iJRASET
International Journal For Research in Applied Science and Engineering Technology

INTERNATIONAL JOURNAL FOR RESEARCH

IN APPLIED SCIENCE & ENGINEERING TECHNOLOGY

Volume: 9 **Issue:** X **Month of publication:** October 2021

DOI: https://doi.org/10.22214/ijraset.2021.38421

www.ijraset.com

Call: 08813907089 | E-mail ID: ijraset@gmail.com

International Journal for Research in Applied Science & Engineering Technology (IJRASET)
ISSN: 2321-9653; IC Value: 45.98; SJ Impact Factor: 7.429
Volume 9 Issue X Oct 2021- Available at www.ijraset.com

A Decentralized, Secure, Peer-to-Peer Multi-Voting System on Ethereum Blockchain

Ashmita Pandey
Nepal Academy of Science and Technology (NAST), Nepal.

Abstract: ***A decentralised, Secure, Peer-to-Peer Multi-Voting System on Ethereum Blockchain is a distributed ledger technology (DLT) that permits virtual votes to be transacted in a peer-to-peer decentralized network. Those transactions are validated and registered through every node of the network, so creating a transparent and immutable series of registered events whose truthfulness is supplied through a consensus protocol. Smart contract automates the execution of agreement that runs routinely as soon as the conditions are satisfied. Smart contract would not need any third parties consequently prevents time loss. By Eliminating the requirement for third parties, consequently, allows numerous processes to be extra efficient and economical. The system is secure, reliable, and anonymous. Smart contract is enforced for the Ethereum network using the Ethereum wallets and also the Solidity language. Users are capable of submit their votes immediately from their Ethereum wallets, and those transaction requests is handled with the consensus of each single Ethereum node. This creates a transparent environment for e-voting. A lot of concerning efficiency of the peer-to-peer decentralized electoral system on Ethereum network along with application and the outcomes of implementation are provided in this paper.***

Keywords**: *Blockchain, Distributed Ledger Technology (DLT), Consensus Protocol, Smart Contracts, Ethereum, Solidity.***

I. INTRODUCTION

A. Background Theory

Voting is a way to create a collective call or express an opinion amongst a group or a assembly or electorates [1]. Since the 17th century, vote casting has been the same old mechanism through which present day representative democracy has operated. Voting is moreover applied in numerous private groups and teams, like clubs, companies, and voluntary associations [2]. With the fast development of the internet and understanding technologies, numerous typical offline services like voting, mail, payment, are migrating to online ones [3]. The online voting is known as digital balloting (e-voting). It is an digital method for casting and counting votes. Users of e-voting are voters and election government. The elector can publish his/her or her votes electronically to the election government from any place through e-balloting [4]. The election government are responsible for aggregation votes from voters. E-voting can save time and energy with excessive efficiency and adaptability, this is acquiring extra and greater attentions in place of historic balloting. With the event of web, e-voting have become the important method that of the various organizations [5]. Kiayias et al.[6] projected an efficient E2E verifiable e-voting system with out setup assumptions. Ahene et al. [7] projected a certificates much less deniable authenticated encryption and its application to e-voting system. Kshetri and Voas [8] projected a blockchain-enabled e-voting system.

B. Problem Statement

Most of E-voting is an effective and cost-effective method for engaging in a voting procedure, that has feature of being magnanimous data and real time and requesting excessive safety[9]. However, problems on safety of internet and privateness of communication are full-grown. Anonymity required through e-voting can't meet through encryption alone [10]. As an example, a vote shouldn't be traceable back to the elector in e-voting. E-voting makes use of computers, mobile devices, and internet to perform the complete vote procedure, that is a research discipline of cryptography with the fundamental and signature algorithms[11]. How to layout a greater stable and practical e-voting system has becoming a famous topic within the area of industry and data safety [12]. To enhance the security and anonymity of the e-voting, we present strategies to take benefit of blockchain to create new e-voting systems.

II. LITERATURE REVIEW

The government of Republic of Estonia is one among the primary to implement a fully on-line and comprehensive e-voting solution [13]. They use smart digital ID cards and private card readers (distributed by the government) for person-wise authentication [14]. For voters to attend the elections by listing the candidates and casting a vote, there's a special web portal in addition as an equivalent desktop app. The quantifiability of this method is another question.

Since Republic of Estonia has a comparatively tiny population, it's exhausting to estimate if such a system would work flawlessly in, say, China[15]. The constant need for the ID card and therefore the reader device isn't nice, too, because of the additional price of manufacturing, distributing, and carrying (for voters) them. Switzerland is another one of the few countries collaborating in the electronic voting trend. Some mentions for the e-voting are as follows.

A. Strawpoll.Me

It's a straightforward web site permits that enables everybody to make questionnaires and allows responsive others' polls with votes. Individuals will share personal hyperlinks to any created poll (as long as they recognize the link) and other people who have the link will vote and one browser will solely use onevote. The safety here, in terms of citizen authentication, duplicate votes and non-repudiation of votes, is extremely weak.

B. Electionrunner

They have a mobile application and an internet platform that individuals will produce and share elections with different users. Individuals will outline who can vote in this election and the way long it'll last and so they share this election to attested subscribers of electronic runner. However, one still should trust the central authority in Electronic Runner Iraqi National Congress. It's still one step far from being a 100% transparent and efficient e-voting platform.

C. TIVI

It is designed by the corporate Smartmatic. It's a web ballot solution supported biometric authentication. Tivi ensures many security properties like eligibility since it provides totally different authentication techniques, vote's secrecy because of the encoding mechanism and taking advantage from Blockchain technology, universal verifiability and vote's integrity are warranted. However, this method has some weaknesses. In fact, it doesn't offer any mechanism to safeguard voters from coercion.

D. Follow My Vote

Each elector needs a webcam and a government-issued ID to authenticate himself. A trustworthy authority verifies the identity of every elector, authorizes solely eligible voters to cast their ballots and provides them with pass-phrases required just in case of adjusting their votes within the future. Once voting and casting his ballot to the election Blockchain, every elector is in a position to check his vote counted within the ballot box. Even so, this electoral system doesn't meet many security properties. Indeed, it needs a trustworthy authority to confirm elector confidentiality and conceal the correspondence between the voters' real identity and their voting key. If this authority is corrupted, votes are not any longer anonymous.

E. Open Vote Network

It is a boardroom scale online electoral system written as a smart contract on Ethereum. This smart contract is owned by an administrator who is accountable of the election set up and voter's authentication. This electoral system ensures votes confidentiality since they're encrypted before being cast. Every elector can ensure his vote has been recorded as cast and cast as supposed by inspecting the Blockchain. Whereas, Open Vote Network isn't coercion resistant. It supports only elections with 2 choices (yes or no) and with a most of fifty voters because of the mathematical tools that they used. Finally, it must trust the election administrator to confirm that solely eligible voters have the right to vote.

III.METHODOLOGY

The primary objective of the project is to construct a secure and transparent e-voting based on ethereum. Leverage the precise attributes of blockchain technology to layout the better voting systems.

A. E-voting Properties

In recent 30 years, increasingly more e-voting protocols has been published.

1) *Privacy:* Anyone can't know whom the voter voted for.
2) *Individual Verifiability:* The voter can confirm his/her ballot is counted efficiently after he voted.
3) *Eligibility:* Only the legal voters can sign up the voting event.
4) *Accuracy/Completeness:* Every votes needs to be counted efficiently.
5) *Transparency:* The system is transparent and everyone can see the real time results of the voting process.
6) *Uniqueness:* The voter can only vote once.
7) *Robustness:* Anyone can't influence or adjust the final voting result whilst tallying.

ISSN: 2321-9653; IC Value: 45.98; SJ Impact Factor: 7.429
Volume 9 Issue X Oct 2021- Available at www.ijraset.com

B. Smart Contract

1) Election

```
struct Election{
    uint id;
    uint total;
    string name;
    uint optionsCount;
    string[] options;
    uint[] optionVotes;
    mapping(address => uint) userVotes;
}
```

Each contract has a unique ID(id). When an admin creates an election, the ID will be assigned to the election automatically.
"total" is saving the total number of voters. When a new voter votes, this field will be incremented by 1.
"userVotes" is a mapping and will save the votes for the voters. Key of the mapping is the address of the voter and value is the index of the option(candidate). For example when we have 2 candidates, the index for the first one is 1 and the second one is
The mapping for elections is defined here:

```
mapping(uint => Election) public elections;
```

Key of the mapping is the ID of election and value is an election struct that contains all of the information for that election.

2) Voters and Administrators

```
mapping(address => bool) public voters;

mapping(address => bool) public admins;
address[] public adminsList;
```

We have two mappings for saving the list of admins and voters. The key of the mapping is the wallet address and the value is a boolean. When we add a user as an admin or voter, the value for the users will be true in the mapping.

3) Incrementation Field

```
uint public lastElectionId = 1;
uint public lastAdminId = 1;

uint256 public voteFee = 0.1 ether;
```

lastElectionId and lastAdminId are 2 fields for the auto increment ID for elections and admins. The IDs start with 1 and when a new election or admin is defining, the field will be incremented by 1.
voteFee is the amount of ETH that the contract will pay the voters when we add new voters. The voters can use the ETH to pay the gas fees when they are voting.

4) Events

```
event NewElection(string name, uint id);
event UserVote(address user, uint electionId,
    string electionName, uint vote, string voteName);
```

There are 2 events and when a new election is creating or a user is voting, these events will be fired. The website will use the events to get a list of elections and votes and show in the web pages.

ISSN: 2321-9653; IC Value: 45.98; SJ Impact Factor: 7.429
Volume 9 Issue X Oct 2021- Available at www.ijraset.com

5) Constructor

```
constructor(){
    admins[msg.sender] = true;
    adminsList.push(msg.sender);
}
```

The constructor just adds the creator of the contract as an admin. So, the creator will be the first admin and can add new admins and manage the voters.

6) Add Voter

```
function adminAddVoter(address _addr) isAdmin public{
    voters[_addr] = true;

    if(voteFee > 0){
        payable(_addr).transfer(voteFee);
    }
}
```

This function adds a new voter to the contract and just admins can call it. When a new voter is added, the contract will send a voteFee amount of ETH to him/her. The voter can use these ETHs for paying the gas fees for voting transactions.
Note that after deploying the contract, the admin should send some ETH to the contract and the contract should have enough ETH for paying to the voters.

7) Add Admin

```
function adminAddAdmin(address _addr) isAdmin public{
    admins[_addr] = true;
    lastAdminId++;
    adminsList.push(_addr);
}
```

This function allows the admins to add a new admin.

IV. RESULTS

Decentralized application (Dapps) has been created that consists of a web pages created with JS. Ethereum Blockchain and solidity language was used to write smart contract.. Smart Contracts have been deployed using Ropsten Test Network. The Dapp performs wallet operations through the Ethereum client set up in the postman nodes. Handshaking method is used to connect to a network for transactions. Authentication is required for the user on every time a message is to be sent. Supports multiple platforms like both android and web for messaging and messages can be send privately as well. All the transaction history are recorded in blockchain. The deployed contracts and transaction history of the contracts can be viewed through Etherscan.

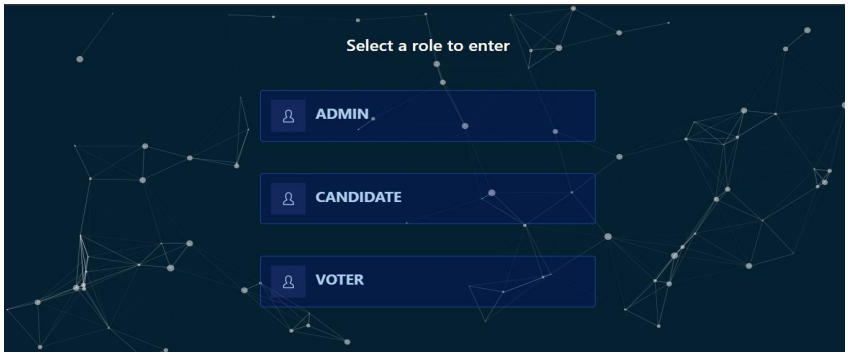


Fig. 1 Login portal for respective roles

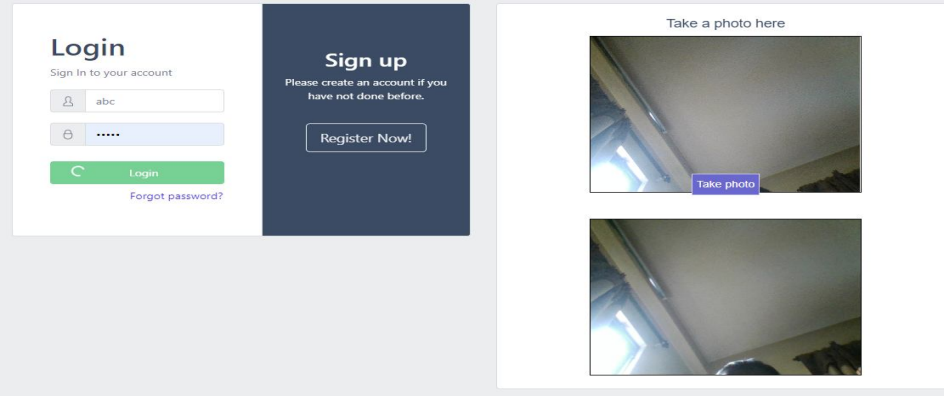


Fig. 1 Login and biometric (Facial Recognition) verification for voters

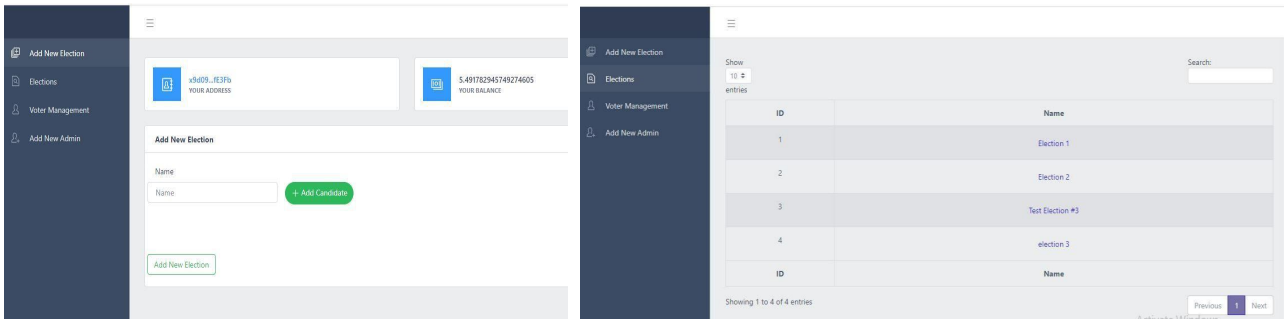


Fig. 3 (a) Interface for adding election by the admin (b) Multiple election happening at the same time

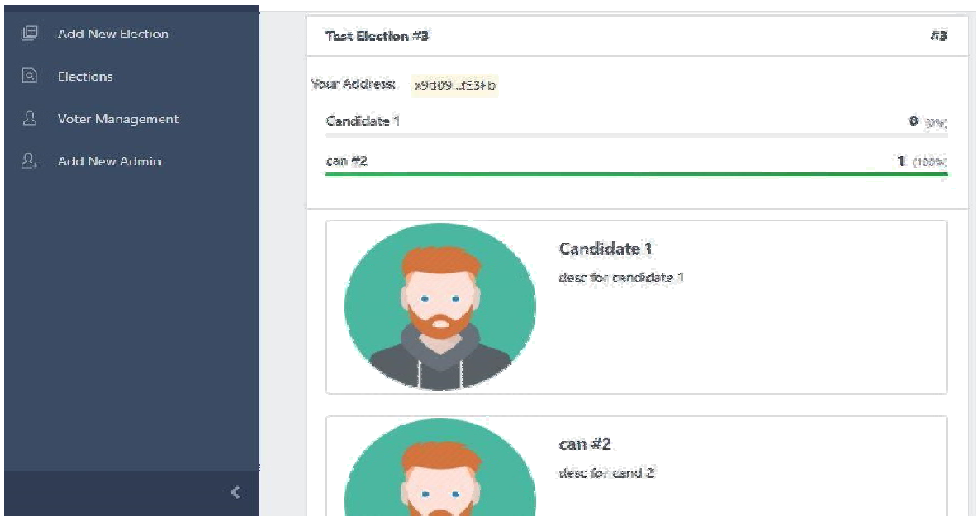


Fig. 4 Candidates photos with descriptions and result of voting

V. CONCLUSIONS

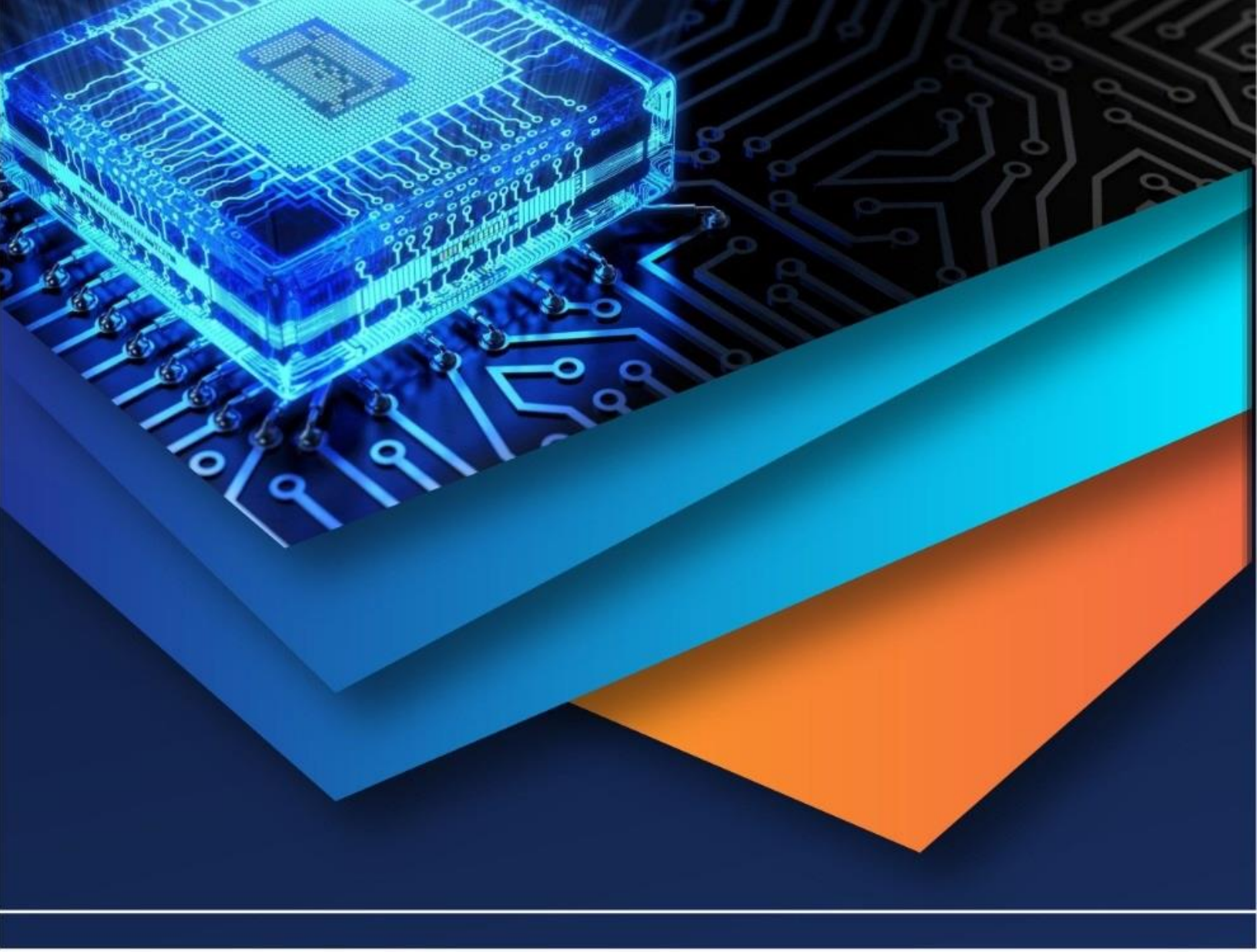
In this paper, implementation of blockchain technology has been discussed. The primary focus of the paper was to build a secure and transparent e-voting based on ethereum. The paper also intends to verify and register digital votes in a peer-to-peer decentralized network on an ethereum network. And maintain voters anonymity ensuring single vote per voter.

VI. ACKNOWLEDGMENT

This study is a part of Innovation for Prosperity Programme, sponsored by Nepal Academy of Science and Technology (NAST), Nepal. The system is still under development. I would like to express my deepest appreciation to NAST and everyone who supported me for this study. I am thankful for their continuous encouragement, invaluable supervision, timely suggestions and inspired guidance.

REFERENCES

[1] Satoshi Nakamoto.Bitcoin: A peer-to-peer electronic cash system.Cryptography Mailing list at https://metzdowd.com, 03 2009.
[2] Vitalik Buterin. A next-generation smart contract and decentralizedapplication platform. 2015.
[3] V. Suma. Security and privacy mechanism using blockchain.Journalof Ubiquitous Computing and Communication Technologies, 01:45–54,09 2019.
[4] Sivaganesan D. Block chain enabled internet of things.Journal ofInformation Technology and Digital World, 01:1–8, 09 2019.
[5] M. A. Uddin, A. Stranieri, I. Gondal, and V. Balasubramanian.Adecentralized patient agent controlled blockchain for remote patient monitoring. In2019 International Conference on Wireless and MobileComputing, Networking and Communications (WiMob), pages 1–8,2019.
[6] Ronald Cramer, Rosario Gennaro, and Berry Schoenmakers. A secureand optimally efficient multi-authority election scheme. volume 8, 102000.
[7] I.-C Lin and T.-C Liao. A survey of blockchain security issues andchallenges.International Journal of Network Security, 19:653–659, 092017.
[8] R. Bulut, A. Kantarcı, S. Keskin, and S¸. Bahtiyar. Blockchain-basedelectronic voting system for elections in turkey. In 2019 4th InternationalConference on Computer Science and Engineering (UBMK), pages 183–188, 2019.
[9] Ohkubo, M., Miura, F., Abe, M., Fujioka, A., and Okamoto, T. An improvement on a practical secret voting scheme. Information Security (1999).
[10] Okamoto, T. An electronic voting scheme. In Advanced IT Tools. Springer, 1996.
[11] Peters, G. W., and Panayi, E. Understanding modern banking ledgers through blockchain technologies: Future of transaction processing and smart contracts on the internet of money. In Banking Beyond Banks and Money. Springer, 2016.
[12] Rivest, R., Shamir, A., and Tauman, Y. How to leak a secret. Advances in CryptologyASIACRYPT 2001 (2001), 552–565. [29] Rivest, R. L., Shamir, A., and Adleman, L. A method for obtaining digital signatures and public-key cryptosystems. Communications of the ACM 21, 2 (1978), 120–126.
[13] Jonker, H., Mauw, S., and Pang, J. Privacy and verifiability in voting systems: Methods, developments and trends. Computer Science Review 10 (2013).
[14] Juels, A., Catalano, D., and Jakobsson, M. Coercion-resistant electronic elections. Towards Trustworthy Elections 6000 (2010).
[15] Spycher, O., Koenig, R., Haenni, R., and Schlapfer, M. ¨ A new approach towards coercion-resistant remote e-voting in linear time. In International Conference on Financial Cryptography and Data Security (2011).



10.22214/IJRASET

45.98

IMPACT FACTOR: 7.129

IMPACT FACTOR: 7.429

INTERNATIONAL JOURNAL FOR RESEARCH

IN APPLIED SCIENCE & ENGINEERING TECHNOLOGY