International Journal of Science and Research (IJSR)
ISSN: 2319-7064
SJIF (2022): 7.942

Electronic Voting System based on Blockchain for Sri Lanka: Conceptual Overview

R. Hansarandi Adithya Rathnayake[1], T. Sameera Bandaranayake[2]

[1]BEng (Hon's), University of Hertfordshire, United Kingdom

[2]BSc. Engineering (Hon's), MBA (AUS), C.Eng., MIE(SL), Sri Lanka Telecom Training Centre, Welisara, Sri Lanka

Abstract: ***This approach, known as electronic voting, provides the most secure form of voting for the election process. Electronic voting in corporate and governmental elections has not been fully addressed. There was enough potential to enhance present techniques and propose new protocols that would make the voting system more resistant to various attacks. This research discussed how blockchain technology might be utilized to build a highly maintainable, scalable, accurate, transparent, and immutable electronic voting system. The research presents an in-depth architectural design and a reference implementation of the Hyperledger Fabric private blockchain technology.***

Keywords: Blockchain, Electronic Voting System, Conceptual Framework, Hyperledger Fabric, Smart Contract, Security

1. Introduction

The current voting procedure was based on pen and paper. Today's Current Population of voters mostly uses ballot paper. Even in Sri Lanka, the system has remained as same for centuries. There were several benefits to paper voting methods[1]. However, paper ballots were provided a variety of costs, integrity, and accessibility concerns[3]. There were substantial expenses associated with conventional paper voting, which made it an expensive venture for governments and, ultimately, their voters[6]. When it comes to electronic voting, refers to any method of voting or comparing that makes use of cutting-edge technology. Numerous polling locations across the globe have already used paper scanners to count paper votes. An electronic voting machine's primary benefit was its speed. At present, electoral voting seems to be a significant probability. However, there were certain downsides to consider with computerized voting. While voting online may seem convenient, moving to paper ballots might threaten the democratic system's credibility. One of the most serious disadvantages of computerized voting machines now was election hacking[2].

Without a robust security framework, hostile actors may compromise the system and alter its output. This was the origin of blockchain. The blockchain technology has the potential to create an apparently impenetrable structure. When people were voting, they need privacy and do not necessarily want to know whom they voted for. Voting on the blockchain enables you to stay anonymous. As with blockchain transactions, voters may maintain anonymity by using their private keys[30]. They may vote methodically without fear of others discovering their vote. Personal privacy may inspire more users to engage and vote. Implementing Blockchain with an evoting system reduced the fault of the voting system in Sri Lanka. To improve the safety of votes by who votes and for whom votes, to improve the efficiency and Consume time consumption of the voting process, and to secure the voter's privacy[27].

2. Literature Review

The development of the Internet over the past two decades has completely changed how people connect, communicate, and trade information. Politics have also been impacted by this growth, which has prompted rising nations to start prospective digital voting initiatives to promote democracy for their citizens. Although digital voting has been available for some time, election officials worldwide were just now beginning to adopt it. Kenya has had many elections throughout the years, and one of the biggest challenges the electoral body has faced was the people's scepticism of the results, especially since the emergence of multiparty. There was much violence around the country in 2007 following the announcement of the presidential election results. Approximately 1, 300 people lost their lives in the immense damage that followed, and approximately 600, 000 had to leave their homes. A large amount of property was also lost. According to the Commonwealth Observer Group's Investigation report for Kenya's 2007 general elections, the Kenyan Electoral Commission was unable to confirm the precision of the counting process, raising concerns about the validity of the election results (Kenya Human Rights Commission, 2007)[12].

For the first time, biometric authentication was used to register voters electronically for the 2013 election. However, there was still variance in how the results were handled and how they were tabulated at the federal level, which feeds instability in various sections of the nation. When the Supreme Court declared the 2018 election's results unlawful owing to a lack of trust, we observed a similar pattern[70]. Our research identified the usage ofBlockchain technology in the development of a voting application as the choice that may address the difficulties mentioned due to the absence of a single point of failure. With the help of blockchain, hundreds of separate computers may work together as a single entity, giving them more overall power than a few centralized servers. Any central database that depends on the accuracy of the data being maintained by a third party was prone to corruption. Structure for the blockchain that only allows appends. It was challenging to update or remove information

that had already been entered on earlier blocks since information can only be added to the database.

What was Blockchain

A blockchain was a basic data structure first proposed by Satoshi Nakamoto in 2008 for the peer-to-peer currency known as Bitcoin. Satoshi Nalaunoto[12] proposed a peer-to-peer payment system[11] that allows cash transactions through the Internet without relying on trust or the need for a financial institution. By design, blockchain was safe, and it's an example of a system with high byzantine failure tolerances 19. Bitcoin was widely regarded as the first use of the Blockchain concept to establish money that could be transferred over the Internet using just encryption to safeguard transactions. A blockchain was a data structure that stores blocks of transactions in an orderly fashion. Every block in the chain was connected to the one beforeit. The stack's foundation was the initial brick. Each new block was built on top of the preceding block, forming a Blockchain stack[18].

Field	Description	Size
Block Size	The size of the whole block.	4 bytes
Block Header	Encrypted almost unique hash	80 bytes
Transaction Counter	The number of transactions that follow.	1 to 9 bytes
Transaction	Contains the transaction saved in the block	Depends on the transaction size

Figure 2.1: Sectional Description of Blockchain

Each stack block was identified as a hash written on the header. The Secure Hash Algorithm (SHA-256) was used to create a fixed-size 256-bit hash that was virtually unique. The National Security Agency (NSA) created the widely utilized algorithm in 2001, which was used as the protocol to protect all federal communications. The SHA-256[15] algorithm will encrypt any size plaintext into a 256-byte binary value. The SHA-256 value was always a 256-bit binary value. A strictly one-way function. The SHA-256 encryption's core concept was shown here[15].

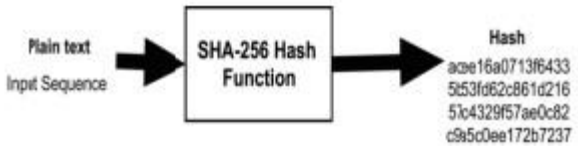


Figure 2.2: Basic Function of the SHA-256

Each header provides information that links a block to the preceding block in the chain, forming a chain that connects to the foundation, the very first block ever produced. The encrypted hash in a block's[43] header was the block's main identification. A digital fingerprint was formed by merging two sorts of data: information about the newly created block and information about the previous block in the chain.

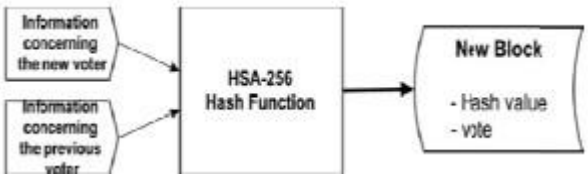


Figure 2.3: Flow Diagram of SHA -256

The Blockchain receives a block as soon as it was produced[8]. When new blocks were received, the system kept a watch on them and updated the chain accordingly. A 'chain' of blocks was the simplest explanation. A block was a collection of data that had been aggregated. Mining was the process of gathering and processing data to fit it into a block. A cryptographic hash (also known as a digital fingerprint) might be used to identify each block. So that blocks can create a chain from the first block (known as the Genesis Block)[6] to the formed block, the formed block contains a hash of the previous block. All the data might be linked together using a linked list structure.

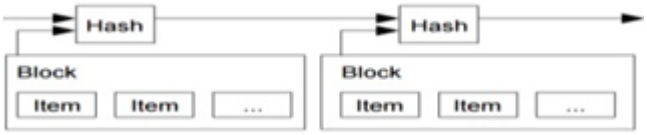


Figure 2.4: Connected Blocks into Chain

Evaluation of Blockchain technology

Blockchain technology was invented by Satoshi Nakamoto. "Bitcoin: A Peer-to-Peer Electronic Cash System" was published in 2008 by a person or group known as Nakamoto, proposing a direct internet payment between two parties. The study's purpose was to solve the problem of duplication, which means that digital money was easy to duplicate and spend. The resulting uncertainty hampered technological adoption[14].

By building a tamper-proof link between each transaction, the Nakamoto paper overcomes this problem. Nakamoto proposed using a public ledger to prevent tampering. To prevent the "double spending" problem, a network may utilize this ledger to validate the transaction history of an electronic currency submitted for payment.

Every computer, or "node, " in blockchain copies the database[9]. All nodes have the same data. This was vital to the success of blockchain technology. As the name implies, the data was kept in blocks. There were multiple transactions in each block, each with its unique reference number. A link to the previous transaction, as well as transaction details. Since the "genesis" block was the first in the chain, each node has access to all previous blocks. The time stamp gives each block in the chain an immutable temporal position.

A hypothetical transaction[18] demonstrates how blockchain works. In a sales contract, a seller promises to sell a widget for one "coin." With each widget sent by the vendor, the buyer's account was debited one cent. Unveiling of a smart contract, in other words, the part of a contract performed by computers was reduced to code that a group of computers checks before beingpermanently stored in the database. When the widget was delivered, the smart contract was

enabled. The other nodes receive the transaction and verify the buyer's identity. It holds the currency promised to the widget seller. Verification may include verifying the buyer's account for sufficient funds for the purchase. To create an immutable record, nodes in the network must solve a mathematical problem to add a new block of transactions to the chain. Consequently, the buyer cannot spend the money he gave the seller since everyone knows he no longer owns it.

Chain management

It's possible that the technology's actual appeal was due to the entire transparency it gives, not the ability to stay anonymous like cryptocurrencies like Bitcoin. The blockchain technology underpinning it has applications in an increasing number of sectors.

"A decentralized platform that executes smart contracts, " Ethereum defined blockchain in 2013. There was also a statement that blockchain "allows developers to establish marketplaces, store debt or promise registries, transfer money in line with instructions made in the past" (e.g., a will or futures contract). Unlike Bitcoin, which was primarily a currency, Ethereum was "aledger technology that corporations were leveraging to build new applications."

Existing systems

Many nations now have computerized voting systems in place. Estonia was the first to do so, and it was the only nation that has done so far. In Estonia's latest election, approximately 30.5 percent of all votes were cast online. To develop a better voting platform, we studied several current systems, like Estonia, identified their weaknesses, and devised a new approach. Estonia issued each resident a national ID card, which served as the voting system's core hub. The voter's identity was protected by this card. The voting procedure begins with the voter entering their card into a card reader after visiting the voting website on the linked computer. The system then requests their PIN and verifies their voting eligibility, allowing them to cast their ballot only after successful authentication. Voters have until four days before Election Day to vote in this procedure. Consumers might vote using their cell phones if a card reader was unavailable. The VFS (Vote Forwarding Server), VSS (Vote Storage Server), and VCS (Vote Control Server) servers were used in this approach (Vote Counting Server)[31].

When a voter submits a ballot, it was first routed via the VFS and VSS, which were both open to the public (where the vote in encrypted and stored until the election period was over). All votes in the VSS were de-identified before being transmitted to the VCS via DVD[34]. This VCS was isolated from all networks; it decrypts and counts all votes before displaying the results. This method has been researched by several researchers, who have uncovered several security issues. This system's centralized functionality allows any attackers or other parties to perform database modifications [3]. This approach also enables voters to vote as often as they like within the four days they have available. In this paradigm, the voter cannot know whether his vote was cast for the correct party, which might lead to any third-party alterations to the casted vote. As a result, the users cannot agree on the final count.

Also found the New South Wales Vote System, which we've modified. This approach solves the problem by allowing the voter to choose a six-digit PIN. The voter theologians' system was based on using an ID and a PIN. Each voter was given a 12-digit receipt number upon successful verification. To verify the vote, the voter must provide their ID, PIN, and receipt number, which was an optional choice[50].

Another system, Team Plymouth Pioneers, devised a Blockchain-based alternative. This was followed by the creation of two blockchains, one for keeping voter information (Voter's Blockchain) and the other for recording vote data (Voter's Blockchain) (Votes blockchain). The voter's Blockchain was used to authenticate their right to vote, and the vote cast was recorded in the votes Blockchain. Once a vote was cast, the information of the corresponding voter was removed from the voter's Blockchain.

Another way to fix this system was to create a situation in which voting for a candidate was linked to a bitcoin transaction. Each voter who intends to vote sends a Ballot Coin to the wallet of the selected party, and the total number of Ballot Coins in each candidate's wallet determines the outcome. Valid votes were only kept on the Blockchain in this manner (Secure Electronic Voting System using Blockchain Technology)[58]

3. Methodology

Idealizing Sri Lankan's Electoral system and Demography

As noted in the chapter on the literature study, the electoral system and population of a nation were dependent on the ultimate design of electronic voting systems. Since the research was conducted in the setting of Sri Lankan elections, the e-voting system's functionality and design were based on Sri Lanka's electoral environment. The method provided in this study still involves the use of voting centers. That was not viable to provide direct e-voting on voter-owned devices in Sri Lanka due to the country's limited internet and technology accessibility and technological literacy. According to the suggested proposal, voters were expected to cast their ballots at polling centers identical to those used under the present system[35].

There were Twenty-two electoral districts comprise Sri Lanka's election system. Therefore, this separation was considered when building the proposed system's architecture. This chapter provided information on the research methods utilized for this Research. The next chapter explains the suggested solution for the electronic voting system while offering details on the reference implementation[39].

As indicated earlier, the proposed electronic voting method requires voters to cast their ballots at polling centers. As previously indicated, the scope of this research will primarily focus on the voting and vote counting phases of elections. Thus, it was presumed that all eligible voters previously were added to the electronic voting system, and the required functions for adding eligible voters to the electronic voting system were supplied at the implementation level.

Once a voter was entered the polling place, they were required to present a valid form of identification. That was

the national identification card or the passport in Sri Lanka. All eligible voters were added to the e-voting system with this unique identifier before the elections (national identity card number was used for the prototype design).

The election officer at the polling location were verified the voter's identification and inserted the reference number into the electronic voting system. The system's next thing was verified the authenticity of the submitted unique reference by comparing it to the data in the ledger. The submitted reference was only demanded legitimate if it was accessible as an eligible voter and a vote has not yet been cast. If the user's information was invalid, the system was planned to return a warning, and the user had been unable to vote. If the input were legitimate, the system would return a temporary token that had been allocated to the voter on the client side if the input was valid. The voter will then cast their ballot, and this information, together with the temporary token, had been transmitted to the electronic voting system.

If the temporary token was legitimate, the electronic voting system was saved the vote in the ledger and updated vote totals. Finally, the system will produce a unique token and return it. The voter can keep this token and subsequently use it to confirm that the vote has been counted.

System components and architecture

Hyperledger Fabric Network Design

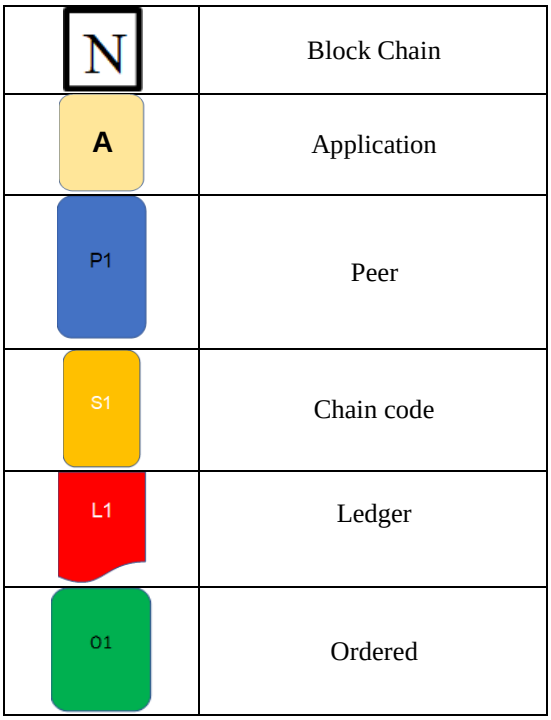
For the electronic voting system, the Hyperledger Fabric blockchain was setup under a single organization. Since the electronic voting system was a single system, all participants have accessed the system's shared information[17]. The blockchain may model this as a single 'organization.'

The 'organization' comprised several 'peers' nodes that manage the voting base. If necessary, the number of peers have been increased or decreased vertically to accommodate the number of voters. Following the concept of Hyperledger Fabric, each "Peer node" will have a 'ledger' copy and a 'world state' DB instance. The 'Couch DB' database was utilized for the 'world state' database as it was the preferred option for production-grade systems utilizing Hyperledger Fabric. At each of these 'peer' nodes, the e-voting 'chain code' comprising numerous Smart Contracts that comprise the whole e-voting system's logic had been implemented. This allows all Peer nodes to participate in electronic voting functions[44].

A multiple node 'ordering service' had been set up to use RAFT as the consensus mechanism. The advice from the Hyperledger Fabric documentation influences the selection of the RAFT consensus method, as it was the preferred algorithm at the time of this research[19]. For all "peer" and "ordering service, " a single "channel had connected nodes." Multiple Channels may be utilized to subdivide the network, if necessary. Nevertheless, with this suggested system, all 'peer nodes' must be engaged in the e-voting features and share information. Consequently, a single 'channel' was utilized to connect all 'peer nodes' and sustain the flow of information.

Two 'Certificate authority' instances served as 'Membership Service Provider' (MSP) of the 'organization' and 'ordering service nodes. According to the design of the Hyperledger Fabric platform, separate "certificate authorities" were required for each "organization" and "orderer service." These instances of 'Certificate authority' were used for the authentication and authorization of network participants[70].

According to the proposed scenario, electronic voting was possible while some voters cast their ballots on paper. A certain organizer wants to conduct a vote that allows for electronic voting. There was a registration deadline announced. Until now, every voter eligible to vote may signal their desire to vote online. After entering the system using credentials obtained from the voting organizer (for example, x.509 certificates), the user must be notified about using the system (decisions were changed later if registration time was not over)[48].



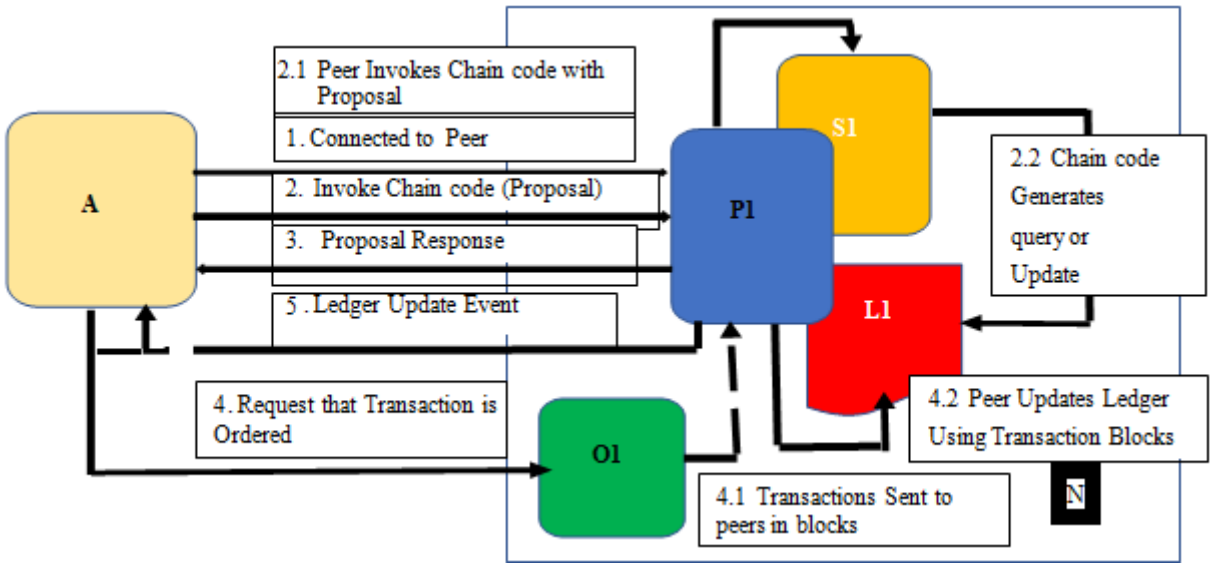


Figure 3.3: Network Design

Design of the Application API Layers

A service application layer composed of REST web services serves as access points to the Smart Contracts. Interact with the distributed ledger system. The Hyperledger Fabric Software Development Kit (SDK) provides the capabilities necessary to connect safely and effectively with Smart Contracts in the network[64].Admin, the services give access to administrative functions such as election definition, voter registration, and ballot validation. Through REST APIs, users may register, start and finish voting periods, and publish results. Client services give access to voting-related features such as voter identification. REST APIs were used for validation, saving votes, and producing vote references. Administrative clients link to the administration service cluster and voting center clients. Link to the cluster of Client service providers[30].

These REST services utilize NodeJS. The primary justification for picking NodeJS is. Supported by the default SDK of the Hyperledger Fabric. It was crucial to realize that this application layer contains no capabilities or data. The e-voting system's logic was handled via a communication layer with the blockchain, in addition to Intelligent Contracts. The following diagram depicts the system architecture of the proposed electronic voting system.

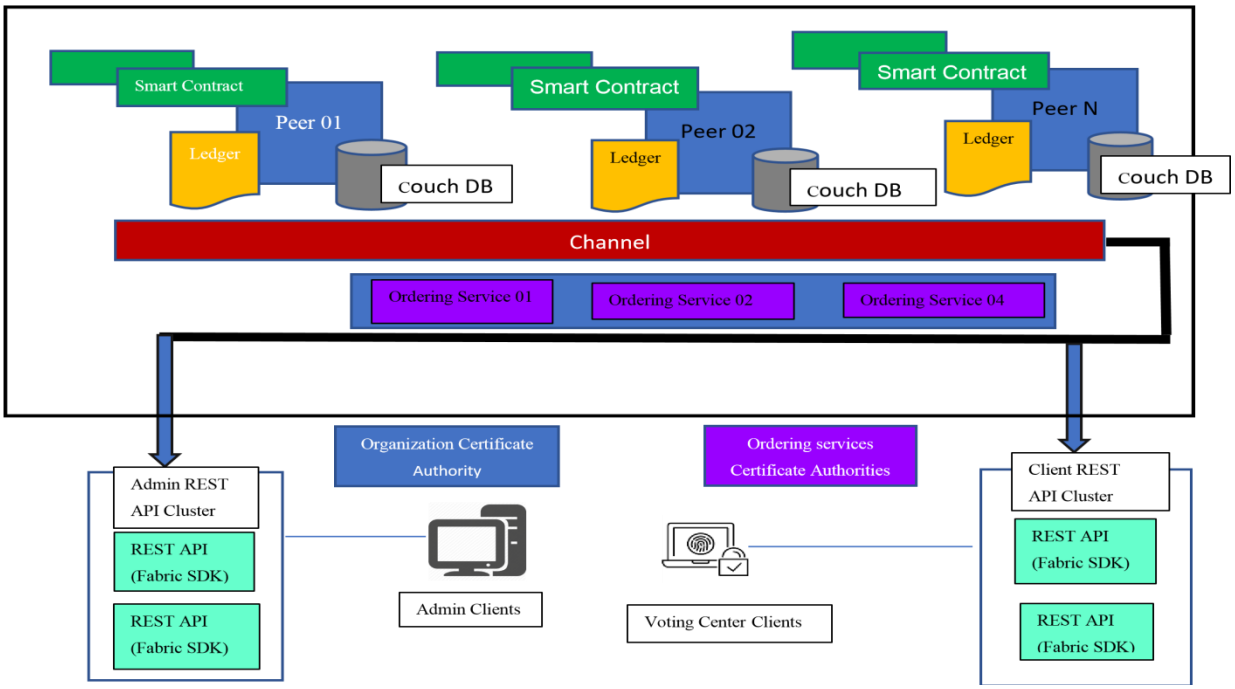


Figure 3.5: Architecture of the Proposed E-Voting System Flow Chart

Aspects of the E-voting system's deployment

The Hyperledger Fabric blockchain platform was intended as docker images that were deployment ready. Each 'peer' requires two Docker containers, one for the 'peer' and the other for 'CouchDB.' Instances of the 'Ordering Service' were deployed as Docker containers. Two more Docker containers were built for the Certificate Authorities (MSP). Admin REST services and client REST services were deployed in distinct Docker containers.

Since this suggested system requires many Docker containers, a container orchestration solution such as Docker Swarm or Kubernetes was employed for management purposes[38]

Steps of the voting process

a) Network configuration,
b) Voting configuration,
c) User registration,
d) Voting

a) Network configuration

In the first phase, the chief administrator specifies the permissions (read, write) and the number of nodes each organization has. Then, it expands the network, adds nodes for each organization where CAs were situated, loads logic (chain code), and defines the ordering of nodes that had been involved in achieving consensus on adding transactions in the ledger.

b) Voting configuration

Each Dep administrator created the extra data (start/end of voting and registration, list of voters) required to conduct voting among departmental voters. This information must be entered into the ledger since it was required for the local election. Also, at this step, two key pairs were formed for each unit. The public one was recorded to the ledger, while the private one was stored in the private data collection, a Hyperledger Fabric mechanism restricting data access. After each user's data was downloaded, the list of accessible polls was updated.

c) User Registration

This step was essentially required for several reasons: To keep the ability of a voter to vote using paper-based ballots (if the user was not registered, he can only vote in the conventional manner) and to protect the privacy of the voter's vote and maintain eligibility.

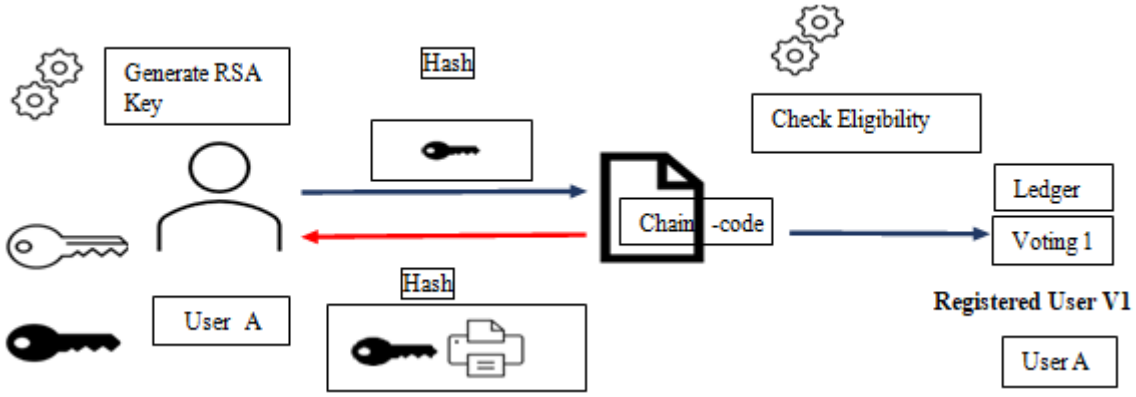


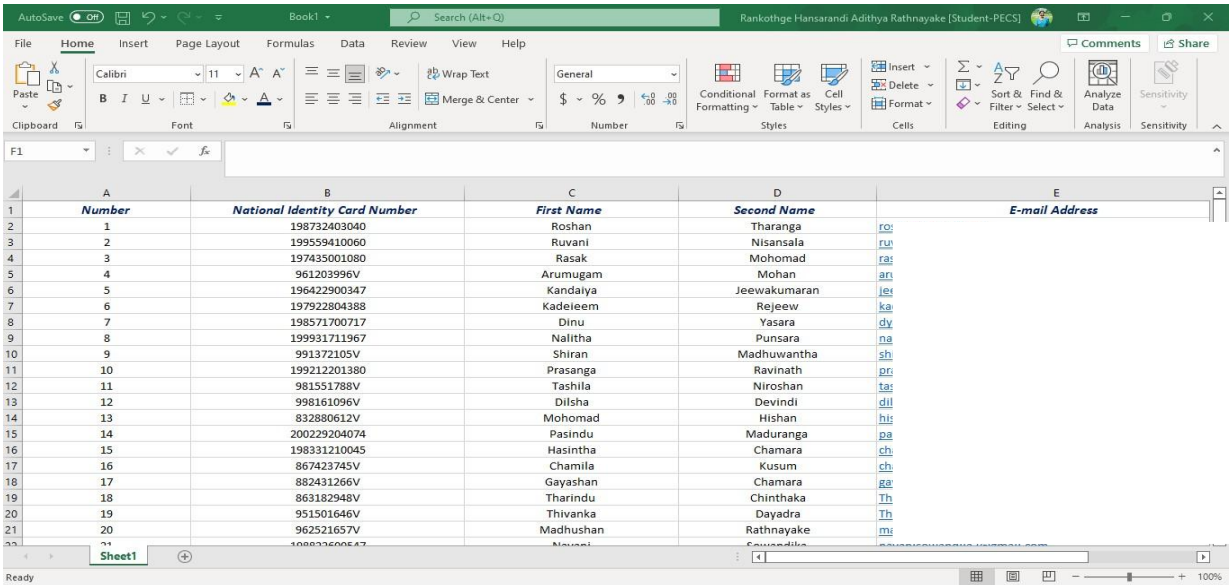
Figure 3.10: User Registration for E - Voting

O Registering a Public Key that corresponds to a Private Key.

The person was Only Known by Voter and NIC. The user has a signed public key delivered to the Chain code anonymously via the Identity mixer. Both Public and Privet Keys had been examined. If they were accurate, the public was added to the distributed ledger. During the voting phase, voter requests were anonymous; therefore, eligibility may be checked using public keys.

O Testing the Registration Process and Validation

Validation Process and Test Registration Runs were tested Using Dummy Data sets which Have to be True and Accurate within the department of Person Registration of Sri Lanka. The process was combined with the dummy data set and the configuration test. While feeding the Data from the Input side, the Process Validated the processors and had been given the proper next steps as mentioned above.



Number	National Identity Card Number	First Name	Second Name	E-mail Address
1	198732403040	Roshan	Tharanga	ro:
2	199559410060	Ruvani	Nisansala	ru
3	197435001080	Rasak	Mohomad	ra
4	961203996V	Arumugam	Mohan	ar
5	196422900347	Kandaiya	Jeewakumaran	je
6	197922804388	Kadeieem	Rejeew	ka
7	198571700717	Dinu	Yasara	dy
8	199931711967	Nalitha	Punsara	na
9	991372105V	Shiran	Madhuwantha	sh
10	199212201380	Prasanga	Ravinath	pr
11	981551788V	Tashila	Niroshan	ta
12	998161096V	Dilsha	Devindi	dil
13	832880612V	Mohomad	Hishan	hi
14	200229204074	Pasindu	Maduranga	pa
15	198331210045	Hasintha	Chamara	ch
16	867423745V	Chamila	Kusum	ch
17	882431266V	Gayashan	Chamara	ga
18	863182948V	Tharindu	Chinthaka	Th
19	951501646V	Thivanka	Dayadra	Th
20	962521657V	Madhushan	Rathnayake	ma

Figure 3.11: Dummy Data Set of Voters and Necessary Inputs

- Obtaining a Blind Signature (Sub Step).

Each user creates a pair of keys (public) and (private) and a random integer upon registration. The hash function over the voter's public key has Functioned with each other. The outcome of this expression and the voter's election preferences were transmitted to the Chain code, which was responsible for the registration logic. It verifies if the current user was permitted to vote based on information from the CA (Election Commissionand the Department for Registration of Persons). If genuine, Voter's Identity was signed through the department's private key. The received data is transmitted back to the user. Then, the Chain code records information to the ledger indicating that the current user has gotten a blind signature. After the voter registration process, the list of voters (if supplied) was utilized to prevent revoting[43].

4. Results and Discussion

Designing and Implementing the Application.

The initial thing that needed to be covered was designing and implementing the application. The Whole Design was implemented using the Hyperledger Fabric and With the Smart Contracts[44]. The implementation is the same for both Web applications and the Mobile application. As a result, the mobile application (APK) and the web application Were implemented to make the basic desires. Used the mentioned platform and Successfully Ran the System In a Small Spaced (4GB RAM, Intel(R) Core (TM) i3-10110U CPU @ 2.10GHz 2.59 GHz) Device. The designs Performance had been dependent on the device and the type of memory it has. To make more reliable on the system or the proposed application More Spaced or connected Hubs were preferable. And enhanced thetime accuracy, and Technical Limitations were Reduced.

They were handling the possibly large Number of entries and their conversion into a single or a few blockchains regarding the situation.

Here the Data Collective Method was giving access to the CA's else the authority to the Election Commission of Sri Lanka and the Provincial Respectable department. The Test Transmission is done using Correct NIC and Real Personal Details as a Dummy Data set. And the data were stored in the administrative code storage, which links to the process of the Verification of the Person Identity.

Creating Specific Authorities & Blocking the Reverse Engineering Process

The Specific Authorities were Defined Through the Hyperledger fabric using X.509 Certificates within to Hyperledger Fabric. The processors of the Organizations were Clarified as Org, Dep, and V types[76]. Those are Election commission of Sri Lanka, Department of personal Registration and also the Provincial Authorities. In Voting Configuration Process, The Department Administration has the admin Purpose but the Throughout Hyperledger Fabric. The Mechanism Restricts the Data Access, which only shows a made-up Public Key (X13vRZzqgL41). This restricts the Reverse Engineering, which was dug into the privacy Data and can't decode since the flow was forward only to the Couch DB and the Storage. The Selection CouchDB Over LevelDB, Considered the scenario and the Limitations of the reverse biased data process and the Limitation within the large number or entries which occurred by LevelDB.

```
jsonBody['$class'] = "BVCSL";
jsonBody['voteId'] = "t" + Math.abs(hash((new Date()).getTime().toString() + voterId));
jsonBody['ballot'] = ballotId;
jsonBody['newOwner'] = candidateId;
console.log(jsonBody);
```

Figure 4.3: Public Key Appearance as a Final Output

Protect the Voter's Privacy & Encrypt and Authority

The methodology Network Configuration Chapter Covered how to protect the Voter's privacy so that Others Cannot See the Voter's ID. The User Registration Section on the methodology clearly defined and made public but specific Key Using Person's NIC and that were Proceed only when the Voter's NIC was Valid and after verifying it from the person registration Department of Sri Lanka. As mentioned above, that generated key also Prevents the reverse biased process. That makes voter's Privacy Secure. Encrypt and authority in here is the Only Viewers had been the One Admin from the Named Authorities like Election Commission in Sri Lanka, Department of Registration persons and subdivision and Proportional system at district and provincial levels. The Assigns CA's were had been Connected with the Hyperledger and Part of the created Blocks.

Table 4.2: Time Counting and Result Evaluation

Voting Process Time				Transaction Speed		
Samples (Individual Voters)	Min (s)	Max (s)	Average (s)	Min (ms)	Max(ms)	Average (ms)
First 100	2	5.07	0.0307	1600	2500	9
Rest 900	2	4.38	0.0026	370000	160000	233.33

Reducing the Time of the Counting Process

One can see that response times vary with the number of concurrent users consuming the system when looking at the prototype system. In the prototype configuration, a single system with two core CPUs and 4 GB of RAM was shared by two peer nodes, two CouchDB nodes, and one REST service. As you can see, when the number of Voters increases, the Transaction speed was Decreased. The prototype system can process 100 voters in less than one minute with only three concurrent users, even with the worst-case response time. Assumed it takes 10 seconds for a single "voter." To assess the scalability of the prototype system, it

must be deployed with enough resources and services separated. Response times vary with the number of concurrent users consuming the system. However, it has been shown that the average reaction time of the voting stages fluctuates between three and four seconds when considering three concurrent voters.

Since the Paper Ballot traditional voting system was takes more than 10 minutes for the transaction Process and even takes hours to collect and evaluate the results. The proposed system was more accurate than the Traditional one: the Voter Registration and the process time slots are displayed in the above Figures. Manipulate the rejected Votes and Block the Fake Votes.

Eventually, there won't have any fake Votes since the Authorities were Making Up the Public key with Registered NIC Numbers, As mentioned in the Blind Signature chapter in methodology. Double Voting is Also disabled in the scenario.

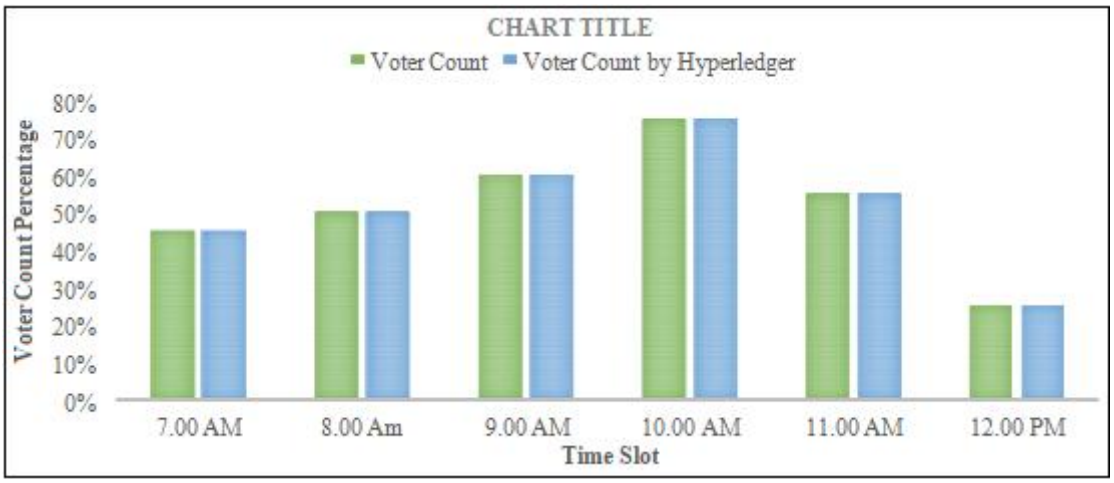


Figure 4.6: Voter Count Accuracy

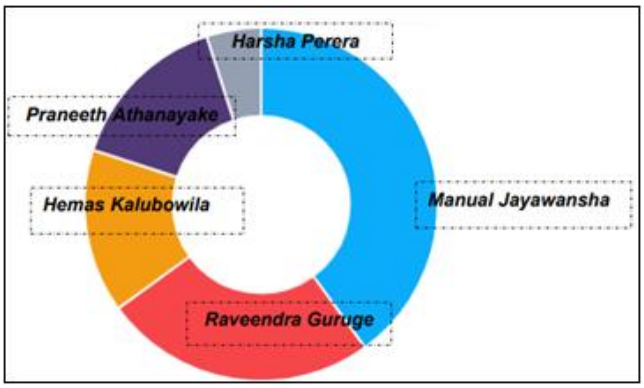


Figure 4.9: Test Run Result Using Dummy Vote Set

Advantages and effectiveness of the traditional voting system and the Blockchain-based voting system. For The use of Easily Compare, the given table had been presented the Advantages and Disadvantages Between E -voting a system, Ballot based Voting systems, and the Proposed one

Table 4.2.2: Comparison between Different Voting Systems and Important Facts

Factors	Type of the Voting System		
	Ballot Based System	Electronic Voting Machin	(Proposed Blockchain approach)
Accessibility	Low	Low	Average (When the system was interconnected to the large scale one system, Probability of accessibility had been less on less Run
Validity of Ballot	Low	Good	Good.
Fraud Prevention	Average	Average	Good
Vote Tally Time Factor	Extremely Slow	Good	Advance
Ease for Voter Turn Out	Low	Low	High
Adoption Rate	High	Average	Negligible
Cost Factor	Expensive	Extremely Expensive	Average (Less on Long Runs)
Training Required	Low	Low	High
Scalability	Low	Low	High

5. Conclusion

Every registered voter had been able to vote via any Internet-connected device. In addition, the proposed technology addresses aspects that were not currently addressed, such as a secure timing of voting abroad, the automatic management of electoral lists, integration of the identification process with that of advanced voting secrecy, and automatic and trustworthy mechanisms to ensure the security of voting.It was anticipated that the suggested

solution architecture, prototype system, and published data would serve as a foundation for future research on private blockchains for e-voting systems[71].

Since the Generated Pk was unique to each Voter and It creates within the Voter's Unique NIC number. Choose CouchDB Over LevelDB since the LevelDBhas the high risk of backward Process and the Limitation within the Entities or the large number of entries. When Using the Couch DB there was an extra advantage of store and Clouding within the forward only Process. Is someone breaks the Rules and Wanted to Back the Proceed It's Impossible since the Couch DB is a storage which can't decode.

In this case when the Voter amount Increase the higher the time laps occurred.As Suggested, it will mitigate while working with the industrial Equipment and Supplies. The finally critical requirements were manipulating the Rejected and Fake Votes. As discuss within the Result section the Fake votes were negotiable than to the traditional voting Procedure. Because of the Unequally generated PK.

The goal of the design and testing of the proposed electronic voting system was to determine the viability of a decentralized solution capable of satisfying the most stringent criteria of both public settings and private corporate consortiums. Based on preliminary findings, it was evident that blockchain met the requirements for electronic voting systems. Include openness, consistency, and resiliency. In addition, the advancement was apparent. Enables blockchain technology to automate activities in an immutable and safe manner[29].

6. Further Development

Implementation Scenario &Increase the Efficiency

To simulate a production-grade deployment and evaluate the system's capabilities, the proposed system must be deployed in a distributed network with several worker nodes. And, while using Hyperledger fabric

It's better to Combine with IBM developer Platform for record and Finalize the Implementation in Friendlier Environment. The Coding and The Development Method will be different from the given method. But the Basics with the Development Process will be based on Suggested Scenario.

Data from CouchDB was accessible via an HTTP URI. This enables do HTTP actions on data (GET, DELETE, PUT, and POST). With indices, the state database enables querying huge quantities of chain code more effective and versatile, and Level DB provides a straightforward, quick database with less overhead than CouchDB.

For the testing Purpose or research Purpose, suggest using the Upgrade Version of the Hyperledger fabric alone with the Docker Software. Make sure to match the Versions and Upgrade them as same. And convert the operating System into the Ubuntu for the latest version as well, since the Hyperledger was the Linux based Platform. Because the Version of all above will be dependable criteria for the Time efficiency and Transaction speed. Moreover, the hashes generating speed is dependent on the Type of the Computer than we wanted to test the scenario so far.

References

[1] Abuidris, Y., Kumar, R. and Wenyong, W., 2019, December. A survey of blockchain based on evoting systems. In Proceedings of the 2019 2nd International Conference on Blockchain Technology and Applications (pp. 99-104).

[2] Adeshina, S.A. and Ojo, A., 2019, December. Maintaining voting integrity using Blockchain. In 2019 15th International Conference on Electronics, Computer and Computation (ICECCO) (pp. 1-5). IEEE.

[3] Agbesi, S. and Asante, G., 2019, November. Electronic voting recording system based on blockchain technology. In 2019 12th CMI Conference on Cybersecurity and Privacy (CMI) (pp. 18). IEEE.

[4] Alam, A., Rashid, S.Z.U., Salam, M.A. and Islam, A., 2018, October. Towards blockchain-based evoting system. In 2018 international conference on innovations in science, engineering and technology (ICISET) (pp. 351-354). IEEE.

[5] Alvi, S.T., Uddin, M.N. and Islam, L., 2020, August. 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) (pp. 228-233). IEEE

[6] Androulaki, E., Barger, A., Bortnikov, V., Cachin, C., Christidis, K., De Caro, A., Enyeart, D., Ferris, C., Laventman, G., Manevich, Y. and Muralidharan, S., 2018, April. Hyperledger fabric: a distributed operating system for permissioned blockchains. In Proceedings of the thirteenth EuroSys conference (pp. 1-15).

[7] Androulaki, E., Cachin, C., De Caro, A., Kind, A. and Osborne, M., 2017, January. Cryptography and protocols in hyperledger fabric. In Real-World Cryptography Conference (pp. 12-14).

[8] Antipova, T. and Rocha, Á. eds., 2019. Digital Science. Springer

[9] Anwar ul Hassan, C., Hammad, M., Iqbal, J., Hussain, S., Ullah, S.S., AlSalman, H., Mosleh, M.A. and Arif, M., 2022. A Liquid Democracy Enabled Blockchain-Based Electronic Voting System. Scientific Programming, 2022.

[10] Aswale, N.S., Mali, M.S., Irale, S.S., Dhoka, S.S., Mudaliar, T.H., Machhale, G.G. and Sonkamble, R.G., 2021, May. Privacy Preserved E-Voting System Using Blockchain. In Proceedings of the International Conference on Smart Data Intelligence (ICSMDI 2021).

[11] Berdik, D., Otoum, S., Schmidt, N., Porter, D. and Jararweh, Y., 2021. A survey on blockchain for information systems management and security. Information Processing & Management, 58(1), p.102397.

[12] Bishop, M. and Wagner, D., 2007. Risks of e-voting. Communications of the ACM, 50(11), pp.120120.

[13] Brotsis, S., Kolokotronis, N., Limniotis, K., Bendiab, G. and Shiaeles, S., 2020, October. On the security and privacy of hyperledger fabric: Challenges and

open issues. In 2020 IEEE World Congress on Services (SERVICES) (pp. 197-204). IEEE.
[14] Buchsbaum, T.M., 2004. E-voting: International developments and lessons learnt. In Electronic voting in Europe-Technology, law, politics and society, workshop of the ESF TED programme together with GI and OCG. Gesellschaft fürInformatik eV.
[15] Casado-Vara, R. and CoRCHaDo, J.M., 2018. Blockchain for democratic voting: How blockchain could cast of voter fraud. Oriental journal of computer science and technology, 11(03), p.2019.
[16] Cheema, M.A., Ashraf, N., Aftab, A., Qureshi, H.K., Kazim, M. and Azar, A.T., 2020, November. Machine Learning with Blockchain for Secure E-voting System. In 2020 First International Conference of Smart Systems and Emerging Technologies (SMARTTECH) (pp. 177-182). IEEE.
[17] Chaieb, M., Yousfi, S., Lafourcade, P. and Robbana, R., 2018, October. Verify-your-vote: A verifiable blockchain-based online voting protocol. In European, Mediterranean, and Middle Eastern Conference on Information Systems (pp. 16-30). Springer, Cham
[18] Cooley, R., Wolf, S. and Borowczak, M., 2018, September. Blockchain-based election infrastructures. In 2018 IEEE international smart cities conference (ISC2) (pp. 1-4). IEEE.
[19] Curran, K., 2018. E-Voting on the Blockchain. The Journal of the British Blockchain Association, 1(2), p.4451.
[20] Denis González, C., Frias Mena, D., Massó Muñoz, A., Rojas, O. and Sosa-Gómez, G., 2022. Electronic Voting System Using an Enterprise Blockchain. Applied Sciences, 12(2), p.531.
[21] Díaz-Santiso, J. and Fraga-Lamas, P., 2021. E-Voting System Using Hyperledger Fabric Blockchain and Smart Contracts. Engineering Proceedings, 7(1), p.11.
[22] Fauziah, Z., Latifah, H., Omar, X., Khoirunisa, A. and Millah, S., 2020. Application of Blockchain Technology in Smart Contracts: A Systematic Literature Review. Aptisi Transactions on Technopreneurship (ATT), 2(2), pp.160-166.
[23] Garg, K., Saraswat, P., Bisht, S., Aggarwal, S.K., Kothuri, S.K. and Gupta, S., 2019, April. A comparitive analysis on e-voting system using blockchain. In 2019 4th International Conference on Internet of Things: Smart Innovation and Usages (IoT-SIU) (pp. 1-4). IEEE.
[24] Gerlach, J. and Gasser, U., 2009. Three case studies from switzerland: E-voting. Berkman Center Research Publication No, 3, p.2009.
[25] Gibson, J.P., Krimmer, R., Teague, V. and Pomares, J., 2016. A review of e-voting: the past, present and future. Annals of Telecommunications, 71(7), pp.279-286.
[26] Graf, M., Küsters, R. and Rausch, D., 2020, September. Accountability in a permissioned blockchain: Formal analysis of hyperledger fabric. In 2020 IEEE European Symposium on Security and Privacy (EuroS&P) (pp. 236-255). IEEE.
[27] Hardwick, F.S., Gioulis, A., Akram, R.N. and Markantonakis, K., 2018, July. E-voting with blockchain: An e-voting protocol with decentralisation and voter privacy. In 2018 IEEE International Conference on Internet of Things (iThings) and IEEE Green Computing and Communications
[28] (GreenCom) and IEEE Cyber, Physical and Social Computing (CPSCom) and IEEE Smart Data (SmartData) (pp. 1561-1567). IEEE.
[29] He, Z.G.X. and Zou, P., Voting System Based on Blockchain. Halpin, H. and Piekarska, M., 2017, April. Introduction to Security and Privacy on the Blockchain.
[30] In 2017 IEEE European Symposium on Security and Privacy Workshops (EuroS&PW) (pp. 1-3). IEEE.
[31] Hanifatunnisa, R. and Rahardjo, B., 2017, October. Blockchain based e-voting recording system design. In 2017 11th International Conference on Telecommunication Systems Services and Applications (TSSA) (pp. 1-6). IEEE.
[32] Hjálmarsson, F.Þ., Hreiðarsson, G.K., Hamdaqa, M. and Hjálmtýsson, G., 2018, July. Blockchainbased e-voting system. In 2018 IEEE 11th international conference on cloud computing (CLOUD) (pp. 983-986). IEEE.
[33] Hwang, W.Y. and Kim, H.K., 2020. A Study on Implementation of BlockChain Voting System using Hyperledger Fabric. The Journal of Korea Institute of Information, Electronics, and Communication Technology, 13(4), pp.298-305.
[34] Jinasena, T.M.K.K. and Gangodawila, N., Blockchain-based Secure, Reliable, and Distributed Voting System for Decision Making in Government Policies and Projects
[35] Johnson, D., 2019. Blockchain-based voting in the US and EU constitutional orders: a digital technology to secure democratic values?. European Journal of Risk Regulation, 10(2), pp.330-358. 35. Jun, M., 2018. Blockchain government-a next form of infrastructure for the twenty-first century. Journal of Open Innovation: Technology, Market, and Complexity, 4(1), p.7.
[36] Kamil, M., Bist, A.S., Rahardja, U., Santoso, N.P.L. and Iqbal, M., 2021. COVID-19: Implementation e-voting blockchain concept. International Journal of Artificial Intelligence Research, 5(1), pp.25-34.
[37] Khan, K.M., Arshad, J. and Khan, M.M., 2020. Investigating performance constraints for blockchain based secure e-voting system. Future Generation Computer Systems, 105, pp.13-26.
[38] Kang, B.B. and Jang, J. eds., 2019. Information Security Applications: 19th International Conference, WISA 2018, Jeju Island, Korea, August 23–25, 2018, Revised Selected Papers (Vol. 11402). Springer.
[39] Kirillov, D., Korkhov, V., Petrunin, V., Makarov, M., Khamitov, I.M. and Dostov, V., 2019, July. Implementation of an e-voting scheme using hyperledger fabric permissioned blockchain. In International Conference on Computational Science and Its Applications (pp. 509-521). Springer, Cham.
[40] Kshetri, N. and Voas, J., 2018. Blockchain-enabled e-voting. Ieee Software, 35(4), pp.95-99.
[41] Kumar, D.D., Chandini, D.V., Reddy, D., Bhattacharyya, D. and Kim, T.H., 2020. Secure electronic voting system using blockchain technology. International Journal of Smart Home, 14(2), pp.31-38. 42. Maaten, E., 2004. Towards remote e-voting: Estonian case. In Electronic voting in

EuropeTechnology, law, politics and society, workshop of the ESF TED programme together with GI and OCG. Gesellschaft fürInformatik eV.

[42] Mechkaroska, D., Dimitrova, V. and Popovska-Mitrovikj, A., 2018, November. Analysis of the possibilities for improvement of blockchain technology. In 2018 26th Telecommunications Forum (TELFOR) (pp. 1-4). IEEE.

[43] McCorry, P., Shahandashti, S.F. and Hao, F., 2017, April. A smart contract for boardroom voting with maximum voter privacy. In International conference on financial cryptography and data security (pp. 357-375). Springer, Cham.

[44] Mirza, E.Z., Shaikh, A., Khalifa, N., Khan, Y. and Shaikh, A., 2020. Use of Blockchain for Secure E-voting

[45] Misra, S., Gervasi, O., Murgante, B., Stankova, E., Korkhov, V., Torre, C., Rocha, A.M.A., Taniar, D., Apduhan, B.O. and Tarantino, E. eds., 2019. Computational Science and Its Applications– ICCSA 2019: 19th International Conference, Saint Petersburg, Russia, July 1–4, 2019, Proceedings, Part VI (Vol. 11624). Springer.

[46] Moubarak, J., Filiol, E. and Chamoun, M., 2018, April. On blockchain security and relevant attacks.

[47] In 2018 IEEE Middle East and North Africa Communications Conference (MENACOMM) (pp. 1-6). IEEE.

[48] Mukherjee, P.P., Boshra, A.A., Ashraf, M.M. and Biswas, M., 2020, June. A hyper-ledger fabric framework as a service for improved quality e-voting system. In 2020 IEEE Region 10 Symposium (TENSYMP) (pp. 394-397). IEEE.

[49] Nakaike, T., Zhang, Q., Ueda, Y., Inagaki, T. and Ohara, M., 2020, May. Hyperledger fabric performance characterization and optimization using goleveldb benchmark. In 2020 IEEE International Conference on Blockchain and Cryptocurrency (ICBC) (pp. 1-9). IEEE.

[50] Nasir, Q., Qasse, I.A., Abu Talib, M. and Nassif, A.B., 2018. Performance analysis of hyperledger fabric platforms. Security and Communication Networks, 2018.

[51] Osgood, R., 2016. The future of democracy: Blockchain voting. COMP116: Information security, pp.1-21

[52] Padmavathi, U. and Rajagopalan, N., 2021. Concept of blockchain technology and its emergence. In Blockchain Applications in IoT Security (pp. 1-20). IGI global.

[53] Panja, S., 2021. Zero-Knowledge Proof, Deniability and Their Applications in Blockchain, E-Voting and Deniable Secret Handshake Protocols (Doctoral dissertation, Indian Statistical InstituteKolkata).

[54] Patel, D., Nandi, S., Mishra, B.K., Shah, D., Modi, C.N., Shah, K. and Bansode, R.S., 2020. IC-BCT 2019. Springer Singapore.

[55] Popovski, L., Soussou, G. and Webb, P.B., 2018. A brief history of blockchain. Leg. News

[56] Prosser, A., 2014. Transparency in evoting: lessons learnt. Transforming Government: People, Process and Policy.

[57] Rathee, G., Iqbal, R., Waqar, O. and Bashir, A.K., 2021. On the design and implementation of a blockchain enabled e-voting application within iot-oriented smart cities. IEEE Access, 9, pp.3416534176.

[58] Rathnayake, R.A.T.L., 2022. Blockchain-Based E-Voting System for Elections in Sri Lanka (Doctoral dissertation).

[59] Saberi, S., Kouhizadeh, M., Sarkis, J. and Shen, L., 2019. Blockchain technology and its relationships to sustainable supply chain management. International Journal of Production Research, 57(7), pp.2117-2135.

[60] Sadia, K., Masuduzzaman, M., Paul, R.K. and Islam, A., 2020. Blockchain-based secure e-voting with the assistance of smart contract. In IC-BCT 2019 (pp. 161-176). Springer, Singapore.

[61] Shakhovska, N., 2017. Advances in intelligent systems and computing. Springer International Pu.

[62] Shakhovska, N. and Stepashko, V. eds., 2017. Advances in Intelligent Systems and Computing II: Selected Papers from the International Conference on Computer Science and Information Technologies, CSIT 2017, September 5-8 Lviv, Ukraine (Vol. 689). Springer

[63] Sharma, A., Schuhknecht, F.M., Agrawal, D. and Dittrich, J., 2018. How to databasify a blockchain: the case of hyperledger fabric. arXiv preprint arXiv:1810.13177.

[64] Soni, Y., Maglaras, L. and Ferrag, M.A., 2020, June. Blockchain based voting systems. In European Conference on Cyber Warfare and Security (pp. 241-248). Academic Conferences International Limited.

[65] Stephen, R. and Alex, A., 2018, August. A review on blockchain security. In IOP Conference Series: Materials Science and Engineering (Vol. 396, No. 1, p. 012030). IOP Publishing.

[66] Swan, M., 2015. Blockchain: Blueprint for a new economy. " O'Reilly Media, Inc.".

[67] Tarasov, P. and Tewari, H., 2017. The future of e-voting. IADIS International Journal on Computer Science & Information Systems, 12(2).

[68] Taş, R. and Tanrıöver, Ö.Ö., 2020. A systematic review of challenges and opportunities of blockchain for E-voting. Symmetry, 12(8), p.1328.

[69] Taylor, P.J., Dargahi, T., Dehghantanha, A., Parizi, R.M. and Choo, K.K.R., 2020. A systematic literature review of blockchain cyber security. Digital Communications and Networks, 6(2), pp.147156.

[70] Vasant, P., Zelinka, I. and Weber, G.W., 2018. Intelligent computing & optimization. In Conference proceedings ICO (p. 804).

[71] Wisessing, K., Ekthammabordee, P., Surasak, T., Huang, S.C.H. and Preuksakarn, C., 2020. The prototype of thai blockchain-based voting system. International Journal of Advanced Computer Science and Applications, 11(5).

[72] Wüst, K. and Gervais, A., 2018, June. Do you need a blockchain?. In 2018 Crypto Valley Conference on Blockchain Technology (CVCBT) (pp. 45-54). IEEE.

[73] Yamashita, K., Nomura, Y., Zhou, E., Pi, B. and Jun, S., 2019, February. Potential risks of hyperledger fabric smart contracts. In 2019 IEEE International Workshop on Blockchain Oriented Software Engineering (IWBOSE) (pp. 1-10). IEEE.

[74] Yi, H., 2019. Securing e-voting based on blockchain in P2P network. EURASIP Journal on Wireless Communications and Networking, 2019(1), pp.1-9.

[75] Yli-Huumo, J., Ko, D., Choi, S., Park, S. and Smolander, K., 2016. Where was current research on blockchain technology?—a systematic review. PloS one, 11(10), p.e0163477.
[76] Zhang, R., Xue, R. and Liu, L., 2019. Security and privacy on blockchain. ACM Computing Surveys (CSUR), 52(3), pp.1-34.
[77] Zheng, Z., Xie, S., Dai, H.N., Chen, X. and Wang, H., 2018. Blockchain challenges and opportunities: A survey. International journal of web and grid services, 14(4), pp.352-375.