Trustless Infrastructure for decentralised applications using zero knowledge protocols

Abhishek S [1], Aditya Shanbhag [1], Sachit Girish [1], Vignesh R S [1], Dr. Manjunatha P B [2]
[1] *Department of Artificial Intelligence and Machine Learning, Bangalore Institute of Technology, Bangalore*
[2] *Assistant Professor, Department of Artificial Intelligence and Machine Learning, Bangalore Institute of Technology, Bangalore*

Abstract— In this article, a pioneering approach to private voting on the blockchain is introduced. This method incorporates an anonymous authentication system based on Zero-knowledge Proof (ZKP) technology. The proposed strategy involves the development of a Solidity smart contract responsible for managing and executing the private voting process on the blockchain. Specifically, the framework enables designated voters to anonymously submit their votes while their identities are verified using ZKP. The authentication process occurs locally on the voter's device, with only the verification phase conducted on the blockchain to reduce computational burden. Within the smart contract, a verifier is implemented to validate the anonymous authentication proof provided by each voter. If the proof is deemed valid, the voter's anonymous vote is registered and stored securely. This innovative solution represents a significant advancement in the realm of private voting on blockchain platforms, offering potential benefits for bolstering transparency, security, and privacy within electoral systems.

Keywords—authentication, identity, zero-knowledge, zero knowledge-proof, smart contract.

I. INTRODUCTION

Voting systems have been the subject of active research for decades with the aim of minimizing the cost of holding a voting process, keeping anonymous and confidential the identity of eligible people to participate in the voting[1]. In recent years, blockchain technology has been integrated into electronic voting, often referred to as digital voting. Leveraging blockchain platforms and smart contracts enhances the security of voting data. Additionally, many blockchain voting systems prioritize user privacy, thereby increasing the anonymity of participants in the voting process.

Consider a scenario where an institution seeks to gauge the popularity of films nominated for theatrical release or a talent competition aims to rank contestants through audience voting. However, such systems may face challenges from individuals attempting to manipulate the outcome by submitting fraudulent votes or engaging in multiple voting attempts. Consequently, the need arises for mechanisms within blockchain voting systems to mitigate such behaviors.

Combining blockchain, digital voting, and zero-knowledge proof technologies offers a potential solution to authenticate participants anonymously prior to voting. This approach simplifies the authentication process and prevents malicious users from exploiting the system. Digital voting, facilitated by blockchain technology, ensures immutable recording and maintenance of election results. This can be achieved through the implementation of specialized blockchains for voting or by utilizing blockchain features like smart contracts. A successful digital voting system should enable easy authentication of voters, accessibility from any location, affordability, and restrict participation to authorized individuals.

Digital voting is a type of voting that uses blockchain technology as a ledger to record and maintain election results that cannot be changed. This work can be done and implemented in two ways, 1) a special blockchain is implemented for voting, which brings limitations that must be addressed and resolved in order to improve the security of voting, 2) the other way is to use blockchain features such as smart contract support, in such a way that a smart contract is embedded and people who intend to vote can easily refer to the contract and register their vote. A digital voting system should be able to: 1) facilitate the authentication of people authorized to vote, 2) be usable from any place, 3) be cheap or free to use, 4) only authorized people can participate in voting. Among the advantages of digital voting, it is possible to vote online and remotely without the need to wait in line for a long

time, as well as the most important feature of digital voting, voting anonymously. By assigning a public address to people, blockchain allows people to participate in voting anonymously, but today, with the development and emergence of different blockchains and the implementation of new features, such as the possibility of adding people's identities on the blockchain, or blockchain exploration tools that are used to record the number, type and time of transactions made on blockchain has caused that by assigning a public key to a person, the person's anonymity is not guaranteed in the blockchain[2], also, a digital voting should be implementable on all blockchains that support Solidity smart contract to increase the usability of this framework. For this purpose, a technology such as zero knowledge proof can be used to authenticate voters in digital voting. With the help of this technology, any person authorized to participate in voting can participate in voting with any address (public key) on the blockchain without the identity of the voter being revealed, because the identity of people is independent of their public address on the blockchain.

Despite the advantages of digital voting, concerns regarding anonymity persist due to evolving blockchain features and tools for transaction analysis. To maintain anonymity, digital voting systems should ideally be deployable across all blockchains supporting Solidity smart contracts. Zero-knowledge proof (ZKP) is an interactive verification protocol that enables verification of secret data without revealing private information. An advanced form of ZKP, called zero-knowl edge succinct non-interactive argument of knowledge (zkSNARK), improves upon this mechanism by reducing the proof size and simplifying verification. The implementation of this protocol does not require a complex process, and it will not be useful for a malicious user to repeatedly perform authentication operations in order to obtain additional useful information[3].

II. RELATED WORK

Now we take a look at the researches done in the field of digital voting, we analyze and examine them to find out the difference between the conducted research.

A. *Votium*

A voting framework on the blockchain that provides the possibility of participating in anonymous voting. This framework uses zero knowledge proof and smart contract system to conduct anonymous voting in such a way that people can be added to the voting using their public blockchain address but from another fixed address that is available in the framework to perform the vote registration transaction.

B. *E-Voting*

It proposes a blockchain-based e-voting system that addresses some of the limitations of existing systems and evaluates some popular blockchain frameworks for building a blockchain-based e- voting system. Specifically, it assesses the potential of distributed ledger technologies through the description of a case study. That is, the process of an election and the implementation of a blockchain-based program that improves security and reduces the cost o f hosting an election.

C. *Follow My Vote*

Follow My Vote is an open-source blockchain-based voting system that offers end-to-end verifiability and security. The system uses a combination of public and private keys to ensure that each voter can only vote once and that their vote is encrypted and kept confidential. The system also allows for real-time vote counting and results reporting, making it faster and more efficient than traditional voting systems.

D. *Horizon State*

Horizon State is another blockchain-based voting system that offers end-to-end verifiability and security. It uses smart contracts to ensure that votes are recorded accurately and that results are transparent and tamper-proof. The system also offers a range of additional features, such as secure voter identification and real-time vote counting, making it a robust and reliable option for digital voting.

F. SecureVote

SecureVote is a blockchain-based voting system that offers end-to-end verifiability and security. It uses smart contracts to ensure that votes are recorded accurately and that results are transparent and tamper-proof. The system also offers a range of additional features, such as secure voter identification and real-time vote counting, making it a robust and reliable option for digital voting.

Overall, these research studies have shown that blockchain-based digital voting systems have the potential to provide secure, transparent, and efficient ways of conducting elections. However, there are still

challenges to be addressed, such as ensuring voter privacy and preventing tampering of votes.

III. PROBLEM STATEMENT

The current voting process is plagued by numerous challenges that compromise the accuracy, legitimacy, and security of the voting results. These challenges include issues of reliability, transparency, and privacy. Instances of voter fraud and manipulation, along with concerns regarding the security and integrity of electronic voting systems, have raised doubts about the fairness of the voting process. Moreover, traditional voting systems often rely on centralized authorities, which not only restrict access and participation but also leave them vulnerable to corruption and manipulation.

The research proposes a smart contract-based voting system on the blockchain, utilizing zero-knowledge proofs (ZKPs) to address challenges like reliability, transparency, and privacy in traditional voting systems. ZKPs enable anonymous verification of voter identity while safeguarding personal information. The system aims to ensure fairness and accuracy by integrating ZKP authentication with private voting on Ethereum, thus ensuring immutability of results. Challenges such as compatibility, scalability, and security are acknowledged and addressed through innovative elements like imposing a minimal cost requirement to deter fraudulent activities. Overall, the system aims to enhance the reliability, transparency, and inclusivity of the voting process by leveraging ZKP technology and blockchain.

However, developing a smart contract-based voting system presents its own set of challenges, primarily due to the diversity of blockchain languages, rules, and restrictions. Compatibility issues arising from various blockchains need to be addressed during the development and implementation of the system. Additionally, scalability, efficiency, and security are crucial aspects that demand attention to ensure a successful voting process on the blockchain. Transaction speed, network congestion, and the prevention of attacks and manipulation attempts are key factors that must be carefully considered. The proposed system incorporates innovative elements to tackle these challenges effectively. First, the use of ZKPs for anonymous authentication of voters introduces transparency and reliability to the voting process while preserving the privacy and anonymity of participants. By implementing ZKPs, the system ensures that only eligible voters can engage in the voting process without compromising their identities.

IV. SYSTEM MODEL

Digital voting represents an innovative approach to voting that leverages blockchain and smart contract technology to enable eligible voters to cast their votes without revealing their identities. In this section, we outline the various components of the digital voting system and elucidate how they operate in conjunction.

The digital voting system comprises three primary components:

- The digital voting's smart contract
- The authentication using Zero-knowledge proof
- The user interface

A. *Overview*

Consider a private voting system, where voters can publicly register their votes while keeping their identities hidden. This type of voting system is specifically designed for scenarios such as elections involving representatives, where the representatives are known by a select group of individuals known as "people concerned." The primary objective of the Z-Voting project is to ensure the anonymity of these representatives when submitting their votes.

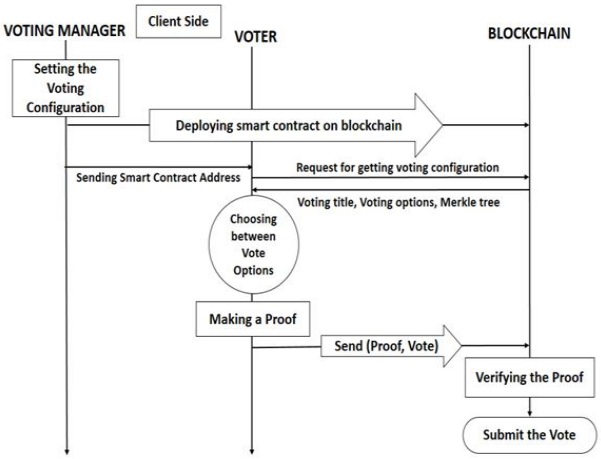

Fig1. Interactions between users and blockchain

In this system, authentication refers to the process of verifying that a person is a member of the eligible individuals who can participate in the voting, without disclosing their identity. The authentication process must be conducted securely, and the blockchain provides a secure environment for processing this authentication.

However, conducting processing operations on the blockchain can be costly, particularly for complex operations. To mitigate costs while maintaining security, the Z-Voting system implements a zeroknowledge-proof encryption mechanism as the authentication method. This mechanism utilizes a smart contract on the blockchain as the verifier and the voter's machine as the prover.

The prover, in this case, refers to the voter who wishes to participate in the voting. Their responsibility is to convince the verifier, represented by the smart contract, by constructing a proof of their eligibility to participate in the voting. The proof must be verifiable to prevent malicious actors from generating fraudulent proofs and illegitimately participating in the voting process.

To ensure a cost-effective and secure authentication process, the Z-Voting system leverages the computational capabilities of the voter's machine. The processing and creation of the authentication proof are performed on the voter's machine. This proof serves as evidence that the individual has successfully authenticated their identity, meeting the predetermined conditions for eligibility in a particular vote.

In the Z-Voting system, a dedicated section is required within the digital voting process to validate the authentication proofs provided by the voters. Once the proofs are approved, the individuals are authorized to register their votes. This model of authentication can be implemented as a zero-knowledge-proof encryption system. Under this system, voters generate their authentication proofs according to predefined conditions and transmit these proofs to the voting smart contract on the blockchain. After the smart contract verifies the authenticity of the proofs, the voters are allowed to register their votes.

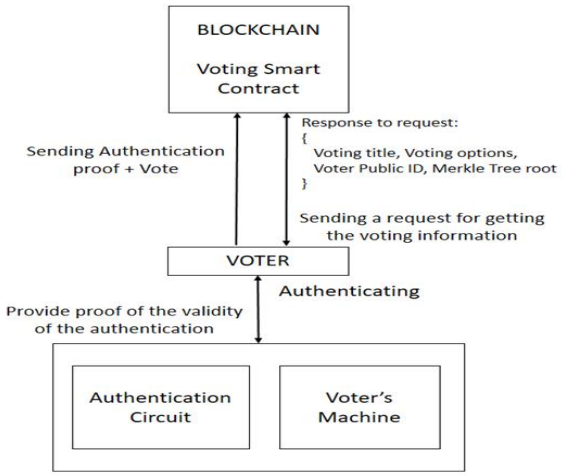

Fig2. Overview of Authentication and Voting process

It is important to note that since voting is conducted on the blockchain, and each voting process involves its unique set of participants, a unique approver is required for each voting instance. Additionally, the authentication verification process takes place on the blockchain, providing benefits such as immutability and tamper resistance, which ensure the security of the authentication process. The computational requirements for authentication are minimal, resulting in negligible costs for the voters.

B. *Voting Key Pair*

The logic used to build an anonymous authentication system is very simple. Since public and private key pairs are used in the blockchain, any person with the private key can create the public key, so, to prove authentication, the person in question only needs to have the private key and extract the public key from the private key by performing a secure process. Now, since in different blockchains, the method of encryption and extracting the public key from the private key are different from one another, and also to increase the usability of this anonymous voting framework in different blockchains, in the proposed anonymous authentication system, each person who intends to participate in the voting process is assigned a VotingID, this VotingID is generated by an expression called the VotingKey, which is a set of random words, using the Pedersen hash function (similar to the addresses on the blockchain that are made from a private key and a public key).

The VotingID is a public address that can be made available to the public, but the VotingKey is a private key and a person should not share this key with anyone under any circumstances. Another advantage of using a pair of keys (voting ID, voting key) is that voters

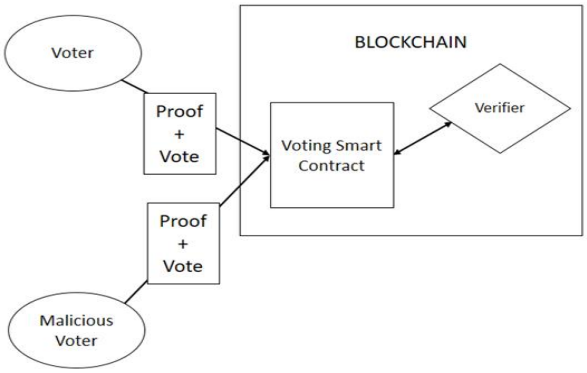

Fig3. The overview of sending proof and vote to the smart contract will not have to use a specific address on the

blockchain to register their vote and can use any address on the blockchain to participate in voting. We will learn more about the reason for this later.

C. *Anonymous Authentication*

Authentication involves verifying participants' eligibility in the private voting framework while preserving voter privacy. To achieve this, authentication processing occurs on the voter's device. Verifiability of authentication is ensured through zero-knowledge proof cryptography, with the voter acting as the prover and the private voting framework as the verifier.

To initiate the voting process securely, a designated individual known as the Voting Manager collects the VotingIDs of eligible participants and initiates the authentication system. Subsequently, the voting information and verifier are transmitted to the blockchain through a transaction, commencing the voting process. Upon the voting contract's registration on the blockchain, eligible voters access the contract to cast their votes. They create authentication proofs based on the voting information and submit these proofs to the contract for validation using the embedded verifier.

The authentication process is implemented using the Circom language to construct a circuit that accepts input parameters such as the list of public VotingIDs, the Merkle tree root, the voter's VotingKey, and the index of the public VotingID. The circuit generates the voter's VotingID from their VotingKey using the Pedersen hash function. This generated VotingID is compared with the list of public VotingIDs, and if the conditions are met, a Nullifier is outputted. The Nullifier indicates successful authentication.

After producing the Nullifier, the zero-knowledge proof system creates a proof of the processing and output of the circuit. The voter submits this proof to the voting smart contract, where the embedded verifier validates it. Upon approval, the voter's vote and Nullifier are recorded on the smart contract.

The prover/Voter:

```
Function Authentication ({
    VotingKey,
    MerkleTreeRoot,
    index,
     Voters' list})
   {
      Var VotingID = PedersenHashFunction
(VotingKey);
      Voters' list[index] = VotingID;
      Var NewMerkleTree = makeTree (Voter' list);
      if (MerkleTreeRoot == NewMerkleTree)
      {
          Return True;
      }
      else
      {
          Return False;
      }
   }
```

Pseudo Code 1. Authenticating and making proof

The Verifier/Digital Voting smart contract:

```
Function Vote ({
    Proof,
    Vote})
  {
    Require (Verify (Proof));
    if (Nullifier.doesNotRegisteredAlready)
    {
        Submit (Vote);
    }
    else
    {
        Return 'You have already voted'
    }
 }
```

Pseudo Code 2. Verifying proof and submitting vote

D. *Wallets and Account's Address*

All transactions on the blockchain are signed by the sender's address and broadcast on the network, including votes. To cast a vote, the sender's account address is used to initiate a transaction on the blockchain. The unique advantage of the proposed anonymous authentication system is that voters are not required to use a specific address. This is possible because of the ability to register identities on the blockchain through multiple blockchains, such as the Polkadot blockchain. As a result, voters do not need to use the address associated with their true identity. The anonymous authentication system uses a different method for authentication compared to the blockchain address.

IV. PERFORMANCE EVALUATION

The anonymous authentication system is a pivotal component of the private digital voting framework. To implement this framework, we utilized Solidity for

developing the voting smart contract, Circom for creating the authentication circuit and generating proofs, and JavaScript for crafting the user interface to enhance user experience. To evaluate the performance of the private digital voting framework, we conducted tests on popular blockchains that support Solidity, such as Ethereum, Moonbeam, and Tron, focusing on several key aspects:

Privacy: Preserving privacy is fundamental to the private digital voting framework, allowing voters to cast their votes anonymously. However, voters must adhere to specific guidelines to safeguard their anonymity, as discussed in previous sections. It's crucial to avoid using accounts that allow identity registration on the blockchain to ensure anonymity. Moreover, the unique Nullifier generated for each vote prevents the identification of voters by intercepting Nullifier values across different voting sessions.

Fees: Fee rates vary across different blockchains, with no fixed rate applicable universally. Additionally, storing information on the blockchain incurs costs, and the expense increases with more participants in the voting process.

Delay: The delay refers to the time required for authentication and proof creation, influenced by factors such as the processing power of the voting machine and the number of eligible voters. As the number of eligible voters increases, so does the time required for authentication and proof creation.

Number of messages exchanged: Assessing the number of messages exchanged is crucial for evaluating the private digital voting framework. During voter registration, communication with the smart contract involves obtaining information such as the voting title, voters list, and Merkel tree root. No cost is incurred for retrieving information from the blockchain. Each vote registration involves a single transaction on the blockchain, minimizing the exchange of messages.

V. CONCLUSION AND FUTURE IMPROVEMENTS

Implementing a secure and reliable digital voting system necessitates the development of a smart contract compatible with various blockchains and possessing specific characteristics such as low processing power and data storage volume. By adhering to specific coding structures and avoiding unnecessary information processing in the smart contract, it can be registered and implemented across all blockchains supporting Solidity smart contracts.

Merkle trees are crucial for ensuring the security and authenticity of digital voting. By incorporating the Merkle tree root obtained from eligible voters into the smart contract, the likelihood of verifying fake proofs by the Verifier is significantly reduced. Several enhancements can be made to the digital voting system:

1. Stop function: This function allows the voting manager to stop voting, for example, consider the situation when the number of votes obtained has reached the required quorum and there is no need for the votes of others, in this case, the voting manager will be able to terminate the voting by calling this function.

2. Parent smart contract: Creating a mother smart contract in such a way that a child contract is created by the mother contract to start a voting, and the address of the child contract is stored in the mother contract, in this case, the mother contract becomes a ledger that allows people to see all the voting done, the number of votes adopted, etc. in it. It should be noted that each of the smart contracts will be a child of an independent digital voting and there is no commonality except in the body and logic used in digital voting.

3. Fee-Free vote registration: The possibility of making digital voting fee-free in such a way that a sufficient amount of fees needed to register the vote of eligible people is sent to the address of the smart contract by the Voting manager and after the voter is authenticated and in the condition that he has not registered his vote before. The vote registration transaction fee should be paid by the smart contract.

By implementing these improvements and maintaining strict coding structures, digital voting can become a more accessible and secure method of democratic decision-making.

REFERENCE

[1] Hjálmarsson, F.Þ., et al. – "*Blockchain-based e-voting system*", *2018 IEEE 11th international conference on cloud computing (CLOUD)*, 2018.

[2] Yu, H., Z. Yang, and R.O. Sinnott, - "*Decentralized big data auditing for smart city environments leveraging blockchain technology",* IEEE Access, 2018.

[3] Bao, Z., B. Wang, and W. Shi. – "*A privacy-preserving, decentralized and functional bitcoin e-*

voting protocol. in *2018 IEEE SmartWorld, Ubiquitous Intelligence & Computing, Advanced & Trusted Computing, Scalable Computing & Communications, Cloud & Big Data Computing, Internet of People and Smart City Innovation",*2018.

[4] Chi, Po-Wen, Y.H. Lu and A. Guan - *"A Privacy-Preserving Zero-Knowledge Proof for Blockchain,"* in IEEE Access, vol. 11, 2023.

[5] M. Dieye - *"A Self-Sovereign Identity Based on Zero-Knowledge Proof and Blockchain,"* in IEEE Access, vol. 11, 2023.

[6] B. Chavali, S. K. Khatri and S. A. Hossain - *"AI and Blockchain Integration"*, 2020 8th International Conference on Reliability, Infocom Technologies and Optimization (Trends and Future Directions) (ICRITO), Noida, India, 2020.

[7] M. Wöhrer and U. Zdun - *"Domain Specific Language for Smart Contract Development"* 2020 IEEE International Conference on Blockchain and Cryptocurrency (ICBC), Toronto, ON, Canada, 2020.

[8] A. W. Abreu and E. F. Coutinho - *"Motivating Web and Blockchain Application Modeling"*, 2020 IEEE International Conference on Software Architecture Companion (ICSA-C), Salvador, Brazil, 2020.

[9] Y. C. Tsai, R. Tso, Z. -Y. Liu and K. Chen - *"An Improved Non-Interactive ZeroKnowledge Range Proof for Decentralized Applications"*, 2019 IEEE International Conference on Decentralized Applications and Infrastructures (DAPPCON), Newark, CA, USA, 2019.

[10] Z. Wang, L. Yang, Q. Wang, D. Liu, Z. Xu and S. Liu - *"ArtChain: Blockchain Enabled Platform for Art Marketplace"*, 2019 IEEE International Conference on Blockchain (Blockchain), Atlanta, GA, USA, 2019.

[11] A. R. Yadlapalli, N. Mohite, V. Pawar and S. Sachdeva - *"Artificially Intelligent Decentralized Autonomous Organization"*, 2019 4th International Conference on Information Systems and Computer Networks (ISCON), Mathura, India, 2019.

[12] S. Wang, L. Ouyang, Y. Yuan, X. Ni, X. Han and F. -Y. Wang - *"Blockchain-Enabled Smart Contracts: Architecture, Applications, and Future Trends"*, in IEEE Transactions on Systems, Man, and Cybernetics: Systems, 2019.

[13] R. Taş and Ö. Ö. Tanrıöver - *"Building A Decentralized Application on the Ethereum Blockchain"*, 2019 3rd International Symposium on Multidisciplinary Studies and Innovative Technologies (ISMSIT), Ankara, Turkey, 2019.

[14] J. D. Harris and B. Waggoner - *"Decentralized and Collaborative AI on Blockchain"*, 2019 IEEE International Conference on Blockchain (Blockchain), Atlanta, GA, USA, 2019.

[15] F. Wessling and V. Gruhn - *"Engineering Software Architectures of BlockchainOriented Applications"*, 2018 IEEE International Conference on Software Architecture Companion (ICSA-C), Seattle, WA, USA, 2018.

[16] W. Cai, Z. Wang, J. B. Ernst, Z. Hong, C. Feng and V. C. M. Leung - *"Decentralized Applications: The Blockchain-Empowered Software System"*, in IEEE Access, 2018.

[17] M. Wohrer and U. Zdun - *"Smart contracts: security patterns in the Ethereum ecosystem and solidity"*, 2018 International Workshop on Blockchain Oriented Software Engineering (IWBOSE), Campobasso, Italy, 2018.

[18] J. Eberhardt and S. Tai - *"ZoKrates - Scalable Privacy-Preserving Off-Chain Computations"*, 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), Halifax, NS, Canada, 2018.