Original scientific paper
Received: 2022-03-02
Accepted: 2022-04-24

PRIVACY AND VERIFIABILITY IN A PUBLIC REMOTE-CAPABLE BLOCK-CHAIN E-VOTING

Roberto ANIĆ BANIĆ, RIT Croatia, rxa6313@rit.edu

***Abstract*—Voting privacy and verifiability are the building blocks of modern democracy. While many non-remote-capable voting systems provide privacy, verifiability, and sometimes even coercion-resistance in some manner or another, these requirements are a big challenge for a remote-capable voting system. By applying the blockchain technology some of these requirements are fulfilled, however many other technologies, including encryption schemes, distributed computing, and others are needed to satisfy the others. This paper explores the technologies used in current and previous voting systems, their applications, and the actual voting systems themselves.**

I. Introduction

In this era of the technological revolution, it is hard to believe that one of the most important systems that decide our freedom, rights, and way forward is still not fully transparent and subject to public scrutiny. This system is voting, the centerpiece of most modern countries, a democratic process that in theory allows us to fairly choose our leaders by respecting the vote of the majority. Yet even today the voter can never be sure if his vote was counter properly, fraudulently, or not counted at all. Adiputra et al. (2018) explain the issues of physical voting systems and how they can be manipulated by using the example of the referendum in Catalonia, Spain in 2017. This process could greatly benefit from being implemented using modern-day blockchain technology which could allow every single voter to verify their votes independently and be sure that a malicious actor did not falsify the results of an election or any sort of vote. Modern E-Voting systems already exist in countries like Estonia but suffer from a lot of issues. Adiputra et al. (2018) also show that one of the main issues of this system is voting verifiability, and that is one of the main problems this project aims to solve, alongside other privacy concerns, and bring trust and confidence in a fair democratic voting process to every voter. This paper explores the privacy and verifiability of modern voting systems, both physical and remote, and explores if these methods apply to remote blockchain E-Voting systems.

II. Terminology

Since this paper focuses on the privacy and verifiability components of a public blockchain (ledger) E-Voting system it is a requirement to be aware of some of the basic terms used to describe the process of voting, and the blockchain itself. In particular, the following terms are used.

A. Blockchain

A blockchain is a form of an append-only database, popularized by a character known as Satoshi Nakamoto in 2008 by creating Bitcoin. It is one of the perfect technologies to use for an E-Voting system. It provides a great solution to issues such as voting security, anonymity, and verifiability through various cryptographic techniques integrated in addition to the blockchain (Pawlak et al., 2018). However, it primarily serves the simple purpose as a distributed append-only database, which can provide a live record of current votes, along with ensuring that records cannot be retroactively changed.

B. Privacy

When it comes to privacy, there are several basic terms. The first is the Secret Ballot (also known as the Australian ballot (The Editors of Encyclopaedia Britannica, 2015)), a capstone of modern democracy (Voter Privacy, 2022). The secret ballot was first introduced in France in 1831 (Smyth, 2018), but in its most modern form, it was first implemented in the states of Victoria and South Australia. It is a guarantee that a voter's identity in an election, referendum, or any other voting process, is anonymous. By having this guarantee, the possibility of vote coercion, vote purchasing, or any other

fraudulent voting activity in which a voter is influenced illegally by a third party, is greatly reduced. The voting process is usually performed as follows: a voter marks their ballot in a private space (often a designated booth) and places it in a (previously inspected to be empty) box with a small opening on the top. In this way, a third party can't discover the contents of a voter's ballot (The Editors of Encyclopaedia Britannica, 2015).

C. Coercion Resistance

Coercion resistance is a measure of how resistant a system is to a potential coercer determining if a coerced voter is complying with their demands. While this seems like a relatively simple problem to solve by the way of simply turning off any sort of vote verifiability in the system is completely nullifies the second goal of the system, to enable each voter to verify their vote was cast correctly. While enabling voters to vote remotely most certainly does not introduce the problem of vote-coercion and vote-buying it does have the potential to exacerbate them (Juels, Catalano, & Jakkobson, 2005).

D. Receipt-Freeness

Receipt-freeness ensures that a voter cannot provide any sort of evidence/proof that reveals in which way they voted. In a traditional physical election system, a voter is required to keep their vote private (Benaloh & Tuinstra, 1994), and by using traditional voting booths, and disallowing any sort of visual recording devices this is easily achieved. Some systems use trusted third parties as a way to "hide" the receipt from a voter, however, this is not applicable to a remote voting system use-case (Alpert et al., 1998).

Todays' physical system in use by Croatia is in fact, receipt-free. As such, there is no evidence or proof that a voter could provide to a potential vote purchaser that he has voted a specific option. Even in the case of a voter taking photographic evidence of their vote, they could always request a second ballot to cast their actual vote and use the prior photographic evidence as proof.

In the case of an electronic voting system however this becomes a real problem, and most individually verifiable voting systems suffer the same problem. To allow a voter to verify their vote was recorded and tallied as cast they need to be provided some sort of proof. In a simple blockchain system, that would contain of a randomly generated vote ID which when supplied to the voter would allow them to verify their vote on a public distributed ledger. While this is a major advantage to the voter by making the option of verifying their vote was properly recorded possible, it also traditionally prevents them from lying to the vote purchaser. The possible solutions to this will be discussed later in this paper.

E. Verifiability

Vote verifiability is the ability of a voter or a third party to verify a single vote / a set of votes. The different types or verifiability are as follows:

1) Individual Verifiability, ensures that a voter is able to verify that a ballot containing their vote is in the recorded set of all votes.
2) Universal Verifiability, ensures that any third party has the possibility to tally up all the votes in the system and verify that it is the same as the vote count used by the governing authority to determine the result of an election/referendum.
3) End-to-end Verifiability, ensures that a voter can verify the following:
    a) Cast as Intended, their choice was correctly denoted on the ballot as chosen.
    b) Recorded as Cast, their choice was recorded as it was cast.
    c) Tallied as Recorded, their ballot was included in the final tally.
4) Voter Eligibility Verifiability, ensures that any party can verify that any vote in the system came from a voter that is eligible to vote.

III. Current Technological Solutions

A. Privacy through anonymized voter IDs

In modern electronic E-Voting systems maintaining privacy is quite a simple task, usually, it is the case of applying basic voter eligibility tokens which are generated as an anonymized ID used for verification that a voter is eligible at all. However, this solution alone prevents any receipt freeness if the ID is stored alongside the vote. The ID itself in that case serves as a receipt.

A blockchain-based E-Voting system could implement these voter IDs as a way to also satisfy the constraint of Voter Eligibility Verifiability. For a voter to be allowed to vote on a certain election they would need to provide some proof of existence. Usually, this would be done through either physical registration beforehand at postal offices, police stations, or

other government institutions. In the case of the Croatian "E-Gradani" system however, we can most certainly rely on registering voters through the system as it has also been deemed secure for many other applications such as retrieval of sensitive personal information, reading medical history, etc. A voter would after requesting registration receive a unique randomly generated identification token which gets written to the "voter registry blockchain" to "activate" that token for future use. No personal data is stored alongside this token. It is the responsibility of the voter not to reveal or even possibly sell this token. Unfortunately, in any remote-voting system, it is impossible to confirm if the voter is actually who they say they are without an overreach into their privacy.

B. Privacy through homomorphic encryption

Homomorphic encryption allows computations on encrypted data without first decrypting it. The result, when decrypted with the corresponding private key, is equivalent to the output produced had an appropriate operation been used on the original decrypted data. An example is shown below, $\odot$ and $\circledast$ being the appropriate operations, and pub being the public encryption key:

$$E_{pub}(msg_1) \odot E_{pub}(msg_2) = E_{pub}(msg1 \circledast msg2)$$

Some popular schemes include RSA, ElGamal, Goldwasser-Micali, Benaloh, Paillier. There are others but not all of them allow an unbounded number of operations. The main issue with homomorphic encryption models, however, is the fact that while, yes, it enables universal verifiability, is also that it doesn't in itself provide full end-to-end verifiability without combining it with some other system such as mix-nets. Usually, the implementation of such other systems results in a complete negation of any coercion resistant measures, or a loss of individual verifiability (Acquisti, 2004; Hirt & Sako, 2000). Systems such as Microsoft ElectionGuard (Features - ElectionGuard, 2022)] while coercion resistant, do not provide any verification of how a specific vote was recorded, only that it was tallied as recorded. While there is a feature that allows the voter to spoil a ballot, there is still needed inherent trust in the machine used to vote. This further shows that there is also no possibility of remote voting.

A blockchain-based E-Voting system could very well make use of homomorphic encryption by encrypting the votes (Matile & Killer, 2018), but it is not useful in the sense that by doing so you still need to trust the authority that the vote was indeed recorded as cast.

C. Designated verifier proofs

A proof system allows a voter to prove that an encrypted vote contains a specific answer. A designated verifier proof, in contrast to a regular non-interactive proof, is not transferrable (Jakobsson et al., 1996). Therefore, the voter cannot prove to anyone but himself that he voted a specific way. The issue with designated verifier proofs is, even though they could be useful in the sense that one would have to identify himself via a smart-card, as mentioned by Jakobsson et al. (1996) it is still up to the voter to make sure that the smart-card and the access codes to it is secure. Therefore, coercion resistance isn't achievable through such an implementation. There do exist relatively modern zero-knowledge proof methods which are do enhance coercion resistance but they are not applied in any of the reviewed systems (Chaidos & Couteau, 2018).

D. Recorded-as-cast verification through ballot auditing

Many systems, such as Microsoft's ElectionGuard (Features - ElectionGuard, 2022) aims to preserve privacy by storing the voter's choice in an encrypted form. When the voting machine prints out a receipt, it contains the ciphertext form of the voter's choice. A voter, which is not cryptographically literate, cannot be convinced that the ciphertext form is actually their vote. To help with that many systems allow a voter to potentially "spoil" a ballot. In simple terms, after a voter casts their vote, the machine will print the ciphertext proof, which the voter can see. However, a voter can subsequently choose to not vote, but "spoil" the ballot, and by that see what the expected output would be. A voter can then choose to decrypt the vote, via the machine to find out if the voting machine cheated or not. Prêt à Voter also implements a continuing auditing scheme that works similarly (Ryan et al., 2009).

IV. Potential voting system candidates

A. Prêt à Voter

Prêt à Voter is a voting system devised by Peter Ryan of the University of Luxembourg. By using a public ledger and a receipt with an onion (an encrypted key that contains a way to decode the vote shown on the receipt) Prêt à Voter allows the voter to confirm that their vote has been: cast-as-intended (by comparing their receipt and the ledger record), recorded-as-cast (again, by comparing their receipt and the ledger record), and tallied-as-recorded. This system, however, is not suitable for a remote voting system of any sort, because it cannot be adapted as such that it prevents voter coercion in any way.

B. Civitas

Civitas is the first electronic voting system to implement coercion resistance, universal and voter verifiability, which is suitable for remote voting (Clarkson et al., 2008). It provides coercion resistance by way of fake credential generation which are indistinguishable to a coercer from a real credential. The algorithms and processes in use by Civitas are unfortunately very computationally expensive during the vote tabulation phase (Clarkson et al., 2008). Civitas additionally has time expense issues when it comes to fake and duplicate votes since the complexity of the operation is , N being the number of votes. However, this can be solved by splitting up the vote system across blocks of voters. Unfortunately, Civitas in its original design does not provide cast-as-intended end-to-end verification which is a major verifiability issue (Jonker et al., 2013).

C. Provotum

Provotum is an end-to-end remote electronic voting system utilizing a permissioned blockchain. Killer et al. (2020), explains, "It operates in a fully distributed fashion by using Smart Contract, Distributed Key Generation, Homomorphic Encryption, and Cooperative Decryption, as well as employing client-side encryption, which enables ballot secrecy, while the Blockchain forms an audit trail, enabling public and End-to-end Verifiability". Even though Provotum does not have cast-as-intended verification capabilities, it does leave the door open to future work for enabling cast-as-intended verification through secure devices such as smartphones which provide secure enclaves. The system, unfortunately, because of being developed according to Swiss legislation, does not permit casting of multiple ballots as a coercion resistance measure.

V. Proposed enhancement to Provotum

The proposed enhancement to Provotum would be the following: a third-party implementation of cast-as-intended verification using the Secure Enclave of iOS devices. Such an application should bring forth and explain to a layman how their vote is being verified, and eventually, it should also be validated by an independent third party. There would be no particular need for the use of special devices with capabilities of "secure storage of secret elements" (Hofmann, 2020) since all modern iOS capable devices already support such features. It would also enable the voter to convince themselves of the fact that the device and corresponding application operate correctly by casting test votes. A challenge of implementing such a feature pertains to the secure feature of the Secure Enclave which disallows any import of an external key, nor an export of an internal key. The Secure enclave only allows storage of 256-bit elliptic curve private keys (by means of generating them inside the Secure Enclave), and various cryptographic operations on that key. This poses a challenge since Provotum is not internally based on such a key size, and Elliptic Curve Cryptography (ECC) is not the only type of cryptography utilized by Provotum. Therefore all cryptographic elements of Provotum not compatible with Secure Enclave key computations and storage would need to be modified to work alongside it efficiently and securely.

VI. Conclusion

Through the research of previous and current voting systems, it is apparent that no current voting system can completely satisfy privacy and verifiability without sacrificing coercion resistance. It is not surprising since those properties of voting schemes have been shown incompatible by Chevallier-Mames et al. (2010) before. While many have tried to design coercion-resistant systems that are partially verifiable, this is most certainly not the solution for a system used in the real world. In practice, with every voting system in use today, a voter always has a possibility to sell their vote with relative proof. Provotum is a promising voting system that satisfies the largest amount of voting system requirements put forth in this paper, and one of its biggest current weaknesses is that it has no integrated cast-as-intended verification. An example of a third-party implementation of such a feature with no special hardware (while complying with local regulations) would go a long way to increasing public trust in the voting system. Future research will consist of evaluating the iOS Secure Enclave feature as a secure storage facility for Provotum-based blockchain voting systems, research on the necessary modifications to the Provotum key generation protocol, and an implementation of the former as a proof-of-concept.

References

References

[1] Acquisti, A. (2004, April). Receipt-Free Homomorphic Elections and Write-in Voter Verified Ballots. Carnegie Mellon University. https://www.heinz.cmu.edu/ acquisti/papers/acquisti-electronic_voting.pdf

[2] Adiputra, C. K., Hjort, R., & Sato, H. (2018). A proposal of blockchain-based electronic voting system [Paper presentation]. 2018 Second World Conference on Smart Trends in Systems, Security and Sustainability (WorldS4), London, United Kingdom.

[3] Alpert, D., Ellard, D., Kavazovic, O., & Scheff, M. (1998, December). Receipt-Free Secure Elections 6.857 Final Project. https://syrah.eecs.harvard.edu/files/syrah/files/6857-98.pdf

[4] Benaloh, J., & Tuinstra, D. (1994). Receipt-free secret-ballot elections (extended abstract). Proceedings of the tewnty-sixth annual ACM symposium on Theory of computing - STOC '94, 544-553. https://doi.org/10.1145/195058.195407

[5] Chaidos, P., & Couteau, G. (2018). Efficient designated-verifier non-interactive zero-knowledge proofs of knowledge. Advances in Cryptology – EUROCRYPT 2018, 193-221. https://doi.org/10.1007/978-3-319-78372-7_7

[6] Chevallier-Mames, B., Fouque, P.-A., Pointcheval, D., Stern, J., & Traore, J. (2010). On Some Incompatible Properties of Voting Schemes. In Lecture Notes in Computer Science: Vol. 6000. Towards Trustworthy Elections (pp. 191-199). Springer Nature. https://doi.org/10.1007/978-3-642-12980-3_11

[7] Clarkson, M. R., Chong, S., & Myers, A. C. (2008). Civitas: Toward a secure voting system [Paper presentation]. 2008 IEEE Symposium on Security and Privacy, Oakland, CA, United States. https://sci-hub.mksa.top/10.1109/SP.2008.32

[8] The Editors of Encyclopaedia Britannica. (2015, May 5). Australian Ballot — politics — Britannica. Encyclopedia Britannica. Retrieved March 21, 2022, from https://www.britannica.com/topic/Australian-ballot

[9] Features - ElectionGuard. (2022). ElectionGuard. Retrieved March 23, 2022, from https://www.electionguard.vote/overview/Features/

[10] Hirt, M., & Sako, K. (2000). Efficient Receipt-Free Voting Based on Homomorphic Encryption. In Lecture Notes in Computer Science: Vol. 1807. Advances in Cryptology — EUROCRYPT 2000 (pp. 539-556). https://doi.org/10.1007/3-540-45539-6_38

[11] Hofmann, A. (2020). Security Analysis and Improvements of a Blockchain-based Remote Electronic Voting System [Unpublished master's thesis]. University of Zurich. https://www.merlin.uzh.ch/contributionDocument/download/14015

[12] Jakobsson, M., Sako, K., & Impagliazzo, R. (1996). Designated verifier proofs and their applications. Advances in Cryptology — EUROCRYPT '96, 143-154. https://doi.org/10.1007/3-540-68339-9_13

[13] Jonker, H., Mauw, S., & Pang, J. (2013). Privacy and verifiability in voting systems: Methods, developments and trends. Computer Science Review, 10, 1-30. https://doi.org/10.1016/j.cosrev.2013.08.002

[14] Juels, A., Catalano, D., & Jakobsson, M. (2010). Coercion-Resistant electronic elections. Towards Trustworthy Elections, 37-63. https://doi.org/10.1007/978-3-642-12980-3_2

[15] Killer, C., Rodrigues, B., Scheid, E. J., Franco, M., Eck, M., Zaugg, N., Scheitlin, A., & Stiller, B. (2020). Provotum: A blockchain-based and end-to-end verifiable remote electronic voting system. 2020 IEEE 45th Conference on Local Computer Networks (LCN). https://doi.org/10.1109/LCN48667.2020.9314815

[16] Matile, R., & Killer, C. (2018). Privacy, Verifiability, and Auditability in Blockchain-based E-Voting [Master's thesis, University of Zurich]. University of Zurich - Department of Informatics (IFI). https://files.ifi.uzh.ch/CSG/staff/rodrigues/extern/theses/mp-raphael-christian.pdf

[17] Pawlak, M., Guziur, J., & Poniszewska-marańda, A. (2018). Voting process with blockchain technology: Auditable blockchain voting system. Advances in Intelligent Networking and Collaborative Systems, 233-244. https://doi.org/10.1007/978-3-319-98557-2_21

[18] Ryan, P., Bismark, D., Heather, J., Schneider, S., & Zhe Xia. (2009). PrÊt À voter: A voter-verifiable voting system. IEEE Transactions on Information Forensics and Security, 4(4), 662-673. https://doi.org/10.1109/TIFS.2009.2033233

[19] Smyth, B. (2018, February 23). A foundation for secret, verifiable elections.

[20] Voter Privacy – EPIC – Electronic Privacy Information Center. (2022). EPIC – Electronic Privacy Information Center. Retrieved March 23, 2022, from https://epic.org/issues/democracy-free-speech/voter-privacy/