Shiraz University

Large-scale and Semi-anonymous E-voting System Based on Ethereum Network Blockchains

Mohsen Raji*
School of Electrical and Computer Engineering, Shiraz University, Shiraz, I.R. Iran

Vahid Ghareghani† and Sayed Ali YaghoubNejad‡
B.Sc, School of Electrical and Computer Engineering, Shiraz University, Shiraz, I.R. Iran
(Dated: September 26, 2021)

Abstract:

Traditional voting (paper voting) is a conventional way to take people's opinions into action and bring democracy. However, this system requires tons of paper and it is quite expensive. On the other hand, electronic voting (E-Voting) systems are considered as an alternative to paper-ballot-based voting which provides cost efficiency and speed and eliminates human error but computer-based systems are vulnerable to malicious actions such as cyber-attacks and the security of E-voting systems are in question. The answer to the security issues is to use a decentralized platform such as blockchains (in this case Ethereum platform) to solve the single point of failure problem and maintain the voting process robustly. nevertheless, the transactions on Ethereum blockchains are rather transparent. In another word, common blockchains can not provide voters anonymity and privacy by themselves.

Another issue about blockchains is scalability. Considering the fact that the blockchains are basically decentralized networks and their peers need to keep redundant data, the average transaction per second is quite low for a country-scaled voting system. This illuminates why scalability is a major problem with blockchains platforms despite its advantages.

In this article, we purpose and implement[a] a concept that provides transparency where the voting should be transparent and meanwhile, maintain anonymity in order to preserve voters' privacy. Furthermore, the purposed system maintains scalability as well as anonymity.

Keywords: Electronic Voting System, Blockchains, Ethereum, Zero Knowledge Token, Zero Knowledge Proof

I. INTRODUCTION

More than half of the world's countries are considered democratic countries. Although their governments may vary in terms of political structure, religion, and culture, they all grant the right to their eligible citizens to exercise their power and take their part in determining the country leaders, using election and voting systems.

There is almost two option to hold an election. Using an old-school paper-voting system or using an E-voting system. The paper-voting system is expensive and despite enormous expenses, ensuring that the election is free and democratic is quite challenging. On the other hand, the E-voting system is cheap, fast, and considering that nowadays almost everybody has access to the Internet, makes it available for everyone to use.

All of the mentioned features make the E-voting system getting more and more popular, however, it brings

* Email Address: mraji@shirazu.ac.ir
† Email Address: vahidgh.vgh@gmail.com
‡ Email Address: s.ali.yaghoubnejad@cse.shirazu.ac.ir
[a] GitHub Link

its own challenges. A practical voting system should be transparent to provide an undoubted election, be anonymous to protect voters' privacy, and be robust and secure against threats in the form of interruption, interception, penetration, and manipulation.

Blockchains networks can be the solution to these challenges. Ever since the birth of *Bitcoin* and its white paper publishment in 2008, blockchains have been used in order to make monetary transactions and commercial trading more secure. Then the manifestation of *Ethereum* [1] and *EVM*[2] makes it possible to deploy smart contracts on the blockchains networks so the blockchains can be used for other purposes. Nowadays *EVM* based networks are more considered as a decentralized platform for *DAOs*[3].

In this paper, we discuss an E-voting system based on the Ethereum network that its decentralization provides more security and reliability against malicious actions, especially if the mining nodes have been under the control of different nominees' parties. Nevertheless, using a decentralized platform, naturally, brings redundancy and within scalability issues about which we argue in the following sections.

II. RELATED WORKS

In 2018 in a paper entitled *"Towards Secure E-Voting Using Ethereum Blockchain"* proposed to use a smart contract on Ethereum blockchain to hold an election. The proposed system simply used a smart contract to which the voters send their transactions and increase the number of votes of the corresponding candidate. This method is quite practical and simple in terms of public and onymous voting.

Also in 2018 in a paper entitled *"DATE: A Decentralized, Anonymous, and Transparent E-voting System"*, a fully on-chain voting system was proposed which is not only focused on transparency but also privacy. In this paper, an effective e-voting system is proposed for the voters to minimize their trust in the authority of the government. They ensure the transparency of elections by putting all messages on the Ethereum blockchain. Meantime, the privacy of individual voters is protected via an effective ring signature mechanism.

In another paper published in 2021 entitled *"d - BAME: Distributed Blockchain-based Anonymous Mobile Electronic Voting"* implemented to implement an E-voting system on IoT devices such as smartphones to increase voter turnout of the election process. It was also suggested to use blockchains running smart contracts as a publicly accessible and tamper-resistant bulletin board to permanently store votes and prevent double voting.

III. TRANSPARENCY

Even with increasingly advanced technological improvement and the effect of electronic systems on people's lives, the voters may still not be confident about the accuracy, exactness, and freedom of an election held on an electronic systems platform. So an E-voting system should be able to provide adequate transparency measures to preserve voters' satisfaction. In order to do so, the user should be registered in the system with his national ID, and then a single vote token would be minted and transferred to his address (wallet). Meanwhile, an event is generated which indicates that a person with a specific ID number is registered and received a ballot token and then this event propagates into the whole network. Thus, every user and mining nodes have access to every ballot's information and the voters for whom the ballot was minted. So, each and every voter not only can check whether there is but one ballot that was minted for him but also can examine the whole ballots that have been generated.

After the registration phase has been finished, the admin revokes the permission of minting ballots hence, there is no one who can mint ballots and the total supply of ballots wlould be equal to the voters' number.

This level of transparency can clearly affect the anonymity of the voting system and threaten the voters' privacy. So, the system should be adopted to conceal the voters' ballots on the election day to maintain voters' anonymity.

IV. ANONYMITY

A confident election required that all information of voters go public. Obviously, it is a major issue when it comes to the anonymity of voters. A practical election must maintain anonymity as well as transparency. In another word, each ballot should be counted anonymously, accurately, and efficiently. The solution that we came up with is to use a similar solution which *Benjamin Diamond* from *JPMorgan's Quorum team* found to solve the anonymous tokens transference issue. The proposed system is called Zether[4] based on zkSNARKs which is considered a zero-knowledge proof design. *zk-*

[1] For more information about Ethereum, read Appendix-A
[2] Ethereum Virtual Machine
[3] Decentralized Autonomous Organization

[4] Zero-knowledge Ethereum

SNARKs can be used in practice for different types of computations.

A basic Zether system for confidential transfer of tokens works as follows[5] :

- *ZSC*[6] is deployed on the network. There is a one-to-one mapping between an *ERC20* contract and the corresponding *ZSC*. In *ZSC*, accounts are identified by public keys.
- *ZSC* maintains mappings between accounts and encrypted balances
- The user should fund an account with ERC20 tokens and obtain an equal amount of shielded tokens (Let's call them ZTH) in exchange. The ZSC is designated as the escrow of the ERC20 tokens.
- To transfer tokens anonymously, the sender should create a confidential transfer by encrypting the value to send using both their public key and receiver's public key, and a zero-knowledge range proof which proves that the encrypted value is positive, and the user's balance after the transfer is positive.
- The transaction with the payload is sent to *ZSC*, which updates the encrypted state of both the sender and the receiver after verifying the proof.
- To withdraw the tokens, the recipient should create a zero-knowledge proof for the knowledge of the balance the account holds without revealing the corresponding private key.
- Then the recipient should send the transaction to ERC20 with the proof, at which point the *ZSC* credits the equal amount of ERC20 tokens back to the user's Ethereum address.

The anonymity of casting ballots is just like *Zether*. Suppose the ERC20 tokens which the voters send the ballots tokens to *ZSC* and the recipient wallets actually act as the candidates' ballot boxes. In this scenario:

- The voters register and then send their ballots to *ZSC*
- On the voting day they send their ballots to the corresponding candidate address through an encrypted transaction to *ZSC* smart contract.
- Then after the election has finished, all candidates' agents send a transaction to *ZSC* smart contract and withdraw their ballots token.

In fact in this E-voting system, *ZSC* acts as an agent who conceals the voter's vote and the information of the candidate for whom they cast their ballots. This is how we protect the privacy of voters and maintain anonymity as well as transparency.

V. SCALABILITY

VI. IMPLEMENTATION

CONCLUSIONS

[1] Benjamin E.Diamond, *Many-out-of-many Proofs and Applications to Anonymous Zether* , J.P. Morgan AI Research, 2020

[2] Benjamin E.Diamond, *Anonymous Zether: Infrastructure* , J.P. Morgan AI Research, 2020

[3] Arya Wicaksana, Moeljono Widjaja, Vasaki Ponnusamy, M N Talib, Mamoona Humayun,Najm Us Sama, *Towards Secure and Auditable E-Voting System with Go Ethereum*, Turkish Journal of Computer and Mathematics Education, 2021

[4] Ali Kaan Koç, Emre Yavuz, Umut Can Çabuk, Gökhan Dalkılıç, *Towards Secure E-Voting Using Ethereum Blockchain*, 2018

[5] Wei-Jr Lai, Yung-chen Hsieh, Chih-Wen Hsueh, Ja-Ling Wu, *DATE: A Decentralized, Anonymous, and Transparent E-voting System*, 1st IEEE International Conference on Hot Information-Centric Networking (HotICN 2018), 2018

[6] Ehab Zaghloul, Tongtong Li, Jian Ren, *d-BAME: Distributed Blockchain-based Anonymous Mobile Electronic Voting*, 2021

[7] Satoshi Nakamoto, *Bitcoin: A Peer-to-Peer Electronic Cash System*, 2008

[5] For more information visits https://docs.kaleido.io/kaleido-services/token-zkp/architecture/

[6] Zether Smart Contract

Appendix: Appendix-A

Ethereum Blockchain The Ethereum blockchain is an ordered and transaction-based state machine proposed in 2013 and the currency runs on Ethereum is called the

ether. The construction of a blockchain relies on miners, who mined a new block via the proof of work (PoW) consensus algorithm. PoW is a computationally complex puzzle which makes the information on blockchain immutable unless the majority of miners are malicious. Different from Bitcoin, there are two types of accounts in the Ethereum blockchain:

- Externally owned account: Public-private key pairs are generated for allowing users to send transactions to off-chain counterparts with specific addresses.
- Contract account: Sets of functions are deployed by users through a transaction, in which the functions are controlled by written codes rather than users directly.

On Ethereum, the main fields of a transaction include:

- Source/from: A signature comes from an exterior-owned account, allowing others to verify the correctness of a transaction.
- Destination/to: It contains an address that can be either from an exterior-owned account or a contract account.
- Data: It contains the compiled contract codes or instructions for the contract, or we can also store data on it as records.
- Gas price: The exchange rate between ether and gas[7].
- Gas: The cost that senders should pay to miners, which is usually proportional to the complexity or amount of computation associated with the involved instructions, caused by the transaction.

[7] Actually after August 15th, 2021, Ethereum has activated a major change called the "London hard fork" which is changed the concept of gas limit and gas price calculation. However, the test network on which we test, has not changed yet.