ISSN (Online): 2583-7052

International Journal of Advanced Trends in Engineering and Management (IJATEM)
pp. 132-141

Article Title: Trustworthy Electronic Voting Using Adjusted Blockchain

Trustworthy Electronic Voting Using Adjusted Blockchain

Elba Rajathi A[1], Evelyn Tabitha E[2], Mary Isha D[3]

[1] PG Student, Department of Computer Science and Engineering
PET Engineering College, Tirunelveli, India.
[2,3]AssistantProfessor, Department of Computer Science and Engineering
PET Engineering College, Tirunelveli, India.

ABSTRACT

E-voting is among the key public sectors that can be disrupted by blockchain technology. The idea in blockchain- enabled e-voting (BEV) is simple. To use a digital- currency analogy, BEV issues each voter a "wallet" containing a user credential. Each voter gets a single "coin" representing one opportunity to vote. Casting a vote transfers the voter's coin to a candidate's wallet. A voter can spend his or her coin only once. However, voters can change their vote before a preset deadline. Here, we argue that blockchains might address two of the most prevalent concerns in voting today: voter access and voter fraud. The idea is as follows. Eligible voters cast a ballot anonymously using a computer or smartphone. BEV employs an encrypted key and tamperproof personal IDs. For example, the mobile e-voting platform of the Boston-based startup Voatz employs smart biometrics and real-time ID verification. The public ledger ties each cast ballot to an individual voter and establishes a permanent, immutable record. No bad actor can engage in nefarious activities because such activities will be evident on the ledger or corrected by a peer-to-peer consensus network. To compromise the network, hackers would need to successfully hack most of the blocks (files with transaction records) before new blocks were introduced. The blockchain's audit trail ensures that no vote has been changed or removed and that no fraudulent and illegitimate votes have been added. Putsimply, blockchains enable the creation of tamper-proof audit trails for voting. In this article, we highlight some BEV implementations and the approach's potential benefits and challenges.

Keywords: Blockchain, BEV, Smartphone.

1 Introduction

Blockchain could be a data structure that could be a growing list of information blocks. The knowledge blocks area unit coupled along, such recent blocks can't be removed or altered. Blockchain is the backbone Technology of Digital Cryptocurrency BitCoin. The Blockchain is a distributed database of records of all transactions or digital events that have been executed and shared among participating parties. Each transaction is verified by the majority of participants of the system. It contains every single record of each transaction. BitCoin is the most popular cryptocurrency, an example of the blockchain. Blockchain Technology first came to light when a person or Group of individuals named 'Satoshi Nakamoto' published a white paper on "BitCoin: A peer-to-peer electronic cash system" in 2008. Blockchain Technology

ISSN (Online): 2583-7052

International Journal of Advanced Trends in Engineering and Management (IJATEM)
pp. 132-141

Article Title: Trustworthy Electronic Voting Using Adjusted Blockchain

Records Transaction in Digital Ledger which is distributed over the Network thus making it incorruptible. Anything of value like Land Assets, Cars, etc.

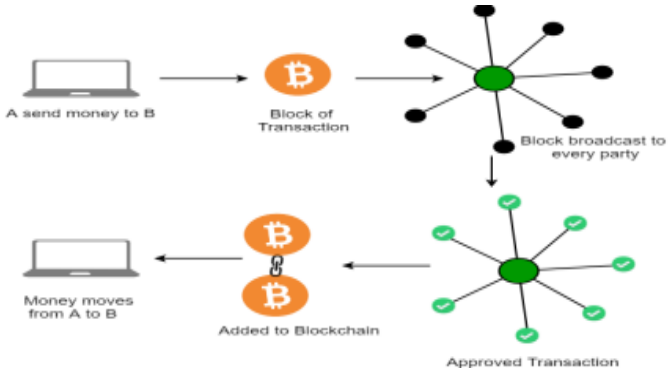


Figure 1: *Transaction*

1.1 Network of nodes

A node is a computer connected to the Blockchain Network. Node gets connected with Blockchain using the client. Client helps in validating and propagating transactions onto the Blockchain. When a computer connects to the Blockchain, a copy of the Blockchain data gets downloaded into the system and the node comes in sync with the latest block of data on the Blockchain. The Node connected to the Blockchain which helps in the execution of a Transaction in return for an incentive is called Miners.

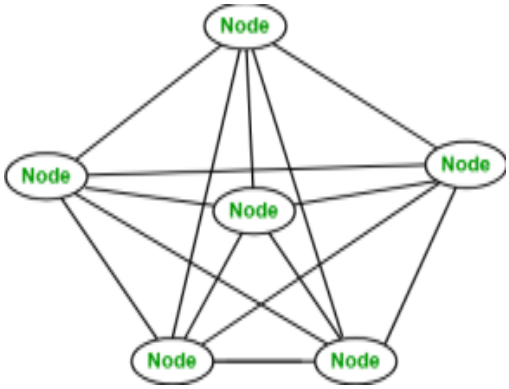


Figure 2: *Network of nodes*

1.2 Building trust with blockchain

Blockchain enhances trust across a business network. It's not that you can't trust those who you conduct business with, it's that you don't need to when operating on a Blockchain network. Blockchain builds trust through the following five attributes:

Distributed: The distributed ledger is shared and updated with every incoming transaction among the nodes connected to the Blockchain. All this is done in real-time as there is no central server controlling the data.

Secure: There is no unauthorized access to Blockchain made possible through Permissions and Cryptography.

ISSN (Online): 2583-7052

International Journal of Advanced Trends in Engineering and Management (IJATEM)
pp. 132-141

Article Title: Trustworthy Electronic Voting Using Adjusted Blockchain

Transparent: Because every node or participant in Blockchain has a copy of the Blockchain data, they have access to all transaction data. They themselves can verify the identities without the need for mediators.
Consensus-based: All relevant network participants must agree that a transaction is valid. This is achieved through the use of consensus algorithms.
Flexible: Smart Contracts which are executed based on certain conditions can be written into the platform. Blockchain Network can evolve in pace with business processes.

1.3 Benefits of block chain technology

Time-saving: No central Authority verification needed for settlements making the process faster and cheaper.
Cost-saving: A Blockchain network reduces expenses in several ways. No need for third-party verification. Participants can share assets directly. Intermediaries are reduced. Transaction efforts are minimized as every participant has a copy of shared ledger.
Tighter security: No one can temper with Blockchain Data as it is shared among millions of participants. The system is safe against cybercrimes and Fraud.
Collaboration: It permits every party to interact directly with one another while not requiring third party negotiation.
Reliability: Blockchain certifies and verifies identities of every interested party. This removes double records, reducing rates and accelerating transactions.

1.4 Application of blockchain

- Leading Investment Banking Companies like Credit Suisse, JP Morgan Chase, Goldman Sachs and Citigroup have invested in Blockchain and are experimenting to improve the banking experience and secure it.
- Following the Banking Sector, the Accountants are following the same path. Accountancy involves extensive data, including financial statements spreadsheets containing lots of personal and institutional data. Therefore, accounting can be layered with blockchain to easily track confidential and sensitive data and reduce human error and fraud. Industry Experts from Deloitte, PwC, KPMG and EY are proficiently working and using blockchain-based software.
- Booking a Flight requires sensitive data ranging from the passenger's name, credit card numbers, immigration details, identification, destinations, and sometimes even accommodation and travel information. So the sensitive data can be secured using blockchain technology. Russian Airlines are working towards the same.
- Various industries, including hotel services, pay a significant amount ranging from 18-22% of their revenue to third-party agencies. Using blockchain, the involvement of the middleman is cut short and allows interacting directly with the consumer ensuring benefits to both parties. Winding Tree works extensively with Lufthansa, Air France, Air Canada, and Etihad Airways to cut short third-party operators charging high

ISSN (Online): 2583-7052

International Journal of Advanced Trends in Engineering and Management (IJATEM)
pp. 132-141

feesBarclaysuses Blockchain to streamline the Know Your Customer (KYC) and Fund Transfer processes while filing patents against these features. Keep track of and manage the inventory of medicines.

2 Literature Survey

[1] A Systematic Literature Review and Meta-Analysis on Scalable Blockchain-Based Electronic Voting Systems, Authors: Uzma Jafar, Mohd Juzaiddin Ab Aziz, Zarina Shukur, and Hafiz Adnan Hussain. Electronic voting systems must find solutions to various issues with authentication, data privacy and integrity, transparency, and verifiability. On the other hand, Blockchain technology offers an innovative solution to many of these problems. The scalability of Blockchain has arisen as a fundamental barrier to realizing the promise of this technology, especially in electronic voting. This study seeks to highlight the solutions regarding scalable Blockchain-based electronic voting systems and the issues linked with them while also attempting to foresee future developments. A systematic literature review (SLR) was used to complete the task, leading to the selection of 76 articles in the English language from 1 January 2017 to 31 March 2022 from the famous databases. This SLR was conducted to identify well-known proposals, their implementations, verification methods, and various cryptographic solutions in previous research to evaluate cost and time. It also identifies performance parameters, the primary advantages and obstacles presented by different systems, and the most common approaches for Blockchain scalability. In addition, it outlines several possible research avenues for developing a scalable electronic voting system based on Blockchain technology. This research helps future research before proposing or developing any solutions to keep in mind all the voting requirements, merits, and demerits of the proposed solutions and provides further guidelines for scalable voting solutions.

[2] Survey on Voting System using Blockchain Technology, Authors: Mayur Shirsath, Mohit Zade, Ritesh Kumar Talke, Praful Wake, Maya P. Shelke. The use of information technology has in some ways revolutionized in many sectors. E-voting is said to be a symbol of modern democracy. While research on the topic is still emerging, it has mostly focused on the technical and legal issues instead of taking advantage of this technology and implementing it for good cause. Usefulness of e-voting will perform best when compared with the existing framework. The word Vote means to choose a candidate from a given list of candidates who will lead the organization or the group .The main goal of voting is to practice voting in such a way that every person votes to elect their leader. Most countries in the world, India is no exception, had trouble voting. Voting is still carried out in countries in physical mode. This physical mode process is not safe as it can be manipulated by members of voting commitment. There are many issues such as voting stations being too far and improper voting tools. The proposed flagship internet-based online voting system supported by blockchain technology solves this very problem. Blockchain technology uses encryption and hashing techniques with which it makes voting secure. In this case, each vote is considered as a unique transaction. A private blockchain is

ISSN (Online): 2583-7052

International Journal of Advanced Trends in Engineering and Management (IJATEM)
pp. 132-141

created using a peer to peer network where we store voting transactions. This application is programmed in such a way so that the details of voting are abstract from the user. Users will be given enough time for voting with the system running. The main purpose of this paper is to come up with a new unique solution, which does not require any technical skills. In this project, the concept of developing an electronic voting system using blockchain technology is implemented.

3 Proposed System

The voter's name must exist in the voting list to enable himself to visit the polling station for the purpose of voting. It is the responsibility of the voter himself to ensure that once he attains the age of eighteen years, his name should be present in the voting list. This can be done by consulting the respective offices, e.g. National Database and Registration Authority (NADRA) in Pakistan. The voting lists are published a few weeks earlier than the elections. The individual having his name in the voting list is eligible to vote and presents his original identity to the polling staff. Before casting the vote, the voter has to be authenticated by the biometric system. The record of the voter is checked with the help of NADRA's database. Once the voter has passed the authentications check, he is brought to the voting screen to vote. From the voting machine the names and respective party symbols of each candidate are displayed and the voter can vote according to his will. The confirmation screen seeks the confirmation of the voter and records the vote casted by the voter. The voter can vote only once, and once the vote is casted is voting record is marked as ''voted'', which restricts the voters from voting again. The name of the voter can be blocked or eliminated from the list of eligible voters list for the current elections, once he has casted the vote. The polling process continues until the voting time ends or all the voters in the voting list have casted their votes.

3.1 System Design

Data Flow Diagram

The DFD is also called a bubble chart. It is a simple graphical formalism that can be used to represent a system in terms of input data to the system, various processing carried out on this data, and the output data is generated by this system.

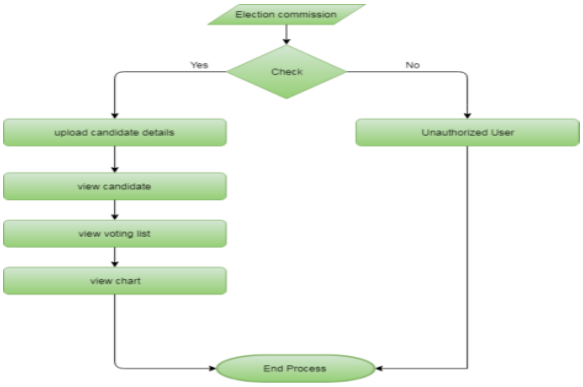
User

ISSN (Online): 2583-7052

International Journal of Advanced Trends in Engineering and Management (IJATEM)
pp. 132-141

Article Title: Trustworthy Electronic Voting Using Adjusted Blockchain

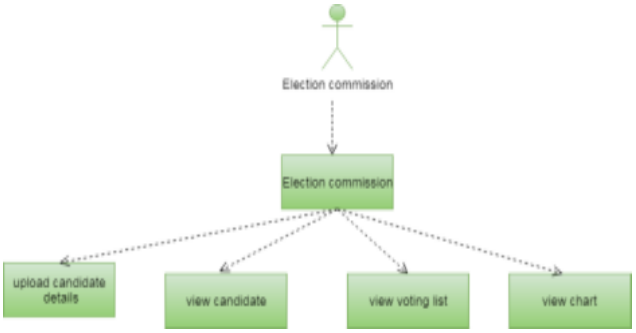
Election Commission



Use Case Diagram: A use case diagram in the Unified Modeling Language (UML) is a type of behavioral diagram defined by and created from a Use-case analysis. Its purpose is to present a graphical overview of the functionality provided by a system in terms of actors, their goals (represented as use cases), and any dependencies between those use cases. The main purpose of a use case diagram is to show what system functions are performed for which actor. Roles of the actors in the system can be depicted.

User

Election Commission

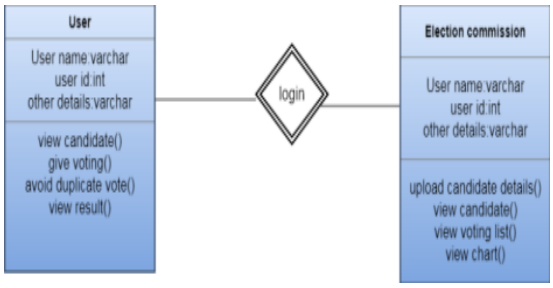


Class Diagram: In software engineering, a class diagram in the Unified Modeling Language (UML) is a type of static structure diagram that describes the structure of a system by showing the system's classes, their attributes, operations (or methods), and the relationships among the classes. It explains which class contains information.

ISSN (Online): 2583-7052

International Journal of Advanced Trends in Engineering and Management (IJATEM)
pp. 132-141

Article Title: Trustworthy Electronic Voting Using Adjusted Blockchain



Activity Diagram: Activity diagrams are graphical representations of workflows of stepwise activities and actions with support for choice, iteration and concurrency. In the Unified Modeling Language, activity diagrams can be used to describe the business and operational step-by-step workflows of components in a system. An activity diagram shows the overall flow of control.

3.2 Modules

Polling Process: The electronic voting system is executed in a way that it deploys many individuals at different levels. In order to develop an effective block creation system, it is important to understand the actual execution on ground. In the conduct of the elections, the election commission and the NADRA (National Database and Registration Authority) have a big role to play. NADRA is the national registration authority in Pakistan and is responsible for the registration and issuance of identity documents to the citizens of Pakistan. The NADRA is responsible to ensure that each citizen of the country has its record available and the biometrics of each individual are also available. The biometric authentication is used in the voter's authentication on the polling day. The election commission is responsible for making the electoral lists available which are verifiable from the base records. The authenticated voters can vote according to the provision provided to them and the usage of technology is made to get the vote recorded and tabulated accordingly. It is also the responsibility of the election commission to declare the results when polling station wise and constituency wise tabulation has been made.

Block Chain: Blockchain has three different types, i.e. public blockchain, private blockchain, and consortium blockchain. Bitcoin and Ethereum are the examples of public blockchain, anyone and from anywhere can join them and can get relieved at the time of his will. This is proofed by the complex mathematical functions. The private blockchain is the internal-public ledger of the company and the joining on that blockchain is granted by the company owning that blockchain. The block construction and mining speed is far better in the private blockchain as compared to public blockchain due to the limited nodes. The consortium blockchain however exists among the companies or group of companies and instead of the consensus the principles of memberships are designated to govern the blockchain transactions more effectively. This research uses consortium blockchain as the blockchain is to be governed by a national authority in the country.

ISSN (Online): 2583-7052

International Journal of Advanced Trends in Engineering and Management (IJATEM)
pp. 132-141

Article Title: Trustworthy Electronic Voting Using Adjusted Blockchain

Hashing: Hashing is the process of changing the arbitrary and variable size input to a fixed size output. There are different functions that perform hashing of different levels. MD5 algorithm is widely used for hashing purposes and it provides a 128 bit or 32 symbols long hash value. MD5 is the latest algorithm in the series while before that Md2, Md3, and Md4 also existed [40]. The algorithm was designed to be used as a cryptographic hashing algorithm but it faces some problems that reduce the production of unique hash value and hence it faces some vulnerabilities. Race Integrity Primitives Evaluation Message Digest (RIPEMD) is a family of hash functions developed by Hans Dobbertin in 1996. This algorithm was designed to replace the MD5 as a more secure alternative. It has a few variations that have emerged over time including RIPEMD-128, RIPEMD-160, RIPEMD256, and RIPEMD-320.

Proofs: In Proof of work deals with the mining / creation of the blocks in such a way that it can be proved that a significant effort has been made for the resolution of the mathematical problem introduced for the creation of a block in the blockchain. The mathematical complexity is increased on the creation of every new block so make the creation of the block complex and a rewarding scenario. The increasing complexity is introduced with the help of the hash functions, merkle trees, and the nonce value. Proof of Stake revolves around the identification of the stakes in the blockchain. The holders of assets are subject to have more priority in the creation of the blocks. The likelihood that only a few creators of the blocks may control the entire blockchain by virtue of the assets that they have, can't be ignored. This concept is applicable in the consortium blockchain or the private blockchain where the holding companies may need administrative access to the blockchain. Proof of Burn n deals with the burning of the coins that are gained over a period of time. This burning process works as a fuel for the creation of new blocks. This proof of burn concept ensures that the individuals don't become powerful enough by increasing their stakes in the network. The burn process is recorded by sending the coins / proof of work to an arbitrary address that may be designated by the network itself.

System testing: The purpose of testing is to discover errors. Testing is the process of trying to discover every conceivable fault or weakness in a work product. It provides a way to check the functionality of components, sub-assemblies, assemblies and/or a finished product. It is the process of exercising software with the intent of ensuring that the Software system meets its requirements and user expectations and does not fail in an unacceptable manner. There are various types of tests. Each test type addresses a specific testing requirement.

3.3 Types of tests

Unit testing: Unit testing involves the design of test cases that validate that the internal program logic functioning properly, and that program inputs produce valid outputs. All decision branches and internal code flow should be validated. It is the testing of individual software units of the application .it is done after the completion of an individual unit before integration. This is a structural testing, that relies on knowledge of its construction and is

ISSN (Online): 2583-7052

International Journal of Advanced Trends in Engineering and Management (IJATEM)
pp. 132-141

invasive. Unit tests perform basic tests at component level and test a specific business process, application, and/or system configuration. Unit tests ensure that each unique path of a business process performs accurately to the documented specifications and contains clearly defined inputs and expected results.

Integration testing: Integration tests are designed to test integrated software components to determine if they actually run as one program. Testing is event driven and is more concerned with the basic outcome of screens or fields. Integration tests demonstrate that although the components were individually satisfaction, as shown by successfully unit testing, the combination of components is correct and consistent. Integration testing is specifically aimed at exposing the problems that arise from the combination of components. Functional test Functional tests provide systematic demonstrations that functions tested are available as specified by the business and technical requirements, system documentation, and user manuals. Functional testing is centered on the following items: Valid Input: identified classes of valid input must be accepted. Invalid Input: identified classes of invalid input must be rejected. Functions: identified functions must be exercised. Output: identified classes of application outputs must be exercised. Systems/Procedures: interfacing systems or procedures must be invoked. Organization and preparation of functional tests is focused on requirements, key functions, or special test cases. In addition, systematic coverage pertaining to identifying Business process flows; data fields, predefined processes, and successive processes must be considered for testing. Before functional testing is complete, additional tests are identified and the effective value of current tests is determined. System Test System testing ensures that the entire integrated software system meets requirements. It tests a configuration to ensure known and predictable results.

Black Box Testing: Black Box Testing is testing the software without any knowledge of the inner workings, structure or language of the module being tested. Black box tests, as most other kinds of tests, must be written from a definitive source document, such as specification or requirements document, such as specification or requirements document. It is a test in which the software under test is treated as a black box you cannot “see” into it. The test provides inputs and responds to outputs without considering how the software works. 6.1 Unit Testing: Unit testing is usually conducted as part of a combined code and unit test phase of the software lifecycle, although it is not uncommon for coding and unit testing to be conducted as two distinct phases. Test strategy and approach Field testing will be performed manually and functional tests will be written in detail. Test objectives all field entries must work properly. Pages must be activated from the identified link. The entry screen, messages and responses must not be delayed. Features to be tested Verify that the entries are of the correct format no duplicate entries should be allowed .All links should take the user to the correct page.

Integration Testing Software integration testing is the incremental integration testing of two or more integrated software components on a single platform to produce failures caused by interface defects. The task of the integration test is to check that components or software

ISSN (Online): 2583-7052

International Journal of Advanced Trends in Engineering and Management (IJATEM)
pp. 132-141

applications, e.g. components in a software system or – one step up – software applications at the company level – interact without error. Test Results: All the test cases mentioned above passed successfully. No defects encountered. 6.3

Acceptance Testing: User Acceptance Testing is a critical phase of any project and requires significant participation by the end user. It also ensures that the system meets the functional requirements. Test Results: All the test cases mentioned above passed successfully. No defects encountered

4 Conclusion

Mistrust in the voting is not an uncommon phenomenon even in developed countries. Electronic voting, however, has emerged as an alternative but still not being practiced at a large scale. Electronic voting is anticipated to have a great future yet the past is not that glorious. In some countries e-voting is not an option while few are in a process to eliminate the security, verifiability, and anonymity concerns. There are issues that require immensely deep consideration by the legislatures, technologists, civil society, and the people. This research has proposed a framework based on the adjustable blockchain that can apprehend the problems in the polling process, selection of the suitable hash algorithm, selection of adjustments in the blockchain, process of voting data management, and the security and authentication of the voting process. The power of blockchain has been used adjustably to fit into the dynamics of the electronic voting process.

Reference

1. EIU the 2017 Democracy Ranking. Accessed: On August 3, 2018. [Translated]. Accessible From: https:/infographics.economist.com/2018/Democracy Index.

2. Science Direct. Democracy Online: An Analysis of Web sites of the New Zealand Community. Accessed: first of August 2018. [Translated]. About: https: /www. science direct. com/article/pii/S0740624X0000033.

3. M. O. Spycher Volkamer; E. Dubuis, Year: 2011, "Measures to Build Confidence in Internet Voting," in Proc. 5 Ins. Admin. Admin. Theory Work. Electron-Electron. Governance, pp. 1-6.

5. E. Bølanger; R. Nadeau, "Multiparty Votes Public Confidence and Voting: Canadian Example," Eur. J. Res. in Diplomacy, Vol: 44, no: 1.