COMPUTING
WITH
PLYMOUTH
UNIVERSITY

Digital Voting with the use of Blockchain Technology

Team Plymouth Pioneers – Plymouth University

Andrew Barnes, Christopher Brake and Thomas Perry

Word count: 2992

Contents

1. Summary

The aim of this report is to outline our proposal to solving the issues of digital voting by using blockchain technology. The report starts by introducing the problems with current voting practices, it then goes into a brief explanation of what blockchain technology is and how it is currently used. The following section looks at present day deployments of digital voting and the issues they face. The main section of the report is a detailed breakdown of our proposed design followed by an analysis of potential flaws and threats. The final section is a conclusion of how we feel our design solves the issue at hand.

2. Introduction

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, but is it not time to bring voting into the 21st century of modern technology? 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.

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 blockchains.

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. With the use of blockchains a secure and robust system for digital voting can be devised. This report outlines our idea of how blockchain technology could be used to implement a secure digital voting system.

3. What is a Blockchain and how is it Commonly Used?

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. ('Genesis Block', 2015) 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

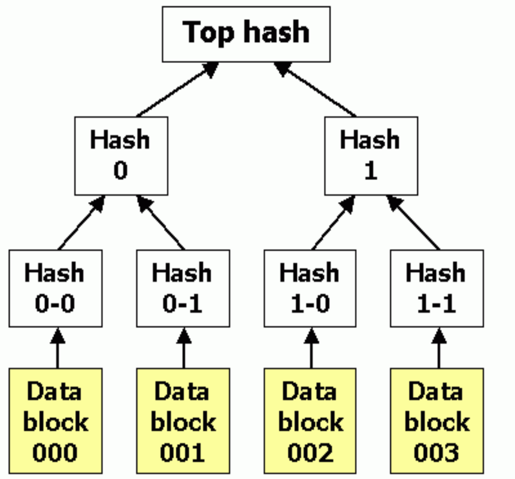


Figure 1: Hash table

modify the block that records the transaction as well as all following blocks, as seen in Figure 2. (Bitcoin.org, 2009)

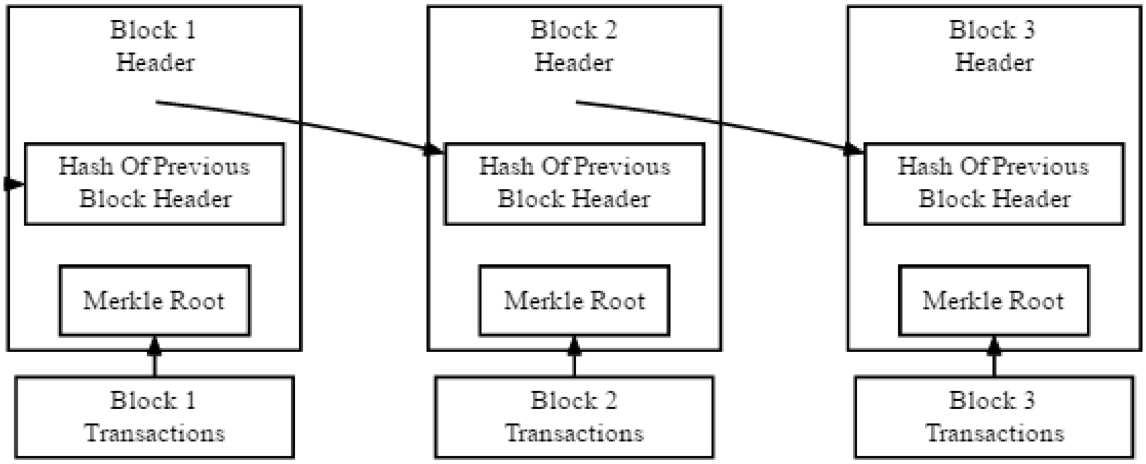


Figure 2: Simplified Bitcoin Block Chain (Source: Bitcoin.org, 2009)

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.

4. Current Digital Voting Systems

A number of digital voting systems are currently in use in countries around the world. We researched some of these systems to familiarise ourselves with current implementations, particularly Estonia.

Estonia has had electronic voting since 2005 and in 2007 was the first country in the world to allow online voting. In the 2015 parliamentary election 30.5% of all votes were made though the nation's i-voting system (Vabariigi Valimiskomisjon, 2016). The bases of this system is the national ID card that all Estonian citizens are given. These cards contain encrypted files that identify the owner and allows the owner to carry out a number of online and electronic activities including online banking services, digitally signing documents, access their information on government databases and i-voting. (*Electronic ID Card*, no date)

In order to vote, the voter must enter their card into a card reader and then access the voting website on the connected computer. They then enter their PIN number and a check is made to see if they are eligible to vote. Once confirmed, they are able to cast/change their vote up until four days before election day. The voter may also use a mobile phone to identify themselves for i-voting if they do not have a card reader for their computer. However, this process requires a specialised SIM card for the phone. (Estonian Ministry of Foreign Affairs, 2015)

When a voter submits their vote, the vote is passed though the publicly accessible vote forwarding server to the vote storage sever where it is encrypted and stored until the online voting period is over. Then the vote has all identifying information cleaned from it and is transferred by DVD to a vote counting server which is disconnected from all networks. This server decrypts and counts the votes and then outputs the results. Each stage of this process is logged and audited.

During the 2013 Local Election, researchers observed and studied the i-voting process and highlighted a number of potential security risks with the system. One such risk is the possibility of malware on the client side machine that monitors the user placing their vote and then later changing their vote to a different candidate.

Another possible risk is for an attacker to directly infect the servers though malware being placed on the DVDs used to set up the servers and transfer the votes. (Springall *et al*., 2014) However, this report has also come under criticism from the Estonian Information Systems Authority. (Veldre, 2014)

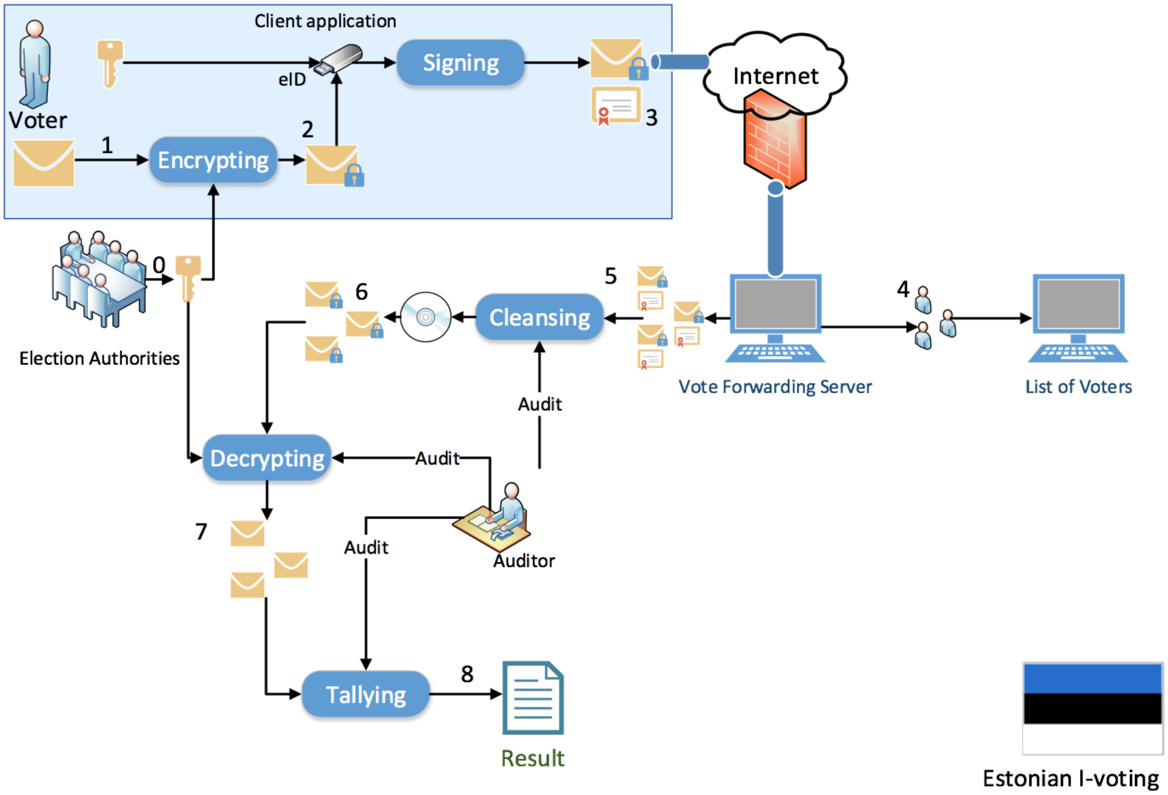


Figure 3: Estonian Digital Voting System (Source: R. Verbij. "Dutch e-voting opportunities." Master thesis, University of Twente, 2014)

5. Our Proposal

For our design we tried 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.

5.1 Registration

The first aspect of our design is the registration process, verifying a voter is essential in establishing security within the system. Making sure that someone's identity isn't being misused for fraudulent purposes is important, especially when voting is considered, where every vote matters. A design of our registration process can be found in Appendix B Figure 4. 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 (an example would be a UK citizen's national insurance number), postal address, optional email address and a password. All of 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 which is distinctly different from the vote blockchain.

Once someone has registered an automated government miner analyses the transaction and if they haven't been awarded or denied a vote the miner will make the decision as to whether to verify the user or not. If the user is verified, they will be sent a ballot card with their information on it to both their home address and email address if provided. They will also be sent a randomly generated password to use on the polling stations. Once this correspondence has been sent, the miner will create a transaction giving the user a vote from an infinite government pool of votes on the voter blockchain.

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.

5.2 Voting Mechanism and Architecture

When deciding on the architecture we took strong inspiration from both the distributed and availability of the Bitcoin network and the aggregation process of traditional voting. 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. (Appendix B Figure 5)

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. We decided to apply this method to prevent any one person being able to decrypt the voting data before the end of voting deadline. 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. A diagram of this can be seen (Appendix B Figure 7)

5.3 The Voting Process

When it is time to vote, authentication of a user requires three distinct pieces of evidence; their identification number (e.g. UK citizens have national insurance numbers), the password supplied on registration, their ballot card which contains a QR code. 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. (Each constituency is to be equipped with its own web server and URL to ensure votes are aggregated within the right network.)

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 have a vote, then the station will then allow the user to continue to the voting screen. If not, then system will respond to the user appropriately. See diagram Appendix B Figure 6 to see the process.

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 particular 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.

6. Analysis of the Design

Within our proposal we have tried to design a service and system that minimises the size of attack vectors to prevent potential malicious attacks. We have tried to evaluate and analyse our design from various perspectives to make sure we have thought about each step of the voting process. This section of the report discusses the potential risks associated with our proposal and suggests actions that can be taken to help mitigate them.

One risk is if a voter were to forget their ID, password or polling card on the day of voting. In this case the voter will be unable to cast their vote as they cannot enter the system. Possible risk mitigations include the voter returning later that day with the correct information or the implementation of a backup authentication service such as by phone. Alternatively, a forgotten password system could be added to the voter registration website; this could work in much the same way as recovering a password works on other websites. However, this increases the risk of a hacker attempting to change a voter’s password without their knowing.

A 51% attack is a potential threat to our proposed design. The basis of the attack being that someone could theoretically control a majority of the digital voting mining hash-rate, leading to them being able to manipulate the public ledger. The chances of this type of attack occurring are slim due to the immense cost needed to purchase hardware capable of this scale of processing.

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 clients device to establish a secure connection to the polling station.

7. Conclusion

To close, our service 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 actually present.

The blockchain containing information of who has registered to vote also allows our service to ensure each voter in unique and as described in section 5.1. 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 as described in section 5.3. 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.

Also, due to the encryption mechanism we are using (as described in section 5.3) 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.

8. References

Bitcoin.org (2009) *Bitcoin Developer Guide*. Available at: https://bitcoin.org/en/developer-guide#block-chain-overview (Accessed: 27 September 2016)

Electronic ID Card (no date) Available at: https://e-estonia.com/component/electronic-id-card/ (Accessed: 25 September 2016).

Estonian Ministry of Foreign Affairs (2015) *Estonian Internet Voting System*. Available at: http://mfa.ee/sites/default/files/content-editors/2015%20Parliamentary%20elections%20Internet%20voting%20system.pdf (Accessed: 25 September 2016)

Genesis block (2015) Available at: https://en.bitcoin.it/wiki/Genesis_block (Accessed 27 September 2016)

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

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)

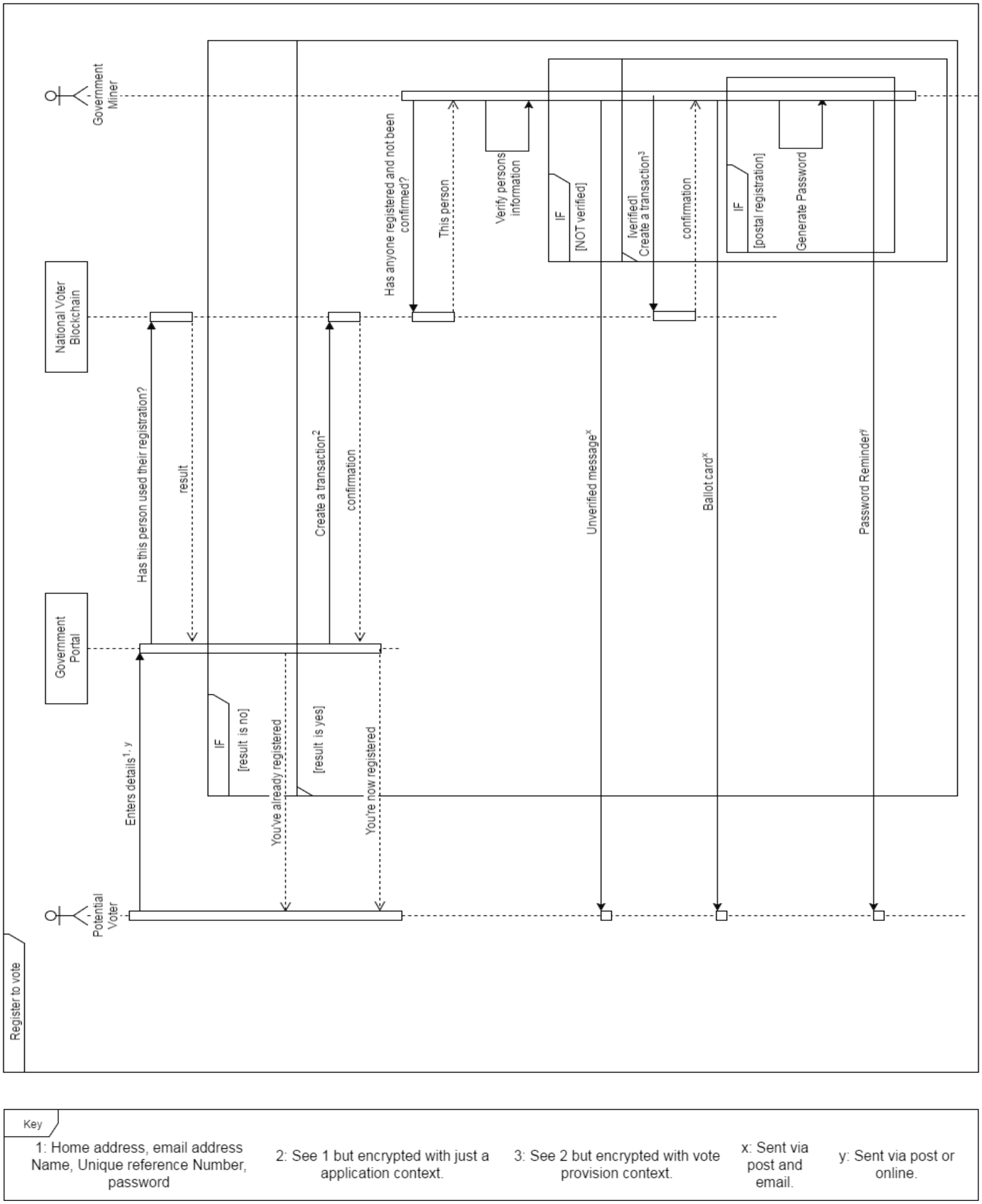
Vabariigi Valimiskomisjon (2015) Available at: http://www.vvk.ee/voting-methods-in-estonia/engindex/statistics (Accessed: 25 September 2016).

Veldre, A. (2014) *E-Voting is (too) Secure*. Available at: https://www.ria.ee/en/e-voting-is-too-secure.html (Accessed: 27 September 2016)

9. Appendix A – Assumptions

1. The country uses a constituency based system for elections.
2. All eligible voters have a unique identifying number or other such reference.
3. There is a stable and consistent internet connection to all polling stations.

10. Appendix B



1: Home address, email address Name, Unique reference Number, password

2: See 1 but encrypted with just a application context.

3: See 2 but encrypted with vote provision context.

x: Sent via post and email.

y: Sent via post or online.

Figure 4: Registration Architecture

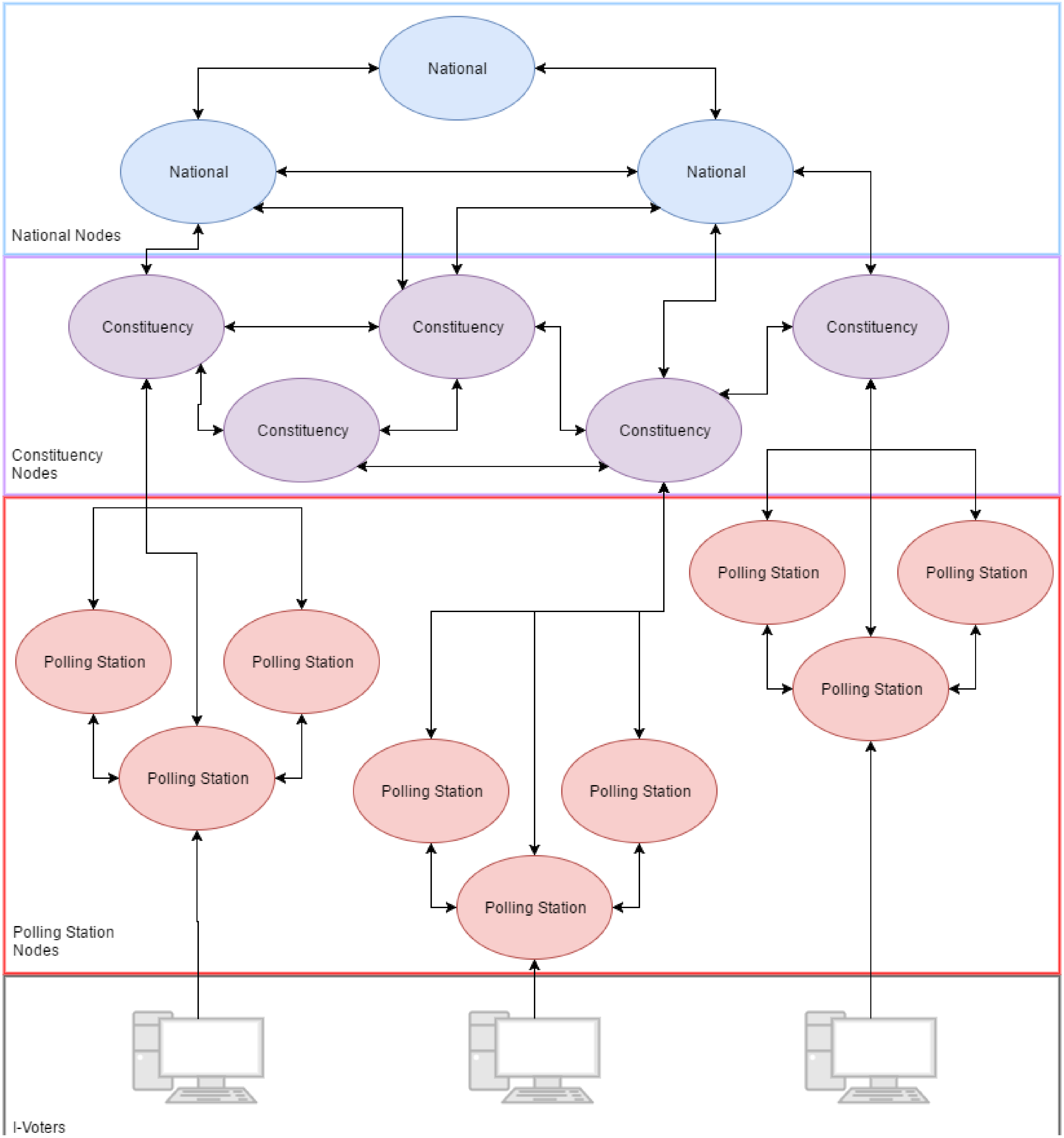


Figure 5: Overview of Node Architecture

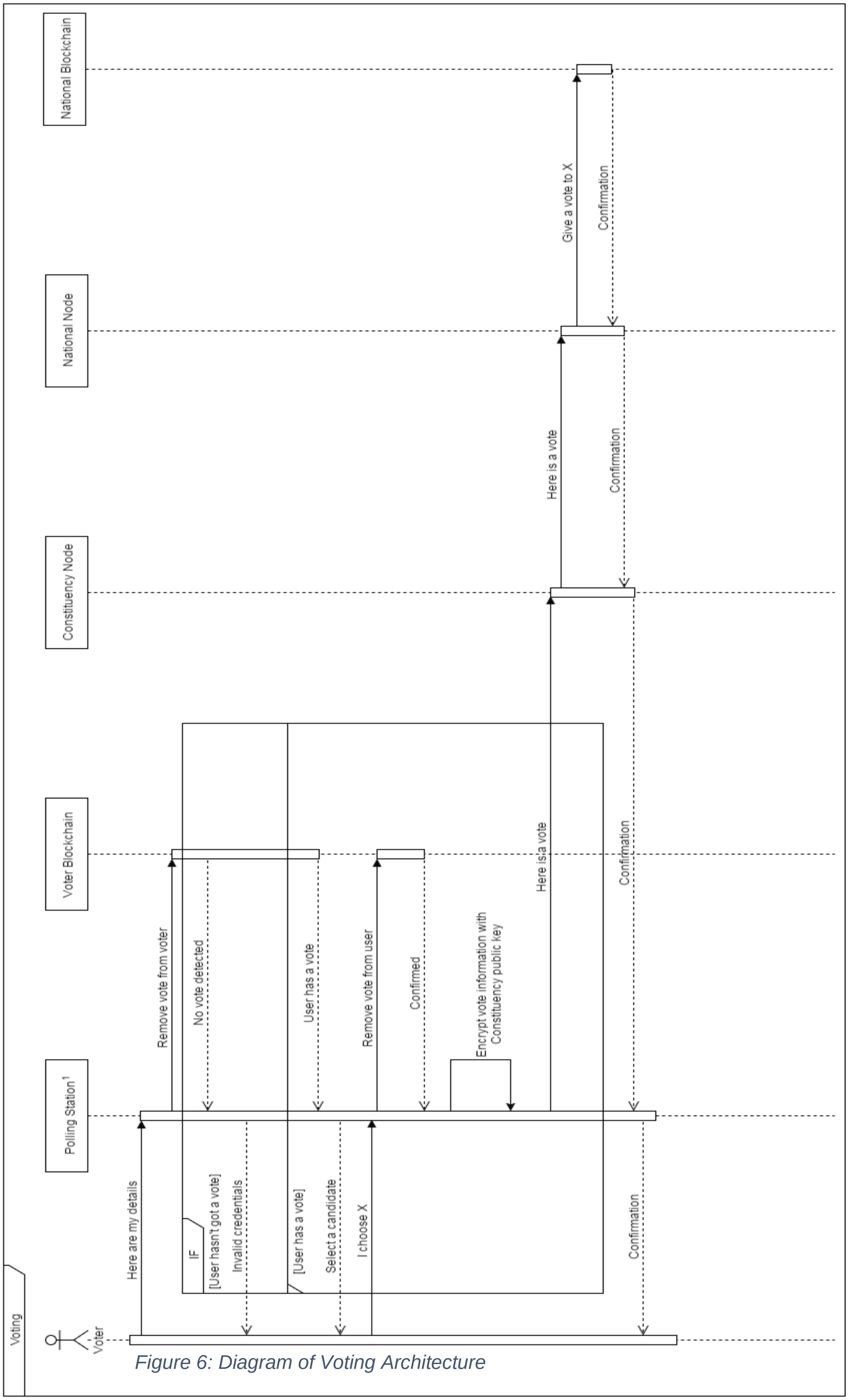


Figure 6: Diagram of Voting Architecture

Key

1: Can be either a virtual or physical polling station in the voters constituency.

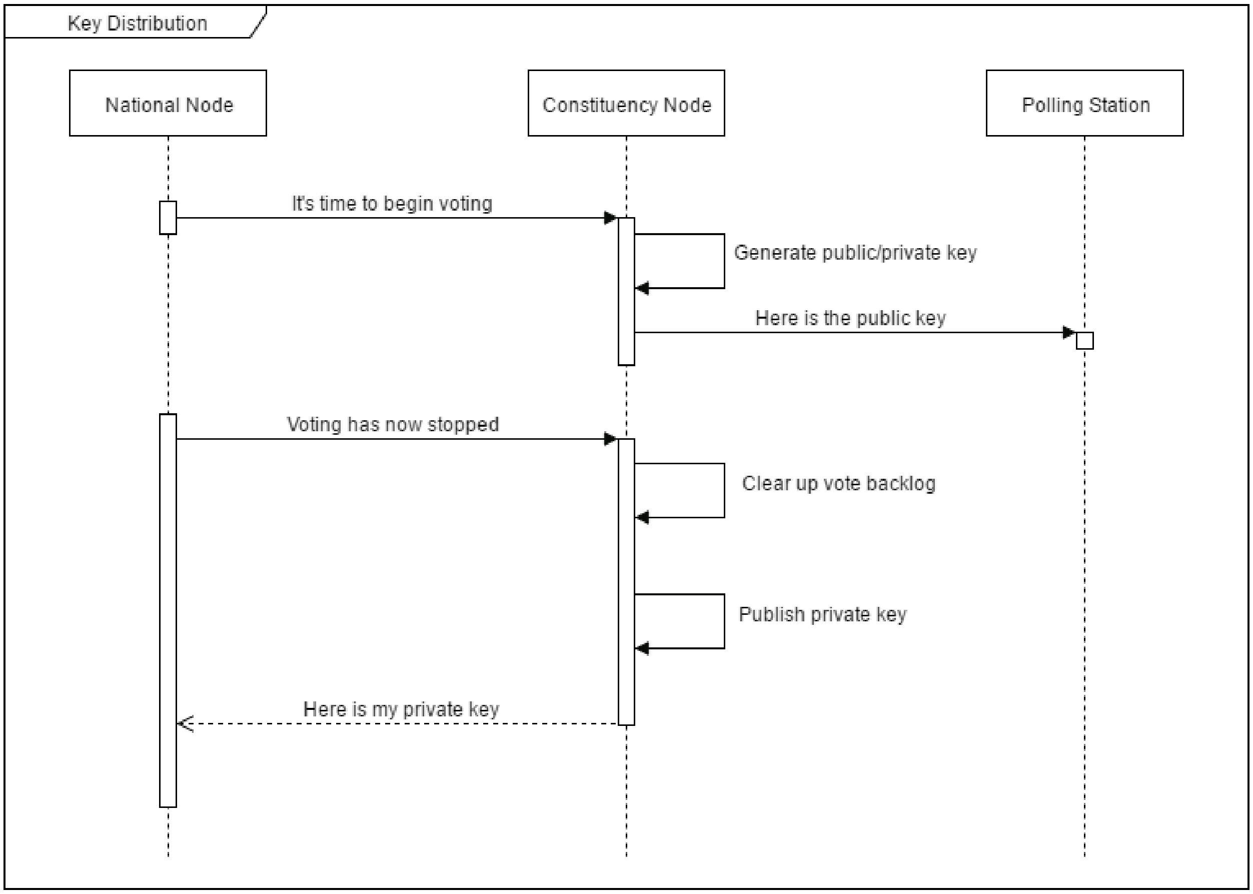


Figure 7: Diagram of Key Pair Encryption