A Proposal of Blockchain-based Electronic Voting System

Cosmas Krisna Adiputra, Rikard Hjort, and Hiroyuki Sato
Dept. of Electrical Engineering and Information Systems
The University of Tokyo
Tokyo, Japan
fcosmas, hjort, schukog@satolab.itc.u-tokyo.ac.jp

Abstract—The Estonian electronic voting system which is a leading electronic voting system still suffers from universal verifiability issues and may need improvement of its availability. To solve the problems, in this paper we propose a blockchain-based electronic voting system. A blockchain is a distributed database, where the complete data is shared among all participants in the network. A blockchain system by its nature has several advantages that suit an electronic voting system. Its distributed architecture provides high availability to the system because it does not rely on a centralized server. As all participants have complete data, the protocol allows them to verify each block that is appended to the chain. We try to combine the double envelope encryption technique and blockchain technology for our proposed electronic voting system.

Index Terms—blockchain, e-voting, availability, universal ver-ifiability

I. Introduction

Democracy and voting are pillars of modern society, but the traditional paper ballots are prone to fraud and failure; ballots can be miscounted, or ballots sent via mail might get lost in transit. The traditional voting system also carries the costs of human resources, ballot deployment, and security measures. A massive amount of money is usually spent every election in every country.

Declining trends of participant rate in some countries have also appeared in recent years. [1] One of the reasons seems to be that youths find going to voting centers to vote impractical. [2, p. 31-32] Therefore, the need for a more practical voting system is increasing. As the internet may be a promising platform for youth engagement in politics [3], internet voting seems like a natural way to increase participation.

Some special adverse conditions also need to be considered. In Catalonia, Spain, a local referendum was held in 2017. However, the referendum had been declared illegal by the central government in Madrid, and on referendum day police stormed voting centers, confiscating ballot boxes and allegedly used violence against voters [4]. This is one example of the problematic nature of holding a democratic vote during an unstable state of affairs.

For electronic voting systems to be viable, we consider it necessary that they are easier to use and at least as secure as secure as traditional elections, and must be able to eliminate human error. This is difficult to achieve because electronic voting systems need strong encryption to guarantee security, integrity, and anonymity of the vote, while still being au-ditable. This must be ensured and still result in a user-friendly application, which is often hard to achieve.

Below is a requirement list for making a voting system applicable to the real-world, based on [5]–[7].

availability: An e-voting system must remain available during the whole election and must serve voters connect-ing from their devices.
eligibility: Only eligible voters must be allowed to cast a ballot, and only one vote per voter count.
integrity: A voting system must guarantee the integrity of the vote.
anonymity: The connection between the vote of a user and the user herself must not be reconstructable without her help (and preferably not even with her help).
fairness: The (partial) results must be secret until the tallying has ended.
correctness: The election results must be appropriately counted and correctly published.
robustness: The system should be able to tolerate (some) faulty votes.
universal verifiability: After the tallying process, the results are published and must be verifiable by everybody.
voter verifiability: The voter must be able to verify that her ballot arrived in the ballot box.
coercion freeness: The system must provide security mechanisms to prevent a coercer from forcing a voter to place a vote for a specific party or candidate; or even to see that she voted [8].

When Bitcoin was introduced in 2008 [9], it enabled transactions of funds without a trusted middleman. However, the underlying technology, called “blockchain”, has found many further uses, both by means of building on top of Bitcoin and by creating new blockchain protocols. A blockchain is an immutable ledger of events, and those events can be any kind of data. Ethereum [10] uses the ledger to perform arbitrary (Turing complete) computing tasks and data storage. So-called colored coins [11] use the Bitcoin blockchain for creating a framework of digital currencies with extra capabilities. A blockchain is, contrary to popular belief, not secret or

978-1-5386-7280-8/18/$31.00 ©2018 IEEE

anonymous. Rather, it is pseudonymous, meaning all activity is visible to anyone, but every actor may hide behind a “name” with no connection to their real identity, much like on an online message board.

A prolific use case for blockchain technology is democratic voting [12]. This could allow for democratic votes that can be easily monitored by outside observers, making miscounting next to impossible. Available products like Follow My Vote [13] and Sovereign [14] aim to revolutionize voting by making vote counting transparent, yet privacy-preserving. Both products let users pass on their votes to delegates, or vote on their own, through an application interface, as well as verify that their votes have been counted correctly. However, they do not explicitly present the implementation. Therefore, it is difficult to analyze how their blockchains are applied to voting.

We aim to design and build a blockchain-based voting system that can handle the most adverse conditions imaginable. Based on the requirements we stated previously, the voting system in Catalonia’s referendum would have needed improvement in its availability. We need a voting system that does not allow third-party to easily disturb or dismiss a legal referendum or election. This may happen either when some central authority prohibits a democratic vote, or when infrastructure and safety and trust issues make it hard to hold a physical vote, or both. By utilizing the strengths of blockchain that distributes trust to participant in its network, we can improve the availability of a voting system without relying on social trust. Also, the openness of blockchain can improve the universal verifiability of a voting system. In this paper, we propose our first blockchain-based electronic voting system that solves availability and universal verifiability issues in the current electronic voting systems.

Outline: The remainder of this paper is organized as fol-lows. Sect. II is an account of previous work. Sect. III presents the building blocks for our proposed system. Sect. IV describes our blockchain-based electronic voting system proposal. Our current implementation is described in Sect. V. In Sect. VI, we elaborate on our result and the analysis of it. Sect. VII gives the conclusion. Finally, the discussion about future extensions is described in Sect. VIII.

II. Related Work

Some governments have already implemented electronic voting systems and use them for parliamentary elections. These include the Estonian e-voting system [15]; the D.C. Digital Vote-By-Mail System(DVBM) [16]; and Civitas [5]. Since Estonia is considered a leading country in e-voting systems and has several years of practical experience, we are using that system as our baseline of a real, working e-voting system in this paper.

A. Estonian E-Voting System

Estonia has been using its e-voting system since 2005 and successfully uses electronic voting for all of their elections. National ID cards are used for voter authentication. [17] Despite being widely used, the voting system still has some vulnerabilities, notably to state-level attackers. A state-level attacker is powerful enough to perform timing attacks by having access to major parts of the network and having the capacity to log and analyze messages. [18]

A summary of the features of the Estonian e-voting system can be found in [17, Table 4.1]. Based on the table, the Estonian e-voting system is a centralized e-voting system with dedicated servers in one data center. Also, it has so far not allowed the public to verify the tallying result after an election finishes.

III. Preliminaries

In this section, we outline some of the basic concepts behind blockchain technology. Readers knowledgeable in blockchain and cryptography may want to skip this section.

A. Public Key Cryptography

In real-world e-voting systems, asymmetric cryptography is heavily used to de-/encrypt or sign a ballot [17, Sect. 3.1], employing systems such as RSA [19]. With public key encryption, both parties in communication can maintain a public and private key-pair. The public key of every party may be known by everyone, whereas the private key must be kept secret. Party 1 may encrypt a message for Party 2 using Party 2’s public key, which creates a ciphertext which only Party 2 can decrypt. Party 1 can also sign any message using their private key so that Party 2 (or anyone else listening in) can verify that the message is indeed from that Party 1.

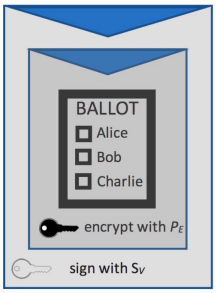

Fig. 1. Double Envelope—a signed and encrypted ballot, P_E being the public key of the election, and S_V the secret key of the voter.

A schematic of double envelope encryption is shown in Fig. 1. It shows a message sent from a voter to the election server. The ballot is encrypted election’s public key into a ciphertext, which becomes one “envelope”. After the voter signs the inner envelope with their private key it becomes a “double envelope” which can be sent to the election server.

B. Cryptographic Hash Function

A cryptographic hash function is a particular class of hash function that is suitable for use in cryptography. It maps data of arbitrary size to a bit string of fixed size. It is designed to be a one-way function, i.e., irreversible. By making the output string large enough, brute-force attacks (trying every possible input) becomes intractable. Password verification and the

proof-of-work used in blockchain employs cryptographic hash functions. Fig. 2 shows the general idea how a cryptographic hash function works.

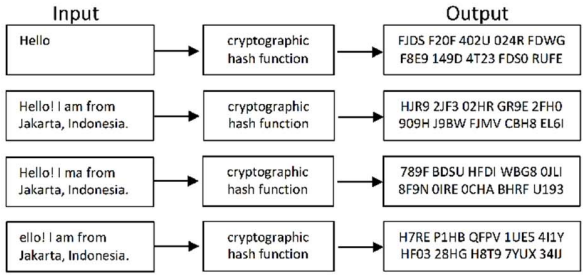

Fig. 2. Avalanche effect: a small change in the input of a cryptographic hash function drastically changes the output.

According to Cryptodox, “a cryptographic hash function should behave as much as possible like a random function while still being deterministic and efficiently computable” [20]. A cryptographic hash function is considered insecure if either of the following is computationally feasible:

Finding a previously unseen message that matches a given hash value.

Finding collisions, in which two different messages have the same hash value.

C. Blockchain

A blockchain is a distributed database, where the complete data is shared among all participants in the network. Data, which is supposed to be stored in this database, is packed into blocks with a defined maximum size and verified with a specific hash. A blockchain secured by the “proof of work” scheme dictates that this hash must fulfill some hard-to-achieve property, e.g., having a certain number of leading zeros, a number which may increase or decrease depending on the how fast blocks are created [9]. To achieve this, the participants add a nonce to the block, an essentially meaningless number, and try to find the correct hash by modifying the nonce between attempts to create a block with a hash that fulfills the proof-of-work condition. When such block is created, it may be sent to the network which will then accept it, append it to the chain of blocks, and work may then starts on creating a new block of data. The process is diagrammed in Fig. 3. The process of packing data into blocks and performing proof-of-work is called mining. Each block also contains a reference to the hash of the previous block so that, if any data gets changed in a previous block, the change would cascade through the list of blocks, giving them all new, invalid hashes.

A discoverer, who finds the correct hash for some packets, is granted some incentive. The amount of these granted incentive is controlled by the protocol.

Data in the blockchain is represented as transactions be-tween two or more users. Since all transactions are public, each user knows data of all other users. Before the transactions are added to the blockchain, the inputs of the transactions

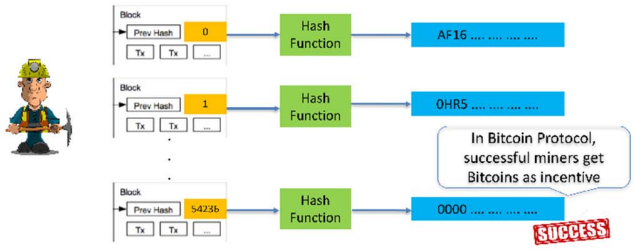

Fig. 3. A miner needs to find a nonce that fulfill the requirement of the blockchain protocol

are checked. This verification is possible due to the public transactions stored in a blockchain as shown in Fig. 4.

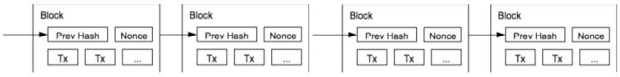

Fig. 4. A simplified blockchain architecture [9]

There are two main ways to participate in maintaining the network:

1) By setting up a full node, which means having the complete blockchain locally stored. These nodes verify that the contents and hashes of the blocks conform to the protocol, which ensures the blockchain’s integrity. In the case of Bitcoin, the verifiers ensure that no illegal transactions are made and that a miner has performed a correct proof of work. They also exchange blocks in the blockchain with each other so that everyone may keep a common state. It is necessary to have an active internet connection to participate.
2) Mine new transactions and find new hashes to generate new blocks. If a correct hash is discovered, it is sent to the network and can be verified by the full nodes.

D. Why Blockchain for E-Voting System?

A blockchain has several advantages, which make it a robust and secure alternative to other databases:

high availability: Completely distributed with many nodes storing the complete database.

verifiability: Each block contains the hash of its previous block and is appended to the blockchain. Everyone can calculate the hash and verify them.

integrity: It is hard to alter an older value in the chain, since all following blocks have to be re-calculated, which needs much computational power due to the proof-of-work.

IV. System Design

The main idea of our proposal is described in Fig. 5. We combine the idea of double envelope encryption and blockchain technology to implement our system. The figure consists of 3 sides: voter’s side, electoral commission’s side, and the blockchain network. To begin with, we need to assume a few things for our system to work properly.

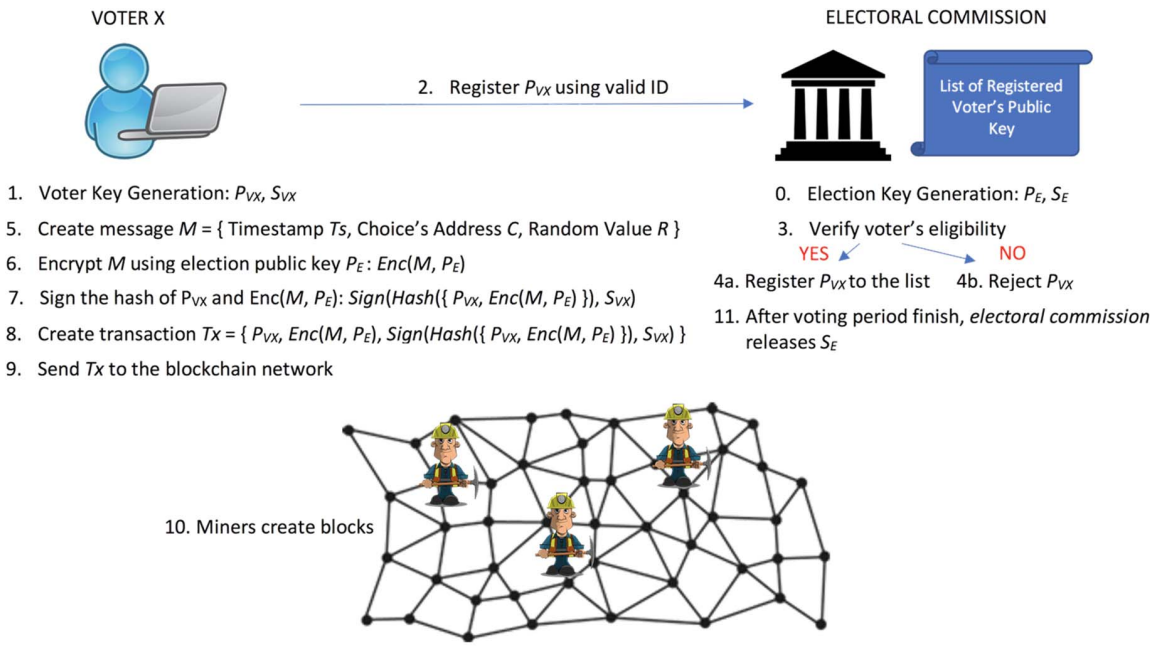

Fig. 5. Our proposal of blockchain-based electronic voting system

The election is correctly set up.

The voter's computer or device can be trusted.

There is a third party, electoral commission, that can be trusted to organize an election.

Not all trustees of the election are compromised. A proof-of-work blockchain can only work properly if less than 50% of the computational resources in the network are trying to cheat by changing the blockchain in a malicious way.

No. 0 to no. 4 in Fig. 5 show preparations needed for the election. At the beginning, the electoral commission (or another election manager) generates a key-pair for the election (P_E; S_E) which later is used for encrypting and decrypting messages of voters. Then, each voter needs to generate their own key-pair. In Fig. 5, ($P_{V\,X}$; $S_{V\,X}$) denote the key pair of voter X. This key pair is later used for signing the message created by the voter herself.

Voters need to register their public key $P_{V\,X}$ to the electoral commission for their voting eligibility using a designated valid ID. The electoral commission then verifies each voter's ID and registers the corresponding public key $P_{V\,X}$ to a public list; or rejects it if the voter is not eligible. It is crucial that each voter keeps their public key secret in this scheme and only sends it to the governing body.

After the registration finishes, a voter can start making a transaction T x that is described in Fig. 5 from no. 5 to 9. Firstly, a voter creates a message,

$$M = fT\ s;\ C;\ Rg; \tag{1}$$

which consists of a timestamp T s, the voter's choice address C, and a random value R. Timestamp T s shows the time when a voter votes.The timestamp T s also allows a voter to do multiple votes, so only the latest vote is counted. The voter's choice address C contains any value that points to the voting candidates, e.g., their public keys. A random value R is needed to prevent an attacker to guess the voter's key pair from encrypted messages created by the voter herself[1]. Secondly, the voter encrypts the created message M using election public key P_E denoted as $Enc(M; P_E)$. Thirdly, the voter signs the hash of her public key $P_{V\,X}$ followed by the encrypted message $Enc(M; P_E)$.

$$Sign(Hash(fP_{V\,X};\ Enc(M;\ P_E)g);\ S_{V\,X}) \tag{2}$$

denotes the said signature.

At this point, a voter can create her transaction T x. A transaction,

$$T\ x = fP_{V\,X};\ Enc(M;\ P_E);\ Signg; \tag{3}$$

contains the voter's public key $P_{V\,X}$, the encrypted message $Enc(M; P_E)$, and the signature of hash, Sign, combining both previous data described in (2). Lastly, the voter can send the transaction T x to the blockchain network.

Miners in the blockchain network collect transactions and create blocks. After a block containing a specific number of transactions is created and appended to the chain, any voter can verify that the vote is collected. The voter can wait for a few more blocks to be added on top to make sure that the block containing her transaction is inside the longest chain.

[1]Without this random value an attacker could easily guess a voter's choice by brute force; the limited number of participants in any given election means it would be easy to just try every possible vote and encrypt it with the voter's public key to see if it matches the transaction that voter sent.

This process continues until the voting period finishes. After the voting period finishes, the electoral commission destroys all the public keys they have on record and releases the election private key S_E, so everyone can start counting votes and verifying the result.

An attacker can not easily tamper votes. First, the voting message, M is encrypted with double envelop scheme. The attacker needs to figure out how to decrypt the encrypted message, Enc(M; P E) to tamper it. Then, although the attacker can decrypt it, only changing the vote and re-encrypt it will not make the vote valid. The signature described in (2) will tell that the vote has been tampered with. Everyone can verify the signature by using public key $P_{V\ X}$ and calculate the hash of the public key $P_{V\ X}$ and its corresponding encrypted message Enc(M; P E) that can be seen from the transaction. Therefore, the attacker also needs to figure out how to make the signature valid. Second, changing or removing a collected transaction inside a block changes the hash of the block itself. So, an attacker needs to re-calculate all hashes of next blocks which needs huge computational work.

V. Current Implementation

We are trying to implement our system, starting from a simple blockchain implementation. The conditions of our current implementation are:

No proof-of-work is implemented

One block contains only of one transaction.

Data are sent in JSON format via P2P network

A node has two interfaces to communicate. An HTTP interface is used for controlling the node, such as publishing transactions. A WebSocket interface is used for P2P com-munication with other nodes. Our current HTTP Interfaces commands are:

/mineBlock : tell a node to mine sent message

/Blocks : list all blocks a node has

/peers : list all peers a node has

/addPeer : add a new neighboring node to a node

VI. Result and System Analysis

TABLE I

QUALITATIVE EVALUATION OF OUR PROPOSED SYSTEM BASED ON E-VOTING CRITERIAS

Eligibility	Coercion	Availability	Anonymity	Integrity
# / # (ID)	4 / 4	# /	4 / 4	# / #
Correctness	Robustness	Fairness	Voter Verifiability	Univ. Verifiability
# / #	# / #	# / #	# / #	/ #

Estonian E-Voting System [17] / Proposed System

: completely fulfilled, # : fulfilled, 4 : partly fulfilled, : not fulfilled

As we are setting Estonian e-voting system as our baseline system, we are going to qualitatively compare it with the proposed system mainly on its availability and universal verifiability. In terms of availability, our proposed blockchain-based e-voting system can handle adverse conditions, such as natural disasters or physical attack on centralized system servers. By the nature of blockchain, all participants (nodes) in the blockchain network have roughly the same database. Any successful attacks on some of the nodes will not dismiss the whole process of election or referendum. As long as a voter has access to the blockchain network, she can always vote. Therefore, It improves the availability of a voting system as it can handle adverse conditions by decentralizing the data.

At the end of an election, an electoral commission can share the election secret key, S_E. Thus, anyone is able to open the encrypted messages which contain the ballot and verify the result of the election by herself. This is also one advantage that the Estonian e-voting system does not provide [17].

Ideally, voters are also the miners in the blockchain. If there are more voters participate in mining the blocks, the system becomes more decentralized and secure. However, there is still no incentive for the voters in our current proposal except the ability to vote without going to a voting center. In that case, government can also help mining the blocks as we discussed in Sect. IV that it is very difficult for an attacker to tamper votes.

In terms of coercion, our system reduces coercion as it allows voters to multi-vote.A voter can vote freely after the coercion disappears as only the last vote counts.This is a common problem that needs to be solved in electronic voting systems as a trade-off of not coming to a voting center.

Our proposed system needs many things to be done on the voter's side, such as key-pair generation, message encryption, hash calculation, data signature, and sending the transaction to the blockchain network. It is not easy to use for people in general. However, letting a third-party do these procedures may compromise the proposed system. For example, a third-party may keep a voter's secret key if the voter let the third-party do key-pair generation for the voter.

Our system relies heavily on the trust of the electoral commission side. The electoral commission can relate voters and their choices because voters register their public keys with their IDs to the electoral commission. The electoral commission also holds the election secret key, let it able to see the message created by voters. However, election secret key leakage can give massive damage to the election itself as it allows people to see the partial result of the election. This leakage can lead to the discontinuation of the election. Therefore, the electoral commission needs to protect the election secret key.

Verification time of a vote depends on the voting system protocol. In our system, we have not decided the protocol for mining a block in details. This protocol determines the time to create a block. A voter needs wait for some blocks to be confident that her vote is collected and written inside a particular block.

VII. Conclusion

In this paper, we proposed a blockchain-based voting system and did an early stage implementation of our system. The advantages and disadvantages of using blockchain as an e-voting system were also described. We also gave a qualitative

evaluation to our proposed system by using the criteria de-scribed in Sect. II and analysis of it.

Our proposed system still has wide room for improvements as described in Sect. VIII. Also, it needs time to popularize blockchain for a voting system as it is a novel idea and voting itself is a crucial matter in a democratic country. However, we believe improvements in future e-voting systems will provide a better solution to the current issues.

VIII. Future Work

We will continue on the implementation of our system and measure its performance. However, there are still some improvements that can be applied to our system.

A. Anonymity and Coercion Freeness

In our system, the electoral commission can relate voters and their choices; it violates the anonymity of its system. Originally, Bitcoin protocol only provides pseudonymity as only user's public addresses and not real IDs are written inside a block. However, an attacker can still relate users and their public addresses by watching their transactions. Some projects have been started to improve the anonymity of the bitcoin protocol, such as Mixcoin [21] and Dash [22]. They try to create a new tier in the blockchain network to mix transactions into a pool to increase the anonymity of the protocol.

To mix transactions without another node getting involved, some technologies can be applied. Blind signatures [23], homomorphic encryption [24], mix-nets [25], and one-way aggregate signature can be considered for future improvements.

B. Proof-of-Work

A typical proof-of-work may not be suitable for a blockchain voting protocol, because mining needs much com-putational power and thus monetary resources to find the cor-rect hash. It is also thinkable that organizations with complete data centers or mining pools use their superior computational power to find the correct hashes faster than other volunteers. This is a problem because if a mining pool has the power to provide 51% of the network's computational power, they can define the longest chain.

One considerable solution is to randomly pick the node to mine the next block. To guarantee the integrity of our blockchain, we need some full nodes staying online during the election. If many nodes are online, it is unlikely for a malicious node to get picked, which also secures the network. In this idea, we leave computational power and let small devices to be a node.

References

[1] "Election turnout likely second-lowest in postwar period, estimate says," The Japan Times, Oct 2017. [Online]. Available: https://www.japantimes.co.jp/news/2017/10/23/national/politics-diplomacy/election-turnout-likely-second-lowest-postwar-period-estimate-says/

[2] P. A. Azocar, Youth voter participation: involving today's young in tomorrow's democracy. International IDEA, Stockholm, 1999.

[3] V. C. Eze and K. Obono, "The influence of internet use on the political participation of youth in ikeja, lagos." Journal of Pan African Studies, vol. 11, no. 6, 2018.

[4] E. Nelson and J. Petzinger, "What you need to know to catch up on Catalonia's convoluted bid for independence," pp. 1–9, oct 2017. [Online]. Available: https://qz.com/1111079/catalonia-independence-crisis-everything-you-need-to-know-to-catch-up/

[5] M. R. Clarkson, S. Chong, and A. C. Myers, "Civitas: Toward a secure voting system," in 2008 IEEE Symposium on Security and Privacy (sp 2008), May 2008, pp. 354–368.

[6] S. Delaune, S. Kremer, and M. Ryan, "Verifying privacy-type properties of electronic voting protocols," J. Comput. Secur., vol. 17, no. 4, pp. 435–487, Dec. 2009. [Online]. Available: http://dl.acm.org/citation. cfm?id=1576303.1576305

[7] S. Kremer, M. Ryan, and B. Smyth, Election Verifiability in Electronic Voting Protocols. Berlin, Heidelberg: Springer Berlin Heidelberg, 2010, pp. 389–404. [Online]. Available: https://doi.org/10.1007/978-3-642-15497-3 24

[8] T. Okamoto, "Receipt-free electronic voting schemes for large scale elections," in Proceedings of the 5th International Workshop on Security Protocols. London, UK, UK: Springer-Verlag, 1998, pp. 25–35. [Online]. Available: http://dl.acm.org/citation.cfm?id=647215.720390

[9] S. Nakamoto, "Bitcoin : A Peer-to-Peer Electronic Cash System," White Paper, pp. 1–9, 2008.

[10] G. Wood, "Ethereum: a secure decentralised generalised transaction ledger," Yellow Paper, pp. 1–32, 2014.

[11] M. Rosenfeld, "Overview of colored coins," White paper, bitcoil. co. il, p. 41, 2012.

[12] J. B. Koven, "Block The Vote: Could Blockchain Tech-nology Cybersecure Elections?" aug 2016. [Online]. Avail-able: https://www.forbes.com/sites/realspin/2016/08/30/block-the-vote-could-blockchain-technology-cybersecure-elections/fn#g5816df3f2ab3

[13] Follow My Vote, "Follow My Vote Launches Crowdfunding Campaign For Veri able Open-Source Blockchain Voting Software , Making Voting Honest And Convenient For All," 2016. [Online]. Available: https://followmyvote.com/

[14] K. Leary, "Blockchain could be about to change how you vote," sep 2017. [Online]. Available: https://www.weforum.org/agenda/2017/09/blockchain-could-be-about-to-change-how-you-vote

[15] E. Maaten, "Towards remote e-voting: Estonian case." in Proceedings of the 1st Conference on Electronic Voting, 01 2004, pp. 83–100.

[16] S. Wolchok, E. Wustrow, D. Isabel, and J. A. Halderman, "Attacking the washington, d.c. internet voting system," in Financial Cryptography and Data Security. Berlin, Heidelberg: Springer Berlin Heidelberg, 2012, pp. 114–128.

[17] C. Meter, "Design of Distributed Voting Systems," Master's thesis, Heinrich-Heine-Universitt Dsseldorf, 2017. [Online]. Available: http: //arxiv.org/abs/1702.02566

[18] E. English and S. Hamilton, "Network security under siege: the timing attack," Computer, vol. 29, no. 3, pp. 95–97, Mar 1996.

[19] R. L. Rivest, A. Shamir, and L. Adleman, "A method for obtaining digital signatures and public-key cryptosystems," Communications of the ACM, vol. 21, no. 2, pp. 120–126, 1978.

[20] Cryptographic hash function. [Online]. Available: https://cryptodox. com/Cryptographic hash function

[21] J. Bonneau, A. Narayanan, A. Miller, J. Clark, J. A. Kroll, and E. W. Felten, "Mixcoin: Anonymity for bitcoin with accountable mixes," Lecture Notes in Computer Science, vol. 8437, pp. 486–504, 2014.

[22] E. Duffield and K. Hagan, "Darkcoin: Peer to Peer Crypto Currency with Anonymous Blockchain Transactions and an Improved Proof of Work System," White Paper, 2014. [Online]. Available: https://pdfs.semanticscholar.org/b05d/a03086ac0b24d316bc604b25c9859df34339.pdf

[23] S.-I. Kang and I.-Y. Lee, "A study on the electronic voting system using blind signature for anonymity," 2006 International Conference on Hybrid Information Technology, vol. 2, pp. 660–663, 2006.

[24] C. Gentry, "A fully homomorphic encryption scheme," Ph.D. dissertation, Stanford University, Stanford, CA, USA, 2009, aAI3382729.

[25] R. Haenni, P. Locher, R. Koenig, and E. Dubuis, "Pseudo-code algorithms for verifiable re-encryption mix-nets," in Financial Cryptography and Data Security, M. Brenner, K. Rohloff, J. Bonneau, A. Miller, P. Y. Ryan, V. Teague, A. Bracciali, M. Sala, F. Pintore, and M. Jakobsson, Eds. Cham: Springer International Publishing, 2017, pp. 370–384.