ISSN (Online) 2394-6849

International Journal of Engineering Research in Electronics and Communication Engineering (IJERECE)

Vol 8, Issue 2, February 2021

Digital Voting with use of Blockchain Technology and Artificial Intelligence

[1] Vikash Kumar Singh, [2] Durga Sivashankar [3] Neha Kumari

[4] Anand Sivasankaran [5]Dattatraya Hebbar

[1] Societe Generale GSC, [2] Honeywell Technology and Services Pvt Ltd.,

[3] Academician ,[4] GenieTrox[5] Societe Generale GSC

Abstract: Democratic voting is a crucial and serious event in any country. The most common way in which a country votes is through a paper based system. Digital Voting with usage of Blockchain Technology and Artificial Intelligence aims to outline our proposal to solving the issues of manual voting . Security of digital voting is always the biggest concern when considering to implement a digital voting system. With the use of blockchains a secure and robust system for digital voting can be devised.

INTRODUCTION

Digital voting is the use of electronic devices, such as voting machines or an internet browser, to cast votes. These are sometimes referred to as e-voting when voting using a machine in a polling station, and I-voting when using a web browser. Blockchain technology originates from the underlying architectural design of the cryptocurrency bitcoin. It is a form of distributed database where records take the form of transactions, a block is a collection of these transactions

Our idea explains how blockchain technology could be used to implement a secure digital voting system

PROPOSAL

. Our design is to create a system that doesn't entirely replace the current voting but rather integrates within a current system. We decided to do this to allow for as many different ways to vote as possible, this is so voting can be accessed by the majority of the population.

Registration

The first aspect of our design is the registration process. To allow users to register to vote our proposed service utilizes both postal based forms as well as web forms requiring the same information to ensure we cater for those without a direct internet connection. This information includes their national identity number, postal address, optional email address and a password. All this information then forms a transaction for the user agreeing with the government that they are asking to vote; this transaction is then created on the voter blockchain

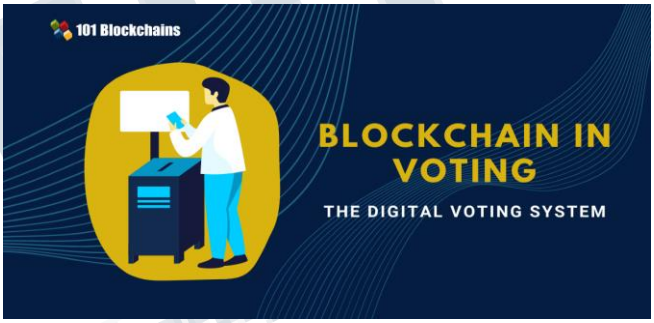

Figure – Blockchain in Voting

During this process, a voter blockchain is used to keep a record of both transactions taking place at each stage of this process for each voter:

1. Firstly, a transaction is created when a user 'registers'.
2. The next transaction is created when a government miner authorizes that user's right to vote.

After the correspondence is received by the user, they can then await voting to open to use their credentials to vote. It is important to note that this voter blockchain will never contain details of the vote cast by the user

Voting Mechanism and Architecture

As part of our design we have an encryption method based on public and private keys and have implemented a structure where the data is segregated within the blockchain. This segregation has been achieved by getting the constituency level nodes to generate keys pairs. The public keys are then distributed to the connected polling station nodes, which then use the public key to encrypt any vote made to that polling station. The data is then stored in an encrypted format within the blockchain and

ISSN (Online) 2394-2320

International Journal of Engineering Research in Electronics and Communication Engineering (IJERECE)

Vol 8, Issue 2, February 2021

propagates out to the entire network.

If a hacker manages to get hold of a constituency private key, they would only be able to decrypt certain sections of the blockchain, so would never know the full outcome of the vote. Once the voting deadline has passed, the software within the constituency nodes publishes the private keys to allow the blockchain network to decrypt the data, which in turn means the votes can then be counted.

The Voting Process

As there are two methods of voting (web browser, physical polling station) the way the user will input the authentication details shall differ; however, in order to vote they are required to provide all three pieces of information. It is also important to note that each user will have been registered at a certain constituency so they will only be able to vote at a local polling station within that constituency or via the internet at the URL provided on the ballot card.

Behind the scenes the polling station will consult the voter blockchain to ensure the voter has not already used up their vote. If the user does not have a vote, then the station will then allow the user to continue to the voting screen.

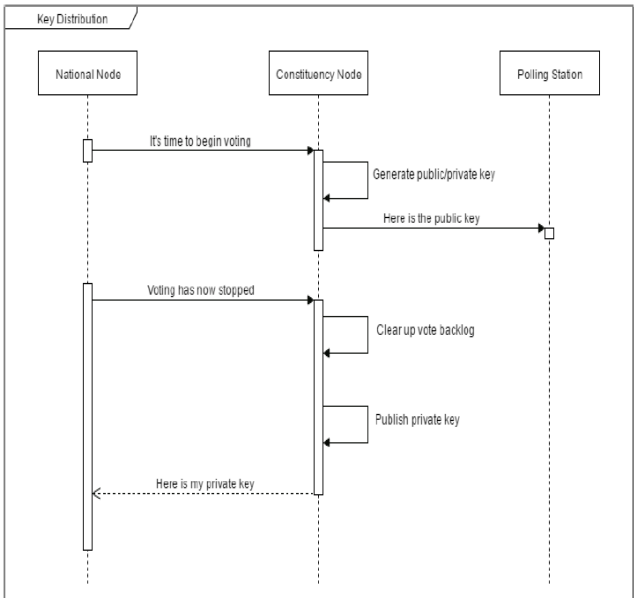

Figure – Diagram of key Pair Encryption

After selecting their vote (from the selection of options including abstention) and then confirming the submission, the vote will become a transaction, it will be encrypted with the relevant constituency's public key. This transaction is then passed to the constituency node where it is added to a block and the update is then pushed to all other nodes connected to that constituency node. The connected nodes then pass the data on to their peers until the whole network is updated. Once the vote has been confirmed the polling station will then generate a transaction to remove the user's vote within the voter blockchain.

It is important to note that there are two distinct blockchains being held; one which contains transactions relating to which users have registered and which users still have a vote, the second containing the contents of the vote (such as what party was voted for.). Through the use of these two distinct blockchains we ensure voter anonymity when selecting their vote.

ANALYSIS OF DESIGN

We also have the added security of an auditor who checks and keeps track of people connecting to the network and the locations of each node. This is a feature that current systems such as bitcoin lack. (Learncryptography.com, 2016) The online aspect of the voting within our system is the largest attack vector for hackers as they could potentially exploit voters through their own devices in a host of ways. To combat this software could be developed that could be downloaded onto the client's device to establish a secure connection to the polling station

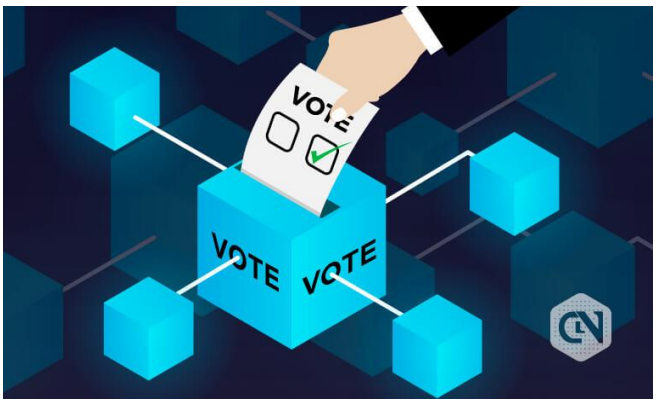

Figure :Digital Voting

ISSN (Online) 2394-2320

International Journal of Engineering Research in Electronics and Communication Engineering (IJERECE)

Vol 8, Issue 2, February 2021

Conclusion

To conclude, our proposal comprises of a geographically distributed network comprising of machines from both government and public infrastructure; this infrastructure houses two distinctly separate blockchains, one for voter information such as who has voted and the other for vote information such as what has been voted. These blockchains are held completely separately to remove any threat to link votes for certain parties back to individual voters while maintaining the ability to track who has voted and how many votes are present. Once registered you are then allocated a vote after verification of your details has been completed.

To ensure these registered voters are who they say they are when voting begins there is a 3 factor authentication method. Further to this we also need to ensure they are not forced to vote in a particular way so we have incorporated a double-check service where by users shall be prompted a second time to confirm their submission before the vote is sent; this also then allows us to almost eradicate accidental votes. It would be close to impossible for any person(s) to gain access to all the votes without first taking control of the entire service network. Moving on from this the publication method of the private keys allows anyone to read the blockchain of votes and decrypt them with the newly available constituency private keys to verify the result of the election

REFERENCES

[1] Genesis block (2015) Available at: https://en.bitcoin.it/wiki/Genesis_block (Accessed 27 September 2016)https://www.techrepublic.com/pictures/

[2] Learncryptography.com. (2016). Learn Cryptography - 51% Attack. Available at: https://learncryptography.com/cryptocurrency/51-attack (Accessed 29 Sep. 2016)

[3] Springall, D., Finkenaur, T., Durumeric, Z., Kitcat, J., Hursti, H., MacAlpine, M., Halderman, J.A. (2014) Security Analysis of the Estonian Internet Voting System. Available at: https://jhalderm.com/pub/papers/ivoting-ccs14.pdf (Accessed: 25 September 2016)