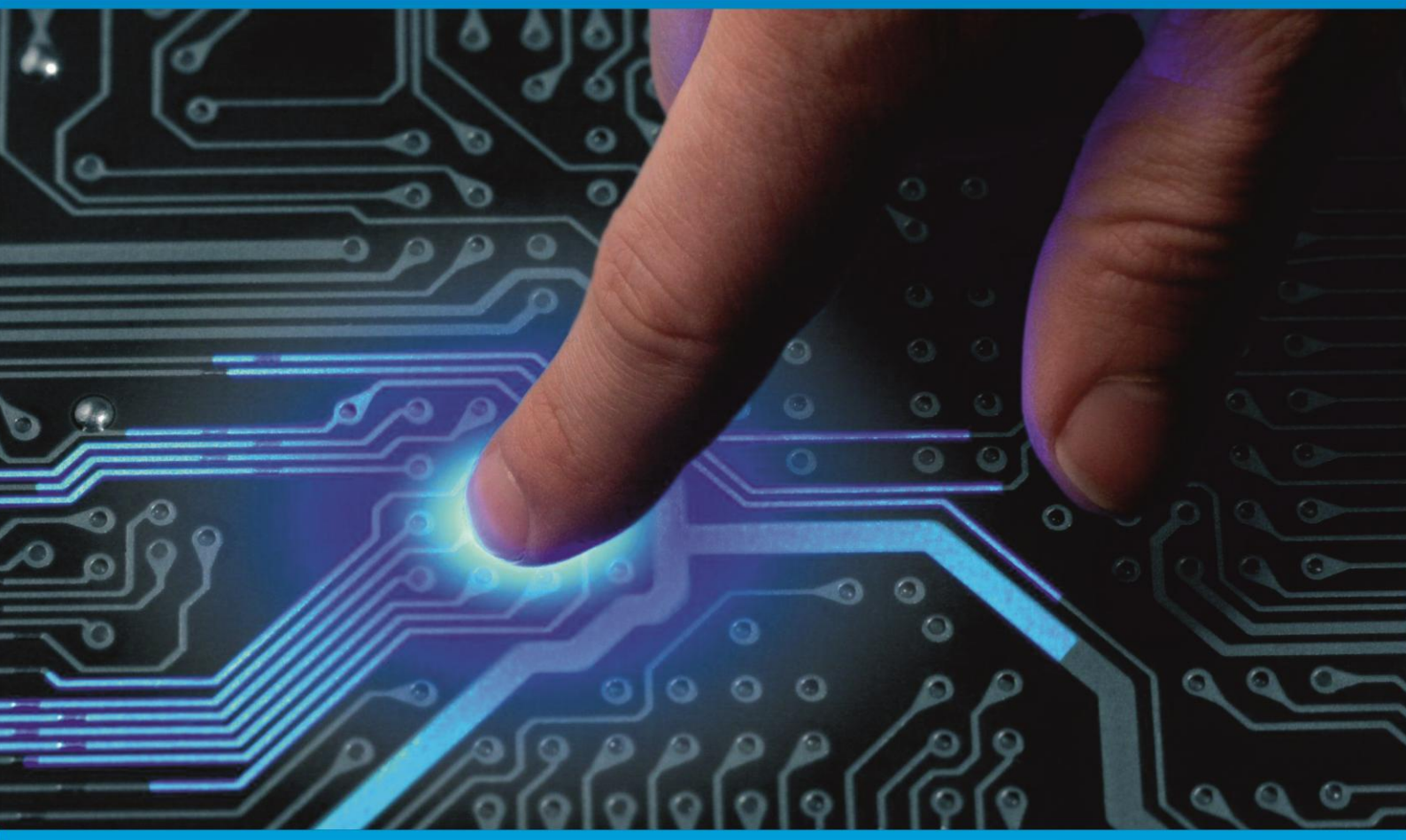
IJIRCCE

e-ISSN: 2320-9801 | p-ISSN: 2320-9798



INTERNATIONAL JOURNAL OF INNOVATIVE RESEARCH

IN COMPUTER & COMMUNICATION ENGINEERING

Volume 9, Issue 4, April 2021

INTERNATIONAL STANDARD SERIAL NUMBER INDIA

Impact Factor: 7.488

International Journal of Innovative Research in Computer and Communication Engineering

| e-ISSN: 2320-9801, p-ISSN: 2320-9798| www.ijircce.com | |Impact Factor: 7.488 |

|| Volume 9, Issue 4, April 2021 ||

| DOI: 10.15680/IJIRCCE.2021.0904173 |

Blockchain Based E-Voting System

Abhishek Bhosle[1] , Krishna Gogi[2], Danish Siddiqui[3], Ms. Smita Bansod[4]

BE Student, Dept. of I.T., Shah & Anchor Kutchhi Engineering College, Mumbai University, India[1,2,3]

Assistant Professor, Dept. of I.T., Shah & Anchor Kutchhi Engineering College, Mumbai University, India[4]

ABSTRACT: Electronic voting (e-voting) is a symbol of modern democracy activities. Due to the high ballot privacy and verifiability, e-voting system has been booming in the recent years. Particularly, Bitcoin, a digital currency system based on the cryptography, is highly open and transparent for the individual transaction. In other words, anyone can access to the transaction contents via blockchain. Besides, regarding to anonymous way it trades, the transaction of Bitcoin is untraceable. In order to prove the feasibility of protocol. This design implemented a fine web voting system software through PHP and JavaScript programming languages. A security analysis, software performance analysis and evaluation are presented in the last section. 2 On account of the pseudonymous of Bitcoin address and the openness of the blockchain, which is consistent with part of e-voting requirement. This paper proposed an e-voting protocol based on blockchain by using the ring signature algorithm. The requirements can be satisfied with ballot-privacy, individual verifiability, eligibility, completeness, uniqueness, robustness, and coercion-resistance

I. INTRODUCTION

Voting, the scheme used the blind signature to blind the message the voter used to vote and send it to the administrator [14]. After this seminal paper has been released, a lot of e-voting software had been implemented and used for the market, such as the EVOX and SENSUS. In this scheme it also has its weakness, it requires all voters must vote and once someone abstains from voting, the result can tamper. The administrator cannot find out who tamper the result. In 1996, Juang and Lei proposed a blind signature based voting scheme but requires everyone should attend the voting event. After 3 years, M. Ohkubo, F.Miura and M.Abe promoted the FOO scheme by using a threshold encryption protocol and the Mix-Net communication channel which can keep the privacy of the voter. For the voters, they can need not to participate the tallying part of the event and they can walk away after voting [25]. With the development of e-voting system, there are a series of criminal behaviors related to the e-voting, such as electoral fraud, threat a voter or vote buying. To deal with these problems, many new requirements or properties of e-voting scheme have been proposed likes the receipt-freeness and coercion-resistance. The receipt-freeness means that the voter cannot prove the vote result to anyone after voting. In 1994, Benaloh discussed the terminology named receipt-freeness firstly[2]. Although Benaloh uses homomorphic encryption to make the implementation of receiptfreeness, Martin Hirt argued that it will not be valid if there are more than one tally authority. In 1995, V.Niemi and A.Renvall raised a scheme by adopting the receipt so that the voter cannot prove who he or she votes for[24]. At the same time, K Sako and J Kilian proposed the first Mix-Net based protocol satisfied with receipt-freeness [30]. This protocol is under the assumption that there is no private channel between the voting station and the voters. After one year, Okamto uses a non-anonymous channel, a private channel and the bulletin board to propose a voting scheme satisfied receipt-freeness[26]. Unfortunately, this protocol has been proved does not satisfy with receipt-freeness. In 2000, M.Hirt and K.Sako use homomorphic ElGamal encryption technique to design a private channel protocol with receipt-freeness, but this protocol does not suit for the large-scale election[15]. In 2001, O.Baudron proposed a new scheme to satisfy this property by using Paillier cryptosystem and the zero-knowledge proof[1]. In recent years, a lot of researchers focus on the receipt-freeness and coercion-resistance of e-voting. In 2010, Juels introduced the new direction of e-voting which named coercionresistance and proposed a scheme[18]. In 2012, O.Spycher and R.Koenig promote his scheme by adding the random integer f. The proposed scheme will get the encrypted integer C. The tally authority can judge if there is any fake ballot through decrypting C to the random integer f[32]. The coercion-resistance can be satisfied further. By the developing of the decentralized digital currency, some researchers argued a way to vote and tally on the blockchain. In 2015, Czepluch discussed the application domains of the blockchain and argued that blockchain can use for the e-voting [11] . At the same time, Z.Zhao and THH.Chan proposed a way to vote using Bitcoin and zk-SNARKs

With the properties named privacy, verifiability and irrevocability [34]. In 2016, a protocol using Zerocoin has been proposed and ensures most properties of the e-voting[33]. However, using a Zerocoin is hard to make the implementation to the software. At the same year, C.Jason, Paul and K.Yuichi proposed a protocol using blind-signature and Bitcoin cards [16]. However, it cannot protect the privacy in some situation, for instance, if the

| e-ISSN: 2320-9801, p-ISSN: 2320-9798| www.ijircce.com | |Impact Factor: 7.488 |

|| Volume 9, Issue 4, April 2021 ||

| DOI: 10.15680/IJIRCCE.2021.0904173 |

administrator knows the Bitcoin address of the voter, the administrator can know who the voter is by linking the address and message on the blockchain. 1.2.2 Related Applications The research of e-voting system is widely used nowadays. Some partial practices are listed as follows. In 2000, e-voting has been used in US Election[8]. Although it is an experiment in some area of Florida, it was a milestone in the development of e-voting. In 2002, United Kingdom tried out an electronic voting system. 16 public authorities were awarded to build the e-voting system. After 1 year, more than 18 authorities were award[22]. In 2004, US election used an electronic voting system DRE for the first time[5]. India uses this system for parliamentary elections on a national scale. In 2007, France UMP party made a history of internet-based voting.More than 31,000 voters vote in UMP to in 2007 French Presidential election[13]. This was the first mass E-voting activity in history. In 2009, China used electronic voting for the election of the grass-roots organization in Hangzhou. There were 3122 residents enrolled this voting activity with an electronic touch screen[21]. In 2014, the election of Ministry of National Education(France) received 1,760,000 ballots[21]. It took the lead in legal and security network voting, thus popularized the channels of network voting.
In 2008, the founder of Bitcoin S.Nakamoto published a paper [23] to specify a cryptocurrency system based on the peer-to-peer network. The Bitcoin has changed the traditional way of the cash payment system. With the development of the Bitcoin, Blockchain technology has aroused the attention of people. The blockchain is a public ledger, all individuals can synchronize the latest ledger into local and they have no permission to tamper the content of the public ledger. To distinct various blockchain, there are two categorizations of the blockchain[27]. One is classified by the requirement of the network nodes to the verification process.

• **Permissionless blockchain:** No central service or authority is required to compute during the verification process. Usually, this computational process happens in the device of anyone.

• **Permissioned blockchain** : There is a central network used for confirming the verification nodes.

Another one is classified by the publicity of the blockchain.

• **Public blockchain**: Anyone in the world can read, download, broadcast the transaction of the blockchain.
• **Private blockchain**: The blockchain only belongs to the individual, government or an organization which is not public.

In recent years, the Bitcoin and Ethereum are ever-increasing popular. They both are the permissionless and public blockchain. For the Bitcoin, it has 2 sub network, the Bitcoin network and the test net. The test net is the testing environment of the Bitcoin network. In this network, the coin does not has any value. It is free to use and get the test coin form the faucet[19]. Ethereum is a digital currency similar to Bitcoin. It is also a complete set of decentralized application platform. While using Ethereum for digital currency trading, anyone can publish and use decentralized applications on Ethereum. Ethereum's advantage is that it provides a complete toolchain for decentralized application development, deployment. By using smart contract, it makes block-chain-based application development extremely convenient.
Since the birth of the blockchain, the blockchain has the properties of decentralization, decentralized trust, common maintenance, data reliability, privacy protection. It has been unprecedented attention and its development is very rapid.
• **Decentralization:** The blockchain is decentralized. There is no central computing devices to store the ledger of transactions. Every node of blockchain store the same copy.
•**Hard to forge:** Due to its decentralization, every block should be distributed to every node around the world.
•**Transaction traceable:** Each transaction in the blockchain is open and transparent. Every transaction details includes the sender address and the receiver address, which anyone can trace a transaction.

In this paper, we proposed a protocol based on Bitcoin. For each transaction, everyone can download the information from the blockchain. In the Bitcoin, every Bitcoin address has no relation to its personal identity. Therefore the blockchain is pseudonymous for anyone and has the transparent transactions, which has the same requirements for the e-voting properties

E-voting scheme Properties:

In recent 30 years, more and more e-voting protocols has been published. The major properties of e-voting scheme can be described from the papers wrote by Cranor[10], Cetinkaya[6] and Fujioka[14]. Basic Properties Ballot privacy: Anyone cannot know whom the voter voted for. The ballot is hidden from outside observers. Individual verifiability: The voter can verify his ballot is counted correctly after he voted. Eligibility: Only the legal voters can enroll the voting

| e-ISSN: 2320-9801, p-ISSN: 2320-9798| www.ijircce.com | |Impact Factor: 7.488 |

|| Volume 9, Issue 4, April 2021 ||

| DOI: 10.15680/IJIRCCE.2021.0904173 |

event. Accuracy/Completeness: Every vote should be counted correctly. Fairness: Nothing can influence the result of voting. If the system leaks the voting result or the authority adds a voter during the voting, the event can be defined as unfair. Uniqueness: Every voter can only vote once. The voter will have no permission to vote more if he votes. Robustness: Anyone cannot influence or modify the final voting result when tallying. Advanced Properties Universal Verifiability: Anyone can verify the eligibility of each ballot and the impartiality of the result. Receipt-freeness: The voter cannot receive or try to build any receipt after he voted to prove how he vote. Coercion-Resistance: There is no coercer can cooperate with the voter. The voter cannot prove who he voted.

Blockchain:

Generating a Bitcoin address:

To broadcast a message on the blockchain, the participators need a Bitcoin address. By using SHA256, RIPEMD160 Hashing and Base58 Encoding, the Bitcoin address can be generated as Fig

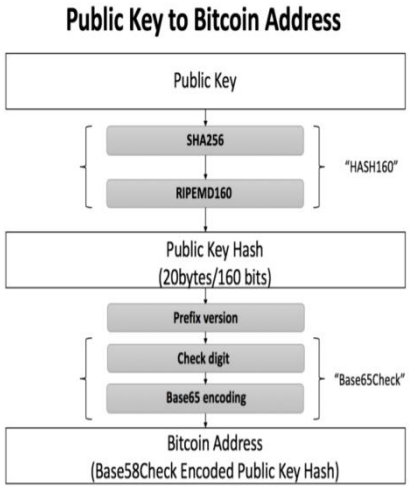


Fig.1.1. Public Key to Bitcoin Address

1. Generate the private key by Elliptic Curve Digital
   Signature Algorithm, generally named secp256k1. The size of the Bitcoin private key is 256 bits.

2. Generate the Bitcoin public key from the Bitcoin private key (x, y) with the DER format.

3. Hash the Bitcoin public key as PKhash160 into hash160 by producing the SHA256 and RIPEMD160 algorithm.

4. Add the prefix of the version at the head of PKhash160 according Table 2.1. Define the intermediate hash value of public key fingerprint = prefix ix + PKhash160, which is also named the fingerprint.

5. Define Sha256(Sha256(fingerprint)) as the check digit d. Adding the d at the end of fingerprint.

6. Generate the final Bitcoin address by encoding fingerprint + d with the Base65 encoding algorithm. Define address = Base65(fingerprint+d) as the final Bitcoin address.

Methodology

OP RETURN To discuss the OP RETURN of the blockchain. we should consider the transaction first.
For each transaction on Bitcoin, it contains the input script and the output script as the fig

The Figure is shown the transaction between Alice and Bob who are the transaction participators.

| e-ISSN: 2320-9801, p-ISSN: 2320-9798| www.ijircce.com | |Impact Factor: 7.488 |

|| Volume 9, Issue 4, April 2021 ||

| DOI: 10.15680/IJIRCCE.2021.0904173 |

Here is an example of a transaction between Alice and Bob with the reference of "haha" on the blockchain of test net.

Define the Bitcoin address of Alice as mxLqfJvTTEojWVZVTanEcXs1kXaBkdoqfX, and the Bitcoin address of Bob as n4Kc1AwFos3aZRvD3Tc9imzeMeA8E9DEUr.

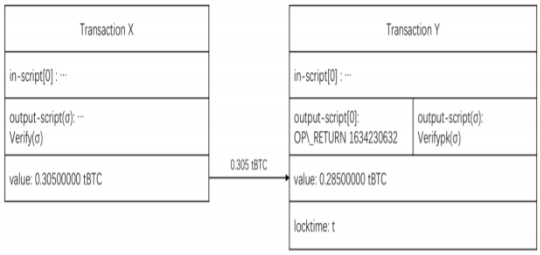


Fig.1.2. Transaction between Alice and Bob

Alice creates Transaction Y with the input of one transaction. In order to confirm Transaction Y in the blockchain, the input-script [0] should refer to the Transaction X. The output script of Transaction Y contains 2 parts. One is the signature for Transaction Y which is signed by the private key of Alice SK. Another is the OP RETURN code which is the reference of "haha". OP RETURN is a stack-based script without loops. As it is defined in the protocol of Bitcoin, it can store up to 80 bytes in the transaction. The lock time t means the Transaction Y should not be placed before time t [34].

To confirm this transaction before t, the transaction creator Alice should pay the mining fees to the miner. The miner can use the PoW(Proof of Work) algorithm to find a block including Verifypk(σ). Finally, the Bob will receive the money with the reference of "haha". Further, to specify this example, this example has been made in the network of test net. The details can be listed in the Table.

From the Table, we can see that output-script [0] indicates the OP RETURN which is 1634230632. To decode the OP RETURN, we can use hex2bin() algorithm to convert it to the characters.

Transaction ID	025e4fd916832c4028b1bcc446c8a41c10798fbea49793ce245ccf700e621d4f
input[0]	mprsHi9HKpn9bH14ZZV7YC7mxdRJ6wws7r(0.12249999)
input-script[0]	3045022100b7a6e8aa5cd553e4c21ad68e851c140c3e87d3eefc4d0a 3045022100ae906a357c927d170f19710aca1de3c5ebcbe2c60fe9 626b24ed876d7f23fad40220354d0b0c254679817deac98f4fcfa 33be48eaf74c77a2e0b4db2046747cb2b3d0102ce592b293c66 88ca587dea59780acca8da8215d4d3261db338e9ea39fc46ae19
input-value[0]	0.30500000
output[0]	OP_RETURN 68616861
output-script[0]	OP_RETURN 1634230632
output-value[0]	0.00000000
output[1]	n4Kc1AwFos3aZRvD3Tc9imzeMeA8E9DEUr
output-script[1]	OP_DUP OP_HASH160 fa25611aeed75a33a9fc8cc83d2039059c37d837 OP_EQUALVERIFY OP_CHECKSIG
output-value[1]	0.28500000
tx_hex	0100000001cfbd41e842b9f6752b8a76e4803ded991bdbf0c1ec193e5add bfc8467c1b6d1c010000006b483045022100ae906a357c927d170f19710a ca1de3c5ebcbe2c60fe9626b24ed876d7f23fad40220354d0b0c25467981 7deac98f4fcfa33be48eaf74c77a2e0b4db2046747cb2b3d012102ce592b 293c6688ca587dea59780acca8da8215d4d3261db338e9ea39fc46ae19ff ffffff020000000000000000066a046861686120e0b2010000000001976a9 14fa25611aeed75a33a9fc8cc83d2039059c37d83788ac00000000

Fig.1.3. An example of Bitcoin testnet transaction

In this example, by decoding the OP RETURN 1634230632, we can get the message "haha". The OP RETURN can store the messages. In this implementation, we use it to store the ring signatures and candidate id.

Cryptography:

RSA Algorithm RSA algorithm is a kind of asymmetric the cryptographic algorithm which used to encrypt and decrypt the messages[29]. Its security is based on the difficulty of large integer decomposition. There are many implementations in reality. The specific algorithm can be described as follows.

1. Choose two different large prime numbers.
2. Define $n = pq$, $\phi(n) = (p - 1)(q - 1)$.

| e-ISSN: 2320-9801, p-ISSN: 2320-9798| www.ijircce.com | |Impact Factor: 7.488 |

|| Volume 9, Issue 4, April 2021 ||

| DOI: 10.15680/IJIRCCE.2021.0904173 |

3. Choose e ∈ [0, ϕ(n) − 1].
4. Calculate the modular multiplicative inverse of ϕ(n) as d which ensures ed = 1 mod ϕ(n).
5. Define e, n as public key and p, q, d as private key
6. Encryption: Give the message x, compute y = x d mod n to encrypt the message by using the public key (e, n).
7. Decryption: Give the ciphertext y, compute x = y d mod n to encrypt the message by using the private key (p, q, d).

Ring Signature

In 2001, Rivest, Shamir and Tauman proposed a question that how to leak a secret[28]. To answer this question, they told a story about a member of cabinet informs against Prime Minister. Bob is a member of the cabinet who wants to leak a message about the illegal actives about the Prime Minister to the journalist. To ensure his safety, Bob must inform him an anonymous channel then the journalist can easily verify his identity of the cabinet. To solve this problem, Bob cannot use a group signature scheme to send the message because he cannot confirm if the group administrator is controlled by the Prime Minister.

They proposed a new scheme called ring signature, and each member of the cabinet is the ring member and everyone is equal and anonymous.

The ring signature scheme can be described as follows. Supposing the scheme has a number of n members. For each user ui , he has his own public key yi and his private key xi and they sit down in a ring as the Figure .

The scheme can be divided into 3 parts: Generating a key pair, generating a ring signature and verifying the signature.

Generating a key pair: A key pair generator algorithm for the signer through computing the symmetric key ki . The algorithm can compute each public key yi and private key xi from the ki .

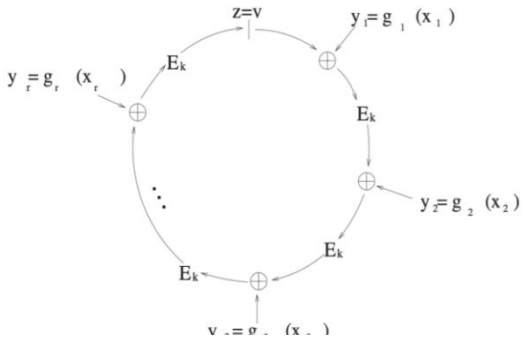


Fig.1.4. Ring signature

Generating a ring signature: By inputting the message m, numbers of n and its public keys list L = y1, y2, y3, .., yn and the private key xi of the signer, the algorithm can output a signature which is called the ring signature as σ.

Verifying the signature: By inputting the message m and the ring signature σ. If σ is the signature of m, output true and else output false. For the ring signature, the security properties and advantages can be separated as anonymity and unforgeability [28].

1. Unconditional anonymity. Even if the attacker steals all private keys of the voters, the probability of confirming the identity of voter will be less than 1/n, which n is numbers of all members in the ring.
2. Unforgeability. Even if the outside attacker tampers a ring signature in accordance with the message m without any private key of the voters, the coincidence probability can be overlooked.
3. Compared to the group signature scheme, there is no administrator in the group for the ring signature scheme. Every member is equal and the scheme does not need any trusted third party.

Implementation

The proposed protocol consists of three entities: Voters (Vi), RA (Registration Authority), EA (Election Authority) and Bitcoin Address Pool.

Voters (Vi): The voters should be a set of lists. For each voter to vote can be defined as Vi.

Candidate(Ci): The candidates should be a set of lists. For each candidate to vote can be defined as Ci.

| e-ISSN: 2320-9801, p-ISSN: 2320-9798| www.ijircce.com | |Impact Factor: 7.488 |

|| Volume 9, Issue 4, April 2021 ||

| DOI: 10.15680/IJIRCCE.2021.0904173 |

RegistrationAuthority (RA): The voters should sign up as a register in the current e-voting system at first. The voter should save their public keys (PKi) and Bitcoin address (Ai) into this system and the system transfer it to the database. For the RA, it provides the candidate (Ci) to the voters.

Election Authority (EA): The election authority is responsible for tallying the votes. The EA has its own Bitcoin address (AE). When the voting has been finished, the EA should start counting the votes and transfer the result to the voting system.

Bitcoin Address Pool: The Bitcoin address pool is a list of all Bitcoin addresses generated from the EA system randomly by using ECC algorithm. The private key SKAi of each address will store into the EA system.

Public supervision: To build this protocol, some of the content should be public and be supervised under anyone as the open-audit part. Anyone can check its completeness and validity. All public keys of the voter PK , the EA's Bitcoin address AEA and the sets of (σ,sha256(σ)) should be public through the inner API of the system without any permission

Protocol

Preparation Phase: The details of this phase can be described in order as follows.

1. The EA saves his own private key of the Bitcoin(SKb) into the system.

2. The system will generate EA's Bitcoin address (AEA) from his private key of Bitcoin (SKb).

3. The EA creates a new voting item with the voting id(Li), title, limitation of the voting numbers(n) and the description of this voting item.

4. The EA system will generate the numbers of the n bitcoin addresses (A1, A2...An) as the Bitcoin Address Pool automatically.

First Registration Phase: The details of this phase can be described in order as follows.

1. The candidate(Ci) takes his passport and authenticate to the RA in person.

2. The RA verifies the identity of the candidate and ask his name, his personal description and save it into RA system.

3. The RA will generate and give him his candidate id(Ci).

4. The voter(Vi) takes his passport and authenticate to the RA in person.

5. The RA verifies the identity of the voter and asks the email address of the voter then sends him an email with an random registration code link as LKi to avoid multiple registrations.

6. The LKi is generated randomly and has no relationship with the name of voter and his email address.

Second Registration Phase: The details of this phase can be described in order as follows.

1. The voter opens the registration links LKi .

\2. The voter Vi generates his key pair (SKi ,PKi).

3. The voter Vi saves his public key PKi into the system.

4. At the end of the registration, the set of voters should be fixed as a number of n.

Publish Phase: The details of this phase can be described in order as follows.

1. On the voting cut-off date, the EA decides to start the voting which means the ring of public keys has been confirmed and the RA should not accept any registration requests.

2. EA creates k BTC in his own Bitcoin account. 3. EA pays a fixed amount of bitcoin k/n as the voting fees to each

| e-ISSN: 2320-9801, p-ISSN: 2320-9798| www.ijircce.com | |Impact Factor: 7.488 |

|| Volume 9, Issue 4, April 2021 ||

| DOI: 10.15680/IJIRCCE.2021.0904173 |

Ai , such as 0.0001 BTC. (Once the voter voted, the voting fees would send back to EA)

Voting Phase: The details of this phase can be described in order as follows.

1. The voter chooses the candidate Ci he vote for and the current voting id Li .

2. The RA returns the public keys set (PK1,PK2,PK3...PKn) to the voter.

3. The voter uses his private key SKi and all public keys PK to sign the signature of the candidate Ci as σ(Ci ,SKi ,(PK1,PK2,PK3...PKn)). The system saves the set of (σ,sha256(σ)) at the same time.

4. The voter selects a Bitcoin address Ai to publish from the Bitcoin Address Pool and EA returns the private key SKAi of the address to the voter.

5. The voter Vi pays all balance of Ai the to EA address AEAwith an OP RETURN of the commitment(sha256(σ(Ci,SKi ,(PK1,PK2,PK3...PKn))),Ci ,Li).

Tallying Phase: The details of this phase can be described in order as follows.
1. The system returns all sets of (σ,sha256(σ)) and all public keys PK automatically.

2. The system fetches all transactions in EA Bitcoin address AEA automatically.

3. The system fetches the OP RETURN form each transaction and verify the signature σ validity.

4. The system counts each valid transaction and add 1 to the candidate Ci.

5. If the voter Vi is absent, mark it as the abstain from voting.

6. If the Bitcoin transaction history has more than twice transactions from the same Ai , count the first and ignore others.

Verification Phase: The details of this phase can be described in order as follows.

1.The system returns all public keys (PK1,PK2,PK3...PKn) automatically.

2. For each voter Vi , he can use a set of all public keys (PK1,PK2,PK3...PKn), the ring signature σ, the candidate Ci to verify his vote.

3. The voter Vi can use the transaction id to fetch the commitment from the blockchain to verify if the signature is published in the right way

II. RELATED WORK

For a long time, many researchers are devoting to design a secure and efficient e-voting protocol. The first thesis related to cryptographic e-voting protocol was published by Chaum in 1981 and he used an anonymous commutation channel to encrypt the ballot [7]. With the developing of cryptography, a lot of protocols with its own properties had been proposed. In 1982, Richard A. DeMillo proposed a protocol requires all voters must participate and encrypt the ballot of each voter and at the end cast the ballots [12]. In 1985, Cohen and Fisher proposed a cryptographic protocol which can hold a secure ballot election. However, it requires the voting stage should at the same time [9]. The protocol encrypts the ballot by using homomorphism theorem and the government will release the tally result. In 1992, Fujioka, Okamoto and Ohta proposed a practical secret e-voting scheme(FOO) used for the large scale elections, which can ensure the privacy of voters and the fairness ofvoting. The scheme used the blind signature to blind the message the voter used to vote and send it to the administrator [14]. After this seminal paper has been released, a lot of e-voting software had been implemented and used for the market, such as the EVOX and SENSUS. In this scheme it also has its weakness, it requires all voters must vote and once someone abstains from voting, the result can tamper. The

| e-ISSN: 2320-9801, p-ISSN: 2320-9798| www.ijircce.com | |Impact Factor: 7.488 |

|| Volume 9, Issue 4, April 2021 ||

| DOI: 10.15680/IJIRCCE.2021.0904173 |

administrator cannot find out who tamper the result. In 1996, Juang and Lei proposed a blind signature based voting scheme but requires everyone should attend the voting event.

After 3 years, M. Ohkubo, F.Miura and M.Abe promoted the FOO scheme by using a threshold encryption protocol and the Mix-Net communication channel which can keep the privacy of the voter. For the voters, they can need not to participate the tallying part of the event and they can walk away after voting [25].
With the development of e-voting system, there are a series of criminal behaviors related to the e-voting, such as electoral fraud, threat a voter or vote buying. To deal with these problems, many new requirements or properties of e-voting scheme have been proposed likes the receipt-freeness and coercion-resistance.
The receipt-freeness means that the voter cannot prove the vote result to anyone after voting. In 1994, Benaloh discussed the terminology named receipt-freeness firstly[2]. Although Benaloh uses homomorphic encryption to make the implementation of receiptfreeness, Martin Hirt argued that it will not be valid if there are more than one tally authority. In 1995, V.Niemi and A.Renvall raised a scheme by adopting the receipt so that the voter cannot prove who he or she votes for[24]. At the same time, K Sako and J Kilian proposed the first Mix-Net based protocol satisfied with receipt-freeness [30]. This protocol is under the assumption that there is no private channel between the voting station and the voters. After one year, Okamto uses a non-anonymous channel, a private channel and the bulletin board to propose a voting scheme satisfied receipt-freeness[26]. Unfortunately, this protocol has been proved does not satisfy with receipt-freeness. In 2000, M.Hirt and K.Sako use homomorphic ElGamal encryption technique to design a private channel protocol with receipt-freeness, but this protocol does not suit for the large-scale election[15]. In 2001, O.Baudron proposed a new scheme to satisfy this property by using Paillier cryptosystem and the zero-knowledge proof[1].
In recent years, a lot of researchers focus on the receipt-freeness and coercion-resistance of e-voting. In 2010, Juels introduced the new direction of e-voting which named coercion resistance and proposed a scheme[18]. In 2012, O.Spycher and R.Koenig promote his scheme by adding the random integer f. The proposed scheme will get the encrypted integer C. The tally authority can judge if there is any fake ballot through decrypting C to the random integer f[32]. The coercion-resistance can be satisfied further.
By the developing of the decentralized digital currency, some researchers argued a way to vote and tally on the blockchain. In 2015, Czepluch discussed the application domains of the blockchain and argued that blockchain can use for the e-voting [11] . At the same time, Z.Zhao and THH.Chan proposed a way to vote using Bitcoin and zk-SNARKs with the properties named privacy, verifiability and irrevocability [34]. In 2016, a protocol using Zerocoin has been proposed and ensures most properties of the e-voting[33]. However, using a Zerocoin is hard to make the implementation to the software. At the same year, C.Jason, Paul and K.Yuichi proposed a protocol using blind-signature and Bitcoin cards [16]. However, it cannot protect the privacy in some situation, for instance, if the administrator knows the Bitcoin address of the voter, the administrator can know who the voter is by linking the address and message on the blockchain.

III. RELATED APPLICATIONS

The research of e-voting system is widely used nowadays. Some partial practices are listed as follows. In 2000, e-voting has been used in US Election[8]. Although it is an experiment in some area of Florida, it was a milestone in the development of e-voting.In 2002, United Kingdom tried out an electronic voting system. 16 public authorities were awarded to build the e-voting system. After 1 year, more than 18 authorities were award [22].
In 2004, US election used an electronic voting system DRE for the first time [5]. India uses this system for parliamentary elections on a national scale. In 2007, France UMP party made a history of internet-based voting. More than 31,000 voters vote in UMP to in 2007 French Presidential election[13]. This was the first mass E-voting activity in history. In 2009, China used electronic voting for the election of the grass-roots organization in Hangzhou. There were 3122 residents enrolled this voting activity with an electronic touch screen [21].
In 2014, the election of Ministry of National Education (France) received 1,760,000 ballots [21]. It took the lead in legal and security network voting, thus popularized the channels of network voting.

IV. PROPOSED SYSTEM

The idea of adapting digital voting systems to make the public electoral process cheaper, faster and easier, is a compelling one in modern society. Making the electoral process cheap and quick, normalizes it in the eyes of the voters, removes a certain power barrier between the voter and the elected official and puts a certain amount of pressure

| e-ISSN: 2320-9801, p-ISSN: 2320-9798| www.ijircce.com | |Impact Factor: 7.488 |

|| Volume 9, Issue 4, April 2021 ||

| DOI: 10.15680/IJIRCCE.2021.0904173 |

on the elected official. It also opens the door for a more direct form of democracy, allowing voters to express their will on individual bills and propositions. In this project, we introduced a unique, blockchain-based electronic voting system that assures security and cost efficient election while guaranteeing voters privacy. By comparison to previous work, we have shown that the blockchain technology offers a new possibility for democratic countries to advance from the pen and paper election scheme, to a more cost- and time-efficient election scheme, while increasing the security measures of the todays scheme and offer new possibilities of transparency.

V. COMPARATIVE ANALYSIS

Traditional voting system uses centralized approach which can be attacked easily while our proposed system uses decentralized approach which provides high security. The traditional approach is a time consuming process while our project proposes a hands-on voting system allowing to vote from anywhere in the world. It takes time for declaration of results when used traditional approach whereas our project would provide the results as soon as the time limit is reached. Our approach is comparatively less expensive than the traditional one. E-voting provides us high security, transparency confidentiality and non- repudiation. Also, the usual E-voting system are more concentrated over assembly elections and an e-voting poll can only be made by the heads. Our system proposes a Multi-purpose voting system in which the E-voting system is indeed handled by the voting system but it does not specifically concentrate only on assembly election but also an e-voting system for some other cause can be made by visiting the same web application. The purpose of an e-voting system can be from making a poll for election of class representative in college, for a survey by a data scientist, elections in office, etc.

Protocol	Pros	Cons
Based on Quantum Blockchain.	anonymous, binding, non-reusable, verifiable, eligible, fair and self-tallying	The main disadvantage of it does not provide auditability consistency
Used blockchain as a transparent ballot box.	Abide by the underlying of e-voting properties. Allow a degree of decentralization. Provide for the elector to modify/update their votewithin the allowable voting phase.	It does not provide privacy, consistency and auditability.
Design blockchain-based protocol named Verify-Your-Vote (VYV).	Eligibility , Fairness, Vote privacy, Receipt-freeness, Verifiability	This protocol not support the anonymity.
Design the blockchain-based protoco without a trusted third party.	Public Verifiability ,Dependability , Dependability, Consistency, Auditability, Transparency, Anonymity.	The robustness and fairness is the limitations.
Proposed protocol preserves end-to-end privacy.	Detectability, correct ability.	It does not provide consistency and fairness.
Proposed blockchain based protocol using homomorphic ElGamal encryption	It guarantee and protect the anonymity of the voting scheme.	The main disadvantage not support robustness.
Designed a synchronized model Designed a user credential model. Designed a withdrawal model.	Achieves the essential security and privacy requirements of e-voting process.	Countermeasures attacks is problem.
Used Prêt à Voter e-voting method.	Secure digital voting without jeopardizing cryptographic hashes to secure end-to-end verification.	It allowed multiple votes to one user.
Combining the secret sharing scheme and homomorphic encryption.	It provide preserving the anonymity of the voter's identity.	The fairness is the main problem in this scheme.
Design smart contract using the ethereum wallets and the Solidity language.	Design Android a pplication for the voting system.	The main disadvantage not support robustness and not support the receipt-freeness feature.
The proposed system security scheme is based on Merkle root hash.	Transmitted data privacy, Voter confidentiality. No duplication cases during the voting.	The robustness and anonymity is the limitations.

Fig.5. Comparative Analysis

| e-ISSN: 2320-9801, p-ISSN: 2320-9798| www.ijircce.com | |Impact Factor: 7.488 |

|| Volume 9, Issue 4, April 2021 ||

| DOI: 10.15680/IJIRCCE.2021.0904173 |

VI. EVALUATION

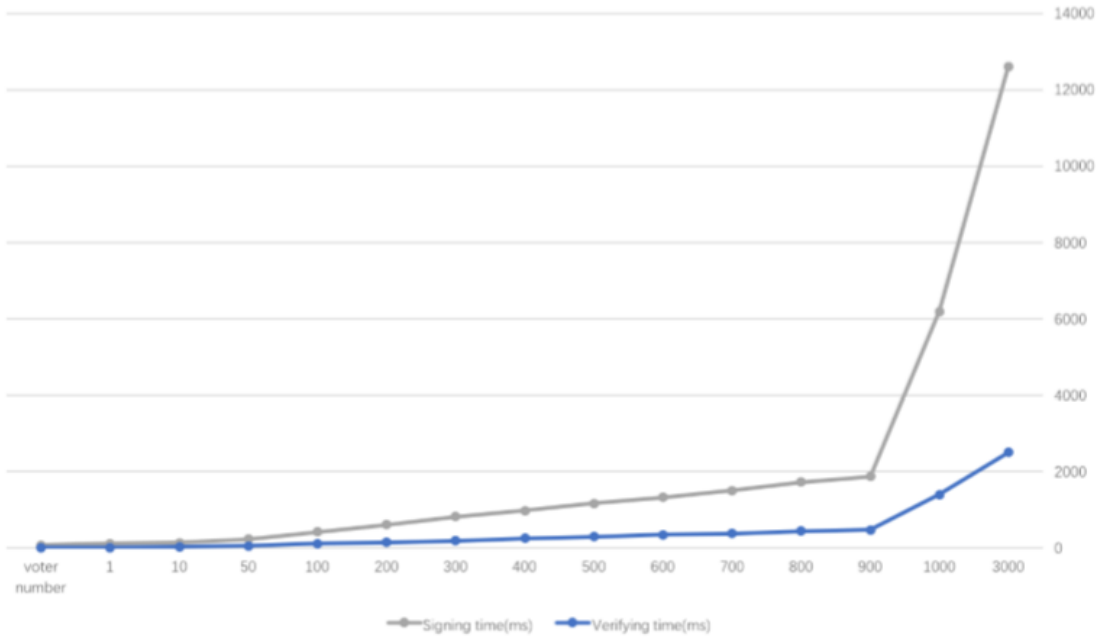


Fig.6.1. The relationship between voter numbers and the time of signing and verifying

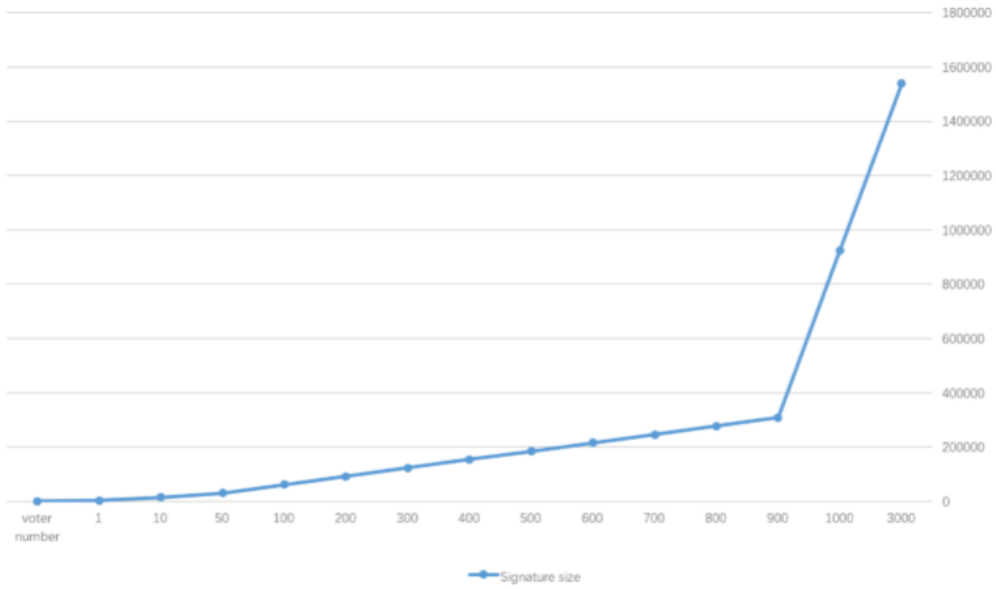


Fig. 6.2. The relationship between voter numbers and the signature key size

VII. CONCLUSION

Even though the generated protocol satisfied with the properties of ballot-privacy, individual verifiability, eligibility, completeness, uniqueness, robustness, and coercion-resistance. However, it does not fulfill the needs of fairness and receipt-freeness.

| e-ISSN: 2320-9801, p-ISSN: 2320-9798| www.ijircce.com | |Impact Factor: 7.488 |

|| Volume 9, Issue 4, April 2021 ||

| DOI: 10.15680/IJIRCCE.2021.0904173 |

In the performance evaluation, the protocol works efficiently for ring signature, especially when the number of the voter is less than 3000. Therefore, the efficiency of ring signature algorithm is limited by the number of participants.

The primary advantage of this protocol is to guarantee the authenticity of electronic voting. As every ballot will be broadcasted to the blockchain once voting starts. Moreover, as blockchain is a decentralized public ledger, ballots result are represented in a real time and cannot be modified by an individual, which satisfies the design of open-auditing.Block Votes confirmed the feasibility of the proposed protocol in disguise. The purpose of selecting test net as the blockchain network , primarily rests with its free of charge and ease when comparing with Bitcoin and Ethereum. Beyond that, the high similarity degree to Bitcoin network structure is another principal reason to appointed test net to broadcast voting result

VIII. FUTURE WORK

Blockchain based e-voting protocol still have a large room for improvement, such as improving its transparency, fulfilling unconsummated functions within current status, and reducing public API.

As for Block Votes, functions like switching more networks between Bitcoins, test net and Litecoin can be appended. In addition, accomplishment multiple voting within one vote can be an ideal topic for further study.

REFERENCES

[1] Baudron, O., Fouque, P.-A., Pointcheval, D., Stern, J., and Poupard, G. Practical multi-candidate election system. In Proceedings of the twentieth annual ACM symposium on Principles of distributed computing (2001), ACM, pp. 274–283.
[2] Benaloh, J., and Tuinstra, D. Receipt-free secret-ballot elections. In Proceedings of the twenty-sixth annual ACM symposium on Theory of computing (1994), ACM, pp. 544–553.
[3] Bitcoin-Wiki. Confirmation - bitcoin wiki. https://en.bitcoin.it/wiki/ Confirmation.
[4] bitcoinfees.21.co. Predicting bitcoin fees for transactions. https://bitcoinfees. 21.co/.
[5] Card, D., and Moretti, E. Does voting technology affect election outcomes? touchscreen voting and the 2004 presidential election. The Review of Economics and Statistics 89, 4 (2007), 660–673.
[6] Cetinkaya, O., and Cetinkaya, D. Towards secure e-elections in turkey: requirements and principles. In Availability, Reliability and Security, 2007. ARES 2007. The Second International Conference on (2007), IEEE, pp. 903–907.
[7] Chaum, D. L. Untraceable electronic mail, return addresses, and digital pseudonyms. Communications of the ACM 24, 2 (1981), 84–90.
[8] Christian Schaupp, L., and Carter, L. E-voting: from apathy to adoption. Journal of Enterprise Information Management 18, 5 (2005), 586–601.
[9] Cohen, J. D., and Fischer, M. J. A robust and verifiable cryptographically secure election scheme. Yale University. Department of Computer Science, 1985.
[10] Cranor, L. F., and Cytron, R. K. Sensus: A security-conscious electronic polling system for the internet. In System Sciences, 1997, Proceedings of the Thirtieth Hawaii International Conference on (1997), vol. 3, IEEE, pp. 561–570.
[11] Czepluch, J. S., Lollike, N. Z., and Malone, S. O. The use of block chain technology in different application domains. The IT University of Copenhagen, Copenhagen (2015).
[12] DeMillo, R. A., Lynch, N. A., and Merritt, M. J. Cryptographic protocols. In Proceedings of the fourteenth annual ACM symposium on Theory of computing (1982), ACM, pp. 383–400.
[13] Fraunholz, B., and Unnithan, C. E-governance: enabling the french web 2.0 revolution? In Foundations of e-government (2007), [International Conference on EGovernance] Academic Publishing, pp. 344–359.
[14] Fujioka, A., Okamoto, T., and Ohta, K. A practical secret voting scheme for large scale elections. In International Workshop on the Theory and Application of Cryptographic Techniques (1992), Springer, pp. 244–251.
[15] Hirt, M., and Sako, K. Efficient receipt-free voting based on homomorphic encryption. In Advances in CryptologyEUROCRYPT 2000 (2000), Springer, pp. 539–556.
[16] Jason, P. C., and Yuichi, K. E-voting system based on the bitcoin protocol and blind signatures. TOM 10, 1 (2017), 14–22.
[17] Jonker, H., Mauw, S., and Pang, J. Privacy and verifiability in voting systems: Methods, developments and trends. Computer Science Review 10 (2013), 1–30.
[18] Juels, A., Catalano, D., and Jakobsson, M. Coercion-resistant electronic elections. Towards Trustworthy Elections 6000 (2010), 37–63.
[19] kiwi. Bitcoin test net sandbox. https://testnet.manu.backend.hamburg/faucet.
[20] Lee, K., James, J. I., Ejeta, T. G., and Kim, H. Electronic voting service using block-chain. The Journal of Digital Forensics, Security and Law: JDFSL 11, 2 (2016), 123.

INNO SPACE

SJIF Scientific Journal Impact Factor

Impact Factor:
7.488

ISSN INTERNATIONAL STANDARD SERIAL NUMBER INDIA

निस्केयर NISCAIR

INTERNATIONAL JOURNAL OF INNOVATIVE RESEARCH

IN COMPUTER & COMMUNICATION ENGINEERING

9940 572 462 6381 907 438 ijircce@gmail.com

www.ijircce.com

Scan to save the contact details