Blockchain Voting System network

4.2 Auditable Blockchain Voting System Process Overview

The voting in ABVS is organized in a three phases: (i) election preparation or setup; (ii) voting; (iii) counting and verification. In the setup stage software and hardware components are signed and certified. The election officials select institutions which will function as nodes of the blockchain system. Finally, vote identification tokens are generated and distributed.

In the voting phase, the voters identify themselves at their polling stations and randomly select voter identification tokens. They cast their votes using VITs and the client applications. Moreover, they receive VVPATs which are disposed into ballot boxes for verification in the final stage. The trusted-nodes mine blocks containing votes and reach consensus. It is important to note that at this stage, the blockchain remains private.

In the final stage, the system is deactivated and the counting applications determine the result of the voting. Lists of remaining VITs are made public in order to allow verification of the number of votes in the chain. Furthermore, when the nodes reach the final consensus the blockchain is made public, so each voter can check his vote and report inconsistencies through the dedicated application.

4.3 Auditable Blockchain Voting System Initial Testing

The initial tests of ABVS were focused on two main elements:

- the blockchain validation time,
- RAM space required by the blockchain.

The main goal of these tests was to determine a reference point for the equipment needed for a real voting. The tests were conducted one a machine with the following specification:

1. Processor: Intel(R) Core(TM) i5-7300 CPU @ 2.60 GHz 2.70 GHz.
2. RAM: 32.0 GB (31.8 GB usable).
3. System type: 64-bit operating system, x64-based processor.

The tested ABVS was implemented in Python programming language version 3.6. The tests were run for chains of length 20,000, 40,000, 80,000, 160,000, 320,000, 640,000 and 1,280,000 blocks. Chains longer than 1,280,000 blocks were causing memory error on the tested machine, which limited tested lengths at this stage. The values presented in the following diagrams are averages obtained form 40 separate testing cycles.

Figure 5 presents a diagram of blockchain validation time with respect to the blockchain length. This value informs how much time would take to obtain voting results from a single ABVS node. Not surprisingly it is a relatively quick process. For the shortest chain the validation took 2.46 s and for the longest one 158.51 s.

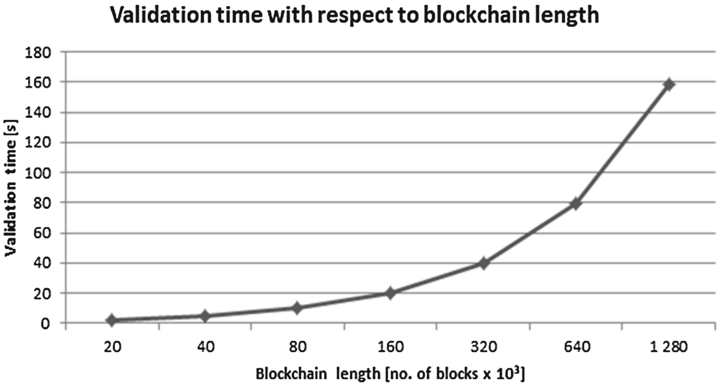

Fig. 5. Validation times with respect to blockchain length

Figure 6 presents a diagram of blockchain size in RAM with respect to blockchain length. The shortest chain takes 6.5 MB of RAM memory and the longest takes 415.1 MB of RAM memory. As mentioned above longer chains

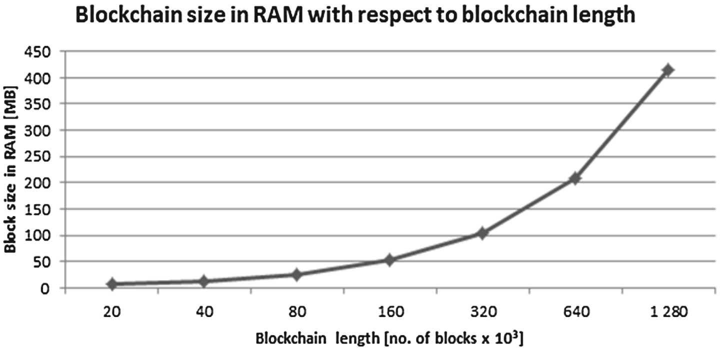

Fig. 6. RAM size of the blockchain with respect to its length

caused memory errors, which prevented testing of longer chains at this stage. This may be a result of limits forced by operating system on operational memory for a single process or optimisation problem. These issues must be solved before the next stage of the testing.

5 Conclusions

There are many existing voting solutions, which have different benefits and issues. However, they share a few common problems, for example, lack of transparency and verifiability, or lack of commonly accepted standards. Recently developed blockchain technology may be a solution to the problems of auditability of e-voting systems. Integration of blockchain and electronic voting may provide the voters with a system, in which they can follow their vote and supervise the calculation of the results. Due to this, election frauds would become much more difficult.

Auditable Blockchain Voting System is a non-remote supervised internet voting system, which utilizes blockchain technology. It is intended as an end-to-end verifiable electronic voting system, allowing the common voters to follow their votes and verify the final results. To achieve this, ABVS utilizes voter-verified paper audit trails to provide point of reference for blockchain verification and Vote Identification Tokens allowing the voters to identify their votes without providing any personal information. It is important to note that the goal of the system is to improve and enhance the existing voting process in Poland.

In this paper, ABVS components and its overall voting process are described. Furthermore, the results of the initial testing are presented. The conducted tests showcased that the equipment used for testing is inadequate for the task of handling long blockchains or there exists some optimization issues of the ABVS prototype.

References

1. Satoshi, N.: Bitcoin: a peer-to-peer electronic cash system (2008). https://bitcoin.org/bitcoin.pdf. Accessed 2018
2. Zhao, J.L., Fan, S., Yan, J.: Overview Of Business Innovations and Research Opportunities in Blockchain and Introduction to the Special Issue Financial Innovation, pp. 2–28. Springer, Heidelberg (2016). https://doi.org/10.1186/s40854-016-0049-2
3. Drescher, D.: Blockchain Basics: A Non-technical Introduction in 25 Steps, 1st edn. Apress, Frankfurt am Main (2017). https://doi.org/10.1007/s11408-018-0315-6
4. Karame, G., Audroulaki, E.: Bitcoin and Blockchain Security. Artech House Inc., Norwood (2016). https://doi.org/10.1007/s11408-018-0315-6
5. Risius, M., Spohrer, K.: A blockchain research framework - what we (don't) know, where we go from here, and how we will get there. Bus. Inf. Syst. Eng. **59**(6), 385–409 (2017)
6. De Faveri, C., Moreira, A., Arajo, J.: Towards security modeling of e-voting systems, In: Proceedings of IEEE 24th International Requirements Engineering Conference Workshops (REW), Beijing (2016)

7. Lehoucq, F.: Electoral fraud: causes, types, and consequences. Ann. Rev. Polit. Sci. **6**(1), 233–256 (2003)
8. Willemson, J.: Bits or paper: which should get to carry your vote? J. Inf. Secur. Appl. **38**, 124–131 (2018)
9. Ojo, A., Adebayo, S.: Blockchain as a next generation Government 3.0 - information infrastructure: a review of initiatives in D5 countries. In: Ojo, A., Millard, J. (eds.) Government Next Generation Government Technology Infrastructure and Services Public Administration and Information Technology, vol. 32, pp. 283–298. Springer, Cham (2017)
10. Enterprise Estonia, Factsheet on Estonian blockchain technology (in English) (2012). https://e-estonia.com/wp-content/uploads/facts-a4-v03-blockchain.pdf. Accessed 8 Feb 2018
11. Akwei, I.: Sierra Leone is first country in the world to use blockchain technology to vote, March 2018. https://face2faceafrica.com/article/sierra-leone-first-country-world-use-blockchain-technology-vote. Accessed 22 Apr 2018
12. Stallings, W.: Cryptographic Hash Functions. In: Cryptography and Network Security: Principles and Practice, (6th edn.), pp. 313–354. Pearson Education Inc. (2013)
13. Morabito, V.: The Security of Blockchain Systems, pp. 61–78. Business Innovation Through Blockchain, Springer, Cham (2017)
14. Zheng, Z., Xie, S., Dai, H., Chen, X., Wang, H.: An overview of blockchain technology: architecture, consensus, and future trends. In: Proceedings of IEEE International Congress on Big Data (BigData Congress), Honolulu (2017)
15. Mingxiao, D., Xiaofeng, M., Zhe, Z., Qijun, C.: A review on consensus algorithm of Blockchain. In: Proceedings of IEEE International Conference on Systems, Man, and Cybernetics (SMC), Banff (2017)
16. Ethereum Foundation: "Ethereum Project", Ethereum Foundation, August 2014. https://www.ethereum.org/. Accessed 20 Apr 2018
17. Coin Sciences: MultiChain, Coin Sciences (2015). https://www.multichain.com/. Accessed 20 Apr 2018
18. Wolf, P., Nackerdien, R., Tuccinardi, D.: Introducing electronic voting: essential considerations. International Institute for Democracy and Electoral Assistance, 1 December 2011. https://www.idea.int/publications/catalogue/introducing-electronic-voting-essential-considerations. Accessed 22 Jan 2018
19. Zhou, Y., Zhou, Y., Chen, S., Wu, S.S.: MVP: an efficient anonymous E-voting protocol. In: Proceedings of Global Communications Conference (GLOBECOM), Washington (2016)
20. Ochoa, X., Pelez, E.: Affordable and secure electronic voting for university elections: the SAVE case study. In: Proceedings of 4th International Conference on eDemocracy & eGovernment (ICEDEG), Quito, Ecuador (2017)
21. Caarls, S.: E-voting handbook: key steps in the implementation of e-enabled elections. Council of Europe, November 2010. https://www.coe.int/t/dgap/goodgovernance/Activities/E-voting. Accessed Jan 2018
22. Schneider, A., Meter, C., Hagemeister, P.: Survey on remote electronic voting. arXiv preprint arXiv:1702.02798 (2017)
23. Fouard, L., Duclos, M., Lafourcade, P.: Survey on Electronic Voting Schemes. project AVOT, University of Grenoble (2017)
24. National Democratic Institute: Common Electronic Voting and Counting Technologies. https://www.ndi.org/e-voting-guide/common-electronic-voting-and-counting-technologies. Accessed 22 Jan 2018

25. United Nations Development Programm: Feasibility study on Internet Voting for the Central Electoral Commission of the Republic of Moldova: Report and preliminary roadmap. Central Electoral Commission of the Republic of Moldova, Chisinau (2016)
26. Agora Technologies: Agora_Whitepaper_v0.2.pd (2015). https://agora.vote/Agora_Whitepaper_v0.2.pdf. Accessed 20 Apr 2018
27. Bistarelli, S., Mantilacci, M., Santancini, P., Santini, F.: An end-to-end voting-system based on BITCOIN. In: Proceedings of Symposium on Applied Computing, SAC2017, New York (2017)
28. Follow My Vote: The online voting platform of the future. https://followmyvote.com. Accessed 26 Jan 2018
29. State Electoral Office of Estonia: General framework of electronic voting and implementation thereof at national elections in Estonia, 20 June 2017. https://www.valimised.ee/sites/default/files/uploads/eng/IVXV-UK-1.0-eng.pdf
30. Heiberg, S., Willemson, J.: Verifiable internet voting in Estonia. In: Proceedings of 6th International Conference on Electronic Voting: Verifying the Vote (EVOTE), Lochau (2014)
31. Council of Europe – Committee of Ministers: Recommendation CM/Rec(2017) 51 of the committee of ministers to member states on standards for E-voting, 14 June 2017. https://search.coe.int/cm/Pages/result_details.aspx?ObjectID=0900001680726f6f. Accessed 26 Jan 2018
32. Ad hoc Committee of Experts on Legal, Operational and Technical Standards for e-voting (CAHVE): Explanatory memorandum to recommendation CM/Rec(2017) 5 of the committee of ministers to member states on standards for E-voting, 14 June 2017. https://search.coe.int/cm/Pages/result_details.aspx?ObjectID=090000168071bc84
33. Noizat, P.: Blockchain Electronic Vote. In: Handbook of Digital Currency, Elsevier Inc., pp. 453–460 (2015)
34. Xu, X., et al.: A taxonomy of blockchain-based systems for architecture design. In: Proceedings of IEEE International Conference on Software Architecture (ICSA), Gothenburg (2017)