

E-Voting System based on Blockchain Technology

Submitted in partial fulfilment of the requirements for the award of degree of

BACHELOR OF ENGINEERING IN COMPUTER SCIENCE &ENGINEERING



**CHANDIGARH
UNIVERSITY**
Discover. Learn. Empower.

**Submitted to:
ER. Anup lal yadav**

**Submitted by:
KUMAR AAKARSHAN**

(18BCS6640)

Mentor Signature (name and ecode)

**DEPARTMENT OF COMPUTER SCIENCE & ENGINEERING
Chandigarh University, Gharuan**

CERTIFICATE

This is to certify that the work embodied in this Project Report entitled “ **E Voting System based on Blockchain Technology**” being submitted by “ **KUMAR AAKARSHAN**” - UID “ **18BCS6640**”, 8th Semester for partial fulfillment of the requirement for the degree of “ **Bachelor of Engineering in Computer Science & Engineering** ” discipline in “ **Chandigarh University** ” during the academic session Jan-june 2022 is a record of bonafide piece of work, carried out by student under my supervision and guidance in the “ **Department of Computer Science & Engineering**”, Chandigarh University.

DECLARATION

I, KUMAR AAKARSHAN student of **Bachelor of Engineering in Computer Science & Engineering, 8th Semester , session: Jan – june 2022, Chandigarh University**, hereby declare that the work presented in this Project Report entitled “ **E-Voting System based on Blockchain Technology**” is the outcome of my own work, is bona fide and correct to the best of my knowledge and this work has been carried out taking care of Engineering Ethics. The work presented does not infringe any patented work and has not been submitted to any other university or anywhere else for the award of any degree or any professional diploma.

Student details and Signature

NAME: KUMAR AAKARSHAN

UID:18BCS6640

BONAFIDE CERTIFICATE

Certified that this project report “E-voting system using blockchain .” is the bonafide work of “ KUMAR AAKARSHAN” who carried out the project work under my/our supervision.

Signature of HOD

Signature of Supervisor

Bachelor of Engineering, Computer Science and Engineering Submitted for the project viva-voce examination held on

INTERNAL EXAMINER

EXTERNAL EXAMINER

To our parents, teachers and all the well wishers out there . . .

Abstract

Online voting is a trend that is gaining momentum in modern society. It has great potential to decrease organisational costs and increase voter turnout. It eliminates the need to print ballot papers or open polling stations—voters can vote from wherever there is an Internet connection. Despite these benefits, online voting solutions are viewed with a great deal of caution because they introduce new threats. A single vulnerability can lead to large-scale manipulations of votes. Electronic voting systems must be legitimate, accurate, safe, and convenient when used for elections. Nonetheless, adoption may be limited by potential problems associated with electronic voting systems. Blockchain technology came into the ground to overcome these issues and offers decentralized nodes for electronic voting and is used to produce electronic voting systems mainly because of their end-to-end verification advantages. This technology is a beautiful replacement for traditional electronic voting solutions with distributed, non-repudiation, and security protection characteristics. The following article gives an overview of electronic voting systems based on blockchain technology. The main goal of this analysis was to examine the current status of blockchain-based voting research and online voting systems and any related difficulties to predict future developments. This study provides a conceptual description of the intended blockchain-based electronic voting application and an introduction to the fundamental structure and characteristics of the blockchain in connection to electronic voting. As a consequence of this study, it was discovered that blockchain systems may help solve some of the issues that now plague election systems. On the other hand, the most often mentioned issues in blockchain applications are privacy protection and transaction speed. For a sustainable blockchain-based electronic voting system, the security of remote participation must be viable, and for scalability, transaction speed must be addressed.

ACKNOWLEDGEMENT

I wish to express my sincere gratitude to Er. Anup lal yadav, Assistant Professor, Chandigarh University for providing me an opportunity to work on the project at “E-voting system using blockchain”.

I sincerely thank Er. Anup lal Yadav for the guidance and encouragement in carrying out this project work. I also wish to express my gratitude to the officials and other staff members of Chandigarh University who rendered their help during the period of my project work.

I also thank Dr.Reema Goyal, HOD of Final year students BE – CSE Chandigarh University for providing me the opportunity to embark on this project.

Date: 18-05-2022

Name: kumar aakarshan

Voting System based on Blockchain Technology

Table of Contents

Table of Contents	6
Introduction	11
1.1 Overview	25
1.2 Main Objective	26
1.3 Specific Objective	27
Fundamentals of Blockchain Voting:	27
Verifying Voter Identity	29
Maintaining Anonymity & the Secret Ballot	29
1. Increased Transparency in the Voting Process	31
2. Reduced Fraud & Election Rigging	32
3. Everyday Voting in Real Time	33
4. Corporate Governance & Autonomous Organizations	34
5. Increased Voter Engagement	36
1.4 Scope	36
1. Encryption	36
2. Authentication and permission	39
Security protection	39
Permission	39
1.5 Company	41
System Analysis	43
1.1 The Existing System	43
Types of Electronic Voting	43
Remote Voting System	44
Internet Voting (i-Voting)	44
SMS (Short Message Service) Voting	44
Direct Recording System	44
1.2 Vulnerabilities with the existing system	50
1.3 Blockchain-Based Voting	54
A. Evaluating Blockchain as a Service for E-Voting	65
B. Security analysis	67
C. Legal issues	68

Project Summary	75
v.1 Summary	75
v.2 Futures Works	76
v.3 References	78

Introduction

In every democracy, the security of an election is a matter of national security. The computer security field has for a decade studied the possibilities of electronic voting systems, with the goal of minimizing the cost of having a national election, while fulfilling and increasing the security conditions of an election. From the dawn of democratically electing candidates, the voting system has been based on pen and paper. Replacing the traditional pen and paper scheme with a new election system is critical to limit fraud and having the voting process traceable and verifiable.

Electronic voting machines have been viewed as flawed, by the security community, primarily based on physical security concerns. Anyone with physical access to such a machine can sabotage the machine, thereby affecting all votes cast on the aforementioned machine.

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

A worthy e-voting system must perform most of these tasks while complying with a set of standards established by regulatory bodies, and must also be capable to deal successfully with strong requirements associated with security, accuracy, integrity, swiftness, privacy, auditability, accessibility, cost-effectiveness, scalability and ecological sustainability.

Electronic voting technology can include punched cards, optical scan voting systems and specialized voting kiosks (including self-contained direct-recording electronic voting systems, or DRE). It can also involve transmission of ballots and votes via telephones, private computer networks, or the Internet.

In general, two main types of e-voting can be identified:

- e-voting which is physically supervised by representatives of governmental or independent electoral authorities (e.g. electronic voting machines located at polling stations);
- remote e-voting via the Internet (also called i-voting) where the voter submits their votes electronically to the election authorities, from any location.

Elections are fundamental pillar of a democratic system enabling the general public to express their views in the form of a vote. Due to their significance to our society, the election process should be transparent and reliable so as to ensure participants of its credibility. Within this context, the approach to voting has been an ever evolving domain. This evolution is primarily driven by the efforts to make the system secure, verifiable and transparent. In view of its significance, continuous efforts have been made to improve overall efficiency and resilience of the voting system. Electronic voting or e-voting has a profound role in this. Since its first use as punched-card ballots in 1960's, e-voting systems have achieved remarkable progress with its adaption using the internet technologies (Gobel et al, 2015). However, evoting systems must adhere to specific benchmark parameters so as to facilitate its widespread adoption. These parameters include anonymity of the voter, integrity of the vote and non-repudiation among others. Blockchain is one of the emerging technologies with strong cryptographic foundations enabling applications to leverage these abilities to achieve resilient security solutions. A Blockchain resembles a data structure which maintains and shares all the transactions being executed through its genesis. It is primarily a distributed decentralized database that maintains a complete list of constantly germinating and growing data records secured from unauthorized manipulating, tampering and revision. Blockchain allows every user to connect to the network, send new transactions to it, verify transactions and create new blocks (Rosenfeld, 2017; Kadam et al, 2015; Nakamoto, 2009). Each block is assigned a cryptographic hash (which may also be treated as a finger print of the block) that remains valid as long as the data in the block is not altered. If any changes are made in the block, the cryptographic hash would change immediately indicating the change in the data which may be due to a malicious activity. Therefore, due to its strong foundations in cryptography, blockchain has been increasingly used to mitigate against unauthorized transactions across various domains (Nakamoto, 2009; Kraft, 2015; Narayanan et al, 2015). Bitcoin remains the most distinguished application of blockchain however researchers are keen to explore the use of blockchain technology

to facilitate applications across different domains leveraging benefits such as non-repudiation, integrity and anonymity. In this paper, we explore the use of blockchain to facilitate e-voting applications with the ability to assure voter anonymity, vote integrity and end-to-verification. We believe e-voting can leverage from fundamental blockchain features such as selfcryptographic validation structure among transactions (through hashes) and public availability of distributed ledger of records. The blockchain technology can play key role in the domain of electronic voting due to inherent nature of preserving anonymity, maintaining decentralized and publicly distributed ledger of transactions across all the nodes. This makes blockchain technology very efficient to deal with the threat of utilizing a voting token more than once and the attempt to influence the transparency of the result.

IMPORTANCE OF VOTING

The power to vote for your country is an important part of a democratic country like India. While many in our country are eligible to cast vote, few are enthusiastic about it. In the 2019 Lok Sabha elections, the voter turnout was 67.11% which is the highest turnout in the history of India. With every election, there has been a positive increase in voter turnout. Such an increase in voting is a positive welcome, as each and every vote counts for a better future of our country.

Reasons to vote

It's our right: India's democratic underpinnings are based on election results. Our legislatures and parliaments are elected by, for, and for the people. We are fortunate to have the constitutional right to vote. We take it for granted, but the constitution guarantees us the right to vote for whom we want and to change our minds. Agent of change: Your vote has the potential to make a significant difference. You can vote for a better government if you are dissatisfied with the current one. If people do not vote, the same party will be in power for another five years. Finally, if the country is left with a bad administration, it is the people's fault for voting incorrectly or not at all. Your vote counts: Every vote counts. Though it seems like an endless sea of people are there to vote, every vote counts. When the national attitude changes from thinking "my vote doesn't make a difference", then the numbers increase and a multitude of people voting will make the difference. The responsibility lies on every individual.

NOTA: The Indian government has made it possible for voters to cast their ballots even if they are unsatisfied with any of the candidates. NOTA stands for None of the Above, and it's a crucial vote for individuals who aren't satisfied with any of the candidates. NOTA voting means that none of the candidates are suitable. NOTA votes

are counted, but if the majority of the votes are NOTA, the party with the next largest majority will be elected.

Process of Elections

The Election Commission of India was established to oversee the election process and guarantee that it ran smoothly. The Election Commission is in charge of everything relating to elections, including election supervision, control, and direction, as well as election conduct. The following is an overview of the voting process that you should be aware of. You first need to be registered on the Electoral Roll which is a list of eligible voters. You can apply voter id online as well as at the VRECs, at designated locations or through a Booth Level Officer.

You will be issued a Voter ID which you need to present at the polling booth.

The responsibility lies on the citizen to be aware of who is standing for

Elections.

It is also the responsibility of the citizen to find out where the polling booth is in their respective constituency.

You can vote on the Electronic Voting Machines.

If you speak only English, you should familiarise yourself with the symbols of the candidates, because the names of the candidates will be listed in alphabetical order in the respective state's language.

All you have to do is press the blue button next to your desired candidate's name and symbol. You can also vote NOTA.

You will receive a mark of ink on your finger that signifies that you voted.

While it helps identify if you have already voted, it is also a proud symbol you can bear.

Disadvantages of Electronic Voting

Despite the particular advantages to electronic voting system, there are also drawbacks to the system. The cons of the electronic voting system should be considered seriously by all concerned before taking any kind of random decision on e-voting. These are:

1) Vulnerability to hacking: According to the Congressional Research Service of Election Reform and Electronic Voting Systems, vendors and Election jurisdictions generally state that they do not transmit election results from precincts via the internet, but they may transmit them via a direct modem connection or Virtual Private Network (VPN). However, even this approach may be subject to attack via the internet, especially if encryption and verification are not sufficient. That is because telephone transmission systems are themselves increasingly connected to

the internet and computers to which the receiving server may be connected, such as through a local area network (LAN), may have internet connections. So, using internet would be out of the question in case of Bangladesh where we continuously have history of suspicion over electoral fraud.

2) Voter verified paper audit trails: All fully-electronic (touch screen, DRE, internet) voting systems are subject to the limitations and risks of computer technology. This includes the inability to detect the presence of hardware and/or software that could be used, deliberately or inadvertently, to alter election outcomes. According to Rebecca Mercuri, PhD, president, Notable Software, democratic elections require independent verification that all balloting choices have been recorded as intended and vote totals have been reliably and indisputably created from the same material examined by the voters.

A Voter Verified Paper Ballot (VVPB) provides an auditable way to assure Voters that their ballots will be available to be counted. Without VVPB there is no way to independently audit the election results.

3) Susceptibility to fraud: Voting fraud is not either present everywhere or absent everywhere. Especially in our country, there have always been allegations of fraud by all the losing political parties. Fraud comes in Degrees and increments. A malicious voting system created and distributed by one vendor to hundreds of thousands of polling booths, can systematically falsify millions of votes. Although some may believe that tampering with an electronic voting machine is extremely hard to do, computer scientists have tampered with machines to prove that it is quite easily done. However, if people have access to the machines, and know how to work them, they can take the memory card out of the machine, which stores the votes, and in place they put their own memory Card with a virus that can tamper with the votes. It is a fraud on a large scale and wholesale level. Stuffing a ballot box, in contrast, works at a retail level. A tamperer, however malicious and skilled, can stuff only as many ballots as might plausibly be cast at the polling place, but a faulty and corrupted voting system (malicious DRE software) could affect far more votes.

4) Accuracy in capturing voters' intent: If a touch screen is used in the elections, the sensors in touch screen devices can be knocked out of

Alignment by shock and vibration that may occur during transport. Unless these sensors are realigned at the polling place prior to the start of voting, touch screen machines can misinterpret a voter's intent. For example, a voter might touch the part of the screen identified with candidate X, but candidate Y's would light up instead.

5) Political ties of manufacturers: The present government's decision not to keep the provision of caretaker government and to hold next general Election under a

political government and the election commission, has made the attempt of using e-voting system more unreasonable and unfair.

Our election commission itself were also subject to considerable amount of criticism because of its controversial comments and actions during the emergency period after January 11 takeover, and also during the last 2008 general elections. Considering our political culture, it is undeniably a fact that any manufacturer or company hired for the e-voting system will tailor the e-voting machines according to the 'needs' of the current political party in power. So these machines will be subject to scrutiny, distrust and inquiry from all the other political parties in the country.

6) Malicious software programming: Any computer software is basically generated from software programming and coding. And all these softwares could be tampered with by a computer programmer who knows the source code. Testing electronic voting systems for security problems, especially if they were intentionally introduced and concealed, is basically impossible. If Malicious coding is inserted by programmers into commercial software that are triggered by obscure combinations of commands and keystrokes via the computer keyboard, then election results can change completely.

7) Physical security of machines: Regarding physical hardware controls, many of the DRE (direct recording electronic voting machine) models under examination contained weaknesses in controls designed to protect the system.

According to the USA Government Accountability office, all the locks on a particular DRE model were easily picked, and were all controlled by the Same keys. Also a particular model of DRE was linked together with others to form a rudimentary network. If one of these machines were accidentally or intentionally unplugged from the others, voting functions on the other machines in the network would be disrupted. In addition, reviewers found that switches used to turn a DRE system on or off, as well as those used to close the polls on a particular DRE terminal, were not protected.

8) Secure storage of cast votes: The votes that are cast using the electronic voting machines, are stored in a safe storage or space in the computer machine memory. But, Doug Jones, PhD, Professor of Computer Science at University of Iowa explained in his book, Secure Electronic Voting, 'For over a decade, all direct recording electronic machines have been required to contain redundant storage, but this redundant storage is not an independent record of the votes, because it is created by the same software that created the original record. As a result, the multiple files are of limited use to check the correctness of the software.'

What Is a Blockchain?

A blockchain is a distributed database that is shared among the nodes of a computer network. As a database, a blockchain stores information electronically in digital

format. Blockchains are best known for their crucial role in cryptocurrency systems, such as Bitcoin, for maintaining a secure and decentralized record of transactions. The innovation with a blockchain is that it guarantees the fidelity and security of a record of data and generates trust without the need for a trusted third party.

One key difference between a typical database and a blockchain is how the data is structured. A blockchain collects information together in groups, known as blocks, that hold sets of information. Blocks have certain storage capacities and, when filled, are closed and linked to the previously filled block, forming a chain of data known as the blockchain. All new information that follows that freshly added block is compiled into a newly formed block that will then also be added to the chain once filled.

A database usually structures its data into tables, whereas a blockchain, like its name implies, structures its data into chunks (blocks) that are strung together. This data structure inherently makes an irreversible timeline of data when implemented in a decentralized nature. When a block is filled, it is set in stone and becomes a part of this timeline. Each block in the chain is given an exact time stamp when it is added to the chain.

How Does a Blockchain Work?

The goal of blockchain is to allow digital information to be recorded and distributed, but not edited. In this way, a blockchain is the foundation for immutable ledgers, or records of transactions that cannot be altered, deleted, or destroyed. This is why blockchains are also known as a distributed ledger technology (DLT).

First proposed as a research project in 1991, the blockchain concept

predated its first widespread application in use: Bitcoin, in 2009. In the years since, the use of blockchains has exploded via the creation of various cryptocurrencies, decentralized finance (DeFi) applications, non-fungible tokens (NFTs), and smart contracts.

Blockchain Decentralization

Imagine that a company owns a server farm with 10,000 computers used to maintain a database holding all of its client's account information. This company owns a warehouse building that contains all of these computers under one roof and has full control of each of these computers and all of the information contained within them. This, however, provides a single point of failure. What happens if the electricity at that location goes out?

What if its Internet connection is severed? What if it burns to the ground? What if a bad actor erases everything with a single keystroke? In any case, the data is lost or corrupted.

What a blockchain does is to allow the data held in that database to be spread out among several network nodes at various locations. This not only creates redundancy but also maintains the fidelity of the data stored therein—if somebody tries to alter a record at one instance of the database, the other nodes would not be altered and thus would prevent a bad actor from doing so. If one user tampers with Bitcoin's record of transactions, all other nodes would cross-reference each other and easily pinpoint the node with the incorrect information. This system helps to establish an exact and transparent order of events. This way, no single node within the network can alter information held within it.

Because of this, the information and history (such as of transactions of a cryptocurrency) are irreversible. Such a record could be a list of transactions (such as with a cryptocurrency), but it also is possible for a blockchain to hold a variety of other information like legal contracts, state identifications, or a company's product inventory.

Transparency

Because of the decentralized nature of Bitcoin's blockchain, all transactions can be transparently viewed by either having a personal node or using blockchain explorers that allow anyone to see transactions occurring live. Each node has its own copy of the chain that gets updated as fresh blocks are confirmed and added. This means that if you wanted to, you could track Bitcoin wherever it goes.

For example, exchanges have been hacked in the past, where those who kept Bitcoin on the exchange lost everything. While the hacker may be entirely anonymous, the Bitcoins that they extracted are easily traceable. If the Bitcoins stolen in some of these hacks were to be moved or spent somewhere, it would be known.

Of course, the records stored in the Bitcoin blockchain (as well as most others) are encrypted. This means that only the owner of a record can decrypt it to reveal their identity (using a public-private key pair). As a result, users of blockchains can remain anonymous while preserving

Transparency

Is Blockchain Secure?

Blockchain technology achieves decentralized security and trust in several ways. To begin with, new blocks are always stored linearly and chronologically. That is, they are always added to the “end” of the blockchain. After a block has been added to the end of the blockchain, it is extremely difficult to go back and alter the contents of the block unless a majority of the network has reached a consensus to do so. That’s because each block contains its own hash, along with the hash of the block before it, as well as the previously mentioned time stamp. Hash codes are created by a mathematical function that turns digital information into a string of numbers and letters. If that information is edited in any way, then the hash code changes as well. Let’s say that a hacker, who also runs a node on a blockchain network, wants to alter a blockchain and steal cryptocurrency from everyone else. If they were to alter their own single copy, it would no longer align with everyone else’s copy. When everyone else cross-references their copies against each other, they would see this one copy stand out, and that hacker’s version of the chain would be cast away as illegitimate. Succeeding with such a hack would require that the hacker simultaneously control and alter 51% or more of the copies of the blockchain so that their new copy becomes the majority copy and, thus, the agreed-upon chain.

Such an attack would also require an immense amount of money and resources, as they would need to redo all of the blocks because they would now have different time stamps and hash codes.

Due to the size of many cryptocurrency networks and how fast they are growing, the cost to pull off such a feat probably would be insurmountable. This would be not only extremely expensive but also likely fruitless. Doing such a thing would not go unnoticed, as network members would see such drastic alterations to the blockchain. The network members would then hard fork off to a new version of the chain that has not been affected. This would cause the attacked version of the token to plummet in value, making the attack ultimately pointless, as the bad actor has control of a worthless asset. The same would occur if the bad actor were to attack the new fork of Bitcoin. It is built this way so that taking part in the network is far more economically incentivized than attacking it.

BLOCKCHAIN+VOTING = BLOCKCHAIN BASED VOTING SYSTEM





After 2000, voting machine problems made international headlines. The government appropriated money to fix the problems nationwide. Unfortunately, electronic voting machines although presented as the solution have largely made the problem worse. **This doesn't mean that these machines should be abandoned**, but they need to be designed to increase both their accuracy, and peoples' trust in their accuracy. **This is difficult, but not impossible.**

Before we can discuss electronic voting machines, we need to explain why voting is so difficult. Basically, a voting system has four required characteristics:

1. **Accuracy**. The goal of any voting system is to establish the intent of each individual voter, and translate those intents into a final tally. To the extent that a voting system fails to do this, it is undesirable. This characteristic also includes security: It should be impossible to change someone else's vote, ballot stuff, destroy votes, or otherwise affect the accuracy of the final tally.
2. **Anonymity**. Secret ballots are fundamental to democracy, and voting systems must be designed to facilitate voter anonymity.
3. **Scalability**. Voting systems need to be able to handle very large elections. One hundred million people vote for president in the United States. About 372 million people voted in India's June elections, and over 115 million in Brazil's October elections. The complexity of an election is another issue. Unlike many countries where the national election is a single vote for a person or a party, a United States voter is faced with dozens of individual elections: national, local, and everything in between.
4. **Speed**. Voting systems should produce results quickly. This is particularly important in the United States, where people expect to learn the results of the day's election before bedtime. It's less important in other countries, where people don't mind waiting days or even weeks before the winner is announced.

Through the centuries, different technologies have done their best. Stones and pot shards dropped in Greek vases gave way to paper ballots dropped in sealed boxes. Mechanical voting booths, punch cards, and then optical scan machines replaced hand-counted ballots. New computerized voting machines promise even more efficiency, and Internet voting even more convenience.

More Information:

Voting whether conducted through the traditional ballot or via electronic means forms the basis on which democracy depends. With the rise in technological impact on the youth of the country and the various anomalies faced by the current electoral process, using technology to modify the existing process is necessity of the hour. However for any new technique to take the place of current voting system, the said system needs to satisfy certain minimum criteria. Electronic Voting has taken center place in research with the intention of minimizing the cost associated in setting up the voting process, while ensuring the electoral integrity is maintained by fulfilling privacy, security and compliance requirements.

The current method, whether electronic or not has proved to be unsatisfactory with respect to transparency. It can be very difficult for the voters to be assured that the vote he/she has casted during the election reflects in the election result. Electronic voting using Direct Recording Electronic do not generate receipt on successful casting of votes. No record of election except vote count is made public by the government, which means that the voters are not assured of any external interference in case of government conducting the process of vote recounting[2]. Replacing the traditional method with electronic method using Blockchain technique has the ability to prevent potential frauds that may take place during election.

Blockchain technology is a distributed network of interconnected nodes. A copy of distributed ledger is assigned to each node, each of which contains a complete history of all the transactions that have been processed by the network. Each transaction processed generated a hash. The hash created depends not only on the current transaction but also on the hash of the previous transaction. Thus any small change on the data will impact the hash of the transaction. If a transaction is approved by a majority of nodes it is written to the block. This allows the users to remain autonomous while using the system. A basic analysis of Blockchain suggests that it provides the potential of making the voting process more secure and reliable.

A **blockchain**, originally **block chain**, is a growing list of records, called blocks, that are linked using cryptography. Each block contains a cryptographic hash of the previous block, a timestamp, and transaction data (generally represented as a Merkle tree).

By design, a blockchain is resistant to modification of the data. It is "an open, distributed ledger that can record transactions between two parties efficiently and in a verifiable and permanent way". For use as a distributed ledger, a blockchain is typically managed by a peer-to-peer network collectively adhering to a protocol for inter-node communication and validating new blocks. **Once recorded, the data in any given block cannot be altered retroactively without alteration of all subsequent blocks, which requires consensus of the network majority.** Although blockchain records are not unalterable, blockchains may be considered secure by design and exemplify a distributed computing system with high Byzantine fault tolerance. Decentralized consensus has therefore been claimed with a blockchain.

I.1 Main Objective

In this current paper we shall present how the blockchain technology can overcome, improve and make the e-voting system efficient than ever.

Since each country has different laws and implementations, proposing a definitive structure is almost impossible. The suggested solution in this paper is specifically for problems of conventional paper elections in Democratic Republic of Congo. Despite the solution is specific to one country, it may be taken as a general application, and can be customized to other countries. Security and privacy of votes and voters and the speed of counting votes and announcing the results are discussed in the solution.

There are some attempts to remove problems of traditional election system. These attempts try to benefit from online systems to automate the whole process. Electronic voting was used in elections of Austrian Federation of Students in 2009 and in some elections in Switzerland. Although e-voting makes selection operation easy, privacy and security worries still continue. To dissipate problems of both conventional and e-voting elections, e-voting can be improved using Blockchain mechanism. Blockchain has impressive features to overcome troubles

of voter's security, privacy and data integrity of votes.

Blockchain is an inalterable and an easy confirmable system. Under favor of these qualifications, Blockchain has a significant potential to be an alternative to traditional elections.

It brings smart solutions to central authority problem in terms of all blocks having all data in the chain. Also, it is impossible to change an information in a block since it is discerned by other blocks which have whole data. Consequently, Blockchain increases the security of information by keeping the entire data in all blocks, and removes the need for an official center to provide a secure election. As mentioned before, counting votes and making election results publicly available takes considerable time. Blockchain solves this problem by its nature. Since the last node on the chain keeps all information, it is enough to look for only the last node for the results. This reduces the waiting time dramatically. Thus, incomplete and official results are explained at the same time. The Blockchain will allow the government of the Democratic Republic of Congo to manage efficiently to voting system

I.2 Specific Objective

Fundamentals of Blockchain Voting:

Blockchain voting is similar to analogue voting that we're used to. The same concepts and processes apply. In order to cast a digital vote, a citizen would need to register and prove their citizenship in a given jurisdiction. We could then record that identity and citizenship on the blockchain associated with that user's key.

Next, a citizen needs a ballot to cast a vote. In the blockchain, this would likely take the form of a special voting token that would be deposited in the user's account. This token would also likely have a time limit in which it could be used to vote, after which it would burn itself via a smart contract or become useless.

Casting a vote on the blockchain would involve sending the voting token (the ballot) to a specific address. Voters would know which address aligns with which candidate or referendum. Sending a token to that address would represent a vote.

Technically, that sounds simple enough. The vote gets registered on the

blockchain where its immutable, verifiable, and transparent. We can easily count up the votes to declare a winner to the election. In addition, we can build nice user interfaces that automate and hide the process of sending a token to a specific address. Instead, voters would see a simple online interface for them to select a candidate or proposal and click submit.

Verifying Voter Identity:

If that first explanation sounded simple and you wonder why we're not voting on the blockchain already, just hold on. It's actually a lot more complicated than that. There are a lot of issues that need a resolution first.

One major issue is verifying voter identity. In order for blockchain voting to work, we need a system that prevents people from voting more than once or voting in an election where they're not a citizen. That gets tricky on the blockchain because it relies on a central authority to verify citizenship or residency documentation.

A blockchain solution would likely rely on submitting passport or driver's license scans. Then that identity might be connected with a mobile device via a password and two-factor authentication or biometrics (like a fingerprint). The idea is to verify that the person who submitted the citizenship documents is the same person who is actively at the computer or smartphone at the time of the vote.

Maintaining Anonymity & the Secret Ballot:

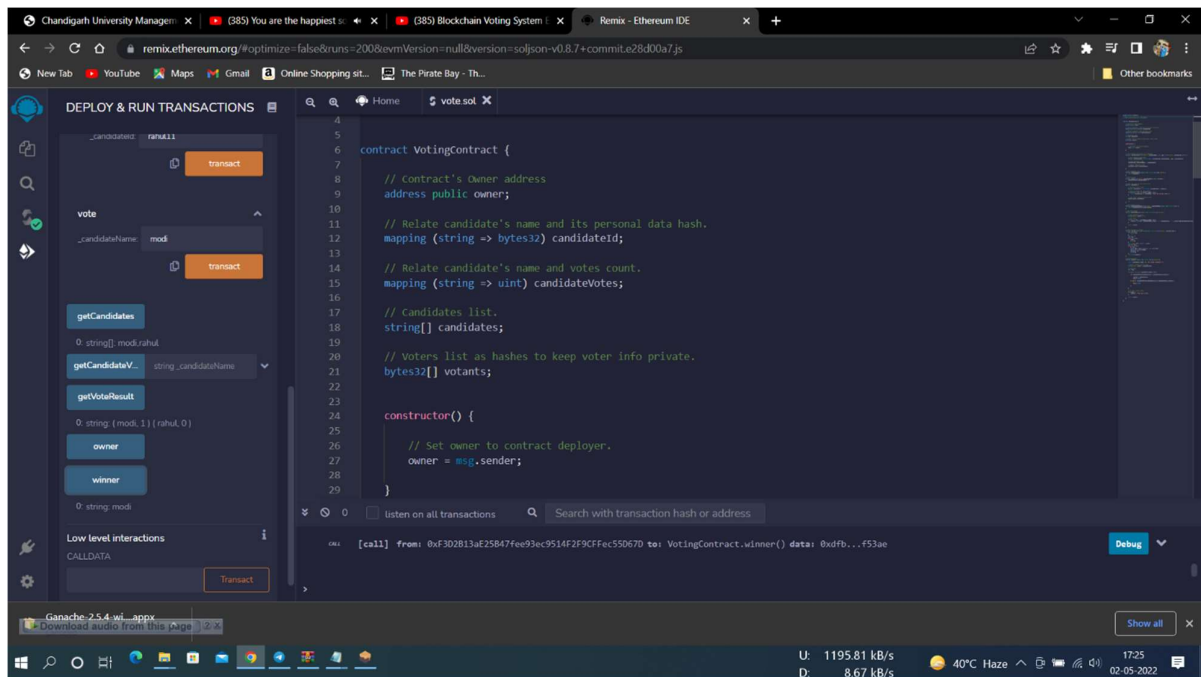
Once we've verified identity and eligibility to vote, however, we need to separate it from the ballot itself. Importantly, one of the key parts of democracy is the secret ballot. Nobody should know how you voted so they can't influence your vote in any way.

With blockchain voting, the information that registers on the blockchain shouldn't include identifiable information. This means that information about the sender of the voting token has to be hidden. There are different ways to accomplish this, including zero knowledge proofs, ring transactions, or various encryption methods. Each has its benefits, drawbacks, and technical challenges. True anonymity at the same time as verified identity is the big challenge of

blockchain voting.

Cybersecurity experts generally agree that blockchains are unhackable (with the right network size and consensus algorithm). Logic proofs and statistics indicate that it becomes increasingly unlikely that a block can be compromised once the network confirms it. However, the

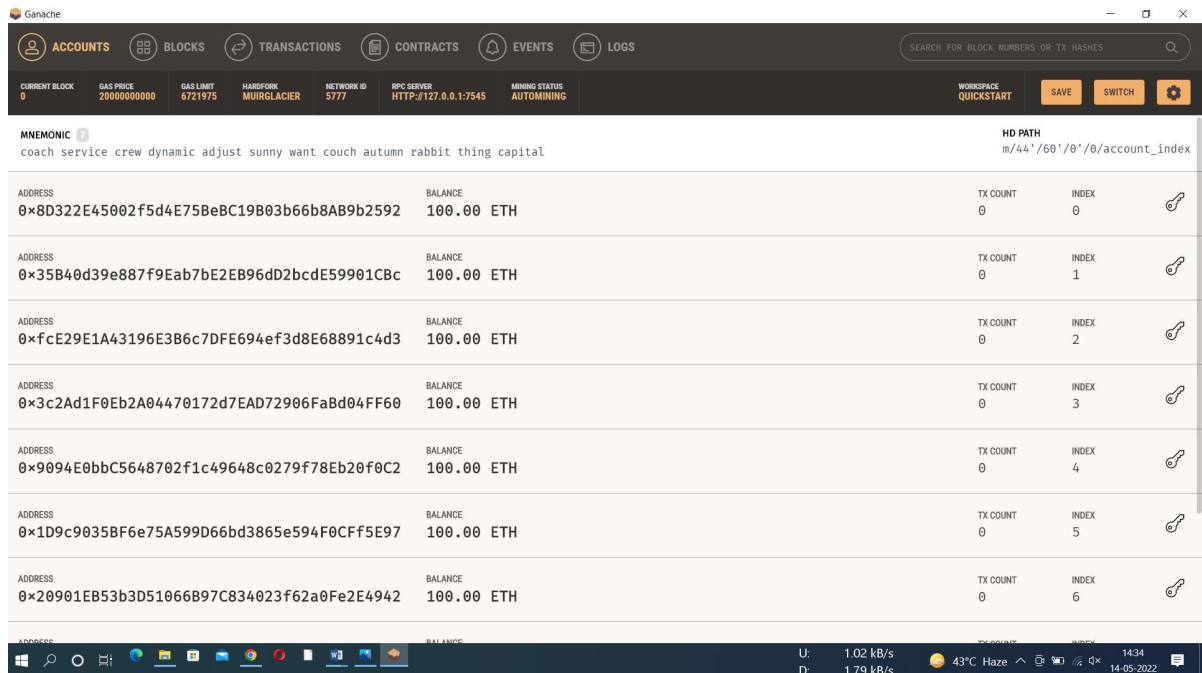
anonymity needed for voting is more difficult to secure and be certain that it won't be compromised.



1. Increased Transparency in the Voting Process

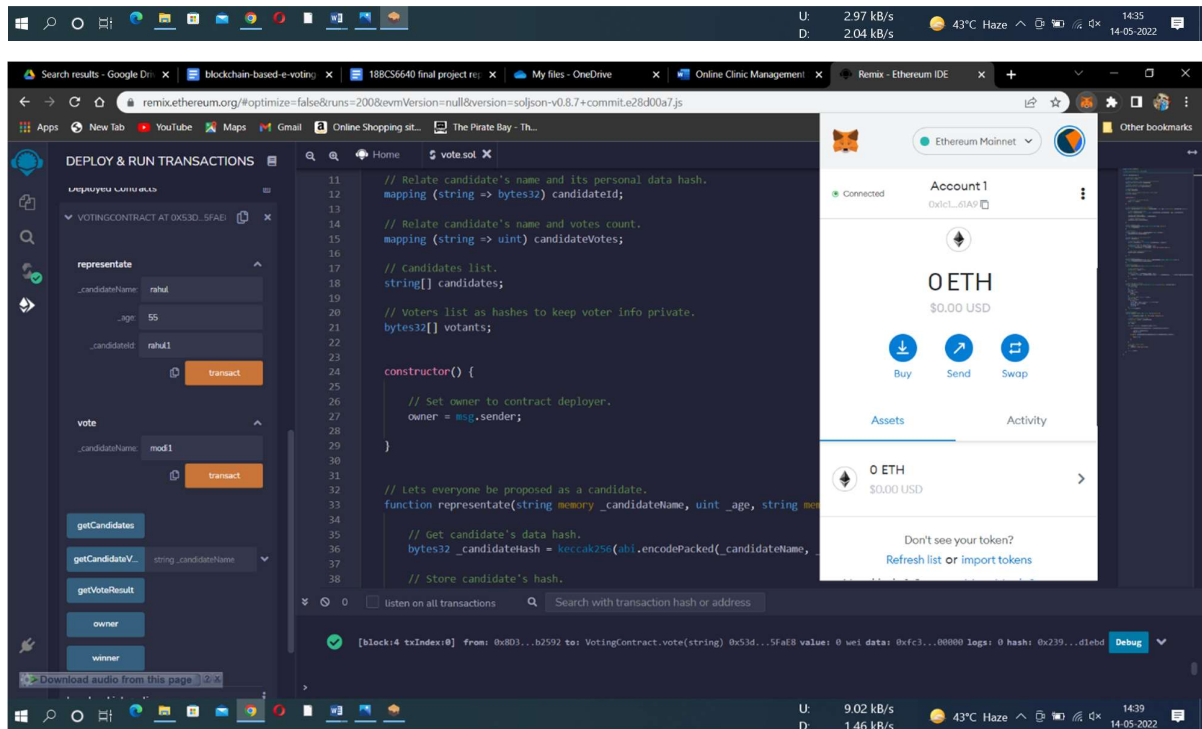
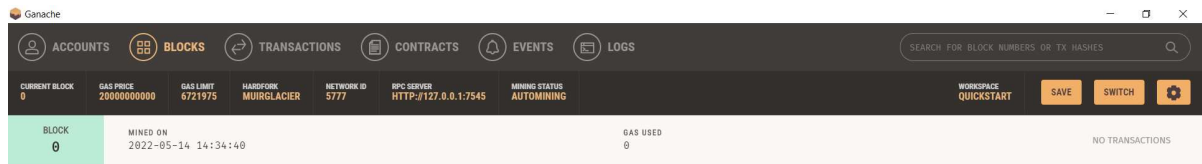
The biggest benefit of blockchain voting is increased transparency. Right now, once you cast your vote, you don't really know what happened to it. You trust the poll workers to count it correctly. However, there's no way to be sure that your vote counted.

On the blockchain it could be possible to track your vote and see that it ended up in the right place. Even though it wouldn't have your information tied to it, your vote would exist on the blockchain for all of history.



2. Reduced Fraud & Election Rigging

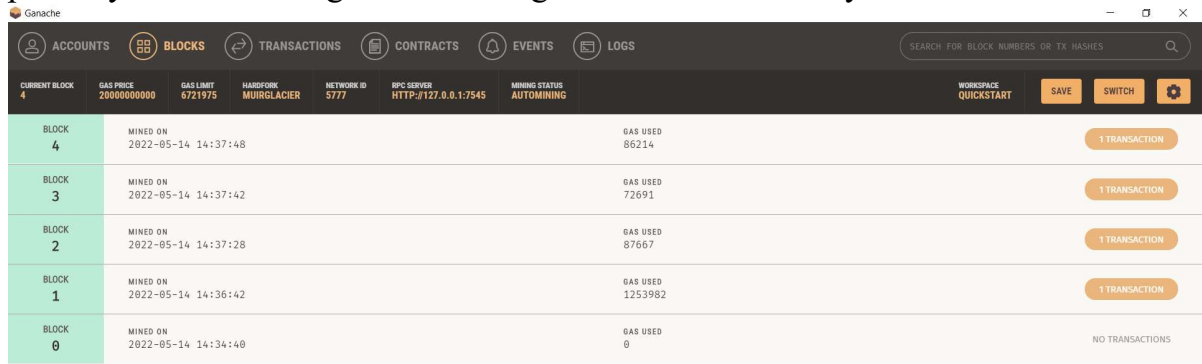
A side effect of increased transparency is reduced fraud. It becomes harder to cheat the system or vote in the wrong jurisdiction with blockchain identity verification. **Moreover, in countries where dictators rig elections, the blockchain could bring true democracy.** Of course, initiating a blockchain voting system requires buy-in from the current government. However, over time blockchain could become an international voting standard, with the world community advocating for blockchain governance in all nations.



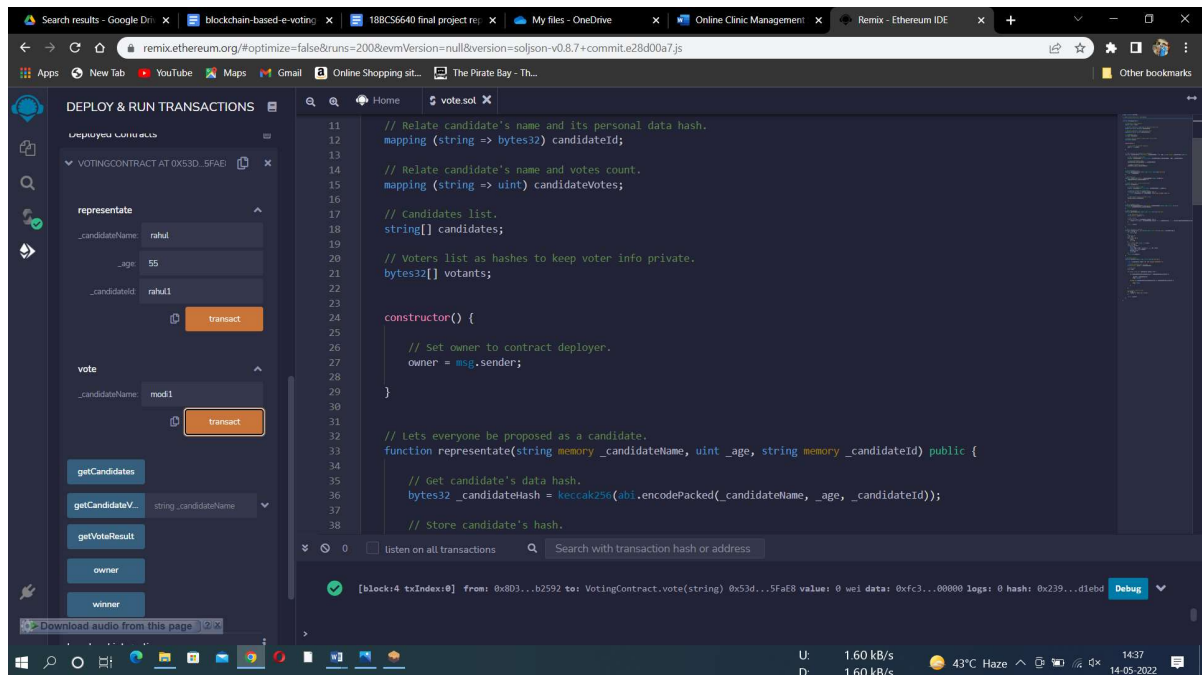
3. Everyday Voting in Real Time

If blockchain makes voting transparent, then we can follow and tally votes in real time. This means that elections can happen on a much shorter time span. Additionally, if they are digital, they require less investment in polling infrastructure. As a result, elections could be held with a short lead time to vote on a referendum quickly.

This could completely change daily life. Imagine if you could vote on your phone on how traffic in your city would be routed today or whether to increase taxes to pay for a new park in your community. Voting could become highly targeted, even neighborhood specific. There would be little overhead to voting more often, possibly making voting a daily occurrence.



ACCOUNTS	BLOCKS	TRANSACTIONS	CONTRACTS	EVENTS	LOGS
CURRENT BLOCK 4	GAS PRICE 2000000000	GAS LIMIT 0721975	HARDFORK MUIRGLACIER	NETWORK ID 5777	RPC SERVER HTTP://127.0.0.1:7545
					MINING STATUS AUTOMINING
					WORKSPACE QUICKSTART SAVE SWITCH
BLOCK 4	MINED ON 2022-05-14 14:37:48	GAS USED 86214	1 TRANSACTION		
BLOCK 3	MINED ON 2022-05-14 14:37:42	GAS USED 72691	1 TRANSACTION		
BLOCK 2	MINED ON 2022-05-14 14:37:28	GAS USED 87667	1 TRANSACTION		
BLOCK 1	MINED ON 2022-05-14 14:36:42	GAS USED 1253982	1 TRANSACTION		
BLOCK 0	MINED ON 2022-05-14 14:34:40	GAS USED 0	NO TRANSACTIONS		

The screenshot shows the Remix Ethereum IDE interface. On the left, there's a 'DEPLOY & RUN TRANSACTIONS' panel with a 'VOTING CONTRACT AT 0x53D...5FAD' deployed. It includes input fields for 'representate' (candidate name, age, candidate ID) and 'vote' (candidate name), along with buttons for 'transact', 'getCandidates', 'getCandidateV...', 'getVoteResult', 'owner', and 'winner'. The main editor displays a Solidity contract named 'vote.sol' with the following code:

```

11 // Relate candidate's name and its personal data hash.
12 mapping (string => bytes32) candidateId;
13
14 // Relate candidate's name and votes count.
15 mapping (string => uint) candidateVotes;
16
17 // Candidates list.
18 string[] candidates;
19
20 // Voters list as hashes to keep voter info private.
21 bytes32[] votants;
22
23
24 constructor() {
25
26     // Set owner to contract deployer.
27     owner = msg.sender;
28 }
29
30
31 // Lets everyone be proposed as a candidate.
32 function representate(string memory _candidateName, uint _age, string memory _candidateId) public {
33
34     // Get candidate's data hash.
35     bytes32 _candidateHash = keccak256(abi.encodePacked(_candidateName, _age, _candidateId));
36
37     // Store candidate's hash.
38

```

At the bottom, a console log shows a successful transaction: '[block:4 txIndex:0] from: 0x803...b2592 to: VotingContract.vote(string) 0x53d...5Fa8 value: 0 wei data: 0xfc3...00000 logs: 0 hash: 0x239...d1ebd'.

4. Corporate Governance & Autonomous Organizations

The Governments aren't the only institutions that could benefit from blockchain voting. Employees or shareholders could vote for initiatives within a company as well. It's possible to even imagine ownerless businesses where every decision is an open vote from shareholders.

5. Increased Voter Engagement

A big advantage of blockchain voting could be increased engagement. If blockchain makes digital voting possible from your smartphone or computer, voting becomes as easy as logging in and casting your ballot in just a few minutes. This would likely increase voter turnout drastically, leading to more direct democracy. Alternatively, it could lead to voting fatigue, where voters realize they liked electing representatives to worry about policy for them.

I.3 Scope

1. Encryption

When a block stores new data it is added to the blockchain. Blockchain, as its name suggests, consists of multiple blocks strung together. In order for a block to be added to the blockchain, however, four things must happen:

1. A transaction must occur. Let's take the example of an impulsive Amazon purchase. After hastily clicking through multiple checkout prompts, you go against your better judgment and make a purchase. In many cases a block will group together potentially thousands of transactions, so your Amazon purchase will be packaged in the block along with other users' transaction information as well.
2. That transaction must be verified. After making that purchase, your transaction must be verified. With other public records of information, like the Securities Exchange Commission, Wikipedia, or your local library, there's someone in charge of vetting new data entries. With blockchain, however, that job is left up to a network of computers. When you make your purchase from Amazon, that network of computers rushes to check that your transaction happened in the way you said it did. That is, they confirm the details of the purchase, including the transaction's time, dollar amount, and participants.
3. That transaction must be stored in a block. After your transaction has been

verified as accurate, it gets the green light. The transaction's dollar amount, your digital signature, and Amazon's digital signature are all stored in a block. There, the transaction will likely join hundreds, or thousands, of others like it.

4. That block must be given a hash. Not unlike an angel earning its wings, once all of a block's transactions have been verified, it must be given a unique, identifying code

Block	Mined On	Gas Used	Transactions
BLOCK 4	2022-05-14 14:37:48	86214	1 TRANSACTION
BLOCK 3	2022-05-14 14:37:42	72691	1 TRANSACTION
BLOCK 2	2022-05-14 14:37:28	87667	1 TRANSACTION
BLOCK 1	2022-05-14 14:36:42	1253982	1 TRANSACTION
BLOCK 0	2022-05-14 14:34:40	0	NO TRANSACTIONS

U: 0.55 kB/s
D: 0.79 kB/s
43°C Haze
14:38
14-05-2022

Search results - Google Dr... blockchain-based-e-voting x 18BCS6640 final project re... My files - OneDrive x Online Clinic Management x Remix - Ethereum IDE x

remix.ethereum.org/#optimize=false&runs=200&evmVersion=null&version=soljson-v0.8.7+commit.e28d00a7.js

Apps New Tab YouTube Maps Gmail Online Shopping sit... The Pirate Bay - Th...

DEPLOY & RUN TRANSACTIONS

UNDEPLOYED CONTRACTS

VOTINGCONTRACT AT 0x53D...5FAE

representate

_candidateName: rahul

_age: 55

_candidateId: rahul1

transact

vote

_candidateName: mod1

transact

getCandidates

getCandidateV...

string _candidateName

getVoteResult

owner

winner

```
11 // Relate candidate's name and its personal data hash.
12 mapping (string => bytes32) candidateId;
13
14 // Relate candidate's name and votes count.
15 mapping (string => uint) candidateVotes;
16
17 // Candidates list.
18 string[] candidates;
19
20 // Voters list as hashes to keep voter info private.
21 bytes32[] voters;
22
23
24 constructor() {
25
26     // Set owner to contract deployer.
27     owner = msg.sender;
28
29 }
30
31 // Lets everyone be proposed as a candidate.
32 function representate(string memory _candidateName, uint _age, string me
33
34 // Get candidate's data hash.
35 bytes32 _candidateHash = keccak256(abi.encodePacked(_candidateName,
36
37 // Store candidate's hash.
38
```

Account1

0x1c1...61A9

0 ETH

\$0.00 USD

Buy Send Swap

Assets Activity

0 ETH

\$0.00 USD

Don't see your token?

Refresh list or import tokens

[block:4 txIndex:0] from: 0xb03...b2592 to: VotingContract.vote(string) 0x53d...5fae value: 0 wei data: 0xfc1...00000 logs: 0 hash: 0x239...d1ebd Debug

U: 9.02 kB/s

D: 1.46 kB/s

43°C Haze

1439

14-05-2022

called a hash. The block is also given the hash of the most recent block added to the blockchain. Once hashed, the block can be added to the blockchain.

When that new block is added to the blockchain, it becomes publicly available for anyone to view even you. If you take a look at Bitcoin's blockchain, you will see that you have access to transaction data, along with information about when ("Time"), where ("Height"), and by who ("Relayed By") the block was added to the blockchain.

2. Authentication and permission

In order to prevent illegal devices accessing the e-Voting system, we use public key cryptography to authenticate the system entities. The biggest difference is that we introduce a peer-to-peer authentication methodology without third party based on blockchain.

Security protection

In the e-voting system, ensure the reliability of the voters' devices provides security protection. Even if a device has passed the authentication of other nodes, it still has the risk of being attacked by malicious users due to software or system vulnerabilities during the execution of the task. The intruder usually will modify the network entity to leave a backdoor in the device to prepare for subsequent infiltration and modify the key configuration file in the device and cause damage to the entire network. In order to discover potential intrusions quickly, we regularly verify that whether critical data have been tampered with.

Permission

1) Enrollment Control

We use a permission chain with access control rights ensured by the system administrator for the proposed system. A device needs to register in blockchain

before it accesses to the network. The access control layer in the permission chain ensures that only devices with legal identities can register information in the blockchain.

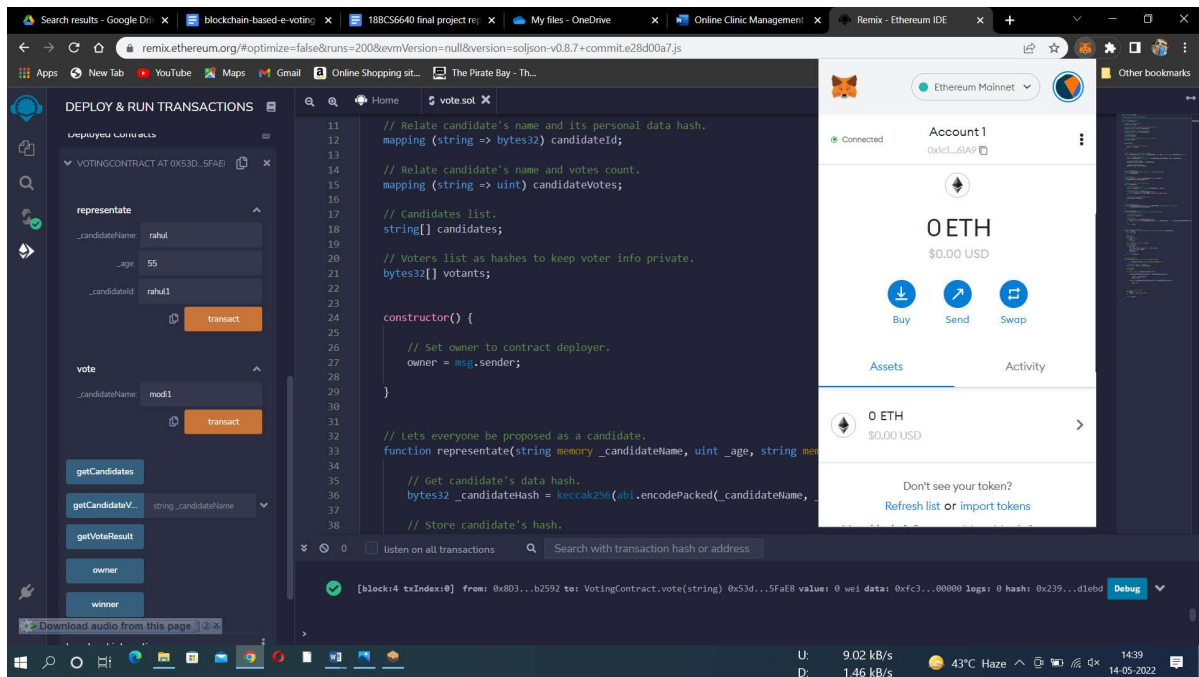
2) Secure Channel

For simplicity, we assume a secure information channel to avoid man-in-the-middle attacks (MITM). It means that no third party can intercept and modify messages. This secure channel

is mainly used to ensure the integrity of the information. Nodes can communicate with each other and verify information reliably.

3) Fast Synchronization

When a device registers in the blockchain, it only needs to request the ledger from a small number of nodes rather than performing long-term synchronization of block data. The nodes for synchronization are selected randomly, so we can assume that these nodes are trustworthy.



I.4 Company

This paper evaluates the use of blockchain as a service to implement an electronic voting (e- voting) system. The paper makes the following original contributions: (i) research existing blockchain frameworks suited for constructing blockchain based e-voting system, (ii) propose a blockchain-based e-voting system that uses “permissioned blockchain” to enable liquid democracy.

The reminder of this paper is organized as follows: In chapter II, we discuss the System analysis: we shall look at the existing issues with the current system, how

to fix them with using blockchain technology, the feasibility and the development requirement. In chapter III, we present our blockchain based e-voting system, we discuss some of the security and legal considerations and limitations regarding designing an electronic voting system for national elections, the flow chart and the E-R diagram.

Chapter II: System Analysis

The Existing System

The Electronic Voting (e-Voting) has effectively replaced the traditional paper-based voting system. The Electronic Voting System aids the voter to cast his vote through a digital or an electronic medium. The Electronic Voting is implemented through Electronic Voting Machines (EVM), Short Messaging Service (SMS) using Smart Phones, Remote or Internet Voting (i- Voting) over Internet, etc.

Electronic Voting is a system which helps the voter to record his choice for a particular candidate securely and privately. The e-voting system is an integrated system designed using a micro controller which generates the results based on the opinion of the people

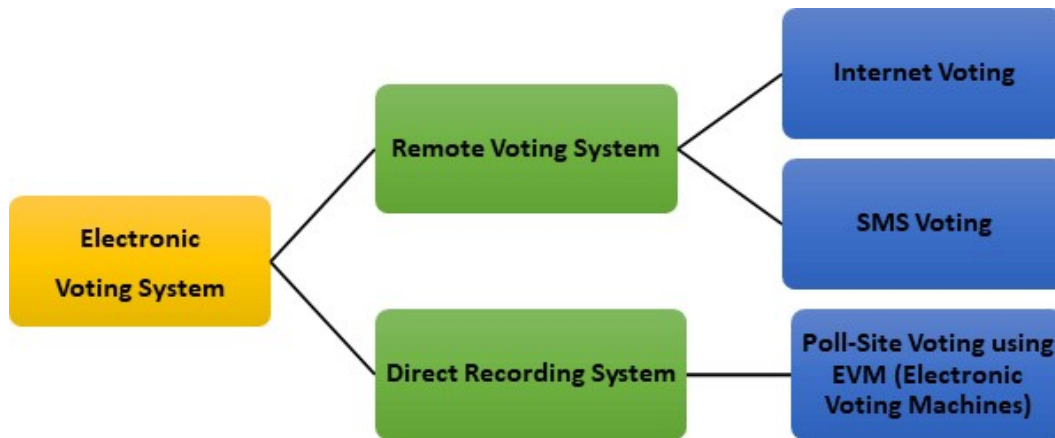
The Election process is made simple using Electronic Voting System. The first procedure involves logging into the website with the voters registered details. Then the user or voter selects a candidate according to his personal choice. This is called submission of ballots digitally. The system records the details and stores the voter's information in the database and computers help in counting and displaying voter's results.

Most popular type of Electronic Voting includes Electronic Voting Machines (EVM) and recording votes via telephones, private computer networks, or the Internet (i-Voting) using a smart phone.

Types of Electronic Voting

There are different types of Electronic Voting namely:

- Remote Voting System
- Direct Recording System



Remote Voting System

A Remote Voting System can be of two types. They are:

- ☐ Internet Voting
- ☐ SMS Voting

Internet Voting (i-Voting)

Internet Voting is a type of e-Voting done remotely via internet. In this system the voter can participate from any location. Few countries like France, Switzerland, Estonia use Internet Voting (i-Voting) for National Level Elections. Internet Voting is also popular among television shows.

SMS (Short Message Service) Voting

SMS voting system is used in popular television shows where the audience votes by sending SMS to a specific number. Mobile Phones are used to send an SMS.

Direct Recording System

Poll-Site Voting using Electronic Voting Machines (EVM'S) is a popular example of Direct Recording System. Till now, 21 countries have used EVM for national level polls such as United Kingdom (UK), Australia, France, Germany, Canada, India, Italy, Belgium, Brazil, Estonia, Namibia, Netherlands, Norway, Peru, Romania, Switzerland, Venezuela , Philippines.

06 out of 21 countries are still using EVMs for the polls. India is one such country. The Election Commission of India collaborated with Bharat Electronics and Electronics Corporation of India

Ltd to design and devise an effective, faster and reliable Electronic Voting System and thus first Electronic Voting Machine came into existence in the year 1982.

The EVM's are used in National Elections and the participant has to go to the specific location called the voting booth to cast his vote. The entire process is supervised by Government Electoral Authorities. EVM displays a list of names of candidates and the user selects his preferred candidate by pushing the button against the name. The LED glows and selection is displayed on the screen which confirms the choice of the user.

Different parts of world have reacted differently to the use of EVMs. North America and some parts of Europe have shown a decreasing interest to EVMs whereas South America and Asia have shown a rapid growth in interest towards EVM technology.

How does Electronic Voting work?

Architecture of both **EVM (Direct Recording System)** and **Internet (Remote) Voting System** is discussed in detail.

EVM (Direct Recording) System Architecture

The **Electronic Voting Machine** System consists of the following components:

- ☐ Power Unit
- ☐ Voting Unit
- ☐ Control Unit
- ☐ Display Unit
- ☐ Confirmation

Unit Power Unit

Generally, Power Unit consists of a Voltage Regulator as it requires fixed output voltage regardless of varying input voltage.

Voting Unit

Voting Unit consists of Resistors connected to press buttons. The user selects his

candidate by pressing the button against the name displayed.

Control Unit

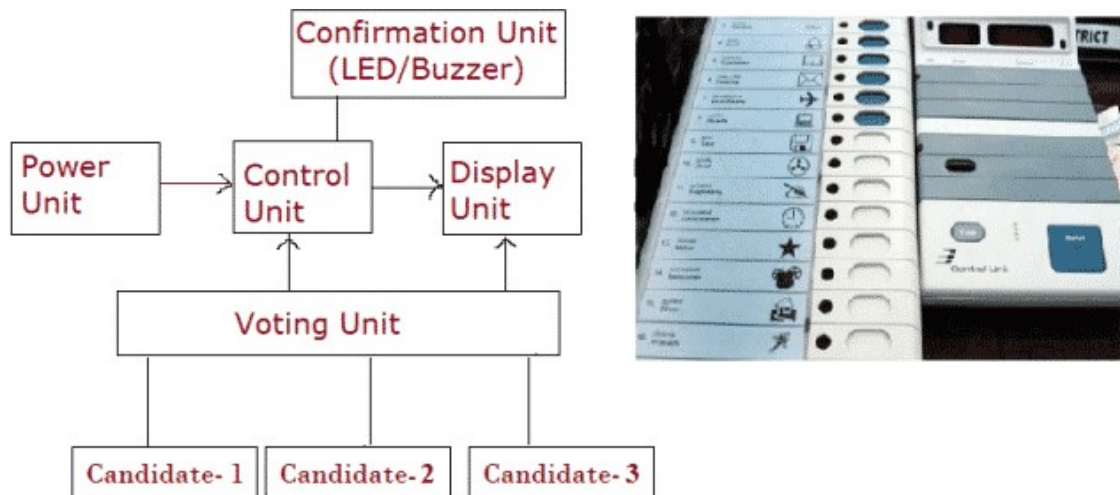
Micro controller is used as the Control Unit which stores the voters data. This unit consists of a CPU, RAM, ROM, I/O Ports and Timers.

Display Unit

Display Unit is Liquid Crystal Display (LCD). When the user pushes a button on the EVM, the result is displayed on the Display Unit which is in textual format.

Confirmation Unit

Buzzer and LED forms the Confirmation Unit. Once the button is pushed by the User on the Voting Unit, Buzzer beeps and LED glows indicating that a particular button is selected which acts as a Confirmation to the User. Buzzer is an audio-signaling device which produces sound in the range of 2-4 KHz. LED is a semiconductor device which acts as a light source.



Internet Voting System (Remote Voting) Architecture

Internet Voting or Online Voting System helps the users to cast their vote from internet connected computer or a mobile anywhere in the world. In this system, the voter's login to the specific website and their identity is authenticated. It is followed by voting process. Once the process is completed, the user logs off from the system.

Online voting increases the voter's participation and it is easier than the poll site voting.

The database contains voter's information like Name, Age, Telephone Number etc. It is responsible for collecting, storing and maintaining the data.

Server

The server is responsible for authentication of the user based on the details entered by the user.

Mixnet

Mixnet is mixed networks that are a set of protocols that aids in Encrypted communication by using a chain of proxy servers called as **Mixes** which take in messages, shuffle and send them randomly to the next destination.

Decryption Mixnet involves decrypting messages by using private key and the message order is shuffled by the node and transmits the result to the next node.

Tallying and Result Consolidation:

The completion of voting process is followed by Result consolidation after the tally process of votes.

Vulnerabilities with the existing system

Technology is transforming democracy on a lot of different levels, and they're not entirely connected. But they all create vulnerabilities in the way that society forms political opinions, expresses those opinions and translates them into election results.

One form of Russian meddling in the 2016 election, for example, was social media campaigns, which affect political discourse at the level of opinions formed by individuals. But the second prong the hacking into campaigns, like John Podesta's e-mail was just so sinister in the way it was picking only on one side. That gets to the very roots of how open societies traditionally rely on information gathering and the media in order to make sound political decisions.

And then there's the third form of hacking: going after the machinery of elections, the infrastructure, polling places, voter registration systems, etcetera. That's where most of my work has been.

No research group had ever had access to a U.S. voting machine in order to do a security analysis, and an anonymous group offered to give us one to study. Back then there was quite a dispute between researchers who hypothesized there would be vulnerabilities in polling place equipment and the manufacturers that insisted everything was fine.

It has moved away from a position of hubris. Now that there have been major academic studies there is scientific consensus that there will be vulnerabilities in polling place equipment.

Sometimes the risks or probable failure modes of new technology are totally foreseeable. And that was certainly the case in voting. As paperless computer voting machines were being introduced, there were many computer scientists who before anyone had even studied one of these machines directly were saying, "This

just isn't a good idea to have elections be conducted by, essentially, black box technology."

On the other hand, the ways in which these failures will be exploited and the implications of that exploitation are sometimes a bit harder to foresee. When we did the first voting machine study 10 years ago, we talked about a range of different possible attackers, dishonest election officials and corrupt candidates. But the notion that it would be a foreign government cyber- attack, that that would be one of the biggest problems to worry about well, that was pretty far

down on the list. Over the past 10 years cyber warfare went from something that seemed like science fiction to something you read about every almost every day in the newspaper.

2016 really did change everything. It taught us that our threat models were wrong. we think it caught much of the intelligence community off guard, and it caught much of the cybersecurity community off guard. It was surreal to see Russia get so close to actually exploiting the vulnerabilities to harm us.

One possibility is that attackers could infiltrate what are called election-management systems. These are small networks of computers operated by the state or the county government or sometimes an outside vendor where the ballot design is prepared.

There's a programming process by which the design of the ballot the races and candidates, and the rules for counting the votes gets produced, and then gets copied to every individual voting machine. Election officials usually copy it on memory cards or USB sticks for the election machines. That provides a route by which malicious code could spread from the centralized programming system to many voting machines in the field. Then the attack code runs on the individual voting machines, and it's just another piece of software. It has access to all of the same data that the voting machine does, including all of the electronic records of people's votes.

So how do you infiltrate the company or state agency that programs the ballot design? You can infiltrate their computers, which are connected to the internet. Then you can spread malicious code to voting machines over a very large area. It creates a tremendously concentrated target for attack.

As Bruce Schneier describes it, technology adds more steps to the process and thus increases the possibility of error with each additional step, all of which are

largely unseen by the voter. Put Murphy's Law of 'whatever can go wrong, will go wrong' into play, and one can surmise that technology will most likely falter. Not only does the technology create more errors in the electronic workings, but the voters can also commit mistakes due to confusion with the user interface. The terminology is confusing, different machines produce different interfaces, and even the audio guides to help the disabled may prove more confusing than helpful.

With the advent of electronic machine voting also comes the higher possibilities of fraudulent machines and practices. First of all, the technology is "black box software," meaning that the

public is not allowed access into the software that controls the voting machines. Although companies protect their software to protect against fraud (and to beat back competition), this also leaves the public with no idea of how the voting software works. It would be simple for the company to manipulate the software to produce fraudulent results. Also, the vendors who market the machines are in competition with each other, and there is no guarantee that they are producing the machines in the best interest of the voters and the accuracy of the ballots.

Lastly, vote accuracy is also an issue, because voters have no way of confirming their vote, and there is also no way of conducting a recount with direct-recording electronic (DRE) in the current system voting. With DRE, there is no paper trail, no verification, and thus no scrutiny of the processes. Voter anonymity is also a problem. Voters have to provide much of their personal information to the systems for voter verification, and with that comes the problem of keeping voter information safe and keeping voters anonymous.

Blockchain-Based Voting

Considering today's technology, blockchain may create one of the most prominent alternatives to traditional voting in terms of security, consistency and speed. While designing a chain for voting in a crowded country, the system should be secure. Many aspects should be considered in order to construct a secure blockchain-based election system. First factor is human for such a system. In the solution, human interference is absolutely prohibited.

The proposed system will be consisting of nodes (computers in design) that is closed to human interference. Any input that cannot be considered as vote will be ignored in this system. For such a system, stealing votes or changing votes are totally blocked. Second issue is saving system from hackers. In order to manipulate votes, hackers need to enter the system as a citizen at proposed solution. Also, it is guaranteed that a citizen can only vote for one time. When

citizen cast a ballot, e-government system will be informed without revealing any information about vote. Then, e-government system marks that person as voted. Since the system takes electorate data from e-government, it is not possible for a marked person to vote again. Although a hacker is obtained the citizen information and entered to the system, he cannot vote more than one time.

In a blockchain system, every transaction is related to the previous one. So, changing an accepted transaction is impossible for such a system. Due to the consistency of the blockchain,

data will always be consistent and voting will be reliable. In a case of manipulation of the system such as changing votes or stealing votes, other connected nodes will already be synchronized. So, the changed data will be identified instantly. Details of the system will be explained below after the use case diagram and explanation of it.

As you can see in the Fig. 1, standard use case of the election system is about the citizen and government. Government in this system only provides the authorization of using a leveled architecture are explained below in detail. Furthermore, consensus of the system is satisfied using DPoS algorithms.

If the whole country would have been represented with a single blockchain, synchronization of the system would have a performance issue due to abundance number of ballots and the distance between voting centers. Distance in connected systems is always cause to latency. For a system that includes all the country under the same blockchain, latency between two voting centers would be a big problem, because for instance for Turkey, expected latency would be around 100 ms at least. This is a huge value for a system that consist of ten thousand of centers and there would be voting at each center simultaneously. In this case, synchronization of the system would take lots of time. So, in order to decrease latency, chains are distributed over levels. From lowest level to highest level, there will be different chains at each level, and connections between levels will be provided with a secure system.

At the lowest level, there will be a chain that consist of nodes (machines / voting centers) where citizens will perform their voting about election. Due to the relatively less number of nodes in the system, synchronization will take affordable amount of time at the lowest level. When the number of nodes is arranged in a good pattern (i.e. there will not be overload at the chains that will cause enormous latency), system will perform well. Citizen will go to the center and will enter the system with the identity that is provided by the government.

We considered to build a system that is working on the citizens who can vote or prevention of the citizens who already voted for that election. Also, government and citizens determine the candidates that will be participating in that election. The ballot box information, candidates and citizen ballot box relation will be provided by the government which is the trusted party in the elections. After citizen's vote, it is added to the blockchain that we will be proposed below and any vote has a guarantee from the system about being immutable. Since a chain contains all the citizen votes anonymously at the end of the election, the official results will be announced within minutes

after the election terminates. Any concerning third party can get the chain and count the votes for being sure that voting is really trusted.

We propose a system that has a leveled structure. There will be different number of levels in that system according to necessities of the country. In order to provide a fast, consistent and secure system, system is designed in a leveled architecture. This number will change from country to country according to features of the country. Reasons behind government's system that will hold the data about citizen for specified voting. If a citizen has not voted yet, citizen will be able to vote one of the candidates. Candidates' will be hold in a database that will also be stored at government related system, because they are already hold. When the authentication process is satisfied, citizen will vote with choosing one of the proposed candidates or blank vote for those who do not want to vote one of the candidates. In this system, proposed candidates will be taken from database that includes relation between ballot boxes and candidates. Thus, there will be only appropriate candidates. It can be the government of any country, in our case it's the Democratic Republic of Congo government. We will be using e- devlet system. Since most of the authentication system used across the government related systems are managed by e-government system, it will not be hard to implement this system relying on this system. When the user passes the authentication phase, citizen will see whether he has voted previously or not. If citizen has not voted yet, citizen will choose desired candidate according to the steps explained above.

At the second lowest level, there will be a cluster of chains that stores data that are coming from below level. In this level, facilities of blockchain technology are used to make system consistent. We considered that 2 levels will be enough. The system at the second level can have about 700 nodes considering population of the country. That brings a huge performance improvement to the system because the number of connected nodes decrease in this structure in a considerable amount. Additionally, if the node numbers at the 2nd or upper levels are increased, performance increases exponentially. For a country, which has more

citizens, level number can be increased in order to decrease collisions between transactions. Consequently, system can be considered as a scalable system.

Communication between levels are ensured using communication protocols. This communication is need to be done periodically. So, there will be a time delay between synchronization of levels. Because, if each vote was considered instantly, there would be a huge bottleneck. This synchronization will provide consistency through the system. For a country such as DR Congo, according to our calculations, this synchronization time should be

5 minutes. That means, at the end of each 5 minutes period, each node cluster will send the chain data to the upper level node. At this level, data will be synchronized between nodes using a different synchronization algorithm. For this level, we designed an algorithm explained below. You can see the visualization for this two-leveled example in Fig. 2. As you can see there are voting centers which are using same blockchain in their selected area. Also, you can think the voting centers as numerous voting machines but for the sake of simplicity we represent them as voting centers. Moreover, you can see that level 1 nodes are using the same blockchain among the level 1 nodes.

It is stated that vote centers are nodes of blockchains. There will be a file at each node (voting center) that stores the number of data that indicates the number of votes accepted from upper level at previous synchronization step. At every specified time intervals, voting will be stopped for a very short time period in order to synchronize blockchain data between levels. When the data is arrived to upper level from lower chain nodes, it will be checked in order to satisfy consistency. If the consistency of the data is ensured, answer will be a flag that indicates the data is accepted. At this point, nodes at the level 0 will be waiting an answer from level 1 (and level 1 from level 2, so on). If arrived flag tells the votes are accepted, the files at each node (voting centers) will be updated. So, nodes at the lowest level of one of two levels will always know that how many votes have been accepted at above level. Additionally, data will be added to blockchain at the level that the data is arrived (if the communication is between level 0 level 1, indicated level here is level 1). This data will be considered as a transaction block, that means all the new votes (votes coming after from the previously added votes) are considered as a vote cluster and considered as array in computer scientific terms. This vote cluster will be a block that will be added to chain.

At the synchronization phase, if the data coming to the upper level from different machines are inconsistent, that will be a case that should be considered with a

care. In this case, if the consensus could not be satisfied, the data will not be accepted from highest level of the two levels and the “decline” flag will be sent to the lower one. In this case, same data should be sent to the upper level again. Until the consistency is satisfied, this procedure will be continued, and with this procedure, consistency will be satisfied at each level.

It is stated above that the all nodes at the lower levels know that the data is accepted if the answer states, so, they can continue working. But in order to satisfy consistency through the system, delays between synchronizations should be arranged very carefully. If the delay between levels becomes a small amount of time, the time spent for synchronization may grow

much. On the contrary, if the delay becomes a big amount of time, the data that will be sent between levels takes an enormous size and to transfer this data becomes a problem. So, in order to not bottleneck the system, this delay between levels should be chosen carefully. With the well-designed synchronization times between levels, a high performance providing consistent system would be obtained.

Block structures in levels can be seen below. The election related data are stored in block as shown below through the system. As seen in Fig 3. and Fig 4. we propose two types of blocks: one is for building blockchain at the lowest level of the architecture, that stores candidate info, ballot box info, a “nonce” field that will be used for hashing and a prev_hash info that will be used when creating block that will be added to the blockchain, and other one is consisting of two fields: one is prev_hash field that will be used in order to build blockchain and other one, “lotb” keyword that indicates list of the blocks. Attribute “nonce” is a state of art in the blockchain technology which provides additional security to each hash. For each chain, you select a pattern such as “hash must start with 4 trailing zeros”, while creating hash from the block system look to the hash pattern if it does not fit the pattern then it changes the “nonce” string until hash pattern is valid for the chain. It requires more computational power because it will run hash algorithm multiple times until pattern is matched but it also increases the security since if any malicious party create a hash and try to add that block to the chain, it also has to know the hash pattern. Since chain pattern will be different for each election, third parties cannot predict or create a hash that can be accepted.

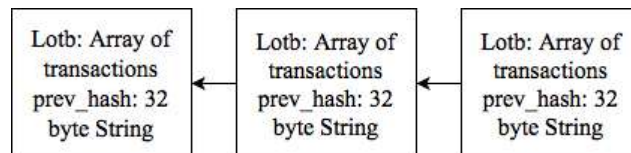


Figure 3: Block structure at level 1 or more

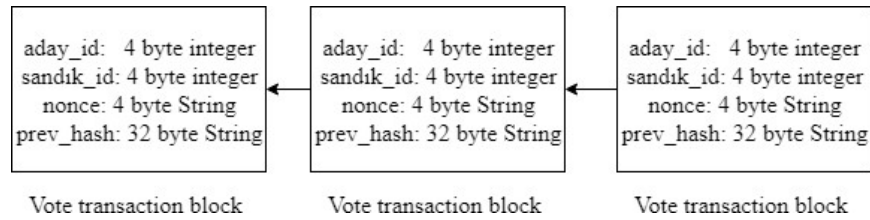


Figure 4: Block structure at level 0 (lowest level)

At the lowest level (level 0), each block will be consisting of one transaction and at each block, whole related information about transaction (in proposed e-voting case, this block indicates a vote) are stored. At the upper levels, the votes coming from one below level are stored in clusters that is sent through different time segments, and all of them are stored as a monolith

structure. When this data is arrived, a new block is processed with the prev_hash data and added as a block to the blockchain at described level. When a new block is being tried to add to the chain, according to the Delegated Proof of Stake of Ethereum, it is added and data consistency is satisfied. Adding block to the chain is very costly operation. Therefore, there are some implementations and research about this operation. In Ethereum based Smart Contracts system has been discussed for different purposes. Researchers think that smart contracts can be applied in e-voting and this project implements Smart Contracts. Smart Contracts reduce the cost of the transactions and it does not rely on a third party to operate. Turing-completeness feature of the Ethereum allows to create customized and more powerful contracts

➤

Feasibility and development requirement

In this paper, we consider existing electronic voting systems, blockchain-based and non- blockchain-based, and evaluate their respective feasibility for implementing a national e-voting

system. Based on this, we devised a blockchain-based electronic voting system, optimizing for the requirements and considerations identified. In the following subsection, we start by identifying the roles and component for implementing an e-voting smart contract then, we evaluate different blockchain frameworks that can be used to realize and deploy the election smart contracts. In the last subsection, we will discuss the design and architecture of the proposed system.

A. Evaluating Blockchain as a Service for E-Voting

Table III shows a comparison between the three blockchain frameworks that we consider for implementing and deploying our election smart contracts. Those are Exonum, Quorum and Geth.

TABLE III: Framework Evaluation

	Exonum	Quorum	Go-Ethereum
Consensus	Custom-built BFT algorithm	QuorumChain and Raft- based consensus	PoW, PoS and PoA
Transaction p/s	up to 5000 transactions p/	Dozens to hundreds	Depends
Private support	Yes	Yes	Yes
Smart Contract Language	Rust	Solidity	Solidity
Programming Language	Rust	Go, C, JavaScript	Go, C, JavaScript
Decentralized	Yes	Partially	Optional

1) Exonum: Looking at the Exonum blockchain, it is robust end to end with its full implementation done with the programming language Rust. Exonum is built for private blockchains. It has a customized Byzantine algorithm that is used to achieve consensus in the network. With that consensus algorithm, Exonum can support up to 5000 transactions per second. Unfortunately, the limitation of the framework is that Rust is the only programming language in the current version, which limits the developers to the constructs available in

that language. To solve this limitation, Exonum is planning to introduce Java-bindings and platform-independent interface description to make Exonum more developer- friendly in the near future.

2) Quorum: Is an Ethereum-based distributed ledger protocol with transaction/contract privacy and new consensus mechanisms. It's a Geth fork and is updated in line with Geth releases. Quorum changed up the consensus mechanism and aimed more towards

consortium chain-based consensus algorithms. Using this consensus allows it to support from dozens to hundreds of transactions per second.

3) Geth: Go-Ethereum or Geth is one of three original implementations of the Ethereum protocol and it runs smart contract applications exactly as programmed without possibility of downtime, censorship, fraud or third-party interference. This framework supports development beyond the Geth protocol, and is the most developer-friendly framework of the frameworks we evaluated. The transaction per second (transaction rate) is dependent on whether the blockchain is implemented as a public or private network. Because of these capabilities, Geth was the framework we chose to base our work on, any similar blockchain framework with the same capabilities as Geth should be considered for such systems.

B. Security analysis

1) DDoS: To successfully DDoS a distributed system such as we have proposed, the attacker must DDoS every single bootnode in the private network. The individual or institution would be immediately located if that would occur. Each node is implemented with a Byzantine fault tolerance algorithm, which helps locating failed nodes in the system.

2) Authentication vulnerability: Each individual is identified and authenticated by the system by presenting an electronic ID from Auðkenni and the corresponding 6-digit PIN in the voting booth. Without supervision, an individual could vote for multiple people, if the individual had knowledge of the PIN for each corresponding electronic ID he has. To further address this vulnerability in the near future, a biometric scan could be introduced.

3) Sybil: Sybil attack is known against centralized systems, where an individual creates a large number of nodes in an attempt to disrupt network operation by hijacking or dropping messages. Since our proposal is running in a private network no individual has the access to create one. Even the consensus protocol that is used in our system is prone Sybil attacks. Private

blockchains solve many of today's security problems using strong cryptography features and the limited access to the ledger, without negating the transparency aspect the blockchain technology offers.

C. Legal issues

1) Remote voting: Remote elections provide no coercion resistance because of the non-supervised factor in a remote election. Remote elections can therefore not guarantee the privacy that people have when they cast their vote in a voting booth. Family members or a

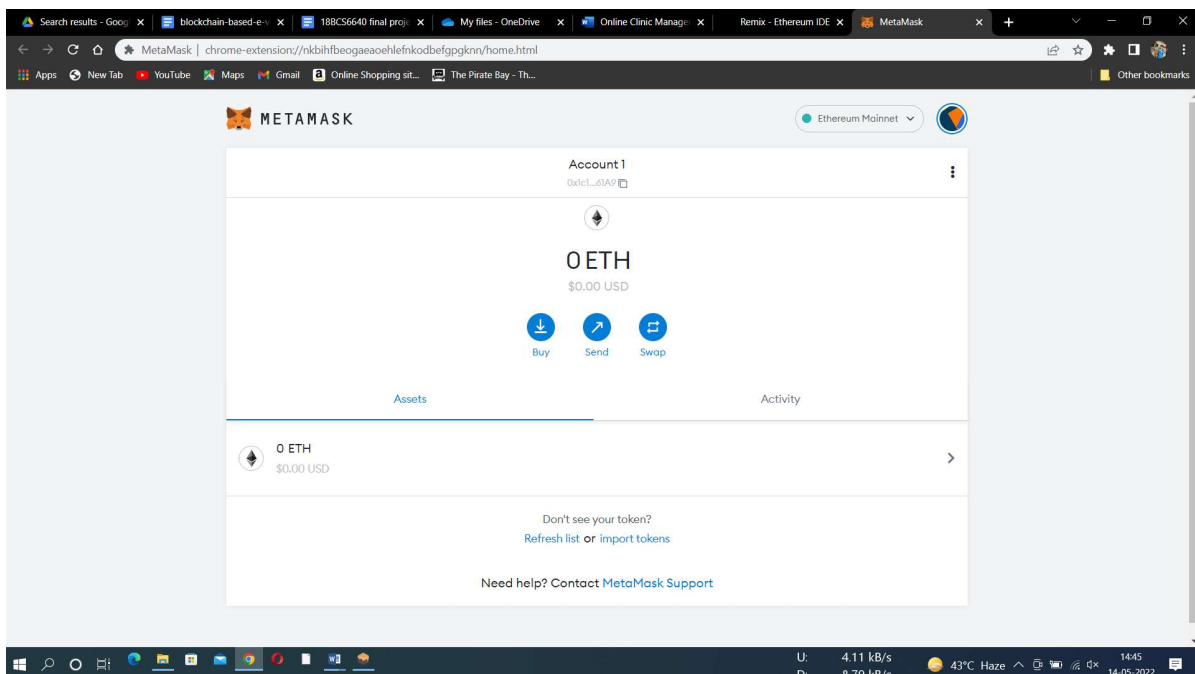
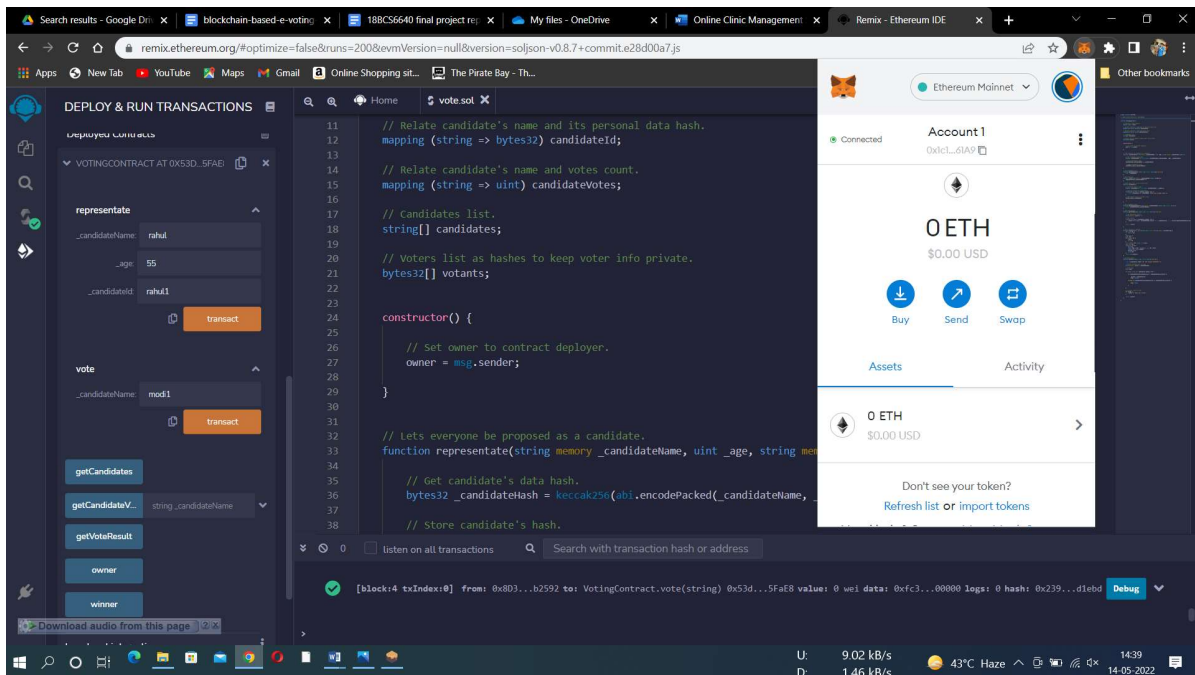
coercer can watch over your shoulder while you're voting, which could lead to a misconfigured result. If elections are hosted on a website for example it could easily be taken down by people with good hacking skills and the mindset to do so. People could identify themselves as another person and therefore vote for another person and even multiple people.


2) Transparency: In the today's election scheme, no method of transparency can be offered to participants of the election. When an individual place his ballot in the box at his voting district, there is no guarantee from the scheme that his vote was counted and counted correctly. Any individual vote can be misplaced, counted incorrectly because of human error or simply because the party which the voter voted for could be disliked by the individual which counted the vote. This transparency is non-existent because no ballot has information on who casted aforementioned vote. To introduce transparency in the process of an election would require a new law which would allow government officials to provide the services which allow such method of transparency

3) Voter privacy: In every pen and paper election scheme, voter's privacy is a key element. The law forbids any individual or entity to be able to know from a single vote, who gave aforementioned vote. If such information could be gathered for each vote, such information could then leak to the public which would allow for listing every single individual who voted for a single party/candidate. To satisfy the privacy of each voter, no individual vote should be traceable back to the voter.

Application used for Project:

1. Metmask Wallet
2. Ganache
3. Remix IDE
4. Solidity







Ganache

v2.5.4

CREATE A WORKSPACE

Quickstart for a one-click blockchain or create a new workspace for advanced setup options.

 **QUICKSTART**
ETHEREUM

 **NEW WORKSPACE**
ETHEREUM

Search results - Google

blockchain-based-e

18BC5640 final proj

My files - OneDrive

Online Clinic Manage

Remix - Ethereum IDE

MetaMask

26°C Haze

23:16

03-04-2022

remix.ethereum.org/#optimize=false&runs=200&evmVersion=null&version=soljson-v0.8.7+commit.e28d00a7.js

Apps

New Tab

YouTube

Maps

Gmail

Online Shopping sit...

The Pirate Bay - Th...

Other bookmarks

DEPLOY & RUN TRANSACTIONS

loaded contracts

VOTINGCONTRACT AT 0x53D...5FAB

representate

_candidateName

rahul

_age

55

_candidateId

rahul1

transact

vote

_candidateName

mod1

transact

getCandidates

getCandidateV...

string _candidateName

getVoteResult

owner

winner

vote.sol

```
11 // Relate candidate's name and its personal data hash.
12 mapping (string => bytes32) candidateId;
13
14 // Relate candidate's name and votes count.
15 mapping (string => uint) candidateVotes;
16
17 // Candidates list.
18 string[] candidates;
19
20 // Voters list as hashes to keep voter info private.
21 bytes32[] votants;
22
23
24
25
26
27 constructor() {
28     // Set owner to contract deployer.
29     owner = msg.sender;
30 }
31
32 // Lets everyone be proposed as a candidate.
33 function representate(string memory _candidateName, uint _age, string memory _candidateId) public {
34     // Get candidate's data hash.
35     bytes32 _candidateHash = keccak256(abi.encodePacked(_candidateName, _age, _candidateId));
36
37     // Store candidate's hash.
38 }
```

listen on all transactions

Search with transaction hash or address

[block:4 txIndex:0] from: 0x803...b2592 to: VotingContract.vote(string) 0x53d...5faE8 value: 0 wei data: 0xfc3...00000 logs: 0 hash: 0x239...d1ebd

Debug

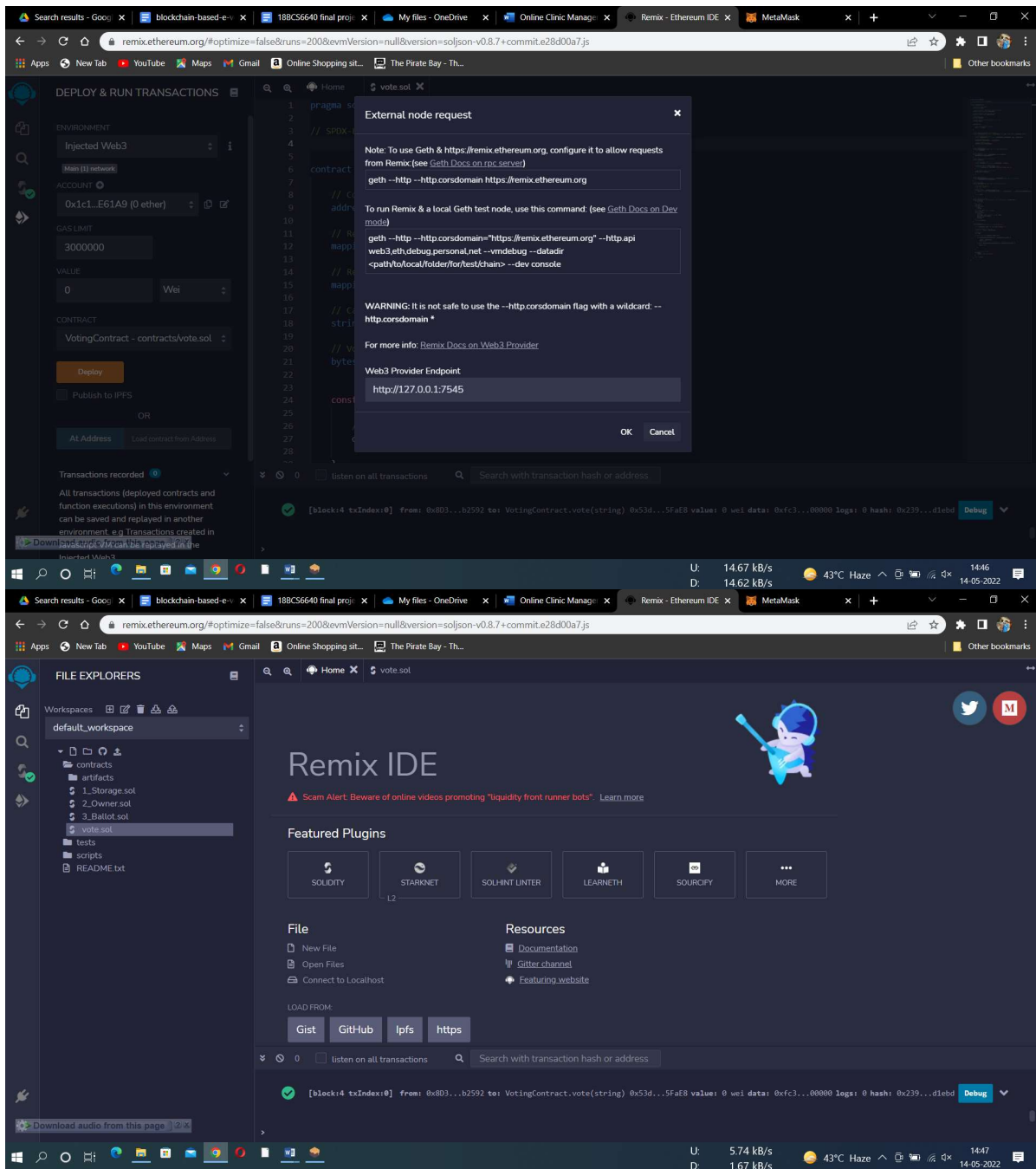
U: 1.37 kB/s

D: 1.72 kB/s

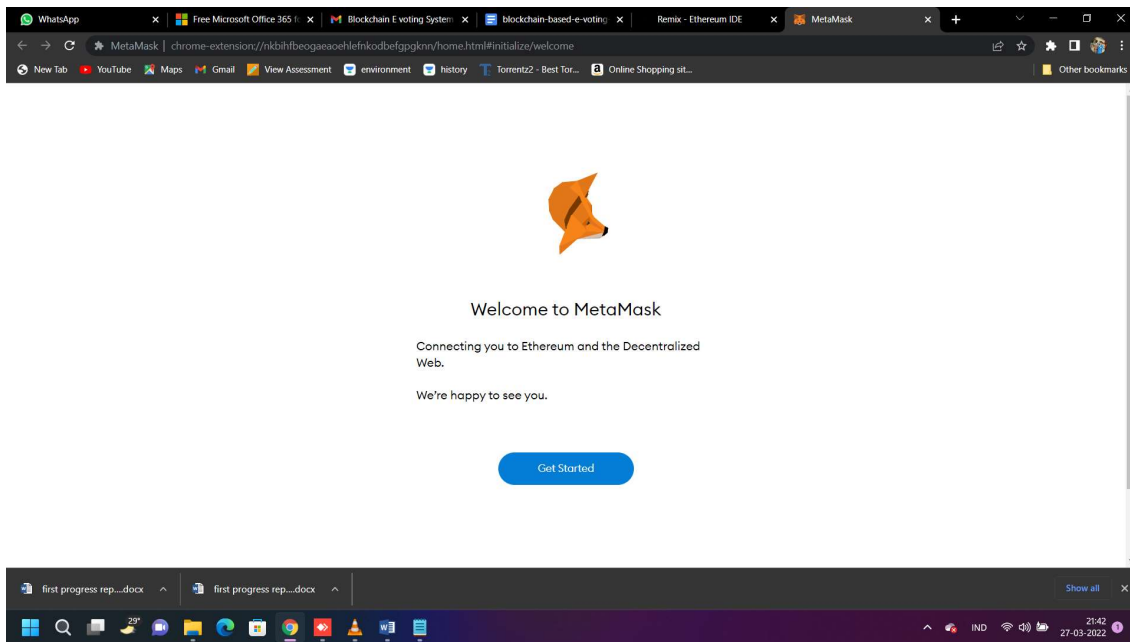
43°C Haze

1446

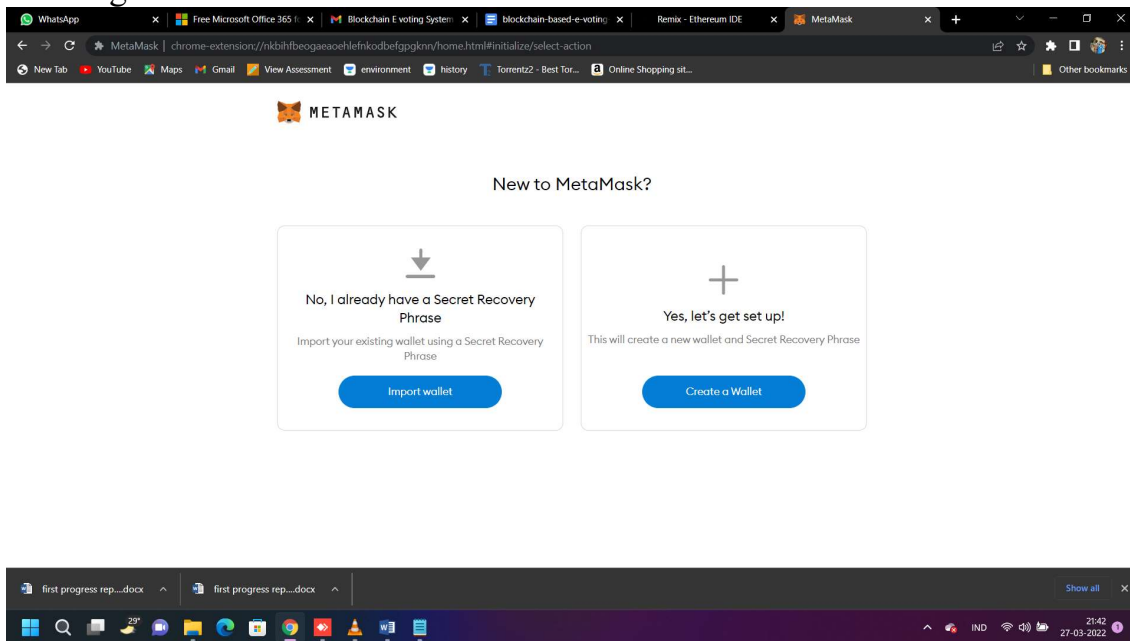
14-05-2022



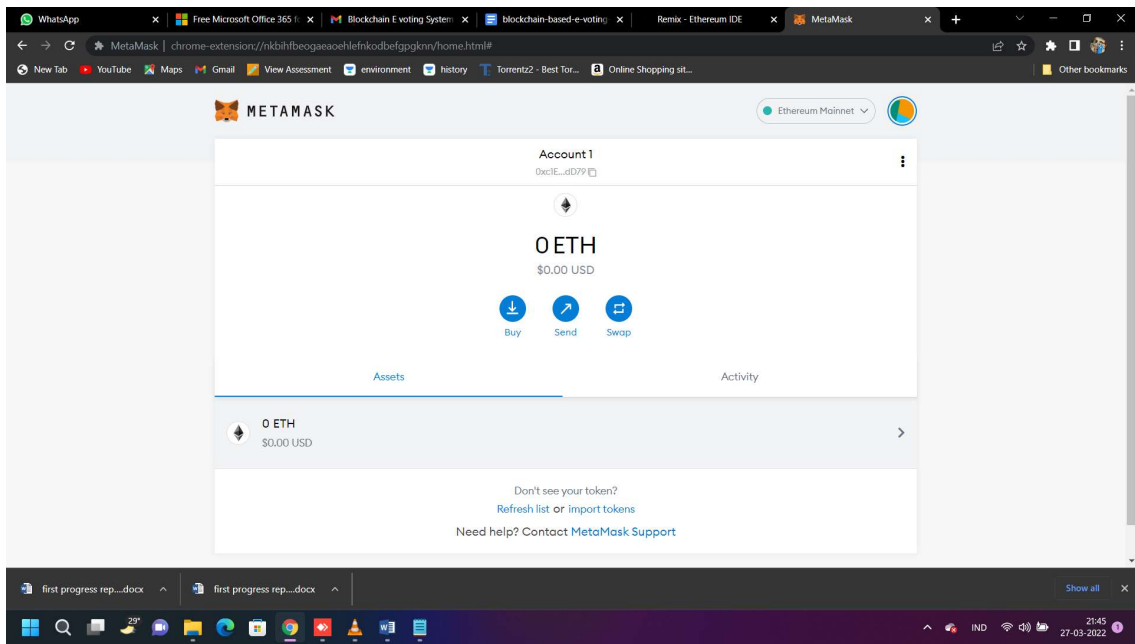
Metamask:

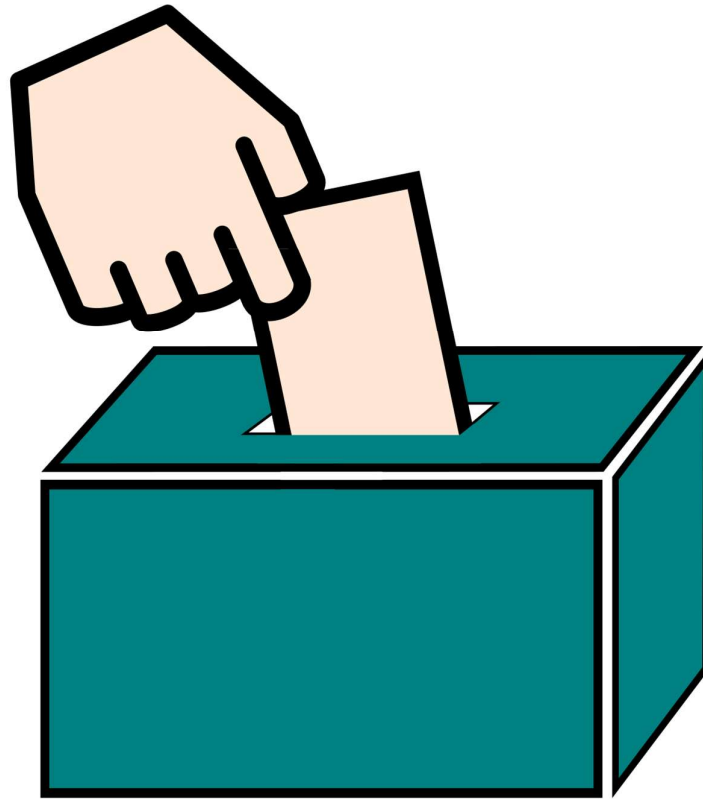


Creating metamask wallet:



Metamask wallet:





Conclusion

To Overcome all the Shortcomings in the Present Voting System, we came up with the Modern Technology of Blockchain i.e. E-Voting System using Blockchain. By using this modern technology, following things can be Achieved:- Cheap Voting System, Accurate Voting System, Fast Voting System.

Every Citizen desires to have a Transparent and Direct Form of Democracy which is clear cut obtained from this E- Voting System using Blockchain. Faith of People on the Voting System is Increased therefore, many People Come Forward for Voting, thereby Increasing the Percentage of the People Voted. The Pen and the Paper Election is Eradicated thereby creating Accuracy in the Voting System. Everybody Prefers Time ,and Cost Efficient Systems so this E-Voting System using Blockchain is apt for Transparent Democracy. Ethereum Private Blockchain allows hundreds and hundreds of Transactions in a Second. Utilisation of the Smart Contracts lower the Load on the Blockchain. For Countries with Greater Population, some additional Technology should be added in this E-Voting System using Blockchain to avoid Errors. The main reason behind this system is to present an idea of implementation of blockchain in the voting system.

Futures Works

Democracies depend on trusted elections and citizens should trust the election system for a strong democracy. However traditional paper-based elections do not provide trustworthiness. In this paper, we proposed a blockchain based e-voting system which provides a trusted, secure and fast voting system for Turkey. Proposed system is suitable to apply in another country whereas integration is hard work since each country has different laws and election system changes

between countries.

References

- R. Hanifatunnisa and B. Rahardjo, "Blockchain based e-voting recording system design," 2017 11th International Conference on Telecommunication Systems Services and Applications (TSSA), Lombok, 2017, pp. 1-6.
- R. Krimmer, A. Ehringfeld, and M. Traxl, "The Use of E-Voting in the Austrian Federation of Students Elections 2009," Internet: <https://pdfs.semanticscholar.org/6b8f/34a5bd3e7eabc7e3a9a3f008187e4415e26a.pdf> [Nov. 26, 2018]
- "The Geneva Internet Voting System," Internet: https://www.coe.int/t/dgap/goodgovernance/Activities/E-voting/EVoting_Documentation/passport_evoting2010.pdf [Nov. 25, 2018]
- F. Þ. Hjálmarsson, G. K. Hreiðarsson, M. Hamdaqa and G. Hjálmtýsson, "Blockchain- Based E-Voting System," 2018 IEEE 11th International Conference on Cloud Computing (CLOUD), San Francisco, CA, 2018, pp. 983-986.
- S. Ølnes, J. Ubacht and M. Janssen, "Blockchain in government: Benefits and implications of distributed ledger technology for information sharing", Government Information Quarterly, vol. 34, no. 3, pp. 355-364, 2017.
- A. Barnes, C. Brake, and T. Perry, "Digital Voting with the use of Blockchain Technology," Available: <https://www.economist.com/sites/default/files/plymouth.pdf> [Nov. 20, 2018]
- A. Barnes, C. Brake, and T. Perry, "Digital Voting with the use of Blockchain Technology," Available: <https://www.economist.com/sites/default/files/plymouth.pdf> [Nov. 20, 2018]
- M. Pawlak, A. Poniszewska-Marańda and N. Kryvinska, "Towards the intelligent agents for blockchain e-voting system," Procedia Computer Science, vol. 141, pp. 239-246, 2018.
- P. Tarasov and H. Tewari, "The Future of E-voting," IADIS International Journal on Computer Science and Information Systems, vol. 12, no. 2, pp. 148-165.
- Bartolucci, S., Bernat, P., & Joseph, D. (2018). SHARVOT: Secret SHARe-Based VOTing on the Blockchain. 2018 IEEE/ACM 1st International Workshop on Emerging Trends in Software Engineering for Blockchain (WETSEB), 30-34.
- Reyna, C. Martín, J. Chen, E. Soler and M. Díaz, "On blockchain and

- its integration with IoT. Challenges and opportunities", Future Generation Computer Systems, vol. 88, pp. 173-190, 2018.
- Wang, J. Sun, Y. He, D. Pang and N. Lu, "Large-scale Election Based On Blockchain", Procedia Computer Science, vol. 129, pp. 234-237, 2018.
 - Internet: <https://lisk.io/academy/blockchain-basics/how-does-blockchain-work/delegated-proof-of-stake> [Nov. 25, 2018]
 - Internet: <https://www.turkiye.gov.tr/> [Nov. 25, 2018]
 - Alharby, Maher, and Aad van Moorsel. "Blockchain Based Smart Contracts : A Systematic Mapping Study." Computer Science & Information Technology (CS & IT), 2017

Internet: <https://sonuc.ysk.gov.tr/> [Nov. 16, 2018]
J. Yli-Huumo, D. Ko, S. Choi, S. Park and K. Smolander, "Where Is
Current Research on Blockchain Technology?—A Systematic Review," PLOS
ONE, vol. 11, no. 10, 2016.
<https://electricalfundablog.com/electronic-voting-works-types/>
[https://cs.stanford.edu/people/eroberts/cs181/projects/2006-
07/electronic- voting/index_files/page0002.html](https://cs.stanford.edu/people/eroberts/cs181/projects/2006-07/electronic-voting/index_files/page0002.html)
[https://www.scientificamerican.com/article/the-vulnerabilities-of-our-voting-
machines/](https://www.scientificamerican.com/article/the-vulnerabilities-of-our-voting-machines/)

