Secure Electronic Voting via Blockchain
Final Report

Joe Johnson, Cameron Jordal, Colton Trebbien

ABSTRACT:

This paper looks at a novel method for secure electronic voting based on an adaptation of blockchain technology. As demand for accessibility in elections grows, as well as the threat of malicious third parties seeking to alter the outcomes of elections, the pressure for a new, secure digital voting system is mounting. This paper sought to achieve this by building a public-verifiable, blockchain-based database that would be inherently tamper-proof. We found that by using cryptographic hash functions and asymmetric encryption of vote casting, or voting transactions, we could ensure both the privacy necessitated by a voting system as well as the integrity created by a publicly available and verifiable database.

KEYWORDS:

blockchain, electronic voting, cryptography, secure elections

INTRODUCTION:

Voting allows people to make decisions about issues that are important to them, that represent their voice, and their opinion. In order to facilitate a valid election, the voting system used needs to be able to accurately and securely count all votes. In recent times, there have been many controversies stemming from today's global elections that have brought attention to the security and validity of our current voting systems. People have worries about the possibilities of fraud, miscounting of votes, and officials and governments making it harder to register or cast a vote in the first place. Current voting systems are also still paper-based when we live in a world where the internet has the potential to reach millions of people in a fast and efficient time. Recent research done in India has shown that not only is electronic feasible - but in many cases - can lead to a decrease in electoral fraud (Debnath, 2017). This still leads to the question of ‘how do we ensure and verify the security and anonymity of votes being made? A new advancement in technology, blockchain, has been brought up as a potentially secure new online voting system. In this paper, we discuss our findings and go into the strengths and weaknesses of such a blockchain voting system as well as implement a coded version of how a blockchain voting system would work.

RELATED WORK:

It's important to understand what requirements make a strong voting system and Rura, B. Issac and M. K. Haldar, go in-depth in the paper “Secure electronic voting system based on image steganography” into the requirements that an electronic voting system, or any voting system for that matter, should have. Starting with completeness, all votes made using the voting system need to be counted and tailed correctly. The system also has to be sound, that outside or unauthorized voters can not disrupt or affect the voting process. Voters also shouldn't be able to vote more than the specified amount of times permitted. Privacy is another important factor to take into account as all votes should be kept secret and to that end, voters also shouldn't be able to obtain a receipt or copy of their vote to share with others. This is because it can lead to coercibility where others could entice voters with discounts or threaten them to vote a certain way. It also has to be convenient for voters to cast their votes quickly and effectively and for an E-voting system, it also has to be possible for voters to vote from anywhere at any given time during an election period. This list of requirements for a satisfactory voting system is a good tool to use when analyzing our own voting procedure and when trying to figure out how reliable, secure and robust our implementation is.

“Electronic Voting Recording System Based on Blockchain Technology” by S. Agbesi and G. Asante in which they propose a solution to implement a secure and transparent system, through

blockchain, for stakeholders to have visibility of the entire process of vote recording and storage. In the paper, they also gave thorough explanations of the required parts or terminologies of a blockchain system including what a block, ledger, DLT(Distributed ledger technology), public-key cryptography, and cryptic hash functions all accomplish and piece by piece, come together to work inside the blockchain system. Their implementation is not completely online but instead acts as a secure tallying phase once voting has finished a place of polling. After voting is done, the polling station will make a transaction between them and an election node. It would include the polling station ID, the results in the form of tokens, and a verification code. The transaction is then signed using the private key of the Polling station. Before the election is even taken place the pooling nodes would have broadcasted their public keys to all the nodes. After that, a new block is created and broadcasted to all the nodes where the election nodes would verify the source using the nodes public key and confirm the verification code. The block is then added to the node once it's verified. This system although not online shows how after voting has ended a secure way to handle the results.

In Aicha Fatrah, Said El Kafhali, Abdelkrim Haqiq, and Khaled Salah's paper "Proof of Concept Blockchain-based Voting System" they explain how a blockchain voting system could potentially be designed by using a token-based system in turn for casting a vote inside a blockchain framework. First, a voter would send their personal information to the election administrators and when confirmed as a verified, eligible voter, they are then issued a token to their voting wallet. In their paper, they explain how the token is coded in a way that it can only be spent once, and can only be used when voting for a candidate. This avoids the possibility of double voting and others trying to send tokens to other people. Once they have the token they are able to cast it to the candidate of their choosing. This paper utilizes a zero-knowledge proof to validate each voter's ballot. Voters would be able to see their identity on the blockchain to keep track of their vote to confirm it was counted and tallied correctly. Miners In this system would validate the transactions and add the new blocks to the system.

Our implementation uses many of the ideas from these papers to help us understand and create an online voting system using blockchain. The above papers don't commit to a complete online voting system and most of their implementations are just used as a more secure voter database. Although this report mainly focuses on the actual blockchain implementation, the system as a whole is explained including voter authorization.

BLOCKCHAIN:

One of the reasons why blockchain has become a huge emerging technology is because it's designed with trust in mind. In the system, different parties can interact with each other without having to worry about trusting one another.

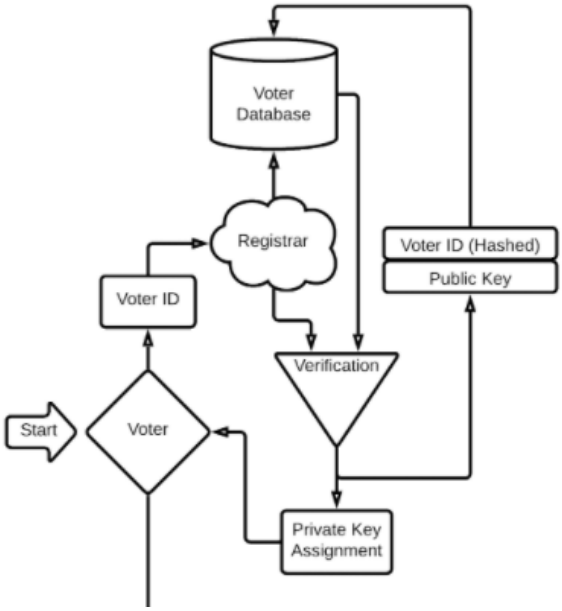
Blockchain is a decentralized public ledger technology meaning which means it acts as a public-recorded keeping scheme, where everybody in the public would have access to the available data. For more common uses of blockchain with cryptocurrencies such as bitcoin, ethereum, or - upcoming contender - dogecoin, the transaction between entities is what is stored inside the blockchain block. These transactions are commonly stored on a merkle tree where every transaction or leaf node is made with a cryptographic hash and every non-leaf node is a hash of its respective child nodes. In short, this data structure allows for efficient security as anyone could come along and verify that the hashing of data is non-irregular all the way to the top of the tree. It also allows for scaling and maintains the integrity of the transactions. For our implementation and for our voting system purposes, we consider the transaction itself to be a vote and we omit the use of a merkle tree not because it isn't efficient, but we have a different voter verification system and our implementation will probably not be used on such a scale that it requires the use of a merkle tree. As voting elections become larger, however, it would be wise to implement this data structure since creating a hash for each transaction is inefficient and not very scalable. In order to keep things less convoluted for potential voters as well who want to know how the system works, it's best to keep the implementation down to easier to explain levels such that someone who has no previous cryptology knowledge would be able to trust the system they are using.

Each block contains a transaction as previously stated, but it also contains a hash of the previous block and a hash of its own. This creates a linked-list structure as each block would be able to point towards its previous block. This is also why it happens to be called a blockchain. The hash is made from the data inside the block along with the hash of the previous block. This is done using a hashing algorithm, the most commonly used is the SHA-256 hashing algorithm. This scheme allows one to verify the integrity of the chain all the way to the root/genesis block.

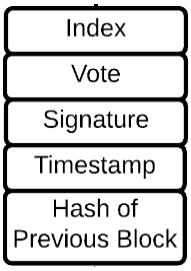
The power of blockchain really comes from decentralization. Blockchain is implemented over a peer-to-peer network. The decentralized nature negates the need for trust in a centrally controlling authority and makes it so that there is no central point of weakness for potential hacks. When a transaction is made, it is broadcasted to all the peers or nodes on the network. Each node holds a copy of the blockchain. Mining nodes would collect transactions. Because of this node system, there is never a guarantee that any particular block or chain will be the best version of the chain. Nodes are incentivized to keep adding blocks to the chain rather than override the old blocks. For many cryptocurrencies, they use a proof-of-work system, where the chain with the most/highest proof of work is what the nodes collectively agree on being the current standing best chain.

DESIGN AND IMPLEMENTATION:

For our design (see Appendix for full diagram), we propose using a blockchain system to help secure online voting. Our implementation starts with an authentication/ registration phase in which potential voters must authenticate themselves with some form of voter ID(s). The voter ID can then be verified by a known and trusted source (such as a government portal). Upon this step, a voter can either be verified as a valid voter or rejected as an invalid one. If verified, the hash of their voter ID(s) can be compared to a public database of hashed voter ID(s), and if, and only if, it does not already exist in the database, then a new private/ public key pair will be generated for the newly verified voter, with the private/public keys going to the voter (the private goes to the voter alone), and the hashed ID as well as the public key getting published in the public database. However, if the voter could not be verified or was shown to have already registered and received a public/private key, they will receive no such keys, and their hashed ID will not be (re)published in the database (partial view seen at right, full view in appendix).



Given that they were granted a private/public key pair though, the voter now has the ability to vote on the blockchain, as they can make a transaction under the name of their public key and sign the digest of the transaction with their private key, verifying the transaction was indeed issued by them and ensuring the integrity of the transaction contents. Once these voting transactions have been made, they can be stored in blocks on the voting blockchain.



Block implementation:

The blocks that make up a blockchain contain all necessary information for keeping track of the transactions that occur. In our case, these blocks are used to account for votes being cast. The block consists of an index (an incrementing number to identify length in the chain), a list of transactions (casting of the vote), signature derived from the private key (encrypted using SHA-256, salted, and buffered), nonce (to ensure no duplicate blocks), and a hash to indicate the previous block that it is

connected to in the blockchain. To allow better processing, the blocks are hashed in SHA-256, which is the same hashing used for public and private key creation, as well as for signing transactions. Rather than the blocks containing the overall value stored at an address (candidate in our case), an examination of the transactions cast would lead to the total at any given location.

Blockchain Implementation:

The blockchain is a system to move, process, and store blocks. In our system, the blockchain was implemented with a list of the current - un-mined - transactions, a list of valid candidates to vote for, and the chain itself (see Appendix for full diagram). The system allows for the registration of candidates, chain replacement, transaction creation, mining, proof-checking, and validation all within its own class. The included files provide testing to demonstrate the capabilities aforementioned.

RESULTS AND ANALYSIS:

Using our list of what a strong voting system requires from Rura, B. Issac and M. K. Haldar's paper as mentioned in the related work part of this paper, we can analyze our blockchain system. Starting with the completeness of the system, all votes are securely counted and put on the public chain for everyone to see as well as verify. In the blockchain system, there is also no worry for human error when it comes to tallying as all the votes are counted up using machines. The public chain also makes it easy to go back and verify if an incorrect vote was added. For the soundness aspect of a blockchain, there are a couple of ways that disruption of voting may occur.

Soundness:

Some people might be worried about the possibility of being able to vote more than once or even being able to send another vote token to another wallet (aside from a candidate's). To be able to double spend a token would be really hard within a blockchain system as each transaction is checked and verified before it's put into a block. If that block somehow ends on the blockchain without the miners verifying it, once the election is over people would verify the blockchain and see that a transaction was made by the same person or if they tried to send it to a wallet that wasn't a registered candidate.

Privacy:

One of the fundamental aspects of our blockchain voting system is it protects the voters' privacy while also still making the system public. This is done through a combination of hashing and asymmetric cyrptopgrahy. By hashing the voters' identifying information, we publicly record their registration as eligible voters and can verify if they have tried to vote more than once, yet their actual identifying information is still unknown to anyone but themselves and the verifier. This, in combination with the use of asymmetric cryptography to tie cryptographically signed votes to a respective hashed I.D, allows voters and the votes they make to be publicly verified without it ever being possible to get the actual, human identity of the voter.

Inexploitability:

In our system, voters wouldn't be able to vote twice. Many people worry when it comes to blockchain if this is a possibility. There are two potential ways that double spending might occur. First with the 51% majority attack. The proof of work is what allows the nodes to add a new block to the chain if all the nodes collectively agree on the integrity of that block. Mining power is distributed, which means it's not in the hands of a single entity. However, if someone is able to get over 50% of the hashing power then they can potentially change the ordering of transactions or reverse transactions they made, which of course would lead to double spending. A 51% attack really depends on the magnitude of the network. For our voting system too, It would be hard to change votes without the private key of the voter and it would be easy to see if someone used the same id more than once or tried to use a fake unique id.
The other one is a race condition, this is where someone tried to send transactions rapidly to the network, the first transaction would look to the receiver like it was valid but the miners would have seen the

double-spend first and rejected it. This is a problem with many cryptocurrencies where the attacker has direct and fast communication with the receiver who would unknowingly think that the transaction was valid. In our system, we aren't sending anything back to a voter and instead are waiting until all votes are made before counting, so the possibility of this attack being a problem is nonexistent.

Eligibility:

We did not tackle the direct implementations of eligibility in this work, however, it should be relatively straightforward to pass a unique set of voting credentials or voting ID(s) to an applicable authority with that kind of information. In the case of an election, that could be handled by a government portal that takes the actual voter ID(s) and can verify if they are valid.

Fairness:

This also has to do with the integrity of our system. But also that none can indicate the tally of the election before all the votes are counted. In the broad aspect of voting, it's impossible to know how anyone is going to vote besides physically watching them vote. Which is a more general potential problem with an online voting system. Since no one is going to the polls and instead are voting behind anonymous screens, it's impossible to know what the voters' circumstances are. This leads to a couple of problems as people could take screenshots or pictures of themselves voting which could then be incentivized by parties with things such as discounts or currency for voting a certain way. The election officials would also have no idea about whether a voter is being forced to vote a certain way or not as their casting is hidden behind a screen.

Robustness:

As mentioned before, The system is robust and votes are correctly counted even if outside parties try to cheat. The list is all publically verified as well which makes it easier than current voting systems to catch acts of fraud.

Uncoercibility & Receipt-freeness :

As mentioned in the fairness category, our system potentially fails when it comes to a lack of coercibility given the nature of online voting. Receipt free-ness is also open for debate as well as our system requires the use of a private/public key system for encryption. A potential voter could theoretically prove their vote, not just from a screenshot, but also if they could show that using their public key matched the same output after encryption. Otherwise, if a voter wanted to keep their vote a secret all they would need to do is keep their private key to themselves.

Convenience & Mobility:

This is where a blockchain online voting system is its strongest. The act of voting should be convenient and shouldnt require a voter to put in large amounts of energy to participate in. There are many pros that come with online voting such as it may lead to increased voter turnout. With the age of the internet that many younger people have now grown up in, it may lead to better turnouts for younger generations which notoriously have low turnout rates. Of course, this system needs the internet to be able to vote which a very small minority don't have access to. This is a simple problem to solve, for areas that aren't covered you can still have electronic voting stations and even with this small issue, it still allows for more people overall with easier access to voting, making this is a fine tradeoff.

CONCLUSION:

Our project has demonstrated a potential new way to secure online voting with blockchain. There are many strengths that an online blockchain voting system brings. The first one and most promiate one is that it's a decentralized system. This protects against attacks where all the data is held by a central authority. It also protects against a central authority trying to control or manipulate the vote. Blockchain also provides efficient verification as the voter registration and votes are public, anyone can check to see

if any tampering has taken place. Anonymity is kept and all votes are private to a certain extent, it doesn't add any new workarounds that don't already exist in current paper-based voting systems. Transparency is also a huge advantage that blockchain offers. Voters can see their votes on the blockchain and also verify that the votes were counted. We also talked about the efficiency and mobility as voters would be able to vote from anywhere with access to the internet and the processing time to count and verify votes is a lot faster than hand counting.

We also covered some potential issues that our online voting system runs into. Because of how we encrypt the vote it's necessary for the voter to keep their private key a secret or else it could potentially be used as a receipt. On the other side of that, if a voter loses their private key, it would be hard for them to verify that their vote was counted on the chain. Another thing that comes from many voting systems is that people need to trust the actual device that they are using to vote on. A compromised device could find their secret key or collect information about the voter. Because people wouldn't have to physically show up to vote, election administrators wouldn't be able to see what circumstances are happening behind the device's screen, who could potentially be watching or forcing some to vote a certain way is dangerous.

DISCUSSION:

For our group, a lot of our time went into researching and mapping out how our voting system would work. Blockchain is a very complex data structure and has a variety of different uses and applications. There is a lot of potential for blockchain to be used to secure online voting, but some issues still remain. As it goes with electronic methods, the risk of hacking goes up considerably, as you open up your system to the world, and when it comes to an election or something that has major impacts with considerable money at stake, malicious actions should be expected. Our solution to combat this was to make data public; however, this does present another risk. If someone was ever able to gain access to your voter ID(s) or private key, they could always look up election data and see who you voted for. This is a problem not currently seen, as ballots are destroyed after being cast. Yet, on the flip side of that, it should also be noted that this apparent weakness can also be a major strength when the vote counting authority itself cannot be deemed trustworthy, as is the case in many parts of the world because the vote-counting authority is - in fact - everyone. Suffice to say there are tradeoffs, yet it is more likely that a lot of the main issues on why online voting hasn't been taken up yet in the majority of the world are not with the system being implemented. We have seen in recent times how large parties cast doubt upon the voting systems used and that reduces the trust that is needed for people to accept and engage in a new election system.

LESSONS LEARNED:

This project has allowed us to really understand *how* blockchain works. Prior to this project, we had a vague to minimal understanding of what blockchain was and we knew nothing about the specific components that comprise blockchain nor how they interact. Furthermore, we acquired insight into ways that blockchain voting could improve most -- if not all-- current voting systems, although some tradeoffs would have to be made. This would be through the accountability, accessibility, and security that a working blockchain system could provide.

REFERENCES:

Aicha Fatrah, Said El Kafhali, Abdelkrim Haqiq, and Khaled Salah. 2019. Proof of Concept Blockchain-based Voting System. In Proceedings of the 4th International Conference on Big Data and Internet of Things (BDIoT'19). Association for Computing Machinery, New York, NY, USA, Article 31, 1–5

Debnath, Sisir, et al. "The Impact of Electronic Voting Machines on Electoral Frauds, Democracy, and Development." *SSRN Electronic Journal*, 2017, doi:10.2139/ssrn.3041197.

E. Febriyanto, Triyono, N. Rahayu, K. Pangaribuan and P. A. Sunarya, "Using Blockchain Data Security Management for E-Voting Systems," 2020 8th International Conference on Cyber and IT Service Management (CITSM), Pangkal Pinang, Indonesia, 2020, pp. 1-4, doi: 10.1109/CITSM50537.2020.9268847.

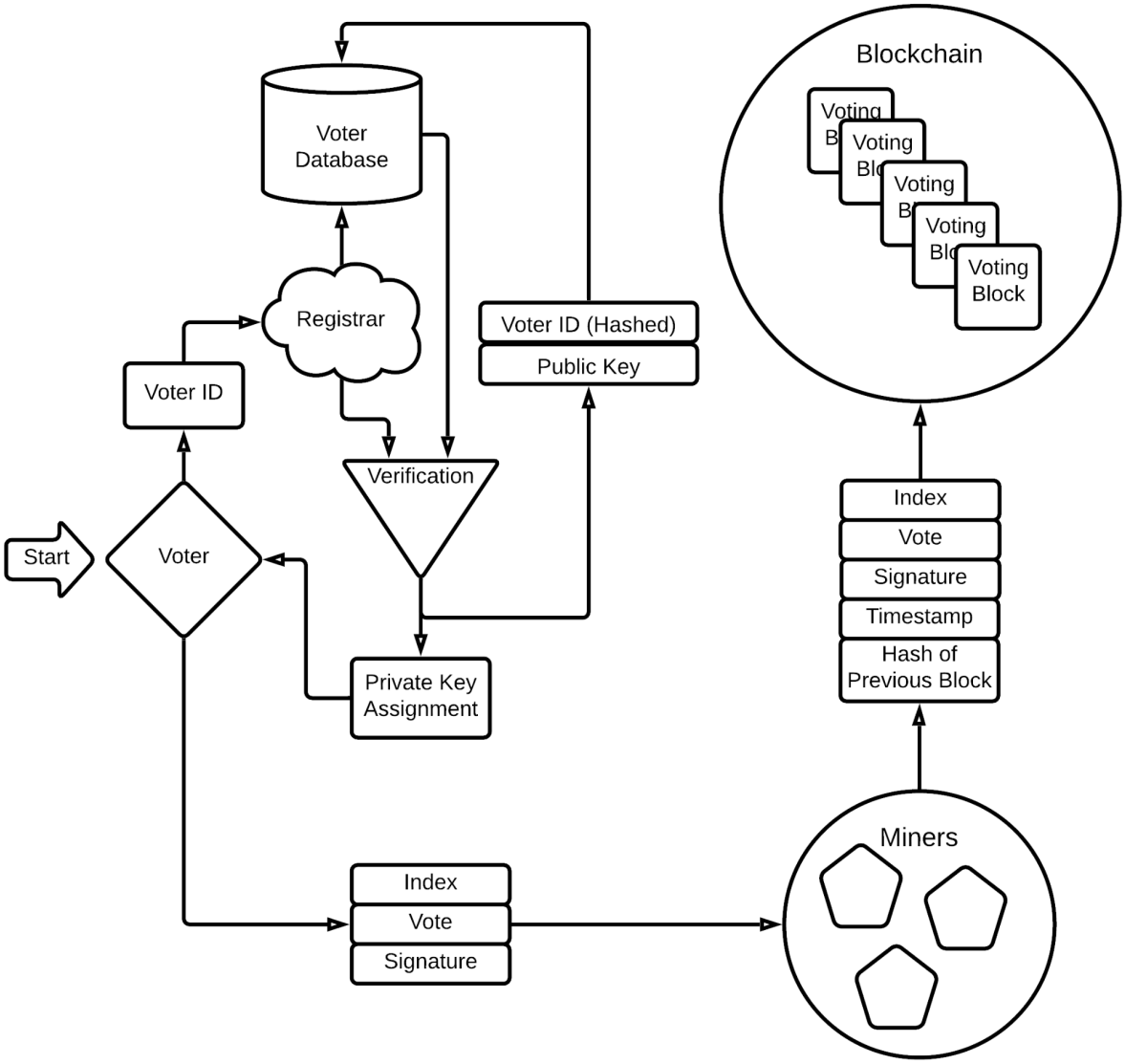
K. Patidar and S. Jain, "Decentralized E-Voting Portal Using Blockchain," 2019 10th International Conference on Computing, Communication and Networking Technologies (ICCCNT), Kanpur, India, 2019, pp. 1-4, doi: 10.1109/ICCCNT45670.2019.8944820.

L. Rura, B. Issac and M. K. Haldar, "Secure electronic voting system based on image steganography," 2011 IEEE Conference on Open Systems, Langkawi, 2011, pp. 80-85, doi: 10.1109/ICOS.2011.6079268.

N. Kshetri and J. Voas, "Blockchain-Enabled E-Voting," in IEEE Software, vol. 35, no. 4, pp. 95-99, July/August 2018, doi: 10.1109/MS.2018.2801546.

S. Agbesi and G. Asante, "Electronic Voting Recording System Based on Blockchain Technology," 2019 12th CMI Conference on Cybersecurity and Privacy (CMI), Copenhagen, Denmark, 2019, pp. 1-8, doi: 10.1109/CMI48017.2019.8962142.

APPENDIX:


Blockchain
Voting Block
Voting Block
Voting Block
Voting Block
Voting Block
Voter Database
Registrar
Voter ID (Hashed)
Public Key
Voter ID
Verification
Start
Voter
Index
Vote
Signature
Timestamp
Hash of Previous Block
Private Key Assignment
Index
Vote
Signature
Miners