Anonymous Blockchain based model for e-Voting

Marija Taneska
Faculty of computer science and engineering
Ss. Cyril and Methodius, University Skopje, North Macedonia
marija.taneska@students.finki.ukim.mk

Fat Halimi
Faculty of computer science and engineering
*Ss. Cyril and Methodius, University*Skopje, North Macedonia
fat.halimi@students.finki.ukim.mk

Abstract—**In this paper, we analyze the provided security, anonymity, and privacy provided by Zcash and Monero. We focus on the description for the e-voting framework based on Zcash and Monero using their anonymity advantages. Analyzing advantages and disadvantages of Zcash and Monero, we make comparation between them, and conluded that Monero is more secure than Zcash, and we recommend using Monero for serious e-Votings. Our key is to give a sparkle to Blockchain developers to create a legitimate framework or system that would be based on Zcash and Monero Blockchains to realize e-voting.**

Keywords—e-voting, Blockchain, Zcash, Monero

I. Introduction

Voting is an action we perform in several different situations: some examples are song contests, reality shows, associations/councils, company decisions, or politics. Wherever allowed, digital voting systems have been introduced as tools to make it easier for voters to express their choice and to reduce the huge costs of voting in person. However, most digital voting solutions in use nowadays affected by several problems. Digital ledger technologies, especially Blockchains, renew interest in e-voting.

In Section II (e-Voting criteria), we describe the criteria for e-Voting, then in Section III (Blockchains overview), we describe Blockchains and conclude what type of Blockchain satisfies those criteria. In the Section IV (Blockchains overview), we describe how Zcash and Monero work and analyze the provided security, anonymity, and privacy In Section V (e-Voting implementation ideas) is the description of how will be working e-Voting based on Zcash and Monero, in Section VI (e-Voting phases) we describe phases in both implementations. In Section VII (Comparison between Zcash and Monero), we compare them based on their provided security and conclude what is more secure for e-voting. In Conclusion we describe the key features and advantages of using Blockchain for e-Voting.

II. e-Voting criteria

e-Voting must meet the following criteria: Immutability, Equality, Eligibility, Anonymity, No forgery, Verifiability, Scalability, and Stability.

Immutability means integrity too because this step means that no one can have access to votes in terms of deletion or modification. Using the Blockchain we can satisfy these criteria because once a voting transaction is made it is permanent, unchangeable, undeletable.

Equality assures that each vote once is counted and the choice added to a database, that vote should no longer be eligible to go through counting again. With a framework, we would make some changes and add “flags” to the votes once they go through counting.

Eligibility assures that the vote comes from the voter and no one else. We provide eligibility by using zk-SNARKs in Zcash based implementation, in Monero based implementation by using Ring Signatures.

Scalability means that the system should be secure enough, professional enough, and have free data space for millions of voters since this system can be used for political elections.

Stability means that the system should be designed to have a long life, stability depends on scalability.

Anonymity ensures that the Voting system user knows that the voter voted, but not what the voter voted for.

No forgery means that only the legal voters can vote and every voter can vote only once.

III. Blockchain

Blockchain is a peer-to-peer ledger system that allows peers to transact directly with each other eliminating the need for a central authority. Blockchain is a system for recording information about a transaction in a new decentralized way that makes it difficult or impossible to alter. These transactions are stored on sheets or blocks in a digital ledger that is shared among the participants of the network. Consensus on the transactions brings the peer-to-peer network into an agreement.[1] There are two types of Blockchain - public Blockchain and private Blockchain.

A. Public Blockchain

A Public Blockchain is open and full transparency for all and allows anyone to participate in the network, read or write. We can not use the public Blockchain for e-Voting implementation, since it does not satisfy Anonymity criteria. Also, the public Blockchain is decentralized and does not have a single entity that controls the network. Moreover, Blockchain does not have any regulations that the nodes have to follow.

B. Private Blockchain

A Private Blockchain is a permissioned managed Blockchain and participants must consent to join the network. Only entities participating in the transaction know about the transaction performed, others will not be able to access it. Private Blockchain focuses on privacy concerns and provides high efficiency, faster transactions, and better scalability. We can conclude from the previously said that private Blockchain satisfies all criteria for e-Voting described in the previous section.

IV. Blockchains overview

The e-Voting process must be anonymous and private, because of that, we chose Zcash and Monero, which are the most popular private cryptocurrencies, for the base of e-Voting. Below we describe how Zcash and Monero work and offer anonymity and privacy.

A. Zcash

Zcash is a privacy-protecting, digital currency built on strong science. Zcash was first released on October 28, 2016, and it was originally based on Bitcoin's codebase [2]. The Zerocash protocol is being developed into a full-fledged digital currency, Zcash. Zerocash extends the protocol and software underlying Bitcoin by adding new, privacy-preserving payments. Zcash has its unique advantage. Zcash's anonymity relies on a shielded pool, where partial transaction information such as input/output addresses and the transaction value is no more directly available from the Blockchain. Zcash is a cryptocurrency that uses advanced applied cryptography to provide enhanced privacy via shielded addresses. Zcash is the first practical application of zk-SNARKs, a specific type of zero-knowledge proof, a novel form of zero-knowledge cryptography.

zk-SNARK stands for Zero-Knowledge Succinct Non-Interactive Argument of Knowledge, and refers to a proof construction where one can prove possession of certain information, e.g. a secret key, without revealing that information, and without any interaction between the prover and verifier [3]. Zero-knowlegde proof allows the prover to prove the verifier that a statement is true, without revealing any information beyond the validity of the statement itself. Succinct means that the zero-knowledge proof can be validated within a few milliseconds, even in the case of statements related to large-scale programs. Non-interactive refers to a zero-knowledge protocol where the prover and verifier have little to no interaction. This means they can only exchange one proof. Zk-SNARKs records only the proof of the transaction on the Blockchain node, safeguarding the identity of the sender, receiver, and other details associated with the transaction.

Zcash addresses are either private (z-addresses) or transparent (t-addresses). Z addresses are private addresses and only the user can see the balance in the wallet.

Zcash has 5 types of transactions [2], we will describe only the most secure type – shielded transactions that will be used in e-voting. A shielded (private) transaction is a transaction from z-address to z-address. In these transactions, the addresses, transaction amount, and the memo field are all encrypted and not publicly visible. The fact that the transaction has happened is recorded on the ledger, but the sending and receiving addresses and the amount sent are not revealed to the public.

B. Monero

Monero is the leading cryptocurrency, launched in April 2014 and focused on private and censorship-resistant transactions. Monero transactions are confidential and untraceable. Monero is the only cryptocurrency where every user is anonymous by default. The sender, receiver, and amount of every single transaction are hidden through the use of three important technologies: Stealth Addresses, Ring Signatures, and RingCT. [4]

Stealth addresses are an important part of Monero's inherent privacy. They allow and require the sender to create random one-time addresses for every transaction on behalf of the recipient. The recipient can publish just one address, yet have all of his/her incoming payments go to unique addresses on the Blockchain, where they cannot be linked back to either the recipient's published address or any other transactions' addresses. By using stealth addresses, only the sender and receiver can determine where a payment was sent. [5]

Ring signatures are anonymous digital signatures from a member of the group, but they do not reveal which member signs the transaction. To generate a ring signature, Monero uses a combination of keys from the sender's account and links them to the public keys on the Blockchain. This makes it unique, but also private. It hides the identity of the sender, as it is computationally impossible to determine which of the group members' keys was used to produce the complex signature. [6]

RingCT, short for Ring Confidential Transactions, is how transaction amounts are hidden in Monero. RingCT introduces an improved version of ring signatures called "A Multi-layered Linkable Spontaneous Anonymous Group signature" [6], which allows for hidden amounts, origins and destinations of transactions with reasonable efficiency and verifiable, trustless coin generation. [7]

V. E-Voting implementation ideas

The implementation of e-voting, in the best case, would involve two systems that makeup one Voting system. Those would be the system at the end of the user - voter and the system at the end of the state voting organization - The voting system.

We have the Voting system (through which is implemented voting) and two parties: The voting system user (for example State Election Commission) and the Voters for implementing e-voting. In contrast to the traditional Zcash and Monero coins transaction where the user mine coins and then gets them, in e-voting, all transactions are to the Voting system user.

For an implementation based on Zcash, we use the zkSnark protocol and Shielded (private) transactions. We use this type of transaction as the most secure, because the addresses, transaction amount, and the memo field are all encrypted and not publicly visible. As we said all transactions are to the Voting system user and all voters will know that address.

For an implementation based on Monero for the transaction (exchange of the vote from the state commission to the voter and then back to the state commission, we would use Ring CT because thus the way we hide the content of the vote. The content or the vote should not be public because no one should know which person has voted, that's why we would use ring CT and thus way modify the algorithm to show only what is voted but not by who.

VI. E- VOTING PHASES

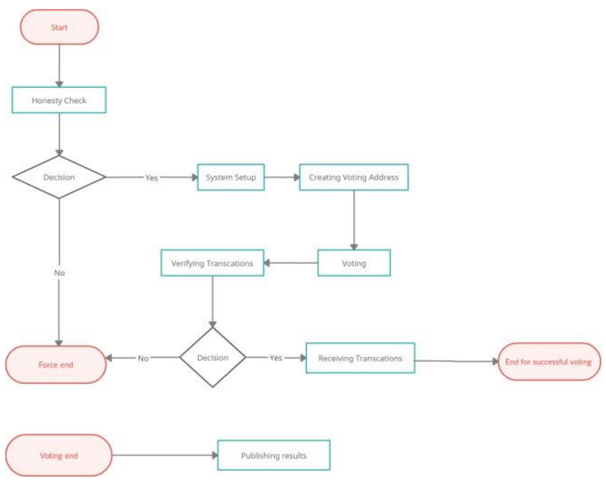

Fig. 1. E-Voting procedure

We have seven phases Honesty Check, System Setup, Creating Voting Address, Voting, Verifying Transactions, Receiving Transactions, and Publishing results. In Fig.1 we show the e-Voting procedure.

1. *Honesty Check*

We need to ensure that each voter will vote only once, because of that we store IDs of voters that voted and we start the e-voting procedure with the Honesty Check phase. In this phase we check Is the ID of the voter is in the database? If it is, that means that the voter has already voted and has no right to vote again, so the procedure ends here. Otherwise, we move on to the second phase.

2. *System Setup*

For an implementation based on Zcash, the System Setup phase is identical to the phase with the same name in Zcash coins transactions [8]. During this sub-phase, the KeyGen function samples the proving key(encrypted proving polynomial) and the verification key (encrypted target polynomial) and stores it as the output. This is done using the RSA protocol [9] by the Trusted Third Party. Next, we store these keys in the ppar string that is stored on the Blockchain, so can be easily accessed by both the prover and the verifier.

The traditional Monero implementation does not request the trusted setup, but a trusted setup is necessary for e-voting

3. *Creating Voting Address*

In Zcash based implementation Creating a Voting, Address is identical to the Creating Payment Address phase in Zcash coins transactions. Using the ECIES encryption [10] we create a public and a secret key for a single user. Following these keys are used in conjunction with a pseudo-random function to generate a public key address or public/private key address pair.

In Monero based implementation Creating Voting Address for the voters is identical to the traditional coin transaction we create random one-time addresses for every voter's transaction (if a voting transaction was not successful, the voter still have the right to vote and his voting address will be different from the previous address). For the Voting system user, we need a static unique address on which it will receive all transactions.

4. *Voting*

The Voting phase as the name suggests is voting from a voter's private address(only known by the voter), in both implementations Blockchain voting token is sent to the voter.

The input in this phase is ppar string if we use Zcash based implementation, for Monero based implementation we do not need the input. This phase in both implementations provides an output tuple that stores the vote and Voting system user. The voting phase is not executed by a Voting system user.

5. *Verifying Transaction*

In Zcash based implementation this phase has two sub-phases, first, the sub-phase is executed by a prover sub-phase, and second by a verifier. The first sub-phase is executed by a prover and takes as input the ppar string. During this sub-phase, the Prover (voter) executes the Prove function. The zk-SNARK proof has a ppar string as input for the second sub-phase. The second sub-phase is executed by a verifier and takes as input the ppar string and zk-SNARK proof which is the result from the previous sub-phase. This sub-phase is similar to Verifying Transaction phase in Zcash coins transaction with pour ledger. During this sub-phase, the Verifier executes the Verify function using the zk-SNARK proof, the public input as stored inside the transaction ledger, and the verification key (part of the ppar string). The Verify function returns a boolean value depending on whether the verifier is convinced that the prover's assertion is genuine. If the verifier is convinced of the zk-SNARK proof (and that the digital signature is valid), the Verifying Transactions phase returns TRUE. If the result is false the procedure ends here.

In Monero based implementation we create the signature for the transaction after the voting, using a random sampling algorithm, the wallet selects a set of global indexes from the histogram provided by the daemon, then the daemon will need to provide the corresponding outputs. The index of the real output is also included in the request for two reasons: as a test whether the daemon sends the correct outputs and to obfuscate the final ring signature from a curious daemon. We use the Multilayered Linkable Spontaneous Anonymous Group signature (MLSAG)[6] which is a generalization of using a key vector. The point of using a key-vector is so that a user can prove they simultaneously have knowledge of both the secret key of the input address and the secret. The above is de-facto the Verifying Transaction.

6. *Receiving Vote*

Following the TRUE result from the previous phase in both implementations, we get to Receiving Vote phase. As we said before the receiver for all voting transactions is a Voting system user. The voter used the Blockchain vote token and the voting system stores voter's username in our database .

7. *Publishing results*

Publishing results is the last phase and it is executed only once by the Voting system user when voting is officially over. The voting system user summarizes votes, adding flags to the votes once they go through counting. The results and according to the appropriate voting protocol announces the winner(s).

.

VII. Comparison between Zcash and Monero

As we discussed in the topic both Monero and Zcash provide great privacy, anonymity, and a possible framework to be made using these Blockchains for e-voting. Both of these Blockchains offer very good privacy but in realization, they are completely different. When we are on Zcash we can say that Zcash is more opt-in but on the other hand on addressing known issues Monero is more practical. As it is already discussed, we know that Monero uses Zero-knowledge proofs with actually it is in a way mathematically provable system to hide details of the transaction, transaction meaning the transfer of a vote but for sure this is not enough to consider protecting privacy. On the other hand, Monero uses older layers but those layers are better studied. Monero's layers tend to obfuscate the source of funds which are ring signatures, hide the amount (the vote in our case) which means we have a confidential transaction, and also the destination which is a stealth address. Even though their layers give extraordinary privacy, in theory, this can never be zero-knowledge, but Monero is slightly on advantage because we don't have proof that Zcash is a bug-free implementation of the theory [11]. Monero is more secure than Zcash, therefore we recommend using Monero for serious e-votings.

Conclusion

Blockchain-based e-voting is the best solution and we can conclude that from key features. No external entity can add, remove or modify votes because it is native to Blockchain technologies. With zk-SNARKs and Ring Signatures of voters, we confirm that is not possible and no one can falsify an identity using another voter identity by abusing Blockchain. Because of token fungibility, each vote is equal to the other.

References

[1] LinuxFoundationX Course, Blockchain: Understanding Its Uses and Implications, available at https://learning.edx.org/course/course-v1:LinuxFoundationX+LFS170x+2T2021/home.

[2] Official Zcash documentation,available at https://zcash.readthedocs.io/en/latest/

[3] Zcash – "What are zk-SNARKs?", available at https://z.cash/technology/zksnarks/

[4] Monero - "What is Monero (XMR)?", available at https://www.getmonero.org/get-started/what-is-monero/

[5] Moneropedia - "Stealth Address", available at https://www.getmonero.org/resources/moneropedia/stealthaddress.html

[6] Nisansala Perera, A Survey on Group Signatures and Ring Signatures: Traceability vs. Anonymity, January 2022

[7] Moneropedia - "RingCT", available at https://www.getmonero.org/resources/moneropedia/ringsignatures.html

[8] Aritra Banerjee, Michael Clear, Hitesh Tewari, Demystifying the Role of zk-SNARKs in Zcash, 2020 IEEE Conference on Application, Information and Network Security (AINS), November 2020

[9] Shireen Nisha, Mohammed Farik, RSA Public Key Cryptography Algorithm – A Review, July 2017

[10] Víctor Gayoso Martínez, L. Hernández Encinas, Carmen Sánchez Ávila, A Survey of the Elliptic Curve Integrated Encryption Scheme, January 2010

[11] Casaleggio, D., Nicola, V. D., Marchesi, M., Missineo, S., & Tanelli, R. (n.d.). A digital voting system for the 21st Century. Retrieved March 27, 2022, from https://www.strateghia.it/wp-content/uploads/FINALE-A_digital_voting_system_for_the_21th_century.pdf J. Clerk Maxwell, A Treatise on Electricity and Magnetism, 3rd ed., vol. 2. Oxford: Clarendon, 1892, pp.68–73