Public Blockchain Technology Model for Indian Polity System.

Annapurna Bala

HOD, Dept. Of Computer Science,
Ch.S.D.St Theresas Autonomous College for Women
Eluru, Andhra Pradesh, India.
annapurnagandrety@gmail.com

Dr.K.L.Saraswathi Devi

*HOD, Dept. O*f Mathematics.
Ch.S.D.St Theresas Autonomous College for Women
Eluru, Andhra Pradesh, India.
saraswathikatneni@gmail.com.

Abstract:

The principles of democracy cannot work fully without trust in the purity of the voting process. It is here that the logic of the whole process of democratic elections is getting weaker and weaker from year to year. 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 is the use of electronic devices, such as voting machines to cast votes in a polling station. Security of digital voting is always the biggest concern when considering to implement a digital voting system. With such monumental decisions at stake, there can be no doubt about the system's ability to secure data and defend against potential attacks. One way the security issues can be potentially solved is through the technology of Public Blockchain technology. Blockchain technology originates from the underlying architectural design of the crypto currency, bitcoin. It is a form of distributed database where records take the form of transactions, a block is a collection of these transactions. With the use of blockchains a secure and robust system for digital voting can be devised.

.Keywords: *Digital voting***,** *Public Blockchain, crypto currency*

1. Introduction

Blockchain, mostly known for Bitcoin and other crypto currencies. It is certainly one of the most talked-about technologies right now. As our societies grew more complex and our trade routes grew more distant, we built up more formal institutions, like banks for currency, governments, corporations. These institutions helped us manage our trade as the uncertainty and the complexity grew, and our personal control was much lower. Eventually with the internet, we put these same institutions online. Indeed, blockchain can be that technology that can help us lower our uncertainties about identity and what we mean about transparency in long distances and complex trades, like in election systems for instance. Blockchain "could revolutionize voting and elections. Using blockchain technology, we can make sure that those who are voting are who they say they are and are legally allowed to vote. Plus, by using blockchain technology, anyone who knows how to use a cell phone can understand the technology required for voting. The application of

blockchain technology could eliminate voter fraud, providing a clear record of the votes cast, and preventing any chance of a rigged election. This process has raised interesting questions for governments about the future use of blockchain in electoral processes, and in the public sector more broadly, and could potentially lead to new ways to ensure the integrity and inclusiveness of the election process. Governments may come to realize that the security and integrity of electoral processes is not just a matter for state control, but also an area that can be guaranteed collectively, supported by blockchain,

2. Public Blockchain technology

A public blockchain network is completely open and anyone can join and participate in the network. The network typically has an incentivizing mechanism to encourage more participants to join the network. Blockchain technology was first used within Bitcoin and is a public ledger of all transactions. A blockchain stores these transactions in a block, the block eventually becomes completed as more transactions are carried out. Once complete it is then added in a linear, chronological order to the blockchain. The initial block in a blockchain is known as the 'Genesis block' or 'Block 0'. The genesis block is usually hardcoded into the software; it is special in that it doesn't contain a reference to a previous block. Once the genesis block has been initialised 'Block 1' is created and when complete is attached to the genesis block. Each block has a transaction data part, copies of each transaction are hashed, and then the hashes are paired and hashed again, this continues until a single hash remains; also known as a merkle root (Figure 1). The block header is where the merkle root is stored. To ensure that a transaction cannot be modified each block also keeps a record of the previous blocks header, this means to change data you would have to modify the block that records the transaction as well as all following blocks, as seen in Figure 2.

(Bitcoin.org, 2009) A blockchain is designed to be accessed across a peer-to-peer network, each node/peer then communicates with other nodes for block and transaction exchange. Once connected to the network, peers start sending messages about other peers on the network, this creates a decentralised method of peer discovery. The purpose of the nodes within the network is to validate unconfirmed transactions and recently mined blocks, before a new node can start to do this it first has to carry out an initial block download. The initial block download makes the new node download and validate all blocks from block 1 to the most current blockchain, once this is done the node is considered synchronised.

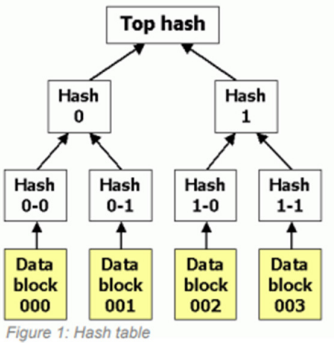

Figure 1: Hash table

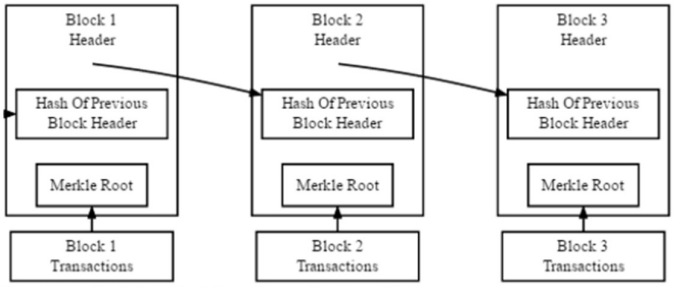

Figure 2: Simplified Bitcoin Block Chain (Source: Bitcoin.org, 2009)

3. Problems with a paper based voting system:

In today's society where electronic technology is growing at an ever increasing rate, it is hard to understand why governments are not converting their paper based election systems to electronic form to guaranty "One Person – One Vote, and to eliminate fraud and corruption. An example of how a paper based voting system is flawed and prone to corruption can be found in the Haitian elections, where the last election was invalidated due to fraudulent paper ballots (produced in Dubai) used to stuff the ballot boxes and elect a president illegally. To repair this damage it has already cost the Haitian government approximately $100,000,000, which could be a recurring cost if the fraud occurred again, and it is difficult to bring charges against the people committing the crime due to lack of evidence and an audit trail that could be used as a "Chain of Evidence" by prosecutors. Another example is when paper election ballots ran out at an American election and additional ballots were produced using a printer and makeshift process for creating the new ballots on white paper instead of the normal blue ballots. People rushed to obtain the new white ballots and quickly completed them and stuffed them into the ballot boxes in a manner that was not traceable and could have been fraudulently submitted, showing that even first world countries suffer from the use of paper based ballots.

4. Challenges:

By allowing for the continued use of paper based voting, it is much too easy for corruption to occur, resulting in the people's voice not being clearly heard, or drowned out entirely by fraud. If the people's voice is not the foundation of our election system, what good is having an election in the first place? The election of fraudulent and corrupt politicians has led to countries that are more dictatorial then democratic, drowning the people in misery brought on by funds being routed to private causes and corrupt individuals instead of being used to support the people where the funds could be used to improve their lives, develop a better infrastructure, or create a better education and medical system, and generally improve the well-being of the countries society. All because politicians who are in charge of setting the direction and foundation of the election system are perhaps a part of the problem themselves.

5. Proposed Model, Blockchanin based Digital voting

To eliminate the problems brought on by the use of paper ballots and integrate safety policies designed to root out fraud and corruption, while guarantying "One Person – One Vote", it is imperative that an electronic voting system be implemented. This system would provide ballot displays on a video screen instead of paper. Help screens would be available to the voter by simply clicking on a button, and data entry validation can guaranty that all necessary ballot fields have been entered correctly – thereby eliminating data entry failures or votes being lost due to illegible hand writing or mistakes (like not punching a hole in the right selection field, or using a pencil / pen that cannot be read by a scanner). But first, you must insure that the voter is who they claim to be and not a name found in the local cemetery or obituary column. Secondly, you must insure that the voter has not voted previously at another site in this election. How do you do that? Using a Voter ID Smart Card that contains the voter's bio-metric data (eye scans, facial recognition, palm scan, finger prints, etc.) stored in the smart card's chip and readable at the voting station would verify that the voter is who they claim to be. But, simply verifying that a person is who they claim to be is only part of the resolution, you must also

have a means to validate that the voter has not previously voted in this election – or that they are an eligible voter in the first place (i.e., felon not allowed to vote, those people on terrorist watch lists, or other reason that would stop a person from being allowed to vote)

6. Implementation

The network is a multi-tiered, decentralised infrastructure which houses the two distinct blockchains, the network is divided into three abstract tiers, National, Constituency and Local. The local tier contains all the digital polling stations across the country, each of which is associated to a constituency node. A local node is setup to only communicate with the other local nodes under the associated constituency node and the constituency node itself. The constituency tier contains all the nodes that are deemed to be at a constituency level. These nodes would be directly connected to each other and to a subset of polling stations depending on location. The national tier is a collection of nodes that are not tied to location, their pure purpose is to mine transactions and add blocks to the vote blockchain, all constituency nodes communicate to a national node and national nodes can communicate with each other. Independent bodies will monitor and audit the voting process. These bodies will host or have access to a national node and will be able to verify that the unencrypted results match the encrypted votes. Individuals and organisations can volunteer to be a national node. These applications are processed by the government to ensure that they meet the minimum requirements set by a governing body. These individuals will also act as miners during counting process. 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 propagates out to the entire network. Due to the fact each constituency will have a different public key means that chunks of data within the block chain will be encrypted differently to a chunk of data next to it. 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.

4. Benefits:

The benefits derived from an electronic voting system

1. Guaranteed “One Person” through a Voter ID Card based on a Smart Card whose chip contains the bio-metric information for the individual.
2. Guaranteed “One Vote” through the electronic voting systems application processing.
3. Audit Trail to use as an Evidence Trail should investigations be warranted for criminal processes, or just to seek ways to improve efficiency.
4. Documentation provided by the system can be used to support prosecution of people committing fraud or corruption.
5. Near Real-Time voting results.
6. Ability to provide voting results immediately upon close of election.
7. Use of Child Records for searching bio-metric information in support of criminal, or even medical research.
8. Elimination of Paper at a great cost savings.

9. Ability to support people with disabilities and those that speak different languages.
10. Ability to provide instructions and examples to assist voters using the system.

5. References

[1]Bitcoin.org (2009) Bitcoin Developer Guide. Available at: https://bitcoin.org/en/developerguide#block-chain-overview

[2] Electronic ID Card (no date) Available at: https://e-estonia.com/component/electronic-id-card/

[3] Genesis block (2015) Available at: https://en.bitcoin.it/wiki/Genesis_block

[4] Learncryptography.com. (2016). Learn Cryptography - 51% Attack. Available at:

https://learncryptography.com/cryptocurrency/51-attack

[5]https://www.ibm.com/blogs/blockchain/2017/05/the-difference-between-public-and-private-blockchain/

[6] Thomas Bronack, White Paper on "The problems with a paper based voting system"