Cryptocurrency Payments Implementation Based on Blockchain Technologies in Addressing Covid-19 in Higher Learning Institutions

Chimuka Moonde, Jackson Phiri
Computer Science Department
University of Zambia
Lusaka, P.O. Box 32379, Zambia
2018248898@student.unza.zm, jackson.phiri@cs.unza.zm

Abstract

With regard to higher education institutions in Africa, it is undoubtedly ineffective, inconvenient, and time-consuming for students to pay student fees. In addition, the rise in the number of students studying in higher learning institutions has led to long frustrating queues and severe overcrowding in the majority of financial institutions when paying student fees. With the advent of Covid-19, the financial institutions and students do not have a favourable situation. This paper seeks to implement a cryptocurrency for higher education institutions. In this study, the proposed payment system was implemented using an object-oriented programming software development methodology.

Keywords
Universities, Blockchain, Blocks, Cryptography and Cryptocurrency.

1. INTRODUCTION

Payment systems have become a critical component of contemporary societies' economic existence. The smooth functioning of payment systems is important for the overall effectiveness and reliability of the payment systems (Payment system oversight and interoperability). The Digital Financial Services Ecosystem maps the overall ecosystem of Digital Financial Services by identifying all key stakeholders as well as looks at the critical elements necessary to make the ecosystem develop so that it encourages and enables financial inclusion policies (Benson et al, 2017).

Digital Financial Services (DFS) refers to accessing financial services through an electronic system or a mobile phone application. Digital Financial Infrastructure includes electronic financial systems, in which funds are deposited, making and receiving payments (Martin and Mauree, 2016). DFS has become a viable avenue for the financially excluded to access formal financial services. Users can safely receive funds, pay bills, make bank deposits, transfer funds, and buy products and services. Most convincing evidence suggests that growing access to formal financial services not only decreases financial exclusion but has also become an important development target to promote economic growth, improve welfare and minimize poverty (Martin and Mauree, 2016). As such, the recent growth of mobile money has allowed millions of financially excluded people to conduct financial transactions relatively cheaply, securely and reliably (Nandhi, 2012).

The education sector is one sector that can greatly benefit from the services provided by Digital Financial Services. In Africa most school systems rely heavily on cash transactions. This cash reliance on financial transactions contributes to inefficiencies, cash leakage and carries risks to security. Furthermore, cash handling can lead to the further spread of Covid-19 among students and different departments in the higher learning institutions that handle cash. Digital Financial Services can provide unique opportunities in educational institutions such as elementary and secondary schools and universities. These opportunities include replacing cash and thus making learning institutions more efficient by improving management, increasing financial support from donors and non-governmental organisations, reducing financial costs and providing a concrete way to develop more multifaceted systems that would otherwise be impossible in a cash environment (Braniff, 2017).

Looking at higher education institutions in Africa, there is no question that a new student fees payment system needs to be introduced. This is owing to existing ineffective, inconvenient and time wasteful student fee payment mechanism. Furthermore, the rise in the number of students studying in higher learning institutions has led to long frustrating queues and overcrowding in most financial institutions during payment of student fees. With the advent of Covid-19 such a situation is not favourable for both the financial institutions and the students. Therefore, the authors were compelled to implement a cryptocurrency.

2. LITERATURE REVIEW

Related systems and technologies were studied to learn how to solve common problems and to gain a better understanding of the solutions currently in place. Best practices in current systems were learnt, and shortcomings were noted in attempt resolve them in the proposed system. The following are similar operational systems that were studied.

2.1. M-Pesa

M-Pesa is a revolutionary unbanked-payment app. The Swahili word for cash is "Pesa" and the "M" is for mobile. At Safaricom dealers, customers turn cash into e-money, then follow instructions on their phones to make payments through their M-PESA account; the system makes money transfers like banks do. The account is very secure, PIN-protected, and supported by Safaricom and Vodafone Group providing 24/7 service. To implement M-Pesa, Vodafone had to marry the extremely divergent cultures of global telecommunications firms, banks and microfinance institutions – and satisfy their vast and frequently conflicting regulatory requirements (Hughes and Lonie, 2007).

Using preloaded data onto the SIM card, M-PESA uses an SMS-based interface to digitally pass money to other phones. A customer visits one of Safaricom 's agents to load money into one's virtual wallet, and trades currency for e-money, which is automatically deposited into their wallet. Customers are able to transfer money to anyone with a cell phone (Hinz, 2014).

2.2. PayPal

PayPal is one of the world's most common payment services. PayPal allows any business or individual to send and receive payments online, in-store or on mobile in a safe, easy and cost-effective manner. To create a decentralized, real-time payments solution, PayPal built on the current financial infrastructure of banks and credit card networks. PayPal enables consumers not to share financial information to send and receive money. To make a purchase, consumers need to enter their mobile number and PIN. PayPal essentially deducts the funds from whatever bank account or credit card, the consumer has linked his or her PayPal account. (Pandy and Crowe, 2017). At the core of the PayPal system lies the concept of a PayPal account. Using a PayPal account, a customer can store funds, send and receive funds. (Williams, 2007).

2.3. Google Wallet

Google Wallet allows users to store on a smartphone their debit cards, credit cards, gift cards and loyalty cards, turning the smartphone into a virtual wallet. Google also automatically redeems deals for the user at participating merchants. Furthermore, a consumer can make purchases online as well as make contactless payments or tap to pay with their mobile phone with the help of near field communication (NFC) (Ghag and Hegde, 2012).

Google Wallet stores encrypted user details on a chip in the mobile phone called the Secure Element. The Secure Element is separate from the mobile phone's operating system, hardware and memory and utilizes both hardware and access control. The chip is designed to only allow trusted programs running on the mobile phone to access the stored information (Ghag and Hegde, 2012).

Google Wallet can be thought of as a container for payment cards, gift cards, loyalty cards and special offers. It is an Android app with a user interface. The user interface is used for securing the wallet with a pass code, handling payment, gift and reward cards, choosing the currently active card, finding unique deals and showing the history of transactions. The secure element of the wallet serves to store sensitive payment, gift and reward card information and to communicate with established POS reader infrastructures (Roland et al, 2013).

2.4. Apple Pay

Apple Pay is a mobile payment system that enables iPhone users (iPhone 6 and higher) to pay for products and services using Touch ID. Opposed to entering or confirming payment card details (credit or debit card) any time a user makes a transaction; users can easily approve payment for items by pressing the iPhone's home button. A payment token stores all the details needed to process the payment from authorization to settlement. Payment card information never leaves the user's mobile phone during an Apple Pay transaction; this information is stored safely in the mobile phone (Huh, 2017).

To set up Apple Pay, users simply add a debit or credit card to the wallet app. The card details can be imported from iTunes, entered manually, or added by taking a picture of a card. After the card verification process, users can start using Apple Pay. Users need to hold their iPhone next to an NFC reader to tap-and-pay in stores. A default payment card can be pre-selected on the wallet app. Users then place a finger on Touch ID (fingerprint scanner) to authenticate and complete the payment process. The wallet app notifies users automatically of verified transactions (Bruce, 2016).

2.5. Samsung Pay

Samsung Pay is a method of making transactions through Samsung's new line of mobile devices. Samsung Pay enables customers to make easy and safe mobile payments at most retailer POS terminals. Taking advantage of a new proprietary technology called magnetic secure transmission (MST) and (NFC), Samsung Pay makes mobile payment more available to both merchants and customers. Samsung used a complex alphanumeric algorithm called tokenization. Furthermore, Samsung partnered with card providers such as Visa and MasterCard, and adopted the VTS (Visa Token Service) platform to move its ambitious project forward. When a user adds a card to their Samsung Pay, a new "virtual random" CC (a new card number with some parameters) is created which implements the mechanism that assigns a token to each card. The token is saved in a token vault related to the original PAN records. Therefore, the mobile device sends a tokenized number in each transaction, instead of using the original CC data (Mendoza, 2016). Card number (PAN) and CVC (card authentication code) are substituted with tokens instead of the actual PAN and CVC. The purpose is to avoid the actual card number from being sent over the internet and subsequently stored in intermediate servers (European Union Agency for Cybersecurity, 2016).

Samsung Pay works with conventional point-of-sale (POS) devices that require magnetic card swipes to be used. The key technology that gives such a superior role to Samsung Pay is called MST. Under this technology, devices that use the Samsung Pay app will produce a magnetic signal containing the same payment information produced by swiping a magnetic card in the POS card reader. Thus, the POS system can recognize the Samsung Pay signal when the mobile device is near enough, even if nothing is swiped on the card reader (Choi and Lee, 2016).

2.6. Blockchain

Relevant literature and documentation were reviewed to gain a better understanding. The following are some of the literature reviewed;

Blockchain is the fundamental technology underlying Bitcoin and other cryptocurrencies (Nguyen, 2016). Blockchain is a distributed ledger system that utilizes a network consensus for documenting and executing transactions. Blockchain has recently gained broader attention as growing numbers of business leaders realize that this disruptive architecture's underlying technology can be applied to almost any sector. The most distinguishing attribute of blockchain is that no single agent has the ability to exercise control over the system activity (Collins, 2016).

The blockchain protocol operates on top of the internet, as a peer-to-peer (P2P) network of computers known as nodes. All nodes retain an identical copy of the transaction’s ledger. The blockchain ensures integrity and security as it is built on a system of distributed consensus system (Memon et al., 2018).

The concept of blockchain originated from two individuals: Stuart Haber and W.Scott Stornetta. They did not actually coin or introduce the word “blockchain". Haber and Stornetta (1991) outlined the principles of what is now called the Blockchain. The following outlines the inherent attributes of blockchain that were fundamental in the implementation of the proposed system;

1. Decentralization. Unlike the centralized architecture that poses many problems including single point of failure and scalability, the blockchain uses a decentralized and distributed ledger to utilize the computing capacities of all participating nodes of the blockchain network, reducing latency and eliminating the single point of fault (Atlam and Wills, 2019). Furthermore, in conventional centralized transaction systems, each transaction needs to be

validated through a central trusted entity such as the central bank. In comparison, a transaction in the blockchain network can be conducted between any two peers (P2P) without the authentication by a central trusted entity (Zheng et al., 2018)
2. Immutability. One of the blockchain's key attribute is the ability to create immutable ledgers so as to ensure the integrity of transactions. Databases may be altered in conventional centralized environments and trust with a third party needs to be established to ensure the integrity of the information. While in blockchain technology, as each block in the distributed ledger relates to the previous block that forms a chain of blocks, the blocks are permanently saved and unchanged as long as the participating node maintains the network (Atlam and Wills, 2019).
3. Security. Blockchain offers greater security since it uses public key cryptography that protects data from malicious actions such as eavesdropping and modification of data at rest or in transit. The blockchain network's participating users put their confidence in the integrity and security features of the consensus mechanism. (Atlam and Wills, 2019).

Since the introduction of public-key cryptography by Diffie and Hellman in 1976, there has been information about the potential for using the discrete logarithm problem in public-key cryptosystems. Although the discrete logarithm problem as first used by Diffie and Hellman was explicitly defined as the issue of finding logarithms in relation to a generator in the multiplicative group of the integer modulo a prime, this definition can be generalized to arbitrary groups, and in particular to elliptic curve groups. The resulting public-key systems offer relatively small block size, high speed and high security. Koblitz et al., (2000) performed an enquiry to investigate the development of elliptic curve cryptosystems from the discovery of Koblitz and Miller in 1985 to current implementation.

3. METHODOLOGY

In this study, the authors adopted an object-oriented software development methodology. It is a design strategy where system designers think in terms of 'things' or real-life objects instead of operations or functions. The object-oriented development methodology ensures that the system being developed is refined and transformed through phases of analysis, design, code and testing. (Hevner, 1992). The object-oriented software development life cycle is an iterative process that has five key phases. The following outlines some of the key phases used in this study;

3.1. Requirement Specification

This is an iterative process which involves communication between stakeholders and project team. In this study, main stakeholders included accountants and students from higher institutions of learning. The authors held discussions with stakeholders to gather the desired system features and better understand their day-to-day processes (Maciaszek, 2007).

The following list highlights the functional requirements for the proposed system;

1. A user should be able to view his/her current balance, private and public keys.
2. A user should be able to input necessary information in order to perform a transaction.
3. A user should be able to view payment information before committing a transaction.
4. A user should be able to sign his/her transaction before committing the transaction to the blockchain.
5. A user should be able to receive feedback that relates to the transaction.
6. A user should be able to send funds from his/her wallet to another wallet.
7. A user should be able to view his/her transaction history.

3.2. Design Specification

The design specification provides a description of the design that will help to realize the specified or identified requirements of the proposed cryptocurrency system. It is a brief description of how the system will meet the user's expectations. It is the bridge between requirements and the implementation that satisfies those requirements (Maciaszek, 2007).

3.2.1. Use Case Diagrams

Use case diagrams are a precursor to use case specifications that capture the overall functionality of a software system at very high-level. As outlined in Figure 1, Use case diagrams often serve as a summary of all use cases in a software system.

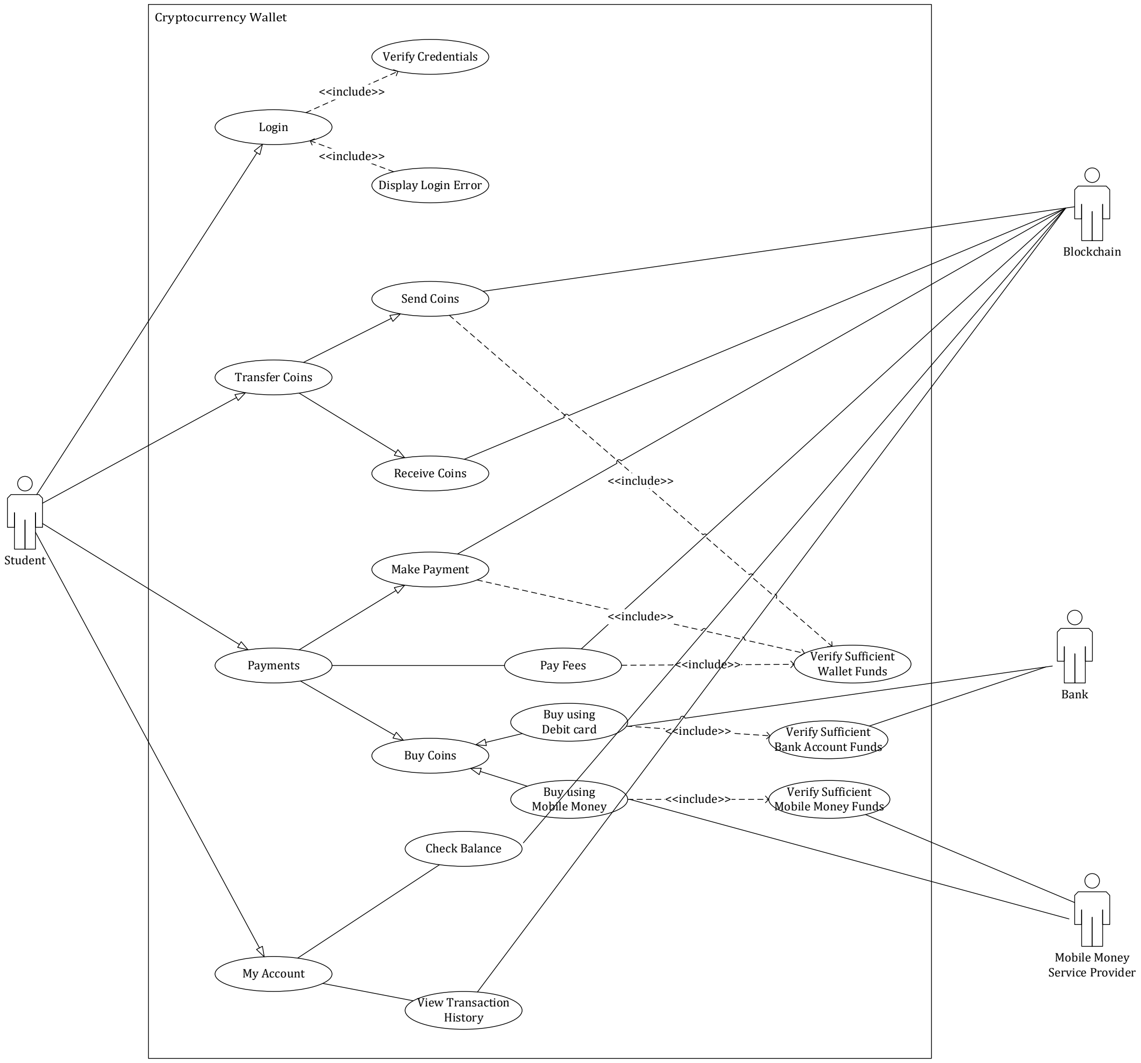


Figure 1. Use Case diagram

3.2.2. Class Diagram

Class diagrams model the type of objects in the system, along with the relationships among them. Figure 2 displays the class diagram for the proposed system. Class diagrams are the most widely-used structural models, showing a static view of the system.

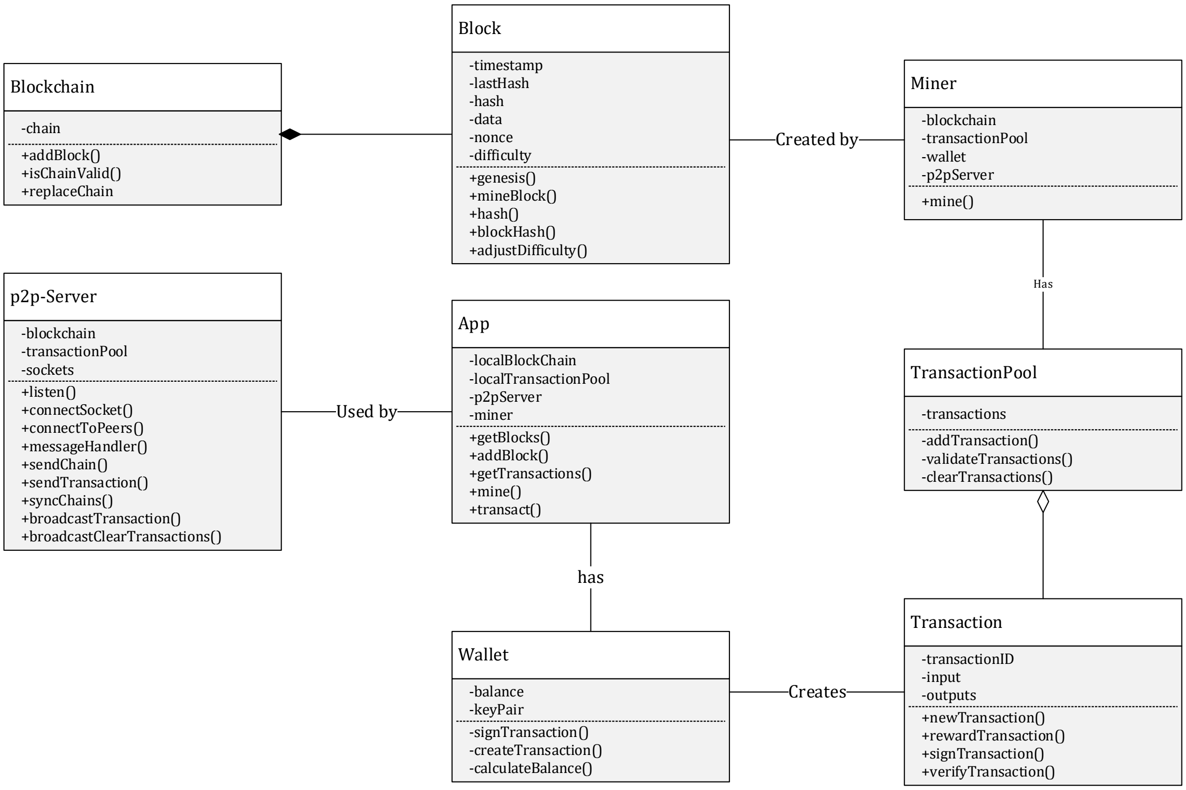


Figure 2. Class diagram

3.3. Implementation

Fundamental in the implementation of the proposed cryptocurrency system was the use of elliptic curve public-key encryption and signature scheme. Cryptography is the transformation of plain text into a different form that secure and immune from intruders. Elliptic curve cryptography is an independently developed public-key cryptography by Victor Miller and Neal Koblitz (Singh and Singh, 2015). As outlined by Hankerson et al., (2004), this study will make use of the following equations;

In Elliptic Curve Cryptography, this study adopted the curve equation of the form;

$$y^2 = x^3 + ax + b \qquad (1)$$

Generation of the key pair was achieved by utilizing equation 2.

$$\langle P \rangle = \{\infty, P, 2P, 3P, \dots, (n-1)P\} \qquad (2)$$

Let E describe the elliptic curve over a finite field F_p. Let P be a point in $E(F_p)$ and assume P has prime order n. The cyclic subgroup of $E(F_p)$ generated by P is Equation 2.

where prime p, the elliptic curve E equation and the point P and its order n, are parameters of the public domain. A private key is an integer d that is generated uniformly at random from the interval [1, n-1] and the related public key is $Q = dP$

Elliptic curve key pair generation was achieved by using the following algorithm;
INPUT: Elliptic curve domain parameters (p, E, P, n).
OUTPUT: Public key Q and private key d.

1. Select $d \in_R [1, n-1]$.
2. Compute $Q = dP$.
3. Return (Q, d).

Encryption of transactional data was achieved by using the following algorithm;

```
INPUT: Plain transactional data denoted as $m$, public key $Q$ and domain parameters ($p$, $E$, $P$, $n$).
OUTPUT: Ciphertext ($C_1$, $C_2$).
    1. Represent the plain transactional data $m$ as a point $M$ in $E(\mathbb{F}_p)$.
    2. Select $k \in_R [1, n-1]$.
    3. Compute $C_1 = kP$.
    4. Compute $C_2 = M + kQ$.
    5. Return ($C_1$, $C_2$).
    6. Transmit $C_1$ and $C_2$
```

Plain transactional data denoted m is first represented as point M, then encrypted by adding it to kQ where k is a randomly selected integer and Q is the public key of the intended recipient of the plain transactional data. The sender transmits the points $C_1 = kP$ and $C_2 = M + kQ$ to the recipient.

Decryption of transactional data was achieved by utilizing the following algorithm;

```
INPUT: Ciphertext ($C_1$, $C_2$), private key $d$, and elliptic curve domain parameters ($p$, $E$, $P$, $n$).
OUT: Plain transactional data denoted as $m$.
    1. Compute $dC_1 = d(kP) = k(dP) = kQ$.
    2. Compute $M = C_2 - dC_1$.
    3. Extract $m$ from $M$.
    4. Return ($m$).
```

The recipient uses his/her private key d to compute $dC_1 = d(kP) = k(dP) = kQ$ and thereafter recovers $M = C_2 - dC_1$

A prototype of the proposed cryptocurrency system was implemented based on the design specification. Implementation is realization of the proposed cryptocurrency system with the blockchain serving as the underlying technology. Implementation is the process of translating design specification to an executable program. The authors implemented the cryptocurrency system using the following programming language and tools;

a) Python version 3.8.
b) JSON.
c) PyCharm version 2019.3.4.
d) Postman version 7.31.1.
e) GitHub.

3.3.1. Blockchain API

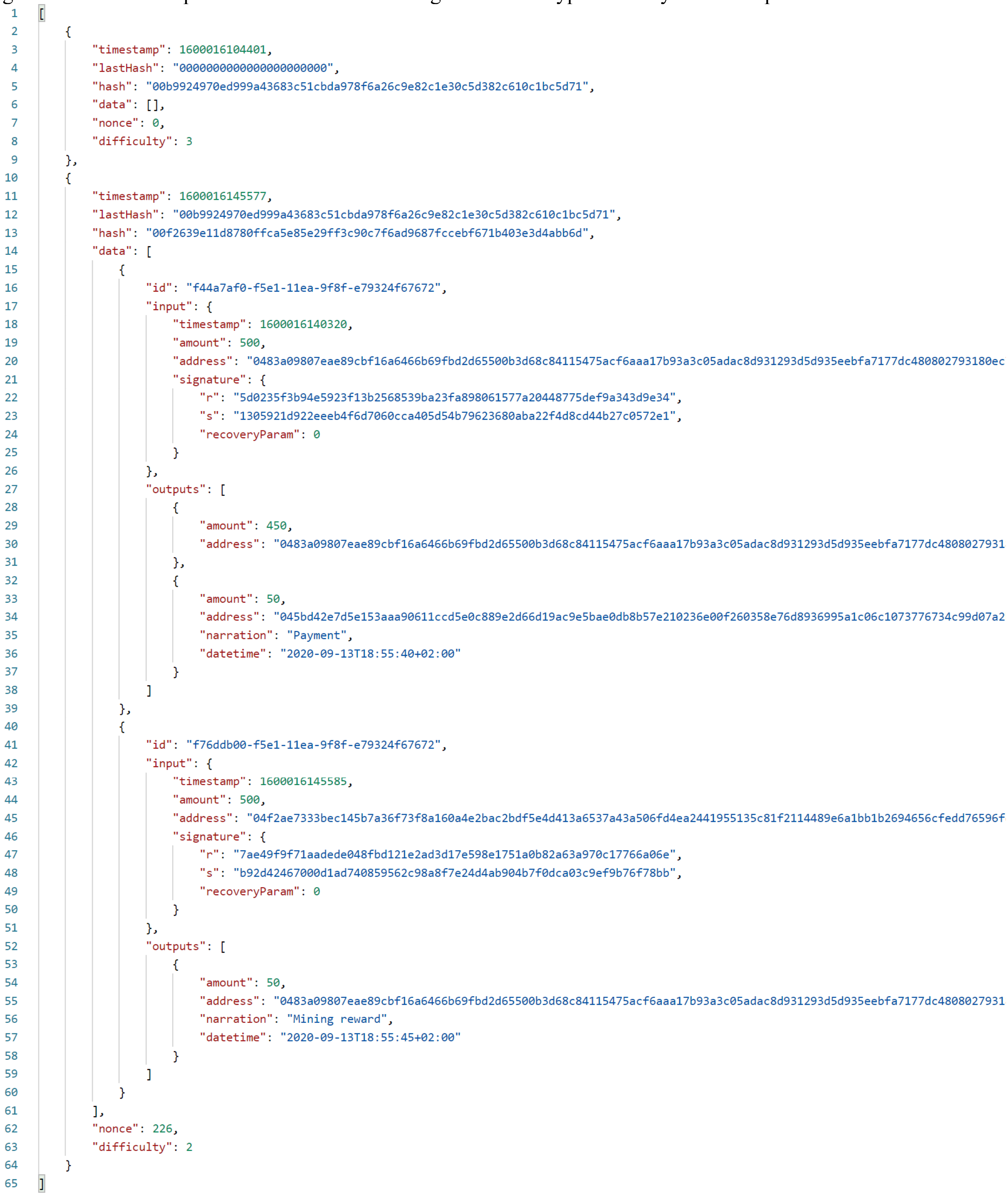
The authors implemented a RESTful API using flask, which is a web application development microframework. The researchers used Python as the programming language, to implement the API, while PyCharm was the development tool the authors used to build the API. The API used JSON as the data-interchange format. The authors used Postman to test the API during development. Furthermore, they used Postman to view the various responses from the endpoints of the API. The inherent characteristics of blockchain were implemented at the core of the API. The API was hosted on Ubuntu 18.04 LTS powered virtual server provisioned from Amazon Web Services.

3.3.2. Code Versioning

The researchers used GitHub as a code version and backup tool while developing the cryptocurrency system. They created a series of two private repositories to store each component of the software system.

4. RESULTS

Figure 3 shows the output obtained from consuming one of the cryptocurrency's API endpoints.



```
[
    {
        "timestamp": 1600016104401,
        "lastHash": "0000000000000000000000",
        "hash": "00b9924970ed999a43683c51cbda978f6a26c9e82c1e30c5d382c610c1bc5d71",
        "data": [],
        "nonce": 0,
        "difficulty": 3
    },
    {
        "timestamp": 1600016145577,
        "lastHash": "00b9924970ed999a43683c51cbda978f6a26c9e82c1e30c5d382c610c1bc5d71",
        "hash": "00f2639e11d8780ffca5e85e29ff3c90c7f6ad9687fccebf671b403e3d4abb6d",
        "data": [
            {
                "id": "f44a7af0-f5e1-11ea-9f8f-e79324f67672",
                "input": {
                    "timestamp": 1600016140320,
                    "amount": 500,
                    "address": "0483a09807eae89cbf16a6466b69fbd2d65500b3d68c84115475acf6aaa17b93a3c05adac8d931293d5d935eebfa7177dc480802793180ec
                    "signature": {
                        "r": "5d0235f3b94e5923f13b2568539ba23fa898061577a20448775def9a343d9e34",
                        "s": "1305921d922eeeb4f6d7060cca405d54b79623680aba22f4d8cd44b27c0572e1",
                        "recoveryParam": 0
                    }
                },
                "outputs": [
                    {
                        "amount": 450,
                        "address": "0483a09807eae89cbf16a6466b69fbd2d65500b3d68c84115475acf6aaa17b93a3c05adac8d931293d5d935eebfa7177dc4808027931
                    },
                    {
                        "amount": 50,
                        "address": "045bd42e7d5e153aaa90611ccd5e0c889e2d66d19ac9e5bae0db8b57e210236e00f260358e76d8936995a1c06c1073776734c99d07a2
                        "narration": "Payment",
                        "datetime": "2020-09-13T18:55:40+02:00"
                    }
                ]
            },
            {
                "id": "f76ddb00-f5e1-11ea-9f8f-e79324f67672",
                "input": {
                    "timestamp": 1600016145585,
                    "amount": 500,
                    "address": "04f2ae7333bec145b7a36f73f8a160a4e2bac2bdf5e4d413a6537a43a506fd4ea2441955135c81f2114489e6a1bb1b2694656cfedd76596f
                    "signature": {
                        "r": "7ae49f9f71aadede048fbd121e2ad3d17e598e1751a0b82a63a970c17766a06e",
                        "s": "b92d42467000d1ad740859562c98a8f7e24d4ab904b7f0dca03c9ef9b76f78bb",
                        "recoveryParam": 0
                    }
                },
                "outputs": [
                    {
                        "amount": 50,
                        "address": "0483a09807eae89cbf16a6466b69fbd2d65500b3d68c84115475acf6aaa17b93a3c05adac8d931293d5d935eebfa7177dc4808027931
                        "narration": "Mining reward",
                        "datetime": "2020-09-13T18:55:45+02:00"
                    }
                ]
            }
        ],
        "nonce": 226,
        "difficulty": 2
    }
]
```

Figure 3. RESTful API Output

The proposed cryptocurrency's blockchain consists of multiple blocks of data chained together like the links of a physical chain. The blocks are linked and secured using cryptography.

The first block in the cryptocurrency's blockchain is called the genesis block. This is the block created after the blockchain is initialized.

Block one contains the following;

- Meta data: nonce, timestamp and difficulty.
- It doesn't have a previous or last hash and this is the only block in the cryptocurrency that won't have a last hash. Conventionally the last hash for the genesis Block is represented with all zeros.
- Its own hash.
- Some data.

Block two proceeds the genesis block and contains the following;

- Meta data: nonce, timestamp and difficulty.
- The last hash. The last hash of block number two is identical to the hash for block number one and that is where the link comes. That is why a blockchain is called a chain or a blockchain because the blocks are cryptographically linked with each other through the hashes.
- Its own hash. This hash is generated based on the block's meta data and data to store.
- Data to store.

The concept of exchanging currency is expressed through objects called transactions. Transactions are the objects that capture the details behind the exchange of currency between two individuals in the cryptocurrency.

Transactions consist of two primary components as illustrated in Figure 3. Firstly, the input of a transaction provides details about the original sender. Input details include a timestamp, balance of the sender as well as the signature of the sender of the transactional data. In addition, details include the sender's public key denoted as address in the input object in Figure 3. Secondly, the transaction consists of output objects. Output objects include details such amount, narration, date time and recipient public key denoted as address in the output object.

5. DISCUSSION

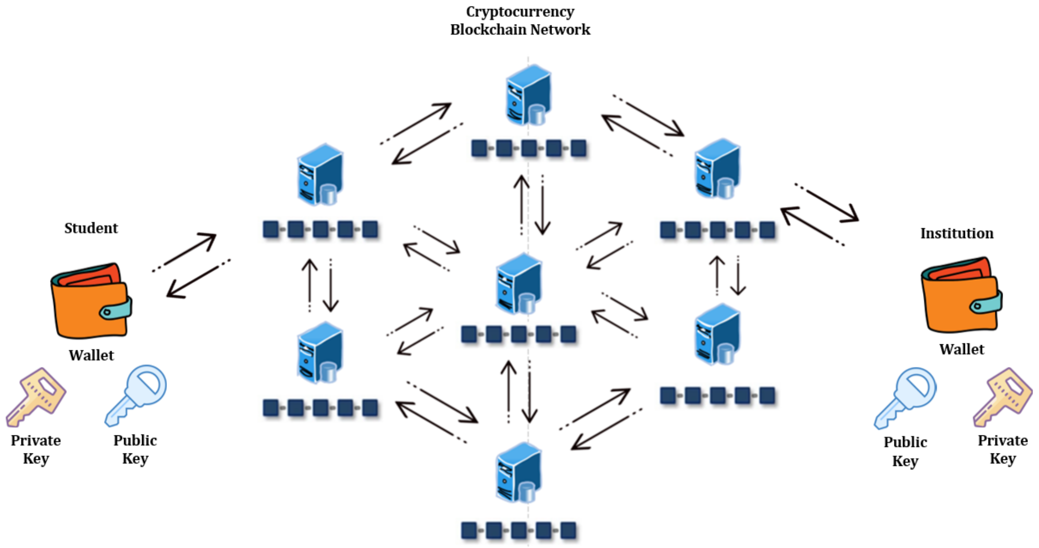


Figure 4. System Architecture

As shown in Figure 4, the cryptocurrency's blockchain is spread over a network of computers, each containing a local copy of the entire blockchain. Decisions on the network are made according to a majority consensus or consensus protocol. Owing to the lack of a central authority, the census protocol creates an irrefutable system of agreement between various nodes across the distributed network. Each node modifies its local copy of the blockchain to ensure it stays in sync with the majority of the network nodes.

According to Nakamoto (2008) cryptocurrency itself is a digital medium of exchange. It has three main features which include blockchain, wallets and mining as outlined below;

5.1. Blockchain

Cryptocurrency leverages the blockchain. It does so in order to keep a database of transactions. a cryptocurrency uses cryptography to add a layer of security to the blockchain. Blockchain is the underlying technology and data structure of the cryptocurrency. As a ledger, the blockchain serves the purpose of storing transactional data. The immutable ledger is used to refer to blockchains to describe the way in which blocks cannot be changed after they are recorded. Therefore, the blockchain is a ledger additionally, it is a distributed ledger. Ledgers do more than just document financial transactions. Ledgers also confirm ownership, confirm identity and status. A ledger consists simply of data structured by rules. Any time a consensus about facts is needed, we use a ledger.

5.2. Wallet

Like a physical wallet, the student's cryptocurrency wallet will help a student track how much cryptocurrency is entitled to them. The wallet will store the balance of the student. In addition, the student's cryptocurrency wallet is closely connected to the concept of private and public key as well as transaction objects. These keys are vital as they serve two primary purposes. Firstly, the private key is used to generate unique digital signatures. For very exchange of currency between the student and the institution, the private key allows the student to generate a unique digital signature to sign the exchange. A student is required to sign the exchange to make the transaction official. Secondly, the student's public key can be used by the institution to verify the student's signature. The public key of a wallet allows other nodes or individuals in the cryptocurrency blockchain network to verify digital signature generated by the wallet's private key. The private and public key pair is generated in such a way that a combination of the signature and the public key can only be deemed valid of in fact the signature was generated by the wallet's private key. The private key must be kept confidential, while the public key can be made widely available. The institution will decrypt the data presented by the signature using the student's public key. If the decrypted data does not match the proposed data, the signature is then deemed invalid. Likewise, if the decrypted data does match the proposed data the signature is valid. It is required that the signature should undergo a verification to check if the underlying transactional data is sent by the supposedly student in order to prevent fraud in the system.

The digital signatures are like unique handwritten signatures, but with far more inherent security. Using digital signatures in cryptocurrency solves the impersonation and tampering problem. Every person who wants to record a transaction in the cryptocurrency's blockchain must stamp transactional data with a unique digital signature.

5.3. Mining

Blockchain mining includes adding transactions to the current blockchain transactions ledger distributed to all blockchain nodes. Although mining is mainly related to Bitcoin, other technologies that use a blockchain also employ mining. Mining involves making a hash of a block that contains data such transactions that cannot be replicated easily, preserving the integrity of the whole network without the need for a central system. Through mining, nodes called miners do the work of adding transactions to the blockchain.

When individuals through wallets submit transactions to the cryptocurrency blockchain network, it takes a little time for those transactions to be validated and added to the blockchain. Transactions are temporarily "unconfirmed". Unconfirmed transactions are transactions that have been sent to the network but not included in the blockchain.

Miners will take a group of these unconfirmed transactions, include them within a block and later add that block to the blockchain. The actual act of mining is accomplished by solving a computational puzzle known as the proof-of-work algorithm. The proof-of-work algorithm is complex mathematical puzzle that is part of the blockchain. Miners include transactions in blocks by solving a proof-of-work algorithm. The proof-of-work algorithm is difficult to solve and computationally expensive. There is a low probability of randomly solving this puzzle. It takes a lot of trial and error to find the solution to the proof-of-work algorithm, which is time consuming and computationally expensive which is why it's called mining.

Once a miner solves the proof-of-work algorithm, the miner gains the authority to submit a valid block containing the transactions to the blockchain. When a miner submits a proof-of-work solution, the solution is tested by other miners in the network. The proof of work algorithm is easily verifiable once another miner has presented the solution. With the agreed upon verification, miners in the network can include a block of transactions to the blockchain.

The complex mathematical puzzle that needs to be solved is to find a number that generates a result that is within a certain range when combined with the meta data and data to be stored in the block and passed through a hash function. This number is called a "nonce" which is a concatenation of "number used once." By random guessing, miners find the nonce. The hash function prevents estimation of what the output will be. Miners guess the mystery nonce value and apply the hash function to the combination of the guessed number and the block data. The resulting hash must begin with a pre-established number of zeroes. There is no way to predict which number will work, as two consecutive integers will yield wildly unpredictable results.

The miner earns some cryptocurrency as compensation for solving the computationally costly proof-of-work algorithm. Miners are actively attempting to mine new blocks in hopes of receiving this currency pay-out, which offers a mechanism for adding transactions to the blockchain.

Mining also gives the cryptocurrency control over the rate of which new blocks are added to the cryptocurrency blockchain and how many transactions come in at once. The difficulty of the proof-of-work algorithm can be adjusted to control the rate of new blocks added to the blockchain.

6. CONCLUSION

The goal of this study was to implement a cryptocurrency for Africa's higher learning institution. The proposal to implement a cryptocurrency as compared to the cash environment was propelled by the realization of how paying of fees by students is undeniably inefficient, costly and time-consuming. Moreover, the growth in the number of students studying in higher educational institutions which always results in long stressful queues and extreme overcrowding in most financial institutions when paying student fees. With the introduction of Covid-19, the situation for financial institutions and students is not favourable. Students are to use the proposed payment system to pay tuition fees and other student fees to their respective higher educational institution. In addition, students are to use the proposed payment to pay for goods and services provided by the institution and other merchants in the institution's premises. This would evidently reduce and to some extent eliminate cash handling by students, financial and education institution. This study was restricted by the lack of design and creation of a mobile application based on iOS or Android that would allow students to communicate with the blockchain. In order to promote interoperability between the proposed system and telecommunications firms, banks and microfinance institutions, a field for further studies would include the design and implementation of a RESTful API.

REFERENCES

Atlam, H.F., and Wills, G.B., Chapter One - Technical aspects of blockchain and IoT. *Role of Blockchain Technology in IoT Applications,* vol. 115, pp. 1 – 39, 2019.

Benson, C.C., Niehaus C., Mashayekhi, M., Clotteau, N., Zimmer, T., Antunes, B., Grin Y., Potgieser, P., Nguyen, Q., Wright, G., Feingold, N., Sathnur, A., Bosini, J., Leach, J., Smirnova, O., Bondarenko, E., *The Digital Financial Services Ecosystem.* ITU-T Focus Group On Digital Financial Services, 2016.

Benson, C.C., Niehaus C., Mashayekhi, M., Clotteau, N., Zimmer, T., Antunes, B., Grin Y., Potgieser, P., Nguyen, Q., Wright, G., Feingold, N., Sathnur, A., Bosini, J., Leach, J., Smirnova, O., Bondarenko, E., *Financial Inclusion,* ITU-T Focus Group On Digital Financial Services*,* 2017.

Braniff, L., Schools in Africa aren't taking advantage of mobile money – Why?. https://www.cgap.org/blog/schools-africa-arent-taking-advantage-mobile-money-why , 2017.Accessed Day: August 23, 2020.

Bruce, E., *Apple Pay Essentials.* Packt Publishing, 2016.

Choi, D., and Lee, Y., Eavesdropping One-Time Tokens Over Magnetic Secure Transmission in Samsung Pay. *10th USENIX Workshop on Offensive Technologies (WOOT 16).* USENIX Association, 2016.

Collins,R.,*Blockchain-A-New-Architecture-for-Digital-Content*, http://www.econtentmag.com/Articles/Editorial/Commentary/Blockchain-A-New-Architecture-for-Digital-Content-114161.htm, Accessed on August 1, 2020.

European Union Agency for Cybersecurity, *Security of Mobile Payments and Digital Wallets.* European Union Agency for Network and Information Security, 2016.

Ghag, O., and Hegde, S., A Comprehensive Study of Google Wallet as an NFC Application. *International Journal of Computer Applications,* vol. 58, no.16, pp. 37-42, 2012.

Haber, S., and Stornetta, W.S., How to Time-Stamp a Digital Document. *Journal of Cryptology,* vol. 3, no. 2, pp. 99-111, 1991.

Hankerson, D., Menezes, A.J., and Vanstone, S., *Guide to Elliptic Curve Cryptography.* Springer, 2004.

Hevner, A.R.,Object-Oriented System Development Methods. *Advances in Computers,* vol. 35, pp. 135-198, 1992.

Hinz, M., M-PESA: The Best of Both Worlds. *Banco Bilbao Vizcaya Argentaria (BBVA)*, 2014.

Hughes, N., and Lonie, S., M-PESA: Mobile Money for the "Unbanked" Turning Cellphones into 24-Hour Tellers in Kenya. *Innovations: Technology, Governance, Globalization,* vol. 2 no.1-2, pp. 63-81, 2007.

Huh, J., I Don't Use Apple Pay Because It's Less Secure ...: Perception of Security and Usability in Mobile Tap-and-Pay. *NDSS Symposium 2017,* 2017.

Joshi T., Gupta S.S., Rangaswamy N., Digital Wallets `Turning a Corner' for Financial Inclusion: A Study of Everyday PayTM Practices in India. *IFIP Advances in Information and Communication Technology,* vol. *552*, pp. 280-293, 2019.

Koblitz, N., Menezes, A., and Vanstone, S., The State of Elliptic Curve Cryptography. *Designs, Codes and Cryptography,* vol. 19, no. 2, pp. 173-193, 2000.

Maciaszek, L. A., *Requirements Analysis and System Design.* Addison-Wesley, 2007.

Martin, R., and Mauree, V., *Commonly identified Consumer Protection themes for.* Focus Group Technical Report, 2016.

Memon et al, Blockchain Beyond Bitcoin: Blockchain Technology Challenges and Real-World Applications. *2018 International Conference on Computing, Electronics Communications Engineering (iCCECE),* pp. 29-34, 2018.

Mendoza, S., *Samsung Pay: Tokenized Numbers, Flaws and Issues,* 2016.

Nakamoto, S., Bitcoin: a peer-to-peer electronic cash system, Available: https://bitcoin.org/bitcoin.pdf, 2018

Nandhi, M.A., Effects of Mobile Banking on the Savings Practices of Low Income Users. *Working paper*, 2012.

Nguyen, Blockchain - A Financial Technology for Future Sustainable Development. *2016 3rd International Conference on Green Technology and Sustainable Development (GTSD)*, pp. 51-54, 2016.

Roland ,M., Langer, J., and Scharinger J., Applying relay attacks to Google Wallet, pp. 1-6, 2013.

Singh, K., Mandal, S. and Mahanti, A., Opportunity Analysis: The Story of Paytm During Demonetisation. *Sixth National Conference for Case Studies (COGNOSCO)*, pp. 1-5, 2017.

Singh, L.D., Singh, K.M., Implementation of Text Encryption using Elliptic Curve Cryptography. *Procedia Computer Science,* vol. 54, pp. 73 – 82, 2015.

Susan, M., Pandy, Ph.D. and Crowe, M., *Choosing a Mobile Wallet: The Consumer Perspective,* 2017.

Williams, D., Encrypted Website Payments. In D. Williams, *Pro PayPal E-Commerce*, Apress, pp. 55-57, 2007.

Zheng et al, Blockchain challenges and opportunities: A survey. *International Journal of Web and Grid Services,* vol. 14, no. 4, pp. 352-375, 2018.

BIOGRAPHIES

Chimuka Moonde is a student pursuing a Master of Science in Computer Science in the Department of Computer Science at the University of Zambia. He earned a Bachelor of Science in Computer Science from the Copperbelt University, where he graduated as the best student in Computer Science. Chimuka has completed several software developments projects with the National Road Fund Agency of Zambia (NRFA), the National Pension Scheme Authority of Zambia (NAPSA) and University of Zambia (UNZA). His research interests include blockchain and software development.

Jackson Phiri is a senior lecturer at the University of Zambia in the Department of Computer Science. He holds a Bachelor of Science degree in Computer Science from the University of Zambia, a Master of Science in Computer Science from the University of the Western Cape and PhD in Computer Science from Harbin Institute of Technology. His research interest includes information management and Security, applied artificial intelligence technologies and ICT for development.