Tangle Electoral System
(DAG based Blockchain Voting)

Raghav Patnecha

Akshay Bahadur

Abstract

Elections are considered to be the means by which an individual can exercise his right to be in a democratic country. However, the process of elections has always been under the scanner since it's never quite transparent as well as efficient. In this paper, we aim to analyze the current technologies used in elections along with the security flaws that are intrinsic to the system. We would also throw some light on how to exploit the power of the internet for solving the system of voting. We propose an alternative method for conducting elections which is secure, efficient and transparent simultaneously. We would also describe our proposal in depth and how it can solve the intrinsic problem of electoral systems using tangle.

KEYWORDS

Electronic Voting System, e-Voting, iota, Tangle, DAG, Indian voting System, Internet Voting, EVM, Blockchain. Voting using Tangle

1. Introduction

The voting system has come a long way since the birth of democracy. During the nascent phase, the voting system solved only the underlying problem, democracy. Nevertheless, since then, the society wants the constitution to secure other aspects as well. Hence, for being fool-proof, the voting system has to be transparent, secure, fair, efficient, unbiased and anonymous. For providing this, the system also evolved from paper ballot to the usage of Electronic Voting machines. This transcending step was enthusiastically appreciated by the society;

however, this system had some inherent vulnerabilities. In this paper we aim to explore the vulnerabilities of the current system and propose an advanced system of voting.

2 Related Work

IOTA[1] is a revolutionary new transactional settlement and data transfer layer for the Internet of Things. It's based on a new distributed ledger, the Tangle, which overcomes the inefficiencies of current Blockchain designs and introduces a new way of reaching consensus in a decentralized peer-to-peer system.The major difference that is worth mentioning (apart from the DAG vs. Blockchain) is how IOTA achieves consensus and how transactions are made. In IOTA, there are no miners. What this means is that each participant in the network that wants to make a transaction has to actively participate in the consensus of the network by approving 2 past transactions. This attestation on the validity of two past transactions ensures that the whole network achieves consensus on the current state of approved transactions, and it enables a variety of unique features that are only seen in IOTA.

3 Vulnerability Analysis

The evm is not cent percent secure[2]. It has been proven that the evm can be tampered with very easily. Firstly, dishonest election insiders can hurt the elections by replacing parts of evm with malicious parts to turn the results of the election in their favour. This can happen in either the manufacture or even years before the actual elections. Secondly, the attacker can use a portable hardware device to change the memory unit of the evm. This would also lead to unjust and unfair elections.

To underline this statement, in 2003, a journalist named Bev Harris wrote an article[3] on July 8, 2003 detailing how to bypass passwords and manipulate

election results on the Diebold GEMS central tally system. The information in Harris's article was subsequently confirmed by internal memos written by Diebold's own engineers.

In October 2006, the Netherlands banned the use of EVMs. In 2009, the Republic of Ireland declared a moratorium on their use. Italy has followed suit. In March 2009, the Supreme Court of Germany ruled that voting through EVMs was unconstitutional, holding that transparency is a constitutional right but efficiency is not a constitutionally protected value.

The usage of evm requires the person to be present where voting is supposed to take place. This also causes hindrance in the process of voting. As a democracy, it is the constitutional right for every individual to cast votes and choose their representative. However, only 60 percent of the total population actually go to the polling booths. This situation raises some severe questions on the present voting system. The case with handicapped is quite disturbing since the polling stations are not properly equipped to handicapped needs.

There is an immediate need of overhauling the overall voting system, which ensures the maximum participation of the masses along with the entire process being secure, transparent and anonymous. The most logical answer would be to use the internet. The internet has been used for decades for transferring information from client to server. However, this time, the situation is different. The information has to be reliable i.e. , the vote has been casted by the specified individual, it should be secure i.e. , no hackers can manipulate the outcome. Furthermore, the voting must be anonymous i.e., the identity of the voter must not be revealed along with his secret ballot, it should be transparent i.e., in case of a dispute – the votes can be recounted for surety. The system must also ensure

that only vote can be casted per individual as well as the total vote count must be reliable.

4 Internet Voting

Now, the real question arises how we can exploit the internet for casting votes[4]. The municipal government tried to implement online-voting, so they organized a mock e-voting scenario just to test the security of their system. Within a few minutes, hacker were able to gain access to the server and manipulate votes, get the identity of voters as well as whom they voted for in the election[5]. This all happened without the government even knowing about the attack. This created a lot of space for scepticism on online-voting. So much so, that computer scientists and security experts are nearly unanimous in opposition to it. Compared with touch screen voting machines, the opportunity for attacks on the Internet is much broader. It might lead to a typical man-in-the-middle attack. The user casting the vote would be unknown to the fact of handing the ballot to a potential hostile attacker who could change the vote. Moreover, neither the voters nor election officials would see anything suspicious. Because of the secret ballot, there is no way for the voter to check that the ballot transmitted to the elections office is the one they filled out on their computer.

5 Possible Solution

Whenever we talk about secure transactions (votes can be considered as a form of transaction in which the user grants his vote to the candidate), the concept of blockchain seems very beneficial. Blockchain is a new way of storing and moving that data, where instead of being held all in one place, the information is atomized and spread over thousands of nodes across a network, all locked together with efficient cryptography[6].

5.1 Blockchain as a voting platform

One solution to this fundamental problem is using blockchain technology to ensure that the votes are secure, anonymous and reliable[7]. Blockchain is a permanent cryptographic record, or ledger, of digital events that's "distributed," or shared among many different parties. It can only be updated by consensus of the participants in the system. Once entered onto the ledger, information can never be erased and it contains a cryptographically verifiable record of every single transaction (vote) ever made. Because "independent authorities" who may not trust each other need to attest to the accuracy of every transaction and "agree" on whether to make it a permanent record or not. This technology is immune to even "insider threats," which is one of the largest vulnerabilities to current systems. Blockchain technology is fault-tolerant, you cannot change the past, you cannot hack the present, you cannot alter the access to the system, every node with access can see the exact same results, and every vote can be irrefutably traced to its source without sacrificing a voter's vote anonymity. End to end verifiable voting systems will give the voter the ability to verify if their vote is correctly recorded and correctly counted, for instance, if a ballot is missing, in transit or modified, it can even be detected by the voter and caught before the election is over. Many experts believe that in-person voting using paper ballots is the only truly secure and guaranteed way to cast a ballot. Although dedicated elections officials generally run the process without incident, any manual human-based process is bound to be prone to errors and mistakes. Moreover, there are millions of ballots cast absentee by mail, which introduces a completely new set of issues.

5.2 Drawbacks of blockchain as a voting platform

However, there are certain intrinsic problems when it comes to using blockchain as an online voting platform.

- **Scalability**: The problem with blockchain, in general, is scalability. For maintaining consensus, the block chain system undergoes ‘mining’ which requires more computational effort as the number of nodes in the system increases.
- **Proof-of-work**: The proof-of-work guarantees that the next transaction is a valid one and the user is not double spending. However, each node has only one vote irrespective of its contribution to the system.
- **Speed of transaction**: The speed of transaction in blockchain decreases as the number of nodes increases in the system. The voting system requires that each vote must enter into the tally as soon as possible.
- **Susceptible to quantum computing**: The quantum computers are 17 billion times more efficient than classical computers. An attacker can use a blockchain to quickly create its own consensus branch with invalid votes.

6 Tangle

So, to go one step further into the technology of blockchain, we suggest using tangle(made by IOTA Foundation), which is a Directed Acyclic graph to store the transactions. The idea about using block DAGs instead of a blockchain has been around for quite some time now. In blockchain multiple transactions are stored and the blocks are sequentially connected to each other whereas IOTA is based on DAG. IOTA called this DAG tangle. It was suggested to use a tree as a form of ledger instead of a chain. Such a modification reduces confirmation times and improves the overall security of the network

6.1 Working

In tangle, firstly we create the genesis block which has all the tokens present in it. No other token can be generated afterwards. Similarly in case for voting, we will create genesis block which has tokens for all the voters. We propose to use a

national ID system for that i.e., Aadhar card in India. So only people who have enrolled into the ID system can participate in the national elections.

So, we will consider each vote as a node in the tangle. When a vote, casted by an individual, enters the tangle, it will not be a valid one until a number of other votes verify the integrity of that node. The casted vote also has to verify two other unverified votes with an earlier timestamp if it wants to enter the tangle. This will ensure validity of all the votes and eliminate double spending. If a voter tries to cast a vote twice, the other votes will not verify that vote and hence it will become an orphaned vote and not be added to the tangle.

Each machine in the system is responsible for adding votes to tangle. There can be common electronic voting machines which can be used for ballot voting. However, contradictory to the previous system, they will be connected to the internet and also to all other voting machines hence forming the network. The more number of voting machines, the more securely and quickly the votes will be added to tangle. Each voting machine will have the copy of the universal tangle as well as tangle of its own. The sum of all local tangles must be equal to the universal tangle. This will aid in votes recounting.

The process of voting starts with an auto generated cryptographic barcode for each user. The user encrypts the vote with his barcode. The user then signs the encrypted vote with the public key. The authenticity of the vote can be checked with the help of this public key. This makes the voting procedure to be very secure.

Since the voting machine is connected to the internet, the voting can also be done via other internet connecting devices. We propose using smartphones with touch ID as well as strong encryption algorithms to preserve the authenticity of the voter.

The voter can send his encrypted vote to the server. The server checks the authenticity with the public key. After verification, this vote is added to the universal tangle where it verifies two previous votes and waits for its own validation.This part also deals with the scalability issue of the present voting scenario.

Post elections, individual can verify their own votes using their own private cryptographic barcode. This would ensure non repudiation of the votes. This would also help in auditing the voting procedure.

In this way, coercion can be avoided since the election commission will have an actual proof of the votes casted.

We also propose the usage of checksum to make sure that the electronic voting machine are connected to the internet and hence the checksum of that machine would be equal to 1. If not, the checksum of that machine will be 0 and hence, voting can not be continued on that system until internet service is resumed back.

One of the problems with the current voting scenario is the issue of scalability. The current electronic voting machine only supports 64 candidates. There is no provision for voting of a 65th candidate, which might become an issue in the future.
Furthermore, the problem of availability is there with the system. Individuals are supposed to go to the polling booths for casting votes however, with internet, we support the usage of smartphones for the same. Hence, individuals can cast their votes with full authenticity, anonymity, security and integrity.

6.2 How a vote is confirmed

6.2.1 Signing

The voter will cast a vote using a node(computer/mobile) and sign it with his/her private Key which will be obtained by applying a cryptographic hash function to his/her National ID.

6.2.2 Tip Selection

Selecting two other unconfirmed transaction(tips) using Random Walk Monte Carlo algorithm. The random walk Monte Carlo algorithm chooses two unconfirmed votes and check the confirmation level and execute RWMC algorithm N times

6.2.3 Proof of Work

Your node checks if the two votes are not conflicting. Next, the node must do some Proof of Work (PoW) by solving a cryptographic puzzle (hashcash). Hashcash works by repeatedly hashing the same data with a tiny variation until a hash is found with a certain number of leading zero bits. This PoW is to prevent spam and Sybil attacks.

6.2.4 In case of loss of connectivity

A tangle can get branch off and back into the network. This is called **partitioning**. For example, if a vote machine gets offline or gets disconnected from others then the machine can create an offline cluster.

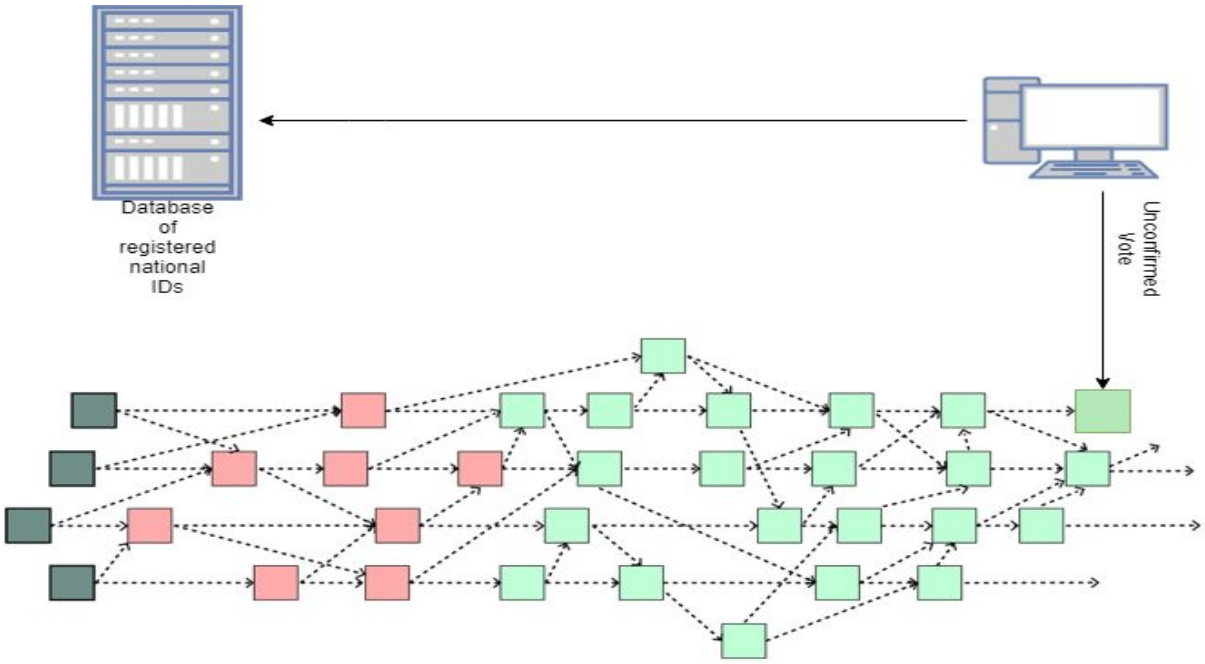

Fig: Working of Tangle electoral system

In the above diagram, the dark green colored votes are confirmed i.e., these votes have been considered successful. The salmon colored votes are confirmed votes with low confidence i.e., other votes must confirm these votes (directly or indirectly) so that they can be considered successful. The light green colored votes are unconfirmed votes that needs to be verified by other votes to enter into the system. At the time of casting votes, the identity of an individual is checked through registered national ID as shown in the above diagram,

7 Security Analysis

7.1 Sybil attack

Sybil attack is when a node takes control of the system and starts manipulating the transactions until the fake transactions become valid and the valid ones are regarded as orphaned transactions. This is not possible with tangle since the validity for each node is mentioned in the genesis block. This means that transactions that are present in the genesis block can only happen.

7.2 DDoS Attack

For an attack to be successful, the attacker's computational power must be greater than that of the whole network. Hence, the more the number of nodes the more secure the system.

7.3 Tamper data

For changing the data in a transaction, the attacker must change all other transactions following that transaction and also make sure that the fake sub tangle must become greater than the actual tangle

8 Advantages of using Tangle over Blockchain

8.1 Scalability

We use tangle over blockchain because the network becomes stronger when the number of transaction or votes increases which is not the case with using blockchain as it takes more time to confirm a vote

8.2 Decentralisation

In tangle there is not concept of mining as every voter is also acting as a vote validator.

8.3 No transaction fees

8.4 Quantum computing protection

It uses Winternitz One-Time Signature Scheme which is a quantum-resistant algorithm.

9 Conclusion

We propose a government backed electoral tangle that could be used as the gold standard to prevent corruption in elections, replacing the need for costly election monitoring programs.

Acknowledgments

The authors gratefully acknowledge the anonymous source who, at considerable risk, provided the EVM for us to study. We also thank the various researchers who have done tremendous amount of research in the field of blockchain and have provided us with some common ground to work upon. The authors would also like to extend their gratitude towards the IOTA community for providing us detailed documentation on which our electoral model is based.

References

1. https://iota.readme.io/v1.2.0/docs
2. https://indiaevm.org/evm_tr2010.pdf
3. https://pgl.yoyo.org/black-box-voting/bbv_chapter-08.pdf
4. http://elections.bc.ca/docs/Internet-Voting-Discussion-Paper.pdf
5. https://www.telegraph.co.uk/technology/2017/07/31/hackers-take-control-us-voting-machines-less-90-minutes/
6. https://bitcoin.org/bitcoin.pdf
7. http://aircconline.com/ijnsa/V9N3/9317ijnsa01.pdf
8. https://tangleblog.com/2017/10/09/explaining-series-new-iota-whitepaper-vers-1-3-summarized/
9. https://eprint.iacr.org/2011/191.pdf