|| Volume 5 || Issue 12 || February 2021 || ISSN (Online) 2456-0774

INTERNATIONAL JOURNAL OF ADVANCE SCIENTIFIC RESEARCH & ET

Multidisciplinary Journal

Double-Blind Peer Reviewed Refereed Open Access International Journal

DIGITAL INDIA DIGITAL VOTING SYSTEM USING ANDROID

Divyansh Paliwal[1], Datta Bhosale[2], Suraj Bargaje[3], Sanket Bhavsar[4], Prof.Vikas Kadam[5]

Dept of Computer Engineering, Savitribai Phule Pune University, Pune, Maharashtra, India[1,2,3,4,5]

--- ***---

Abstract: ***It has long been a challenge to create an electronic voting system that meets legislators' legal requirements. In the field of information technology, distributed ledger technologies is a promising new development. Blockchain systems can be used to benefit from sharing economies in an infinite number of ways. The aim of this paper is to assess how blockchain can be used to incorporate distributed electronic voting systems as a service. The paper elicits the criteria for developing electronic voting systems and addresses the legal and technical drawbacks of implementing such systems using blockchain as a service.***

Keywords: *E Voting, Block Chain, Java, Web, Local Host, Glassfish, JSP, Servlet, Etc*

--- ***---

I INTRODUCTION

For a long time, developing a stable electronic voting system that provides the fairness and privacy of current voting schemes while also offering the openness and versatility of electronic systems has been a challenge. We test an implementation of blockchain as a service to incorporate distributed electronic voting systems in this work-in-progress paper. The paper proposes a new electronic voting system based on blockchain that fixes some of the shortcomings of existing systems and assesses the java programming language's ability to incorporate a blockchain for the purpose of building a blockchain-based e-voting system. In any nation, democratic voting is a crucial and serious case. . The most popular method of voting in a country is on paper, but isn't it time to put voting into the twenty-first century of digital technology? The use of electronic devices to cast ballots, such as voting machines or an internet browser, is known as digital voting. When voting with a computer in a polling station, this is referred to as e-voting, and when voting with a web browser, it is referred to as i-voting. When it comes to implementing a digital voting system, the most important consideration is always security. There should be no question about the system's ability to protect data and defend against future threats when certain important decisions are at stake. The technology of blockchains is one way to potentially address the security issues. The underlying architectural architecture of the cryptocurrency bitcoin gave rise to blockchain technology. It's a type of distributed database in which records are stored as transactions, and a block is a series of transactions. A safe and reliable mechanism for digital voting can be invented using blockchains. This report outlines our vision for using blockchain technology to create a stable digital voting system. Since the 1970s, electronic voting, also known as e-voting, has been used in various ways with fundamental advantages over paper-based systems, including improved reliability and decreased errors. However, there are still obstacles to widespread adoption of such systems, especially in terms of improving their resilience to potential faults. Blockchain is a cutting-edge technology that has the potential to increase the overall resilience of electronic voting systems. The aim of this paper is to use the benefits of blockchain, such as cryptographic foundations and transparency, to create an efficient evoting scheme. The proposed scheme meets the basic criteria for electronic voting systems and achieves end-to-end verifiability. The proposed e-voting scheme is defined in depth, as well as its implementation on the Multichain platform. The paper provides an in-depth analysis of the scheme, demonstrating its efficacy in achieving an end-to-end verifiable e-voting system.

II LITERATURE SURVEY:

1.Satoshi Nakamoto Bitcoin: A Peer-to-Peer Electronic Cash System A purely peer-to-peer version of electronic cash would allow online payments to be sent directly from one party to another without going through a financial institution. Digital signatures provide part of the solution, but the main benefits are lost if a trusted third party is still required to prevent double-spending. We propose a solution to the double-spending problem using a peer-to-peer network. The network timestamps transactions by hashing them into an ongoing chain of hash-based proof-of-work, forming a record that cannot be changed without redoing the proof-of-work. The longest chain not only serves as proof of the sequence of events witnessed, but proof that it came from the largest pool of CPU power. As long as a majority of CPU power is controlled by nodes that are not cooperating to attack the network, they'll generate the longest chain and outpace attackers. The network itself requires minimal structure. Mes- sages are broadcast on a best effort basis, and nodes can leave and rejoin the network at will, accepting the longest proof-of-work chain as proof of what happened while they were gone.

2.Christopher D. Clack, Smart Contract Templates: foundations, design landscape and research directions. In this position paper, we consider some foundational topics regarding smart contracts (such as terminology, automation, enforceability, and semantics) and define a smart contract as an agree- ment whose execution is both automatable and enforceable. We explore a simple semantic framework for smart contracts, covering both operational and non-operational aspects. We describe templates and agreements for legally- enforceable smart contracts, based on legal documents. Building upon the Ricardian Contract triple, we identify operational parameters in the legal documents and use these to connect legal agreements to standardised code. We also explore the design landscape, including increasing sophistication of parame- ters, increasing use of common standardised code, and long-term academic research. We conclude by identifying further work and sketching an initial set of requirements for a common language to support Smart Contract Templates.

3.EppMaaten, Towards remote e-voting: Estonian case This paper gives an overview about the Estonian e-voting system. Paper discusses how the con- cept of e-voting system is designed to resist some of the main challenges of remote e-voting: secure voters authentication, assurance of privacy of voters, giving the possibility of re-vote, and how an e-voting system can be made comprehensible to build the public trust.

4.Paul Gibson, A review of E-voting: the past, present and future Elec- tronic voting systems are those which depend on some electronic technology for their correct functionality. Many of them depend on such technology for the communication of election data. Depending on one or more communica- tion channels in order to run elections poses many technical challenges with respect to verifiability, dependability, security, anonymity and trust. Changing the way in which people vote has many social and political implications. The role of election administrators and (independent) observers is different different when complex communications technology is involved in the pro- cess. Electronic voting has been deployed in many different types of election throughout the world for several decades.

5.Muhammad Ajmal Azad, M2M-REP: Reputation of Machines in the In- ternet of Things 2017. The Internet of Things (IoT) is the integration of a large number of autonomous heterogeneous devices that report information from the physical environment to the monitoring system for analytics and meaningful decisions. The compromised machines in the IoT network may not only be used for spreading unwanted content such as spam, malware, viruses etc, but can also report incorrect information about the physical world that might have a disastrous consequence. The challenge is to design a collabora- tive reputation system that calculates trustworthiness of machines in the IoT- based machine-to-machine network without consuming high system resources and breaching the privacy of participants. To address the challenge of privacy preserving reputation system for the decentralized IoT environment, this pa- per presents a novel M2M-REP (Machine to Machine Reputation) system that computes global reputation of the machine by aggregating the encrypted local feedback provided by machines in a fully decentralized and secure way

6.KashifMehboob Khan Secure Digital Voting System based on Blockchain Technology. Electronic voting or e-voting has been used in varying forms since 1970s with fundamental benefits over paper based systems such as increased efficiency and reduced errors. However, there remain challenges to achieve wide spread adoption of such systems especially with respect to im- proving their resilience against potential faults. Blockchain is a disruptive technology of current era and promises to improve the overall resilience of e- voting systems. This paper presents an effort to leverage benefits of blockchain such as cryptographic foundations and transparency to achieve an effective scheme for evoting. The proposed scheme conforms to the fundamental re- quirements for e-voting schemes and achieves end-to-end verifiability. The paper presents details of the proposed e-voting scheme along with its imple- mentation using Multichain platform.

III. PROPOSED SYSTEM:

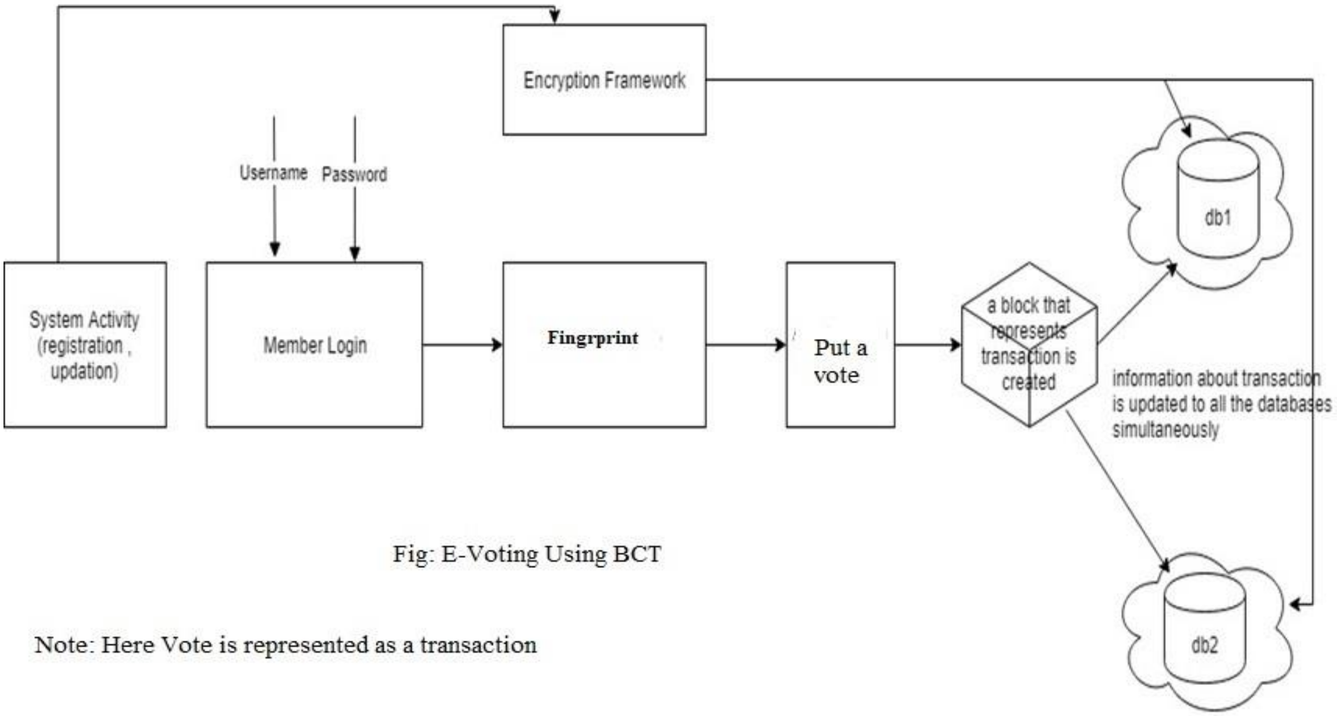
Encryption Framework
Username
Password
System Activity (registration , updation)
Member Login
Fingrprint
Put a vote
a block that represents transaction is created
information about transaction is updated to all the databases simultaneously
db1
db2

Fig: E-Voting Using BCT

Note: Here Vote is represented as a transaction

Algorithm:

AES:

AES is used to encrypt the database. The encryption process uses a set of specially derived keys called round keys. These are applied, along with other operations, on an array of data that holds exactly one block of data, the data to be encrypted. This array we call the state array.

STEPS:

_ Derive the set of round keys from the cipher key.

_ Initialize the state array with the block data (plaintext).

_ Add the initial round key to the starting state array.

_ Perform nine rounds of state manipulation.

_ Perform the tenth and final round of state manipulation

_ Copy the final state array out as the encrypted data (ciphertext).

SHA 256:

SHA-256 (secure hash algorithm, FIPS 182-2) is a cryptographic hash function with digest length of 256 bits. It is a keyless hash function; that is, an MDC (Manipulation Detection Code). A message is processed by blocks of 512 = 16 32 bits, each block requiring 64 rounds A cryptographic hash (sometimes called digest) is a kind of signature for a text or a data file. SHA-256 generates an almost-unique 256-bit (32-byte) signature for a text.A hash is not encryption it cannot be decrypted back to the original text (it is a one-way cryptographic function, and is a fixed size for any size of source text). This makes it suitable when it is appropriate to compare hashed versions of texts, as opposed to decrypting the text to obtain the original version.

IV. CONCLUSION:

Hence digital India digital Voting system will be implemented using fingerprint , AES and block chain. The system will maintain transparent records of voting in the block chain format which will be implemented using SHA

256. Java programming language will be used to developa prototype model for voting system.

REFERENCES:

1. Ahmed Ben Ayed,A Conceptual Secure Block Chain-Based Electronic Voting System,2017 IEEE International Journal of network&Its Applications(IJNSA),03 May 2017[1].

2. RifaHanifatunnisa, Budi Rahardjo, Blockchain Based E-Voting Recording System Design,IEEE 2017[2].

3. Kejiao Li, HuiLi,HanxuHou, KedanLi,Yongle Chen, Proof of Vote: A High- Performance Consensus Protocol Based on Vote Mechanism & Consortium Blockchain, 2017 IEEE 19th International Conference on High Performance Computing and Communications; IEEE 15th International Conference on Smart City; IEEE 3rd International Conference on Data Science and Systems[3].

4.Ali KaanKo, EmreYavuz, Umut Can abuk, GkhanDalkilic, Towards Secure E-Voting Using Ethereum Blockchain,2018 IEEE[4].

5. Supriya Thakur Aras, Vrushali Kulkarni, Blockchain and Its Applications A Detailed Survey, International Journal of Computer Applications (0975 8887) Volume 180 No.3, December 2017[5].