ISSN (Online) 2394-2320

International Journal of Engineering Research in Computer Science and Engineering (IJERCSE)

Volume 11 Issue 7 July 2024

E-voting System using Blockchain

[1] Anukriti Singh, [2] Dr. Dharmendra Yadav, [3] Aditya Ruhela

[1] M. Tech student, Department of CSE, BTU, Bikaner, Rajasthan, India
[2] Professor, Department of CSE, UCET, Bikaner, Rajasthan, India
[3] M. Tech student, BITS Pilani Bikaner Technical University Rajasthan India
Corresponding Author Email: [1] anukriti.singh909@gmail.com, [2] dyadav@cet-gov.ac.in

Abstract*— World is facing a problem fair election. Voting is a biggest challenge for democratic country administration and it is important to safeguards are rights. That is why we need guarantee and security to cast our votes. All the world are digitalized through the integration of technology solution for that one of the best solutions is blockchain. Blockchain is technology to safeguards that type of risk and give safety and also prevention of our data. In this digital era data is everything blockchain are two type public and private key. We have to focus that each voter having uniquely identified by government to approved aadhar number. This application is makes sure that one number is use only one time in the system. Then after cast their vote it make sure that peers get synch up. Then it generated the hash key. In this paper you ensure that blockchain is having so many characteristics like data confidentiality, data integrity and data authenticity. One of those decentralized systems are blockchain technology. That to offer users and developers a broad view of the risks and opportunities associated with blockchain in the e-voting system.

***Index Terms*—electronic voting, blockchain e-voting, authentication, transparency.**

I. INTRODUCTION

The biggest challenge for all the country fair and honest election and some countries are using traditional method of election like ballot paper and EVM (electronic voting machine). But in modern era many countries are using digitalization voting process through blockchain they are also called e-voting system [1]. The first country started E-voting system is Estonia in 2005. The country citizens having national identification card (ID Card) them contain encrypted data which are help to verifying the identity owner. Like we can sign-in with phone also for the voter friendly it can SIM Card authenticate for Mobile-ID [2-3]. We need save and secure election like risk free crowds reached polling station safety in remote area also. election is costly and subject of voters' intimidation it has a most of the chance to human error also. It has less transparent. Government spends lot of time and money which we use that to development of our nation [4]. That is a reason their save their time and resource through Blockchain. Blockchain used hash block header block n then block n+1 then block n+2 their switch to previous block and other previous block to block n header again the verifying that it is peer to peer [P2P]. A blockchain is a digital ledger of transactions that is duplicated and distributed across the entire network of computer systems on the blockchain. It is a system of recording information in a way that makes it difficult or impossible to change, hack, or cheat the system. Blockchain consists of a very important concept called blocks. Blocks every chain consists of multiples blocks and each block has three basic elements. Data (i.e. transactions), the hash of the previous block and the block hash value. Hash value is a unique value, identifying one block. It depends on the blocks content (data and previous block hash), so each block has its unique hash value, and it's identifying this block only.

Therefore, each block can reference or point to the block before, which means the four-block is taking a reference to the third one is taking a reference to the second, and so on and thus a chain of block is formed which we call as blockchain. The key element that make blockchain immutable is cryptographic hashes, which is why blockchain is immutable. Comparison of traditional, electronic and blockchain e-voting system. Election is the process through which people can express their political opinion. Their cast public vote to choose a political leader. Voting is given the right to select any party's person whose you want to give a chance to your leader or representative those who get majority of vote he or she is new representatives in that particular area or constituency. Voting provides solutions in different fields like business, electing the CEOs and students' union president election etc. In Indian across any citizen whose age 18 year there getting opportunity for right to vote. On the election day, government employees are appointed as election officer to take responsibility to do fair and transparent election. Traditional Voting is done by manually that time election is held to put seal on the party symbol to cast their vote and drop the stamped slip into the ballot box. then box sealed locked in the voting center to counting center and their starting counting by opening the ballot boxes and separating according to their slips to the parties. After that vote counting in different center, they are adding up and then declared highest number of votes in the constituency and declared the winning name. this process in centralized monitored, maybe if single point of error occurs. We only trust the counting officers should be considered. If any human error is occurred it could be a biggest difference in future. And fake voting is also happened that is why we need technology. For overcome that we use EVM it is a

ISSN (Online) 2394-2320

International Journal of Engineering Research in Computer Science and Engineering (IJERCSE)

Volume 11 Issue 7 July 2024

breakthrough in India. These EVMs is required no manual voting. EVM is free for human error. Now these day EVM is facing problem with the trust of centralized authority is left like hacking issues is also occurs. That is why we need decentralized system like blockchain. Blockchain technology is over the trust issue too. In blockchain voting your data is secure and save we don't need extra security it is less time consuming. It is cheaper than other traditional methods. Blockchain technology has been present since the 80s, only one reason why this technology is more talked about these days is due to bitcoin. Bitcoin was developed in 2009, now this day bitcoin is most popular because of blockchain. It is secure trustworthy in long time. Blockchain technology implement into e-voting system, all the votes can be recorded, managed, counted, checked, verified by the votes themselves and even. protecting the voter identity and privacy.

II. BACKGROUND REVIEW

A blockchain is a distributed, peer-to-peer database that hosts a continuously growing number of transactions. Each transaction, referred to as a 'block', is secured through cryptography, time stamped, and validated by every authorized member of the database. Blockchain is the underlying technology behind all crypto currencies. Blockchain lays the foundation for many concepts like Smart Contracts, Non-Fungible Tokens (NFTs), etc. Blockchain has spread its applications to medical fields, Logistics and supply Management and many others. In these new technologies world is integrated into our daily life, such as smart phone and social applications and the smart city, smart transportations and smart grids, smart home based on the internet of things (IOT) for that large amount of data will be collected. The world entered the era of big data, the trend of the times and the inevitable demand of the market data sharing and trading now these days world pay more and more attention to the economic value of big data in improving the utility efficiency and the decision making the customer experience and other aspect some third-party big data trading centers have been established. The growth of data a large extend demands, the data trading centers provide the data owners and the data purchasers with the interconnected space. The hosting mode, which depend on the trusted third parties to. One of the biggest cybersecurity issues faced by individual's computer users as well as corporate firms is data theft, not only because it threatens an individual's privacy, but also because it defeats one of the primary purposes of cybersecurity, i.e., Confidentiality. Over the last few decades, several techniques have been proposed to deal with the issue, and many of them have been short lived, the reason being highly skilled cyber criminals. The latest addition is the Blockchain Technology. Data dispersed over the network is prone to pilferage and plagiarism and often it is impossible to trace back to the cybercriminal. Blockchain technology eliminates the issue on many levels.

A blockchain may be defined as a distributed database incorporating information or a book that marks all the events and transactions, executed and shared among concerned parties. The transactions are verified and information entered can never be erased. Every transaction made had a verifiable record. Blockchain Technology finds its use in financial as well as non-financial sectors. Blockchains are public registers such that all transactions are accumulated in list of blocks [1]. When several blocks keep on adding, it leads to a chain like formation. Blockchain Technology is primarily based on the concept of Cryptography and Distributed Systems. Encryption techniques have been known to obscure content, such that it is available only to the intended users. But certain information needs to be available to specific groups of people, and it invites additional risk of the information getting manipulated. Blockchains tackle the issue. When data is accessed and updated, any change made is recorded and verified. Thereafter, it is encrypted so that further changes cannot be made. These changes are then updated into the main records. It is a repetitive process and every time a change is made, the information is preserved in a new block. It is fascinating to note that the first version of the information is well connected to the latest one. Thus, the changes made could be seen by everyone, but only the latest block can be modified. Blockchain imitates a distributed database by incorporating information duplicated across the network in real time. This means that the database has multiple locations and the records are public and easily verifiable. Since there is not centralized version, data corruption is futile. Modifying records is tedious, thus making it easier to detect if someone is trying to do so. Thus, a blockchain could be thought of as a piece of data that has the following properties.

A. Type of Blockchain-

1.Public blockchain networks- A public blockchain is one that anyone can join and participate in, such as Bitcoin. Drawbacks might include substantial computational power required, little or no privacy for transactions, and weak security. These are important considerations for enterprise use cases of blockchain.

2.Private blockchain networks- A private blockchain network, similar to a public blockchain network, is a decentralized peer-to-peer network. However, one organization governs the network, controlling who is allowed to participate, execute a consensus protocol and maintain the shared ledger. Depending on the use case, this can significantly boost trust and confidence between participants. A private blockchain can be run behind a corporate firewall and even be hosted on premises.

3.Permissioned blockchain networks- Businesses who set up a private blockchain will generally set up a permissioned blockchain network. It is important to note that public blockchain networks can also be permissioned. This places restrictions on who is allowed to participate in the network

ISSN (Online) 2394-2320

International Journal of Engineering Research in Computer Science and Engineering (IJERCSE)

Volume 11 Issue 7 July 2024

and in what transactions. Participants need to obtain an invitation or permission to join.

4.Consortium blockchain networks- Multiple organizations can share the responsibilities of maintaining a blockchain. These pre-selected organizations determine who may submit transactions or access the data. A consortium blockchain is ideal for business when all participants need to be permissioned and have a shared responsibility for the blockchain.

III. BLOCKCHAIN

In E-voting personal identity information is held on a blockchain, that puts us just one step away from also being able to vote using blockchain technology. Using blockchain technology can make sure that nobody votes twice, only eligible voters are able to vote, and votes cannot be tampered with. What's more, it can increase access to voting by making it as simple as pressing a few buttons on your smartphone. At the same time, the cost of running an election would substantially decrease. They began by establishing the challenges that e-voting applications face: privacy, lack of evidence, fraud resistance, ease of use, scalability, speed, and evidence, fraud resistance, ease of use, speed and cost. That applications are set to compare e-voting for believed all aspect to create a robust system. In the blockchain technology user cryptographic digital signatures, hash function and blockchain algorithm designed free to maintain the integrity of all blockchain.

A. Hash functions in Blockchain-

The process of scrambling a piece of information or data beyond recognition. They are designed to be irreversible. We pass the input through a hash function to calculate the hash value or digest. Hash function is real-world implementation the same user tries to log-in, the password they input is passed through the function again and the digest is compared to the one stored on the servers. If the re-calculated hash matches the hash stored on the servers during initial sign-up, the log-in s allowed. If the calculated digest is different from the one on the server, the login is denied from the website. Hashing can also be used for integrity checks to ensure the data isn't corrupted. The hash value/digest will always be the same for similar input. Mathematical operations to be carried out on two blocks of data. Both blocks are created by dividing the initial input equal parts and irreversible by design. Can be carried out multiple times, but the final digest must be consistent for the same input.

Hash Algorithm		Digest Size
MD5	----	128 bits
SHA-256	----	256 bits

Hash function must be fast, but not instantaneous should be able to hash in-mass with a reasonable limit to prevent exploitation. Ultra quick algorithms can be tested rigorously for brute force attacks. With enough brute force attacks, not just the hash, entire algorithm can be cracked. Hash digest must be dependent on each bit. If a single character changes, a substantial portion of the digest must change. Helpful in creating as many unique hashed as possible. Hash digest for the plaintext 'Cryptography" will be completely different than when the plaintext "cryptograph".

Voters Plaintext -- Block Hash -- Hash Value

E-voting two votes having same password then it is preventing hash collision there are two exactly same hash values/digests. there is only one hash function for each server, same passwords have same digests after hashing. Salting can help prevent collisions, as we will learn later in this lesson. Mostly common passwords used. In voter having same password we use salting. Salting is process to adding random keyword. Salting is generated unique for every voter in database and is helpful to battle hash collision. Otherwise, if sever is hack then we already used peppering is process to adding the same random value at the voter plaintext. It doesn't change per user, the random value need not be stored on server, the case of data breach, pepper value is safe from further exploitation.

Input into hash function	hash value/Digest
CryptographyRam123	ASDGHKN23459
MyPasswordRam123	ASDFGHKHD675
Werty101Ra123	ATYHJKI2309876

B. Platform for E-voting

E-voting is developing using blockchain we used Ethereum. Ethereum is a most popular platform for creating distribute blockchain applications that support smart contracts. Ether is the native cryptocurrency of the platform. We also used the smart contracts are self-executing contracts which contain the terms and conditions of agreement between peers. They are simply programs stored on a blockchain that run when predetermined conditions are met. They typically are used to automate the execution of an agreement so that all participants can be immediately certain of the outcome, without any intermediary's involvement or time loss. Smart contract eradicates the need for a third-party intermediary of facilitator, essentially giving you full control of the agreement. Smart contract is basically self-executing contract which contain term and condition these are main driving code of blockchain that we developing Ethereum. It is developing using language is solidity. Solidity is a contract-oriented, high-level language for implementing smart contract. It is statically typed, supports inheritance, libraries and complex user-defined types among other features. MetaMask is a wallet that we required snice we know everything happened blockchain is transition we will be will be required a daily life example like Paytm and Phone pay etc. for transaction we required a wallet to handle a cryptocurrency. For performing any transaction on the blockchain we required an account which will have unique account address. This can be created by using the MetaMask chrome extension. MetaMask is a crypto wallet & gateway to

ISSN (Online) 2394-2320

International Journal of Engineering Research in Computer Science and Engineering (IJERCSE)

Volume 11 Issue 7 July 2024

blockchain apps. It generates passwords (in the form of mnemonic) and keys on your device, so only you have access to your accounts and data. It helps users in interacting with the blockchain network.

C. Ganache-

Since working with the main Ethereum network costs actual money for transactions, we are using a local RPC "Ganache". Ganache is a local test network for rapid Ethereum and distributed application development. It can be used across the entire development cycle; enabling us to develop, deploy, and test our dApps in a safe and deterministic environment. It provides us 10 accounts each having 100 ethers for testing purpose.

D. Framework-

Now to interact with our compiled smart contract in a hassle-free manner we use Truffle suite. Truffle is the most popular development framework for Ethereum which makes lots of work easier. This generates an artifact which plays an important role in the successful deployment of our application. It takes care of managing our contract artifacts so we don't have to include support for custom deployments, library linking etc. user is link to the application binary interface is link smart contract truffle is compile through both link with byte code and application binary interface to make a call to a function deployed on network and byte code truffle migrate to deployed on network. we proposed a smart contract-based framework to implement distributed and trustworthy access control. The framework includes multiple access control contracts (ACCs) for access control of multiple subject-object pairs in the system, one judge contract (JC) for judging the misbehavior of the subjects during the access control, and one register contract (RC) for managing the ACCs and JC. A case study was also provided for the access control in blockchain system with one desktop computer, one laptop and two Raspberry Pi single-board computers. The case study demonstrated the feasibility of the proposed framework in achieving distributed and trustworthy access control Blockchain.

IV. RESULT-

In this method we take blockchain mechanisms its simple, fair and transparent. Because of this method people believed government and maybe voting rate should be high in this method. Its save and time save and error free no other central interfere the vote received by the system must be accurate, and every vote casted must be counted and cannot be duplicate or changed or removed. Any tampering of the ballot should be detected by the proposed system and immediately flag the malicious vote. This guarantees the integrity of each block as it would be fairly easy to detect any tampering of vote. E- voting is secure & private and potentially more transparent and scalable. There are immutable records and faster vote count.

V. CONCLUSIONS-

In conclusion, we proposed a blockchain-based electronic voting protocol in this paper. Blockchain is an electronics era and general all the youth and adult are using technology it is easily to understand that method and technology to verification the process of blockchain. Blockchain technology properties to enhance its security features. This system is ensuring all voter results recorded are tamper-proof. E-voting system such as authenticity, integrity, verifiability, anonymity, availability and a general consensus from every participant. The system does not rely on human trust but on computational cryptographic trust. Blockchain voting is secure and hack free that no one is able to corrupt it.

REFERENCES

[1] Clement Chan Zheng Wei#, Chuah Chai Wen# # Faculty of Computer Science and Information Technology, University Tun Hussein Onn Malaysia, Malaysia E-mail: clementchan 1996cc@gmail.com

[2] D. P. Moynihan, "Building secure elections: E-voting, security, and systems theory," Public Administration Review, vol. 64, no. 5. pp. 515–528, 2004.

[3] G. Zyskind, O. Nathan, and A. S. Pentland, "Decentralizing privacy: Using blockchain to protect personal data," in Proceedings - 2015 IEEE Security and Privacy Workshops, SPW 2015, 2015, pp. 180–184.

[4] A. Ben Ayed, "A Conceptual Secure Blockchain Based Electronic Voting System," Int. J. Netw. Secur. Its Appl., vol. 9, no. 3, pp. 01– 09, 2017.

[5] G. Z. Qadhi and R. Taha, "Electronic voting systems: Requirements, design, and implementation," Compute. Stand. Interfaces, vol. 29, no. 3, pp. 376–386, 2007.

[6] M. Rudner, "The Malaysian General Election of 1969: A Political Analysis1," Mod. Asian Stud., vol. 4, no. 1, pp. 1–21, 1970.

[7] D. Springall et al., "Security Analysis of the Estonian Internet Voting System," in Proceedings of the 2014 ACM SIGSAC Conference on Computer and Communications Security - CCS '14, 2014, pp.703–715.

[8] J. A. Halderman and V. Teague, "The New South Wales iVote system: Security failures and verification flaws in a live online election," in Lecture Notes in Computer Science (including subseries Lecture Notes in Artificial Intelligence and Lecture Notes in Bioinformatics), 2015, vol. 9269, pp. 35–53.

[9] M. P. Evans and S. M. Furnell, "Internet-based security incidents and the potential for false alarms," Internet Res., vol. 10, no. 3, pp. 238–245,2000.

[10] J. Hoff stein, J. Pipher, and J. H. Silverman, An Introduction to Cryptography, vol.XVI.2008.