JOURNAL OF ALGEBRAIC STATISTICS
Volume 13, No. 3, 2022, p. 246- 252
https://publishoa.com
ISSN: 1309-3452

Online Voting System

Mrs. Saratha. M

Associate Processor in Computer Science and Engineering, K.S.Rangasamy College of Technology, Tiruchengode-637 215, Namakkal District, TamilNadu

Rubasri. M, Sindhu. M
Department of Computer Science and EngineeringK.S.Rangasamy College of Technology, Namakkal, India.

ABSTRACT

Traditional voting systems should be computerized to reduce the vote counting time, to provide evidence that a vote is being correctly accounted, to reduce fraud, remove errors in filling out ballots, to improve system usability for people with special needs.

E-voting increasingly replacing traditional paper based systems. This raises several security issues, given that democratic principles depend on the electoral process's integrity. An electronic voting system must ensure the voter's authenticity, anonymity. It must also ensure audit ability in a software or hardware environment that could malfunction.

In this System the fingerprints of all voters and details are stored before the election. The voters have to register their fingerprints on the day of election through online; this will be compared with the already stored prints. If both matches their votes will be taken in to the account and if not their vote will be discarded.

So No one can vote for others this will reduce the illegal votes. User can view all the nominees in their district with their corresponding party symbols. They can also view how many votes are registered before they are going to register their votes, this may be useful to know theleading result.

I. INTRODUCTION

Electronic voting systems have been the subject of active research for decades, with the goal to minimize the cost of running an election, while ensuring the election integrity by fulfilling the security, privacy and compliance requirements. Replacing the traditional pen and paper scheme with a new election system has the potential to limit fraud while making the voting process traceable and verifiable. Blockchain is a distributed, immutable, incontrovertible, public ledger. This new technology has

three main features:
(i) Immutability: Any proposed "new block" to the ledger must reference the previous version of the ledger. This creates an immutable chain, which is where the blockchain gets its name from, and prevents tampering with the integrity of the previous entries.

(ii) Verifiability: The ledger is decentralized, replicated and distributed over multiple locations. This ensures high availability (by eliminating a single point of failure) and provides third-party verifiability as all nodes maintain the consensus version of the ledger.
(iii) Distributed Consensus: A distributed consensus protocol to determine who can append the next new transaction to the ledger. A majority of the network nodes must reach a consensus before any new proposed block of entries becomes a permanent part of the ledger. These features are in part achieved through advanced cryptography, providing a security level greater than any previously known record-keeping system.

Blockchain technology is therefore considered by many, including us, to have a substantial potential as a tool for implementing a new modern voting process. This project evaluates the use of blockchain as a service to implement an electronic voting (e-voting) system. The project makes the following original contributions:
(i) Propose a blockchain-based e-voting system that uses "permissioned blockchain", and
(ii) Review of existing blockchain frameworks suited for constructing blockchain-based e-voting system.

The project first provides an overview of blockchain and smart contract technology and its respective feasibility as a service for implementing an e-voting system. A. Design considerations After evaluating both existing e-voting systems and the requirements for such systems to be effectively used in a national election, the following list of requirements is constructed for a viable e- voting system:
(i) An election system should not enable coerced voting.
(ii) An election system should allow a method of secure authentication via an identity verification service.
(iii) An election system should not allow traceability from votes to respective voters.

(iv) An election system should provide transparency, in the form of a verifiable assurance to each voter that their vote was counted, correctly, and without risking the voter's privacy.
(v) An election system should prevent any third party from tampering with any vote.
(vi) An election system should not afford any single entity control over tallying votes and determining the result of an election.
(vii) An election system should only allow eligible individuals to vote in an election.

Blockchain as a service The blockchain is an append-only data structure, where data is stored in a distributed ledger that cannot be tampered with or deleted. This makes the ledger immutable. The blocks are chained

in such a way that each block has a hash that is a function of the previous block, and thus by induction the complete prior chain, thereby providing assurance of immutability. There are two different types of blockchains, with different levels of restrictions based on who can read and write blocks.

A public blockchain is readable and writeable for everyone in the world. This type is popular for cryptocurrencies. A private blockchain sets restrictions on who can read or interact with the blockchain. Private blockchains are also known as being permissioned, where access can be granted to specific nodes that may interact with the blockchain.

In addition to cryptocurrency, blockchain provides a platform for building distributed and immutable applications or smart contracts. Smart contracts are programmable contracts that automatically execute when pre-defined conditions are met. Similar to conventional written contracts, smart contracts are used as a legally binding agreement between parties.

Smart contracts automate transactions and allow parties to reach agreements directly and automatically, without the need for a middleman. Key benefits of smart contracts compared to conventional written contracts are cost saving, enhanced efficiency and risk reduction. Smart contracts redefine trust, as contracts are visible to all the users of the blockchain and can, therefore, be easily verified.
In listening to the problems here there is various problems faced by each and every citizen in the country. The major problem is that there is not a single unique identity/card for all propose for the government departments which are used by the citizens. So there is a multiplicity in card (different cards for different department). So the citizen is suffered to take correct card for a right department. So there is a missing of card is possible. So we are disused to use a unique id/card for all purpose for those activities like id, verification and proofs.

We not yet find a good security in this existing one because there is a theft in major time. We can't maintain these logs for maximum time and we should enter these records later. We should also keep these record safely by avoid accident like fire and natural disasters.
There is missing of records are possible in keeping these record in a paper format. But when we are in a electronic records (E-records) we can be keep safely by maintaining it by the server and back backups we need to keep and we can store Hard disks and other storage areas.

SQL Server also includes an assortment of add-on services. While these are not essential for the operation of the database system, they provide value added services on top of the core database management system. These services either run as a part of some SQL Server component or out-of-process as Windows Service and presents their own API to control and interact with them.

The Service Broker, which runs as a part of the database engine, provides a reliable messaging and message queuing platform for SQL Server applications. Used inside an instance, it is used to provide an asynchronous programming environment. For cross instance applications, Service Broker communicates over TCP/IP and allows the different components to be synchronized together, via exchange of messages

SQL Server Replication Services are used by SQL Server to replicate and synchronize database objects, either in entirety or a subset of the objects present, across replication agents, which might be other database servers across the network, or database caches on the client side. Replication follows a publisher/subscriber model, i.e., the changes are sent out by one database server ("publisher") and are received by others ("subscribers"). SQL Server supports three different types of replication.

II. LITERATURE REVIEW

Paper [1] The author said that if your company is considering creating a project on blockchain, you have two options: working on a public or a permissioned blockchain. The difference between the two is similar to the public and private cloud service. One of them is open to anyone using a certain platform. The other is only available to a select group with permission to use it.
To compare, think of your company's email over VPN versus Gmail.
The public blockchain is Gmail — anyone can sign up and access those services. A permissioned blockchain is a similar to a VPN—only a select group, given access by the company, can use the company email. Third parties are unable to

use it, and they have to get approval to join. Still not sure which to choose? Here's how to decide between the two:

Public Blockchains

You probably recognize the most popular public blockchains — Bitcoin, Ethereum, and Ripple. Use a public blockchain if you want to involve the general population in your business. Anyone in the world can access a public blockchain to create transactions. And most public blockchains use a consensus mechanism called "**proof of work**" — a statement proving you've done the work for confirming the transaction and adding it to the blockchain.

Let's use bitcoin as an example.

Imagine I send you one bitcoin in a transaction.

That transaction goes to a network of millions of nodes. Somewhere, a bitcoin miner confirms the transaction by solving a mathematical puzzle. They were the fastest to solve it, so they win the right to add the transaction to the blockchain. They record the transaction and their proof of work to get paid a commission, which they earn in bitcoin. This is how standard public blockchains work. But the more your network grows, the more nodes you have in the system. The bigger the network, the slower it is to showproof of work. That means the time it takes to confirm a

transaction increases, because there's more data and more miners competing to confirm the same transaction.

Ethereum is another public blockchain platform.

The users create smart contracts, which are more complex than simple value transfers like Bitcoin. Yet all of these contract details are available to Ethereum blockchain users, from the data stored inside contracts to senders and receivers. This includes the code used and any changes made. But what if you want more privacy?

Permissioned Blockchains

A permission-based blockchain consists of a smaller, private group. For instance, 10 banks want to transact with each other— and they want to do it quickly and efficiently. But they don't necessarily want to expose those transactions to the public. So, the group of banks build a permissioned blockchain only they can access. They use it to collaborate, share data, and build trust. And rather than using proof of work, the parties involved use a consensus mechanism called "**proof of stake**" — a simple majority group validation of the transaction. It's simple consent and much faster than the proof of work that a bitcoin miner has to show. The speed of the transactions being confirmed is incredibly quick.

Permissioned blockchains can do around a few thousand transactions per second, as opposed to tens of transactions per second in the public blockchains. Use a permissioned blockchain if you want a small group to work together without interfacing to the general public. In some cases, a group of companies may use a permissioned blockchain to form a consortium that acts as an independent organization. The consortium has a charter — a set of rules including how the blockchain will be used and appoints an administrator to implement and enforce those rules.

So, transparency issues have to be addressed.

Because it's a private group, potentially affecting one or more industries, regulators may need access to the data in order to monitor or audit it. Look into a permissioned blockchain if performance, privacy, and fast transactions are important to you. For example, at Chronicled, we bring companies together and set up permissioned blockchains to create smart supply chains. Right now, we're working with pharmaceutical companies to create a blockchain solution around compliance. Together, this small group is collaborating to meet regulations—without having to worry about releasing sensitive data. But if you want the general population to be investors or users in your business, then a public blockchain likely makes more sense for you. If you're ready to create a small group that works together towards a solution, choose a permissioned blockchain. Either way, you're leveraging the blockchain network to drive your project forward.

Ordinarily, you would go to a lawyer or a notary, pay them, and wait while you get the document. With smart contracts, you simply drop a bitcoin into the vending machine (i.e. ledger), and your escrow, driver's license, or whatever drops into your account. More so, smart contracts not only define the rules and penalties around an agreement in the same way that a traditional contract does, but also automatically enforce those obligations. If you are looking for a more detailed walkthrough of smart contracts please check out our blockchain courses on smart contracts.

As Vitalik Buterin, the 22-year-old programmer of Ethereum, explained it at a recent DC Blockchain Summit, in a smart contract approach, an asset or currency is transferred into a program "and the program runs this code and at some point it automatically validates a condition and it automatically determines whether the asset should go to one person or back to the other person, or whether it should be immediately refunded to the person who sent it or some combination thereof."In the meantime, the decentralized ledger also stores and replicates the document which gives it a certain security and immutability.

Result:

Suppose you rent an apartment from me. You can do this through the blockchain by paying in cryptocurrency. You get a receipt which is held in our virtual contract; I give you the digital entry key which comes to you by a specified date. If the key doesn't come on time, the blockchain releases a refund. If I send the key before the rental date, the function holds it releasing both the fee and key to you and me respectively when the date arrives. The system works on the If-Then premise and is witnessed by hundreds of people, so you can expect a faultless delivery. If I give you the key, I'm sure to be paid. If you send a certain amount in bitcoins, you receive the key. The document is automatically canceled after the time, and the code cannot be interfered with either of us without the other knowing since all participants are simultaneously alerted.

You can use smart contracts for all sorts of situations that range from financial derivatives to insurance premiums, breach contracts, property law, credit enforcement, financial services, legal processes, and crowdfunding agreements.

Formed in 2015, Agora is a Swiss-based voting technology company that has developed an end-to-end verifiable voting solution for governments and institutions. Today's voting systems are slow, costly and exposed to many vulnerabilities that can inhibit free and fair elections. Our team of skilled cryptographers and security scientists has built a blockchain-based solution to provide our partners with a modern, provably secure and cost-effective manner of engaging voters. Elections on Agora's network are tamper-proof throughout the entire voting process and offer full transparency to voters, third-party auditors and the general public.

Their team is passionate about spreading fair and transparent elections around the world, and we believe Agora has the potential to offer great value for global human rights. Agora was born from the combined work of Bryan Ford, who served as the Director of the Swiss Federal Institute of Technology Lausanne's (EPFL) Decentralized and Distributed System Lab (DEDIS) alongside his team of engineers and researchers, and Leonardo Gammar, an accomplished entrepreneur passionate about blockchain, who grew up in diplomatic circles.

Their team of cryptographers has already implemented several large-scale blockchain projects and has many years of experience in providing digital solutions for electoral systems. Of particular relevance, our team previously developed several centralized e-voting frameworks for Swiss Post and the State of Geneva before beginning work on Agora.

Agora stands out as the first blockchain voting solution that is architected to meet the performance needs of a mission critical election. Our technology runs on a custom blockchain that our team has been developing since2015.

In this whitepaper, they presented three technological innovations developed by their team: Skipchain, Cotena and Valeda. Skipchain provides a consensus mechanism with high throughput and efficient transaction validation. Cotena then provides a method for storing cryptographic Skipchain proofs onto the Bitcoin blockchain. Finally, Valeda performs cryptographic proofs validating Skipchain and Cotena data. Our architecture provides end-to-end verifiability with a high level of security.

At the core, their company and technology strive to meet the evolving needs of modern voters. Not only do voters demand greater transparency in their elections, but they also demand more convenient methods of participating. Over the long run, they seek to enable any authorized voter to participate in an election through their own digital device, all while guaranteeing the security and transparency of the electoral procedure.

During the 2013 Local Election, researchers observed and studied the i-voting process and highlighted a number of potential security risks with the system. One such risk is the possibility of malware on the client side machine that monitors the user placing their vote and then later changing their vote to a different candidate. Another possible risk is for an attacker to directly infect the servers though malware being placed on the DVDs used to set up the servers and transfer the votes. (Springall et al., 2014) However, this report has also come under criticism from the Estonian Information Systems Authority.

(Veldre, 2014)

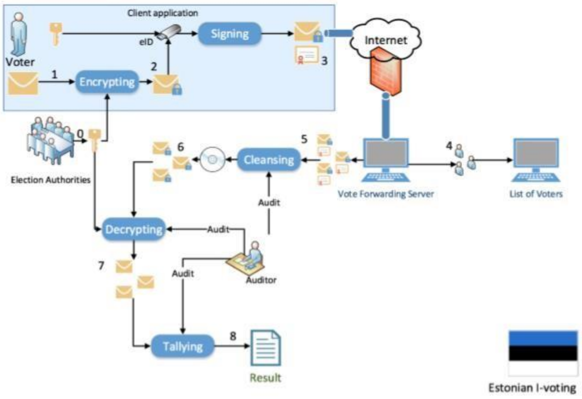

FIG:1 ESTONIAN DIGITAL VOTING SYSTEM (SOURCE: R. VERBIJ. "DUTCH E-VOTING OPPORTUNITIES." MASTER THESIS, UNIVERSITY OF TWENTE, 2014)

Their Proposal

For their design they tried to create a system that doesn't entirely replace the current voting but rather integrates within a current system. Tey decided to do this to allow for as many different ways to vote as possible, this is so voting can be accessed by the majority of the population.

Registration

The first aspect of their design is the registration process, verifying a voter is essential in establishing security within the system. Making sure that someone's identity isn't being misused for fraudulent purposes is important, especially when voting is considered, where every vote matters. To allow users to register to vote our proposed service utilizes both postal based forms as well as web forms requiring the same information to ensure we cater for those without a direct internet connection. This information includes their national identity number (an example would be a UK citizen's national insurance number), postal address, optional email address and a password. All of this information then forms a transaction for the user agreeing with the government that they are asking to vote; this transaction is then created on the voter blockchain which is distinctly different from the vote blockchain.

Once someone has registered an automated government miner analyses the transaction and if they haven't been awarded or denied a vote the miner will make the decision as to whether to verify the user or not. If the user is verified, they will be sent a ballot card with their information on it to both their home address and email address if provided. They will also be sent a randomly generated password to use on the polling stations. Once this correspondence has been sent, the miner will create a transaction giving the user a vote from an infinitegovernment pool of votes on the voter blockchain.

III. PROPOSED METHODOLOGY

The project is to implement the electronic voting system using finger print image authentication. In this, fingerprint will be used for substantiation and to monitor the presence of a person. There will be a central data repository with all finger print scan where mapping will be made for verification to vote for the particular ID number. Traditional voting systems should be computerized to reduce the vote counting time, to provide evidence that a vote is being correctly accounted, to reduce fraud, remove errors in filling out ballots, to improve system usability for people with special needs. E-voting increasingly replacing traditional paper based systems.

This raises several security issues, given that democratic principles depend on the electoral process's integrity. An electronic voting system must ensure the voter's authenticity, anonymity. It must also ensure audit ability in a software or hardware environment that could malfunction. In this System the fingerprints of all voters and details are stored before the election. The voters have to register their fingerprints on the day of election through online; this will be compared with the already stored prints.If both matches their votes will be taken in to the account and if not their vote will be discarded. So No one can vote for others this will reduce the illegal votes. User can view all the nominees in their district with their corresponding party symbols. They can also view how many votes are registered before they are going to register their votes, this may be useful to know the leading result. **Blockchain as a service** The blockchain is an append-only data structure, where data is stored in a distributed ledger that cannot be tampered with or deleted. This makes the ledger immutable. The blocks are chained in such a way that each block has a hash that is a function of the previous block, and thus by induction the complete prior chain, thereby providing assurance of immutability. There are two different types of blockchains, with different levels of restrictions based on who can read and write blocks.

A public blockchain is readable and writeable for everyone in the world. This type is popular for cryptocurrencies. A private blockchain sets restrictions on who can read or interact with the blockchain. Private blockchains are also known as being permissioned, where access can be granted to specific nodes that may interact with the blockchain.

In addition to cryptocurrency, blockchain provides a platform for building distributed and immutable applications or smart contracts. Smart contracts are programmable contracts that automatically execute when pre-defined conditions are met. Similar to conventional written contracts, smart contracts are used as a legally binding agreement between parties.

Smart contracts automate transactions and allow parties to reach agreements directly and automatically, without the need for a middleman. Key benefits of smart contracts compared to conventional written contracts are cost saving, enhanced efficiency and risk reduction. Smart contracts redefine trust, as contracts are visible to all the users of the blockchain and can, therefore, be easily verified.

IV. CONCLUSION

The new system eliminates the difficulties in the existing system. It is developed in a user-friendly manner. The system is very fast and any transaction can be viewed or retaken at any level. Error messages are given at each level of input of individual stages. This software is very particular in reducing the work and achieving the accuracy. It will reduce time be avoids redundancy of data. The user can easily understand the details available from the report. This software will support for the future development.

The software is menu driven. Simplicity is the hallmark of this project.Very large date can be stored and also can be retrieved very easily.

- Speed and accuracy is maintained in the votes withfinger prints.
- Data is entered in formatted manner.
- The report can be taken in any format.
- Modification and maintenance can be made very easily

SCOPE FOR FUTURE DEVELOPMENT

The system is very flexible and user-friendly, so the maintenance based on the changing environment and requirements can be incorporated easily. Any changes that are likely to cause failures are prevented with security and preventive measures could be taken. The coding is done in understandable and flexible method program which helps easy changing.
Since MS-SQL Server and ASP.NET are very flexible tools. User can easily incorporate any modular program in the application.

- It facilitates the user to easily vote by uploading thefinger print once.
- Facilities fast data backup and restoration facility incase of data loss situations.
- If the modules are written as web services, then it canbe used other web sites also.

V. REFERENCES

[1] Ajit Kulkarni, (2018), "How To Choose Between Public And Permissioned Blockchain For Your Project", Chronicled, 2018.

[2] "What Are Smart Contracts? A Beginner's Guide to Smart Contracts", Blockgeeks, 2016. Available at: https://blockgeeks.com/guides/ smart-contracts/

[3] Agora (2017). Agora: Bringing our voting systems into the21stcentury Available at: https://agora.vote/Agora_Whitepaper_v0.1.pdf

[4] Patrick McCorry, Siamak F. Shahandashti and Feng Hao. (2017). A Smart Contract for Boardroom Voting with Maximum Voter Privacy Available at: https://eprint.iacr.org/2017/110.pdf.

[5] Team plymouth pioneers – plymouth university. andrew barnes, christopher brake and thomas perry. Digital voting with the use of blockchain technology.

[6] K. Croman, C. Decker, I. Eyal, A. E. Gencer, A. Juels, A. Kosba, A. Miller, P. Saxena, E. Shi, and E. Gu¨n. On scaling decentralized blockchains. In Proc. 3rd Workshop on Bitcoin and Blockchain Research, 2016.

[7] G. Danezis and S. Meiklejohn. Centrally banked cryptocurrencies. In 23nd Annual Network and Distributed System Security Symposium, NDSS 2016, 2016.

[8] S. Nakamoto. Bitcoin: A Peer-to-Peer Electronic Cash System. November 2008. https://bitcoin.org/bitcoin.pdf, Accessedon 2015-01-01.

[9] R. Horrocks. Error while compiling: Stack too deep.Ethereum Stack Exchange, June 2015. http://ethereum.stackexchange.com/a/6065.

[10] Ethereum. The mix ethereum dapp development tool. GitHub, 2016. https://github.com/ethereum/mix, Accessed on 10/10/2016.

[11] S. Higgins. IBM Invests $200 Million in Blockchain- Powered IoT. CoinDesk, Oct. 2016. http://www.coindesk.com/ibm-blockchain-iot-office/.

[12] J. Clark and A. Essex. CommitCoin: Carbon Dating Commitments with Bitcoin. In Financial Cryptography and Data Security, pages 390–398. Springer, 2012

[13] A. Ekblaw, A. Azaria, J. D. Halamka, and A. Lippman. A case study for blockchain in healthcare: medrec prototype for electronic health records and medical research data. 2016. http://dci.mit.edu/assets/papers/eckblaw.pdf, Accessed on 26/10/2016.

[14] B. Adida. Helios: Web-based open-audit voting. In USENIX Security Symposium, volume 17, pages 335–348, 2008.

[15] S. Higgins. Abu Dhabi Stock Exchange LaunchesBlockchain Voting . CoinDesk, Oct. 2016.http://www.coindesk.com/abu-dhabi-exchange-blockchain- voting/.

[16] P. Boucher. What if blockchain technology revolutionised voting? Scientific Foresight Unit (STOA), European Parliamentary Research Service, Sept. 2016. http://www.europarl.europa.eu/RegData/etudes/ATAG/2016/5819 18/EPRS ATA(2016)581918 EN.pdf.

[17] A. Hertig. The First Bitcoin Voting Machine Is On ItsWay. Motherboard Vice, Nov. 2015. http://motherboard.vice.com/read/the-first-bitcoin-voting- machine-ison-its-way.

[18] P. Aradhya. Distributed Ledger Visible To All? Readyfor Blockchain? Huffington Post, Apr. 2016.

[19] B. Wire. Now You Can Vote Online with a Selfie.Business Wire, Oct. 2016. http://www.businesswire.com/news/home/20161017005354/en/V oteOnline-Selfie.