Secure-Voting System Using Blockchain Technology

Rahul Singh, Khema Raul, Manisha, Vrushali Shivsharan, Prof. Pooja Kadam
[#12]Department of Information Technology
Dhole Patil College of Engineering, Near EON IT Park,
Vitthal Nagar, Kharadi, Pune, Maharashtra 412207.

Abstract: An Online voting protocol provides transparency to the voter that their vote was correctly counted and any party can verify the results of the election. There have been several proposals outlining potential systems, however these have all been built on top of protocols primarily designed as transaction ledgers. In this paper I propose a voting solution, built on the Ethereal protocol, that uses the properties of smart contracts to enforce strict rules surrounding the ballots of an election. These ballots are both independently and universally verifiable and maintain all of the desirable properties of the block-chain (such as immutability). All of this is achieved without sacrificing voter privacy or ballot integrity. The resulting system shows clear potential for Blockchain technology to become a central part of applications wishing to provide transparency and security in public scenarios.

Keywords: Blockchain; secured; intelligence system; voting system;

I. INTRODUCTION

Online Voting System provides the online registration form for the users before voting and makes the users to cast their vote online. The system is to be developed with high security and user friendly. It reduces manual efforts and bulk of information can be handled easily.

Blockchain is based on distributed data structure which shares information among the members across the network. A blockchain is a database shared by every participant in a given system. The block chain stores the complete transaction history of a cryptocurrency or other record keeping system.

Blockchain is a sequence of blocks, which holds a complete list of transaction records like conventional public ledger With a previous block hash contained in the block header, a block has only one parent block.[7] It is worth noting that uncle blocks (children of the blocks ancestors) hashes would also be stored in ethereum blockchain. The first block of a blockchain is called genesis block which has no parent block.

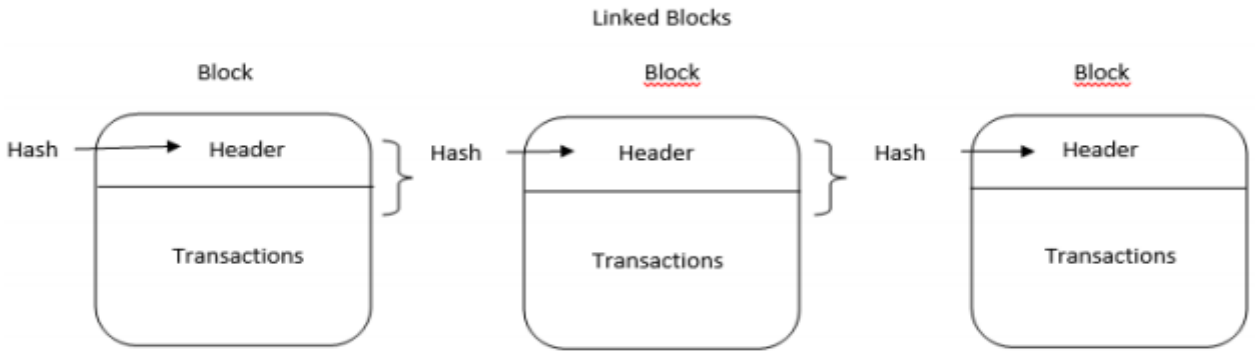


Figure 1: The transaction process of blockchain

Block: A block consists of the block header and the block body. In particular, the block header includes:

- Block version: indicates which set of block validation rules to follow.
- Merkle tree root hash: the hash value of all the transactions in the block.
- Timestamp: current time as seconds in universal time since Jan-uary 1, 1970.
- nBits: target threshold of a valid block hash.
- Nonce: an 4-byte eld, which usually starts with 0 and increases for every hash calculation
- Parent block hash: a 256-bit hash value that points to the previous block

Bit coin introduced the concept of blockchain basically to overcome the issue of double spending problem. A user requests for a transaction. A block is created representing the transaction. After that it is broadcasted to all the nodes of the network.

A. Blockchains: Private Vs. Public

A typical blockchain system consists of multiple nodes which do not fully trust each other. Some nodes exhibit Byzantine behavior, but the majority is honest. Together, the nodes maintain a set of shared, global states and perform transactions modifying the states. Blockchain is a special data structure which stores historical states and transactions. All nodes in the system agree on the transactions and their order. Figure 1 shows the blockchain data structure, in which each block is linked to its predecessor via a cryptographic pointer, all the way back to the first (genesis) block. Because of this, blockchain is often referred to as a distributed ledger.

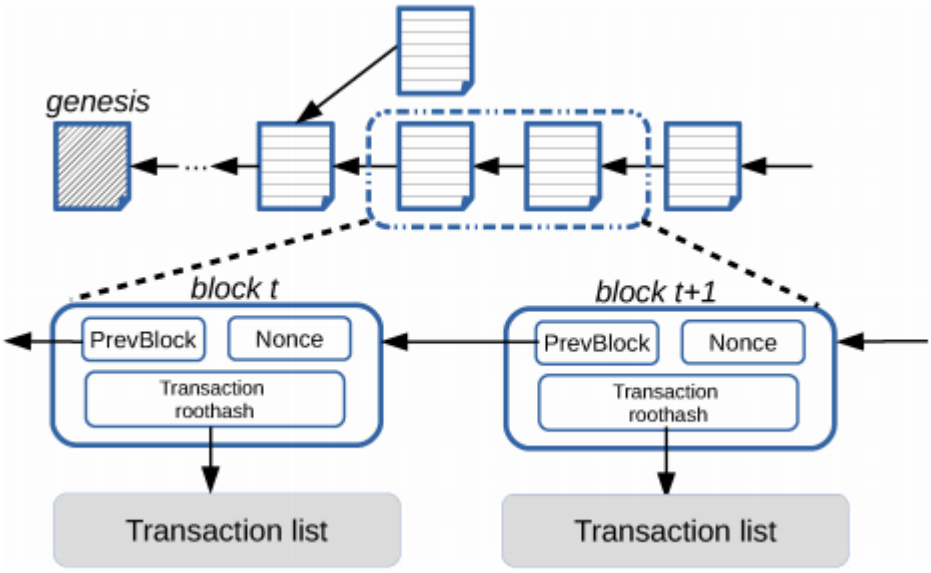


Fig. 2: Blockchain data structure. Transactions are packed into blocks which are linked to previous blocks.

II. LITERATURE SURVEY

Zibin Zheng, Shaoan Xie, Hongning Dai, Xiangping Chen, and Huaimin Wang, "An Overview of Blockchain Technol-ogy: Architecture, Consensus, and Future Trends": has laid down the above diagram for the architecture of the blockchain. And it has also stated the below de nition of the same. Blockchain is a sequence of blocks, which holds a complete list of transaction records like conventional public ledger. There is a previous block that contains the hash in the block header, a block has only one parent block. The rest block of a blockchain is called genesis block which has no parent block. Then the internal blocks of the blockchain are explained in detail. Key characteristics of the system are also listed down in Namely, (a) Decentralization (b) Persistency (c) Anonymity (d) Auditability

2. Tien Tuan Anh Dinh, Rui Liu, Meihui Zhang, "Untangling Blockchain: A Data Processing View of Blockchain Systems.": has the comparison of the different blockchain techniques and its comparison with related to the performance using the BLOCKBENCH. This tool loads the different blockchains in the backend of the frame-work by implementing an interface IBlockchain- Connector and front end to load the workloads by implementing the interface of IWorkload-Connector. Here, we survey the state of the art, focusing on private blockchains involving party authentication it analyze systems in four dimensions: (a) Distributed Ledger (b) Cryptography (c) Smart Contract (d) Consensus Protocol

3. Florian Tschorsch Bjurn Scheuermann, "Bitcoin and Beyond: A Technical Survey on Decentralized Digital Currencies":It has unroll and structure the manyfold results and research directions. We start by introducing the Bitcoin protocol and its building blocks. From there they have continued to explore the design space by discussing existing contributions and results. In the process, we deduce the fundamental structures and insights at the core of the Bitcoin pro-tocol and its applications. It has also shown and discussed, many key ideas that are likewise applicable in various other elds, so that their impact reaches far beyond Bitcoin itself has laid down various protocols used by the miners by bitcoin. The protocols used is of the proof of work to prevent Sybil attacks. Before verifying a transaction and spreading the news about it, participants have to perform some work to proof they are real identities. The work consists of a cryptographic puzzle, which artificially increases the computational cost to verify transactions. Thereby, the ability of verification depends on the computing power, and not on the number of (potentially fake) identities.

4. Massimo Di Pierro, DePaul University, "What Is Blockchain": It has proposed a system for electronic transactions without relying on trust. They started with the usual framework of coins made from digital signatures, which provides strong control of ownership, but is incomplete without a way to prevent double-spending. The network is robust in its unstructured simplicity. Nodes work all at once with little coordination. They do not need to be identified, since messages are not routed to any particular place and only need to be delivered on a best e ort basis. Nodes can leave and rejoin the network at will, accepting the proof-of-work chain as proof

of what happened while they were gone. They vote with their CPU power, expressing their acceptance of valid blocks by working on extending them and rejecting invalid blocks

III. CRYPTOGRAPHY CONCEPT

Blockchain systems make heavy use of cryptographic techniques to ensure integrity of the ledgers. Integrity here refers to the ability to detect tampering of the blockchain data. This property is vital in public settings where there is no pre-established trust. For example, public confidence in crypto-currencies like Bitcoin, which determines values of the currencies, is predicated upon the integrity of the ledger; that is the ledger must be able to detect double spending. Even in private blockchains, integrity is equally essential because the authenticated nodes can still act maliciously.

There are at least two levels of integrity protection.

First, the global states are protected by a hash (Merkle) tree whose root hash is stored in a block. Any state change results in a new root hash. The tree's leaves contain the states, the internal nodes contain the hashes of their children. For instance, Hyperledger v0.6 uses a bucket hash tree, in which states are grouped (by hashing) into a pre-defined number of buckets. Ethereum, on the other hand, employs a Patricia-Merkle tree which resembles a tries and whose leaves are key-value states.

Second, the block history is protected, that is the blocks are immutable once they are appended to the blockchain. The key technique is to link the blocks through a chain of cryptographic hash pointers: the content of block number n + 1 contains the hash of block number n. This way, any modification in block n immediately invalidates all the subsequent blocks. By combining Merkle tree and hash pointers, blockchain offers a secure and efficient data model that tracks all historical changes made to the global states.

Field	Description	Size
Block size	The size of the whole block	4 bytes
Block Header	Encrypted almost unique Hash.	80 bytes
Transaction	Contains the transaction saved in the bolck	Depends on the transaction size.

Table 1: Structure of the Blockchain

III. SYSTEM ARCHITECTURE

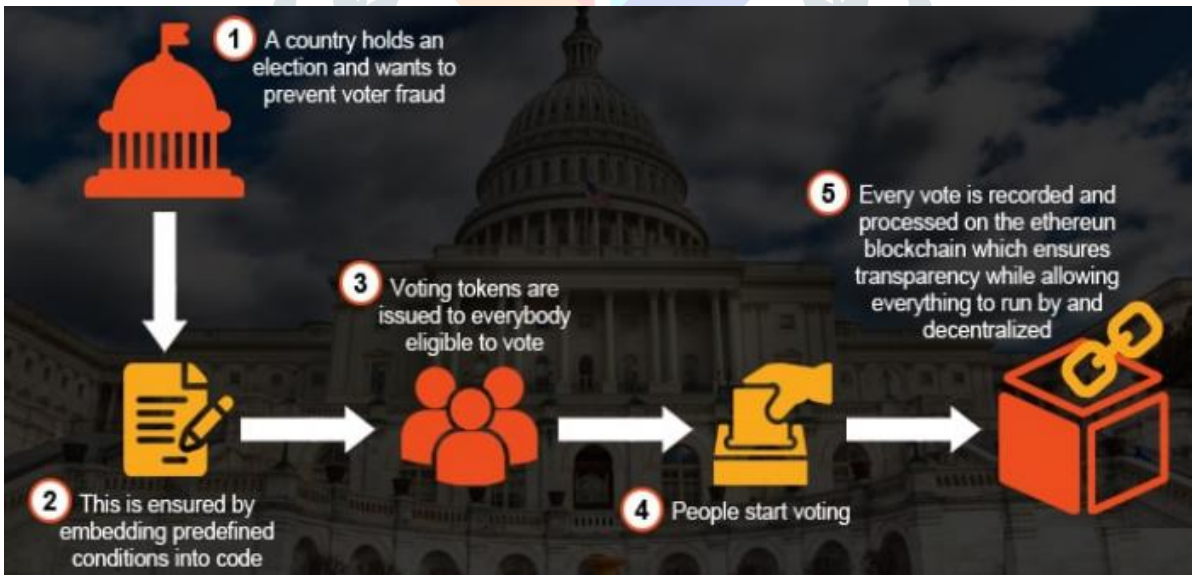


Fig 3. System architecture

IV. METHODOLOGY

Algorithm 1: MD5 Algorithm:

Algorithm:
Step 1. Append Padding Bits. The message is "padded" (extended) so that its length (in bits) is congruent to 448, modulo 512.
Step 2. Append Length.

Step 3. Initialize **MD** Buffer.

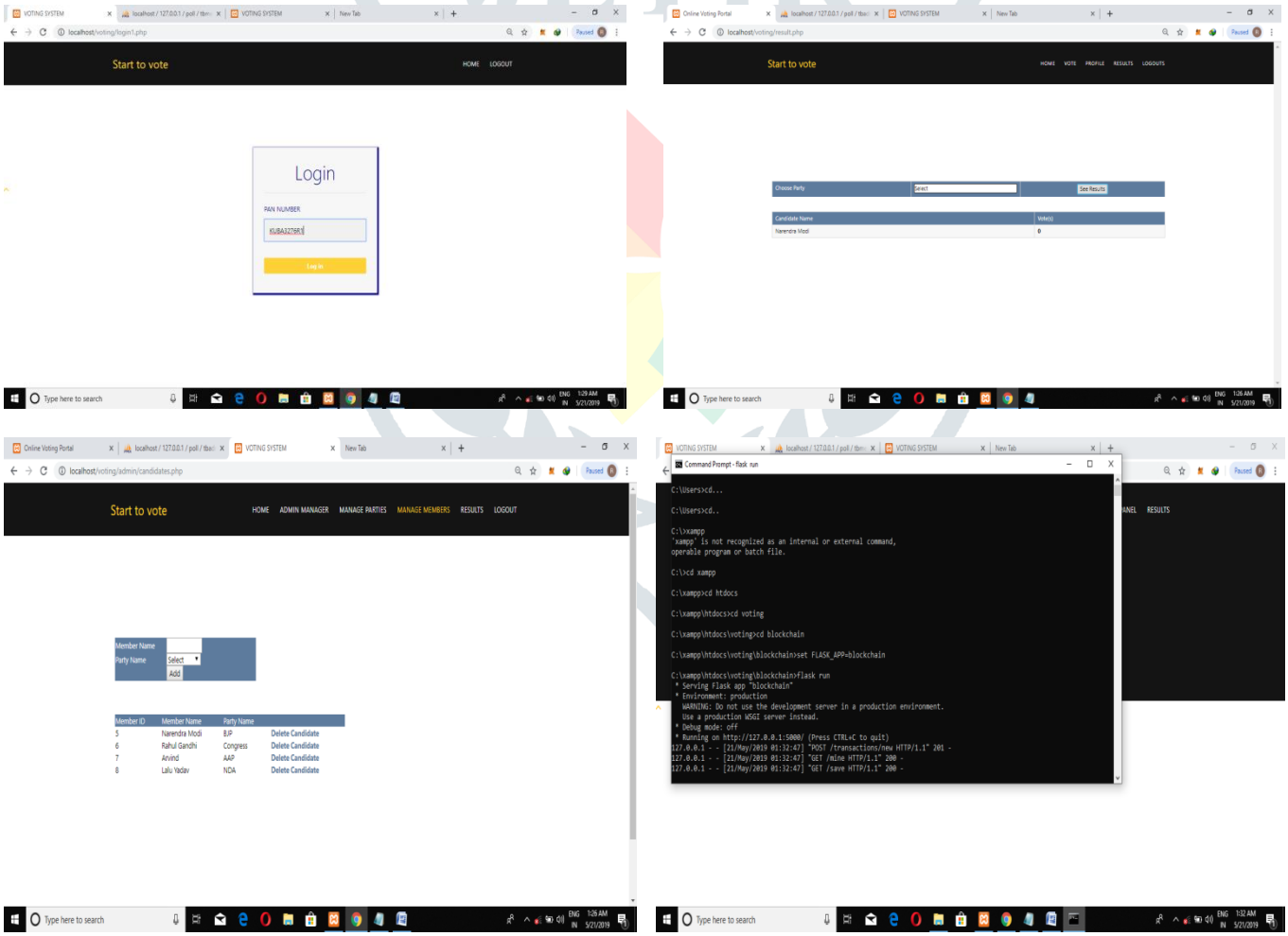
Step 4. Process Message in 16-Word Blocks.

Step 5. Output.

Algorithm 2: SHA Algorithm:

START
Step 1- U=Upload (Data)
Step –2 R=Read () voter Data
Step –3 C(U,R)=Cloud server read uploaded voter data
Step- 4 Check calculate hash value
Generate SHA (file)
key=“da39a3ee5e6b4b0d3255bfef95601890afd80709”
Step 5- Compare(R, key) hash value from existing hash value (k).
Step –6 S=Send (hash) response whether the file already exists or not
Step – 7 If () the file does not exist
{
Script(“Display data does not exist”);
Upload(data,key);
}
Else{
Script(“Display data exit”);
}
Step 8- Store(data,key);
END

V. RESULT



VI. ADVANTAGES OF BLOCKCHAIN

Many of the real time issues can be fixed using blockchain. It can be also applicable for maintaining our financial life. It also has a lot of impact on industries. Some of the major advantages of block chain are

1. Decentralized
Banking sector shackle and handle customers in monopoly way. A huge amount of money is charged to verify the customers own particular assets. After being decentralized also blockchain is still applicable to a large number of users. It also retains some additional advantages such as no middle man scenario and most importantly the whole network is not in control of any one.

2. Distributed
In spite of having a centralized server, the network is still distributed. The data is spread to all over the user and nodes. Henceforth every user has control over the system. Blockchain networks are also compatible with IoTs. In realistic it is unbackable.

3. Immutable
Over time, the process of recovery and undoing gets tougher. So, in that sense, the technology can be said to be immutable. It's a good and bad thing at the very same time. If you are a freelancer, once the client sends you the payment. Such a feature makes the tech more robust and sustainable and more trustworthy among the users.

4. Trustless
Users follow a common consensus algorithm that will verify every transaction and store it one the common ledger. Moreover, everyone can see the all the transactions made. And if any transaction violates this consensus algorithm, the transaction itself gets violated. So, even if the parties don't trust each other, it doesn't matter. The system is designed to ensure safety and common trust among the users.

VII. CONCLUSION

We have proposed an electronic voting system based on the blockchain technology .The system is decentralized and does not rely on trust .Any registered voter will have the ability to vote using any device connected to the internet. The Blockchain will be publicly variable and distributed in a way that no one will able to corrupt it. We will be able to gain transparency into our elections, without compromising voter privacy , and have a way to mathematically prove that the elections results are accurate.

REFERENCES

[1] Zibin Zheng, Shaoan Xie, Hongning Dai, Xiangping Chen, and Huaimin Wang, An Overview of Blockchain Technology: Architecture, Consen-sus, and Future Trends. 2017 IEEE 6th International Congress on Big Data.

[2] Tien Tuan Anh Dinh, Rui Liu, Meihui Zhang, Member, IEEE, Gang Chen, Member, IEEE, Beng Chin Ooi, Fellow, IEEE, and Ji Wang, Un-tangling Blockchain: A Data Processing View of Blockchain Systems. 1041-4347 (c) 2017 IEEE.

[3] Florian Tschorsch Bjurn Scheuermann., Bitcoin and Beyond: A Technical Survey on Decentralized Digital Currencies.

[4] Massimo Di Pierro, DePaul University, What Is the Blockchain

[5] Florian Tschorsch Bjurn Scheuermann, Humboldt University of Berlin, Bitcoin and Beyond: A Technical Survey on Decentralized Digital Currencies

[6] Satoshi Nakamoto, Bitcoin: A Peer-to-Peer Electronic Cash System.

[7] A. Thomson, T. Diamond, S. Weng, K. Ren, P. Shao, and D. J. Abadi, Calvin: fast distributed transactions for partitioned database systems, in Proceedings of ACM International Conference on Management of Data (SIGMOD), Scottsdale, AZ, USA, 2012, pp.112.

[8] F. Tschorsch and B. Scheuermann, Bitcoin and beyond: A technical survey on decentralized digital currencies, IEEE Communications Survey & Tutorials, vol. 18, no. 3, pp. 20842123, 2016.