Blockchain Smart Contract Technology in Digital ID Authentication System for E-Voting

LIN TZU-CHENG

July 22, 2024

Abstract

This research initiative seeks to merge the Digital ID Authentication System with blockchain technology to develop an innovative online voting platform. Drawing from Taiwan's expertise in digital governance, Saint Kitts and Nevis aims to establish a robust digital identity infrastructure encompassing citizen databases, identity card issuance, and digital certificate mechanisms. Integrating blockchain into this framework enhances security and lowers voting expenses, paving the way for a more efficient and transparent electoral process. Our method Partition Decentral Election Method, has demonstrated remarkable cost reduction, slashing total gas expenditure by approximately 63% in scenarios involving 50 voters. This effort sets a benchmark for future online voting and advances the development of between Digital ID Authentication System and E-voting.

1 Background

In 2021, the government of Saint Kitts and Nevis (referred to as SKN) passed a comprehensive National Long-term E-Government Development Roadmaps, highlighting the establishment of Digital Identity Authentication System as a primary objective. With the intention of capitalizing on Taiwan's technological prowess and its extensive experience in digital governance, SKN seeks support in creating a robust digital identity authentication mechanism. The ultimate aim is to position this system as a pivotal infrastructure for a wide array of online services, thereby propelling SKN towards becoming a digital nation and fostering the development of a smart government.

The digital identity authentication system is envisioned as an extension of the existing citizen registration system. In addition to the physical chip ID card, its primary function is to digitize the essential citizen data required for various government services. This digital data is secured with encryption keys, providing the necessary citizen identity verification for government services. The SKN government aspires to establish a cross-agency data exchange and integration mechanism centered around identity authentication, incorporating digital certificates and signature functionalities. This system aims to enable citizens to seamlessly access various government digital services using their digital identity for real-time inquiries.

The technical team from the Taiwan mission in Saint Kitts and Nevis has presented a comprehensive plan for the digital identity authentication system, comprising four main components: (1) a database management system to store the data of all citizens, (2) an identity card issuance system, including modules for identity card management, issuance, printing, and applicant identity verification, (3) the establishment of digital certificates and digital signature mechanisms to provide robust

personal information protection, and (4) application programming interfaces (APIs) for integration with other government services, positioning it as a crucial infrastructure for future online services.

This project aims to devise an online voting system that can seamlessly integrate with the digital authentication system. Beyond serving as a blueprint for other online service systems, it leverages blockchain's decentralized, immutable, transparent, and privacy-preserving features to reduce voting costs for citizens with digital ID cards. Which may serve as a driver for the effective implementation of the digital identity authentication system.

2 Introduction

With the ever-evolving landscape of technology, the progression of blockchain technology has been notable. Blockchain, characterized by its decentralization and immutability, has witnessed continuous advancements in various applications. In this dynamic technological era, the decentralized storage of data across multiple nodes, forming an interconnected and ever-expanding chain, remains a foundational aspect of blockchain.

Bitcoin: A Peer-to-Peer Electronic Cash System [1], authored by Satoshi Nakamoto, proposes a decentralized electronic payment system using cryptographic proof instead of trust. The system enables direct transactions between parties without the need for a trusted third party, addressing the double-spending problem through a peer-to-peer network and proof-of-work mechanism. Transactions are timestamped, hashed into a chain, and broadcasted, with nodes collectively validating and extending the chain. The paper outlines the incentive structure for network participation, mechanisms for simplifying payment verification, handling transaction privacy, and the computational probabilities of network security against potential attacks.

Smart contracts, as a prominent application of blockchain[2], have further underscored the transformative potential of this technology. Programmed in code and residing on the blockchain, smart contracts offer automatic execution and self-enforcement. This eliminates the need for intermediaries or trust in third parties, even governments, making contract execution more efficient, rapid, and cost-effective. The evolution of blockchain technology, has positioned it as a cornerstone in diverse industries, providing secure, transparent, and efficient solutions.

One compelling application is online voting. Leveraging the inherent security and transparency of blockchain, online voting systems can enhance the integrity of electoral processes. Compared to traditional voting systems, blockchain-based online voting offers several advantages. Firstly, it eliminates the need for intermediaries, reducing the potential for manipulation and enhancing the overall trustworthiness of the electoral process. Secondly, the transparency of the blockchain ensures that every vote is recorded and can be audited, addressing concerns about the accuracy of results. Additionally, the decentralized nature of the system reduces the risk of a single point of failure or cyberattacks, enhancing the security of the entire voting process. The decentralized nature of blockchain mitigates the risk of tampering or fraud, providing a trustworthy platform for citizens to cast their votes.

The integration of Digital Identity Authentication System with blockchain technology serves as a motivation for this research, driven by four key reasons.

Firstly, the use of digital signatures within the digital identity cards can be leveraged as a basis for blockchain-based voting. The public-private key pair embedded in the digital identity card can serve as a unique digital signature for each citizen. This mechanism establishes a one-to-one correspondence

between a digital identity and a vote, mitigating the risk of fraudulent multiple voting. The inherent security of the digital identity authentication system, with encryption keys securing citizen data, can seamlessly extend its protection to the digital signatures used in blockchain-based voting.

Secondly, the decentralized architecture addresses the challenge of potential attacks or manipulation by malicious actors. By distributing the voting system across multiple nodes, it becomes significantly challenging for any single individual or entity to compromise the entire system. This distributed nature enhances the overall security of the voting process, making it resilient against unauthorized access and manipulation attempts. The integration with Digital Identity Authentication System ensures that only legitimate citizens with verified identities participate in the voting.

Thirdly, the immutable nature ensures the integrity and transparency of the voting process. Once a vote is recorded on the blockchain, it becomes a permanent and unalterable part of the chain. This characteristic eliminates concerns about tampering or manipulation of voting results, enhancing the overall trustworthiness of the electoral process.

Lastly, the use of smart contracts in blockchain technology introduces automated and self-executing scripts that can enforce predefined conditions for the voting process. This automation reduces the risk of human interference or manipulation of the voting outcome. The transparency of the blockchain, coupled with the automated execution of smart contracts, ensures a fair and equitable electoral process. By preventing individuals from knowing the results in advance without meeting specified conditions, smart contracts contribute to the fairness and integrity of the voting system.

Building upon the aforementioned advantages, this research aims to usher in a new era of voting systems by reducing costs, streamlining processes, and enhancing overall security, transparency, and privacy. The integration of Digital Identity Authentication System with blockchain technology offers a robust foundation, ensuring the uniqueness of each vote through digital signatures, fortifying security against malicious attacks through decentralized architecture, guaranteeing the integrity of the voting process with the immutability of blockchain, and introducing automation through smart contracts to uphold fairness. By leveraging these benefits, the study seeks to not only modernize the electoral landscape but also establish a voting system that is cost-effective, efficient, and trustworthy.

3 Related Work

Lyu et.al proposes a decentralized e-voting system using smart contracts on Blockchain to ensure trust and privacy [3]. It employs linkable ring signatures to maintain voter anonymity and prevent multiple voting, while also utilizing threshold encryption for simultaneous result disclosure to all voters. The system distributes trust among voters, ensuring resilience against malicious actors. However, this system asserts its ability to accommodate approximately 30 to 40 voters due to the computational constraints of Ethereum.

Alvi et.al explores the implementation of a blockchain-based online voting system using Ethereum [4][5], aiming to enhance security, transparency, and reduce costs. It reviews the potential of Ethereum's smart contracts and decentralized applications (dApps) in creating tamper-proof voting systems. Traditional e-voting systems' security issues are discussed, highlighting the benefits of blockchain technology. However, it relies on a centralized election commission for voter registration and key distribution, which poses risks.

4 System Architecture

The voting system includes Setup, Register, Vote, Reveal, and Declare Phases. The proposed election process begins with the deployment of an Ethereum smart contract to manage the election, establishing its rules and parameters, and selecting an appropriate digital signature method. During the register phase, a period is opened for voters to submit and verify their public keys, which are then securely stored on the blockchain. In the subsequent voting phase, registered voters are permitted to submit the hash of their ballot to the blockchain, ensuring both anonymity and the prevention of double voting. Following this, the reveal period is initiated, allowing voters to submit their actual ballots for verification against the previously stored hashes. Finally, the declare phase involves tallying and publishing the results on the blockchain, including the calculation of accuracy rates and the identification of any discrepancies, with the provision to consider re-voting if significant issues are detected.

4.1 Setup Phase

The initiator of the voting process first establishes a contract on Ethereum for voting purposes, specifying the voting topic, candidates, and detailing voting logistics, including dates and times for voting, verification, and result announcement. Additionally, a small amount of candidate information is provided to enable voters to ascertain the legitimacy of the election.

4.2 Register Phase

The primary objective of the Register phase within a voting system is to collect the public keys of eligible voters, ensuring their authentication and enabling their participation in the voting process securely. In a national election scenario, voter registration could be executed through the following:

(1) Registration Stations: Physical stations where citizens register using their digital identity cards. This method guarantees that only individuals possessing legitimate identity cards can enroll and engage in the voting process.

(2) Government-Facilitated Registration: If the initiator is a governmental body, citizens' public keys might already be in possession of the government. Consequently, the Registration phase could be conducted internally, utilizing the government's existing citizen database.

(3) Online Registration Portal: An online platform could be developed where citizens with digital identity cards upload their public keys securely using digital signatures. This approach ensures convenient registration while safeguarding the participation of only those with valid digital identities.

The Register phase acts as the linchpin connecting voters to their public keys, verifying identities, and maintaining voting process integrity. Tailored registration methods effectively authenticate voters, ensuring electoral legitimacy.

4.3 Vote Phase

During the Vote Phase, voters wield the ability to remotely cast their votes worldwide via the internet. With their system-endorsed public and private key pair and their chosen candidate in hand, they initiate the ballot creation process. This involves merging their candidate's number with a random counterpart, then employing a specialized hashing algorithm for irreversible transformation. Following this, the vote's hash undergoes cryptographic signing using the private key and is jointly uploaded

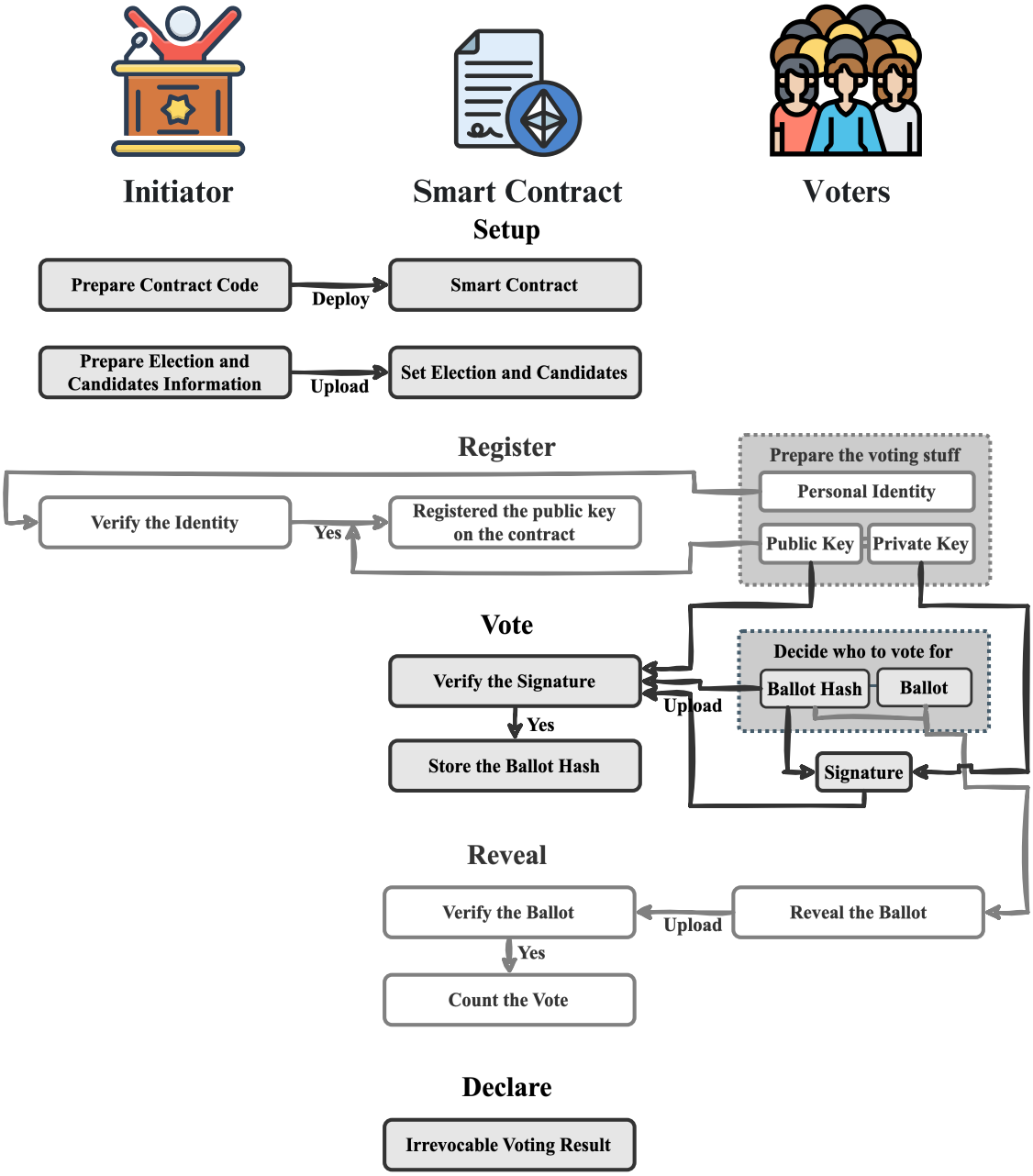


Figure 1: An Overview of System Architecture Work Flow

with the public key to the contract, thereby concluding the voting sequence. Leveraging a predefined function, voters can ascertain the success of their vote by verifying existing records tied to their public key. By meeting the requisite gas fees for miners' computational efforts, they seamlessly integrate their voting outcomes into the blockchain.

4.4 Reveal Phase

In the Reveal phase, voters demonstrate the relationship between their cast ballot and its corresponding hash value, thereby indirectly confirming the existence of a vote for a particular candidate during the vote phase. It is foreseeable that indiscernible candidate numbers may also be included in the pool of hashed ballots. Hence, caution is warranted during the vote phase in selecting and securely storing the ballot to ensure its successful disclosure during the reveal phase for the vote to be counted accurately. The significance of the reveal phase lies in its preventive measure against premature disclosure of voting outcomes, detailed reasons for which will be discussed in the methodology section of the subsequent chapter.

4.5 Declare Phase

In the Declaration Phase, in addition to revealing the actual voting results, metrics such as the vote rate and reveal rate are also disclosed to assess whether the voting outcomes adequately represent the entire community's opinions, detect any discrepancies, and determine if a revote is necessary. In our hypothetical scenario of citizen voting in K-country, we introduce a policy of providing subsidies based on ballot receipts to encourage public participation and increase voter turnout. With smart contracts recording all state transitions, obtaining records of public-private key pairs of voters who have successfully cast and revealed their votes is straightforward. Leveraging this record, the government can provide ETH subsidies to participating voters' accounts, thereby reallocating funds from traditional voting procedures to decentralized miners.

5 Methodology

In this chapter, we delve into four critical technologies utilized in this voting system. First, we explore how ring signatures are employed to ensure voter anonymity. Next, we address the issue of double voting by the same individual using linkable ring signatures. To solve the problem of premature opening of votes, we implement the commit-reveal scheme. Finally, to balance the reduction of overall election costs and the protection of voter privacy, we adopt the partition ring method. This chapter provides a detailed explanation of these four key technologies.

5.1 Ring Signature Scheme

Preserving the anonymity of voting presents a challenge when employing traditional digital signature techniques, as they risk divulging the signer's identity, thus compromising the integrity of the vote. Enter ring signatures, a solution to this problem. The defining characteristic of ring signatures is their capacity to mask the identity of the signer within a group of other signers, forming a circular chain of signatures. Only individuals possessing at least one private key from within the ring can generate such a signature. Conversely, it should be challenging for an individual to generate a legitimate

ring signature for any given message without possessing any of the private keys.

In the context of a ring signature, a group of entities is defined, each possessing their unique public/private key pairs denoted as (pk_1, sk_1), (pk_2, sk_2), ..., (pk_n, sk_n). When an entity, say i, wishes to sign a message (m), they employ their individual secret key (sk_i) alongside the public keys of the other members within the group $(m, sk_i, pk_1, \ldots, pk_n)$. This design enables the verification of the group's authenticity using the group's public key, while preventing the derivation of a valid signature without knowledge of the private keys within the group.

5.1.1 Generate A Ring Signature

Let sk_i be the signer's private key and pk_i be the corresponding public key, g is the base point on the elliptic curve, known as the generator, and "$\cdot$" represents scalar multiplication on the curve, i.e.,

$$pk_x = sk_x \cdot g$$

The hash function $\text{Hash}(m, A)$ where m is the message to be signed and A is a point on the elliptic curve. A reference implementation of the hash function concatenates the byte data of m and A, then applies a traditional hash function (e.g., keccak256) and takes the result modulo N.

$$\text{Hash}(m, A)$$

The signer first collects $n-1$ public keys of other users who have previously used the system.

$$pk_0, pk_1, \ldots, pk_{i-1}, pk_i, pk_{i+1}, \ldots, pk_{n-1}$$

The signer than generates $n-1$ random values:

$$(s_0, s_1, \ldots, s_{i-1}, s_{i+1}, \ldots, s_{n-1})$$

The signer also generates a random value k and calculates c_{i+1}, as the first c to compute.

$$c_{i+1} = k \cdot g$$

Each c_x within the ring signature will be computed using the recursive formula outlined.

$$c_x = \text{Hash}(m, s_{x-1} \cdot g + c_{x-1} \cdot pk_{x-1})$$

This recursive formula dictates that given the knowledge of s_{x-1} and the hash value c_{x-1} corresponding to the $x-1$ public key, the hash value c_x corresponding to the subsequent public key will be derived. It is noteworthy that when $x = 0$, the preceding x effectively becomes $n-1$.

$$\begin{aligned}
c_{i+2} &= \text{Hash}(m, s_{i+1} \cdot g + c_{i+1} \cdot pk_{i+1}) \\
c_{i+3} &= \text{Hash}(m, s_{i+2} \cdot g + c_{i+2} \cdot pk_{i+2}) \\
&\ldots \\
c_{n-1} &= \text{Hash}(m, s_{n-2} \cdot g + c_{n-2} \cdot pk_{n-2}) \\
c_0 &= \text{Hash}(m, s_{n-1} \cdot g + c_{n-1} \cdot pk_{n-1}) \\
c_1 &= \text{Hash}(m, s_0 \cdot g + c_0 \cdot pk_0) \\
&\ldots \\
c_i &= \text{Hash}(m, s_{i-1} \cdot g + c_{i-1} \cdot pk_{i-1})
\end{aligned}$$

To integrate the ring signature, it is imperative to ascertain the correct s_i. The following equation aids in this endeavor, provided sk_i is available. It is noteworthy that the absence of sk_i renders the completion of the ring impossible, consequently invalidating the ring signature. Therefore, only individuals possessing at least one sk_i can utilize the ring signature.

$$c_{i+1} = \text{Hash}(m, s_i \cdot g + c_i \cdot pk_i)$$
$$k \cdot g = s_i \cdot g + c_i \cdot pk_i$$

Rearranging to solve for s_i:

$$s_i \cdot g = k \cdot g - c_i \cdot pk_i$$
$$s_i \cdot g = k \cdot g - c_i \cdot (sk_i \cdot g)$$
$$s_i \cdot g = (k - c_i \cdot sk_i) \cdot g$$

Since scalar multiplication by g is one-to-one:

$$s_i = k - c_i \cdot sk_i$$

The final signature includes the initial hash value c_0, the set of public keys $pk_0, pk_1, \ldots, pk_{n-1}$, and the set of s values $s_0, s_1, \ldots, s_{n-1}$:

$$\sigma_{pks}(m) = \{c_0, pk_0, pk_1, \ldots, pk_{n-1}, s_0, s_1, \ldots, s_{n-1}\}$$

5.1.2 Verify A Ring Signature

The verifier obtains the $\sigma_{pks}(m) = \{c_0, pk_0, pk_1, \ldots, pk_{n-1}, s_0, s_1, \ldots, s_{n-1}\}$ along with the message m. Subsequently, the verifier recalculates the hash values $c_1, c_2, \ldots, c_{n-1}$ using the recursive formula:

$$c_x = \text{Hash}(m, s_{x-1} \cdot g + c_{x-1} \cdot pk_{x-1})$$

Continue this process until c_0' is calculated from c_{n-1}, and verify the signature by checking if:

$$c_1 = \text{Hash}(m, s_0 \cdot g + c_0 \cdot pk_0)$$
$$\ldots$$
$$c_{0'} = \text{Hash}(m, s_{n-1} \cdot g + c_{n-1} \cdot pk_{n-1})$$
$$c_0 = c_0'$$

If the values match, the signature is valid; otherwise, it is invalid.

5.2 Linkable Ring Signature

The anonymity provided by ring signatures opens the door to potential 为 repeated voting by the same individual, as their identity remains indistinguishable. Consequently, Joseph K. Liu et al. introduced the innovative concept of Linkable Ring Signatures [6]. Incorporati a unique identifier $\tilde{y}$ into the signature distnginguishes a specific signer, allowing different messages from that signer to be identified as originating from the same key. Additionally, employing hash functions ensures the complexity of establishing a link between the identifier and the key, thereby preserving anonymity.

Select the list of public keys $pks = \{pk_0, pk_1, \ldots, pk_{n-1}\}$, where each sk_x is a distinct public key. The signer has a private key sk_i corresponding to the public key pk_i.

Two cryptographic hash functions are used:

- H_1: This hash function takes multiple inputs, including the list of public keys pks, the derived value $\tilde{y}$, the message m, and certain intermediate values.
- H_2: This hash function takes the list of public keys L as input and produces a fixed-size output h. This value is unique to the set of public keys and is used to compute $\tilde{y}$.

The value $\tilde{y}$ is a critical component that ensures the linkability property. It is computed in a way that ties it to the signer's private key and the public key list, ensuring that multiple signatures from the same signer can be linked. Allowing signers to generate random $\tilde{y}$ values would break this linkability and compromise the security and integrity of the entire scheme. Therefore, the protocol enforces the computation of $\tilde{y}$ in a specific manner to maintain its cryptographic guarantees.

Algorithm 1 Generating A Linkable Ring Signature

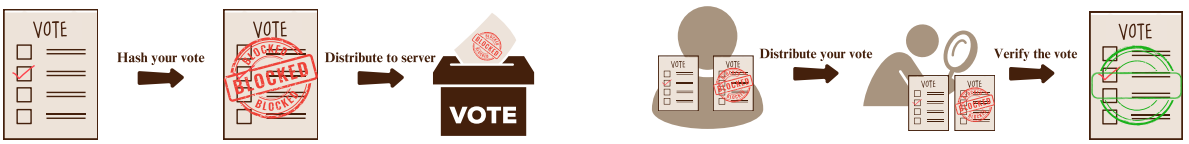
Require: List of public keys $pks = \{pk_0, pk_1, \ldots, pk_{n-1}\}$, signer's private key sk_i, message m
Ensure: Linkable Ring Signature $\sigma_{pks}(m) = (c_0, pk_0, \ldots, pk_{n-1}, s_0, \ldots, s_{n-1}, \tilde{y})$
Compute $h = H_2(L)$ and $\tilde{y} = h^{sk_i}$
Pick a random $k \in \mathbb{Z}_q$
Compute $c_{i+1} = H_1(pks, \tilde{y}, m, g^k, h^k)$
for each x from $i+1$ to $n-1$, and then from 0 to $i-1$ **do**
    Pick a random $s_x \in \mathbb{Z}_q$
    Compute $c_{x+1} = H_1(L, \tilde{y}, m, g^{s_x} y_x^{c_x}, h^{s_x} \tilde{y}^{c_x})$
end for
Compute $s_i = k - sk_i \cdot c_i \mod q$
return $(c_1, s_1, \ldots, s_n, \tilde{y})$

Algorithm 2 Verifing Linkablillity

Require: Two signatures $\sigma'_{sks}(m') = (c'_0, s'_0, \ldots, s'_{n-1}, \tilde{y}')$ and $\sigma''_{sks}(m'') = (c''_0, s''_0, \ldots, s''_{n-1}, \tilde{y}'')$
Ensure: Linkability result: linked (1) or not linked (0)
Verify each signature separately to ensure they are valid
if $\tilde{y}' = \tilde{y}''$ **then**
    return 1 {Signatures are linked}
else
    return 0 {Signatures are not linked}
end if

5.3 Commit-Reveal Scheme

Even with linkable ring signatures, voting systems still face a serious issue: "premature opening." Premature opening means the voting results are known early, which can discourage people from voting. In decentralized systems, there is no mechanism to prevent others in the community from peeking at



(a) Commit Phase (b) Reveal Phase

Figure 2: An overview of Commit-Reveal Scheme

the voting results during the voting phase. It is challenging to cryptographically separate the voting phase from the revealing phase decisively.

To address this, someone proposed the Commit-Reveal Scheme. The Commit-Reveal Scheme is a cryptographic protocol designed to enhance privacy and security in various blockchain applications by splitting the information disclosure process into two distinct phases: commit and reveal. In the commit phase, participants submit a hashed version of their information, effectively hiding the original data while proving its existence. Later, in the reveal phase, they disclose the original information, which the network verifies by comparing it to the initial hash. This two-step process ensures that sensitive data remains confidential during the commitment period and is only revealed at the appropriate time, fostering trust and transparency in activities such as voting, auctions, and sealed-bid contracts.

The following provides a detailed explanation of how the Commit-Reveal Scheme is applied to this voting system. During the voting phase, all voters first generate a ballot composed of a ”candidate number” + ”_” + ”random number”, where the candidate number is the number of the candidate voters wish to vote for, and the random number ensures that the resulting hash is highly unlikely to collide with others. Next, the voter uses the recognized one-way function keccak256 to produce a ballot hash and then signs this ballot hash with the mentioned linkable ring signature. Before the voting phase ends, the voter submits the ballot hash via the vote function of the smart contract.

In the reveal phase, voters disclose the original ballot and its relationship to the ballot hash. The contract first verifies the existence of a legitimate ballot hash submitted during the voting phase, then checks the authenticity of the relationship between the ballot and the ballot hash. If validated, the ballot hash is verified, and the vote is counted. It is crucial that voters remember their ballot during the reveal phase; otherwise, losing the ballot means their vote will not be successfully counted.

5.4 Partition Ring

There remains one final issue with ring signatures that has not been previously discussed: the polynomial time complexity of the computational load. As the number of participants in the ring signature increases, the ring size grows, leading to a larger overhead for each individual signature.

From Figure 3, it can be observed that the Decentral Election Method (DE), which solely relies on ring signatures, results in a polynomial increase in total gas spend. This is because, with more voters, each voter’s ring signature becomes larger, increasing both computational and storage costs.

To address the issue of the ring size increasing with the number of voters, we partition the voters, distributing them into different clusters. Each voter then uses the public keys of other voters within their cluster to sign their ring signature.

However, it is evident that the anonymity of each voter, which was originally hidden among all voters, now becomes limited to their cluster. Consequently, if a cluster contains only two voters, it is easy for one voter to infer the candidate chosen by the other voter, thereby violating the principle of

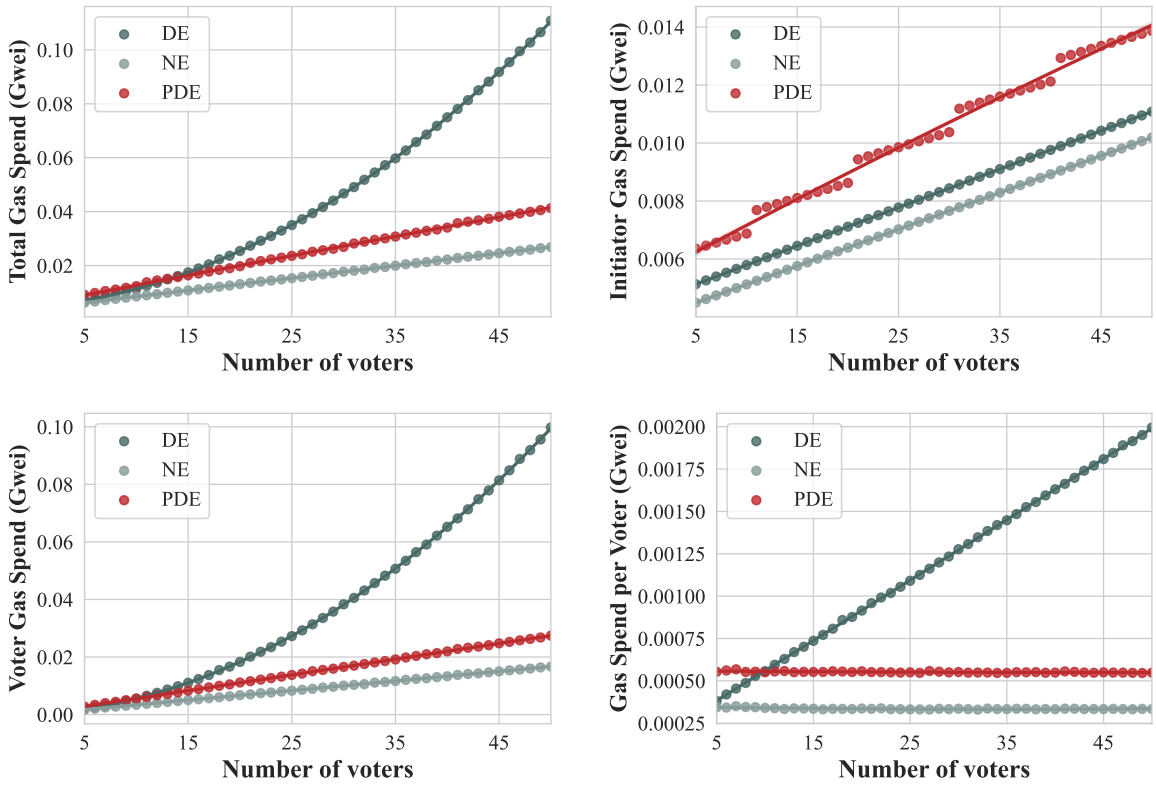


Figure 3: Effect of voter count on gas spend. PDE entails 10 voters within a single cluster.

anonymous voting. Therefore, the size of the clusters must be appropriately determined. The impact of cluster size on the overall election cost will be discussed in subsequent chapters.

This paper proposes partitioning the original large ring into smaller rings and having signatures completed within these smaller rings. The smart contract will then count the votes in a unified manner. Partition Decentral Election Method (PDE) effectively reduces the originally polynomial election costs to a constant.

6 Simulation Result

6.1 Simulation Settings

Our simulation is conducted on the virtual Ethereum chain using Truffle and Ganache. Considering the current operational state of Ethereum, we have set the gas limit to 30 million and the gas price to 20 Gwei. The simulation is performed on a computer with an Apple M1 processor and 16GB of memory, simulating an election scenario where five candidates participate in the voting.

The PDE (with ten voters per cluster) will be compared with the baseline DE and the Naive Election Method (NE), which does not guarantee anonymity by linkable ring signature. We will analyze total gas spend, initiator gas spend, total voter gas spend, and gas spend per voter.

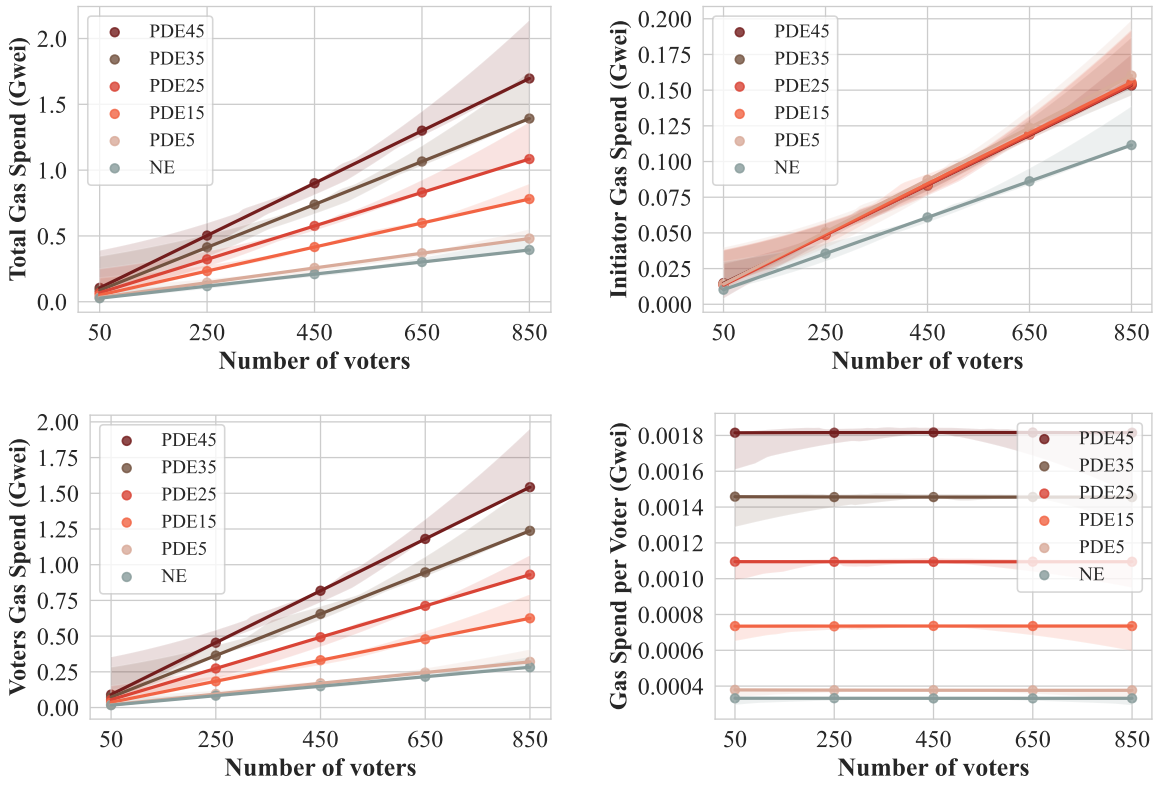


Figure 4: Effect of voter count on gas spend

6.2 Small amount of Voters

In the first part, we discuss the differences among the three methods, with the number of voters ranging from 5 to 45. Since participants exceeding 50 significantly increase the DE method's computation time, experiments with more voters will be conducted in the next section without DE.

From Figure 3, it is observed that the total gas spend in DE increases polynomially, while PDE slightly exceeds NE but maintains a linear growth trend. A deeper analysis reveals an interesting pattern where the initiator gas expenditure in PDE increases in a stepwise manner. This occurs because, whenever the number of voters exceeds ten, an additional cluster must be created, and dummy voters must be added, leading to extra costs for the initiator.

Furthermore, the primary difference between DE and PDE is evident in the growth rate of voter gas expenditure. In DE, each voter's ring signature verification within the election contract incurs increasing computational costs as the number of voters grows, whereas PDE effectively limits this growth. This issue is particularly noticeable in the gas expenditure per voter chart.

From the results, we can observe the optimization achieved by PDE over DE in terms of total gas expenditure. In a scenario with 25 voters, the total gas expenditure for DE is 35,041,151, whereas for PDE it is significantly lower at 23,610,276. This indicates that PDE reduces the total gas expenditure by approximately 33% in this case. In a scenario with 50 voters, the total gas expenditure for DE is 110,852,396, while for PDE it is 41,297,646. This demonstrates an even more substantial reduction, with PDE decreasing the total gas expenditure by approximately 63%.

6.3 For More Voters

From the results shown in Figure 4, we extended the number of voters to nearly a thousand and compared the impact on computational costs by varying the cluster size from 5 to 45. Specifically, for 250 voters, the total gas expenditure for PDE with a cluster size of 45 (PDE45) is 502,662,642 wei, whereas for PDE with a cluster size of 5 (PDE5), it is 144,913,629 wei, resulting in a difference of approximately 3.46 times. For 850 voters, the total gas expenditures for PDE45 and PDE5 are 1,696,045,204 wei and 480,281,370 wei, respectively, with a difference of about 3.53 times. The ratio remains relatively close but shows a slight increasing trend due to the proportionally lower setup costs.

When comparing PDE5 with NE for 250 voters, the total gas expenditures are 144,913,629 wei and 118,654,411 wei, respectively, with a difference of about 1.22 times. For 850 voters, the total gas expenditures for PDE5 and NE are 480,281,370 wei and 393,558,707 wei, respectively, also showing a difference of approximately 1.22 times. This indicates that the difference between PDE5 and NE does not significantly increase with the growing number of voters.

From the results, we can observe that the spending of a single voter is directly proportional to the size of the ring, independent of the number of participants. Conversely, the influence of ring size on Initiator gas spend is negligible.

7 Discussion

7.1 Why the Commit-Reveal Scheme is a Big Deal

Critics may argue that during the vote reveal phase, voters might lack the motivation to reveal their votes if they perceive the election results as already determined, which could decrease reveal rate while reducing the costs borne by the voters. Our perspective is that the cost of revealing a vote is significantly lower than the cost of voting itself; thus, incorporating the commit-reveal mechanism is beneficial for increasing voter turnout. Furthermore, the difference between voter turnout and reveal rates can help determine if a substantial number of voters have failed to reveal their votes. If only a few voters forget to reveal or are dissuaded by the aforementioned reasons, the final outcome remains unaffected. Therefore, we believe the commit-reveal mechanism is essential.

To address this issue, the government could subsidize the addresses where votes are revealed, encouraging all voters to complete both voting and revealing process. By accurately tallying completed ballot addresses, rewarding voters for accurate voting becomes feasible.

7.2 The Immutable Feature of Ethereum: A Catalyst for Online Elcetion

In modern virtual elections, the primary issue lies in the public's lack of trust in government-conducted online elections and the difficulty in verifying the accuracy of the voting results. Despite some degree of transparency provided by the government, the anonymous nature of voting makes it challenging to fully disclose the entire voting process. This situation presents an opportunity for election manipulators to alter results without detection by the populace, who may only sense that the results contradict mainstream opinion, thereby exacerbating social conflicts. This challenge hinders the implementation of online elections worldwide.

Our system leverages the immutable characteristics of Ethereum. Once the smart contract is deployed on the blockchain, even the contract creator cannot alter the election content through methods

outside the provided functions. As long as there are no vulnerabilities in the smart contract, there is no risk of election result tampering by the organizers. Every participant must adhere to the rules of the smart contract, and any disruptive actions will be identified and excluded by Ethereum. Therefore, the emergence of Ethereum can be seen as paving the way for online voting. With the reduction in computational costs, online voting will become increasingly feasible.

7.3 Getting Registration Right: It' s Important!

Registration can be considered the most crucial step in the entire election process because it determines who is eligible to vote. In general scenarios, the initiator of the vote has the authority to decide voter eligibility, which seems reasonable. However, in national elections where each individual is entitled to only one vote, a malicious initiator might secretly assign multiple key pairs to their supporters while giving only one key pair to opposition voters, thereby completely undermining the fairness of the election. The only aspect that the public can verify is whether the number of registrants matches the eligible voter count, but this does not prevent minor instances of vote manipulation.

In the actual voting process, the difficulty for organizers to tamper with the vote lies in the fact that the entire voting process is monitored by multiple parties in real-time. Even if someone possesses multiple ballots, it is difficult to pass identity verification and cast multiple votes. However, the concept of an online system, where possessing a private key equates to having voting rights, disrupts this line of defense, making it possible for organizers to manipulate votes during the register phase.

Thus, the central issue for implementing an online voting system in national elections is how to register eligible voters' public keys while simultaneously monitoring government actions. Various methods for addressing this during the registration phase are mentioned in this paper, but no perfect solution has been found. The widespread adoption of digital identity cards may offer a solution. This issue remains a topic for future work.

8 Conclusion

The exploration of implementing online voting systems, leveraging technologies such as Ethereum's blockchain and ring signatures, demonstrates significant potential for enhancing the integrity and transparency of elections. By employing immutable smart contracts on Ethereum, the system ensures that election results cannot be tampered with, addressing one of the primary concerns in digital voting. Furthermore, the use of ring signatures protects voter anonymity, while linkable ring signatures help prevent double voting, ensuring a fair process.

However, challenges remain, particularly in the voter registration phase, which is crucial for maintaining the system's credibility. Ensuring that only eligible voters participate without allowing opportunities for vote manipulation by malicious actors is a complex issue that has yet a perfect solution.

Overall, while the proposed system shows promise in making online elections more secure and transparent, continuous improvements and adaptations are necessary to address the remaining challenges. The advancements in blockchain technology and cryptographic methods pave the way for a future where online voting could become a trusted and widely adopted method for conducting elections.

References

[1] S. Nakamoto, "Bitcoin: A peer-to-peer electronic cash system," 2008.

[2] V. Buterin *et al.*, "Ethereum white paper," *GitHub repository*, vol. 1, pp. 22–23, 2013.

[3] J. Lyu, Z. L. Jiang, X. Wang, Z. Nong, M. H. Au, and J. Fang, "A secure decentralized trustless e-voting system based on smart contract," in *2019 18th IEEE International Conference On Trust, Security And Privacy In Computing And Communications/13th IEEE International Conference On Big Data Science And Engineering (TrustCom/BigDataSE)*, IEEE, 2019, pp. 570–577.

[4] S. T. Alvi, M. N. Uddin, and L. Islam, "Digital voting: A blockchain-based e-voting system using biohash and smart contract," in *2020 third international conference on smart systems and inventive technology (ICSSIT)*, IEEE, 2020, pp. 228–233.

[5] S. T. Alvi, M. N. Uddin, L. Islam, and S. Ahamed, "Dvtchain: A blockchain-based decentralized mechanism to ensure the security of digital voting system voting system," *Journal of King Saud University-Computer and Information Sciences*, vol. 34, no. 9, pp. 6855–6871, 2022.

[6] J. K. Liu, V. K. Wei, and D. S. Wong, "Linkable spontaneous anonymous group signature for ad hoc groups," in *Information Security and Privacy: 9th Australasian Conference, ACISP 2004, Sydney, Australia, July 13-15, 2004. Proceedings 9*, Springer, 2004, pp. 325–335.