Data and Metadata. 2024; 3:.341
doi: 10.56294/dm2024.341

ORIGINAL

ZkSNARKs and Ticket-Based E-Voting: A Blockchain System Proof of Concept

ZkSNARKs y votación electrónica basada en tickets: una prueba de concepto del sistema Blockchain

Fatih Rabia[1], Arezki Sara[1], Gadi Taoufiq[1]

[1]Hassan First University of Settat, Faculty of Sciences and Techniques, Mathematics, Computer Science and Engineering Sciences Laboratory. Settat, Morocco.

Cite as: Rabia F, Sara A, Taoufiq G. ZkSNARKs and Ticket-Based E-Voting: A Blockchain System Proof of Concept. Data and Metadata. 2024; 3:.341. https://doi.org/10.56294/dm2024.341

Submitted: 06-02-2024 **Revised:** 02-06-2024 **Accepted:** 21-10-2024 **Published:** 22-10-2024

Editor: Adrián Alejandro Vitón-Castillo

Corresponding author: Fatih Rabia

ABSTRACT

Most existing electronic voting systems and the traditional centralized ballot management do not meet the requirements for e-voting trustworthiness today since the rate of development in science and technology is ever-increasing. Despite the blockchain-based providers designing systems that guarantee the transparency of the election, the new systems are not exempted from threats that hackers can leverage to influence the votes. This further supports the evidence presented that Blockchain based systems have progressed but there is always more that can be done especially in terms of further strengthening the transparency, security and authentications to minimize the existing risks. In order to support these vulnerabilities, we are proposing in this paper using zK-SNARK a scheme that meets the basic requirements of electronic voting and ensures the reliability and security of voting. In this scheme, a Merkle tree is used to store each voter's ticket where the ticket hash is created and registered into the tree's leaf. The voter then proves that they possess a valid ticket and are eligible to vote through zk-SNARK proof, which is very secure and efficient in verifying the voter's authenticity. This approach keeps the voting process anonymous yet allows for a fast and secure method of authenticating the voters.

Keywords: ZK-Snarks; E-Voting; Blockchain; Decentralization.

RESUMEN

La mayoría de los sistemas de votación electrónica existentes y la gestión centralizada tradicional de las papeletas no cumplen los requisitos de fiabilidad de la votación electrónica en la actualidad, ya que la tasa de desarrollo de la ciencia y la tecnología es cada vez mayor. A pesar de que los proveedores basados en blockchain diseñan sistemas que garantizan la transparencia de las elecciones, los nuevos sistemas no están exentos de las amenazas que los piratas informáticos pueden aprovechar para influir en los votos. Esto respalda aún más la evidencia presentada de que los sistemas basados en blockchain han progresado, pero siempre se puede hacer más, especialmente en términos de fortalecer aún más la transparencia, la seguridad y las autenticaciones para minimizar los riesgos existentes. Para respaldar estas vulnerabilidades, en este documento proponemos, utilizando zK-SNARK, un esquema que cumple con los requisitos básicos de la votación electrónica y garantiza la fiabilidad y la seguridad de la votación. En este esquema, se utiliza un árbol de Merkle para almacenar el boleto de cada votante, donde se crea el hash del boleto y se registra en la hoja del árbol. Luego, el votante demuestra que posee un boleto válido y es elegible para votar a través de la prueba zk-SNARK, que es muy segura y eficiente para verificar la autenticidad del votante. Este enfoque mantiene el proceso de votación anónimo y al mismo tiempo permite un método rápido y seguro para autenticar a los votantes.

Palabras clave: ZK-Snarks; Voto Electrónico; Blockchain; Descentralización.

INTRODUCTION

Blockchain technology has brought significant changes to almost all industries because of the improved methods and features of security, transparency, and execution it offers to the processes of data and transactions.[1] The shared and unalterable characteristics of blockchain make it well-suited to applications that involve large amounts of data of significant importance to the user and or third parties such as electronic voting systems.[2] Incorporation of blockchain with other state-of-art cryptographic concepts such as zero-knowledge succinct non-interactive arguments of knowledge (zk-SNARKs) further increases the privacy and security of these systems so that the confidentiality of authorities and voters' data is preserved. At the same time, voting counting remains open for verification.

Various current researches have shown how the application of the blockchain benefits to solving of significant problems in other spheres, including healthcare[3] and SCM.[4] For instance, a systematic analysis of blockchain electronic health records (EHR) identifies the ability of blockchain to improve data sharing, access, and privacy by following the General Data Protection Regulation and Health Insurance Portability and Accountability Act.[5] The study also brings into focus that more research has to be conducted in actively building blockchain applications that can fit the regulatory standards that help in the actual implementation and hence earn the trust of the stakeholders.[6]

In like manner, blockchain technology has been recommended to enable better tracking and tracing of operations in the supply chain especially in shipment departments. A case on tracking using the blockchain of containers at Moroccan ports demonstrates how blockchain makes data trustworthy, transparent, and auditable in supply chains. Challenges related to Resource allocation, together with the effectiveness and flexibility provided through the usage of blockchain in IoT devices like RFID, GPS, QR Code, et cetera, make the association between the two areas uniquely beneficial for both the practitioner and the scholar.[7]

The right to vote is considered the primary characteristic of a democratic country; it is the enfranchisement of citizens where people can choose representatives to be in the professional life, vote for cities or governments, or through elections, referenda or opinion polls.[8] Scholars have even proposed to extend the vote from hand to ballot to machine and indeed they have improved the vote but they are less efficient as they know security, privacy, fraud, and integrity issues.[9] With the rapid development of internet technology, the electronic vote has replaced the traditional one, however, unlike traditional voting methods, electronic voting is efficient, flexible and time-saving but the studies show that the utilization of electronic voting still entails the challenges of cost, security, spots of cheating, data integrity, reliability, transparency, secret voting, illiterate voters, skills in information technology.[10]

In light of the increasing implementation of blockchain technology, a number of models of electronic voting have been devised. The application of an enlightened electronic voting system through the use of blockchain technology is a noble idea for enhancing security. An approximate for an e-voting system developed using blockchain technology is the fact that a voter receives transaction IDs. A blockchain explorer and eID allow voters to check their vote on the specific election site to ensure that their vote was properly registered and counted. In this system, to prevent multiple voting and to prevent multiple tokens from getting generated for the same voter, a single voting token is issued to each eligible voter and the network rejects any further voting using the same token[11,12] developed a secure blockchain-based e-Voting system utilizing a blind signature technique to preserve the voter identity. To achieve eligibility, fairness, robustness, integrity; verifiability and vote privacy,[13] proposed the blockchain-based verifiable voting protocol that employs pairings, Identity Encryption (IBE) and Elliptic-Curve Cryptography (ECC)[14] have provided an e-voting system in which they incorporated asymmetric key cryptography together with the signature scheme and the use of blockchain.

Over the years, failures have started to emerge mainly because of the inherent problems associated with the continual enhancement of blockchain technology. While the security is reasonably high, the distributed consensus of most blockchains is prone to traffic analysis and transaction inspection; this might bring out participants' identities, particularly in cases like voting[15]. To address these threats, the existing cryptographic measures have been integrated into distributed voting systems to improve e-voting security. Out of them, zk-SNARKs have come a long way in validating itself as a beneficial technique.

The fully labeled Zero-Knowledge Succinct Non-Interactive Argument of Knowledge (zk-SNARKs) is a novel class of zero-knowledge cryptographic proofs.[16] zk-SNARKs allow proving the actual truth of a statement to a verifier without revealing the statement. This method offers an easier and faster approach to regular zk-SNARKs, as the verification process takes only a few milliseconds.[17] These proofs are typically only hundreds of bytes, even if the statement being proved is quite large.

Some works have previously studied zk-SNARKs on the blockchain, focusing on enhancing security and

efficiency[9] adopted a non-interactive zero-knowledge proof technology with Merkle tree as the means of achieving anonymity in the authentication process. To overcome this, they generated proofs off-chain, but conducted verification on-chain, to minimize the computational load's impact on the blockchain. They applied the Groth16 algorithm for the non-interactive zero-knowledge proofs. They also utilized web3.js technology to ensure the communication between the on-chain and the off-chain components is enhanced.

In another study[18] proposed a basic method for an electronic voting system that is designed to have specific essential properties including anonymity, security, correctness and other over-arching properties of the system. Through the use of blockchain technology and zk-SNARKs, they maintained the anonymity of the voters thus making it possible, secure and sound throughout the election process.

Consequently, toward improving the level of security and anonymity within E-voting systems, this paper proposes the implementation of innovative cryptographic applications, inclusive of zk-SNARKs (zero-knowledge succinct non-interactive arguments of knowledge), in combination with blockchain. Our proposed methodology entails a meticulous process: every voter's ticket is precisely logged down on a Merkle tree; in this context, the ticket hash itself becomes a node of the tree. Such a systematic approach provides a possibility to rapidly and efficiently validate ticket inclusion with the help of Merkle proofs.

Moreover, in our proposed model, the extensive use of zk-SNARK proofing allows voters to guarantee the soundness of their tickets without revealing their identity. By the creation of such proofs, the voters also confirm their own registration in the particular election ticket, the non-voting of the ticket in previous voting processes, as well as the purity of the choice made. This multiple-layered verification further strengthens the e-voting system where the identity of the voter is preserved while at the same time, the authenticity of the entire voting process is guaranteed.

The next sections in this paper will generate an outline of the methodological approach with a definite focus on the architecture as well as the constituents of the proposed model. An explanation of the voting process workflow will be provided in the results section, and the advantages of the reached and determined model will be discussed. Similarly, in the discussion part, this study will discuss the strengths and weaknesses of the proposed system and make a comparison with other refereed literature. The paper also gives recommendations for future improvement of our proposed model in the conclusion part.

METHOD

This theoretical paper puts forward a new e-voting model based on the blockchain and zk-SNARKs that would allow an electoral process that is secure, transparent, undisclosed, and maintains double voting prevention. The ultimate goal of this model is to design a voting system capable of effectively preventing such issues as voting manipulation or fraud, while keeping, at the same time the identity of voters anonymous.

This model also avails blockchain technology as the platform through which all the votes are recorded and controlled. Due to decentralization, every vote is stored in a blockchain registry accessible to all but cannot be altered by anyone. This affirms election transparency where every vote cast in the process can be validated without compromising the voter's identity.

zk-SNARKs are applied to address the privacy paradox in electronic voting systems. This technology enables one to exhibit knowledge of a value without revealing that value and without communicating with the verifier. This means that a voter can convince any verifier that he or she has the right to vote on a particular item and that the voted item is authentic without revealing the item or identity. This non-disclosure verification capability plays a vital role in the privacy and security of the voters' data.

In this work, the proposed model of electronic voting is based on blockchain technology because of its transparency and non-changeability and utilizes zk-SNARKs for the anonymity of the vote. Together, this provides a powerful protection against electoral fraud, while the identity of the voters remains concealed; thus the mentioned conditions for the security and transparency of the electronic elections are met at the highest level.

Model architecture

The proposed e-voting system incorporates zk-SNARKs into the architecture to achieve security, privacy, and accuracy. It consists of several core components that enable the voting process to be secure and anonymous at the same time.

1. Voter: stands for the various people or shareholders allowed to vote in the election. Voters interface with the system using the frontend layer, which manages inputs from users and provides outputs, for instance, registration acknowledgment, ticket creation, and vote exercising.
2. Frontend Interface: the specific touch points where the voters are able to connect with the portal. It is responsible for the management of the interaction between the voter and the back-end service, making it fast and efficient.
3. Backend Service: the components of a system that contain the actual business rules and processes that define the system as well as the data manipulation. It handles zk-SNARK proof generation, scheduling

https://doi.org/10.56294/dm2024.341

and coordinating with the smart contract to guarantee that the actions have been immutably captured on the blockchain.

4. Smart Contract: in the blockchain implementation it handles the features of voter registration, ticket check, and the vote counting besides the election protocols, votes storage, and the zk-SNARK proof validation. It also guarantees that all the votes are genuine and that the voting process follows a set procedure that has been provided in the smart contract.

5. Merkle Tree: this involves the management and the validation of the tickets as being authentic. Every ticket is associated with a leaf node in the Merkle Tree, so people's votes are anonymous while maintaining the ability to verify which people voted and when.

6. zk-SNARK Circuit: it creates zero-knowledge proofs to prove the validity of the vote without violating the voter anonymity. This component is important in making sure that voters are not identifiable while at the same time checking the authenticity of the votes.

7. Blockchain Network: supplies the structural foundation for the smart contract while guaranteeing cast votes' unalterability and openness. Thus, all the operations are recorded in the blockchain network which makes them non-tamperable and transparent.

To ensure vote validity proof, zk-SNARKs are incorporated into the system. In the voting process, voters produce zk-SNARK proofs which are checked by the smart contract on the blockchain. The integration outlined in this paper guarantees the votes received are legitimate, and yet, the voter ballots' anonymity is preserved; thus, it retains some key attributes that strengthen security, privacy, usability, and reliability of the voting process.

1. Security: the system incorporates cryptographic proofs for the voting results that a particular vote is valid through zero-knowledge proofs by withholding the voter's identity through the zk-SNARKs.

2. Anonymity: voters and their choices are unknown thus voters cannot be pressured to vote in a certain way and it is a fair contest.

3. Transparency: the incorporation of blockchain allows all the votes to be secure and counted correctly while at the same time the process of the election can be audited by the public without the compromise of voters' identity.

4. Scalability: large scale and flexibility of the system makes it capable of managing many voters and transaction across varying elections.

5. Integrity: this makes it possible to guarantee that all the votes are genuine while at the same time ascertaining that the election process follows certain laid down procedures.

The figure below illustrates the general scheme within the system:

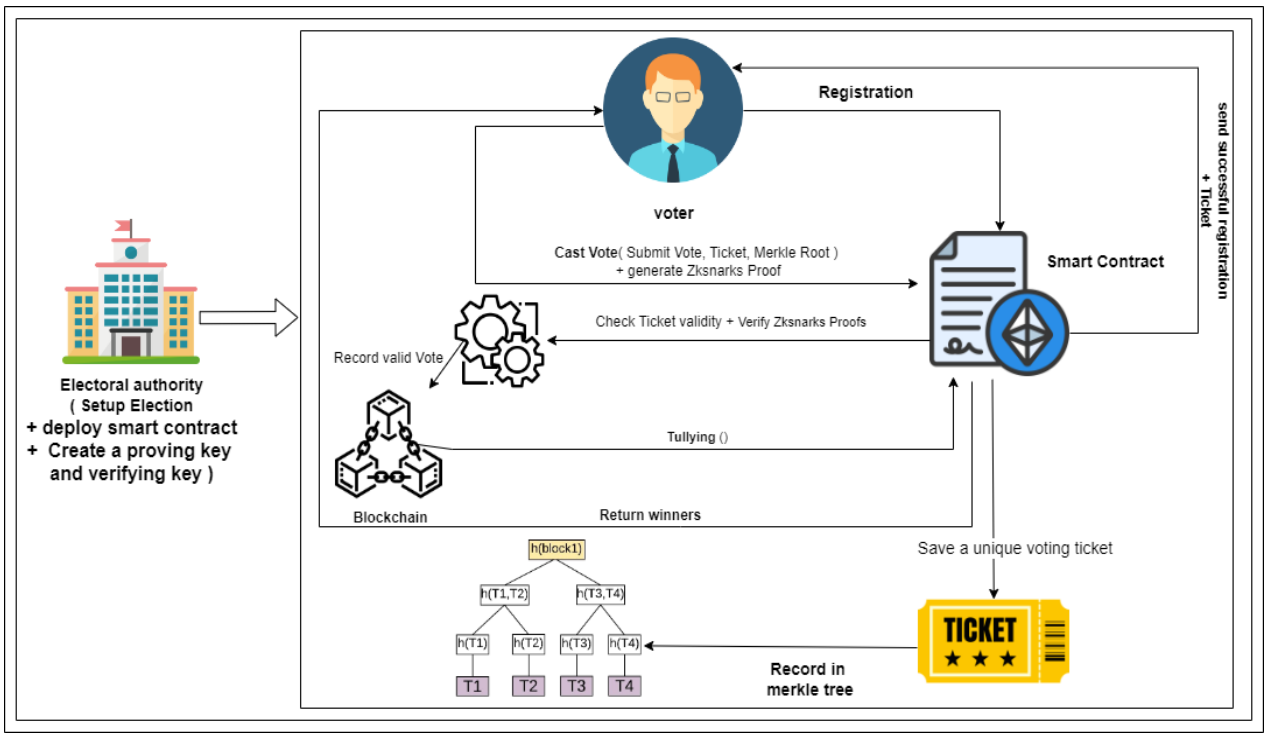

Figure 1. System architecture

https://doi.org/10.56294/dm2024.341

RESULTS

Voting process workflow

Setup Phase and Role of the Electoral Authority

The setup phase is one of the primary building blocks of the zkSNARKs-based e-voting system and the electoral authority has further responsibilities regarding the security, integrity, and, settings of the system. This phase starts with the identification of the voting circuit. The electoral authority ensure that an accurate mathematical description is formulated which contain all the conditions in order for that vote to be valid. This model entails rules for validating the eligibility of voters, checks on each vote as well as the prohibition of multiple voting, which establishes the fundamental structure that the proofs from zkSNARKs will rely on.

After the definition of the circuit the electoral authority performs a trusted setup, an important step to generate the necessary cryptographic parameters for zkSNARKs. This step is conducted in a secure environment to produce two key components: The pairs of keys involved in this process are the proving key (PK) and the verifying key (VK). The proving key is required to create zkSNARK proofs with respect to a particular relation, while the verifying key aims to confirm these proofs. The trusted setup guarantees that these keys are developed in a method that seals up the general stability of the system to threat of compromise.

After the keys are generated, the responsibility of managing and distributing cryptographic keys falls on the electoral authority. The proving key (PK) is also kept with the electoral authority and utilization of the key is done in a manner permitted by the authorities for producing zkSNARK proofs for every vote. On the other hand, the verifying key is consequently disclosed and embedded into the backend. This means that as a result of the public availability of the verifying key anyone including independent observers can perform checks on the zkSNARK proofs to verify the integrity of the voting process.

Besides, the election authority sets the official date of the election during this stage of setup. This entails entering the date of the election in the system and then advising all stakeholders most especially the voters and the candidates. The election date is a crucial factor, as it ensures that all subsequent activities are coordinated within a coherent and easily identified framework, included the registration of voters, the voting process, and the vote counting. Thus, through informing the general public of the date of the election, the election authority is certain that every participant is aware of the forthcoming election.

In general, the setup phase that belongs to the election authority is crucial to provide a properly organized e-voting. The proper definition of the circuit, the safe and proper generation and handling of cryptographic keys, and the proper announcement of the election date are the foundation upon which the correct voting process, its security, and effectiveness are constructed.

Voter Registration

In the presented zkSNARKs-based e-voting system, creating a voter profile and obtaining the right to participate in the voting process are performed through the help of a smart contract. This procedure is used to ensure that only the right voters are issued with the special voting tickets which in the course of voting are incorporated in a Merkle tree for confirmation.

Registration process starts with the voters indicted interacting with the smart contract to forward their identification registration details. In the given integrated smart contract script, the function checks the eligibility of each voter based on the information entered. In response to the verification, the smart contract save an individual voting ticket to the voter. Such tickets are electronic tokens that have the status of giving a vote in the election. Every ticket is individual and associated with a voter, so there are no situations when the same voter votes more than once.

Following the generation of the tickets, the smart contract includes the tickets in a Merkle tree data structure. The Merkle tree is a binary tree in which all the nodes of the bottom level are basically called the leaves and each of them stores hash of the block of data; all the other nodes are also hashes but the hash values stored in these nodes are computed by concatenating hash values of all the child nodes merged together. Concerning the voters' registration process, each of the leaves in the Merkle tree in the other hand represents a single voting ticket.

After Merkle tree is constructed the root hash for Merkle tree is computed. This root hash in turn becomes a favorable summary of the entire Merkle tree and is recorded on the blockchain. The approach of placing the root hash on the blockchain makes it impossible for anyone to tamper with the Merkle tree since such a change will always be reflected on the root hash.

Meanwhile, the Merkle tree incorporated in the blockchain allows for the easiest and most effective checks on the authenticity of the voting tickets during the voting process. In case a voter has at one point clicked the "voting button", they hand in their voting ticket together with a proof of their Merkle based ticket inclusion. Thus, through comparing the Merkle proof with the root hash kept within the blockchain, the system is capable of determining the authenticity of the voting ticket without the necessity to store every ticket within the blockchain.

https://doi.org/10.56294/dm2024.341

Consequently, as depicted in the system of figure 2, the voter registration in the zkSNARKs-based e-voting system is controlled by a smart contract. This process makes it possible for only eligible voters to receive what can be termed as unique voting tickets and these are included in the Merkle tree to make verification easier come the voting stage.

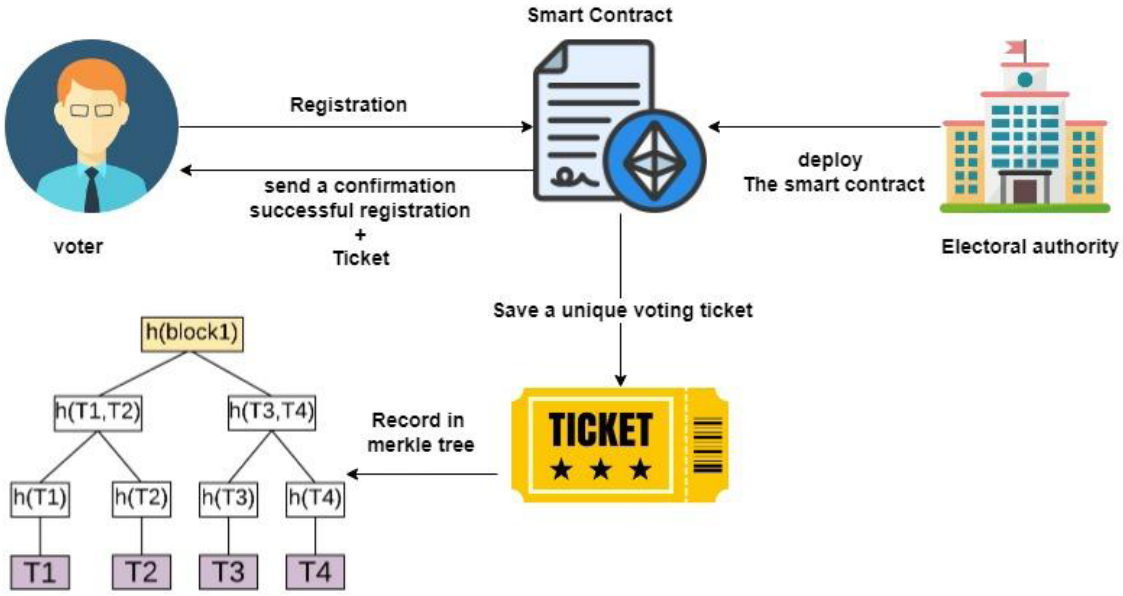

Figure 2. Registration phase

Casting Votes

As depicted in figure 3, the steps involved in the casting of votes in the zkSNARKs based e-voting system, guarantee the integrity of the voting system. It starts with the voter making their vote and sending their unique voting ticket to the backend for verification. This ticket is a non-transferable, electronic token that carries the entitlement of the voter to vote in the election.

The backend further validates the authenticity of the ticket by comparing it against the Merkle root kept on the blockchain. This Merkle root provides cryptographic proof of the validity of all the voting tickets included in the Merkle tree. If the ticket submitted is found in the Merkle tree and assessed to be a valid ticket, the process proceeds. Nonetheless, if the ticket is invalid or was used in a previous voting, the vote is nullified and the voter is informed.

After the ticket has been validated, the voter continues to the process of creating a zkSNARK proof for his vote. The proof is generated using their ticket and vote, while the proving key securely managed by the system to maintain integrity and security. Based on zkSNARK proof the voter has the ability to show the validity of a given vote without showing the vote itself. It consists of the vote, the valid ticket, and any additional identification information that might be needed in the generation of proof, such as a secret key.

After creating the zkSNARK proof, the voter sends the vote to the SC along with the valid ticket and the proof. After that, the smart contract verify snarks proof. If the proof is valid which means it gives a statement that the vote is admissible and has been made according to all regulations outlined in the voting circuit, the ticket, and proof of the vote are captured in the blockchain. This is important, as it makes certain that the vote has been properly recorded and can be verified later if needed.

If the zkSNARK proof is deemed invalid, meaning that the vote does not meet the specified standards or the proof is fake, the vote does not count and the voter receives a notification of the vote's rejection. To this end, the mentioned proof-of-voting verification is strict to ensure the e-voting system and, consequently, the blockchain is protected from invalid ballots.

Tallying votes

The last of the phases of the e-voting system based on zk-SNARKs shown in figure 4 is the tallying phase where the results are produced. In this phase, the smart contract gathers the other revealed votes that were stored at the blockchain. Because of applying zk-SNARKs, the system can confirm the integrity of the votes without disclosing the votes' privacy.

While tallying, the system utilizes the zk-SNARK proofs which were produced during the vote casting to ensure that only clean votes are taken through tallying. These proofs ensure the authenticity of each vote, the ways in which they have been cast in compliance with the rules without disclosing the voter's decision or any

other personal issues.

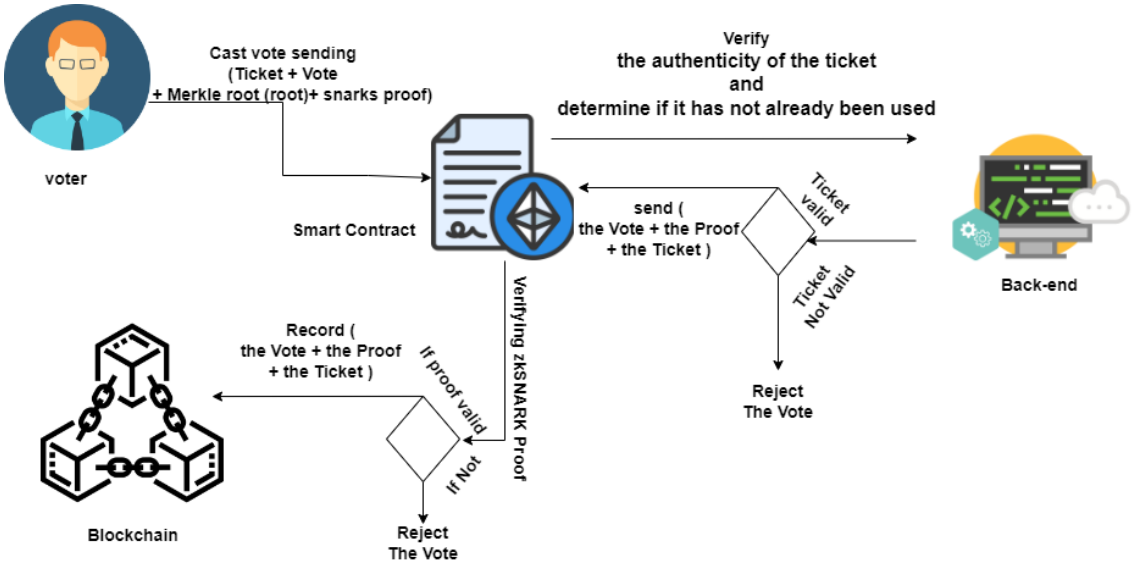

Figure 3. Cast vote phase

After all the votes have been cast and their authenticity has been confirmed, the smart contract tallies it. After this final tally is produced, it indicates to the voter the number of votes that went to a particular candidate or an option.

The utilisation of zk-SNARKs makes certain that the process retains some form of privacy since distinct data are not discernible in the process of checking the proof of correctness. Even though the platform is decentralized, the transparency that comes with blockchain makes it possible for the auditors to go through the tallying and verify that the votes were counted accurately and thereby reassuring the public about the believability of the electoral outcome.

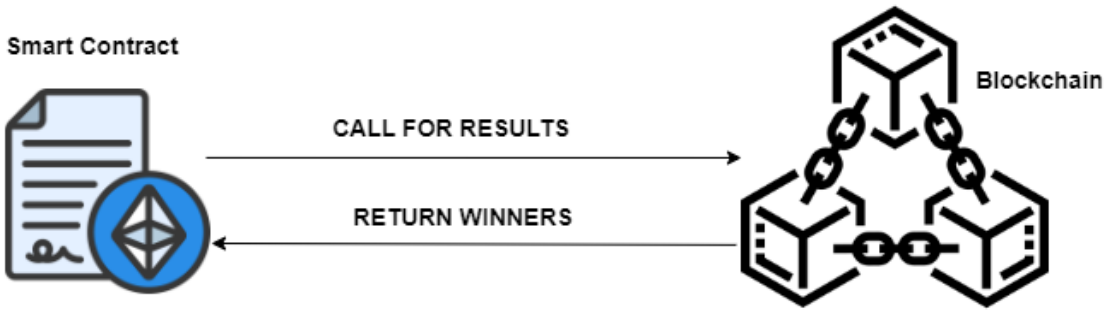

Figure 4. Tallying vote phase

Enhancing voter authentication and anonymity: key benefits of the model

The proposed e-voting system has several major advantages focusing on the improvement of security because it is crucial, particularly in verifying voters while protecting their anonymity. There are essentially two techniques that are being used to facilitate the process of authentication; they are pre-registration and cryptography. In a democracy, the potential voters, register and present relevant identification documents that will ensure that they are bona fide voters. Once participants register for voting, the smart contract saves the unique voting ticket ID for each person. The tickets are hashed and added to the Merkle tree and it assures that the identities of the concerned individuals are not disclosed during the confirmation phase.

The issue of privacy is kept intact through the use of privacy protocols called zk-SNARKs. In voting, the voters use proofs known as zk-SNARKs where they can verify that they are eligible to vote but are not able to disclose their identity or the vote made. By utilizing this cryptographic method, the system ensures that no other person can vote apart from the legitimate voter and that the voter cannot vote for more than one time. The Merkle Tree structure preserves the integrity of voter tickets safely, not connecting the tickets with voters themselves for appropriate voting with only real tickets.

Decentralized storage is also employed in the system whereby votes shall be stored in blocks. On one hand,

https://doi.org/10.56294/dm2024.341

it offers full transparency of the vote, while at the same time giving the record of votes immunity. In contrast, zk-SNARK proofs keep the identity of the voters anonymous and guarantee that votes cannot be pulled back to the same voter. The frontend interface makes it possible for the voters to interact securely and anonymously with the system, and filter all the inputs from the users without any compromise of the system's security and integrity.

Measures to verify voter identity and protect their identity prevent individuals who are not eligible to vote from influencing the results of the election, while still preserving the voters' right to anonymity. These techniques assist the voters to feel assured about the electoral process thus making it secure and personal.

DISCUSSION

The novel e-voting system that we introduce by using zk-SNARKs and Blockchain outperforms previous models in terms of the security and privacy of the voting process. At the core of our system are credible standards for the protection of voters' data, safeguarding against electoral fraud and verifying the authenticity of election outcomes. Encryption is done on all interactions that occur between the frontend interface with the backend service, and the blockchain network. This approach employs complex cryptographic technology in order to make the voters' identities and choices untraceable and immune to interception or modification.

Measures were implemented to ensure the e-voting system is secure and only approved persons can access them. Voter authentication is also a notable element as only registered voters are allowed to vote in the election. Every transaction and vote can be verified on the blockchain, making it easy to determine the results of the elections and establish credibility. One of the main characteristics of our system is the anonymity of the voters, kept safe by zk-SNARKs, which protects both the identity of the voter and his choice. One unique attribute that comes with the use of this system is the fact that there will be no opportunity for multiple voting. The unique ticketing combined with zk-SNARK proofing makes it possible to allow the voters to vote only once on each item. Furthermore, it stores records of all votes, and of all transactions implying that once a vote is cast, it cannot be changed in any way.

However, it is crucial to point out that despite the contribution of our proposed model to the solution of many issues related to e-voting, the model itself has its strengths and weaknesses. It is important to note that the use of zk-SNARKs comes with a certain amount of complexity as well as a certain level of cost. Proving generation and validation are time consuming and hence can cause an increased transaction cost on the blockchain system. Scalability is the other concern, and the proof generation process may likely take considerable time especially when dealing with a large number of voters and circuits in an election. It also comes with adoption issues whereby obtaining the zk-SNARK proofs as well as employing cryptographic methodologies might not be easily understood by the general users. Furthermore, wrong computations or accidental deletion of the Merkle tree root will allow the insertion of invalid votes.

These limitations can act as a base for further research. Optimization of zk-SNARK construction, for instance, circuit depth and proof size are possible frontiers to research. Moreover, Layer 2 options or improved zk-SNARK frameworks, such as Groth16, may contribute towards lower costs. Using Recursive SNARKs that combine several proofs in one proof could be the answer to reducing the complexity and increasing speed. One can perhaps enhance the adoption and the usage of such a paradigm by providing easily accessible interfaces and tools for creating and submitting proofs, coupled with tutorial information. Other measures that might increase the security of the Merkle tree from alteration could include decentralized storage and frequent audits of all the storage places.

A comparison of our model with other existing blockchain e-voting systems demarcates its distinctive developments. For example,[19] study recommends a mixed approach where part of the identity authentication is using zk-SNARKs while the rest is done on-chain and off-chain. While they focuse on remaining cost-efficient and connecting through Layer 2 networks like Polygon, our model aims at a larger scale flexibility across different environments. As stated, [9]approach of applying zk-SNARKs together with Merkle tree technology is aimed at solving key issues of the current e-voting systems such as the possibility of a single point of failure and the possibility of manipulation of the voted data. While their model guarantees privacy and data security and integrity, our system is a more friendly step additionally increases the level of voter's trust and the system's transparency. Further,[18] focus on access and equity through the use of zk-SNARKs to keep the voters' identities private without needing a trusted third party. Whereas they recommend flexibility for the easy implementation of the system by non-technical users, our model includes extra layers of security that help protect against possible risks, such as the 51 % attack, by the integration of sophisticated cryptographical elements. However, each one of these models has provided useful recommendations in the development of secure e-voting systems; this model adds to the accomplishments of these models by presenting an elastic, secure, and user-centric voting system.

https://doi.org/10.56294/dm2024.341

CONCLUSIONS

The proposed zkSNARKs-based e-voting system can address securely and efficiently the problems of secure electronic voting. Through the use of zero-knowledge proofs and blockchain, it is possible to preserve the identity of the voters, the results and check against multiple or fraudulent votes, yet the process can be seen and monitored freely. Tickets and zkSNARKs make it possible to inspect the votes and confirm their correctness and origin. Still, the voters' identity cannot be exposed, further strengthening the vote's security.

With the help of zkSNARKs, our system exhibits the possibility of building effective and safe e-voting systems that can evolve in the future. Thus, contributing to enhancing the reliability of electronic voting systems where the implementation of the presented model could be useful for different election contexts.

This paper provided the conceptual model for a voting system based in zk-SNARKs Blockchain which could be the foundation for a more secure private efficient and fast voting. The schemes and workflows introduced in this paper are enough to give a clear idea about the possibilities of implementing the proposed model. However, though this paper emphasizes the theoretical aspect of the model, the procedures for its application and the further investigation of the model's functioning will be covered in the subsequent paper. This future work will try to prove the efficiency of the proposed model in real life, addressing the challenges of practical implementation and improving the proposed system's stability.

REFERENCES

1. Idrees SM, Nowostawski M, Jameel R, Mourya AK. Security aspects of blockchain technology intended for industrial applications. Electronics. 2021;10(8):951.

2. Tanwar S, Gupta N, Kumar P, Hu YC. Implementation of blockchain-based e-voting system. Multimed Tools Appl. 2024 Jan;83(1):1449–80.

3. Liu G, Xie H, Wang W, Huang H. A secure and efficient electronic medical record data sharing scheme based on blockchain and proxy re-encryption. J Cloud Comp. 2024 Feb 15;13(1):44.

4. Azzi R, Chamoun RK, Sokhn M. The power of a blockchain-based supply chain. Computers & industrial engineering. 2019;135:582–92.

5. Ma S, Zhang X. Integrating blockchain and ZK-ROLLUP for efficient healthcare data privacy protection system via IPFS. Scientific Reports. 2024;14(1):11746.

6. Ettaloui N, Arezki S, Gadi T. An Overview of Blockchain-Based Electronic Health Record and Compliance with GDPR and HIPAA. In: Farhaoui Y, Hussain A, Saba T, Taherdoost H, Verma A, editors. Artificial Intelligence, Data Science and Applications [Internet]. Cham: Springer Nature Switzerland; 2024 [cited 2024 Jul 21]. p. 405-12. (Lecture Notes in Networks and Systems; vol. 838). Available from: https://link.springer.com/10.1007/978-3-031-48573-2_58

7. Nasih S, Arezki S, Gadi T. Blockchain Technology for tracking and tracing containers: model and conception. Data and Metadata. 2024;3:373–373

.

8. Taş R, Tanrıöver ÖÖ. A manipulation prevention model for blockchain-based e-voting systems. Security and communication networks. 2021;2021:1–16.

9. Tang W, Yang W, Tian X, Yuan S. Distributed anonymous e-voting method based on smart contract authentication. Electronics. 2023;12(9):1968.

10. Esteve, J.B.; Goldsmith, B.; Turner, J. International Experience with E-Voting. Available online: https: https://www.parliament.uk/documents/speaker/digital-democracy/IFESIVreport.pdf

11. Hardwick FS, Gioulis A, Akram RN, Markantonakis K. E-voting with blockchain: An e-voting protocol with decentralisation and voter privacy. In: 2018 IEEE International Conference on Internet of Things (iThings) and IEEE Green Computing and Communications (GreenCom) and IEEE Cyber, Physical and Social Computing (CPSCom) and IEEE Smart Data (SmartData) [Internet]. IEEE; 2018 [cited 2024 Jun 1]. p. 1561–7. Available from: https://ieeexplore.ieee.org/abstract/document/8726645/

12. Liu Y, Wang Q. An e-voting protocol based on blockchain. Cryptology ePrint Archive [Internet]. 2017 [cited 2024 May 28]; Available from: https://eprint.iacr.org/2017/1043

13. Chaieb M, Yousfi S, Lafourcade P, Robbana R. Verify-Your-Vote: A Verifiable Blockchain-Based Online Voting Protocol. In: Themistocleous M, Rupino Da Cunha P, editors. Information Systems [Internet]. Cham: Springer International Publishing; 2019 [cited 2024 May 28]. p. 16–30. (Lecture Notes in Business Information Processing; vol. 341). Available from: http://link.springer.com/10.1007/978-3-030-11395-7_2

14. Adiputra CK, Hjort R, Sato H. A proposal of blockchain-based electronic voting system. In: 2018 second world conference on smart trends in systems, security and sustainability (WorldS4) [Internet]. IEEE; 2018 [cited 2024 May 28]. p. 22–7. Available from: https://ieeexplore.ieee.org/abstract/document/8611593/

15. Wang H, Wang Y, Cao Z, Li Z, Xiong G. An overview of blockchain security analysis. In: Cyber Security: 15th International Annual Conference, CNCERT 2018, Beijing, China, August 14–16, 2018, Revised Selected Papers 15 [Internet]. Springer Singapore; 2019 [cited 2024 Jun 1]. p. 55–72. Available from: https://library.oapen.org/bitstream/handle/20.500.12657/23271/1006885.pdf?sequence=1#page=61

16. Ben-Sasson E, Chiesa A, Tromer E, Virza M. Succinct {Non-Interactive} zero knowledge for a von neumann architecture. In: 23rd USENIX Security Symposium (USENIX Security 14) [Internet]. 2014 [cited 2024 Jun 1]. p. 781–96. Available from: https://www.usenix.org/conference/usenixsecurity14/technical-sessions/presentation/ben-sasson

17. Koens T, Ramaekers C, Van Wijk C. Efficient zero-knowledge range proofs in ethereum. ING, blockchain@ing com [Internet]. 2018 [cited 2024 Jun 1]; Available from: http://www.zyxec.ee/zero-knowledge-range-proof-whitepaper.pdf

18. Murtaza MH, Alizai ZA, Iqbal Z. Blockchain based anonymous voting system using zkSNARKs. In: 2019 International Conference on Applied and Engineering Mathematics (ICAEM) [Internet]. IEEE; 2019 [cited 2024 Jun 1]. p. 209–14. Available from: https://ieeexplore.ieee.org/abstract/document/8853836/

19. Marcellino M, Wicaksana A, Widjaja M. Zero-knowledge Identity Authentication for E-voting System.

FINANCING

The authors did not receive financing for the development of this research.

CONFLICT OF INTEREST

The authors declare that there is no conflict of interest.

AUTHORSHIP CONTRIBUTION

Conceptualization: Fatih Rabia; Arezki Sara; Taoufiq Gadi.
Research: Fatih Rabia; Arezki Sara; Taoufiq Gadi.
Drafting - original draft: Fatih Rabia; Arezki Sara; Taoufiq Gadi.
Writing - proofreading and editing: Fatih Rabia; Arezki Sara; Taoufiq Gadi.