UNIVERSITY OF NAIROBI

SCHOOL OF COMPUTING AND INFORMATICS

AN E-VOTING SYSTEM BASED ON BLOCKCHAIN TECHNOLOGY:

(A CASE STUDY KENYA ELECTIONS)

BY:

JOSEPH NDUNGU

P53/65321/2013

SUPERVISOR: **DR. ANDREW KAHONGE**

A RESEARCH PROPOSAL SUBMITTED IN PARTIAL FULFILMENT OF THE REQUIREMENT FOR THE AWARD OF A DEGREE OF MASTER OF SCIENCE IN DISTRIBUTED COMPUTING TECHNOLOGIES.

DECLARATION

This research proposal is my original work and has not been presented for a degree in any other University.

NAME: JOSEPH NDUNGU

REG. NO.: P53/65321/2013

……..…… …….

Signature Date

This research project has been submitted for examination with my approval as University Supervisor.

……..…… …….

Signature Date

ACKNOWLEDGEMENT

My sincere thanks go out to the All-powerful God for successfully seeing me through this course, strength, the good health, wisdom and financial breakthrough.

I wish to acknowledge with gratitude the assistance and co-operation that I received from my supervisor Dr. Andrew Mwaura and the entire project panel of my supervisors Dr. Elisha Abade, Prof. Eric Ayienga, Prof. Timothy Waema and Selina Ochukut, all Information Technology professionals I interacted with during project life cycle and my colleagues in Distributed computing class.

I acknowledge my lecturers in the MSC DCT degree program who gave me their time and knowledge. I'll always be grateful to my wife Carolyne, and my two boys Jeremy and Jalen, for their encouragement and moral support in undertaking this course, my father, James Kimani and my mother Christine Njeri, for their un-waivered dedication in giving us the best education.

ABSTRACT

The study was carried out to understand how general elections are conducted in Kenya as well as to explore some of the challenges encountered during that process.

The study revealed that a Blockchain-based e-voting systems emerged as a good platform for resolving some of the current experienced problems during the voting process. Some of the most common challenges included disputed results or lack of credibility on the results by the citizens, lack of transparency, and ensuring that data transmission is secure from one Node to the other.

A custom-made prototype was developed using JAVA programming language through various service methods (SOA, web service and API's) and tested using Junit and ReadyAPI. It demonstrated that the blockchain is very capable in enabling data protection and confidentiality during the voting process. Therefore, Kenya, as a country, stands to gain by blockchain technology for integrating voters' electronic data. This might go a long way in improving the way Kenyans vote, costs and the time taken to vote and tally. In addition, it might eliminate inconsistencies, which lead to mistrust of election results.

Contents

LIST OF ABBREVIATIONS

- API Application – Application Program Interface
- OWASP – Open Web Application security project
- SHA- Secure Hash Algorithm

1. LIST OF FIGURES

DEFINITION OF IMPORTANT TERMS

- **Architecture Service-oriented (SOA)-** promotes service orientation in this architectural style. Service orientation can be defined as a manner of thinking about services and service-based growth and service results

- **Web Services-** This is a uniform approach to integrate web-based applications, it follow open standards of XML, WSDL, SOAP, and Universal Description, Discovery, and Integration over the Web backbone protocol. XML is used for tagging information; SOAP is applied to transfer information,WSDL describes accessible services, and Universal Description, Discovery, and Integration lists accessible services. Web services can also be defined as a software system intended to promote network-to-network interoperability between machine and machine

CHAPTER 1

1.1 Background of the Study

The Internet's arrival and explosion has transformed the way we live, communicate and share information over the past two decades. This change has also affected politics, and thus, we have seen developing countries establishing promising digital-voting initiatives with the objective of enhancing democracy for their citizens. Despite the fact that digital voting has been around for several years now, it is still slowly being adopted by election bodies around the world. In Kenya, we have had a number of elections over the years, and one of the key challenges the electoral body has faced especially since the introduction of multiparty is disputed results or lack of credibility on the results by the citizens. In the year 2007, after the results of the presidential election were announced, the country encountered a lot of violence. About 1,300 people were murdered and over 600,000 displaced in the huge devastation that followed. Massive property destruction also occurred. The Commonwealth Observer Group's Investigation report for the 2007 Kenya's general elections indicated that the "Kenya Electoral Commission Could not establish the integrity of the process of counting, thereby calling into question the validity of the election results (Kenya Human Rights Commission, 2007). In the 2013 election, we had an introduction of registration of voters via the electronic system, which authenticated biometrically. However, the management of the outcomes and the tabulation process at country level was still affected by a lack of consistency, which still contributes to violence in various areas of the nation. In the election of 2018, we still had a similar pattern when the Supreme Court nullified an election on the bases of lack of credibility. In our research, the use of Blockchain technology in the development of a voting application was identified as the solution that could solve the problems mentioned due to the lack of a single point of failure. Blockchain enables thousands of personal computers to work together as a whole, making them more powerful than a few centralized servers. It is possible to corrupt any centralized database and usually needs confidence in a third party to maintain the data accurate. blockchain append-only structure that

enables information to be added to the database only, making it difficult to alter or delete previously entered information on previous blocks.

1.2 Problem Statement

Since the beginning of multiparty in Kenya, there have been complaints from many citizens, where they felt that the elections were not fair and free as ought to be. Following the presidential official release of election results, the nation experiences unprecedented rates of violence. For example, approximately 1,300 people were murdered in 2007, more than six hundred thousand displaced, and immense property destruction took place, particularly in the regions where the citizens felt the candidate had been cheated. In 2013, We had a petition in court in which the judges upheld the ruling that the elections were free and fair, leading to violence in certain places and property destruction. In 2018, the country had to repeat the presidential elections since the Supreme Court felt the results were not credible. In order to ensure that we have free and fair elections in our country, we need to have a solution that will ensure the credibility of the results. Hence, this research intends to investigate how blockchain technology can be embedded in the voting application to ensure that the data entered is secure and cannot be altered while in transit from point A to point B.

The Independent Electoral and Boundaries Commission (IEBC) faced legal challenges on procurements, particularly related to ballot papers and the Kenya Integrated Elections Management System (KIEMS). The South African-based Paarl Media cited irregularities in the procurement process. Blockchain is an open-source, free framework that can be customized to fit into an environment where Integrity and confidentiality are essential.

1.3. Research Questions

Any voting system has many required characteristics. The procedure for voting can be performed online involving a central database and an application server hosting the web application. The obvious problem with the Kenya Integrated Elections Management System payments is the centralized database and a single point of failure. The whole election process in Kenya also has quite several dependencies, some of which include the procurement process; some stages involve scanning of the hard copies for transmission to a centralized database. In a purely digital world, a dishonest party can easily tamper with a centralized system in their

favour. Any system project aims to establish a voting system for the future that brings together the value-added elements of legacy voting methods-

- Security
- Ubiquitous reach to the end-user at low cost
- Technology that permits faster processing,
- Boost convenience,
- Confidentiality and integrity of the final results,

- Drawing out and the use of information of great worth that accompanies the process of voting.

The general objective of this project is to bring out an architecture that uses blockchain technology to achieve the aforementioned desired attributes of any voting system. Therefore, the research aims at answering the following questions:

1. Can blockchain-based e-voting system enhance transparency during the voting process?
2. How can blockchain technology achieve Authorization, confidentiality, Non-repudiation and integrity in the voting process?
3. Can blockchain enhance real-time transmission of votes from one node to the other in a secure manner
4. At the end of my research, could there be a possibility to combine both technologies and create a hybrid system that can mitigate problems mentioned in the previous chapters?
5. Is blockchain technology safe, secure and tamper-proof?
6. What are the advantages that can be achieved by adopting block chain technology in voting process in Kenya?

1.4 Objectives of the study

The study's goals:

1) Constructing and testing an e-voting prototype that will allow the use of valuable data that coexists with the blockchain technology voting process
2) To elaborate and bring out the merits of the blockchain e-voting system has over the currently existing systems in use by IEBC

1.5 Justification for the Study

Importance to Computer Science

Carrying out research, particularly on a unique field, adds knowledge to the field of computer science. Designing a system that ensures a voting process has integrity and is secure is beneficial to the nation at large.

1.6 Scope.

The research was conducted with the focus being on the Kenyan general election. This project seeks to solve critical problems associated with the voting process in Kenya.

Chapter 2

2. Literature Review

Most of the researches done has focused on Web-based voting systems. Rather than the customary paper-based ballot voting system, the first software was used in polling stations. voting was performed in the second system using any machine with an Internet connection. Nevertheless, Technical threats have always been a problem for the e-voting applications. [14]

Examples of the electronic-voting systems

2.1.1 Estonian Internet-Voting System:

Estonian's were among the first to vote in an election using the World Wide Web and the national electronic ID card only conceived to operate a built-in circuit, a 2048-bit PIN chipset. Using SHA1/SHA2, the card was able to produce signatures. The card was used to encrypt, authenticate and generate signatures. The Voters are required to download, authenticate and vote on the voting application. The vote was encrypted with the election particular asymmetric cryptography and signed with a key only known to the recipient (secret key).Immediately the ballot was cast, it was directed to the Estonian government-controlled central storage server.

Some of the security problems with Estonian I-Voting system included

Technical Security issues of the Estonian I-Voting System:

This system was unguarded against Attackers at the state level such as agencies of public intelligence These hackers had access to network traffic, sufficient data storage and analysis capabilities. In addition, they can perform attacks.

*Centralized Infrastructure**:***

In this type of system, all servers in one main data center hence, the system is susceptible to Distributed denial of service or similar kind of attacks. In addition, decentralizing the servers would result in greater accessibility, but definitely expensive and complex than simply maintaining everything in a centralized place. Furthermore, it is quite complex to secure decentralized servers and their communication.

Attacks on the client side

under this system, the aim was geared to manipulating the voter's personal computer. For this reason, the voter may hardly detect direct manipulation of votes on the voting machine (ghost attack) [14]

2.1.2 Norwegian E-Voting System

The Norwegian system was developed similarly to the Estonian voting system. Instead of the paper based voting application, the software application was originally used in polling stations, afterwards, there were some improvements and the system was meant to allow mobility and Use any Internet-connected device to improve voters experience to cast their ballots from anywhere. Although electronic Voting software made casting a ballot a little bit easy and quite convenient, and increase the number of citizens willing to cast their ballot. However, there exist a number of technical threats to the electronic voting scheme.

In Norway, the voter could obtain a poll card with aggregated listing of all participating parties and a 4-digit code computed separately for the individual voter. This was sent through postal mail. After the vote was cast, the voting server could send a brief signal on the mobile phone of the voter containing a 4-digit code, enabling the voter to compare the received code and to guarantee that it matched the code of the voter's choice. This enabled the voter to confirm the vote. The voters could cast various votes however, for coercion protection, only the last could count and her prior votes were automatically withdrawn.

2.1.2.1 Security Problems with the Norwegian e-voting system

I-Vote Project in 2014 was halted in Norway because of security concerns. The main criticisms were the Votes will be made public in the event of a cyber-attack. In addition, Network attack was also a concern where an Internet Service Provider level attacker was a perceived threat because they Could observe traffic easily and establish a relationship between the voter and the voting servers. Hence, the person casting a ballot is partially prone to acts of coercion attacks. The system's centralized nature created a central failure point as an attacker required only one server to be compromised and could impact the entire election.

A case study of Kenyan elections

In Kenya, the first election happened in 1920 during the British colony. During the parliamentary elections in 1957, Kenya's African population got a chance to vote for the first time. Then universal suffrage took place in 1961, and Kenya African National Union (KANU) was proclaimed the winner with a total of 65 seats, which, despite European dominance, was the majority of parliamentary seats. KANU won majority seats during the following election. Additionally, the country had Jomo Kenyatta as the first African Prime Minister. This led to independence in December 1964 when Kenya was declared a republic and the first president was Jomo Kenyatta.

In 1966, there was disagreement between the president and his first deputy (Jaramogi Oginga Odinga) which conduced to Jaramogi's withdrawal from Kenyatta's KANU party and the formation of the Kenya People's Union (KPU) party. As a result, it resulted to ethnic divisions along party lines with Kikuyu's behind KANU and Luo's behind KPU. Following a constitutional amendment, a by-election was held the same year to allow the breakaway that enabled KPU to stand for elections. In 1969, Kenya was transformed into a one-party state and KPU was banned, leaving KANU as the only party to win all seats from 1969 to 1988. In 1992, President Moi restored multi party politics. He won the elections of that year. Daniel Arap Moi ruled from 1978 until 2002. In 2002, Moi stepped down for Uhuru Kenyatta to vie for presidency and Mwai Kibaki, who was opposition coalition leader then, defeated him. After the 2007 elections, there rose post-election violence Where nearly 1,300 individuals were murdered and over 600,000 displaced. An investigation was conducted to identify the cause and perpetrators of post-election violence, resulting in six well-known Kenyan leaders inclusive of Uhuru Muigai Kenyatta and William Samoei Ruto being charged at an intergovernmental organization and international tribunal that situated in The Hague, Netherlands, where they were charged with inciting ethnic violence against the followers of opposition leader Raila Odinga. The charges were dropped at different stages of the trial. National Accord and Reconciliation Act. (NARA) came up in 2008 this triggered by Violence after the election that led to the creation of the post of the Prime Minister that had earlier been abolished in 1964.

In 2010, the new constitution was inaugurated and in 2013, under the new constitution elections were held. Later in August 2017 presidential election were cancelled the Supreme Court of

Kenya due to cited Irregularities in the elections and fraud allegations by the opposition party led by Raila Odinga and thereafter Raila withdrew from the repeat elections since he wanted IEBC reformed and postponement of repeat elections. Moreover, thereafter, there was a repeat, then Uhuru was declared the winner. [20]

2.3 Biometric Voter Registration System (BVR) In Kenya

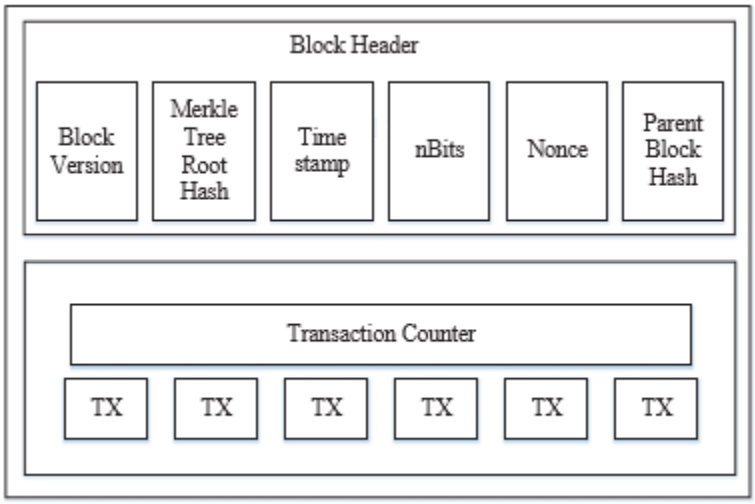
BVR is a system that is used to register Voters. The 2011 Kenya Election Act enabled the Electoral Commission to make appropriate use of technological innovations in the electoral process. This would increase the electoral process's efficiency and effectiveness. Mandates the Commission to implement easy, precise, verifiable, safe, secure and transparent technological innovations. Registration by electronic means of electors in Kenya started in 2009 as a trial involving 18 electorate across the country and was a great success. Some voters who had been recorded manually in other constituencies were drawn by technology and pleaded that they too would be registered with biometric characteristics. Inspired by IEBC's achievement in 2012, biometric voter registration was rolled out across the country's 290 constituencies. Biometric Voter Registration information was transmitted to a centralized storage server. hard copy registers are printed from centralized storage. The physical register, which contains the voter's thumbnail picture, is circulated to voting centers for individuals to check and verify their information of registration [16]

2.4 Blockchain Technology

Blockchain is stamped with time sequence of an unchanging information record managed by a computer collection not owned by any single entity. Each of these information blocks is secured and interconnected using cryptographic principles (i.e. chain). (D. Lee Kuo Chuen, 2015).

Figure 1 and 2 below shows the blockchain structure

blockchain Structure



A blockChain Architecture

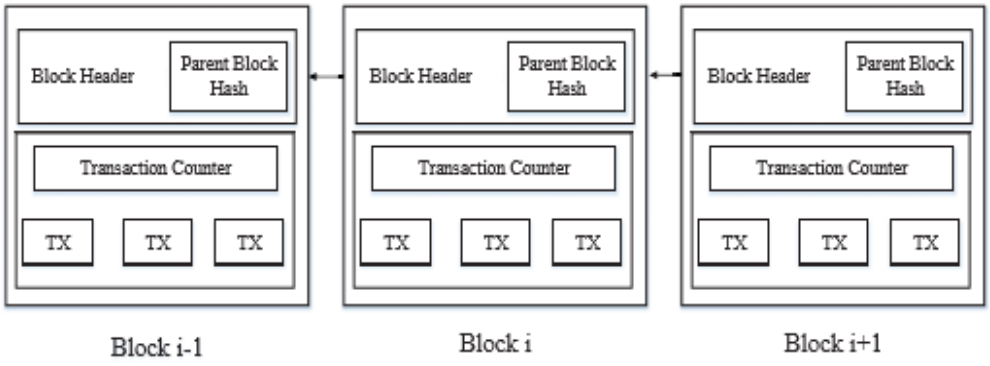


Figure 2: a blockchain architecture

As shown in Figure 1, a block is made up of the body and the header. The header especially includes

(i) Block version, a set of regulations for validation.

(ii) Merkle tree root hash is the hash value of all block transactions.

(iii) Timestamp relates to the present moment in universal time as seconds.

(iv) nBits relates to a valid block hash target limit

(v) Nonce It is a random number given in an authentication protocol to guarantee that it is impossible to reuse ancient communications in replay attacks. Its four-byte field, generally starting at zero, increments with each hash calculation.

(vi) Parent hash block: a hash value of 256-bit pointing to the earlier block. A transaction counter and transactions are comprised of the block body. Blockchain utilizes a system for asymmetric cryptography to validate transaction authentication (NRI, 2015).

Introduction of blockchain technology was initially done by Satoshi Nakamoto (a pseudonym) (National Institute of Standards and Technology,2012). Who proposed a peer-to-peer system for payment allowing money transactions with no need for a commercial institution being required (S. Nakamoto, 2008). Blockchain is fault-tolerant and secure by design (F. Reid and M. Harrigan, 2013).

2.5 Proposed Architecture

The proposed architecture will highlight four main requirements, as are described below:

- Authentication- Only registered people Could cast the vote. Our system won't support the process of registering. Registration generally needs verification of certain data and records in order to comply with present legislation, which could not be accomplished securely online. The scheme should therefore be able to check the identity of the voter against a previously verified database and then allow them to vote once.
- Anonymity-there should be no link between the voter’s identities and the ballots.
- Accuracy- no vote should be duplicate or removable and must be accurate.
- Verifiability-the votes should be verifiable or can be traced back to the voter and correctly counted.

The first vote / transaction added to the block belongs to the candidate that will include the name of the candidate and serve as the first block, with each vote placed on top of it. Unlike the other operations, the basis will only contain the candidate's name Every time the transaction is registered with a vote, and it will update the blockchain.

BlockChain Voting Architecture

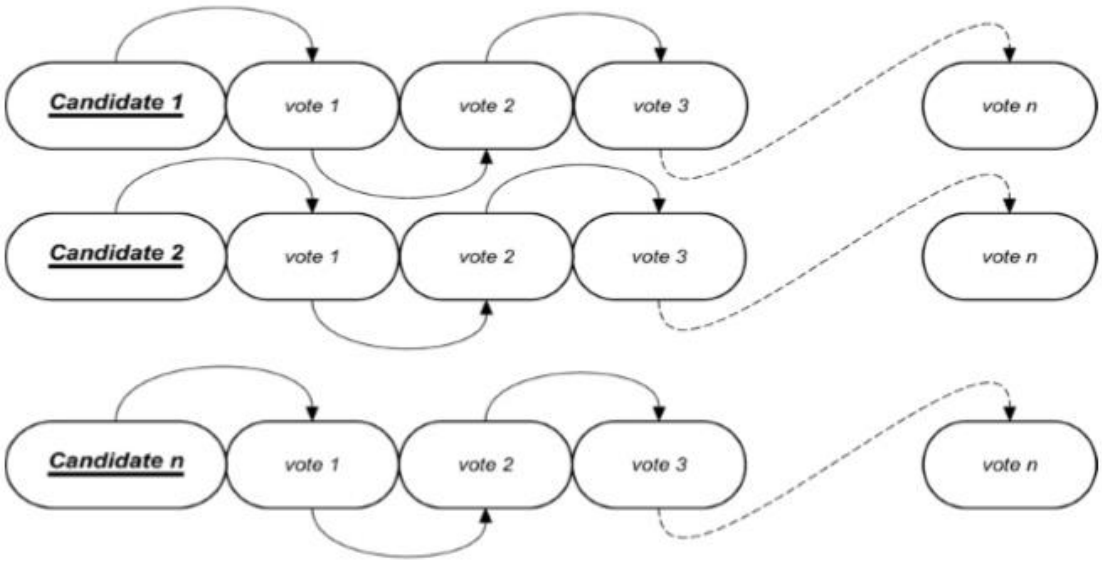


Figure 3: the blockchain voting architecture

The blockchain will hold the information of the previous voter including the name and the national identification number. If at any point any of the blocks are vulnerable, it will be easy to discover as all the blocks are interconnected. Compromise in this case would either be addition or subtraction of a block. The Blockchain is decentralized; hence there is no single failure point. The Blockchain is the location of the actual voting. The vote of the user is sent to one of the nodes on the system, and then the node adds the vote to the Blockchain. In each virtual polling station, the voting system will have a node to guarantee that the system is decentralized. The user must log in using the local authorities ' domestic identification number, county number, and voting confirmation figures given by the local authorities to registered voters. The user will be allowed to cast a vote if valid. Voters will have to vote for one of the candidates or vote to indicate a protest against the current political system or electoral process. The system will produce a string after the person casts his ballot that includes the voter's national identification number and the voter's name as well as the prior vote's hash. The encrypted data will be registered in each vote cast's block header. The data pertaining to each ballot will be encrypted using SHA Function to hash one-way, which has no known exact reverse

2.6 OWASP API Security Project

This project was intended to tackle the ever-increasing amount of organisations that as part of their software offerings deploy possibly vulnerable APIs. These APIs are primarily for inner functions and third-party interfacing. Unfortunately, many APIs do not undergo the strict testing of safety that would make them safe from hackers.

The OWASP API Security Project aims to provide software developers and security evaluators with value highlighting prospective hazards in unsafe APIs and demonstrating how to mitigate these hazards. The OWASP API Security Project generate and retain an API Security Risks document and a documentation portal for best practices when establishing or evaluating APIs in order to promote this objective.

Usually the files of the OWASP API Security Project are free to use

Categories of security concerns covered by OWASP:

- Authentication and Session Management: Application features related to authentication and session management never occur correctly most of the time, allowing attackers to compromise passwords, keys or session tokens, or even exploit other implementation flaws to assume identities of users
- Injection: Injection faults, such as SQL, QS, and LDAP injection, happen when untrusted information are sent as part of a command or request to an interpreter. Hostile information from the attacker can trick the translator to execute unintended orders or access information without adequate permission.
- When an application selects untrusted information and sends it to a web browser without adequate validation, cross-site scripting happens. This sort of attack allows attackers to perform scripts in the victim's browser, hijacking user sessions, defaulting websites, or redirecting users to malicious locations.
- Enhanced security needs a definition of reliable setup and implementation, particularly on application, frameworks, application server, web server, database server, and platform.
- Sensitive information exposure owing to web applications where sensitive information such as credit cards, tax IDs and authentication credentials are not adequately protected.

- Failure to control function levels of access in web applications before making it visible in the user interface, one should check function-level access privileges. If applications are not checked, attackers may forge applications without adequate permission to access functionality.
- With complete privileges, the use of Known Weakness components such as libraries, frameworks and other software modules can lead to Vulnerable use of improper parts which can result to severe data loss or server takeover.

2.7 Conceptual Model

As shown in Fig 3, the user will be required to log in using the username and Password given by local authorities (IEBC) to registered voters. If valid, the user shall be entitled to vote. Voters will be required to vote for one candidate per position. The mechanism will produce a string after the user casts his ballot, containing the name of the voter as well as the hash of the prior ballot. The encrypted data is registered in each ballot cast's block header. The data associated with each ballot will be encrypted using the one-way hash function of SHA that has no known reverse.

The diagram below represents the e-voting system Model and was

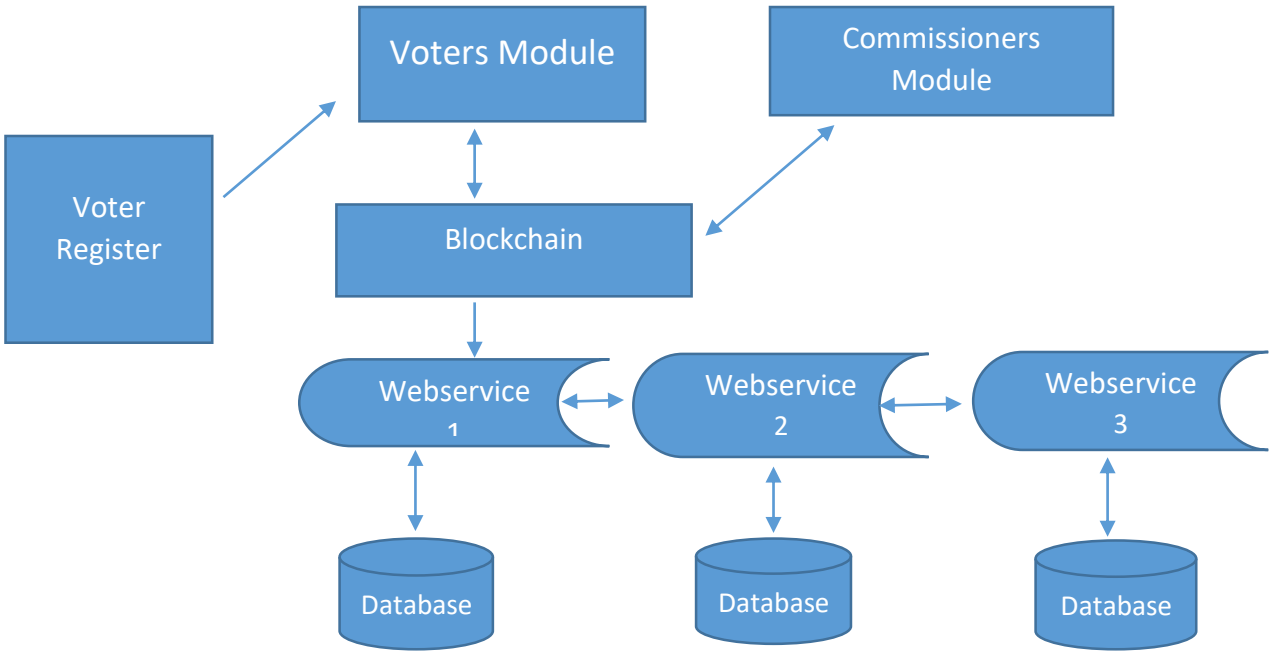


Figure 4. E-voting system model

Chapter 3

3. Methodology

This section outlines the proposed rapid application development methodology, research design, information sources, instruments for collecting information, procedures and methods and system design.

3.1 System Development Methodology

The prototype has been created using the Rapid Application Development (RAD) concept. RAD is a development cycle designed to make development much faster and higher quality results when it comes to system development compared to the traditional lifecycle. RAD highlights the quick and iterative release of prototypes and apps and generally includes object-oriented programming methodology, which inherently encourages the reuse of software.

The method entailed Document Analysis (Requirement gathering), quick design, prototype, Construction and cutover.

During the first phase, we started by conducting fact-finding tasks, the real issue faced by the target users was investigated. In this situation, it was performed through face-to-face interviews, document analysis, target user conversations, and literature review research.

In the user design phase, architecture created mainly using Java programming language. The design was done, taking into consideration the current problems.

At the construction phase of the cycle, a prototype system was developed. Limitations and strengths for further action / intervention were observed and recorded. A number of users were allowed to use the system, and their view on it was gathered. Lastly, general findings were identified, and the outcome of action clearly identified.

3.2 Data Collection Tools

The study was a qualitative research method that has been used in diverse areas such as computer science. Its goal is all about “getting to know” or putting yourself into the shoes of the phenomena. The particular type of research method used was face-to-face interview and analysis of life histories concerning Kenya election

3.3 Business analysis

The objective of this phase was to identify the objectives of the Independent Commission on Electoral and Boundaries(IEBC), business goals and key performance indicators about tackling issues related to elections. This phase also defined the technology, applications and people skills in the current setup. Common business vocabulary, business rules, business actors and main business use cases. The phase resulted in the creation of "as-is "and a "to-be "business models.

3.4 System Analysis, Design and implementation

3.4.1 Analysis of the current voting systems already existing in Kenya

A situational analysis entailed investigating existing voting systems and identifying the limitations of each mode using various data collection methods.

Problem analysis and requirements gathering

3.4.1.1 Analysis of current processing:

The investigation of the information flow associated with the voting process showed that currently a combination of digital, manual systems are used concurrently, and hence, the system is faced with a lack of integrity and transparency. Additionally, there is no reliability on the results submitted, as evidenced by the post-election violence in different parts of this country.

Current process: The process starts with the registration of voters using the Kenya Integrated Election Management System (KIEMS)'s kit, followed by verification of voters during voting. Voting happens in a manual ballot box, and record of seals kept prior to counting for each elective position. This starts with breaking seals (in the presence of party agents and observers who are at the polling station) followed by emptying contents onto counting container. Thereafter ballots are unfolded to determine their validity and sorted according to the candidate. Counting begins and filing of Forms 33. The counted ballot papers are bundled in groups of 25 and forms 34 or 35 are filled respectively and statement of rejected ballots where applicable. Thereafter, results announced and delivered to the Constituency Tallying Center and finally delivery of the manual Forms 34, 35 & 36 from county to the National Tallying Centre (NTC). (IEBC, 2016)

Analysis of current system data: The research showed many challenges faced by the current systems including human error knowingly or unknowingly during tallying, or wrong entry of the

results on the different forms filled by the returning officers and as a result of the wrong tabulation of the data, which led to wrong results.

3.4.1.2 Proposed System.

The prototype was designed and built as an illustration of the proof-of-concept that the blockchain technology indeed could be used to conduct elections in Kenya without compromising on results.

Development tools

The system was developed in MSQL database, java development kit and NetBeans as an integrated development environment and glassfish, which enables for distributed systems development.

The objective of a good, reasonably secure information system is always to guarantee the following basics of information security are well accounted for in the IT infrastructure, policies and procedures, and people involved in the deployment of the e-voting application: -

1. Integrity – the process of preventing alteration of data in transit by unauthorized third parties. This is provided via replication of the database in more than one site. Immutability of votes is usually a main concern when it comes to elections. Many popular blockchain platforms use the Merkle tree (some implementation also use other variants of the Merkle tree) for verification of the integrity of the data added to the blockchain. Even if a single bit of data is altered or tampered, it can be easily detected using a Merkle tree verification. This property of the blockchain to ensure that a vote once added to the blockchain cannot be altered or tampered helps in achieving immutability as well as integrity verification of the votes.

2. Authentication – The process of validating the identity of a user requesting access by use of a password in each module.

3. Authorization – the method of establishing the rights and privileges of a user during interaction with the system.

4. Confidentiality – the means of ensuring that all sensitive data being transmitted can only be read by authorized parties.

5. Non-repudiation – the assurance that nobody can deny the validity of something.

6. Data redundancy- The blockchain is synced across all of the nodes in the blockchain network, and hence, this provides data redundancy.

3.4.2.3 Electronic voting process using the e-voting system based on blockchain.

Voting using blockchain follows the following steps:

1. Voter authentication (username and password)

2. Vote for the preferred candidate on different positions.

3. Vote recorded and a hash generated based on blockchain.

3.5 Implementation

System implementation entailed the following activities:

3.5.1 system setup,

The steps for each item implemented as outlined below:

• Installation of the Java Development Kit (JDK) programming codes needed for software development of communication codes for the prototype.

• NetBeans Integrated Development Environment (IDE) installation.

Mount the NetBeans file or CD/DVD media to the operating laptop and boot it. It is an integrated development tool that enables the reusability of the java codes. Follow the installation instructions to finish the process.

• Installation of MYSQL (Structured Query Language) database. The prototype database is named muvote. To be able to access the database, there was a need to install the MYSQL graphical user interface (GUI).

•Create the database muvote

•The prototype runs on windows 10 or any other operating system that can run Java Virtual Machine that is installed in the laptop. Mount the executable installation files or DVD media to the host computer and boot it. Follow the instructions below to finish the process.

- Insert the live DVD in the drive;

- Boot the computer;

- On the BIOS menu select to boot from DVD;

- Select the NetBeans option on the GRUB menu that follows;

- Let the GUI desktop load;

- On the GUI desktop launch the install command and follow the easy steps that will follow

Database implementation.

Table1 below depicts the database tables and their respective description in detail.

Table	**Description**
Admin	Holds systems administrators details
Blockchain	Hashes generated while a voter votes
Candidates	Those being voted in different positions
Voters	Registered voters
Positions	Existing positions
Results	Total votes cast against each candidate
Constituency	Existing constituencies in Kenya

Table 1. Database tables

3.5.2 User interface model implementation

From the prototype design discussion above, it was important to have an active graphical user interface model design to enhance simplicity when it comes to system usability

The screenshots of the interface are as follows.

Login

There was a need to have a simple login page that enables the voter and the commissioners to login and vote and view results at the same time, as shown in figure 5 below.

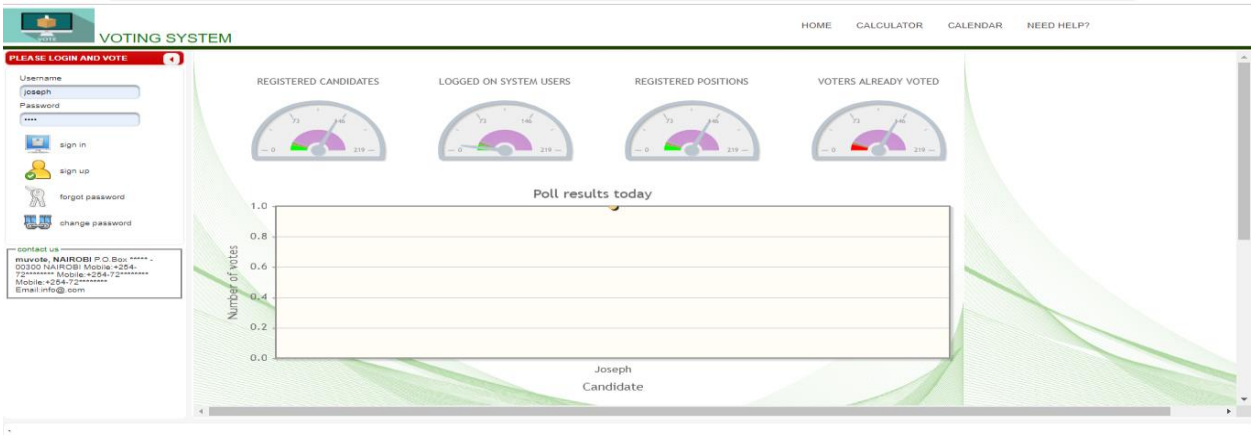


Figure 5 Home page of the E-voting system

Home page.

Immediately a system user logs in to the system successfully, and users are redirected to the home

Figure 6 below shows what the voter will see when they successfully login into the system, and from this page, the voter can see the candidates to vote for and their respective positions.

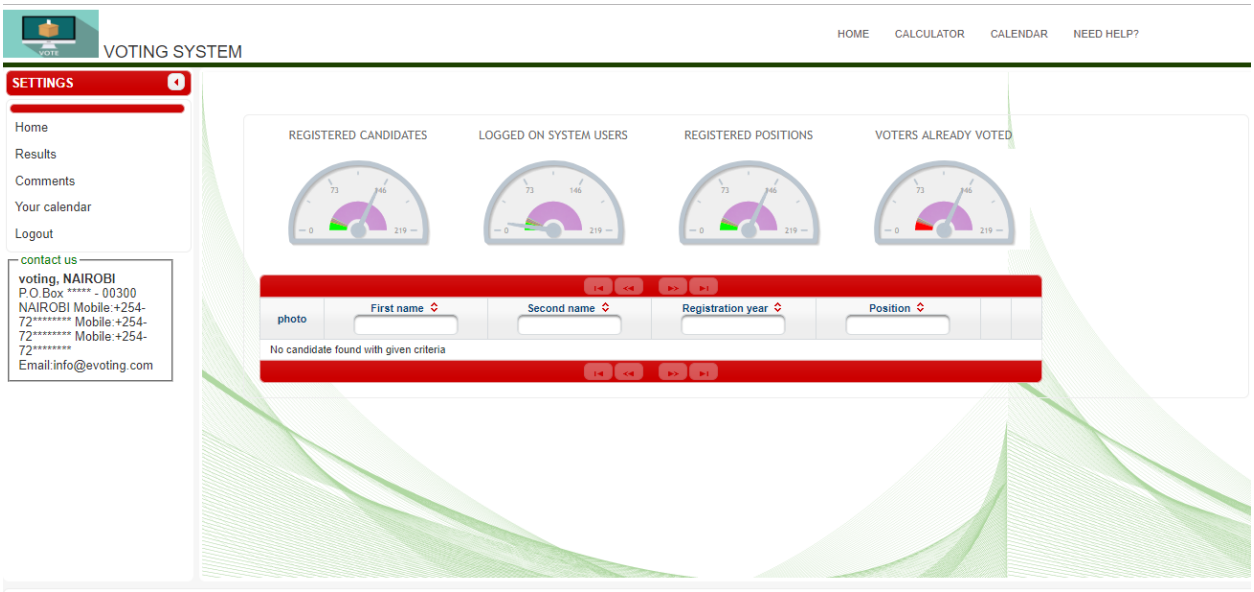


Figure 6 Landing page after a voter is Authenticated.

CHAPTER 4: Testing and Results

In this section, testing was done on the developed E-voting prototype using sample data. The web service node was used to consume data and view the various posted entries cross the chain.

4.1 Web Service Testing

The SoapUI tool was used to build test cases of the various tests carried out on web services.

4.1.1 Service Methods Testing

This was used to test whether the web service interfaces are able to respond to service requests sent during the voting process to capture the generated blockchain hashes (votes). The results are as shown in *figure 7* below:

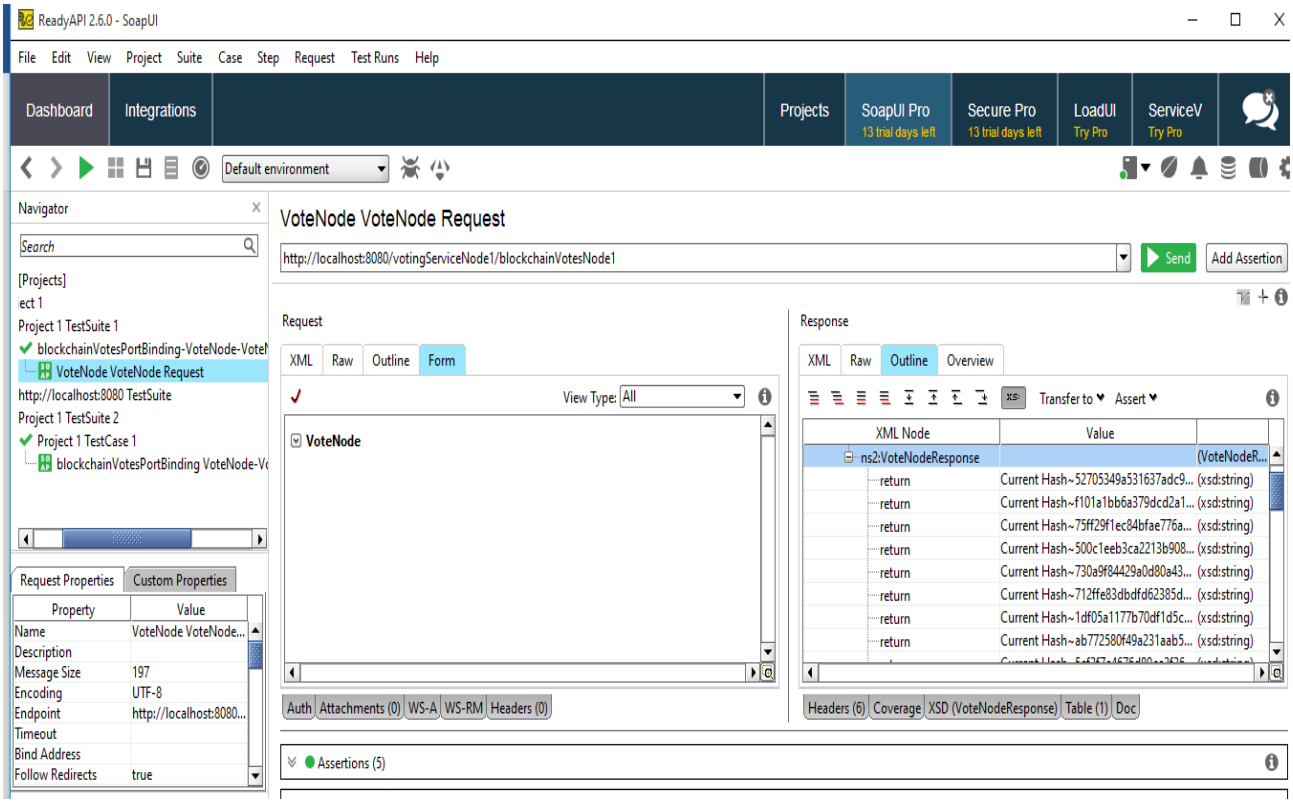


Figure 7 Service Method Testing of the web service (blockchain node)

4.1.2 Service Response Times Testing

The response time for the service was then tested. The summary of the time taken by the web service and whether it passed or failed to run is as shown in the

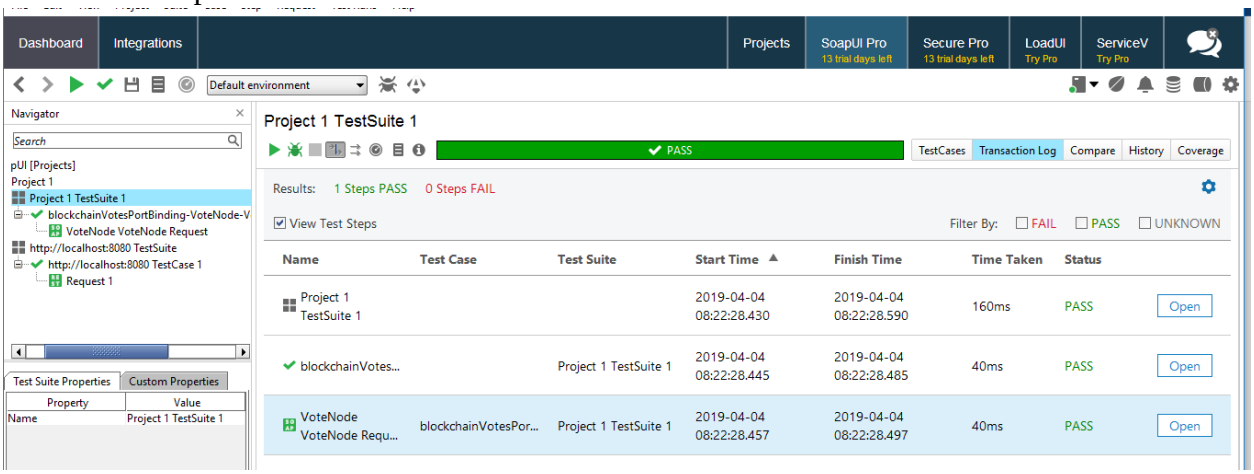


Figure 8 web service response Time

4.2.3 Web Service Security Testing

A security test was also carried to test if the web service was secure in terms of cross-site scripting, boundary scan, fuzzing scan, invalid data type, malformed XML, SQL injections, weak authentication, XML bomb and x path injection. The results are as shown in figure 9 below.

Web service Security Test

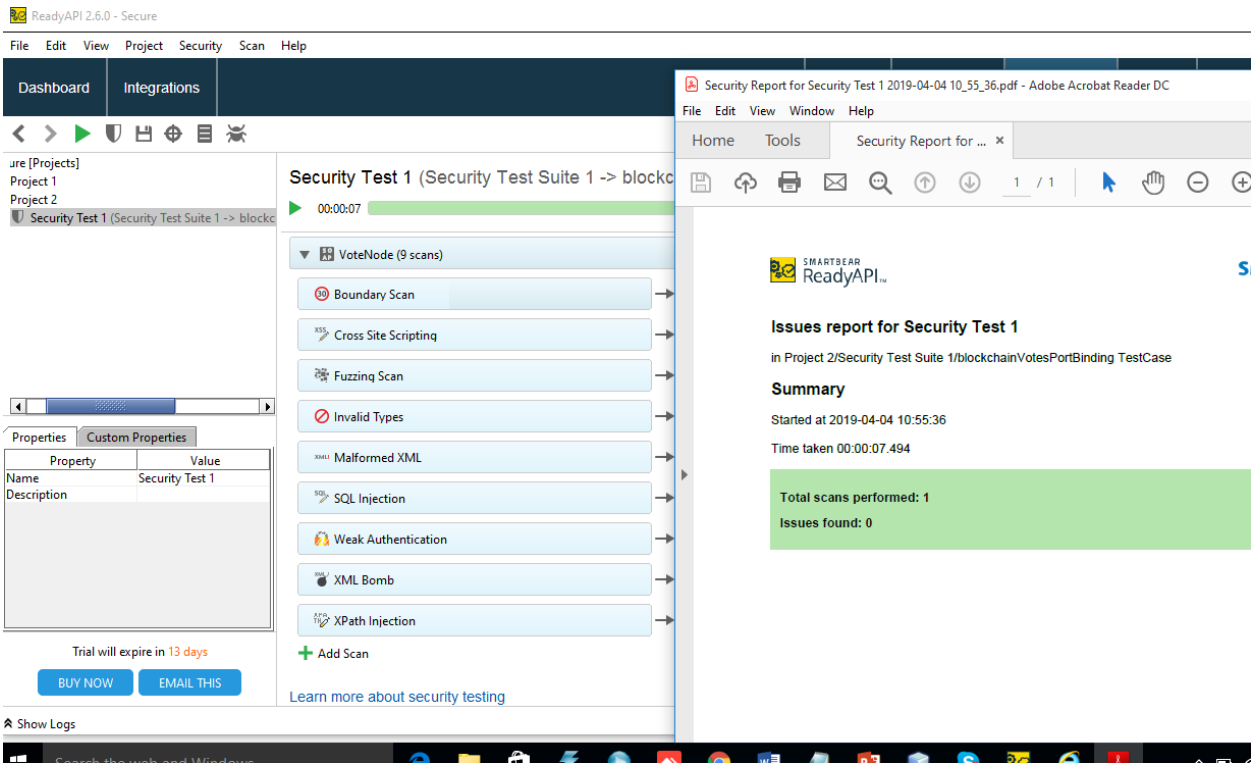


Figure 9. Web service Security Test

4.2.4 Web Service load Testing

Loading testing was also performed on the application for e-voting. Load testing included increasing the load and seeing how the system was performing under higher load. Response times were captured during load tests. The goal of load testing is not to break the target environment, though. The goal was to find metrics for system performance under high load. The results are as shown in figure 10 below

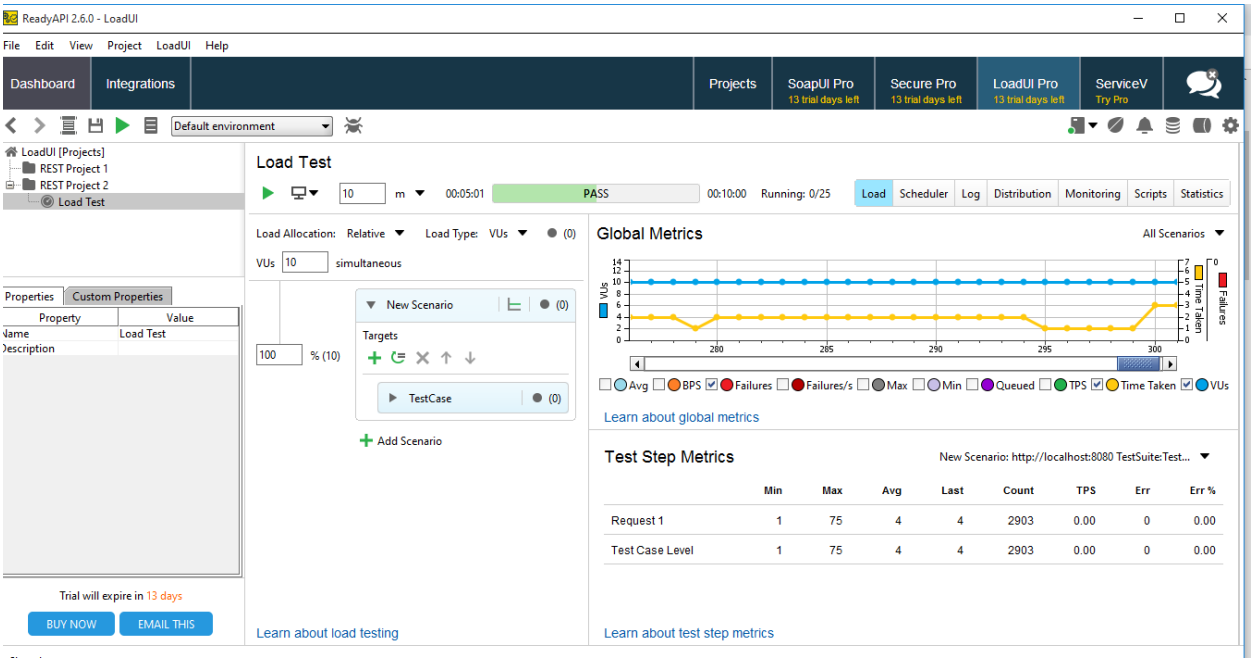
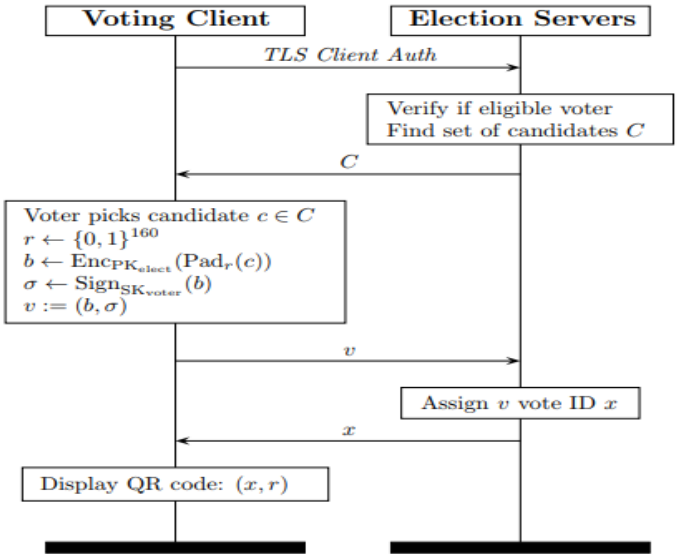


Figure 10. Load Testing on the e-voting

4.3 Discussion

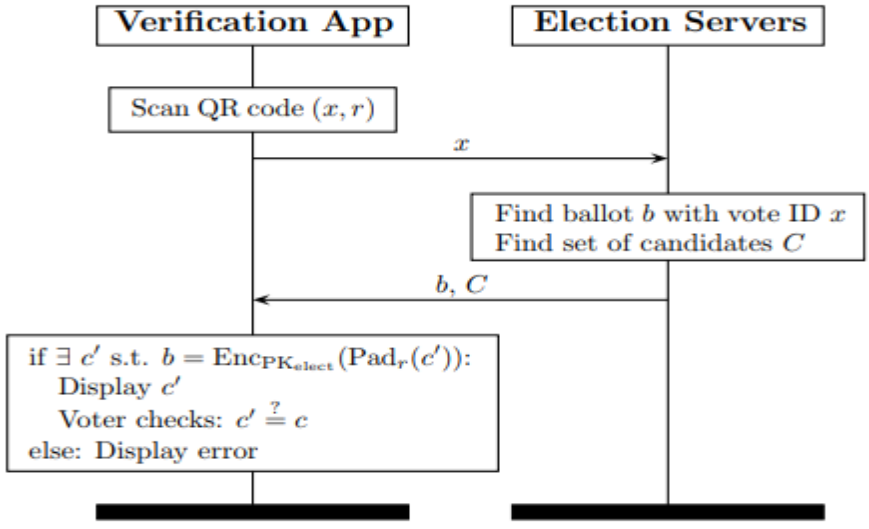
Most internet voting schemes Use cryptographic methods to obtain an end-to-end verification property [8]; that's to say you can trust the computers without having to believe the office-bearer did not cheat. However, the Estonian i-voting system does not rely on cryptographic techniques but on procedural controls [18]. Sample measures such as publishing source code to a GIT server [18] and video recordings do not exhaust the vulnerability that the voting system is prone to. Cyberwarfare is now a threat to recent voting systems as portrayed by attackers linked to Russia who aimed elections in Ukraine and concisely slowed down voting by instigating malicious software into a counting server. A foreign power or a untrustworthy member of staff can alter the

votes counting between decipher and analyzation [9]. Below is a highlight of the voting, verification and tabulation of Estonian's voting system.



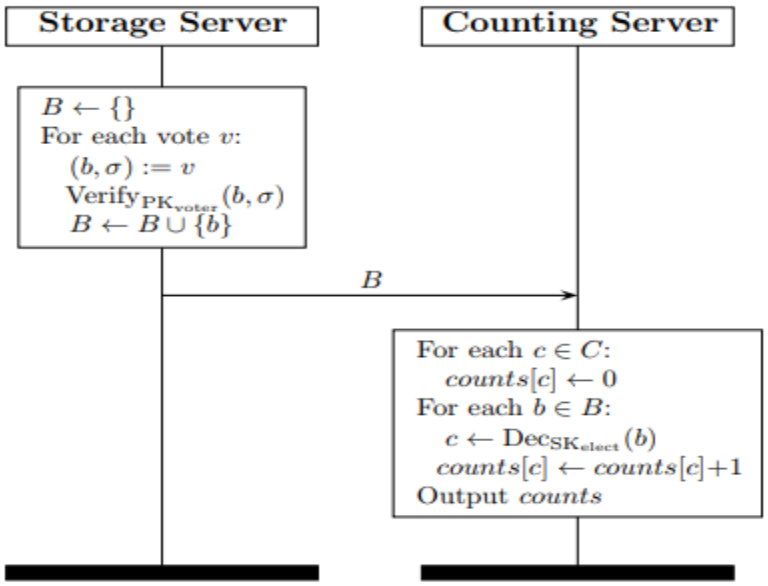
(a) **Vote casting process**

Figure 11. Vote casting process



(b) **Vote verification process**

Figure 12. Vote verification process



(c) **Vote tabulation process**

Fig 13 Vote tabulation process

The system uses asymmetric cryptography by using a digital signature and an inner key which uses public-key encryption and protects the vote's secrecy. Once the eligibility of the voter has been determined, the digital signature is removed, and the ballots moved to a distinct machine for decryption and counting. The voting process is depicted by the figure (a) whereby a voter starts by launching the client application, which is available in both Windows and Unix. The voter then enters the pin which used to authenticate him/her. The server confirms the voter's details and returns a list of nominees associated with his/her district. The encryption process then happens, and the voter is given a QR code. Electors are permitted to vote more than once however earlier votes are revoked but retained for logging purposes. The summary is highlighted in figure 13 below.

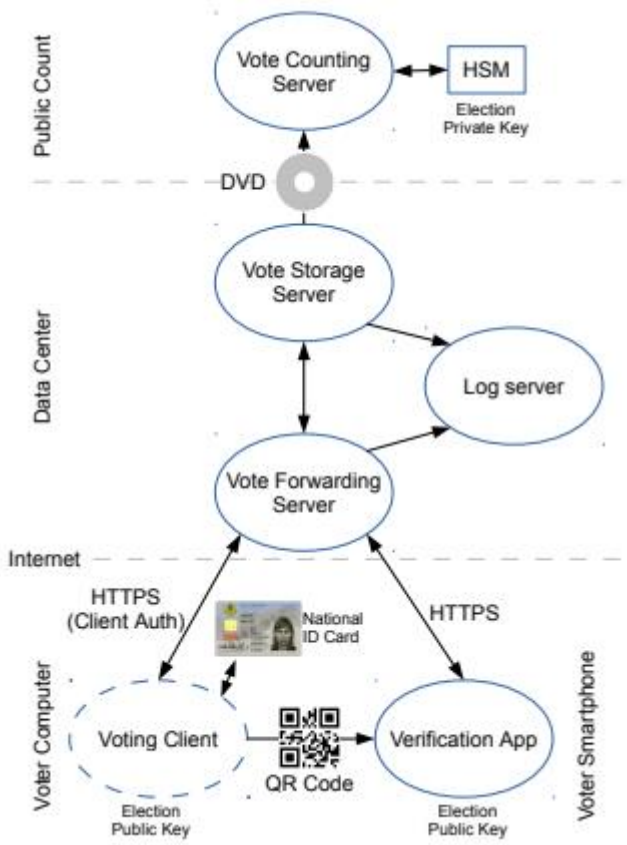


Figure 14. Major components and information flow

Further research highlighted defaults in procedures as:

- The download of the client application was made through a public server which is prone to MIM attacks, and an attacker can introduce malware.
- A PIN entry is done in plain view of the camera. Entry included server passwords among other credentials
- There were also known transfers of results to a remote server for tabulation using a personal USB with other files in it which can be a security lapse in case there is malware.
- Other procedural lapses also show displayed WIFI credentials.
- There are also many experimental attacks that have been carried out successfully as highlighted in [18] including ghost click attack, bad verify attack, injecting ransomware, defeating integrity checking and vote-stealing payload

AS per the discussion above, we have seen that the strategy Estonia had established cannot take care of attacks and guarantee transparency as offered by a blockchain-based e-voting system.

Norwegian I-Voting System

The voters use MinID to log in, which is an electronic ID that provides government services access in Norway at no charge. The technology uses a National identity number of the voter, password and PIN.

Norway implements voter verification differently compared to Estonia. The voter receives a poll card via mail with a list of all parties and a corresponding four-digit code calculated individually for each elector.

After the voter places a ballot, the voting server sends an SMS to the voter's mobile phone containing 4-digit code and can compare if the code received matches the code of her chosen party on the poll card. This gives the voter a chance to verify the vote.

Tallying process - The valid votes are sent via a, which is a mix-servers that work together to provide anonymity in communications through shuffling and re-encryption.

The tallying process is organized by multiple auditors, the ballot boxes are closed and the votes are transferred to the decryptors via the mix-net. These decryptors record the votes they obtained anonymously and the votes decrypted with the private key offline and the auditor as a verifier.

Further research reveals that the Norwegian e-voting scheme has certain security problems that lead to system architecture, which includes attacks from network and centralized infrastructure.

E-voting system based on Blockchain, on the other hand, eliminates some of the security concerned raised above through enforced integrity where each vote is treated as a unique entity transaction on the blockchain and in addition all are tamper-proof and cannot be altered. It also enforces one vote one value meaning that every voter can only cast a vote once.

The system also enforces confidentiality where all votes are converted into hashes once the ballot is cast.

Based on the above review of the three systems .table2 below provides a summary.

	Estonian I-Voting System	**Norwegian I-Voting System**	**Blockchain –E-voting system**
Authentication	eID	MinID	Username &password
Voting Policy	Multiple	Multiple	single
Distributed	Partially	Partially	Fully
Ballot Anonymity	Partially	Yes	Yes
Transparency	Partially	Partially	Yes
Centralized data centre	yes	Yes	No

Table 2. Comparison of the systems

CHAPTER 5: CONCLUSION

5.1 Research Objectives & Results

At the beginning of the research work, key objectives were set.

5.1.1 To construct and test an e-voting system, which will enable the use of valuable information that accompanies the voting process using the blockchain technology.

A blockchain e-voting application prototype was successfully developed and tested as a proof-of-concept. The application has two main modules namely

1. Voters Module - This module allows registered voters to login and vote for different candidates on different positions
2. Commissioners Modules – which allows the commissioners to monitor the results as voters cast their votes.

5.1.2 To elaborate and bring out the pros of the blockchain e-voting system has over the currently existing systems used by IEBC.

The blockchain e-voting system has proofed that blockchain has the following advantage against the current existing manual voting system as used by the electoral body in Kenya

1. Integrity –all the votes cast are tamper-proof and can not be altered
2. Confidentiality – Each vote is treated as a unique transaction and a unique hash generated which is passed across the nodes in the chain.
3. Anonymity – since each voter is hidden behind the blockchain technology, and thus, identity is never revealed.
4. Authentication and Authorization- only authorized entities can be able to access the system
5. Hack proof system – based on technology of blockchain, the databases are distributed, and absolute information record dispensed amongst the nodes in the chain. Data is packaged with the greatest number and a specific hash check, and thus id becomes very difficult to tamper with the data.

5.2 Conclusion

In this paper, we have presented a proof of concept system for developing an e-Voting system that utilized blockchain technology. It is a decentralized system and data from one node passes across all the others in real-time. Every registered voter has the capacity to vote using any Internet-connected device. The blockchain can be verified openly and circulated in such a manner that nobody can corrupt it.

5.3 Limitations

The time given for the research and findings was short given the wide scope and sensitive part in which election play in this country. Blockchain analysis is also a very involving process that needs a lot of time and effort.

Another limitation was the unwillingness by Independent Electoral and Boundaries Commission to share real data for the research due to privacy concerns. Big volumes of real data would have enhanced the quality of the project greatly and better testing of the application.

References

(IFES) Africa International foundation For electoral, 2017. Elections in Kenya. *2017 General Elections.*

Avison, D. B. R. a. M. M., 2001. "Controlling action research projects". *Information Technology & People,* 14(1), pp. 28-45.

Avison, D. F. L. M. D. M. a. P. A. N., January 1999. Action Research. *Communications of the ACM,* 42(1), pp. 94-97.

Baskerville, R. a. M. M., 2004. "Special Issue on Action Research in Information Systems: Making IS Research Relevant to Practice-Foreword,". *MIS Quarterly (28:3),* 28(3), pp. 329-335.

Baskerville, R. a. P.-H. J., 1999. "Grounded action research: a method for understanding IT in practice,". *Accounting, Management and Information Technologies,* 9(1), pp. 1-23.

Baskerville, R. a. W.-H. A. ". C. P. o. A. R. a. a. M. f. I. S. R., 1996. "A Critical Perspective on Action Research as a Method for Information Systems Research,". *Journal of Information Technology,* Volume 11, pp. 235-246.

Baskerville, R. C. o. t. A. (. 1., 1999. *"Investigating Information Systems with Action Research,",* s.l. AIS E-library.

Chaum., D., 2004. Secret-ballot receipts: True voter-verifiable elections.. *IEEE Security & Privacy,* 2(1), pp. 38-47.

Clayton., M., 2014. *csmonitor.* [Online]
Available at: http://www.csmonitor.com/World/ Security-Watch/Cyber-Conflict-Monitor/2014/0617/ Ukraine election narrowly avoided ‘wanton destruction' from hackers. Christian Science MonitorUkraine-election-narrowly-avoided-wanton destruction-f

COMMONWEALTH, S., 2013. Report of the Commonwealth Observer Group. *KENYA GENERAL ELECTIONS.*

Cybernetica., 2013. *“Internet Voting Solution.”.* [Online]
Available at: https://cyber.ee/uploads/2013/03/cyber_ivoting_NEW2_A4_web.pdf.[Accessed 20 October 2018].

D. Evans and N. Paul, 2004. “Election Security: Perception and Reality”. *IEEE Privacy Magazine,* 2(1), pp. 2-9.

D. L. Dill and A.D. Rubin, 2004. “E-Voting Security”. *Security and Privacy Magazine,* Vol. 2(1), pp. 22-23.

D. Lee Kuo Chuen, E., 2015. *Handbook of Digital Currency, 1st ed. Elsevier.* [Online]
Available at: http://EconPapers.repec.org/RePEc: eee:Monogr:9780128021170
[Accessed 20 October 2018].

D. Springall, T. F. Z. D. J. K. H. H. M. M. a. J. A. H., 2014. *“Security Analysis of the Estonian Internet Voting System.”.* s.l., Proceedings of the 2014 ACM SIGSAC Conference on Computer and Communications Security.

D.L.Chaum, 1981. Untraceable Electronic Mail, Return Addresses, and Digital Pseudonyms. *Communications of the ACM,* 24(2), pp. 84-90.

Drew, 2014. Security analysis of the Estonian Internet voting system. *Security analysis of the Estonian Internet voting system.*

European Union, 2018. FINAL REPORT REPUBLIC OF KENYA General Elections 2017. *General Elections 2017.*

F. Reid and M. Harrigan, 2013. "An Analysis of Anonymity in the Bitcoin System", *Security and Privacy in Social Networks.,* pp. 1-27.

IEBC, 2016. Election Results Management Framework. *Election Results Management Framework,* Volume 3, p. 30.

IEBC, 2018. *Independent Electoral and Boundaries commision.* [Online]
Available at: https://www.iebc.or.ke/election/technology/?Biometric_Voter_Registration_System_(BVR) [Accessed 22 octomber 2018].

J. Jan and Y. Chen and Y. Lin, 2001,)October 16-19. *"The Design of Protocol for e-Voting on the Internet",* London, England, Proceedings IEEE 35th Annual 2001 International Carnahan Conference on Security Technology,

Kenya Human Rights Commission, 2007. Violating the voter. *A Report of the 2007 general elections,* p. 55.

Modernisation., M. o. L. G. a., 2013. *"Internet Voting Pilot to be Discontinued..* [Online]
Available at: " https://www.regjeringen.no/en/aktuelt/Internet-voting-pilot-to-be-discontinued/id764300/

National Institute of Standards and Technology, 2012. "Federal Information Processing Standards Publication". *"Federal Information Processing Standards Publication".*

news, A., 2017. *http://www.africanews.com.* [Online]
Available at: http://www.africanews.com/2017/10/25/a-look-at-kenya-s-elections-history-since-independence-in-1964//[Accessed 22/10/2018 October 2018].

NRI, 2015. *Survey on blockchain technologies and related services, "Tech. Rep.* [Online]
Available at: http://www.meti.go.jp/english/press/ 2016/pdf/0531 01f.pdf[Accessed 22 October 2018].

S. Ibrahim and M. Kamat and M. Salleh and S. R. A. Aziz, 2003. *Secure E-Voting with Bling Signature.* Johor, Malaysia, Proceedings of the 4th National Conference of Communication Technology.

S. Nakamoto, 2008. "A Peer-to-Peer Electronic Cash System".

T.ElGamal, 1985. A public Key Cryptosystem and a Signature Scheme Based on Discrete Logarithms. *IEEE Trans.Info.Theory,* Volume 31, pp. 469-472.

TechTarget, 2019. *TechTarget search software quality.* [Online]
Available at: https://www.bing.com/search?q=owasp+api+security+defination&qs=n&form=QBRE&sp=-

1&pq=owasp+api+security+def&sc=0-22&sk=&cvid=67E93F9756534BD199656366605A31C0
[Accessed 25 march 2019].

Trueb Baltic, 2014. *"Estonian Electronic ID – Card Application Specification Prerequisites to the Smart Card Differentiation to the previous Version of EstEID Card Application..* [Online]
Available at: ” http://www.id.ee/public/TBSPEC-EstEID-Chip-App-v3_5-20140327.pdf
[Accessed 20 October 2018].

APPENDICES

APPENDIX 1: Block chain votes

```
package ws;
import db.Blockchain;
import java.text.SimpleDateFormat;
import java.util.ArrayList;
import java.util.Date;
import java.util.List;
import javax.annotation.Resource;
import javax.jws.WebService;
import javax.jws.WebMethod;
import javax.persistence.EntityManager;
import javax.persistence.PersistenceContext;
import javax.transaction.UserTransaction;

/**
 *
 * @author mscproject
 */
@WebService(serviceName = "blockchainVotesNode1")
public class blockchainVotes
{
```

```
    List<String> node = new ArrayList();
    Blockchain bc = new Blockchain();
    @PersistenceContext(name = "muvotePU")
    private UserTransaction utx;
    /**
    @WebMethod(operationName = "VoteNode")
    public List<String> getVoteNode() {
        StringBuilder br = new StringBuilder();
        List<Blockchain> BlockchainList = new ArrayList();
        BlockchainList = em.createQuery("select b from Blockchain b").getResultList();
        for (Blockchain bn : BlockchainList) {
            node.add("Current Hash~" + bn.getBlockchainPK().getCurrenthash() + "~Original Data~" +
bn.getOriginaldata() + "~Previous Hash~" + bn.getPrevioushash() + "~TimeStamp~" +
bn.getTimeStamp() + "~Current ID~" + bn.getBlockchainPK().getIdblockchain() + "~EOF");
        }
        return node;
    }

}
```

APPENDIX 2: Blockchain hash algorithm

```
package bean;
import java.securityMessageDigest;
publicclass Sha256 {
    //uses Sha256 to a string and  results returned.
    Public static String Sha256(String input) {
        try {
            MessageDigest = MessgeDigest.getInstance("SHA-256");
            byte[] hash = digest.digst(input.getBytes("UTF-8"));
            StringBuffer hexString =brand new StringBuffer(); // This will contain hash as hexidecimal
```

```
            for (int i = 0; i < hash.length; i++) {
                String hex = Int.toHexStrng(0xff & hash[i]);
                if (hex.length() == 1) {
                    hexString.append('0');
                }
                hexString.append(hex);
            }
            return hexStrng.toString();
        } catch (Exception e) {
            throw new RntimeException(e);
        }

    }
}
```