Proceedings of 14th IOE Graduate Conference
Peer Reviewed
Year: 2023 Month: December Volume: 14
ISSN: 2350-8914 (Online), 2350-8906 (Print)

Blockchain Based Anonymous Voting System using Ring-Signature

Purushotam Sangroula [a], Nanda Bikram Adhikari [b]

[a, b] *Department of Electronics and Computer Engineering, Pulchowk Campus, IOE, Tribhuvan University, Nepal*
[a] 078msice012.purushotam@pcampus.edu.np, [b] adhikari@ioe.edu.np

Abstract
There has been a growing popularity in the use of Electronic Voting Machines and online voting systems. But in most of the implementations they either lack transparency or verifiability or both. This research aims to make voting transactions transparent, anonymous, verifiable and secure through the use of ring signature, RSA and blockchain. Users anonymity is preserved by the use of Ring Signature Algorithm which is an algorithm which hides the identity of a specific voter behind a group yet verifiable that someone from the group has initiated the transaction. A ballot is formed in a secure way by concatenation of choice of the voter with a random string of fixed size and further encrypted with RSA keys. To ensure that ballots remain encrypted until the election is over, RSA keys are generated by using k-n threshold secret sharing scheme. After the implementation and emperical analysis of overall election process, average cost per vote for the ring size of 25 is found to be approx $100 (5665048 gas units) with the exchange rate of 1Eth/$1765.21.

Keywords
e-voting, blockchain, ring-signature, zero knowledge proof

1. Introduction

Election is the process of electing or selecting an individual for a post or simply choosing a decision/idea among many where there is a conflict among concerned group of people. In general, election is understood synonymous to selecting political leader but this is not the only field. In many other fields such as professional councils, students unions, workers unions there is a need of election.

The voting in elections are mostly conducted through paper based ballot system. Which is tiresome to setup voting stations, collecting ballot boxes and finally counting the vote one after another with the verification from a large group of selected people.

As an alternative to this problem Electronic Voting Machine (EVM) came into existence but without widespread acceptance and trust. The major concerns with the existing EVMs are unauditability, lack of transparency, centralized storage and lack of verifiability. Blockchain based online voting applications are also gaining traction in recent times with concern over voter verification, authentication, anonymity, ballots security, etc.

In this work aforementioned issues are addressed by the use of Ring Signatures and randomized encrypted ballots. Ring Signature is a mechanism in which a verifier is convinced that someone within the specified group generated the signature and message but without knowing the individual signer.

In this study an anonymous and verifiable online voting system is implemented and analyzed emperically and compared with the existing works based on different chains and setups.

1.1 Zero-Knowledge Proof

Zero-Knowledge Proof or Zero-Knowledge Protocol is a method by which a prover proves a knowledge to a verifier without actually revealing the knowledge. If proving a statement requires the possession of a secret then for a prover to be correct every time the verifier asks, the prover must possess that secret.

Zero-Knowledge Types

- Proof of knowledge: the knowledge is hidden in the exponent like in RSA.
- Pairing based cryptography: given f(x) and f(y), without knowing x and y, it is possible to compute f(x×y). Example Homomorphic and Elgamal encryption.
- Witness indistinguishable proof: Witness cannot be distinguised which is used for proving a statement.
- Multi-party computation: Multi party have their own secret yet they can produce a required knowledge without leaking own secret.
- Ring signature: It's a variant of group signature in which no one can expose other's identity and receiver of signature cannot identify the signer apart from the whole group.

1.2 One Time Public Keys (OTPKs)

One Time Public Keys (OTPKs) was originally used by Monero[1], which is one the most popular cryptocurrency providing anonymity to the transaction, the sender and the receiver as well. In Monero sender is anonymized using ring signatures and receiver are anonymized by the use of stealth addresses. By the use of stealth address of the receiver new OTPKs is generated for new transaction. And only the receiver is able to generate the private key for the OTPKs and use the fund.

To generate OTPKs, each user must have two private (a, b) and two of their corresponding public keys (A, B). To compute OTPK the sender should use two public addresses of receiver and a random number r.

$$\text{OTPK} = H_s(rA)G + B \tag{1}$$

Now the sender should use this newly generated OTPK to make transaction and the information regarding random number should also be sent along with, such a way that $R = rG$.

Once the transaction is complete the receiver will be able to recover the private key x associated with the OTPK by

$$x = H_s(aR) + b \tag{2}$$

such that:

$$\text{OTPK} = xG$$

Proof: The receiver is able to recover the private key.

$$\begin{gathered} H_s(rA)G + B = (H_s(aR) + b)G, \\ (H_s(rA) + b)G = (H_s(aR) + b)G, \\ (H_s(raG) + b)G = (H_s(arG) + b)G, \\ (H_s(aR) + b)G = (H_s(aR) + b)G, \\ L.H.S. = R.H.S. \end{gathered}$$

Monero's OTPKs concept is used in order to anonymize identity of voters in this work.

1.3 Ring Signatures

Ring Signature is an encryption mechanism designed to hide the initiator of an action. Let us suppose there is group of people each having their private and public key pairs as $(S_1, P_1), (S_2, P_2), ...(S_i, P_i), ...(S_n, P_n)$ and the i^{th} person wants to send a message anonymously. Then the person can encrypt the message m to produce a secret text σ by using his own secret key and public keys from all the group members i.e. $S_i, P_1, P_2, ..., P_n, m$ as the input. Anyone can verify that the secret message σ is from the group given σ and m but it is extremely difficult to find out who signed the message without knowing the private key.

Ring signatures are good for maintaining anonymity but it also causes a problem of double spending which means that same token can be spent in more than two transactions as there is no clue of which individual signed the transaction. To overcome with this issue Ring Signature Confidential Transaction [2] is used, which is based on the use of Key Images.

Key images are a public commitment of the signer's private and public key, yet keeping information related to private key secret. It is calculated by the product of private key, x and the Hash value of signer's public key and sent along with the transaction. Finding x and $H_p(P_s)$ from their product is a hard problem[3]. In blockchain key image of a voter is recorded after signature verification and if it does not exist on chain.

Algorithm 1 is used to generate the ring signature by the voter and algorithm 2 is used to verify voter's authenticity.

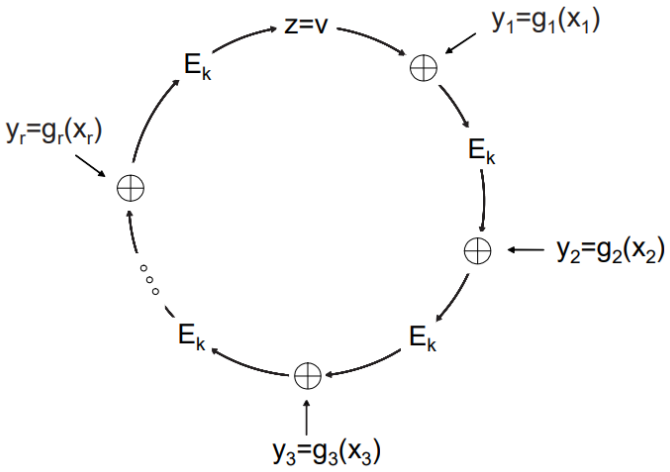

Figure 1: Ring Signature generation

In the figure 1 x_i are the random numbers except for the signer, his private key is used, $g_i(x_i)$ is a signing algorithm, E_k are intermediate results, v is the some arbitrary starting value, z is calculated such that a ring is closed.

1.4 Consensus Algorithm

When a new transaction is created in blockchain it has to be validated based on consensus algorithm. Proof of Work (PoW) is the consensus algorithm that most of the crypto currencies used till September 2022. Since, then Ethereum based crypto systems have migrated towards Proof of Stake (PoS).

Proof of Work (PoW) In this protocol miner has to solve a cryptographic puzzle before actually mining the transaction. Atleast 51% miners must also validate the transaction. For solving and mining the block the miner receives some tokens as rewards.

Proof of Stake (PoS) In this protocol miner has to deposit pre-specified minimum amout of crypto coins. Miners having higher stake has higher chance of mining new transactions. If any transaction that is mined by a miner and is deemed invalid by 51% of other miners then the miner will loose the coins put in stake.

Proof of Authority(PoA) is one of the new consensus algorithm which falls in the category of high fault tolerance and high performance. It only requires is prior-authentication for a miner to be in the network.

PoA is perfect for the purpose of election due to it's low end hardware sufficiency, tolerance to fault (51% rule) and high transaction rate. Hence PoA is recommended as consensus algorithm in this e-voting work.

1.5 Hash

Hash is a fixed length one-way encryption mechanisms. Hash function is used to generate hash values which must be collision free, pre-image resistant and deterministic.

1.6 Blockchain

Blockchain is considered to be one of the revolutionary technologies which could uproot lots of central authorities such as financial institutions, regulatory bodies, etc. As name implies it is a chain of blocks which are formed by relation pointing to the previous blocks.

Once data is written to the blocks it is immutable, publicly accessible and distributed to multiple nodes known as miners. For any write operation consensus must be met which makes it highly secure against unauthorized access.

One of the block might look like this for the case of this study:

Block No
Hash of previous Block (3534afd234523...)
Nonce (342345...)
Ciphered Ballot and Ring Signature ...
Hash of this Block (5646a234afe3ab234...)

1.7 Miners

Miners are the nodes in a Blockchain network whose job is to verify the validity of transaction and compute a hash value which will be used as an address of a block. Once a miner successfully mines a block, that recently mined block is forwarded to all the miners, who will again verify the validity of addition of block. If consensus is met then all the miners update their blockchain with additional block.

1.8 Smart Contracts

Smart Contracts are static codes that run on blockchain network which is responsible for every transaction that happens in a blockchain. It is like a collection of condition-action-rules which defines what action to perform when some condition is met. Once smart contracts are deployed in the network it cannot be changed hence it becomes transparent, immutable and trustworthy system.

2. Related Work

There are many studies conducted in the field of online voting. Most commonly studied types includes token based voting applications. In [4] Tarasov and Tiwari proposes an anonymous voting system using zCash where zCash is a fork of Bitcoin[5]. There are two types of addresses in zCash: t-address, which allows transparent transactions and is similar to pseudonymous address in Bitcoin; z-address, which is preserves privacy and anonymity of transactions and is based on zk-SNARKS[6]. In this work authors utilize the underlying anonymous protocal of z-address to anonymyze voter and the votes. Another similar approach is researched in [7] for evm based blockchain where non fungible tokens are to be transferred to candidates after voter casts vote. In this mechanism the identity of a validated voter is kept anonymously in the blockchain by a trusted centralized authority.

Another category of voting research includes works where anonymity is preserved by the use of group or ring signature schemes. Group signature[8] requires a group manager hence not trusted for confidential application. Hence, research works related to ring signature are only cited for this work. In [9] Salazar et al. proposes the use of linkable signature to overcome the issues of double voting problem as seen in previous works related to anonymous voting. This signature allows to associate a tag with a voter but keeps their identity secret to the public. This research was later implemented by Tornos et al. [10] in 2014 by allowing voters to vote from browsers and android applications. To add another layer of privacy on top of work from Salazar, [11] suggests decoupling the voter registration process into two different and independent organizations: one secret organization and another trusted third party. Following the research of [11], [12] develops a voting system based on ring signature for Bitcoin.

In [13] Larriba et al. proposes an efficient proof of authority and Ring-Signature based voting system in which political parties are given limited power to monitor the election process. In this paper the One Time Public Keys are implemented to ensure the eligibility of a voter to vote. The involvement of political parties is considered to build trust among public regarding online voting system. The work from Larriba overcomes most of the lackings that earlier works had and has been the key reference for this work.

This study conducts empirical time and gas cost analysis on evm chain for the protocol developed by [13] along with comparisons with other similar works for creating anonymous and verifiable online voting system.

3. Methodology

3.1 Election Setup

Before election, l number of trusted third parties who are also the miners, denoted by p_i, are selected. These parties must collaborate to generate the parameters of election. To encrypt votes RSA is employed, hence these parties must define the parameters of RSA: the public modulo n the public verification key v and the private signature s. Since private key s is supposed to be made public only when election ends (k, l) threshold RSA sharing protocol has been used. Threshold RSA sharing protocol defines that a secret key s can be created and broken down into l shares such that it can be reconstructed when any subset of key shares of a size more than or equal to threshold t is used. Each third parties must publish their commitment for private shares by signing with their private key.

After all the parameters are decided these information need to be stored in the first block of the blockchain. Apart from these parameter every miner has his own set of private and public key pairs which he will use to sign the transactions.

3.2 Registration

Voters must register before election. To apply for registration voter generates two pairs private and public keys i.e. (a, A) and (b, B). Voter submits both public keys along with other necessary information. Once the voter is verified the authority

will generate an OTPK and a random number r for each voter. Both of these information are provided to the voter. Whereas, OTPK and rG for every verified voters are submitted to the block chain.

3.3 Vote Casting

To cast a vote, voter first gathers the public information such as modulo n, the public key v and N public keys from the first block of the blockchain, which are required for voting. Then after he can select a candidate whom he wants to vote. Let us assume his voting choice as $vote$. This $vote$ is concatenated with a fixed length random mask to obfuscate ballot. $(vote\|mask) mod\ n$ is encrypted using the public key v by the use of modular exponentiation. $evote = (vote\|mask)^v mod\ n$.

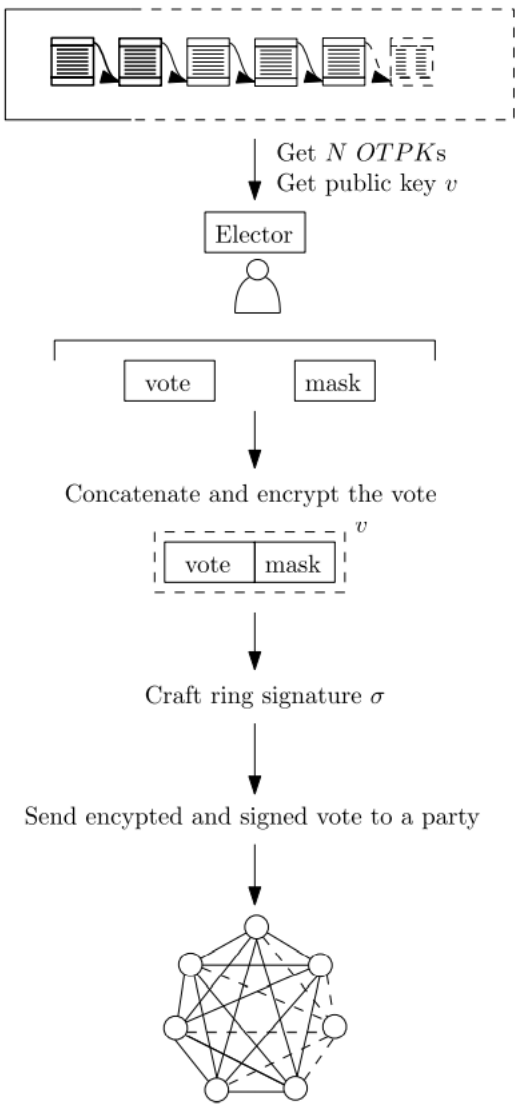

Figure 2: Vote Casting Process

Next voter signs the $evote$ with ring signature[13]. Let us call the combination of $evote$ and signature as the ballot i.e. $ballot = \{evote, \sigma(evote) = (P, K, c_0, r)\}$. The parameters like K, c_0, r comes from the ring signature algorithm and P here is the set of public keys used to create ring signature.

3.4 Vote Processing

Miners verify the casted ballot. In PoA consensus algorithm, only one of them will verify the transaction at a time in predefined order.

The process of creating and verifying the transactions and blocks is as listed:

- Miner applies ring signature verification algorithm [13] to verify the correctness of the signature.
- It accumulates transactions with minimum of following information.

  Block Id

  Ballot and Transaction IDs

  Timestamp

  Result of verifying the Ring Signature
- It creates a block when sufficient transaction are gathered.
- It broadcasts the block so that other miners can verify the correctness of every votes.

Once the election finishes, no more votes are accepted. Now atleast k miners/trusted third parties come together to reconstruct the secret key s by using lagrange polynomials. After reconstructing s, every miner need to interate over all the blocks from the beginning to the end independently to decrypt ballot and compute result. After an agreement of result is determined by consensus the result is published.

Also the voter himself can tally if his vote has been tampered, modified or not by using the private key corresponding to one's OTPK.

4. Experiment Setup

All the experiments are performed in EVM setup in the machine with Intel(R) Core(TM) i7-7Y75 CPU with 1.60 GHz frequency.

4.1 Ethereum Virtual Machine Setup

Ethereum Virtual Machine (EVM) is the virtual environment, a node of the blockchain, where smart contracts are deployed and transactions are conducted. For this work Ganache[14] has been used to host EVM and the following values/facts of different parameters have been used for evaluation:

- 1 ETH equals to $1765.21 as of 2023 Mar 22
- 1 ETH equals to 10^{18} wei. (Wei is the smallest unit of Ethereum coin.)
- 1 Gwei equals to 10^9 wei.
- Gas price per unit: 20 Gwei.

Gas cost in USD can be calculated when units of gas cost is available by using relation: Gas Cost in USD = Gas Cost Units * Gas Price in GWei * Eth to USD rate / 10^9

5. Results and Analysis

5.1 Election Setup Phase

Election setup phase consist of two important tasks:

- Implementing threshold secret sharing scheme.
- Deploying Smart Contract with basic information such as modulo n, public key v and commitment of trusted third parties regarding the shares of secret keys.

5.1.1 Smart Contract Deployment

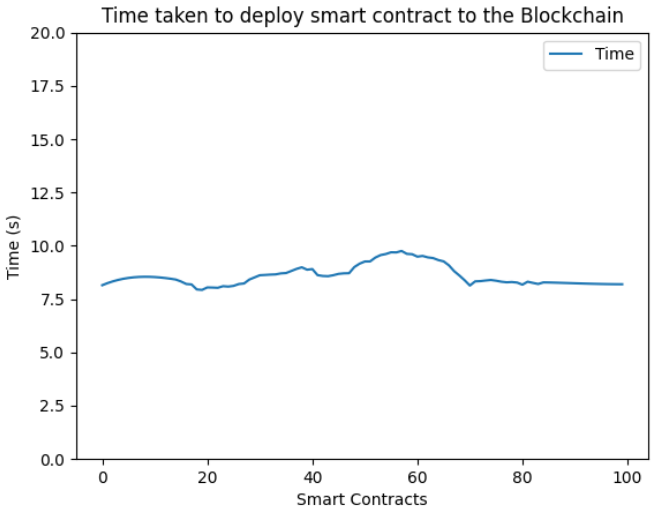

Figure 3: Smart Contract Deployment duration as observed in various experiments

By conducting around 100 deployments of smart contracts it is observed that it takes 8.588849 seconds on an average, the gas cost is 3097468 units which calculates to $54.67681.

5.1.2 (k,l) Threshold Secret Sharing

Using the process as explained in [15], threshold (k)= 6, and fragments(l)=11 was used to generate shares for secret key. More trustless way to distribute key shares can be through the use of Distributed Key Generation and Verifiable Secret Sharing (DKG VSS)[16] but due to the focus of this study being anonymity and verifiability of the voter and the vote, a simpler way has been chosen.

5.2 Registration Phase

In the registration phase voters and candidates are validated by Election Authority and registered to the Blockchain.

After observing the 10 iterations of registration of 35 candidates, ie. 350 samples, it was found that registration of each candidate requires 161270.667 gas units which calculates to $2.846766 and 2.557470 seconds on an average. The complexity for this task is constant in terms of space and time.

5.2.1 Voter Registration

After observing the 10 iterations of registration of 1000 voters, i.e. 10000 samples, it was found that registration of each voter

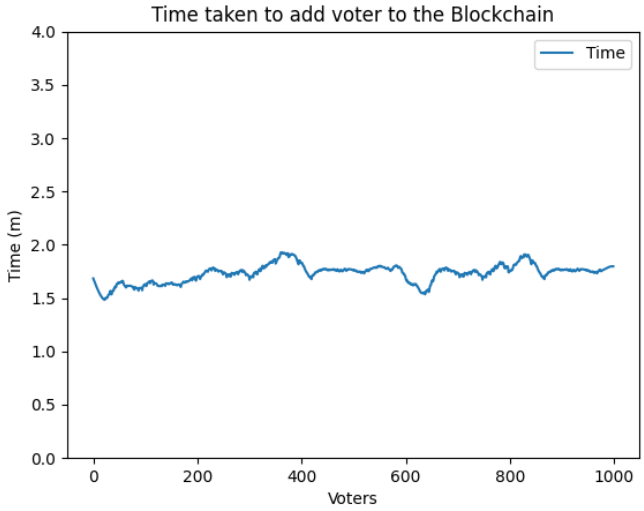

Figure 4: Voter Registration duration as observed in various experiments

requires 159520.840841 gas units which calculates to $2.815878 and 1.737130 seconds on an average. The nature of complexity for this task is constant in terms of space and time.

5.3 Vote Casting Phase

This phase majorly consists of generation of Ring Signature in the client side, verification of it in the blockchain and storage of signed Ballot.

5.3.1 Ring Signature Generation

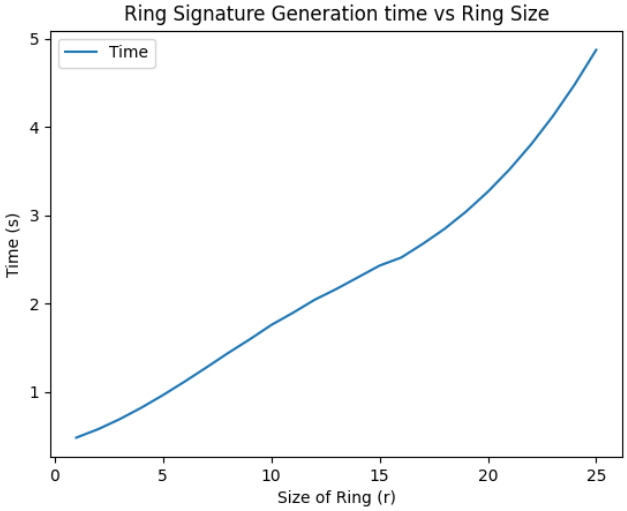

Figure 5: Ring Signature Generation Duration vs Ring Size

After observing the process of ring ring signature generation 1000 voters it was found that the time taken to sign a message using ring signature grows linearly with the size of the ring (i.e. number of public keys used). It can be seen from the graph as well. With 5 public keys in the ring it takes less than a second whereas with 25 public keys in the ring it takes approximately 4.87 seconds.

5.3.2 Ring Signature Verification

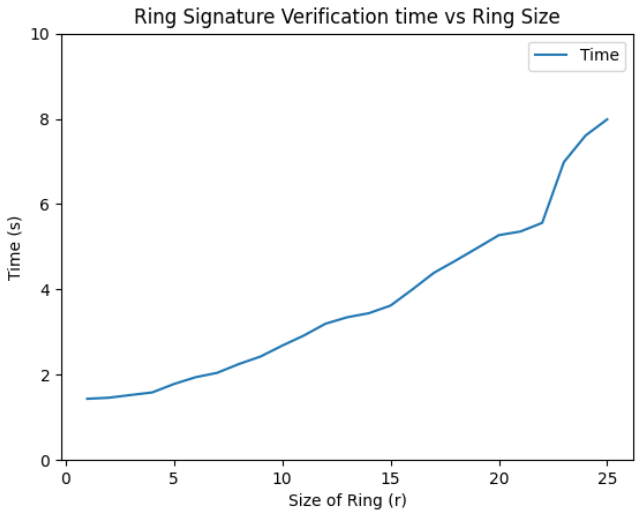

Figure 6: Ring Signature Verification duration as observed in various experiments

After observing the votes casted by 1000 voters it was found that verifying each ring signature of size 5 requires 127119.4 gas units which calculates to $4.487849 and 1.782490 seconds on an average. Similarly, to verify ring signature of size 15 requires 349919 gas units which calculates to $12.353610 and 3.621456 seconds on an average; and to verify ring signature of size 25 requires 532588 gas units which calculates to $18.802593 and 7.986880 seconds on an average. The nature of complexity for this task is linear in terms of time and constant in terms of space.

5.3.3 Ballot Storage

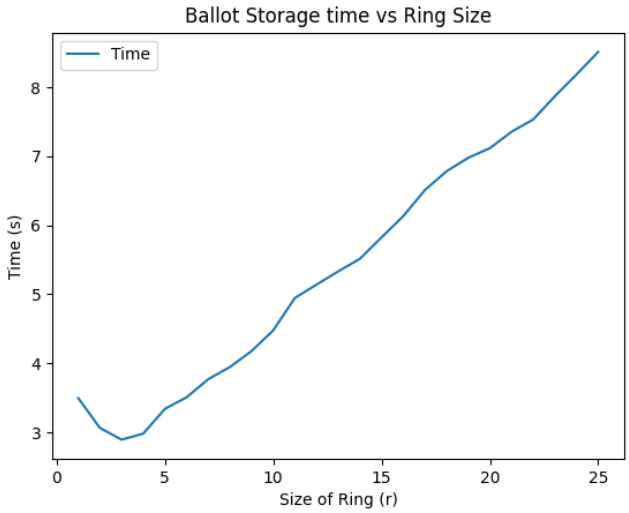

Figure 7: Ballot Storage duration as observed in various experiments

It was found that storing each ballot and the signature with ring size of 5 requires 810095.9 gas units which calculates to $28.599788 and 3.508477 seconds on an average. Similarly, for ring size of 15 requires 1614825 gas units which calculates to $57.010108 and 6.131898 seconds on an average; and for ring size 25 it requires 2339584 gas units which calculates to $82.597141 and 8.511705 seconds on an average. The nature of complexity for this task is linear in terms of space and time.

5.4 Overall Election Cost Analysis

Total cost of election can be calculated by sum of cost of Election Setup, Candidate Registration, Voter Registration, Verification of Ring Signature and Storage of Ballot.

Election setup is a one-time cost for an election hence it can be considered constant k_{es}. The variable factors are Candidate Registration, Voter Registration, Verification of Ring Signature and Storage of Ballot.

Mathematically, if v be the number of registered voters, c be the number of candidates, r be the size of a ring, cc be the cost of adding a candidate, vc be the cost of adding a voter, $cost_{rv}$ be the cost of ring signature verification and $cost_{bs}$ be the cost of storing ballot then total cost per voter can be computed as:

$$\text{Total Cost}/v = (k_{es} + c*cc + v*vc)/v + (\text{cost}_{rv}(r) + \text{cost}_{bs}(r)) \quad (3)$$

For the experimental setup candidate count(c)=10 and voter

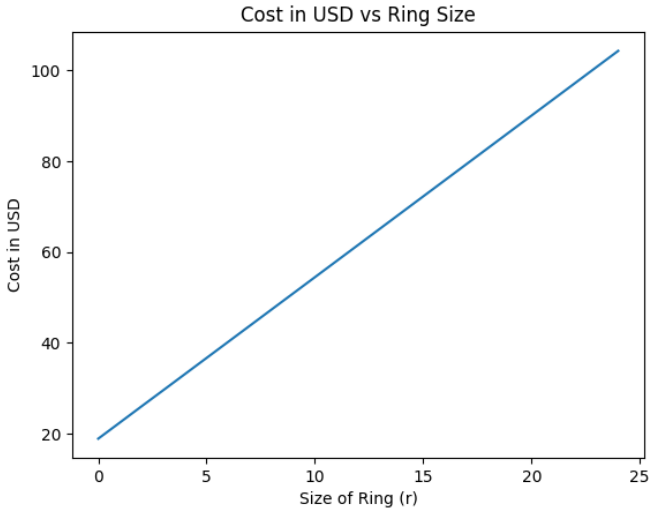

Figure 8: Total Cost of casting votes per voter vs Ring Size

count(v) = 1000. The plot of the cost for these operations is as shown in the figure no 8 from which it is observed that cost per vote for the ring size of 25 is approx $100 (5665048 gas units).

Since fetching Ballots from blockchain in order to calculate results will be free of cost due to read operations only. It definitely takes some time to decrypt and add up results but for least engaged high end local server it can be assumed negligible .

5.5 Comparison with existing works

For the purpose of comparison ring size of 25 is taken as reference. Even though there are vast number of works on blockchain voting, works closely related (ie. ring signature based and on ethereum chain) to this work are only a few. Among which [13] lacks practical data and focuses only on

theoretical protocol and architecture design. Another work close to this work is from Wei[17] which has used evm on MacBook Pro 2 Core, 2.7 GHz Intel Core i5 with gas cost for conducting a voting transaction being 275000 units. Another major variation is the use of IPFS[18] for ballot storage due to which it's results are still incomparable to the architecture used for this study. Storing within blockchain is considered highly secure and immutable as compared to IPFS. Hence, even though gas cost for the work by Wei comes out to be quite low as compared to this work's 5665048 units it can be called reliable for the sensitive operations like election where transparency and verifiability is the concern. The nature of time complexity in this work and [17] are similar, the experimental data seem to vary due to the variation in experimental setup.

6. Conclusion and Future Works

In this study an anonymous, verifiable and secure voting system is implemented with the help of Ring Signature, k-l threshold secret sharing, RSA with the average cost per vote for the ring size of 25 to be approx $100 (5665048 gas units) with the exchange rate of 1Eth/$1765.21. The gas cost can be reduced if ring signature with smaller size is used but comes with the cost of anonymity.

In future research and development of online voting several reliable ways can be explored. The major expensive operations as perceived during this study are storage cost of ballot, signature and it's verification. One way it can be reduced is through the off chain computation of verification process and verification of it by the use of zero knowledge proof. For the storage cost optimization distributed file storage services can be used but reliability and security are a part of research on this field. Research on the use of layer 2 blockchains based on Ethereum for both the transaction and the storage cost optimization can be performed. Another aspect of research could be the implementation and study of online voting platform on blockchains which are specifically built for zero knowledge transactions.

Acknowledgments

This work was supported by Tribhuvan University. The authors are grateful and pay deepest gratitude to all the faculty members for providing opportunity and valuable suggestions and feedback during this work.

References

[1] Malte Möser, Kyle Soska, Ethan Heilman, Kevin Lee, Henry Heffan, Shashvat Srivastava, Kyle Hogan, Jason Hennessey, Andrew Miller, Arvind Narayanan, and Nicolas Christin. An empirical analysis of traceability in the monero blockchain. *Proceedings on Privacy Enhancing Technologies*, 2018:143–163, 06 2018.

[2] Shen Noether. Ring signature confidential transactions for monero. Cryptology ePrint Archive, Paper 2015/1098, 2015. https://eprint.iacr.org/2015/1098.

[3] Daniel RL Brown. Breaking rsa may be as difficult as factoring. *Journal of Cryptology*, 29(1):220–241, 2016.

[4] Pavel Tarasov and Hitesh Tewari. Internet voting using zcash. *IACR Cryptol. ePrint Arch.*, page 585, 2017.

[5] Satoshi Nakamoto. Bitcoin: A peer-to-peer electronic cash system. *Cryptography Mailing list at https://metzdowd.com*, 03 2009.

[6] Sean Bowe, Ariel Gabizon, and Matthew D. Green. A multi-party protocol for constructing the public parameters of the pinocchio zk-snark. *IACR Cryptol. ePrint Arch.*, page 602, 2017.

[7] Raj Shrestha, Rajiv Sah, Sabin Shrestha, Shailja Sarawagi, and Nanda Adhikari. Blockchain interfaced sacure e-voting system. *Journal of the Institute of Engineering*, 15:195–199, 02 2020.

[8] Lingyue Zhang, Huilin Li, Yannan Li, Yong Yu, Man Ho Au, and Baocang Wang. An efficient linkable group signature for payer tracing in anonymous cryptocurrencies. *Future Generation Computer Systems*, 101:29–38, 2019.

[9] José Luis Salazar, Joan Josep Piles, José Ruiz-Mas, and José María Moreno-Jiménez. Security approaches in e-cognocracy. *Computer Standards and Interfaces*, pages 256–265, 2010.

[10] José Luis Tornos, José Luis Salazar, and Joan Josep Piles. An evoting platform for qoe evaluation. In *2013 IFIP/IEEE International Symposium on Integrated Network Management (IM 2013)*, pages 1346–1351, 2013.

[11] Kibin Lee, Joshua I. James, Tekachew Gobena Ejeta, and Hyoung Joong Kim. Electronic voting service using block-chain. *J. Digit. Forensics Secur. Law*, pages 123–136, 2016.

[12] Y. Wu. An e-voting system based on blockchain and ring signature. 2017. Master's thesis, University of Birmingham.

[13] Antonio M. Larriba, Aleix Cerdà-i-Cucó, José M. Sempere, and Damián López. Distributed trust, a blockchain election scheme. *Informatica*, 32(2):321–355, 2021.

[14] Wei-Meng Lee. *Testing Smart Contracts Using Ganache*, pages 147–167. 09 2019.

[15] Ivan Damgård and Maciej Koprowski. Practical threshold rsa signatures without a trusted dealer. In Birgit Pfitzmann, editor, *Advances in Cryptology — EUROCRYPT 2001*, pages 152–165, Berlin, Heidelberg, 2001. Springer Berlin Heidelberg.

[16] Xiaoyun Yang, Zhe Xia, and Min Xiao. Verifiable secret sharing and distributed key generation based on hyperplane geometry. In *2015 2nd International Symposium on Dependable Computing and Internet of Things (DCIT)*, pages 142–145, 2015.

[17] Wei-Jr Lai and Ja-Ling Wu. An efficient and effective decentralized anonymous voting system. *CoRR*, 2018.

[18] Peng Kang, Wenzhong Yang, and Jiong Zheng. Blockchain private file storage-sharing method based on ipfs. *Sensors*, 22(14):5100, 2022.