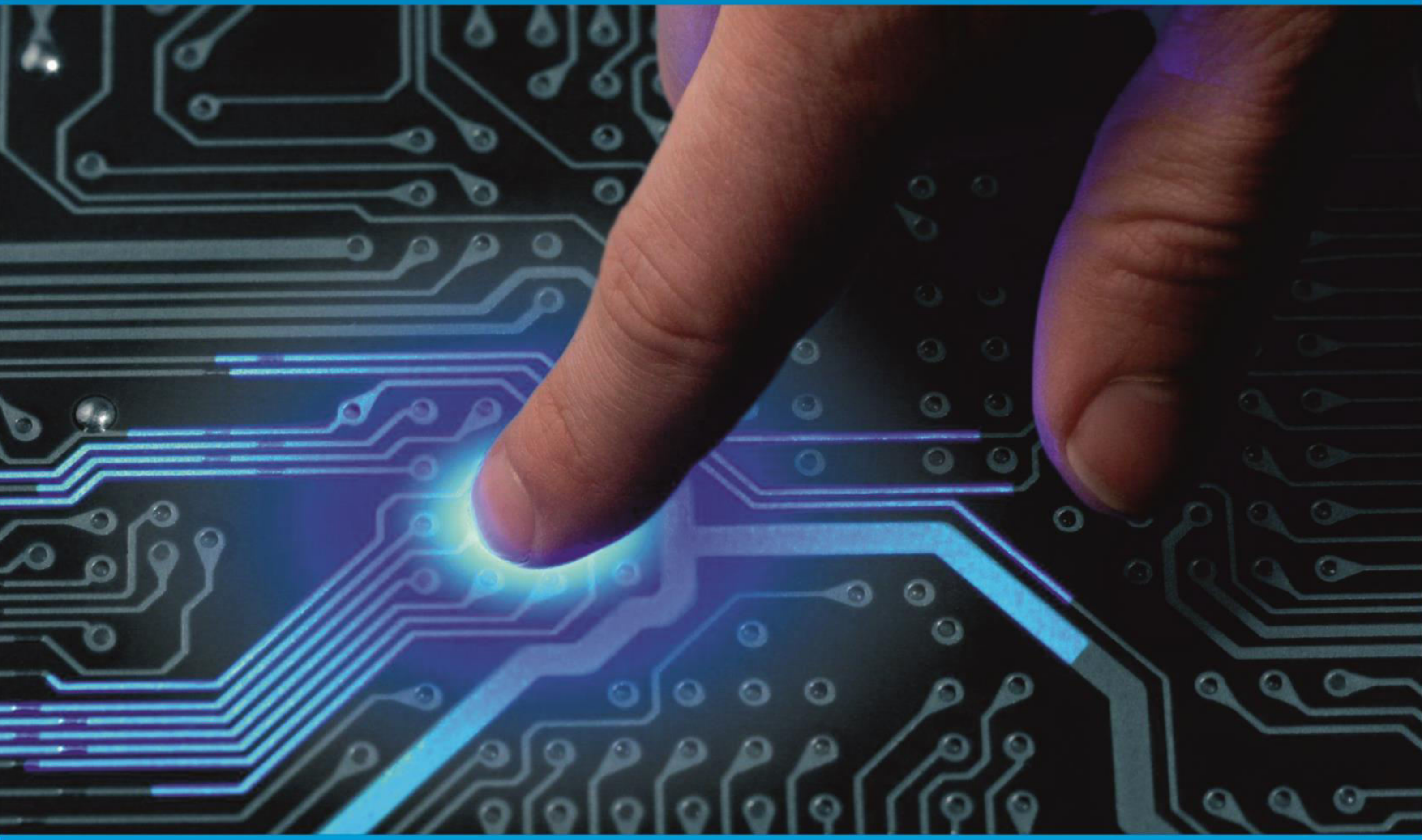
IJIRCCE

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



INTERNATIONAL JOURNAL OF INNOVATIVE RESEARCH

IN COMPUTER & COMMUNICATION ENGINEERING

Volume 9, Issue 3, March 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 3, March 2021 ||

| DOI: 10.15680/IJIRCCE.2021. 0903147|

Blockchain Based E-Voting System Using Ring Signature

K.M.Annammal[1] , T.Manikandan[2], P.Vasanth[2],

Assistant Professor, Department of CSE, Grace College of Engineering, Thoothukudi, India [1]

Student, Department of CSE, Grace College of Engineering, Thoothukudi, India [2]

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.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.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.

I. OVERVIEW

Voting plays an important role in constructing a democratic society. The traditional voting requires voters to cast in appointed polling stations, which usually involves enormous expenditure on time and cost budget. E-voting, a new substantial online voting system which is structured on cryptography technique, has been gradually implemented and emphasized by people. The system supports full-function online voting by general household devices, and the entire polling results will be counted automatically and anonymously. Compared with traditional voting, electronic voting is a more economic system addresses on transparency and impartiality. As e-voting system mainly relies on the internet platform. The crucial challenge for e-voting is the significant security risks it might cause. In order to reduce risks, in the past 40 years, various protocols related to the ballot-privacy, individual verifiability, eligibility, completeness, fairness, uniqueness, robustness, universal verifiability and receipt-freeness have been widely proposed. In particular, the application of e-voting in digital currency has became gradually maturity nowadays. Based on the common security requirements of participants, this paper proposed a blockchain-based protocol associated with the priorities of the ballot-privacy, verifiability, eligibility, completeness, uniqueness, robustness, and coercion- resistance. A BlockVotes software has also been made to verify the feasibility of this protocol, by implementing a real-life online voting website, which allows participants to vote and view the results easily.

II. E-VOTING

Electronic voting (also known as **e-voting**) is voting that uses electronic means to either aid or take care of casting and counting votes.

Depending on the particular implementation, e-voting may use standalone electronic voting machines (also called EVM) or computers connected to the Internet. It may encompass a range of Internet services, from basic transmission of tabulated results to full-function online voting through common connectable household devices. The degree of automation may be limited to marking a paper ballot, or may be a comprehensive system of vote input, vote recording, data encryption and transmission to servers, and consolidation and tabulation of election results.

1.1 Blockchain

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[7]. 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 testnet. The testnet 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.

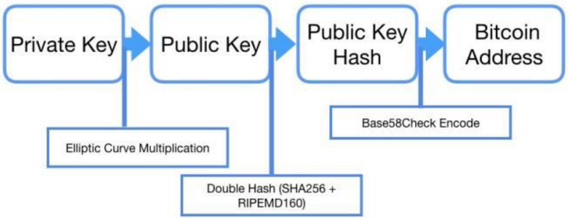
1.2 E-voting scheme Properties

In recent 30 years, more and more e-voting protocols has been published. 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 event. Accuracy/Completeness: Every votes 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.

1.3 Blockchain

Bit Coin Address

A **Bitcoin invoice address**, or simply **invoice**, is an identifier of 26-35 alphanumeric characters, beginning with the number 1 , 3 or bc1 that represents a possible destination for a bitcoin payment. Invoices can be generated at no cost by any user of Bitcoin. It is also possible to get a Bitcoin invoice address using an account at an exchange or online wallet service.



1.4 Properties

- **Decentralization:** The blockchain is decentralized. There is no central computing devices to store the ledger of transactions. Every node of blockchain store the samecopy.
- **Hard to forge:** Due to its decentralization, every block should be distributed to everynode 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, whichanyone can trace a transaction.

II. CRYPTOGRAPHY

2.1 RSA Algorithm

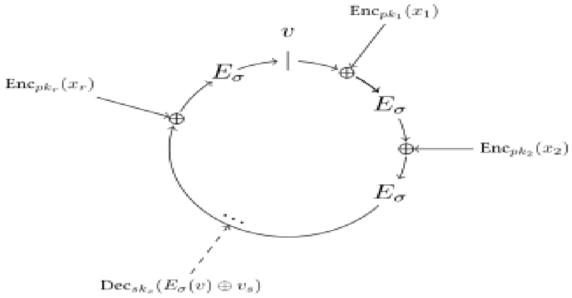
RSA is an algorithm used by modern computers to encrypt and decrypt messages. It is an asymmetric cryptographic algorithm. Asymmetric means that there are two different keys. This is also called public key cryptography, because one of the keys can be given to anyone. The other key must be kept private. The algorithm is based on the fact that finding the factors of a large composite number is difficult: when the factors are prime numbers, the problem is called prime factorization. It is also a key pair (public and private key) generator.

RSA involves a public key and private key. The public key can be known to everyone- it is used to encrypt messages. Messages encrypted using the public key can only be decrypted with the private key. The keys for the RSA algorithm are generated the following way:

1. Choose two different large random prime numbers
2. Define n=pq ,$\emptyset(n)$= (p-1) (q-1)
3. Choose e ∈ [$0, \emptyset(n)$ -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).

2.2 Ring Signature

In cryptography, a **ring signature** is a type of digital signature that can be performed by any member of a set of users that each have keys. Therefore, a message signed with a ring signature is endorsed by someone in a particular set of people. One of the security properties of a ring signature is that it should be computationally infeasible to determine *which* of the set's members' keys was used to produce the signature. Ring signatures are similar to group signatures but differ in two key ways: first, there is no way to revoke the anonymity of an individual signature, and second, any set of users can be used as a signing set without additional setup.


$\mathrm{Enc}_{pk_1}(x_1)$
v
E_σ
$\mathrm{Enc}_{pk_r}(x_r)$
E_σ
$\mathrm{Enc}_{pk_2}(x_2)$
E_σ
...
$\mathrm{Dec}_{sk_s}(E_\sigma(v) \oplus v_s)$

III .PROTOCOL

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 list. For each voter to vote can be the need as Vi.

Candidate(Ci): The candidates should be a set of list. For each candidates to vote can be the need as Ci.

Registration Authority(RA): The voters should sign up as a register in the current e-voting system at rst. 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 shouldstart 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 besupervised under anyone as the open-audit part. Anyone can check its completeness andvalidity. 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.

3.1 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.

3.2 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.

3.3 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.

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

3.5 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 AEA with an OP RETURN of the commitment
(sha256(σ(Ci ,SKi ,(PK1,PK2,PK3...PKn))),Ci ,Li).

3.6 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 fetchs 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.

3.7 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

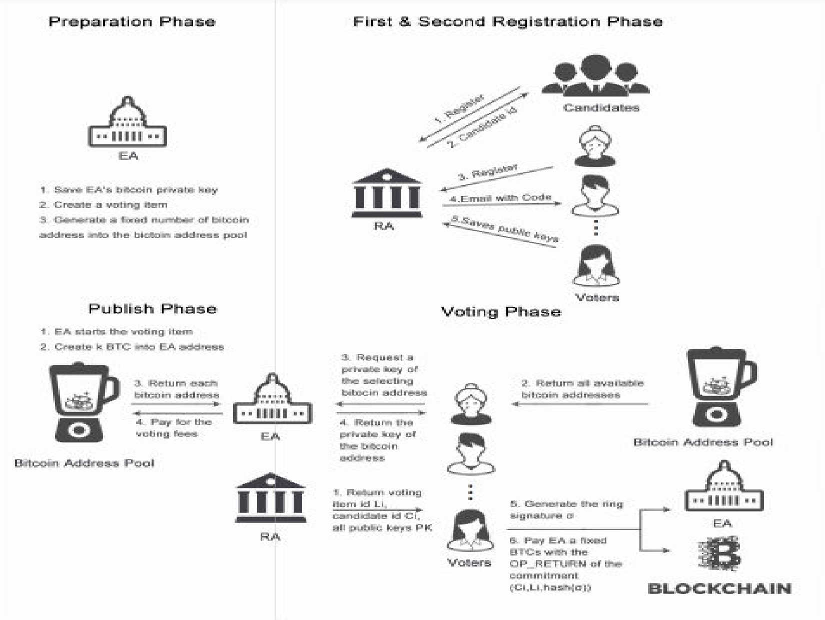

Preparation Phase
EA
1. Save EA's bitcoin private key
2. Create a voting item
3. Generate a fixed number of bitcoin address into the bictoin address pool
First & Second Registration Phase
Candidates
1. Register
2. Candidate id
RA
3. Register
4.Email with Code
5.Saves public keys
Voters
Publish Phase
1. EA starts the voting item
2. Create k BTC into EA address
3. Return each bitcoin address
4. Pay for the voting fees
EA
Bitcoin Address Pool
RA
Voting Phase
3. Request a private key of the selecting bitcoin address
4. Return the private key of the bitcoin address
1. Return voting item id Li, candidate id Ci, all public keys PK
2. Return all available bitcoin addresses
Bitcoin Address Pool
Voters
5. Generate the ring signature σ
6. Pay EA a fixed BTCs with the OP_RETURN of the commitment (Ci,Li,hash(σ))
EA
BLOCKCHAIN

Figure 3.1: Proposed Protocol(Mainly Phases)

IV. 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. 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. BlockVotes confirmed the feasibility of the proposed protocol in disguise. The purpose of selecting testnet 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 testnet to broadcast voting result.

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.

INTERNATIONAL JOURNAL OF INNOVATIVE RESEARCH

IN COMPUTER & COMMUNICATION ENGINEERING