Ring Signature-Based Voting on Blockchain

Alexandra Kugusheva
National Research University, Higher School of Economics,
125319, Moscow, Russia
+7-495-771-3232
akugusheva@hse.ru

Yury Yanovich
Skolkovo Institute of Science and Technology
121205, Moscow, Russia
+7-495-280-1481
Bitfury
123100, Moscow, Russia,
+7-495-477-4477
yury.yanovich@bitfury.com

Abstract—Amid ongoing digitalization, the use case of electronic voting has naturally arisen, with attempts beginning as early as 2000. Blockchain technology has the potential to bring trust and built-in auditing tools to such systems. This paper presents a prototype of the system for collective voting.

It is based on blockchain and linkable ring signatures to ensure the transfer of closed (secret) data without the loss of reliability and with respect for the privacy of group members.

Keywords—electronic voting; blockchain; ring signature.

I. INTRODUCTION

Blockchain technology has experienced at least three powerful spikes of interest over the course of its 10-year history: appearance of cryptocurrencies [1], smart contracts with arbitrary machine logic [2], and initial coin offerings (ICOs) [3]. We are witnessing a fourth surge caused by the growth of private blockchains [4], [5], [6]. Since 2016, private blockchains have been applied in many projects at the state and global enterprise levels [7], [8]. While the most media projects like Libra [9] and TON [10] face regulation problems because of build-in token logic [11], classic private or consortium blockchain frameworks like Hyperledger Fabric [12] and Exonum [13] provided blockchain-based transparency and auditability for the projects in many countries.

There are several successful cases of decentralized solutions in election systems. Media detailed the process of blockchain-based voting for the midterm federal elections in West Virginia [14] and municipal elections in Denver (USA) [15] using Voatz in 2018, and Republican presidential nominee in Utah using Smartmatic-Cybernetica in 2016.

The largest proof-of-concept political blockchain-based voting was in Sierra Leone, Africa [16]. In 2018, the Swiss company Agora, a developer of blockchain-based voting systems, in cooperation with the country's election commission, used blockchain for 280 of roughly 11,200 polling stations to timestamt the results of the voting [17]. Scientists have also proposed a number of blockchain-based solutions for electronic voting [18], [19], [20]. These solutions opine that blockchain is well-suited to electoral systems, although it is not widely used in this area at the moment.

The analysis of the practice of using the technology for voting allows us to formulate three conclusions in the following areas:

- Specially developed solutions for a particular country/company and White label models are both used in practice;
- Usage of open and private solutions are the basis of the electoral platform. While at the early stage, in the period 2009–2016, open solutions dominated, in recent years private blockchain protocols have been mostly implemented in practice;
- Usage of decentralized solutions for political elections is currently applied as a fragment of a mixed system.

The analysis of existing blockchain solutions [7], [21], [22], [23], [24], [25], [26], [27], [28], [29], [30] and electronic voting systems [31], [32] allowed us to identify the main requirements for the system of collective voting:

1. **Trustworthiness:** The proper use of technology helps to overcome the important problem of the modern world—lack of trust of citizens in the governments and legislative authorities of their countries. The blockchain-based e-voting platform provides confidence test at the programmatic level rather than at the procedural level.

2. **Systematicity:** The use of decentralized technology only at a specific stage of the electoral process, for example, for voting or tabulation, does not allow for a fully effective, credible system to be established. Blockchain solutions should be comprehensive and cover all stages of the voting process, from voters identification to the provision of results.
3. **Stability:** Recently, the world has been increasingly shaken by scandals involving real or imaginary interference in elections by sophisticated hacking techniques. Strong and sustainable encryption systems, which are inherent to the best blockchain solutions, will increase confidence in electoral systems.
4. **Intuitiveness:** Developers are well aware that simple and intuitive interface is essential for the success of the project. A user working with a blockchain-based election system should not experience any difficulties.
5. **Cost-effectiveness:** Experience of practical use of blockchain solutions in electoral processes shows their advantages in terms of efficiency-quality ratio over any other, not only paper, but also electronic systems. The effect is achieved by sharply reducing the number of people involved in the organization of an electoral process.

II. Choice of Software Solutions

The terms "electronic voting'' and "blockchain voting'' are often confused. For instance, the platform for e-voting in Estonia is often cited as an example of a blockchain voting system [33]. Meanwhile, this system, which started in 2005, does not use blockchain technology at all.

Electronic voting is a term that encompasses various types of voting that use any electronic during the process.

Blockchain-based platforms and applications are e-voting applications where peer-to-peer encrypted networks and other distributed ledger technology solution functions are used as data transmission networks. By the end of 2019, almost all operational and practically tested blockchain voting platforms are based on private blockchains, whose require user access and restrict who can be a member of the network. Such networks can store public and private information. Each user has his own level of access and certain rights with the ability to view, record and edit.

Private blockchains are noticeably more stable, economical and functional than public ones.

Being developed for a special task or a class of problems, it allows to take into account the content and logic of the processes to be automated to the fullest possible extent at the software and algorithmic level.

However, the majority of private blockchains have a serious drawback in the users' eyes. It is due to the fact that certain trusted nodes with higher levels of authority are responsible for the actions of network users. In other words, most private blockchains are hierarchical, consisting of two or more levels.

The innovation of this prototype of the electoral application is the usage of private blockchain with the usage of ring signatures [34].

A ring signature allows one person in the group to sign on behalf of the group. Its linkable modification also allows external observer checking whether in a set of signatures all signers are different.

Exonum is used as a framework for private blockchain development. Exonum is a flexible tool that allows developers to create individual blockchain projects and implement ready-made solutions at minimal cost. The Exonum framework provides the following advantages

- **Fail-safe:** Each validator node has its own copy of the data. The system continues to operate even if up to a third of all validators are disabled or compromised. Data can be restored across all nodes, even if only one instance is saved.
- **Data invariability:** The blockchain stores the entire transaction history, organised as a chain of blocks.
- **Cryptographic evidence:** When a node responds to a request, in addition to basic data, the node also returns cryptographic evidence that the data provided is actually stored in the database. This data is also checked on the client's side.
- **Fast and reliable consensus algorithm:** The system is Byzantine fault tolerant: even if some nodes behave maliciously, the system continues to process transactions correctly. In practice, the consensus algorithm guarantees stable performance for up to 5,000 transactions per second.
- **Protection against falsification:** To protect the blockchain from fraudulent entries, the hash of its state is periodically stored in the most reliable database available today—the Bitcoin blockchain, which is completely external to the system. Even if someone takes control of the majority of validators, they will not be able to tamper with the transaction history undetected.

Clients will check the database against the last record on the Bitcoin blockchain and flag the invalid data.

- **Easy to use:** The framework's official website provides comprehensive product documentation.

For the defined problem, this framework provides:

- Transparent and effective processes during the entire electoral cycle, from registration to the count of the results;
- Inability to manipulate data at any stage of the voting process;
- A quick check of logs.

A Rust programming language ring signature implementation of an original algorithm from [34] is used to ensure transparency and the necessary level of trust of the participants [35]. This helps to ensure the confidentiality of voting by allowing participants to vote by concealing the true addresses of their wallets. Ring signatures certify that the transaction was initiated by one of the addresses in the address group. Transactions signed with a ring signature refer to several other transactions in the blockchain. From the point of view of a third-party observer, all these transactions may seem to be initial with an equal level of probability.

III. General Architecture and Algorithm

In this prototype [36], blockchain-based voting is similar in principle to conducting transactions using cryptocurrency. Voters receive special tokens from the electoral commission, which we count as votes, and the tokens are then transferred to one of the special accounts assigned to each candidate. To determine the results, it is sufficient simply to check each candidate's accounts after the election. In order to preserve the confidentiality of a voter's choice, ring signatures are used at the time when the transaction is sent.

3.1. Asset Tokenization

Input: A set of public keys for voters, a set of public keys for candidates and voting start and end time.

Output: A set of transactions (it is not known which voter sent the vote, but we know which choice has been made).

One token (vote) is added to each voter's account before the beginning of the poll. Each voter can create a transaction to send their undivided vote to the chosen candidate. The following points should be taken into account during project development:

- Each person votes no more than once.
- Each participant's vote can be checked only by himself/herself. Only the overall results of the election are available to the public. This equirement will be implemented using ring signatures.

The structure of blockchain-based application using ring signatures consists of several parts:

- transactions;
- wallet structure;
- specialized storage;
- service structure.

3.2. Transactions

Transactions describe the state of votes' balance between the participants. There are several types of transactions needed to transfer votes and set up voter lists. Let's review the implemented transaction types in detail:

1. Transaction "Add Candidate" describes behaviour of changes in the list of the candidates set initially in genesis to the block. Public key is required to add a candidate.
2. Transaction "SetVoterList", similarly to the previous transaction, this transaxction changes the list of voters.
3. Transaction "CreateWallet" is necessary to record the active user in the network. In other words, a user can vote or be the one who is voted for, but in order to be able to store tokens, it is necessary to create an entity called "wallet", because wallet stores information about the balance of users.
4. Transaction "Vote" is designed to transfer tokens from the voter's balance to the selected candidate's wallet. Since each voter has only 1 vote, the number of tokens corresponds to the number of votes and is equal to the total number of voters. There is exactly one token on the balance of the voter, which is done in order to avoid a second vote.
5. Transaction "RingSignature" is used to build a ring signature. When launching this transaction with a secret key and voting data (the list of candidates and voters), the user receives a cryptographic signature. It is made, it to avoid fake voting procedures as the ring signature considers confirmed number of voters.

3.3. Wallet structure

Voting process, is implemented by sending tokens from one wallet to another. Structure "Wallet" consists of five fields:

1. "Public key": this field is used to identify the user, public key can be used to understand who owns the wallet.
2. "Name": name of the entity, is specified when starting "Wallet creation" transaction.
3. "Balance": description of the number of user's votes. The balance is either 0 if the voter has already made a choice, or 1 if this is still to be done. It is not possible to vote twice. Candidates, however, may have a balance of any natural number not exceeding the total number of voters, but candidates cannot spend these tokens.
4. "History length": used to display the number of operations performed with this wallet.
5. "History hash": it is necessary to get from a database using the hash operations made with the certain wallet.

For "Wallet" structure it is also used method set_balance. This method allows us to specify the initial state of the wallet, in particular, that the voting fields are initialized in accordance with the data that were sent to the transaction with a single balance.

3.4. Specialized storage

To ensure that the methods work correctly, any changes to the network are reflected in the database. The way of storing information in a blockchain with a ring signature is stored in the file schema.rs. All changes of user wallet (balance, hash, history length, etc.), the list of candidates and the list of voters are recorded in this storage. Unlike regular database structures, schema has the ability to check timestamp tags (when an operation was performed or when a change has been made), Merkle Tree proof, and the state hash value.

The chosen specialized storage has the following advantages:

1. Service Timestamp: Use of timestamp construction allows to prove the time when some operation was performed.
2. Merkle Tree: This is a way to check the immutability of the data. When constructing the tree, all possible objects are hashed, then new hashes are built using the obtained hashes by sequential paired concatenation until the root is generated. Obviously, if somebody replace at least one object, the hash of the root will be changed, so you can state the change of data.
3. State hash: The tree for the states is built in the same way as above, and the whole system changes when the state changes.

3.5. Specialized storage

In order to deploy the network, validators and auditors must be identified. Validators are the nodes that form blocks of transactions from the pool of unconfirmed transactions. Auditors are the nodes that store a complete copy of blockchain and do not participate in block mining. If necessary, they can check any suspicious factor in blockchain.

After defining the nodes, users are installed. There are two categories of users: voters and candidates. The list of candidates is formed in the very first block (genesis block) of the network. After defining the users, the transactions are sent to the pool, in other words, the voting process is running. After block mining, the requested changes in transactions are displayed in blockchain.

IV. Workflow Example

The typical voting procedure workflow contains the following steps

1. **Network creation:** A blockchain network is deployed on a local machine or several computers to support the voting process.
2. **Setting voting parameters:** When creating users, they generate private keys, their corresponding public keys are added to the list of voters, and voting time is set as well as the list of candidates. In operational applications, voters, their public keys, and the list of candidates are taken from know your customer-like procedures performed by voting organizers.
3. **Voting:** Voters send transactions; blockchain validators, among other things, verify the correctness of ring signatures (the sender proves he's a voter) and the fact that no attempt was made to vote more than once by any of the voters due to linkability. All transactions that attempt to vote twice are automatically invalidated and are not added to blockchain.
4. **Results:** at the end of voting, the number of tokens in the candidates' accounts is equal to the number of voters who voted for them.

Demo instructions and code are available at Github [36].

V. Numerical Experiments

We performed experiments on a local machine with 8 GiB RAM, 2 Core Intel Core i5 CPU running @3,1 GHz.

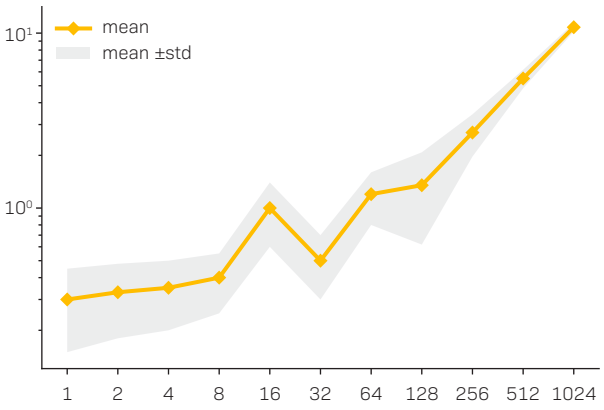

Fig. 1. Mean ring signature generation time [seconds] as a function of participants number.

Figure 1 shows the average time of one transaction creation with a ring signature as a function of the number of voters. Time grows linearly with the growth of the voters number, as more auxiliary generations of standard signature are required.

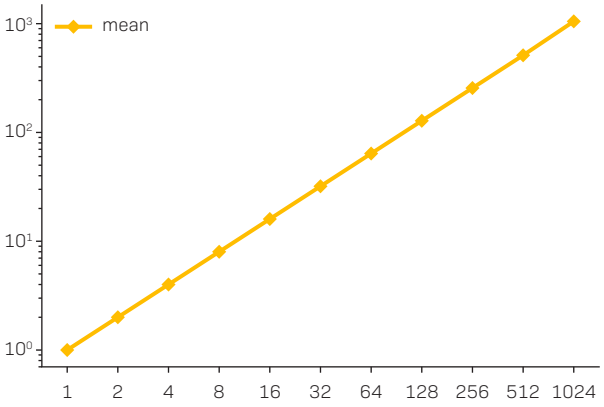

Fig. 2. Mean ring signature verification time [milliseconds] as a function of participants number.

The Figure 2 illustrates the dependence of the average time to verify the generated ring signatures. As expected, the dependence is also linear.

VI. Conclusion

This paper describes the process of developing and implementing a prototype of electronic voting system based on blockchain technology using linkable ring signatures.

The prototype meets three out of five criteria formulated in this work: trustworthiness, systematicity and stability.

The trust of all voters is ensured by using blockchain protocol, open source software and the implementation of ring signatures.

The solution allows us simultaneous implementation of two, usually conflicting, requirements: transparency and privacy.

Systematicity is ensured by using decentralized technology at all stages of the electoral process, from the registration of participants and the organization of the voting process to the tabulation of results.

Stability criterion is achieved by using the Exonum framework, which one of the key advantages is reliability and safety.

Only back-end is implemented in the prototype, while intuitiveness is a feature of the final version of application. Therefore, this criterion requires a front-end to be fulfilled. It is difficult to make a clear judgment on whether the cost-effectiveness criterion is met. Such an assessment should be carried out in the course of using the system in the real world of e-voting. However, the practical experience of blockchain solutions suggests that this technology is highly efficient.

Numerical experiments show that the system works effectively for voting with several thousand participants. For example, standard polling in Russia is upper bounded by 3,000 of voters per polling station [36]. For these cases it is possible to generate and validate transactions in real time using usual computers.

VII. Acknowledgement

This research received no external funding.
The paper is based on Alexandra Kugusheva's bachelor thesis at the HigherSchool of Economics, conducted under the supervision of Yury Yanovich.

References

[1] S. Nakamoto, "Bitcoin: A Peer-to-Peer Electronic Cash System", www.bitcoin.org, pp. 1–9, 2008. [Online]. Available: https://bitcoin.org/bitcoin.pdf.

[2] M. Pilkington, "Blockchain Technology: Principles and Applications", in Research Handbook on Digital, V. Buterin, "Ethereum White Paper: A Next Generation Smart Contract & Decentralized Application Platform", Etherum, pp. 1–36, 2014. [Online]. Available: https://github.com/ethereum/wiki/wiki/White-Paper.

[3] G. Fenu, L. Marchesi, M. Marchesi, and R. Tonelli, "The ICO phenomenon and its relationships with ethereum smart contract environment", in 2018 IEEE 1st International Workshop on Blockchain Oriented Software

Engineering, IWBOSE 2018 — Proceedings, vol. 2018 — Janua. IEEE, 3 2018, pp. 1–7.

[4] V. Buterin, "On Public and Private Blockchains — Ethereum Blog", 2015. [Online]. Available: https://blog.ethereum.org/2015/08/07/on-public-and-private-blockchains/.

[5] Bitfury Group and J. Garzik, "Public versus Private Blockchains. Part 1: Permissioned Blockchains", bitfury.com, pp. 1–23, 2015. [Online]. Available: http://bitfury.com/content/5-white-papers-research/public-vs-private-pt1-1.pdf.

[6] ——, "Public versus Private Blockchains Part 2: Permissionless Blockchains", bitfury.com, pp. 1–20, 2015. [Online]. Available: http://bitfury.com/content/5-white-papers-research/public-vs-private-pt2-1.pdf.

[7] M. Pilkington, "Blockchain Technology: Principles and Applications", in Research Handbook on Digital Transformations. Springer, 2016, pp. 225–253.

[8] Q. Shang and A. Price, "A Blockchain-Based Land Titling Project in the Republic of Georgia: Rebuilding Public Trust and Lessons for Future Pilot Projects", Innovations: Technology, Governance, Globalization, vol. 12, No. 3–4, pp. 72–78, 1 2019. [Online]. Available: https://www.mitpressjournals.org/doi/abs/10.1162/inov_a_00276.

[9] Libra Association, "An Introduction to Libra", 2019. [Online]. Available: https://libra.org/en-US/.

[10] Telegram, "Telegram White Paper", 2018. [Online]. Available: https://icorating.com/upload/whitepaper/gNQ7e9z3lCGi519Wz8mmC0Kg8aA0goeZKAQ802vo.pdf.

[11] J. Brett, "Congress Questions The SEC On Libra, Cryptocurrency And "The Whole Blockchain Phenomenon", 2019. [Online]. Available: https://www.forbes.com/sites/jasonbrett/2019/09/28/congress-questions-the-sec-on-libra-cryptocurrency-and-the-whole-blockchain-phenomenon/#606b5f7e5135.

[12] E. Androulaki, Y. Manevich, S. Muralidharan, C. Murthy, B. Nguyen, M. Sethi, G. Singh, K. Smith, A. Sorniotti, C. Stathakopoulou, M. Vukolic, A. Barger, S. W. Cocco, J. Yellick, V. Bortnikov, C. Cachin, K. Christidis, A. De Caro, D. Enyeart, C. Ferris, and G. Laventman, "Hyperledger fabric", in Proceedings of the Thirteenth EuroSys Conference on — EuroSys '18. New York, New York, USA: ACM Press, 2018, pp. 1–15. [Online]. Available: http://dl.acm.org/citation.cfm?doid=3190508.3190538.

[13] Y. Yanovich, I. Ivashchenko, A. Ostrovsky, A. Shevchenko, and A. Sidorov, "Exonum: Byzantine fault tolerant protocol for blockchains", bitfury.com, pp. 1–36, 2018.

[14] K. Makena, "Nearly 150 West Virginians voted with a mobile blockchain app — The Verge," 2019. [Online]. Available: https://www.theverge.com/2018/11/10/18080518/blockchain-voting-mobile-app-west-virginia-voatz.

[15] C. Loizos, "Voatz, the blockchain-based voting app, gets another vote of confidence as Denver agrees to try it — TechCrunch", 2019. [Online]. Available: https://techcrunch.com/2019/03/07/voatz-the-blockchain-based-voting-app-gets-another-vote-of-confidence-as-denver-agrees-to-try-it/.

[16] M. del Castillo, "Sierra Leone Secretly Holds First Blockchain-Audited Presidential Vote — CoinDesk", 2018. [Online]. Available: https://www.coindesk.com/sierra-leone-secretly-holds-first-blockchain-powered-presidential-vote.

[17] K. Houser, "Hold Up: What Actually Happened in Sierra Leone's 'Blockchain' Election?" 2018. [Online]. Available: https://futurism.com/sierra-leone-election-blockchain-agora.

[18] R. Osgood, "The Future of Democracy: Blockchain Voting", in COMP116: Information Security, 2016, pp. 1–21. [Online]. Available: http://www.nytimes.com/2016/12/09/us/.

[19] N. Kshetri and J. Voas, "Blockchain-Enabled E-Voting", IEEE Software, vol. 35, No. 4, pp. 95–99, Jul 2018. [Online]. Available: https://ieeexplore.ieee.org/document/8405627/.

[20] N. Faour, "Transparent Voting Platform Based on Permissioned Blockchain", pp. 1–34, 2018. [Online]. Available: http://arxiv.org/abs/1802.10134.

[21] M. Swan, Blueprint for a new economy. Cambridge: Cambridge University Press, 2015.

[22] H. M. Kim and M. Laskowski, "Towards an Ontology-Driven Blockchain Design for Supply Chain Provenance", SSRN Electronic Journal, vol. 25, No. 1, pp. 18–27, 8 2016. [Online]. Available: http://www.ssrn.com/abstract=2828369.

[23] K. Korpela, J. Hallikas, and T. Dahlberg, "Digital Supply Chain Transformation toward

Blockchain Integration", in Proceedings of the 50th Hawaii International Conference on System Sciences, 1 2017, pp. 4182–4191.

[24] T.-T. Kuo, H.-E. Kim, and L. Ohno-Machado, "Blockchain distributed ledger technologies for biomedical and health care applications", Journal of the American Medical Informatics Association, vol. 24, No. 6, pp. 1211–1220, 11 2017.

[25] S. Angraal, H. M. Krumholz, and W. L. Schulz, "Blockchain Technology", Circulation: Cardiovascular Quality and Outcomes, vol. 10, No. 9, pp. 5665–5690, 9 2017.

[26] P. Mamoshina, L. Ojomoko, Y. Yanovich, A. Ostrovski, A. Botezatu, P. Prikhodko, E. Izumchenko, A. Aliper, K. Romantsov, A. Zhebrak, I. O. Ogu, and A. Zhavoronkov, "Converging blockchain and next-generation artificial intelligence technologies to decentralize and accelerate biomedical research and healthcare", Oncotarget, vol. 9, No. 5, pp. 5665–5690, 1 2018. [Online]. Available: http://www.oncotarget.com/fulltext/22345.

[27] M. Kouhizadeh and J. Sarkis, "Blockchain Practices, Potentials, and Perspectives in Greening Supply Chains", Sustainability, vol. 10, No. 10, p. 3652, 10 2018. [Online]. Available: http://www.mdpi.com/2071-1050/10/10/3652.

[28] N. Alzahrani and N. Bulusu, "Block-Supply Chain: A New Anti-Counterfeiting Supply Chain Using NFC and Blockchain", in Proceedings of the 1st Workshop on Cryptocurrencies and Blockchains for Distributed Systems — CryBlock'18. New York, New York, USA: ACM Press, 2018, pp. 30–35.

[29] Y. Yanovich, I. Shiyanov, T. Myaldzin, I. Prokhorov, D. Korepanova and S. Vorobyov, "Blockchain-Based Supply Chain for Postage Stamps", Informatics, vol. 5, No. 4, p. 42, 11 2018.

[30] D. Korepanova, S. Kruglik, Y. Madhwal, T. Myaldzin, I. Prokhorov, I. Shiyanov, S. Vorobyov and Y. Yanovich, "Blockchain-Based Solution to Prevent Postage Stamps Fraud", in 2019 IEEE International Conference on Blockchain and Cryptocurrency (ICBC). IEEE, 5 2019, pp. 171–175.

[31] T. Kohno, A. Stubblefield, A. Rubin and D. Wallach, "Analysis of an electronic voting system", in IEEE Symposium on Security and Privacy, 2004. Proceedings. 2004, vol. 2004. IEEE, 2004, pp. 27–40.

[32] D. Bruschi, M. Burmester, L. F. Cranor, D. Chaum, I. Damgard, E. Gerck, D. Gritzalis, J. Groth, S. Ikonomopoulos, D. Jones, M. Karyda, S. Katsikas, A. Kiayias, R. Kies, C. Lambrinoudakis, E. Magkos, F. Mendez, R. Mercuri, L. Mitrou, P. Neumann, R. Peralta, G. Poletti, G. Quirchmayr, E. Rosti, G. Salomonsen, R. Saitman, A. Trechsel, V. Tsoumas and M. Yung, Secure electronic voting, ser. Advances in Information Security, D. A. Gritzalis, Ed. Boston, MA: Springer US, 2003, vol. 7. [Online]. Available: http://link.springer.com/10.1007/978-1-4615-0239-5.

[33] E-Estonia, "i-Voting", 2017. [Online]. Available: https://e-estonia.com/solutions/e-governance/i-voting/.

[34] S. Noether, A. Mackenzie and T. M. Research Lab, "Ring Confidential Transactions", Ledger, vol. 1, No. 0, pp. 1–18, 12 2016. [Online]. Available: http://ledger.pitt.edu/ojs/index.php/ledger/article/view/34.

[35] Decentralisedkev, "Rust Implementation of Multilayered Linkable Spontaneous Anonymous Group", 2019. [Online]. Available: https://github.com/crate-crypto/MLSAG.

[36] Federal Assembly of the Russian Federation, "Federal Law No. 51FZ of May, 18, 2005 — On the Election of Deputies of the State Duma of the Federal Assembly of the Russian Federation (in Russian)." [Online]. Available: https://rg.ru/2005/05/24/vybory-doc.html.