Secure Decentralized Voting System Using Blockchain.

Atharwa Ajay Adawadkar
Department of Computer Science and Engineering
Walchand College of Engineering
Sangli, India.
ashtnemi@gmail.com

Rohit Rajesh Chougule
Department of Computer Science and Engineering
Walchand College of Engineering
Sangli, India.
irohitchougule@gmail.com

Swapnil Shrikant Kesur
Department of Computer Science and Engineering
Walchand College of Engineering
Sangli, India.
kesurswapnil@gmail.com

Nandinee Mudegol
Department of Computer Science and Engineering
Walchand College of Engineering
Sangli, India.
gmudegol@gmail.com

***Abstract*—The ballot system and electronic voting system is being used all over the world for a while now but it has numerous flaws regarding security and transparency. The newly emerging technology named Blockchain holds a huge potential for building more secure software systems. The motive of this paper is to specify why a decentralized voting system built using blockchain is better than the traditional system. This paper illustrates the implementation of a blockchain-based application which improvises the ease to vote, increases transparency and security in voting and is more economical as compared to the current system.**

Keywords—E-Voting, Permissioned Blockchain, Cryptographic Hashing, Byzantine Fault Tolerance Algorithm, Distributed Systems.

I. INTRODUCTION

Current technology enables individuals to communicate straightforwardly. Voice and video calls, messages, pictures and emails travel straightforwardly between remote gadgets, maintaining trust between people, regardless of how far they are. But when it comes to money, people have to trust a third party to be able to complete a transaction. By utilizing math and cryptography, blockchain gives an open decentralized database of any exchange including value - money, goods, property, work or votes, creating a record whose credibility can be confirmed by the whole network.

Elections that are held publicly is the crux of any democracy. Therefore, it is must for the government body to hold free and fair elections to elect the candidates. There are a number of ways implemented by various countries around the world. Electronic voting, ballot based voting are some of the common methods implemented. However, with these methods, the problem of voter confidence if not solved as the voter never knows whether his/her vote has been counted and has not been tampered with. The level of transparency provided by these methods is quite low and arguably the government body can tamper with the election process. In this paper, we propose a system which can solve these problems of voter confidence and transparency by discarding the old offline ways. Our system will be based on the Blockchain technology. Blockchain is generally considered as distributed ledgers of transactions. Voting can also be seen as a kind of a transaction between the voter and the candidate. Thus, we see a lot of scope for the Blockchain technology to be a part of the new generation voting system. Another reason to choose an online way of conducting the elections over offline ways is the rate at which the population of several developing and developed countries are adopting and getting familiar with the internet. In 2015, the International Telecommunication Union assessed 3.2 billion individuals or half of the total populace would be online before the year's over. Of them, around 2 billion would be from developing nations, including 89 million from slightest developed nations [11]. These numbers are increasing day by day and eventually, in the upcoming years more than three fourth of the world's population would be connected to the internet. Thus, our system could be easily deployed to contest free and fair elections. Another advantage of contesting elections online is to increase the number of youth voters taking part in the election process and casting their vote. In most developing countries, the youth of the country often travel away from their hometown for either education or to earn bread and butter. At most constituencies, it is compulsory to cast vote at the hometown. This is not convenient for the youth living long distances from their hometown. Section II is the literature review, Section III illustrates the problem statement and proposed solution, Section IV is Results and Discussion, Section V gives idea about future scope of this system, Section VI enlists all the references.

II. LITERATURE REVIEW

The trend of voting on internet was stared by US in 2000 [4] but Estonia was the first to introduce permanent national internet voting. 14 more countries followed US till 2013 [5]. Out of these 14 countries only 10 plan to reconsider this system for future elections.

The main aim of pioneers of e-voting was to make sure all the votes must be taken into consideration even when the individuals could not physically be present at booth [6].

Envision a fighter abroad or a sailor on a nuclear submarine. Both are serving their country, yet their ability to cast a poll is confined as the coordination of acquiring a truant ticket and getting it back so as to be tallied. This was one of the major flaw which was faced in earlier versions of voting over internet.

Internet Voting across the globe :

France - France led an online essential in 2014, its first, utilizing a framework touted as secure, however, columnists from the news website Metronews demonstrated that it was anything but difficult to rupture the purportedly strict security of the race and vote a few times utilizing diverse names, tossing the result into uncertainty [8].

Finland - Finland investigated the utilization of an online kiosk-based casting ballot framework, which offers expanded security against pressure, and diminishes to some degree the danger of a few types of malware. Be that as it may, early explores different avenues regarding a stand based framework have indicated versatility issues. All the more quite for the US, the frameworks being conveyed and utilized today in the U.S. are not stand based, without even the fractional alleviations a booth framework may offer. Because of huge defects in the framework bringing about lost votes, Finland's Supreme Administrative Court in 2009 abrogated aftereffects of Finnish 2008 civil decision and required a re-vote on a paper tally framework [7].

Australia - Elections of New South Wales in 2011. Issues related to voter endorsement, joining a condition in which voters utilizing truncated ID numbers could sign in and vote. Utilizing ID numbers was relied upon to anonymise the voters, anyway since the structure neglected to sincerely separate ID numbers from votes or voters, the New South Wales Electoral Commission could seek after the votes to the voters utilizing the off base ID numbers, completely invalidating the nation's absence of lucidity required [7].

Flaws in above implementations:

All the aforementioned attempts for e-voting specifically voting over internet shared common issue of security and transparency. Some claim that even EVM can be hacked even though they are not connected to internet [9]. Likewise, the centralization of the I-Voting framework utilized in Estonia makes it powerless against DDOS attacks what could make the elections difficult to reach to voters [10]. Also there is issue of transparency as faced by US in elections of 2000 where voters overseas where not sure if their vote was really taken in the actual count [6].

In this paper we try to address all the above issues by developing a blockchain based voting system.

III. Statement of problem and proposed solution

Design and build a robust and secure voting system using permissioned blockchain network with fault tolerance ability. Also provide a consistent consensus algorithm for the verification and calculation of the results. The system should be remotely usable and easily accessible.

A. Architecture

The system consists of N nodes. Each node has two sets of data structures (Set-1 and Set-2). Each set consists of N queues. A vote consists of unique Voter ID, Party ID, and timestamp. Each block has a Block ID, N encrypted votes, hash of current block, hash of the previous block of the chain (0 for genesis block) and timestamp. The hashing algorithm used is SHA-256. The blocks are stored in local databases of each node. Before making an entry to any database, Byzantine fault tolerance algorithm is used to overcome any tampering done in the votes while transfer of votes between nodes in the blockchain node network. Consistent copy is broadcasted to all nodes and updated in respective databases. Entire platform is connected to a web portal which is used for casting a vote as well as viewing the result statistics.

B. Block Statistics

- Block ID - 4 bytes
- Current Node Hash - 32 bytes
- Previous Node Hash - 32 bytes
- Timestamp - 12 bytes
- Hash of N Votes - 32 bytes

Total Size of each block = 112 bytes.

C. Notations

- Ni - i^{th} Node
- Set-1 - Data structure to store votes broadcasted from other nodes
- Set-2 - Data structure to store untampered votes selected from set 1
- S1qi - queue of set one mapped to i^{th} node
- S2qi - queue of set two mapped to i^{th} node
- dbi - local database of i^{th} node
- bi - i^{th} block in blockchain / row of local database of a node

D. Operation and Control flow of the System

Consider there are 3 nodes in the system as illustrated in the diagram (Figure 1A). User logins on the web portal remotely using any device and gets connected to one of the node (in round robin fashion) and then casts the vote. After casting the vote, user is disconnected from that node. This node (for example N1) sends that vote to Set-1 queue named S1q1 of all nodes as vote was received from node 1.When N2 receives the vote broadcasted by N1 it again broadcasts the vote to N1 and N3. This time they are stored in Set-1 queue named S1q2 as they received the vote from N2. Thus when all the nodes are done with broadcasting, each node has N copies of same vote

and it chooses the vote with maximum frequency and inserts that vote in Set-2 queue named q1 as user was originally connected to N1. This is implementation of Byzantine fault tolerance algorithm to ensure that no vote is changed while being transferred to another node in the blockchain network.

Above scenario occurs N times and therefore no queue in the Set-2 is empty. Once such a situation is occurred, all queues are dequeued simultaneously and a block is formed at each node which is saved to local databases of that node. It must be noted that in this system it is the vote which is being transferred and not blocks, as each node has consistent copy of the votes they locally create block and thus we decrease the traffic of network to a very large extent.

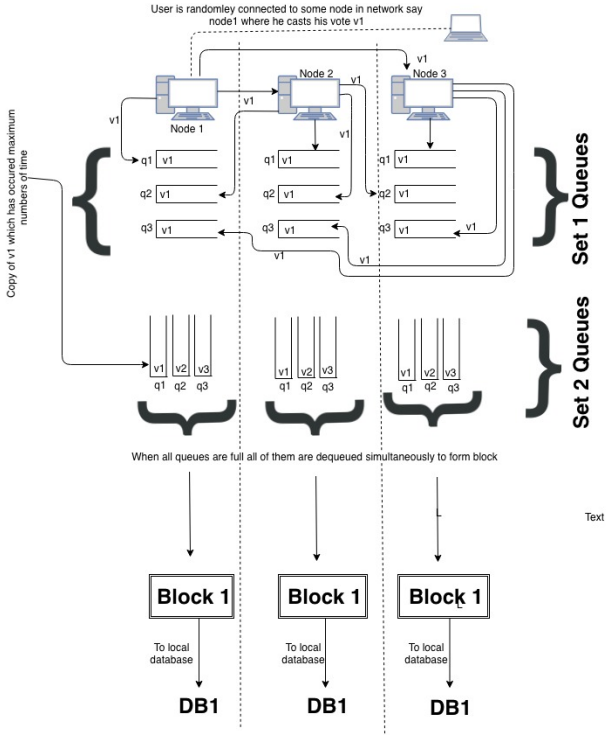

Figure 1A - Operation and Control flow of the System

E. Final Vote verification and calculation

After the voting day, each node has a copy of entire blockchain in their respective databases. The major task to determine if the entry in the block has been tampered with and if so we have to check consistency of each block. (Figure 1B)

A node is selected at random it retrieves row of database which represents a block in blockchain from all the nodes and again uses Byzantine fault tolerance philosophy (Consensus) to determine the consistent copy of that block among all the retrieved rows/blocks. And if any block is found to be tampered then we update the database with the consistent copy of that particular block. Then we update the counter for each party for which the vote is casted. And thus at the end of this process all nodes have 100% consistent blockchain copy. At any instant of time voter is able to verify the vote casted by him/her which makes the system transparent. We analyse the result according to the final consistent copy of Blockchain and give graphical as well as statistical result which is displayed to the voters and the candidates on the web portal.

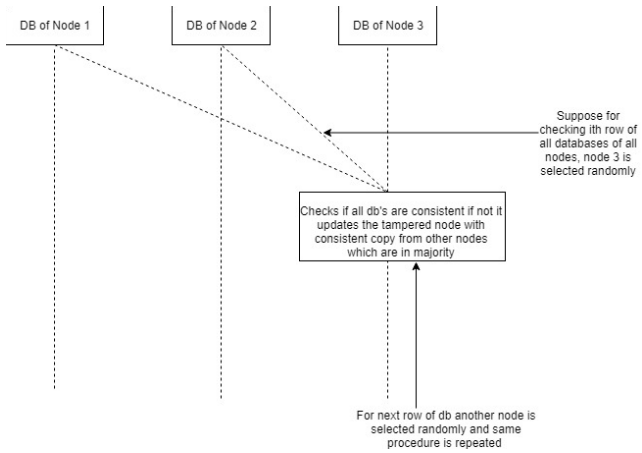

Figure 1B - Final Vote verification and calculation

IV. RESULTS AND DISCUSSION

This paper proposed a blockchain based voting system. Anyone who is connected to the internet can easily cast their vote from any location of the world. The final Blockchain will be verifiable publicly and immutable. Also voters could check if finally their vote was casted correctly.
The system would be highly economical as we don't need to buy all those high end servers to manage our system as they would be needed only for a day or two, we can rent those servers from cloud services such as Amazon AWS or Microsoft Azure. Also possible improvements are mentioned so that they could be addressed in future research papers.

V. FUTURE SCOPE

One major problem which is witnessed by Indian Elections is that many times the candidate and his team manipulate people and trick them in giving vote to someone against their will by threatening them.
This can be brought to an end by incorporating an Image Processing module in this voting system which would analyse the facial expressions of the voter and if the statistics of "fear" , "anxiety", etc emotion is found to be exceeded a certain threshold then that voter can be blocked for casting vote for a particular period of time. So in the end it could be ensured that all the votes casted are genuine. This paper proposed a blockchain based voting system.

VI. REFERENCES

1. National Institute of Standards and Technology, "Federal Information Processing Standards Publication", (2012).
2. S. Nakamoto, "A Peer-to-Peer Electronic Cash System", (2008).
3. F. Reid and M. Harrigan, "An Analysis of Anonymity in the Bitcoin System", Security and Privacy in Social Networks. (2013)
4. Wikipedia. "Electronic voting". https://en.wikipedia.org/wiki/Electronic_voting#Online_voting
5. BBC News. "Has the time now come for internet voting?". https://www.bbc.com/news/business-39955468
6. "The Past and Future of Internet Voting". https://www.brookings.edu/wp-content/uploads/2016/07/pointclickandvote_chapter.pdf
7. "Internet Voting Outside the United States". https://www.verifiedvoting.org/resources/internet-voting/internet-voting-outside-the-united-states/
8. The Independent. "Fake votes mar France's first electronic election". https://www.independent.co.uk/news/world/europe/fake-votes-mar-france-s-first-electronic-election-8641345.html
9. Think Progress. Professor Dan Wallach. https://thinkprogress.org/how-easy-would-it-be-to-rig-the-next-election-819326cbbbd/
10. Ahmed Ben Ayed. "A Conceptual Secure Blockchain - Based Electronic Voting System". International Journal of Network Security & Its Applications (IJNSA) Vol.9, No. 3, May 2017
11. Wikipedia. "Global Internet usage". https://en.wikipedia.org/wiki/Global_Internet_usage