University of Nairobi

School of Computing & Informatics

BLOCKCHAIN TECHNOLOGY – A CASE OF COUNTY ASSETS MANAGEMENT IN KENYA

Francis Ngari Mwaniki

P56/8901/2006

Supervisor

Christopher Chepken (PhD)

A Project Report submitted in partial fulfilment for the award of degree of Master of Science in Computer Science, to the School of Computing & Informatics, University of Nairobi

AUGUST 2018

Declaration

Student

This Project report is my original work and to the best of my knowledge has not been submitted to any other institution for examination

Signature: ____

Date: ____

Name: ***Francis Mwaniki Ngari – P56/8901/2006***

University Supervisor

This Project report has been submitted for consideration and marking with my knowledge and authority as the University Supervisor

Signature: _______________________________ *Date:* _____________________

Name: ***Christopher Chepken (PhD)***

Designation: **Senior Lecturer – SCI - University of Nairobi (Kenya)**

Acknowledgement

First, I wish to acknowledge the invisible hand of Almighty God for giving me the strength and wisdom I needed to realize this project. Glory to Him.

Secondly, I wish to recognize the helpful counsel from my supervisor Dr. Christopher Chepken, whose input and advisory contributed greatly to the success of this project. Thank you.

I also extend my thanks to Dr. Evans Miriti, Dr. Mburu, Prof. Okello-Odongo, Mr. Zachary Kirori, Mr. Erick Karanja and Ms. Nancy Kimaru; for their invaluable support and encouragement I received from them along the paths of completing my MSc Project.

Dedication

To my son, Ronnie Mwaniki – A gift in my life…

Abstract

Integrity of database content is not absolute and cannot be guaranteed under the traditional database management technologies leaving it vulnerable to violation of data integrity requirements. This is so especially where the log files are easily accessible to a single entity who may be a malicious database administrator or an authorized third party. Currently, there is deficiency in fool-proof models and architectures that may guarantee accountability, integrity and traceability of user actions in database systems. Various surveys have been conducted in the past exposing quite a number of data integrity breaches in a public sector on management of public assets. In line with these findings, the objective of the study was to model an immutable peer to peer publicly accessible and distributed resource ledger to mimic consensus management of assets based on the innovative blockchain technology. Surveys were conducted to give further insight into the current asset management systems, and the results integrated into the development of a private-public key cryptosystem - the underlying technology for blockchain as a basis for resource management. An experiment was setup targeting County Government asset management in Kenya in view of assessing applicability of the blockchain technology through validation and verification procedures of various transactions. The generated results indicated that the framework met the three requirements of verifiability, validity and consensus in resource management; and is therefore applicable in resource management applications where data integrity is key such as managing County Government assets.

Contents

List of Figures

List of Tables

List of Acronyms and Abbreviations

AWS	Amazon Web Services
DG	Devolved Government
HTML	Hyper Text Markup Language
HTTP	Hyper Text Transfer Protocol
IBM	International Business Machines
IM	Investment Management
MC	Municipal Council
PC	Personal Computer
PDDI	Pervasive Decentralization of Digital Infrastructure
PHP	Hyper Text Pre-Processor
TA	Transition Authority
UN	United Nations
DBMS	Database Management System

CHAPTER ONE

INTRODUCTION

1.1 Background

The management of public resources with certainty and reliability of information can be a challenge to reckon with in all sectors of Kenyan economy. Specifically, public institutions are actively digitalizing the records management systems for improved reliability According to a report by United Nations Development Programme (UNDP) Annual Report (2014), entitled "An Integrated UNDP Support Programme for the Devolution Process in Kenya", the United Nations (UN) agency rolled out a programme to support the Transition Authority (TA) to undertake measures required for transfer of functions from the national government to the county governments through the support to the unbundling and costing of the devolved functions, supporting the inventory and verification of assets and capacity assessment and rationalization of the public service programme. The report underpins the importance of this transition and may have foreseen quite a number of challenges that needed careful management.

Many database-driven legacy systems are usually prone to unwarranted manipulations in favor of individuals or persons in control. This is usually prevalent in transaction processing activities such as information retrieval, validation and subsequent updates. These malicious and sometimes unintended negative actions aggravate the credibility and integrity concerns of the database state. This is more common in public institutions as well as government agencies where various sensitive but publicly accessible assets such as title deeds, degree certificates and other valuables become exposed to unauthorized manipulations leading to difficulties in their traceability and reliability. In places like local governments, tracing these assets/resources or even holding individuals to account can be a tedious and to some extent an impossible task.

Recent advances in information technology have brought about innovations never imagined before. In a report by AON-AccentureConsulting (2010), titled "Banking on Blockchain: A Value Analysis for Investment Banks", new disruptive technology paradigms continue to emerge to address many social-economic challenges that previously were thought impossible. These new technologies such as blockchain used in digital currencies tend to address a new domain of challenges in the social-economic setup. The key challenge has been and remains on how technology experts can use these novel scientific principles to address challenges that persistently bedevil legacy systems. The dictate to connect known legacy system challenges and rethink new ways based on emerging technologies can greatly push human abilities in the innovation horizon.

Going by the challenges experienced in the transitioning from municipal to county governments, as detailed in the Transition to Devolved Government Act of the Laws of Kenya (2016), the transfer of assets has indicated how difficult it can be to trace and carry out a reliable transition from one regime to another. The Act vests this responsibility to the defunct Transition Authority (TA) to develop and implement transition mechanisms and procedures to guide the process. In its concluding report, the TA exposed the challenges faced by traditional approaches in resource management; especially the transfer of assets from Municipal Councils (MC) to the Devolved Government. Generally, there doesn't exist effective, robust and fool-proof mechanisms to keep track, validate and evaluate public resources with certainty. The accountability of assets belonging to devolved government has remained an enigma due to misuse and misappropriation by the custodians (county employees) – resulting in majority of these assets being illegally transferred to unscrupulous individuals.

In a technology report by Delloitte, (2015), titled "Investment management firms: Positioning for the future with blockchain", Investment Management (IM) leaders have responsibilities beyond managing the issues of the day; they should also position their firms for the future. Part of planning for the future typically entails examining new technologies, when the environment demands. Blockchain is one new technology that should demand IM leadership attention for two reasons. First, this technology has the potential to transform and extend IM business value chains. Secondly, blockchain is in its early stages of development, signaling both risk and opportunity. Therefore, it would be of great interest to model and design a mechanism bridging the old and new technology in view of bringing reliability, accountability and trustless mechanisms in the realms of public asset management.

1.2 Problem Statement

A visit to any public office in any county in Kenya, one would find numerous highly valuable resources (assets) ranging from movables to immovable items. That notwithstanding, there are other numerous resources which are not easily visible and only known to appear in accounts and procurement books. In these books, true information of the asset and its related attributes such as custodianship and location can to a large extent be difficult to establish. To make matters worse, whereas these items are recorded or captured in one form or another, to ascertain the truthfulness of such data remains a complexity given the possibility of data manipulations. These complications of assets traceability continue to bedevil the counties every five years of electoral transitioning hence the public resources continue to be embezzled with little accountability. When a new regime comes into office, they come in with vigor to transform the resource management; but again, the issue of trust, validity of the content and posterity still remains. Of particular interest is posterity; where future traceability of the changes to the assets becomes another critical challenge that can prove very difficult to manage during and after transition periods.

In this project, a qualitative survey was conducted to check out from the industry players' various challenges facing assets handling-databases and in particular in a county government setup.

Thereafter a model/prototype was designed and implemented; integrating the blockchain technology as a way of addressing the observed challenges; and later on, tests were carried out in regard to trustworthiness of data integrity and traceability of assets on a prototype system.

According to one of the reports by the Auditor General (Kenya) (2017), "It is the lack of an inventory of assets and liabilities that has authorities raising red flags about the status of the Sh143 billion worth of property". This is an immense investment in a public set up that technology can be explored to address. This does not necessarily translate into the perception that no technology is in place but rather the problem zeroed into reliability and traceability.

1.3 Objectives

The main objective of the concluded research study was to design, implement and test a framework for county assets management using the innovative blockchain technology.

The specific objectives were to:

i. Analyze existing literature on the possibility of applying blockchain technology in curtailing problems associated with public assets management.

ii. Design and model an immutable distributed public ledger for public asset inventory management.

iii. Design a public interface that can query or explore public resources for purposes of verifying such public records and transactions.

iv. Experiment with the system, collect and collate relevant statistical and performance data.

v. Analyze the results, report on findings and make recommendations.

1.4 Justification

The Kenyan national and local governments have endeavored to come up with various mechanisms of ensuring proper handling of public assets to an extent of putting in place a commission to manage the transitions. One such commission as defined by the Kenyan Constitution is the Transition Authority (TA); of which had the mandate of managing the transfer of assets from the defunct Municipal councils to County government as the new Kenyan constitution was starting to take shape in Year 2013. It had an initial mandate of three years to handle transition complexities. Through the various reports from this Authority, it is evidently clear that the perpetual demon of non-traceability of public assets is far from being defeated due to unreliable and unverifiable traceability techniques. This obviously calls for novel efforts such as the one applied in this research to effectively eradicate this problem or minimize the complexities.

1.5 Scope

The concluded research work aimed at bridging the gap between traditional methods and techniques in public assets management and set modern techniques based on the blockchain technology. This brings to the fore functional and system features such as verifiability, consensus building and transparency and did not consider deeper into other design requirements such as performance, usability and maintainability.

CHAPTER TWO

LITERATURE REVIEW

2.1 Introduction

This section details selected pieces of relevant research studies that have been carried out in the past in the area of blockchain technology in resource management. Sub-section 2.2 provides a guide to the readership on technology resources while 2.3 gives a brief introduction to public asset management. The remainder of this chapter is organized as follows: in sub-sections 2.4 to 2.6 present research works in Blockchain as a promise in public asset management, the principles behind blockchain and the typical applications of this technology. Subsequently the existing lacunas in the application of blockchain-based techniques have been summarized in sub-section 2.7

2.2 Technology Resources

Due to the nascent nature of Blockchain Technology, most readership would be found in technical and technology reports by major government and United Nations (UN) Agencies as well as Investment and Technology firms across the globe notably AON, Delloitte, International Business Machines (IBM), Oracle, Amazon Web Services (AWS) among others. An increasing record of academic papers are also available as pointers to the applicability of the technology especially in asset management. Further, information on Devolved Government in Kenya can be found in the Transition to Devolved Government Act of 2012 and the revised version of 2016 of the Laws of Kenya as well as documented reports by the Transition Authority (TA) of Kenya. Some of these pointers and links have been provided as bibliographic information at the end of this document.

2.3 Public Asset Management

Government and public institutions have invested heavily on behalf of its citizens in various multi-trillion shilling assets. These assets are distributed to all sectors of the economy; ranging from the visible and simple items; to complex intangible and invisible items such patents, infrastructure below the earth surface just but to mention a few. Public servants come and go but some public investments must remain; and assets remain to be accounted for. As such, various systems in form of databases and simple spreadsheet applications have been designed to act as repositories of these assets for purpose of accountability and traceability. According to an article by Shepherd E., (2006) "Why are records in the public sector organizational assets?", records are an essential element in the accountability of government operations, in the maintenance of transparent democracies, through the provision of and access to information and in effect lead to proper formulation and execution of its policies.

The issue of asset management is not unique to public sector but also private entities need to share and exchange critical data. Most of data contained in their systems is critical and product sensitive (such as patents) and any unwarranted manipulation can be costly. This can lead to scenarios where the after-product of using manipulated data must be recalled and subsequently compensating the customer. These kind of challenges have guided a number of researchers in trying to explore applicability of blockchain to address product centric data sharing. A case study by Mattila J, Seppälä T, and Holmström J, (2016) entitled "Product-centric Information Management: A Case Study of a Shared Platform with Blockchain Technology", the authors make an effort to analyze how blockchain technology could be applied to overcome the digital trust and data synchronization issues related to the product-centric information management architectures. Their key motivation being to examine blockchain technology, its unique properties as a new way to produce and to coordinate distributed databases between a high number of participants. Further they state that the results of the qualitative case analysis show that blockchain technology can be a suitable architectural basis for a product-centric management platform. It would significantly enhance the data transparency, data traceability and the verifiability of the product-centric model, allowing different organizations to effectively trust each other's product data.

2.4 Blockchain: An Emerging Technology

The world of technology as initially indicated is exploding and changing for the better of human endeavors. As once the cofounder of Intel Andy Grove once said: “There is at least one point in the history of any company when you have to change dramatically to rise to the next level of performance. Miss that moment – and you start to decline”. This is the moment we are in with the emergent of blockchain set of technologies - perceived to drastically change the way systems architects design applications in the increasingly dynamic distributed environment. Blockchain technology was initially described by a person going by synonym Nakamoto S. (February 2009) in a white paper entitled “Bitcoin: A peer to peer electric cash system”, In this paper, he clearly described how it can work through a combination of the well-known peer to peer networking and private-public key cryptography. Further, he went ahead and coded the structure with an implementation of the popular bitcoin infrastructure – an arguably successful digital cryptocurrency. The original chain is still in operation with little structural changes.

2.5 Blockchain: The Technology

A blockchain is a shared public ledger where transactions are permanently recorded by appending newly validated blocks. The blockchain serves as a historical record of all transactions that ever occurred, from the genesis block to the latest block, hence the name blockchain. According to an article by Professor Michael Mainelli and Mike Smith: “Sharing ledgers for sharing economies: An exploration of mutual distributed ledgers (2015), a blockchain is a distributed ledger which is a transaction database based on a mutual distributed cryptographic ledger shared amongst all nodes participating in a system. It is public in that it is decentralized and shared by all nodes of a system or network. There is integrity as double spending is prevented through block validation.

As a concept of distributed database through peer to peer connectivity, the dataset will not be entirely stored at a single physical location, but rather in a dispersed network of interconnected computers, a concept that can greatly enhance the redesign of public assets repositories. The blockchain does not require a central authority or trusted third party to coordinate interactions, validate transactions or oversee behavior. A full copy of the blockchain contains every transaction ever executed, making information on the value belonging to every active address (account) accessible at any point in history.

In the same study, the researchers indicated that while a third party may be trusted, it does not mean they are trustworthy. Further, they state that in a centralized registry, one can experience three weak points as “sin of commission” — forgery of a transaction; “sin of deletion” — reversal of a transaction; and “sin of omission” — censorship of a transaction. These weak points correspond to the three roles of a trusted third party — validation, safeguarding and preservation; typically lacking among the many custodians of public assets.

Figure 1 illustrates the interactions and the internal composition of nodes in a blockchain architecture. Every node maintains a local database of blocks chained in the time dimension and which is constantly kept up-to-date through update communication from the blockchain system.

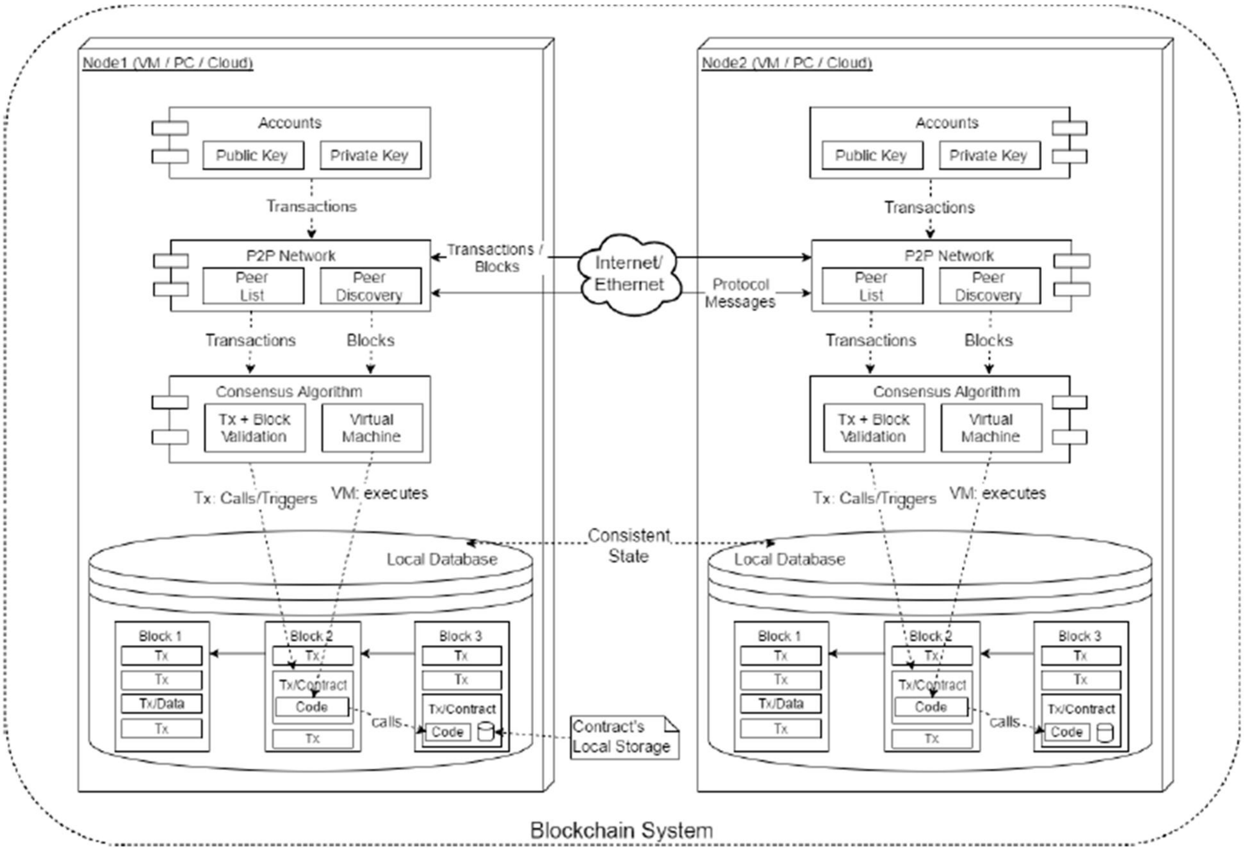


Figure 1: Blockchain System Concepts and Relationships (Source:PDDI – Frameworks)

Any transactions taking place in the blockchain system that results in a new system state are coded by the consensus algorithm that updates the local copy of the database and subsequently relays those updates across the network to other nodes in the system.

2.6 Applications of Blockchain

Blockchain is proving to be a disruptive technology and it has a potential of reconfiguring all human imaginations as pervasively as the Internet did. This is according to a book by Melania Swan (2015) where she foresees blockchain as the architecture for a new decentralized and trust-less engines which are key to future innovations. Given that the concept is relatively new and currently gaining traction, very few systems are completely in production outside research laboratories. But the technology is well developed in the areas of digital currencies and related exchange concepts around the digital assets. But many a report from researchers and commentators, foresee the concept gaining a lot of usage in the management and sharing vital public records such as certificates, Intellectual properties as indicated by a case study by Mattila J, Seppälä, T. and Holmström, J., (2016).

2.7 Research Gaps

The current County implementations of assets recording and management in many setups is done through relational databases or merely via simple spreadsheets and tagging. This has created a big challenge of authenticity and trust especially when recording the public assets besides the critical element of traceability.

In these generic forms of asset recordings, it has opened all forms of fraud mechanisms from basic manipulation of the asset data to situation where the records are deleted or even never recorded. The true details of the data are only dependent and at the mercy of the assigned officer. This has created unparalleled misuse of public resource through unscrupulous transfer.

CHAPTER THREE

METHODOLOGY – DESIGN & IMPLEMENTATION

3.1 Introduction

This chapter comprises two major sections. The first section covers the research methodology that includes the research design approach and methods in 3.2, the data collection in 3.3, the conceptual design in 3.4, the development approach in 3.5, the development framework in 3.6 and the evaluation criteria in 3.7. The second section covers the system design and implementation starting with the system diagram in 3.6

3.2 Research Design

The research design used in this project is an exploratory prototyping approach. After implementing each prototype, a review of objectives was carried out to fine tune the prototype and come up with the next version of the same until the prototype embodies the initial project objectives. The exploratory model as a systems development method (SDM) used to design and develop computer systems or products works best in situations where few, or none, of the system or product requirements are known in detail ahead of time. This approach suited this study since blockchain technology is relatively new and few or no operational systems exist in asset management using blockchain to date.

Based on this approach, the study undertook the following activities:

1. A start of the project, a lot of effort was expended in disseminating blockchain technology and its relevance in asset management. This resulted in the initial conceptual framework illustrated in *Figure 2* below.

2. A first-generation system was put together, based on the information gathered and the ideas formulated in the first step. This formed the basis of further improvements to the prototype.

3. The first-generation system was tested to find out how it performs, what it can and cannot do, and what might be done to improve it. For instance, it necessitated a further re-look into the reward system vis-à-vis who would eventually become the miners for the success of the system

4. A second-generation system was developed from the first one, based on the improvements proposed in the previous step. For instance, as cited in the previous step, the reward mechanism was adjusted to include resourceful county residents with the ability to verify transactions as well as any other outsider due to the extensive computational resource demands of validating a transaction.

5. The second-generation system was tested, as was the first. Its performance was evaluated, and further improvements determined. In this case, the major improvements centered around the usability of the system as well as the reporting. The internal county auditing module was introduced as the foreseer of the verification process.

6. This process was repeated a number of times over the course of the development time until the final system was realized.

3.3 Data Collection

The background information and data used in the analysis phase for this project was gathered from public sources in particular from county government offices through document reviews and directed interviews. The purpose of this fact finding activity was to establish real gaps in the current implementations of asset management systems which guided as a critical factor in the design and implementation of the system. Further, detailed analysis of existing blockchain-based applications, served as a starting point for gaining more knowledge on the possibilities of how to extend these applications. Thereafter, with the help of a modelling approach, models were developed capturing the critical and necessary features for a distributed application of this nature, and finally test data was used to explore the viability of transposing the concept into a prototype application.

The results of these activities were a number of findings that included but not limited to;

1. Lack of reliable asset inventory
2. Poor procurement procedures
3. Un regulated monitoring and disposal of assets
4. Huge financial losses due to inefficiency, theft and misappropriation of asset funds

This pointed to establishment of an efficient and effective framework to:

1. Record and keep an inventory of assets acquired from the defunct Municipal and local governments
2. Manage procurement of new assets and their allocation to different user departments
3. Monitor, validate existence, manage aging and disposal of such assets

3.4 Conceptual Design

As established in section 3.3, a conceptual framework was created centred around a decentralized eco-system of county asset management based on the blockchain technology. In this framework, a number of computing nodes $Node_1, Node_2, \ldots ,Node_N$ were designed to represent mainly the departments of Procurement, Finance, Registry and Audit where each would maintain a copy of the most current county asset database state, *bDb*. This is shown in *Figure 2* below.

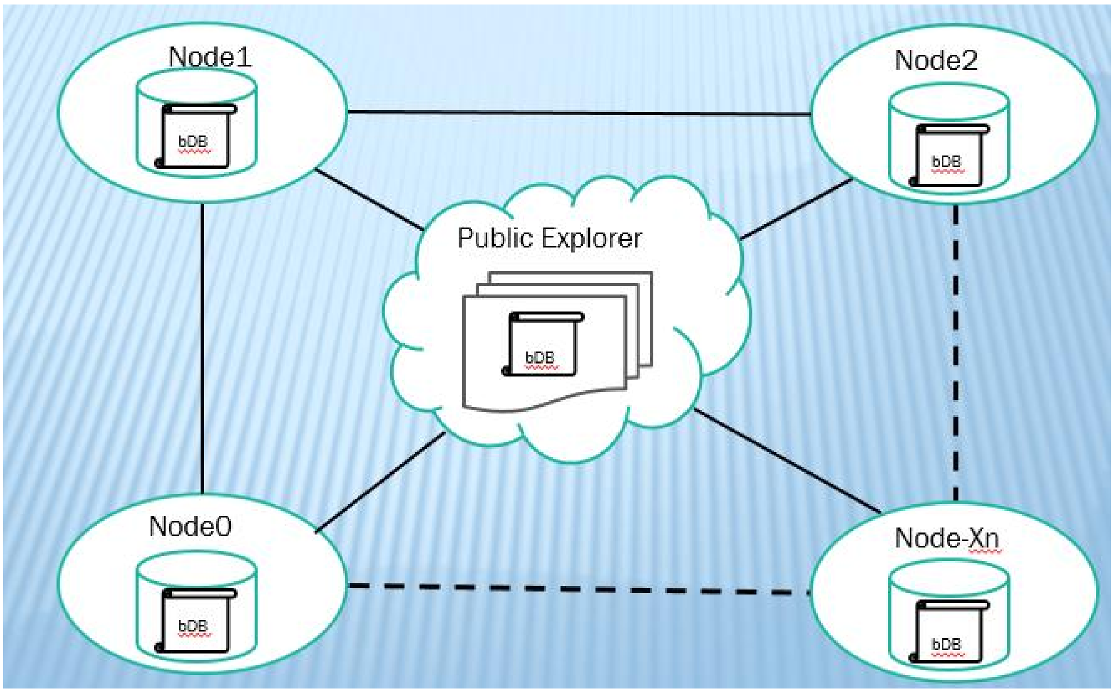


Figure 2: Conceptual Framework [Source: Author]

With the county blockchain infrastructure, any number of miners or verifiers of transactions both within and without the county were envisaged as the '*Public Explorer*'. This is a group of rewardees with the computational capability to compute and verify the blockchain for gain just like in cryptocurrency implementations, besides being a remote-copy hosting for traceability.

3.5 System Development Approach

The project aimed at availing a public interface to query or explore public resources ensuring public transparency. An easily accessible trusted public record of all transactions is of great value. Therefore, core to deliverables included:

1. Tested Models that were utilized in the development and design of a distributed public ledger.
2. A tested prototype of an immutable and trustless distributed database.

In blockchain technology, developers have at their disposal three approaches to building blockchain applications namely;

1. Creating a new blockchain from scratch
2. Re-editing to add functions using script languages on an existing blockchain
3. Piggy-backing a meta-protocol on an existing a blockchain

This project endeavored to building a new blockchain that allowed unrestricted controls in designing various feature set, but at the same time noting that it may turn out to be timing consuming and strenuous in a pool of unknowns. Therefore, on this nascent technology there was need to be aware of its limitations in quick customizing of already existing blockchain infrastructure given its limited feature capabilities, fault-intolerance and scalability issues. The main problem being that most of the blockchain schema in existence are more geared towards minting and managing digital tokens and a few on smart contracts support hence largely inflexible.

3.6 System Analysis

This section covers both the functional and non-functional requirements in section 3.6.1 and 3.6.2. It also elaborates on the system procedures in 3.6.3

3.6.1 Functional Requirements

This subsection contains the functional requirements for a distributed blockchain database of any given county. These requirements are organized by the features discussed so far for an immutable distributed assets repository. A conceptual diagram captures these features well but a further drill in to the conceptual diagram highlights detailed functional requirements of the system as follows:

Security and Auditability

The system applies cryptographic security mechanisms (Public and Private key for each user). It provides support for data encryption, management and enforcement of complex permission settings for participants and third parties. The blockchain's functionality increases the system's reliability as every transaction is associated to a known user cryptographically. Any new transaction that gets affixed to a blockchain results in the transformation of ledger's overall state. Any subsequent iterations led to the previous state being stored resulting into a history log of multiple transactions that are complete and easily traceable. The audit capability of blockchain offers a reliable level of security and transparency over every iteration. From the perspective of cybersecurity, this offers entities with an additional level of reassurance that the data hasn't been tampered at all levels (transaction handling and transmission) and is authentic.

Verifiability

Done with the help of the cryptographic data, the hashed product of the work done and the private node address. Once recorded in the public ledger after peer validation, it becomes immutable and can always be traced back to the particular node. This guarantees both integrity and accountability for the system.

Validity

The system applies cryptographic security mechanisms (Public and Private key for each user). This information is a hashed product of the work done and the private node address. Once recorded in the public ledger after peer validation, it becomes immutable and can always be traced back to the particular node. This guarantees both integrity and accountability for the system.

Accountability and Traceability

For all transactions appended to the blockchain, they are timestamped and signed digitally. This assures that any interested party can trace back or rather audit all transactions at any particular time and locate the corresponding party on the blockchain through their public address. This feature relates to non-repudiation: the assurance that someone can't verify their signature's authenticity on a file, or the authorship of a transaction that they originated.

Scalability

The system provides the ability to secure trillions of transactions or records without compromising the networks synchronization, security, accessibility or data integrity.

Immutability and Data Integrity

Records are guaranteed to be cryptographically secure, with no possibility of bad actors threatening data integrity

Permissioned Access

Writing records is exclusive to subscribed nodes only; third parties can be granted read access, the general public excluded. The permissions architecture goes beyond 'access = everything' and allows third party access to a specific raw data, as deemed appropriate, for interoperability and application requirements.

Decentralized Access

Allowing for equal control over the shared database, between all permissioned participants, and of equal importance. Distributing the number of full copies (nodes) of the ledger to maximize the probability that there will always be a complete record in existence and available for those with permission to access.

3.6.2 System Requirements

The following support requirements were also considered to enhance both the look and feel as well as efficiency of the application.

Usability

An elaborate user interface is critical to the success of any web-based based application such as wallet-like access applications for web and mobile access. A well designed web portal was implemented for block exploration as well as public asset viewing. Various aspects of user interaction were considered as below:

Hardware Interfaces

Since the application runs over the internet, all the hardware required to connect to the Internet forms hardware interface for the system. These include a server for inputting and maintaining County assets initial configuration of the blockchain for subsequent handovers. It acts as a mine pool for initialization of the system but always requires validation from other miners (validators/verification) from time to time to check changes and discrepancies.

The other hardware is a Personal Computer (PC) for county asset managers, county assembly sub-committee on assets as well as mobile phone for anyone else to mine and explore the blockchain. The system also provided storage of initial root blockchain copy for replicating with other Nodes.

Communications Interfaces

The system utilizes the Hyper Text Transfer Protocol (HTTP) for communication over the Internet.

Graphical User Interface

The system provides a uniform look and feel between all interfaces i.e PC as well as a digital image for each feature through icons and toolbars.

Performance

The system is based on blockchain Technology with replication capability to ALL possible Nodes. It takes the initial load time from a set Timestamp which is agreed by ALL the stakeholders leading to agreed nuance (special block number counter). The performance depends upon the proof of stake/Availability algorithm applied.

3.6.3 System Procedures

The key modules for the system are encoded in certain operational procedures, the key amongst them include:

Module: County Asset Managers

The system should:

1. display all the Assets that can be captured
2. allow a user to select/search an Asset
3. display all the available components of the item to capture
4. enable user to add one or more components to the configuration.
5. notify the user about any conflict in the current configuration.
6. allow user to update the configuration to resolve conflict in the current configuration.
7. allow user to confirm the completion of current configuration

Module: Asset details

The system should:

1. display detailed information of the selected Assets.
2. provide browsing options to see asset details.

Module: Product Categorizations

The system should

1. display detailed asset categorization to the user.

Module: Search facility

The system should:

1. enable users to enter the search text on the screen.
2. display all the matching products based on the search
3. display only the required number of matching results on the current screen.
4. enable user to navigate between the search results.
5. notify the user when no matching item is found on the search.

Module: User Details

The system should:

1. allow a user to create profile and set their credentials.
2. authenticate user credentials to view the profile.
3. allow user to update the profile information.

Module: Public Explorer

The system should:

1. provide online help, and sitemap options for customer support.
2. allow users to search from the system
3. Allow the user to categorize search options
4. Verification/Validation capability
5. display and allow user to drill down on search results
6. display the online help upon request.
7. display the Frequently Asked Questions upon request.

3.6.4 Algorithms

Asset Addition Algorithm

```
Begin
    1. Provide the required asset details such as name, code, value.
    2. From the blockchain network get hash of the latest approved asset (HASH1).
    3. Generate a unique hash (HASH2) using details of the asset and HASH1.
    4. HASH2 becomes the hash of the added asset.
    5. The asset is relayed to the rest of the nodes for approval.
    6. If all the nodes approve the asset then it joins the network, else it is rejected
End
```

Validation Algorithm

```
Begin
    1. Using the existing details of an asset compute a hash(HASH1)
    2. Compare HASH1 with the immutable hash in the database.
    3. If there is a difference
    4. The system gives an alert message that the details might have been
       manipulated
    5. else the details are okay
    6. Upon validation of assets for some pre-defined length of time the miner is
       awarded tokens.
End
```

3.7 Detailed System Design

This section details system design beginning with the detailed system architecture in sub-section 3.7.1, followed by system entities and normalization procedures in 3.7.2.

3.7.1 Detailed System Architecture

The detailed system comprises of three key processes as indicated in Figure 3 below, namely:

1. Recording of new assets

   The key departments of Procurement and Finance ensure new assets are procured and recorded in the system.

2. Replication and cloning of new nodes

   The recorded asset details are relayed to the registry and finally to the user departments

3. Authentication mechanisms

   The underlying transactions in 1 and 2 are verified by computing a new block to be added to the existing chain as a proof of an authentic procedure having been performed and completed. This is accomplished by the miners / verifiers through the ‘Public Explorer’ interface under the watch of the county asset management committee chaired by the county assembly nominee.

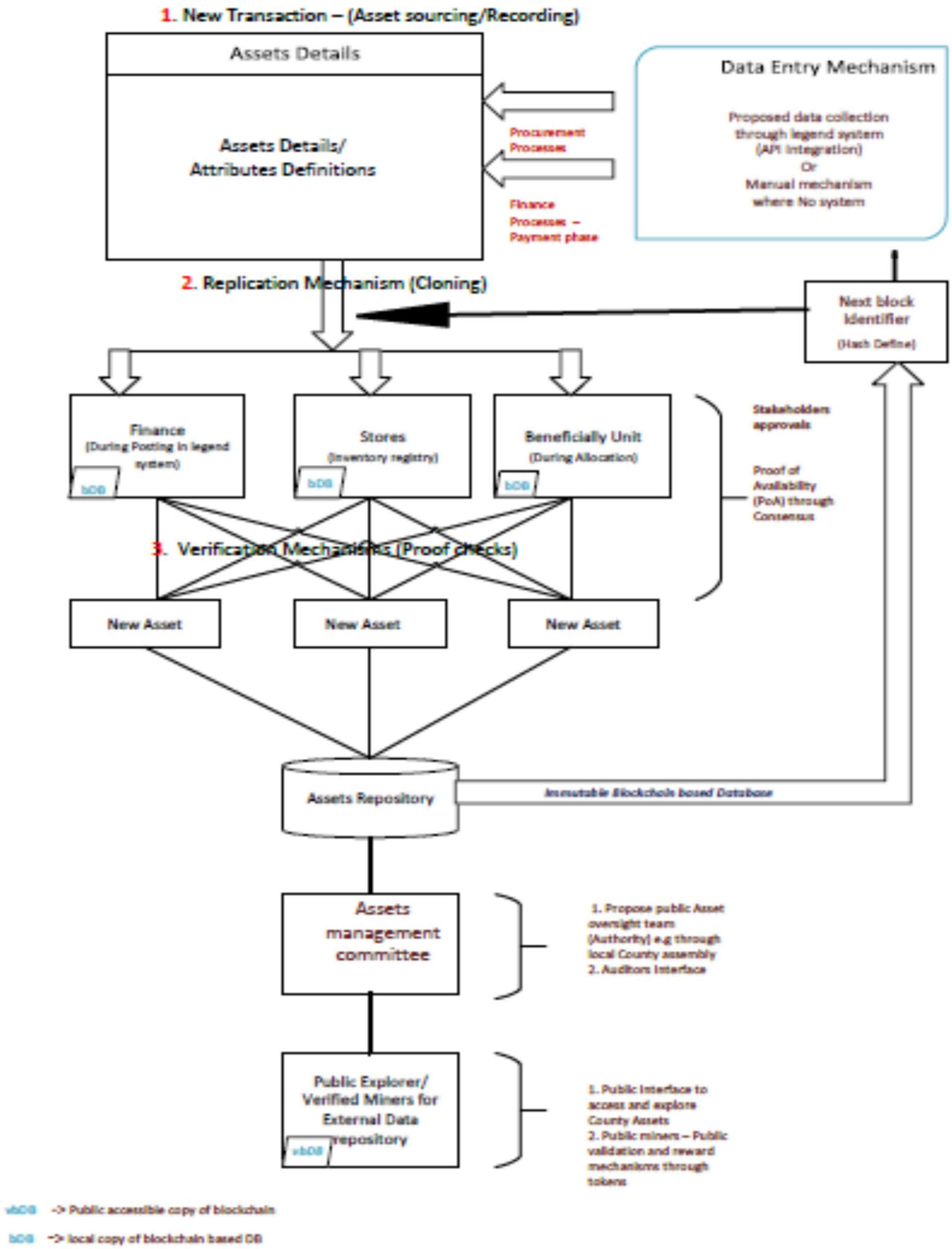


Figure 3: System Architecture [Source: Author]

3.7.2 System Entities

This section details the system design and normalization procedures. It begins with the identification of system entities which are objects, or concepts capable of receiving or issuing commands to other system entities. Next the system processes are identified form the procedural activities that take place. Finally, the user roles and data stores acting as data or information repositories

System Entities

Asset

Refers to tangible items of value including mainly machinery, buildings and office equipment

User

Refers to persons who interact with the system

Role

Refers to a responsibility assigned to a user e.g. an Auditor etc

Miner

Is the verifier of transactions by computing a new block to be added to existing blockchain

Node

Refers to a computational resource mainly a computer system

System Processes

Join Network

Is the act of registering a new node to be part of the existing blockchain ecosystem

Authenticate a User

Process of verifying the authority of a user to user system resources

Clone a Node

The duplication of node

Validate a transaction

The authentication of a transaction with respect to authority against applicable and stated procedures

Play Role

Assumption of a responsibility by a user

Record Asset Details

Capturing of asset data in the asset database

Data Stores

Asset Repository

Main database keeping records of available assets

Users Database

A replica or view of the asset repository for transaction management

User Roles

Auditor/Validators

A user whose responsibilities are verification process and report on system usage

Finance Manager

A user who maintains financial transactions and ensures the right value for money in asset procurement

Procurement Manager

The individual responsible for manning the procurement department

Stores Manager

In charge of the physical asset registry

User Department Manager

In charge of a user departments

Administrator

In charge of the ICT department. Could also be a person in charge of administrative departments in terms of policy

Oversight Committee Manager

Select committee of county assembly - Responsible for oversight roles in conjunction with the audit department

3.7.3 Entity Normalization

In this section, the entity attributes are indicated and reduced to minimize data redundancies

Context Diagram

From 3.7.2, the key entities are represented in a top-level system diagram shown in Figure 4 below

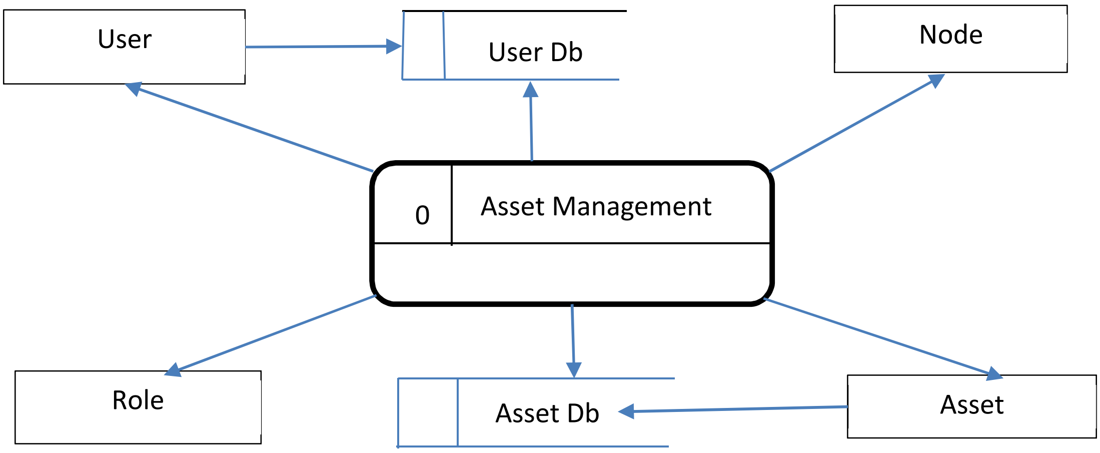


Figure 4: Context Diagram

Entity Attributes

Each of the identified entities is broken down into its constituent attributes as shown in this section

Asset

The asset entity is described by the following properties

- identity
- hash code
- previous Hash code
- creating Node identity
- approving Node identity
- created By
- asset Code
- approved By
- asset Description
- asset Value
- finance Comments
- stores Comments
- stores Approval
- beneficiary Unit Approval
- finance Approval
- beneficiary Unit Comments
- payment Mode
- status

Node

The node entity is described by the following properties

- identity
- ip Address
- clone from Ip
- node Name

- private Key
- number of Users
- public Key
- is Alive ()

Role

The role entity is described by the following properties

- identity
- role Name
- order detail identity
- access Finance Department
- access Stores Department
- access Beneficiary Unit Department

User

The user entity is described by the following properties

- identity
- username
- password
- role identity
- first Name
- last Name

Level 1 Data Flow Diagram

The zoomed-in context diagram indicating the key system entities, data stores and processes is shown as a Level 1 Data Flow Diagram in Figure 5 below

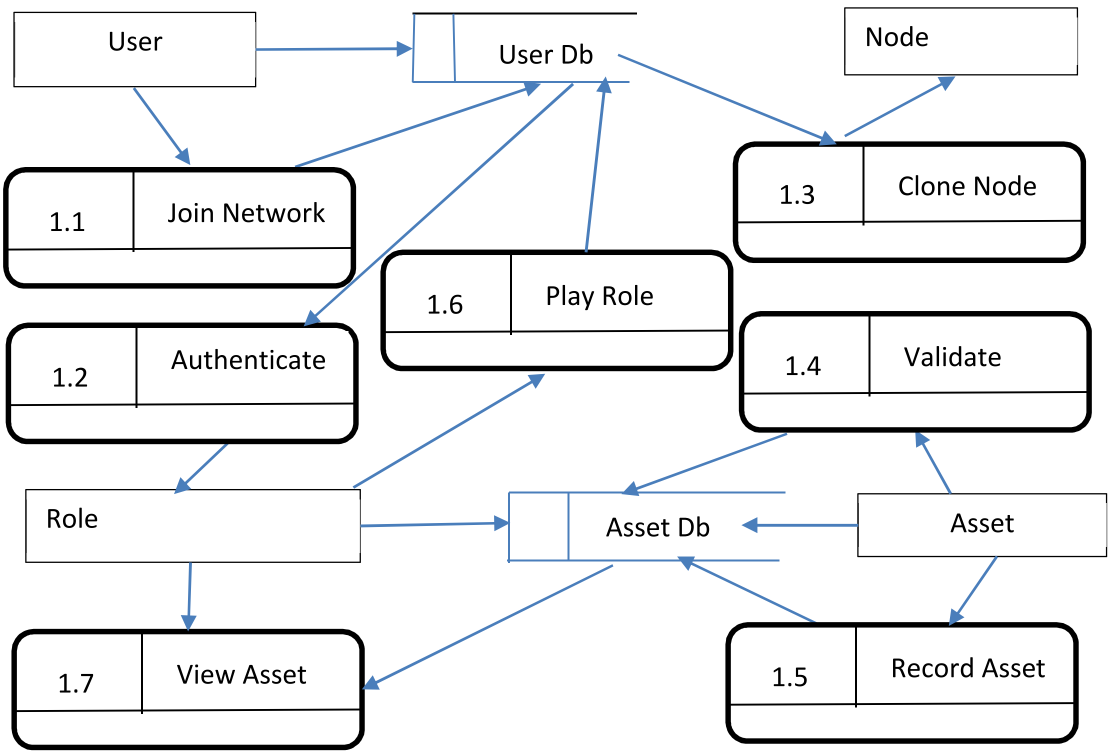


Figure 5: Level 1 Data Flow Diagram

Second (2nd) Level Normalization

In in this section, the first level attributes are reduced by removing redundancies

Asset

After 2nd Level Normalization, the asset entity retains the following attributes with asset code identified as the unique attribute as shown below

- <u>asset Code</u>
- asset Description
- hash code
- previous Hash code
- creating Node identity
- approving Node identity
- created By

- approved By
- asset Value
- payment Mode
- status

Node

After 2nd Level Normalization, the node entity retains the following attributes with IP address identified as the unique attribute as shown below

- IP Address
- asset Code
- clone From IP
- node Name
- private Key
- public Key

Role

After 2nd Level Normalization, the Role entity retains the following attributes with Role Identity identified as the unique attribute as shown below

- role identity
- user identity
- role Name
- order detail identity
- access Finance Department
- access Stores Department
- access Beneficiary Unit Department

User

After 2nd Level Normalization, the User entity retains the following attributes with User Identity identified as the unique attribute as shown below

- user identity
- username
- password
- role identity
- first Name
- last Name

Level 2 Data Flow Diagrams

The level 2 Data Flow Diagrams as shown in this section having been reduced to process levels.

Join Network Process

The procedure for joining a network is:

Begin

1. Submit login credentials
2. Approve credentialsEnd

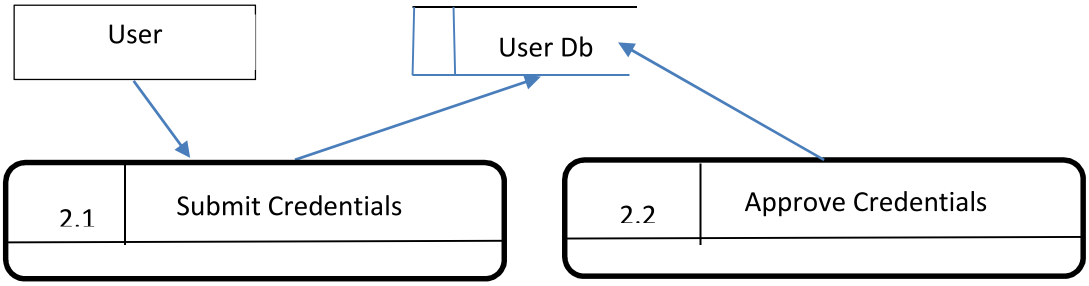


Figure 6: Join Network Process

Authenticate User

The procedure for authenticating is:

Begin

1. Submit Login Credentials
2. Compare against User Database
3. Accept / Deny

End

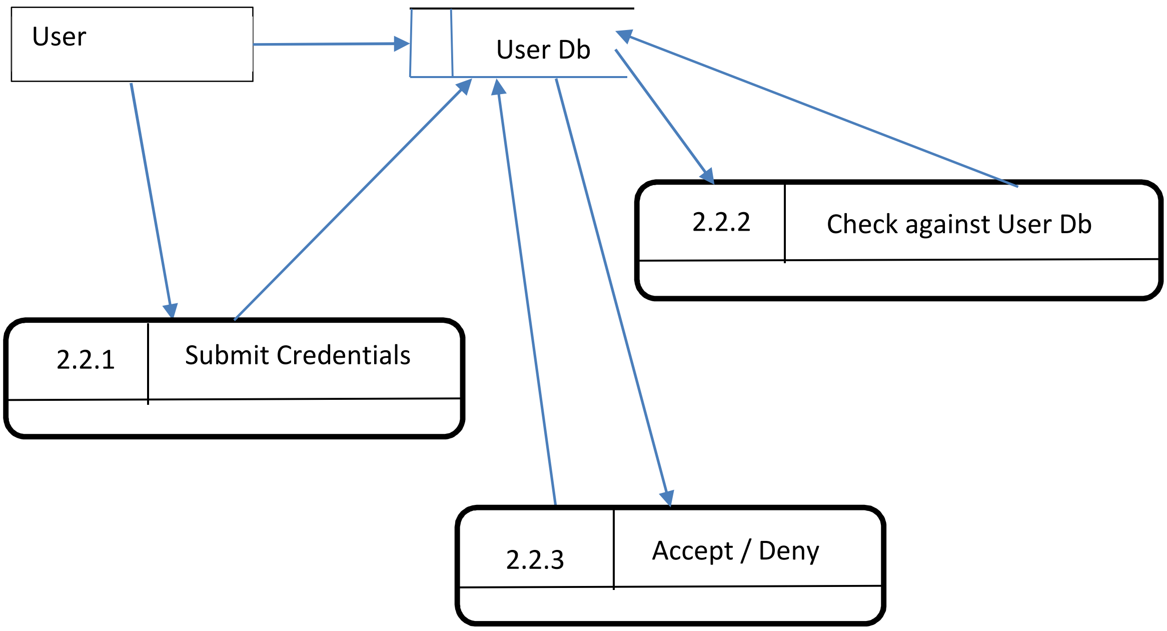


Figure 7: Authenticate User Process

Clone Node Process

The procedure for cloning a node is:

Begin

1 Submit User Credentials

2 Submit User IP address

3 Submit IP address to clone from

4 Submit number of users

End

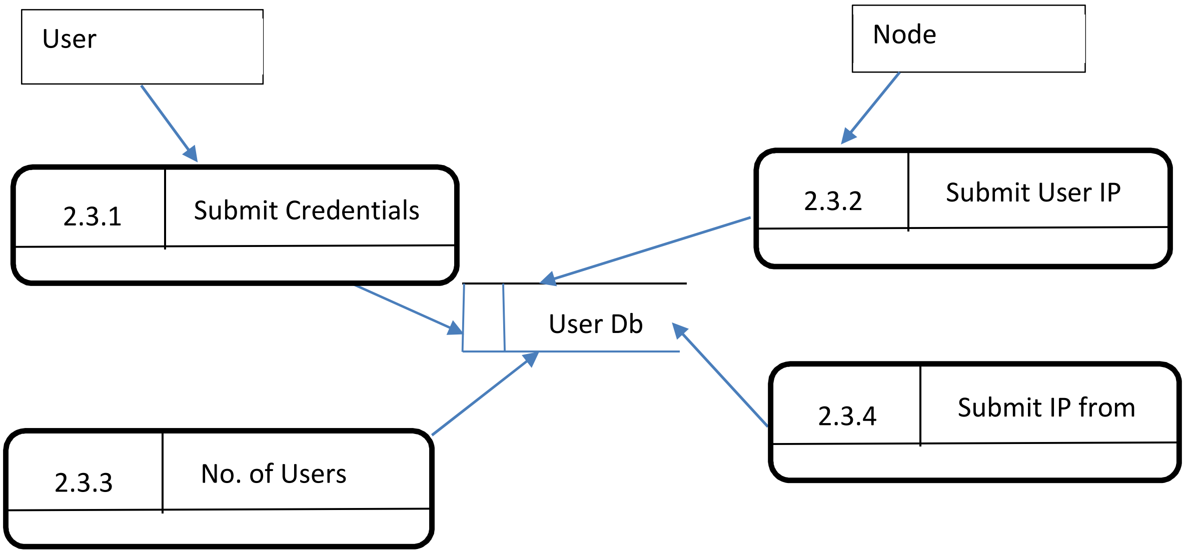


Figure 8: Clone a Node Process

Add a New Asset

The procedure for adding a new asset is:

Begin

1. Provide the required asset details such as name, code, value.
2. From the blockchain network get hash of the latest approved asset (HASH1).
3. Generate a unique hash (HASH2) using details of the asset and HASH1.
4. Relay addition to the rest of the nodes for approval.
5. Approve Reject new asset

End

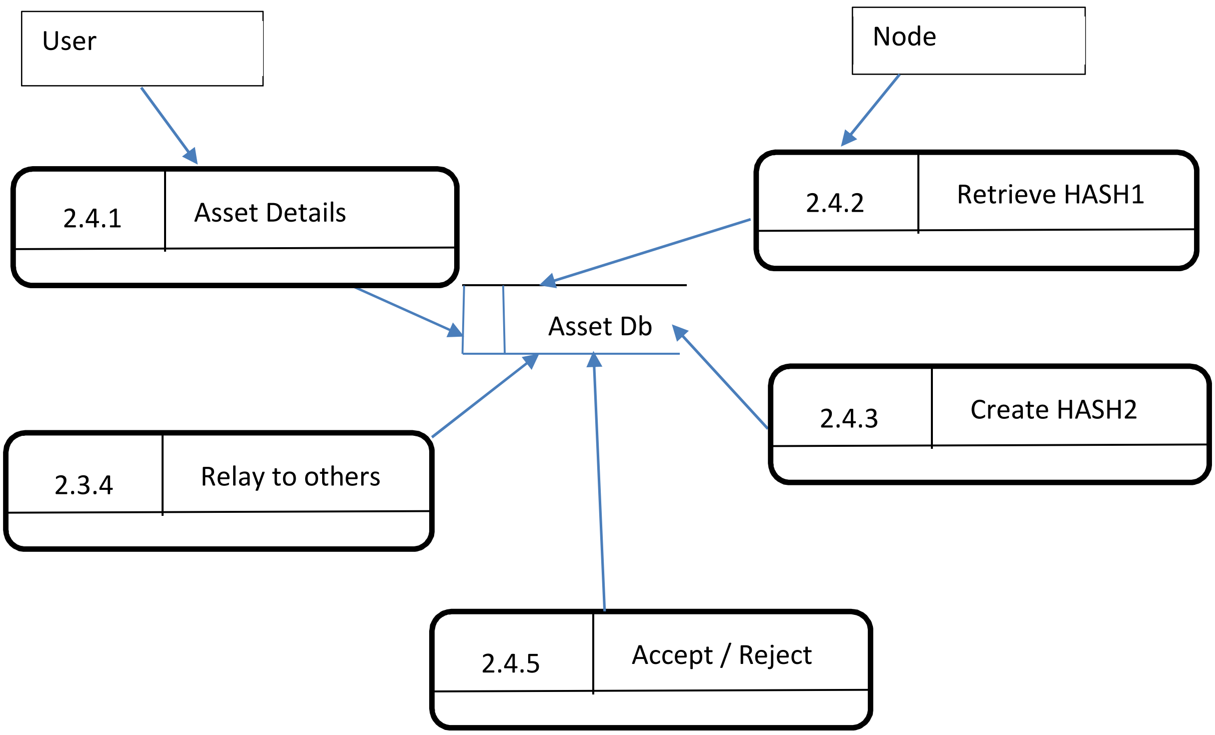


Figure 9: Add Asset Process

Validate Process

The procedure for the validation process is:

```
Begin
    1. Using the existing details of an asset compute a hash(HASH1)
    2. Compare HASH1 with the immutable hash in the database.
    3. If there is a difference // it means that some details must have changed.
    4. Approve / Reject
    5. Award Role.
End
```

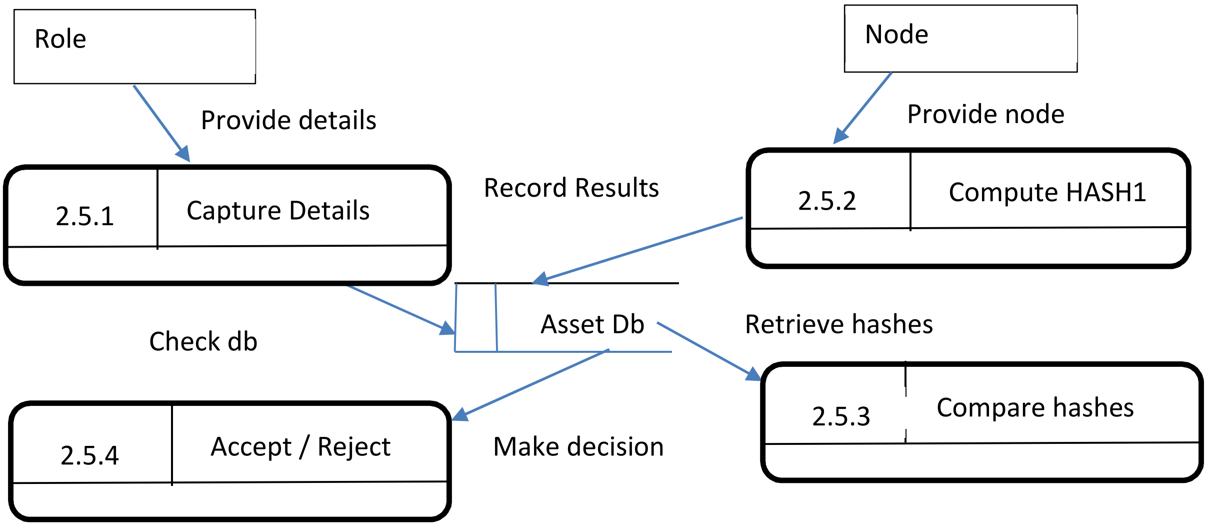


Figure 10: Validate Process

3.7.4 Entity Relationship Diagram

The entity relationship diagram generated from the normalized data in 3.7.3 is shown in Figure 11 below.

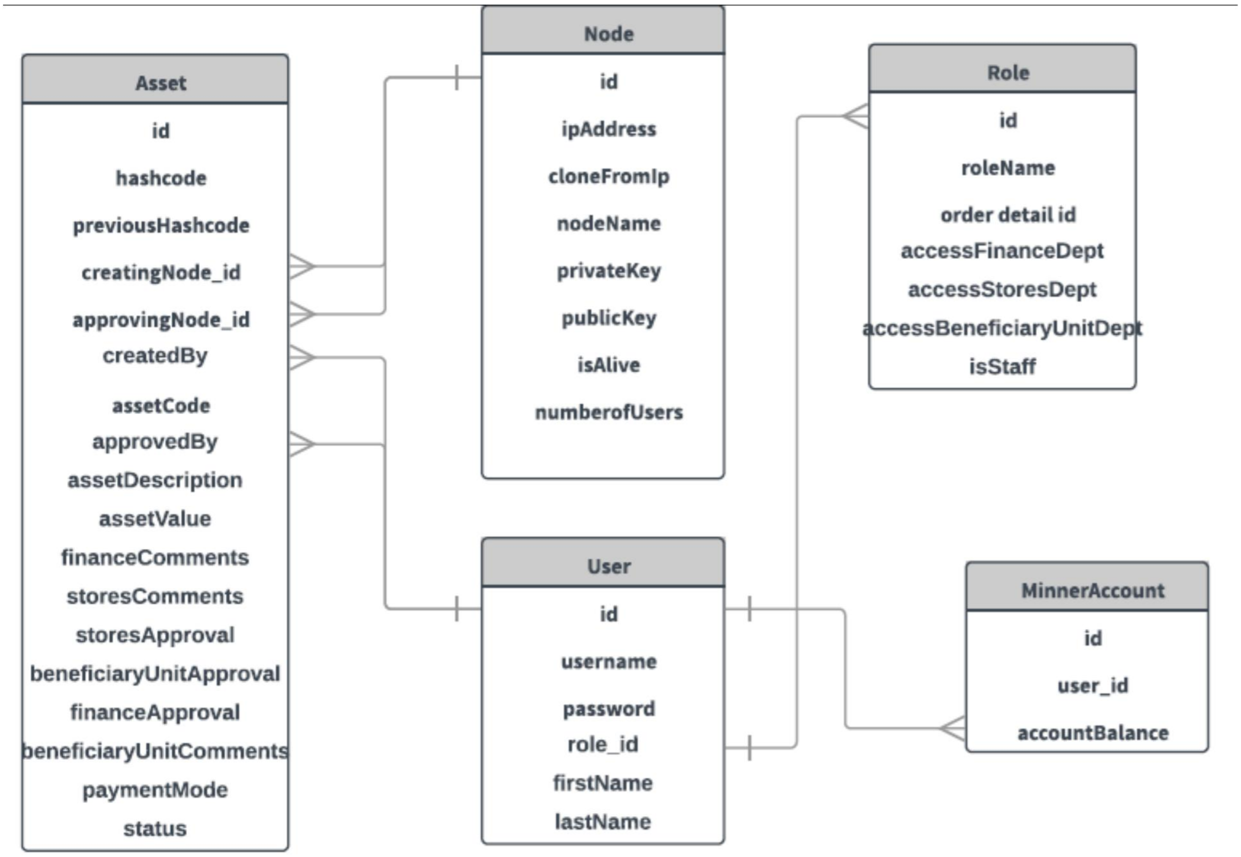
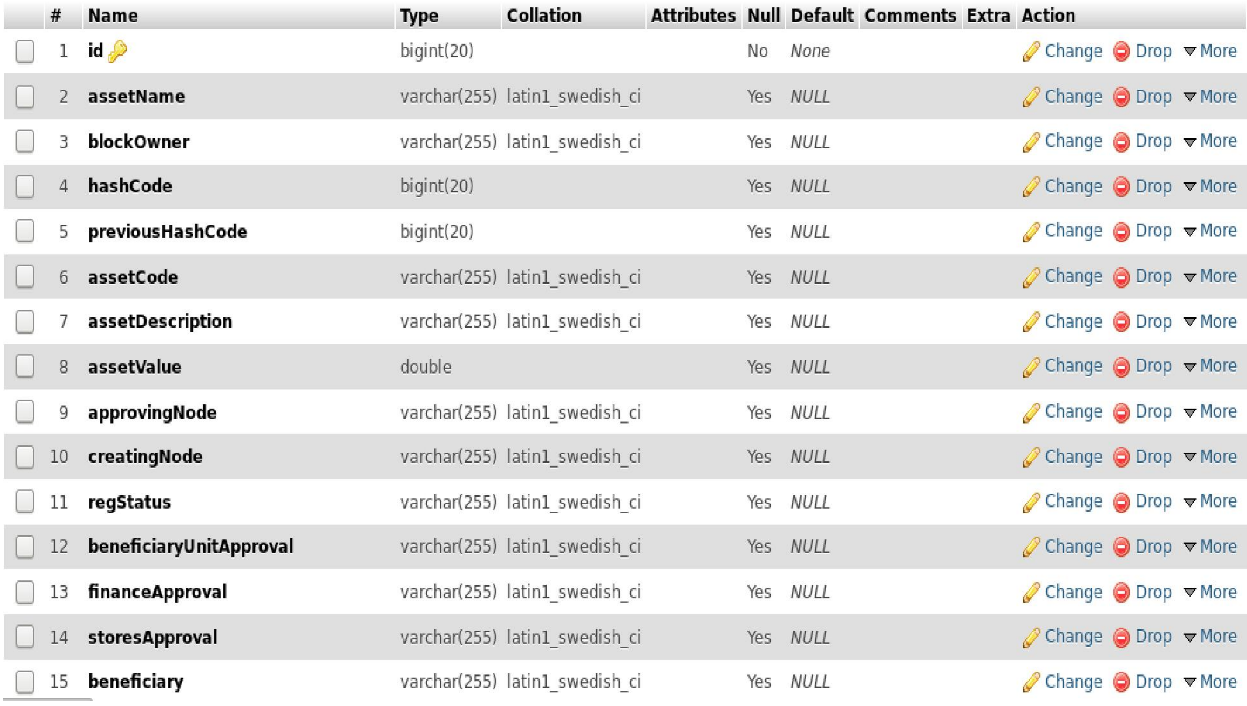


Figure 11: Entity Relationship Diagram

3.7.5 Database Design

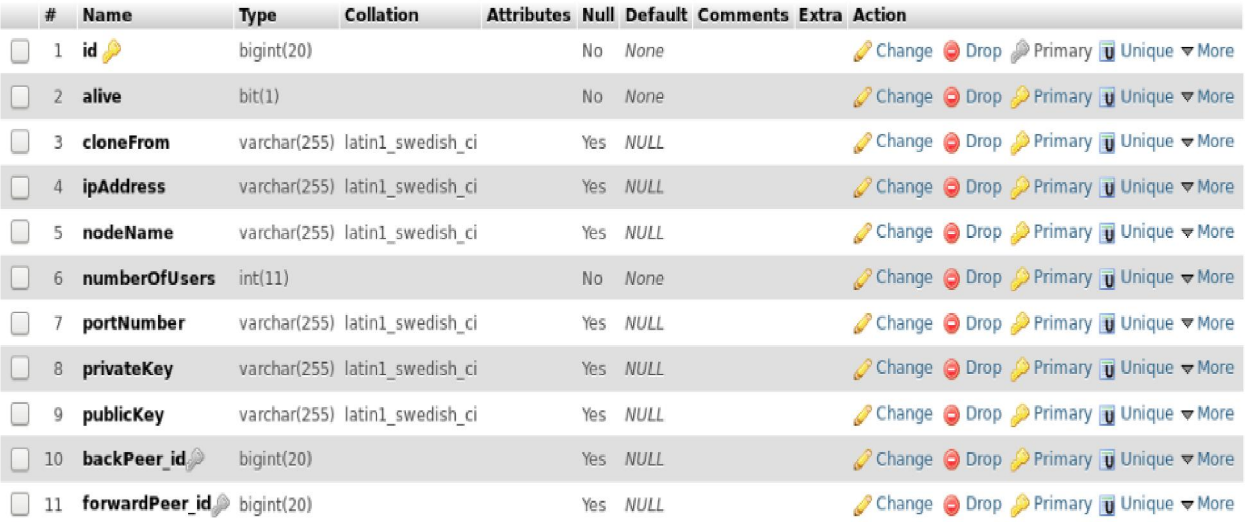
In this section, the database for storing system data is presented as table-designs based on the entity relationship diagram in 3.7.4

Table 1: Assets Table



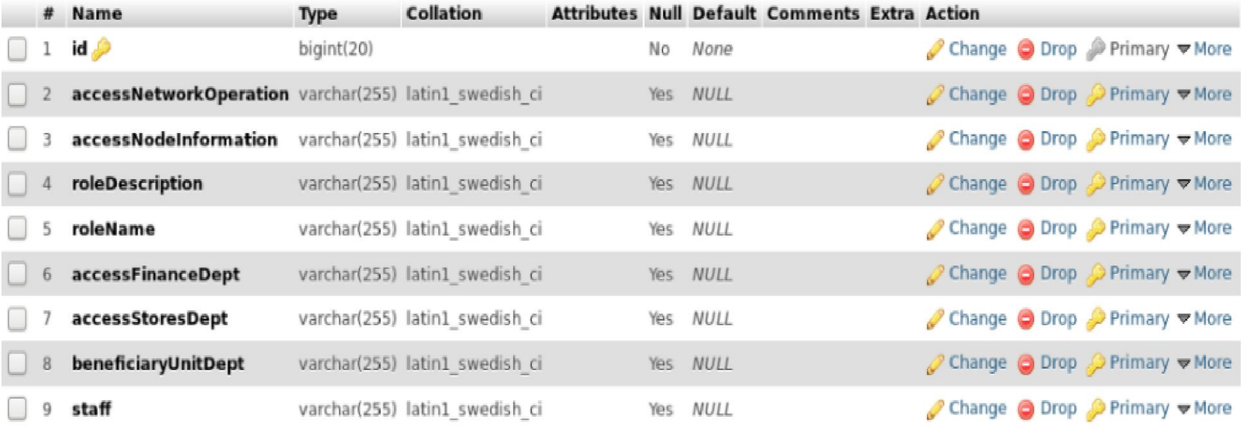
	#	Name	Type	Collation	Attributes	Null	Default	Comments	Extra	Action
□	1	**id** 🔑	bigint(20)			No	*None*			Change Drop More
□	2	**assetName**	varchar(255)	latin1_swedish_ci		Yes	*NULL*			Change Drop More
□	3	**blockOwner**	varchar(255)	latin1_swedish_ci		Yes	*NULL*			Change Drop More
□	4	**hashCode**	bigint(20)			Yes	*NULL*			Change Drop More
□	5	**previousHashCode**	bigint(20)			Yes	*NULL*			Change Drop More
□	6	**assetCode**	varchar(255)	latin1_swedish_ci		Yes	*NULL*			Change Drop More
□	7	**assetDescription**	varchar(255)	latin1_swedish_ci		Yes	*NULL*			Change Drop More
□	8	**assetValue**	double			Yes	*NULL*			Change Drop More
□	9	**approvingNode**	varchar(255)	latin1_swedish_ci		Yes	*NULL*			Change Drop More
□	10	**creatingNode**	varchar(255)	latin1_swedish_ci		Yes	*NULL*			Change Drop More
□	11	**regStatus**	varchar(255)	latin1_swedish_ci		Yes	*NULL*			Change Drop More
□	12	**beneficiaryUnitApproval**	varchar(255)	latin1_swedish_ci		Yes	*NULL*			Change Drop More
□	13	**financeApproval**	varchar(255)	latin1_swedish_ci		Yes	*NULL*			Change Drop More
□	14	**storesApproval**	varchar(255)	latin1_swedish_ci		Yes	*NULL*			Change Drop More
□	15	**beneficiary**	varchar(255)	latin1_swedish_ci		Yes	*NULL*			Change Drop More

Table 2: Nodes Table



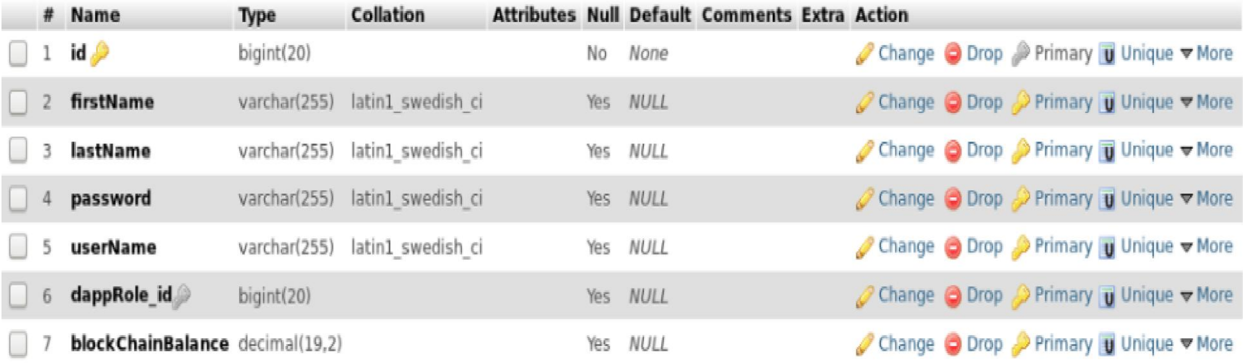
	#	Name	Type	Collation	Attributes	Null	Default	Comments	Extra	Action
□	1	**id** 🔑	bigint(20)			No	*None*			Change Drop Primary Unique More
□	2	**alive**	bit(1)			No	*None*			Change Drop Primary Unique More
□	3	**cloneFrom**	varchar(255)	latin1_swedish_ci		Yes	*NULL*			Change Drop Primary Unique More
□	4	**ipAddress**	varchar(255)	latin1_swedish_ci		Yes	*NULL*			Change Drop Primary Unique More
□	5	**nodeName**	varchar(255)	latin1_swedish_ci		Yes	*NULL*			Change Drop Primary Unique More
□	6	**numberOfUsers**	int(11)			No	*None*			Change Drop Primary Unique More
□	7	**portNumber**	varchar(255)	latin1_swedish_ci		Yes	*NULL*			Change Drop Primary Unique More
□	8	**privateKey**	varchar(255)	latin1_swedish_ci		Yes	*NULL*			Change Drop Primary Unique More
□	9	**publicKey**	varchar(255)	latin1_swedish_ci		Yes	*NULL*			Change Drop Primary Unique More
□	10	**backPeer_id** 🔑	bigint(20)			Yes	*NULL*			Change Drop Primary Unique More
□	11	**forwardPeer_id** 🔑	bigint(20)			Yes	*NULL*			Change Drop Primary Unique More

Table 3: Roles Table



	#	Name	Type	Collation	Attributes	Null	Default	Comments	Extra	Action
□	1	id	bigint(20)			No	None			Change Drop Primary More
□	2	accessNetworkOperation	varchar(255)	latin1_swedish_ci		Yes	NULL			Change Drop Primary More
□	3	accessNodeInformation	varchar(255)	latin1_swedish_ci		Yes	NULL			Change Drop Primary More
□	4	roleDescription	varchar(255)	latin1_swedish_ci		Yes	NULL			Change Drop Primary More
□	5	roleName	varchar(255)	latin1_swedish_ci		Yes	NULL			Change Drop Primary More
□	6	accessFinanceDept	varchar(255)	latin1_swedish_ci		Yes	NULL			Change Drop Primary More
□	7	accessStoresDept	varchar(255)	latin1_swedish_ci		Yes	NULL			Change Drop Primary More
□	8	beneficiaryUnitDept	varchar(255)	latin1_swedish_ci		Yes	NULL			Change Drop Primary More
□	9	staff	varchar(255)	latin1_swedish_ci		Yes	NULL			Change Drop Primary More

Table 4: Users Table

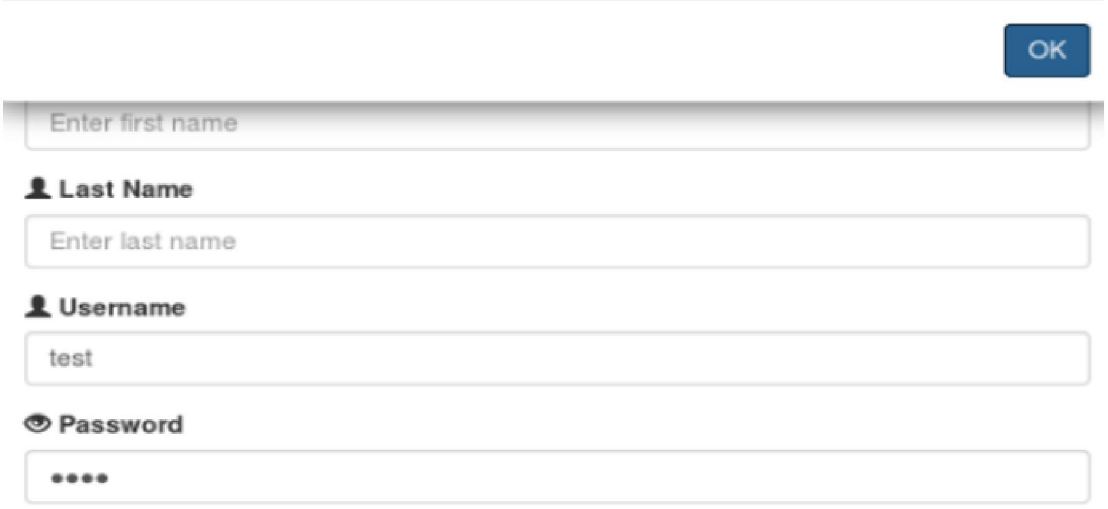


	#	Name	Type	Collation	Attributes	Null	Default	Comments	Extra	Action
□	1	id	bigint(20)			No	None			Change Drop Primary Unique More
□	2	firstName	varchar(255)	latin1_swedish_ci		Yes	NULL			Change Drop Primary Unique More
□	3	lastName	varchar(255)	latin1_swedish_ci		Yes	NULL			Change Drop Primary Unique More
□	4	password	varchar(255)	latin1_swedish_ci		Yes	NULL			Change Drop Primary Unique More
□	5	userName	varchar(255)	latin1_swedish_ci		Yes	NULL			Change Drop Primary Unique More
□	6	dappRole_id	bigint(20)			Yes	NULL			Change Drop Primary Unique More
□	7	blockChainBalance	decimal(19,2)			Yes	NULL			Change Drop Primary Unique More

3.7.6 Input Design

This section details the interaction mechanisms and interfaces between the users and the system as form designs.

Login Form



Enter first name

Last Name

Enter last name

Username

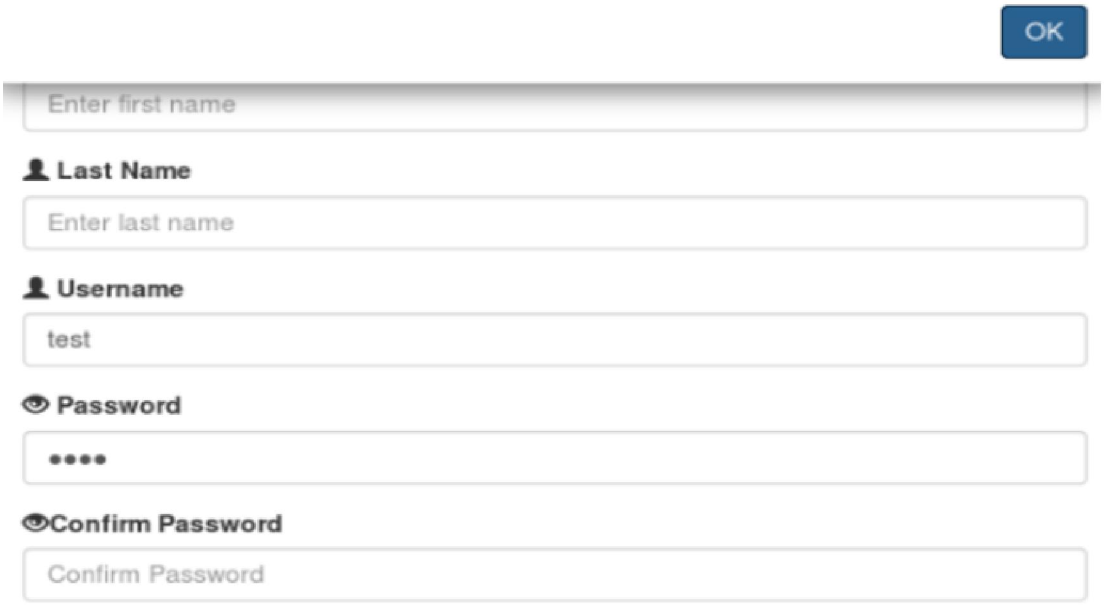
test

Password

••••

Figure 11: Login Form

New User Registration Form



Enter first name

Last Name

Enter last name

Username

test

Password

••••

Confirm Password

Confirm Password

Figure 12: Registration Form

CHAPTER FOUR

TESTING & RESULTS

4.1 Introduction

This chapter reports on the experimentation activities on the developed prototype. Section 4.2 highlights the testing criteria adopted, 4.3 summarizes a number of selected test cases; the test results in the process of verifying and validating the system are given in section 4.4 and sample results in section 4.5.

4.2 System Testing Criteria

The objectives of the system were assessed against the following system features abilities:

1. Enrolment of users who are mandated with key operational procedures.
2. The cloning of new nodes representing user departments whose private system data are requirement for the encryption and validation activities.
3. Verification and validation processes of the key departments of procurement, accounts / finance, registry / store and internal audit.

4.3 Test Cases

Here, a number of test cases are provided to be subjected to the system together with the system expected behavior.

Table 5: Test Cases Table

Test Case Number	Test Case Description	Provided Data	Expected Results	Actual Results	FAIL/PASS
1	User login with incorrect username/password	Username, password	User with the provided username/password does not exist System redirects to error page	User with the provided username/password does not exist System redirects to error page	PASS
2	Login with correct username/password	Username, password	Page redirects to home page	Page redirects to home page	PASS
3	Register asset with the required asset information	Asset code,asset name, asset value,description	Asset Has been added and sent to approving Nodes	Asset Has been added and sent to approving Nodes	PASS
4	Account creation with an existing username	Username,password,first name,last name,password	Sorry.There exists a user with the provided username.Use another username	Sorry.There exists a user with the provided username.Use another username	PASS
5	Validation for data which has not been tampered with	Click the validation button on the explorer section	Details of this asset are correct as provided on the blockchain.Thank You	Details of this asset are correct as provided on the blockchain.Thank You	PASS
6	Validation for data which has been tampered with	Click the validation button on the explorer section	Details of this asset are NOT CORRECT as provided on the blockchain. Kindly contact any county asset manager and report this asset.Thank you.	Details of this asset are NOT CORRECT as provided on the blockchain.Kindly contact any county asset manager and report this asset.Thank you.	PASS
7	Register asset with an existing asset code	Asset code,asset name, asset value,description	Asset with the provide code already Exists!!!!	Asset with the provide code already Exists!!!!	PASS

4.4 System Testing Results

Here, the actual results are presented after subjecting the system to the test data articulated in 4.3 as well as the respective observation after each activity.

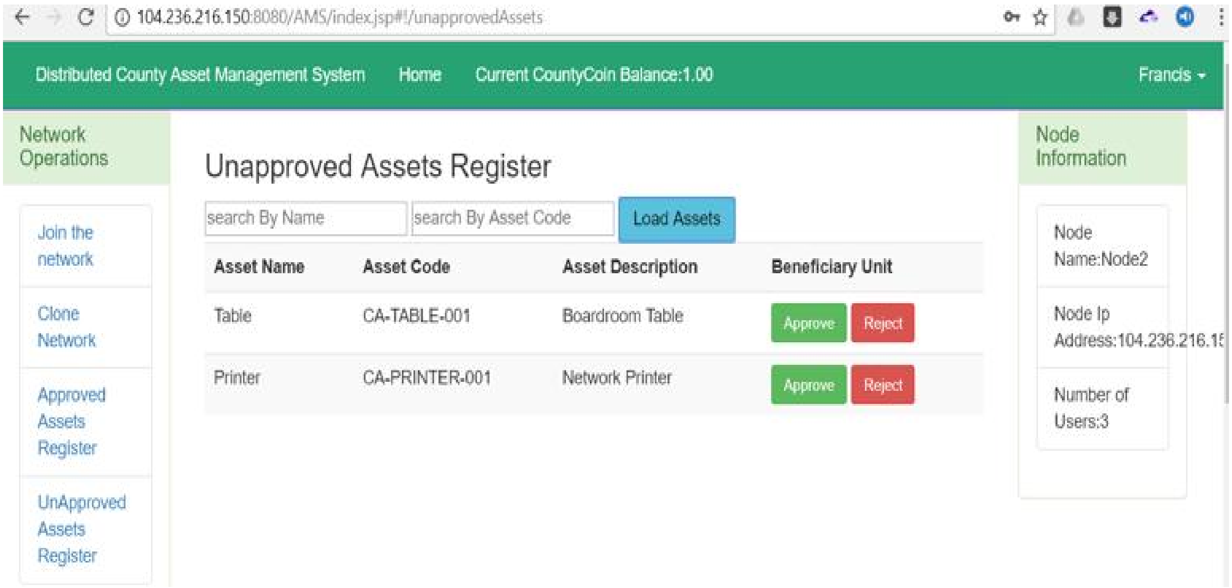
Table 6: Test Results Table

Test Case Number	Test Case Description	Provided Data	Expected Results	Actual Results	REMARKS
1	User login with incorrect username/ password	James.kinuthia, jkinuthia	User with the provided username/password does not exist System redirects to error page	User with the provided username/password does not exist System redirects to error page	OK
2	Login with correct username/ password	Francis, 1 2 3 4 5 6	Page redirects to home page	Page redirects to home page	OK
3	Register asset with the required asset information	CA-TABLET-0010, PDA, 20,000, Portable Computer	Asset Has been added and sent to approving Nodes	Asset Has been added and sent to approving Nodes	OK
4	Account creation with an existing username	stores, stores, Jimmy, Otieno, jotieno	Sorry.There exists a user with the provided username.Use another username	Sorry.There exists a user with the provided username.Use another username	OK
5	Validation for data which has no t been tampered with	Click the validation button on the explorer section	Details of this asset are correct as provided on the blockchain.Thank You	Details of this asset are correct as provided on the blockchain.Thank You	OK
6	Validation for data which has been tampered with	Click the validation button on the explorer section	Details of this asset are NOT CORRECT as provided on the blockchain.Kindly contact any county asset manager and report this asset.Thank you.	Details of this asset are NOT CORRECT as provided on the blockchain.Kindly contact any county asset manager and report this asset.Thank you.	OK
7	Register asset with an existing asset code	CA-PRINTER-004, PRINTER, 600,000, Network Printer	Asset with the provide code already Exists!!!!	Asset with the provide code already Exists!!!!	OK

4.5 Sample Results

The following screens indicate the status of the database at various points during the addition of new assets. Initially, any added asset remains in the unapproved register until it is approved by all the required authorities; afterwhich, it is hashed and gets recorded in the approved asset register.

Unapproved Assets



104.236.216.150:8080/AMS/index.jsp#!/unapprovedAssets

Current CountyCoin Balance:1.00

Unapproved Assets Register

Asset Name	Asset Code	Asset Description	Beneficiary Unit
Table	CA-TABLE-001	Boardroom Table	Approve Reject
Printer	CA-PRINTER-001	Network Printer	Approve Reject

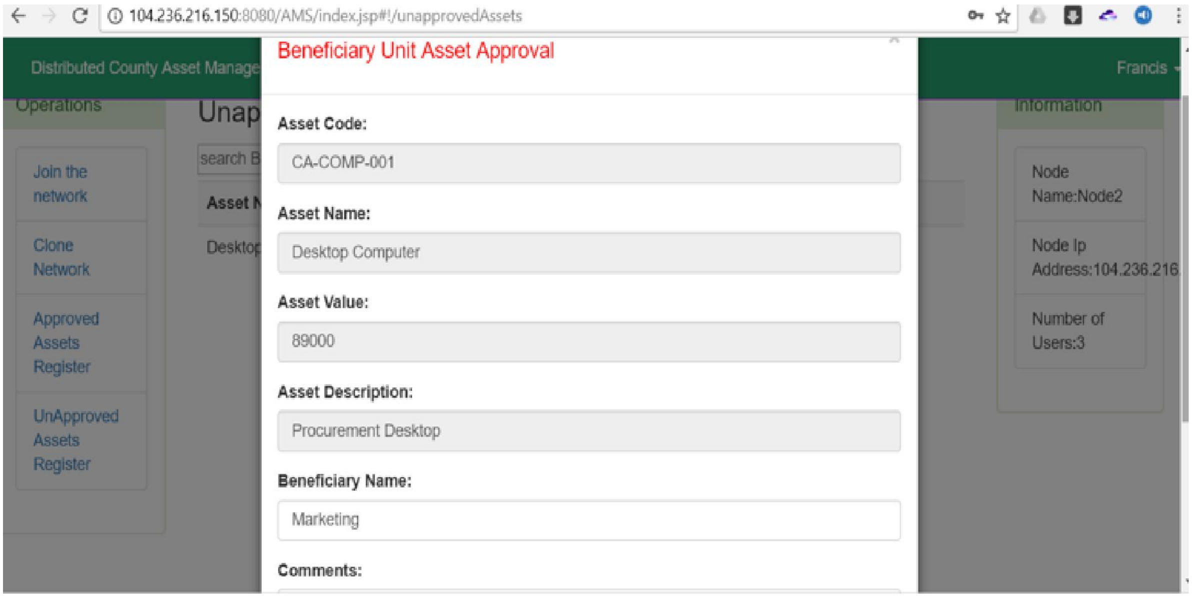
Node Name:Node2

Node Ip Address:104.236.216.15

Number of Users:3

Figure 13: Unapproved Assets Screen

Approval of an Asset


104.236.216.150:8080/AMS/index.jsp#!/unapprovedAssets
Distributed County Asset Manage
Francis
Operations
Join the network
Clone Network
Approved Assets Register
UnApproved Assets Register
Unap
search B
Asset N
Desktop
Information

Beneficiary Unit Asset Approval

Asset Code: CA-COMP-001

Asset Name: Desktop Computer

Asset Value: 89000

Asset Description: Procurement Desktop

Beneficiary Name: Marketing

Comments:

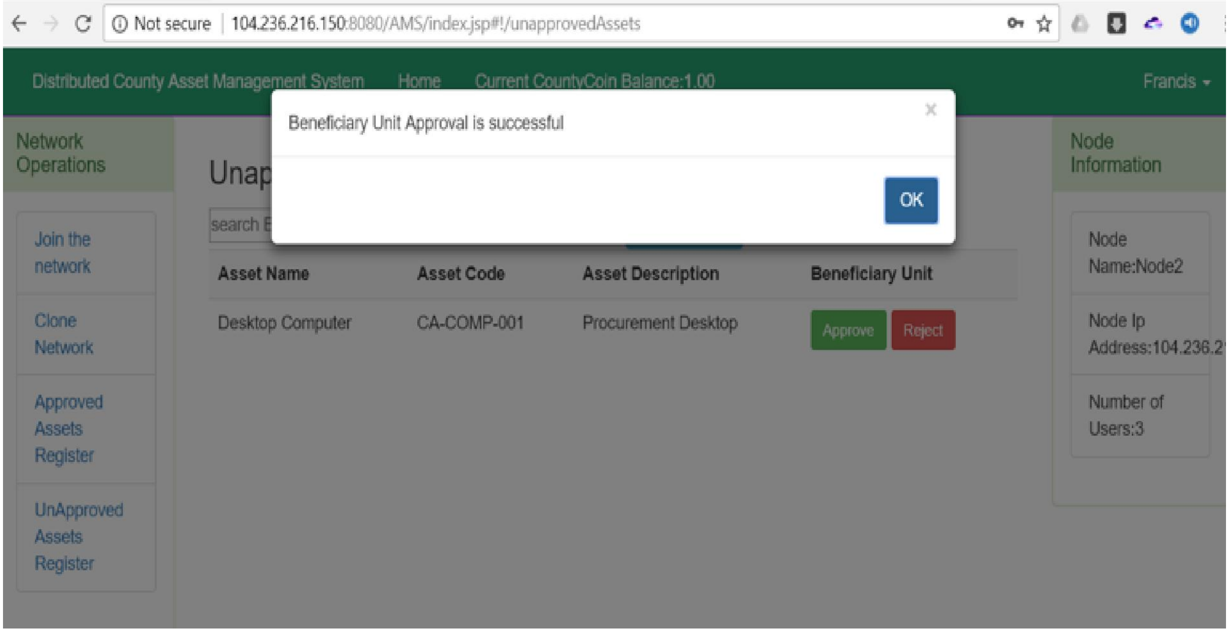
Node Name:Node2

Node Ip Address:104.236.216

Number of Users:3

Figure 14: Approval Asset Screen

Asset Approval Confirmation


Not secure | 104.236.216.150:8080/AMS/index.jsp#!/unapprovedAssets
Distributed County Asset Management System
Home
Current CountyCoin Balance:1.00
Francis
Network Operations
Join the network
Clone Network
Approved Assets Register
UnApproved Assets Register
Unap
search E
Node Information
OK

Beneficiary Unit Approval is successful

Asset Name	Asset Code	Asset Description	Beneficiary Unit
Desktop Computer	CA-COMP-001	Procurement Desktop	Approve Reject

Node Name:Node2

Node Ip Address:104.236.2

Number of Users:3

Figure 15: Asset approval confirmation screen

CHAPTER FIVE

DISCUSSION

5.1 Introduction

In this chapter the major system modules and procedures are reported with regard to their functionality and results obtained. This is given in section 5.2 as system functions, and finally as analysis of system sample results in section 5.3

5.2 System Functions

The project successfully analyzed, designed and developed an asset management system with bias on county governments in Kenya. In the system, the county governments can easily record existing assets, procure new assets without the worry of misappropriation of funds, track asset usage and disposal among other things. The general system functionality is outlined in the following sections.

Joining the Network

It is functionally possible for any user whether a county government employee or a miner to join the network through their respective nodes / computers. The four key administrative departments that are vital for the correct operation of this system are:

1. Procurement,
2. Finance,
3. Registry and
4. Audit

The authorized personnel in these departments assume the roles of their respective managers in the departments and must join the network by providing the following details:

1. Username
2. Password

Other interested members of the public may also join at free-will in which case they are paid some tokens for validating transactions based on their validation/computational power.

Cloning of New Nodes

For a node / user to participate in the network, the user must clone it by providing the following information:

1. Username
2. Password
3. IP Address of Cloning Node
4. IP Address of the Node to clone from

After this process, the node becomes part of the larger peer network and may be involved in transaction validation

Addition of New Assets

It is the role of the procurement department to initiate asset additional process upon which other validating departments must take charge and subsequently make validations based on their respective authorities. To add a new asset, the following information is required:

1. Asset code
2. Asset Name
3. Asset Description
4. Date Added

User Authentication

Any registered user must login into the system in order to use it by providing the following details:

1. Username
2. Password

Validation of Transactions

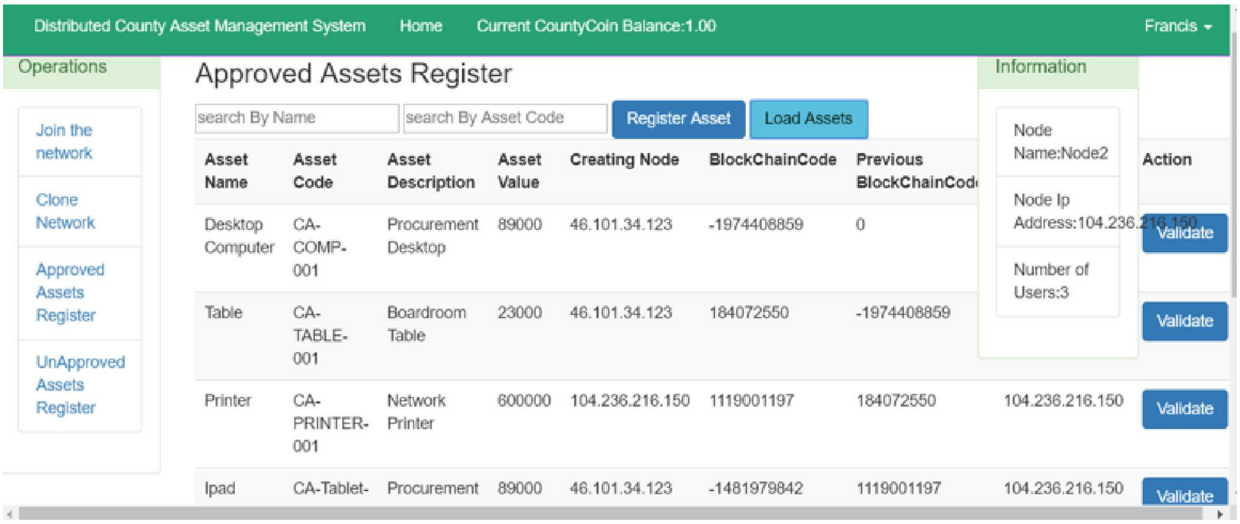
Any approved asset may be validated to ensure data integrity and consistency. This may be done by any of the four authorities namely: Procurement, Finance, Registry and Audit.

5.3 Results Analysis

In this section a selected number of results were subjected to further discussions with respect to the overall attainment of system objectives.

Approved Assets Register

The fundamental principle of ensuring the success of the study was to provision a distributed database that is both immutable and facilitates traceability. The output screen of approved assets on Figure 16 is evident that the assets blockchain-code of previous entry is captured. Any new entry holds a record of the previous item in the block through its blockchain-code. This facilitates traceability and accountability. Further, the blockchain-code algorithm ensures that the blockchain code number is unpredictable as seen from the ‘almost’ random blockchain-codes/hashes and any changes/manipulation of the database entries will always affect the hash output.



Approved Assets Register

Node Name:Node2

Node Ip Address:104.236.216.150

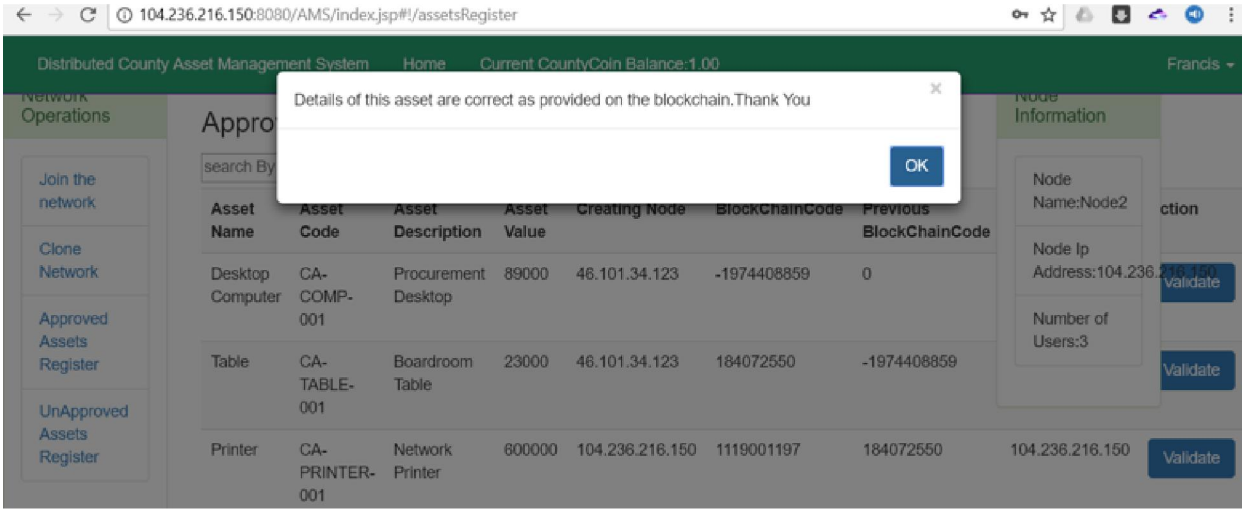
Number of Users:3

Asset Name	Asset Code	Asset Description	Asset Value	Creating Node	BlockChainCode	Previous BlockChainCod		Action
Desktop Computer	CA-COMP-001	Procurement Desktop	89000	46.101.34.123	-1974408859	0		Validate
Table	CA-TABLE-001	Boardroom Table	23000	46.101.34.123	184072550	-1974408859		Validate
Printer	CA-PRINTER-001	Network Printer	600000	104.236.216.150	1119001197	184072550	104.236.216.150	Validate
Ipad	CA-Tablet-	Procurement	89000	46.101.34.123	-1481979842	1119001197	104.236.216.150	Validate

Figure 16: Approved Assets register screen

Assets Record Validation

The asset validation output indicates that it is both possible to validate the integrity of records as well as to ascertain impossibility to violate data integrity without detection as seen from the error prompts in Figure 17.



104.236.216.150:8080/AMS/index.jsp#!/assetsRegister

Details of this asset are correct as provided on the blockchain.Thank You

Node Name:Node2

Node Ip Address:104.236.216.150

Number of Users:3

Asset Name	Asset Code	Asset Description	Asset Value	Creating Node	BlockChainCode	Previous BlockChainCode		Action
Desktop Computer	CA-COMP-001	Procurement Desktop	89000	46.101.34.123	-1974408859	0		Validate
Table	CA-TABLE-001	Boardroom Table	23000	46.101.34.123	184072550	-1974408859		Validate
Printer	CA-PRINTER-001	Network Printer	600000	104.236.216.150	1119001197	184072550	104.236.216.150	Validate

Figure 17: Asset record validation screen

CHAPTER SIX

CONCLUSIONS AND RECOMMENDATION

6.1 Introduction

Blockchain, as a distributed ledger technology, and its supported infrastructure of tokenized digital smart contracts – holds the key to unlock radical innovations in resource management by eliminating over-reliance on intermediaries, drive business efficiency, transparency and cost savings through an immutable and auditable public ledger. This thesis investigated how this novel technology could be used to address some of the issues that contribute to the inefficiency and lack of trust in the management of public assets. In particular, it focused on the design of a framework for mutual verification and validation of transactions. This chapter summarizes the main results of the thesis with respect to how the study objectives were met, the limitations that may have hindered their full realization, the lessons learned and presents future research directions.

6.2 Summary of results

In this research work, an application-specific exploration was carried out to test the possibility of applying the novel blockchain technology in public resource management and in particular the management of County Government Assets in Kenya. It was established that this wonderful technology – though still at its nascent stage, holds great promise in changing the way people traditionally understood and undertook resource management. Specifically, a trustless and immutable distributed asset management database was developed and tested for use in a County Government setup. If implemented in real environment, it holds the potential of extensively saving on running costs by eradicating the need for complicated administrative procedures as well as increase levels of security, integrity, trustworthiness and accountability of assets.

One unique feature in a blockchain system is a validator commonly known as a 'Miner'. Here, there is a great potential for government institutions to create synergies in protecting each other assets and related. Of particular interest are the Schools of Computing that have immense opportunities to provide computing facilities for verification and validation through hosting a repository (node/s), and; in the process of doing so, they get opportunity for income generation via recharging the tokens to county governments. This is just but to mention a few of great opportunities contained in this noble technology.

6.3 Open Issues

In this section we discuss some open issues in the applicability of blockchain technology in asset management. These open areas are temporarily anchored in the limited knowledge base in terms of existing frameworks and standards. Blockchain technology has emerged as a primary enabler for verification-driven transactions between parties that do not have complete trust among themselves. For instance, Bitcoin uses this technology to provide a provenance-driven verifiable ledger that is based on consensus among parties. Nevertheless, the use of blockchain as a transaction service in non-cryptocurrency applications, for example, business networks, is at a very nascent stage. Whereas the blockchain supports transactional provenance, the data management community and other scientific and industrial communities are assessing how blockchain can be used to enable certain key capabilities for business applications. In this regard, we identify a number of areas that remain open to researchers of blockchain technology: (1) leverage existing capabilities of mature data and information systems, (2) enhance data security and privacy assurances, (3) enable analytics services on blockchain as well as across off-chain data, and (4) make blockchain-based systems active-oriented and intelligent.

Other area of concern and of interest is in enhancing systems development tools and related libraries to easily support blockchain system development process. Of particular interest is the

DBMS tools being adopted in the development of a blockchain system. Blockchain concepts requires that the end result structure such as ledger or database must be "intelligent" i.e. knowing its own state to make it immutable. Implementing this remains an open space and much is required in research work and related creative thinking.

6.4 Future Work

Despite the great potential of blockchain in asset management, it faces a few challenges, which might limit its real system applicability in the near future. In line with this documented blockchain-based asset management framework, the following areas of improvements were identified:

1. Development of an area specific application system for actual deployment.
2. Further testing procedures with additional test cases and test data to explore all possible error loopholes.
3. Model unique mechanism of managing asset-aging feature where depreciation and subsequent removal is done via blockchain architecture – To manage retired asset categories. Due to immutability of the blockchain database, there is high possibility of depreciated assets to continue existing in the system infinitely. But currently, interminable assets like title-deeds, academic certificates, patents etcetera, are well catered for in this designed blockchain based system.

REFERENCES

Melanie Swan, (2015). Blockchain*: Blueprint for a new economy*

Mainelli M., Smith M., (2015). Journal of Sharing ledgers for sharing economies*, EY Global Financial Services Institute*, Volume 3 – Issue 3.

Mattila J., Seppälä T., Holmström J., (2011). Product-centric Information Management: A Case Study of a Shared Platform with Blockchain Technology, *Industry Studies Association Conference*, Minneapolis, USA.

Shepherd E., (2006). Why are records in the public sector organizational assets? *Records Management Journal*, Vol. 16 Issue: 1.

U.S. Department of Commerce, in consultation with National Economic Council, *The Competitiveness and Innovative Capacity of the United States:* Article: January 2012.

Nakamoto S., (2009). Bitcoin: A Peer-to-Peer Electronic Cash System. Retrieved from: “https://bitcoin.org/bitcoin.pdf”

Narayanan A., Bonneau J., Felten E., Miller A., Goldfeder S. (2016). Bitcoin and Cryptocurrency

Technologies*, Princeton University Press*.

Mohan Venkataraman, Murali Vridhachalam, Alex Rosen, and Brian Arthur, (2017). Adopting

Blockchain for enterprise asset management (EAM)

Guest Writer, (2017). Eight Practical Blockchain Use Cases for International Development

UNDP Annual Report 2014. An Integrated UNDP Support Programme for the Devolution Process in Kenya. Project No: 00083473

Transition to Devolved Government Act, (2016), National Council for Law Reporting. URL www.kenyalaw.org

APPENDICES

APPENDIX I: INTERVIEW TRANSCRIPTS

Interview Transcript - to County Government – Administration official (Meru County)

1. Q: In the year 2013, Meru County Government came to existence as defined by the new Kenyan constitution; what was the mode of recognizing of county assets that were being transferred from Municipal council?

   A: At first, it was managing chaos. Obvious things like building and land were easily recognizable but many of non-obvious items remained to be established.

2. Q: What would you say of the greatest challenge you faced come the year 2013 during the handover of Municipal assets to the new County Set up?

   A: Bulky records of assets with insufficient details of precision

3. Q: We can now count close to Five years since the transitioning begun, what can you say of success/failure rates?

   A: Asset management is a progressive agenda over time due to asset status changes. It can be quite hard to measure success/failure.

4. Q: You are also planning to transition to new County administration after elections; what challenge are you foreseeing or already manifesting in regard to County Assets management and related?

   A: Traceability and mishandling of assets cannot be ruled out due to political interference and political actors being already deep in asset management to some extent

5. Q: What are the differences of Municipal Asset management and new County Government Assets management? I know there are similarities, please mention as well.

   A: I think it one and the same… Challenges of recording is manifested in either

6. Q: How easy was it to verify and trace the local government assets and the related truth of status?

   A: This has remained a difficult undertaking especially in getting the true data of some Assets. But so much achievement so far as computerization processes continues.

7. Q: What was the missing connection in handling Asset management complexity?

   A: I can only mention that with proper digitalization, some unexplainable complexities can be handled

8. Q: Would you say that the current structure of County government assets management is sufficient to safeguard public assets?

   A: So much is required I would say…

9. Q: Where would you find faults in regard to assets documentation in a county set up?

   A: Main one being bulkiness of assets records and tracking

10. Q: What are the areas that remain gray/undefined in managing county assets?

    A: Quite many… But of particular, again digitalization should be foremost to bring reliability

11. Q: What is your forethought future management of county assets in relation to recording tracking and subsequent tracking?

    A: With proper digitalizing, so much can be achieved, that is my belief

APPENDIX II: SAMPLE ALGORITHMS

Asset Addition Algorithm

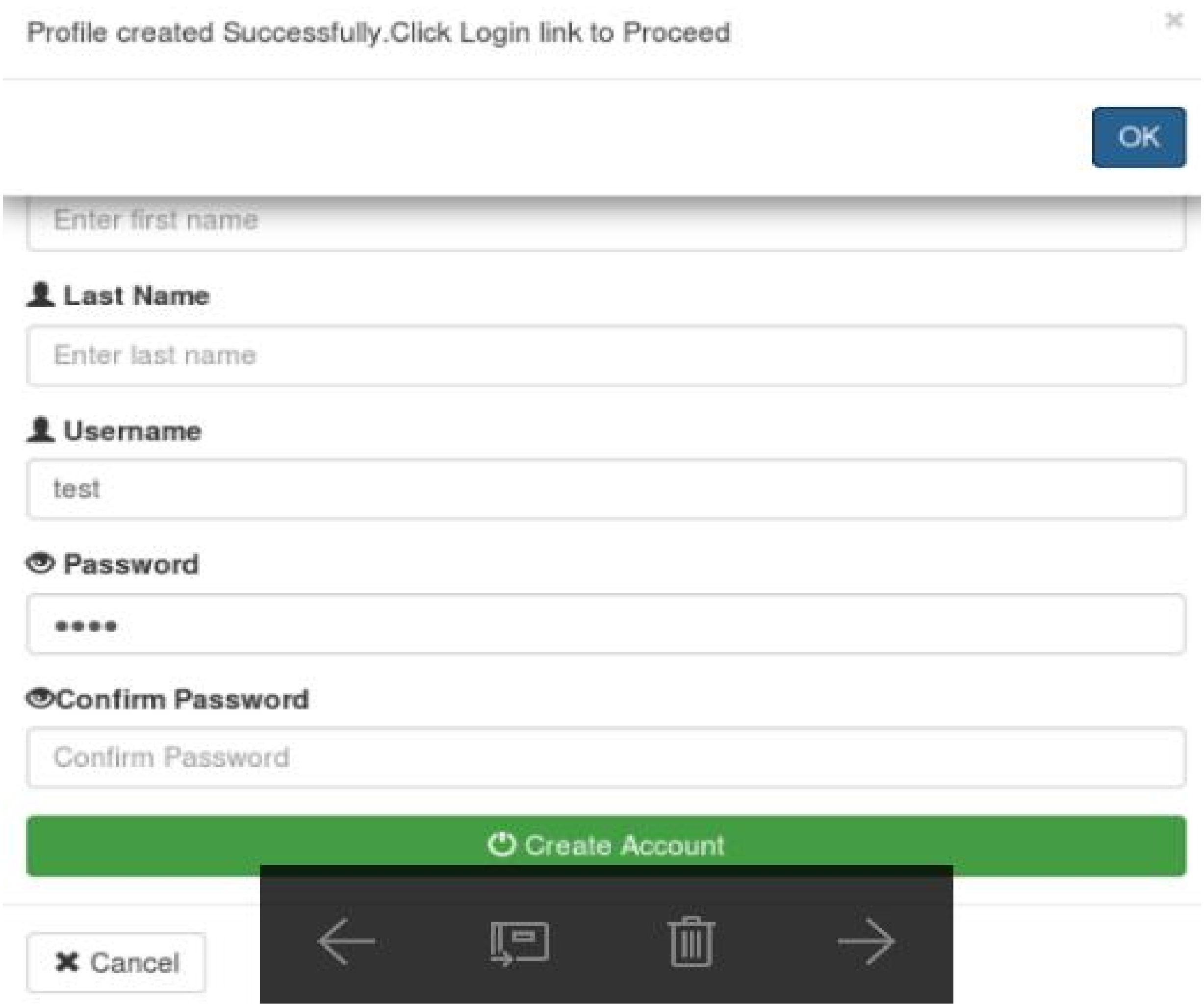
1. Begin
2. Provide the required asset details such as name, code, value.
3. From the blockchain network get hash of the latest approved asset (HASH1).
4. Generate a unique hash (HASH2) using details of the asset and HASH1.
5. HASH2 becomes the hash of the added asset.
6. The asset is relayed to the rest of the nodes for approval.
7. If all the nodes approve the asset then it joins the network, else it is rejected
8. End

Validation Algorithm

```
1. Begin
2. Using the existing details of an asset compute a hash(HASH1)
3. Compare HASH1 with the immutable hash in the database.
4. If there is a difference //it means that some details must have changed.
5. The system gives an alert message that the details might have been manipulated
6. else the details are okay
7. Upon validation of assets for some pre-defined length of time the miner is awarded
   tokens.
8. End
```

APPENDIX III: SAMPLE SYSTEM INTERFACES

Successful Account Creation



Profile created Successfully.Click Login link to Proceed

Enter first name

Last Name

Enter last name

Username

test

Password

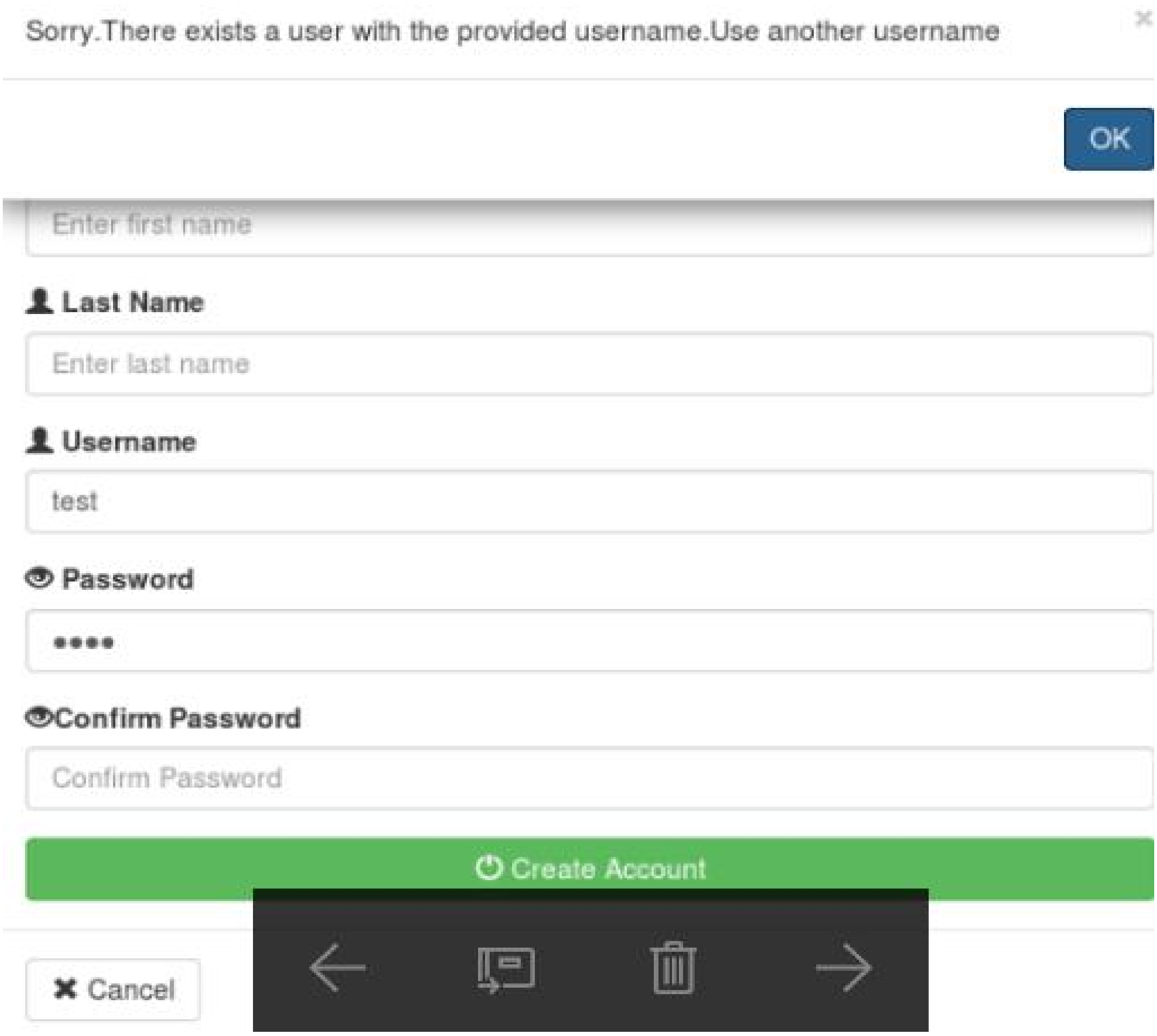
••••

Confirm Password

Confirm Password

Figure 18: Sample System interface – Successful Account creation

Unsuccessful Account Creation



Sorry.There exists a user with the provided username.Use another username

OK

Enter first name

Last Name

Enter last name

Username

test

Password

••••

Confirm Password

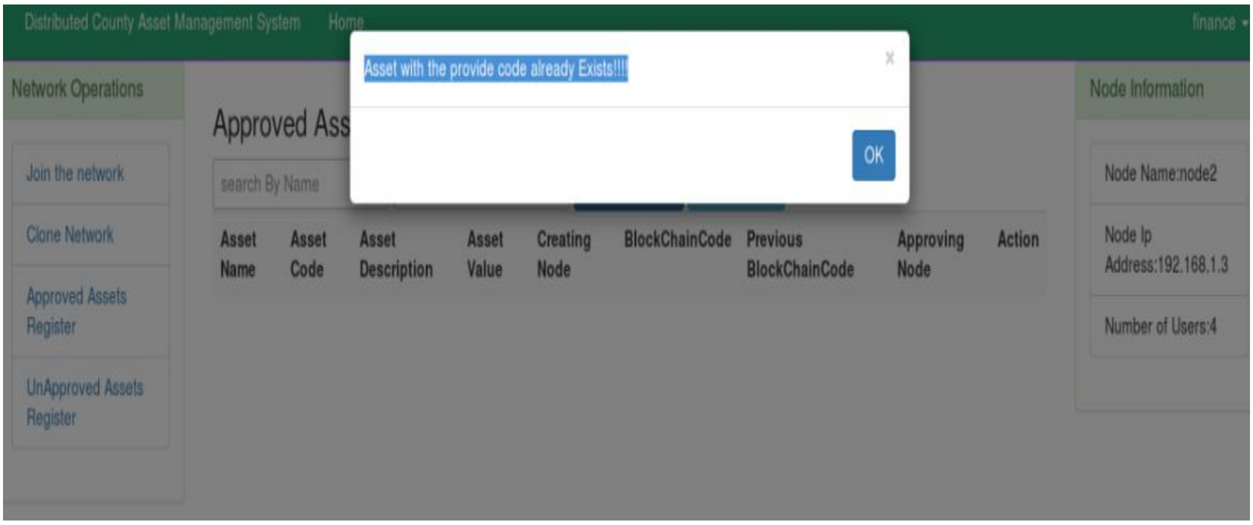
Confirm Password

Create Account

✖ Cancel

Figure 19: Sample System interface – Unsuccessful Account creation

Register Asset with Existing Code



Asset with the provide code already Exists!!!

Asset Name	Asset Code	Asset Description	Asset Value	Creating Node	BlockChainCode	Previous BlockChainCode	Approving Node	Action

Node Name:node2

Node Ip Address:192.168.1.3

Number of Users:4

Figure 20: Sample System interface – Validation test

APPENDIX IV: SAMPLE CODE LISTING

Sending Asset to Peer Node Code

```
String assetToPeer=JsonUtil.convertObjectsToJson(block);
        System.out.println(assetToPeer);
                    try {
                Client client = Client.create();
                WebResource webResource = client

Resource("http://"+currentNode.getCloneFrom()+":8080/AMS/api/nodeApi/receiveAssetForApproval
");
                //String input = "{\"singer\":\"Metallica\",\"title\":\"Fade To Black\"}";
                ClientResponse response1 = webResource.type("application/json")
                  .post(ClientResponse.class, assetToPeer);
                if (response.getStatus() != 200) {
                        throw new RuntimeException("Failed : HTTP error code : "
                           + response.getStatus());
                }
                System.out.println("Output from Server .... \n");
                String output = response1.getEntity(String.class);
                System.out.println(output);
        } catch (Exception e) {
                e.printStackTrace();
        }
```

Asset Validation Code

```
  @Override
  public String validateAsset(long id) {
        List<AssetBlock> blockList = em.createQuery("select b from AssetBlock b where b.id=
:id").setParameter("id", id).getResultList();
        if (blockList == null) {
            return null;
        } else {
            AssetBlock block = blockList.get(0);
            String[] assetProperties = {block.getAssetCode(), block.getAssetValue().toString(),
block.getAssetDescription()};
            Object[] contents = {Arrays.hashCode(assetProperties), block.getPreviousHashCode()};
            int calculatedHashCode = Arrays.hashCode(contents);
            if (block.getHashCode() == calculatedHashCode) {
                return "Details of this asset are correct as provided on the blockchain.Thank You";
            } else {

                return "Details of this asset are NOT CORRECT as provided on the blockchain.Kindly
contact any county asset manager and report this asset.Thank you.";
            }
        }
    }
```

User Code

```
    @Override
    public String validateAsset(long id) {
        List<AssetBlock> blockList = em.createQuery("select b from AssetBlock b where b.id=
:id").setParameter("id", id).getResultList();
        if (blockList == null) {
            return null;
```

```
  } else {
    AssetBlock block = blockList.get(0);
    String[] assetProperties = {block.getAssetCode(), block.getAssetValue().toString(), block.getAssetDescription()};
    Object[] contents = {Arrays.hashCode(assetProperties), block.getPreviousHashCode()};
    int calculatedHashCode = Arrays.hashCode(contents);
    if (block.getHashCode() == calculatedHashCode) {
      return "Details of this asset are correct as provided on the blockchain.Thank You";
    } else {
      return "Details of this asset are NOT CORRECT as provided on the blockchain.Kindly contact any county asset manager and report this asset.Thank you.";
    }
```