Secured E-voting system using Etherum Block Chain Technology

Bhavya K Seth[1] Anjan K Koundinya[2] Anil G N[3]
[1,2,3]Department of Computer Science and Engineering
[1,2,3]B M S Institute of Technology and Management, Avalahalli, Yelahanka, Bengaluru, India

Abstract— In a modern democracy it is vital to have total participation of its citizen in electoral process. Many nations have electronic and internet based voting system that will enhance the involvement of its citizens in the process. The problem with the voting system is that it can be breached and manipulated by power hungry political outfits. There are existing systems which are electronic tamper proof and resilient systems that avoid tampering with electoral process. It is desirable to have internet based polling system to achieve totality in election process for abroad citizens. The electoral agency spends lot of exchequer money to conduct free and fair elections in the nation. However it is also observed that all do not participate in the process. In order to have total inclusion of its citizen in a tamper less manner, it very crucial to have an electronic and web based electoral process. The market value of such systems is very high and runs in billions of the dollars. The system proposed here is intended to adequately address the cost factor, transparency and enhanced trust in the electoral process. The proposed system incorporated the aplomb uses Blockchain technology to make voting process more transparent and secured. The system uses current technology such like client server authentication integrated with a Blockchain to ensure the important aspects such as transparency, security and inspection that ensures privacy for voters. Particularly, Ethereum which is a decentralized digital currency platform based on the cryptography, is open and transparent for the individual transaction. In order to prove the working of protocol, this design implemented is a web based voting software that runs through ReactJS which is a Javascript framework. The experimental implementation is limited to small-scale elections. The systems can run contracts with location and device isolation that ensures total privacy of voting. The cost of designing this architecture is incredibly less as compared to the cost of current paper/ballot based voting system. There are solid social benefits to using the system along with an easier and quicker voting process which will lead to higher voter count. This system can be implemented for most of the countries as the internet involvement in the world increases.

Key words: Decentralization, Ethereum Blocks, Token, Distributed Ledger, Ether

I. INTRODUCTION

Voting plays an important role in the Democratic countries. Human Rights which people wish to have are being violated and their essential freedom provided by their constitution are being seized. In such a scenario, having a trustworthy and transparent election is something that is supreme for the freedom of the citizens. Besides, the previously proclaimed systems implemented do consists of variety of technologies, such as , homomorphic encryption ,blind signature, ring signature, Mix-Net, etc. In particular, there is a great involvement of e-voting using digital currency in the market. Secured voting [1] involves or ensures total participation for all the stakeholder of the public system.

In peer-to-peer networks, tasks are partitioned among peers, who share a portion of their computational power (in the form of processing power, disk storage, etc.) to other participants in the network, thus removing the need for central coordination in the form of stable hosts or servers. Instead of using a single solution/infrastructure, Blockchain and DLT [3] (Distributed Ledger Technology) technologies essentially bond together to form a new type of base that adheres on top of the existing systems, integrates with it and processes together. And in doing so, they are rapidly and secretly changing the way companies, regulations and other firms communicate and share data.

The process of voting involved two types of step in the vintage process, that is, inscribing(authorising) to vote and the process involved in voting. The proposed architecture will be including an additional step, that is, verifiability of the vote. As electronic voting majorly depends on the Internet, the decisive challenge for electronic voting is the security issues involved in it. In order to eliminate the potential risk to minimal level, various contracts/agreements related to the privacy, individual validation[4], eligibility, intactness, fairness, uniqueness, robustness, universal validity have been widely submitted. The Blockchain is like a Linked list which consist of a set of nodes. These set of nodes are based on a peer-to-peer network. Consistency is maintained at each node by applying a solid algorithm.

To specify the design and working of the Blockchain, the Ethereum [2] is a one type of representation of the Blockchain. To know about basic working of Blockchain, we should have a basic idea of the block. Every block consist of block header and the main part of the block which includes serialized transaction raw. The transaction raw has a unique ID called the transaction ID which is the hash based value of the transaction taking place. By storing the preceding block ID into the succeeding block, all nodes are connected with the block headers which is also called the chain. When adding a new block to the chain, the Blockchain will use Keccak[5] algorithm to create a new ID for transaction which is unique for that node. New node will be added to the chain only if all the preceding nodes accept it

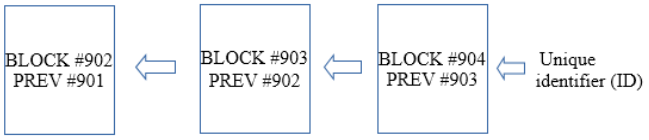

Figure 1: unique identifier in each block

II. PROBLEM STATEMENT

The ballot system can easily be manipulated by power hungry organizations therefore the current system is an alternative and effective approach to eliminate the degraded system with the new online voting system using Blockchain. The current system looks to eradicate the unlawful activities from the election to make it highly secure and transparent. The system uses existing technology such as a client server approach

combined with the Blockchain architecture to ensure impressions such as transparency, security and perceptibility are achieved to ensure freedom interference for voters. The overall cost of designing the architecture is materially less as compared to the cost of present ballot based architecture. The Blockchain consists of pack full of nodes based on a peer-to-peer network. For every node involved, it maintains the consistency of the data. New node will be added to the chain only if all the preceding nodes accept it.

III. PROPOSED WORK

Electronic voting systems is the area of research from decennary, with the aim to diminish the cost of perform an election, while ensuring the election uprightness by fulfilling the security and privacy requirements. Replacing the traditional paper method with a new election system has the strength to limit deception while making the voting process actively traceable and verifiable. Blockchain is a distributed, immutable, incontrovertible, public ledger.

The present technology has three main attributes:

- Immutable: newly added block must always refer to the preceding model of the ledger. This creates an immutable chain and prevents meddling with integrity of the preceding appearances.
- Verifiable: the system is peer-to-peer network, replica and widely distributed over multiple positions. This ensures removing single point of failure and ensures third party verifiability.
- Distributed Consensus: a distributed consensus protocol determines who can append the next new transaction to the ledger.

A. Authentication using client-server approach

Username and password is the most easier approach that doesn't need any additional software on the client side. This approach is easy to remember. Users with their VoterID can login to the system with the secret password provided by the government agencies. Incorrect VoterID and password combination will not connect to the blockchain voting page. Most the real time databases [6] are used to store VoterID and password of millions of users which can be retrieved in most efficient way.

Features of client-server approach:

1) Authentication: Authentication feature lets only authorised users access your application.
2) Storage: compatible with large amount of data stored in the database.
3) Real-time Database[6]: Database used is highly and consistently dependable even if the connection is lost but data is completely maintained.

B. Arbitration Server

Arbitration server is mainly used to resolve discourse between the client and the server or between the server and users. Arbitrators are the entities which are semi-trusted in the modern world utilizing social network for any business related transaction. Before any transaction takes place the users and servers, communication parties have to agree on a set of arbitrators. After the agreement they receive a resource like deposit from the participants. The demonstration of the usage of arbitrators in the scope of conditional mystery. A user interacts with a server in an unspecific way as long as the terms for anonymous communication are entertained. When a server identifies a disobedience of the terminology, it manifests to the arbitrators that a breach took place. The number of transactions carried out across the network grows incredibly every day.

Peer to peer, machine to machine, and clients-servers carry out independent agreements with no aid of central authority. A Certificate Authority is an eminent example centralized approach, a centralized entity is a part of the public key infrastructure. The digital arbitration [7] structure comprises of four entities: Users, servers, certificate authority and arbitrators.

C. Blockchain

1) Blockchain as an amenity:

The blockchain is similar to Linked List data structure which appends nodes at the end of the list. The blocks are linked in such a way that each block consist of hash which is a function of the preceding block. There are two different types of Blockchains, with different levels of obligations such as who can read and write the blocks. We are using public Blockchain which is readable and writable for everyone. To be more specific the current structure ueses Ethereum to build smart contracts.

2) Types of nodes in the Chain:

District node: Represent each voting district.

Bootnode: Each centre with legalized access to the network will be hosting a bootnode. Bootnode helps to co-ordinate and discover the District node.

D. Ethereum

Ethereum is an open and publically used platform which is based on decentralized and distributed evaluation platform that provides an additional smart contract functionality. Ethereum Virtual Machine (EVM) is a runtime machine which is used to execute smart contracts. Ethereum Virtual machine is built using a programming language called Solidity. Solidity is an object oriented and stack based programming language with predefined set of instructions and limited set of arguments. Ethereum Virtual Machine is a decentralized machine which runs all the processes. Execution of smart contracts takes place locally at each node of a network. Each node will in verify and group the transaction sent from the users to form blocks and then appends these blocks to the chain. Once the grouping is done a reward is collected as part of the completion process. The entire process starting from sending, validation and collection of reward is mining process and the nodes involved in the process are called miners. Every instruction the EVM executes involves a fee which is regarded in terms of fuel called GAS. Complex instructions require more fuel when compared to simpler ones. There are two main purpose of GAS. It motivates coders to write quality code by avoiding undesirable and poor quality code and at the same time it ensures that the operations are successfully executed. A fee is charged when a fuel is needed. The fee depends on the

amount of fuel needed which in turn depends on the complexity of the instructions that the node executes.

E. Smart Contracts in Ethereum:

Smart contracts [8][9] are like conditional statements which gets executed only when a particular pattern is met. Like the traditional contracts tie the parties together on varies agreements even the Smart contracts does the same. They automate the transactions and allow the parties to reach the conclusion automatically without any help of the intermediary person.

Deploying a smart contract in the Ethereum platform there is a notable creation transaction which is to be executed, that introduces an agreement to the blockchain. The contract is allocated with a unique address during this procedure, which is 160-bit identifier, and its code is inserted to the blockchain. On the completion of creation of smart contracts, now the smart contracts consists of address, balance and some amount of predetermined executable code.

Related to e-voting the Smart contracts consist of three levels: (1) The agreement about the role in election, (2) the process of election and (3) the smart contract based voting transaction used.

1) Different roles in election: The different kinds of roles involved in election are:

- Controller: manages the entire process of election. Different committed institutions are involved in this role. The election controllers create the entire process of election, register the new and existing voters and decide the dates of the election and assign permissioned booths or nodes.
- Voter: Citizens who have right to vote. Voters cast their vote and verify their precious vote once done with voting process.

2) E-voting process: Blockchain deployed Smart contracts are used to represent the e-voting process in this work by the Controllers. For each voting area a smart contract is defined. The main jobs in the e-VOTING PROCESS ARE:

- Formation of election: using a smart contracts the Election controllers create election booths in which the controllers defines a list of valid voters for each voting area. The smart contracts are then written onto the blockchain, where district nodes gain access to interact with their corresponding smart contract.
- Registration of voters: this phase is handled by the controllers.
- Calculation of votes: Calculation of votes is done immediately once the voter votes. It is done using smart contracts.
- Verification: In the e-voting process every valid voter receives a unique ID of his vote. In The current e-voting system, voters can use the unique ID and go to the authorized office or site And verify the vote.

F. Solidity (Ethereum Programming Language)

Solidity[10] is an object-oriented complete programming language whose syntax is almost similar to JavaScript programming language and it is a statically typed language. Since it is an object oriented language it supports encapsulation, inheritance and polymorphism. User can define complex data types. In Solidity language Contracts are similar to classes defined in JavaScript. Contracts are usually made up of variables and classes just like the classes used in any other object oriented programming language.

G. SHA-3 (Secure Hash Algorithm 3)

SHA-3[11] (Secure Hash Algorithm 3) is the modern element of the secure hash algorithm kin, which adheres to modern standards. SHA-3 was released by the NIST on August 5, 2015. Keccak is said to be the antique algorithm from which SHA-3 is been derived therefore SHA-3 is said to be the subgroup of Keccak Algorithm. There is functionality of Key Stretching in SHA-3 which is present in SHA-2.

Design of SHA-3 is such that it is well organised in hardware side and time consuming on the software side. SHA-3 takes almost double the time to run on software implementation contrast to SHA-2 and about a quarter of the time to run on the hardware implementation. Since it takes almost takes twice the time to run on Software implementation, on way to compromise is to reduce the number of iterations to half the original number. Hardware implementation is easier for attacker to use and crack it resulting to crack SHA-3 passwords accurately eight times faster than SHA-2 passwords. SHA-3 is not made to use as a password hash function like SHA-2.

Sponge construction is the main idea behind the Keccak Algorithm. Sponge construction uses a large number of random permutation which allows to absorb (inputs) any amount of data and releases (outputs) any amount of data thus acting as a pseudorandom function with respect to all the preceding inputs. Flexibility is the main characteristic feature of this algorithm. Keccak shows an extensible stand against the collision attacks: After several years of cryptanalysis and a lot of effort, the largest number of Keccak rounds for which actual collisions were found was only 2.

Keccak algorithm uses an approach where it takes random length inputs and generate fixed length output. The Keccak versions submitted to the SHA-3 competition have an internal state size of b = 1600 bits, and an output size n of either 224, 256, 384 or 512 bits. The internal permutation of Keccak consists of 24 application of a non-linear round function, applied to the 1600-bit state. Keccak/SHA-3 has found to be much slower than BLAKE2 in software implementation.

Keccak offers an advantage of at least 4 times better performance with only few percentage of more budget and the same hardware requirements or less than Blake. Using Keccak in processors like Intel, ARM or any other processor this would use up to 25 128-bit registers to hold the state and all round constants, processing rounds individually, or 13 128-bit registers to hold just the state, and processing a group of rounds, with the round constants generated on the fly. There could also be a special 1600-bit register just for the Keccak state. This would give Keccak a similar performance advantage as AES was given with appropriate CPU instructions, and could make it faster than Blake-2, almost certainly so for a 256-bit hash, where the performance is already quite close.

H. Verifiability of the vote.

When it comes to e-voting Scientists usually talk about the trust, that one must rely on voting process. But there are two

contradictory statements. First, they argue that it should not be necessary to trust e-voting systems, which would be the case if they are provably secure. Second, for an e-voting system to be successful, the public must trust it.

E-voting is an alternative to the native paper based voting. If there are improvements in the case of trust, count and other factors then paper based voting can easily be transformed to E-voting.

When it comes to trustworthiness, paper voting seems to have better advantage because it is less complex and preferable method for novice voters but still the E-voting may is more dependable, because it eradicates any kind of human error for example the counting of the ballots and thus results in trustworthiness and confidence among the citizens.

For E-voting, the trust relations are a bit more complex and should involve expertise controllers to handle the entire voting process.

Verification of E-voting means that every machine where voter can vote has to be tested by the testing agency involving the controllers. A small number of machines has to be tested before the actual election process. Two types of verifiability must be present in every election: One is, every voter can verify his/her vote is properly applied to their desired candidate and other is, anyone can check that the calculated result is correct.

One of the main problems of election system is vote buying. Therefore, people should not be able to prove to whom they voted, even if they want to. This makes it impossible for someone who forces the voters to vote in a certain way, or someone who buys their vote, to check if they actually voted the candidate they wanted to.

The property of the voter not being able to show the buyer whom they voted is called receipt-freeness.

IV. CONCLUSION

The value of Ethereum will grows with the number of interesting applications deve loped and used. The bubbling of applications created (even before the finalization of Ethereum) gives us an indication that the moveme nt is well launched. Opening the platform encourages its deve loped by anyone who is interested in doing so. Another growth vector will be the Ethereum interconnection with everyday devices. A computer isolated from its environment has little va lue , whereas its networking increases tenfold its possibilities. The few Ethereum interconnection projects already show a lot of potential. Existing applications include applications such as Board Room which is a voting system (useful for managing an organization) , event or market prediction applications (such as Augur or Gnosis). Finally, Ethereum is a vast and ambitious ecosystem on which a digital revolution will be built. Many systems that we all use can be rebuilt or upgraded to Ethereum, with the advantage of reducing or eliminating the centralization of these systems.

REFERENCES

[1] Ali Kaan Koç, Emre Yavuz, Umut Can Çabuk, Gökhan DalkÕlÕç, "Towards Secured E-Voting Using Ethereum Blockchain" ,March 2016.
[2] Gavin Wood, "Ethereum A Secure Decentralized Generalized Transaction Ledger EIP-150 Revision", March 2016.
[3] Maher Alharby and Aad van Moorse, "Blockchain Based Smart Contracts: A Systematic Mapping Study", April 2011,DOI : 10.5121/csit.2017.71011.
[4] Wolter Pieters, "Verifiability Of Electronic Voting Between Confidence And Trust", July 2014.
[5] Itai Dinur , Orr Dunkelman and Adi Shamir, "New attacks on Keccak-224 and Keccak-256",June 2017.
[6] Sonam Khedkar , Swapnil Thube, "Real Time Databases for Applications", June -2017,e-ISSN: 2395 -0056.
[7] Dan Brownstein , Shlomi Dolev , Niv Gilboa and Ofer Hermoni, "Digital arbitration for trusted communication", Brownstein et al. Journal of Trust Management (2016) 3:3 DOI 10.1186/s40493-016-0024-x
[8] Karthikeyan Bhargavan ,Antoine Delignat-Lavaud ,Cédric Fournet ,Anitha Gollamudi,Georges Gonthier, Nadim Kobeissi , Aseem Rastogi, Thomas Sibut-Pinote,Nikhil Swamy, Santiago Zanella-Béguelin, "Formal Verification of Smart Contracts",2016.
[9] Maximilian Wöhrer and Uwe Zdun, "Smart Contracts: Security Patterns in the Ethereum Ecosystem and Solidity",978-1-5386-5986-1/18, 2018
[10] Friðrik Þ. Hjálmarsson, Gunnlaugur K. Hreiðarsson, Mohammad Hamdaqa, Gísli Hjálmtýsson, "Blockchain-Based E-Voting System",DOI 10.1109/CLOUD.2018.00151,2018.
[11] Shu-jen Chang, Ray Perlner, William E. Burr, Meltem Sönmez Turan , John M. Kelsey, Souradyuti Paul and Lawrence E. Bassham, "Third-Round Report of the SHA-3 Cryptographic
[12] Hash Algorithm Competition", http://dx.doi.org/10.6028/NIST.IR.7896, March 2012

