Compact Spiral Asymmetric encryption Distributed Ledger –Secured and authentication Mobile Payment System in Higher Institutions

B Sravani[1], Dr S Pradeep [2], A Damodar [3], K Kumar Swamy

[1]Assistant professor, Dept of CSE, Malla Reddy Engineering College for Women
[2]Assistant professor, Dept of CSE, Malla Reddy Engineering College for Women

[3]Assistant professor, Dept of CSE, Malla Reddy Engineering College for Women

4Assistant professor, Dept of CSE, Malla Reddy Engineering College for Women

(UGC Autonomous Campus) Maisammguda, Secunderabad, Telangana, India.

[1]sravanibusabi@gmail.com ,[2]pradeep.sunkari87@gmail.com

[3]Kankala.kumar24@gmail.com ,[4]damodardaniel@gmail.com

Abstract: Looking at the higher learning institutions, there is no question that the current methods for paying student fees are inefficient, inconvenient, and wasteful of time. In addition, 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. This paper sought to design and implement a secure block chain-based payment system for higher learning institutions in developing countries. 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. In this study, object-oriented software development methodology was used to implement the proposed payment system. The proposed system consists of a mobile e-wallet, RESTful API, and blockchain as the core component of the API.

Keywords: ***e-wallet; mobile wallet; block chain; cryptography***

1. INTRODUCTION

Payment systems have become a vital constituent of the economic life of contemporary societies. The smooth functioning of payment systems is critical to the overall effectiveness, efficiency and interoperability. Digital financial services map the ecosystem by identifying all key stakeholders and examining the critical elements required to improve the ecosystem, promote and allow policies for financial inclusion (Benson, 2017).

In addition, the digital financial services framework defines participants within the ecosystem and their functions. The players are users (consumers, companies, government agencies, and non-profit groups), who need digital and interoperable financial products and services; the suppliers (banks, other licensed financial institutions, and non-banks), who supply digital products and services; the financial, technological, and other infrastructure that makes them possible; the governmental policies, laws, and regulations which enable them to be delivered in an accessible, affordable and safe manner (Benson, 2016).

The expression digital financial services refers to the use of an electronic device or mobile phone application to access financial services. Digital financial services include automated financial services among which are storing funds, and making and receiving payments (Martin and Mauree, 2016). Digital financial services have become a viable way for the unbanked to access formal financial services. Most compelling evidence indicates that increasing access to formal financial services does not only reduce financial exclusion, but it has also become an important development goal for stimulating economic growth, increasing welfare and reducing poverty (Martin and Mauree, 2016). As such, the recent growth of mobile money has allowed millions of people who were financially excluded from the formal financial system to carry out financial transactions relatively cheaply, securely and reliably (Nandhi, 2012).

Money transfer and payment applications focused on mobile phones have been accepted as the means for bringing banking facilities to users beyond the traditional finance system. Mobile banking systems provide various advantages for the community, including improved profitability and capital transfers, helping to control cash balance and improving volatile income protection (Deloitte, 2014).

A sector that can highly benefit from the services provided by digital financial services is the education sector. Most school systems in developing countries rely significantly on cash transactions. This reliance on cash for financial transactions contributes to inefficiencies, cash leakage and carries security risks. Digital financial services will be able to provide unique opportunities in institutions of learning such as primary and secondary schools as well as universities. These opportunities include replacing cash, thus bringing efficiency to institutions of learning by improving management, increasing financial support from donor and non-governmental organizations, reducing financial costs, as well as laying a concrete way to developing more multifaceted systems that otherwise would not have been feasible in a cash environment (Braniff, 2017).

Looking at higher learning institutions, there is no doubt that the existing student fees payment mechanisms are ineffective, inconvenient, and time-wasting. Inefficient collection processes are especially troublesome for students in remote and hard-to-reach locations, and affect the productivity and efficiency of the workforce in accounting departments and administration. Moreover, the increase in the number of students studying in higher education institutions has led to long stressful queues and overcrowding in most financial institutions during payment of student fees. Payment via the proposed system will save time and money spent traveling to nearby cities to locate approved bank branches to deposit money. The proposed system also would eliminate the risk of carrying large sums of money by students.

2. RELATED WORK

Relevant systems and technologies have been analyzed to learn how common problems have been tackled and to obtain a deeper understanding of the approaches currently in place. Best practices in the existing systems were learnt and shortcomings noted to seek and resolve them in the proposed system. The following are related existing systems and applications that were studied.

2.1 E-Wallets

M-Pesa is an innovative payment service for the unbanked. “Pesa” is the Swahili word for cash and the “M” is for mobile. Customers turn cash into e-money at Safaricom dealers and then follow simple instructions on their phones to make payments through their M-PESA accounts; the system provides money transfers as banks do. The account is very secure, PIN-protected and supported with a 24/7 service provided by Safaricom and Vodafone Group. To implement it, Vodafone had to marry the incredibly divergent cultures of global telecommunications companies, banks, and microfinance institutions–and cope with their massive and often contradictory regulatory requirements (Hughes and Lonie, 2007). Using data preloaded on the SIM card, M-PESA utilizes a SMS-based interface to transmit money virtually to other phones. To load money into one's virtual account, a customer visits one of Safaricom agents and exchanges currency for e-money, which is automatically deposited into their account. Customers can transfer money to anyone who owns a mobile phone (Hinz, 2014).

Paytm (earlier written as PayTM) began its journey as a recharge and bill payment platform which made its way into the e-commerce market. The Paytm wallet facilities ease of payment on almost all possible needs of daily life ranging from daily or monthly essentials, utilities (electricity bill, metro card, gas and water), entertainment, travel, mobile recharge, electronic gadgets, appliances, fashion and many more (Singh and Singh, 2015). A user can pay through scanning QR codes or entering a merchant's registered number. Users have the facility to add credit or debit cards, especially bank accounts to transfer money to Paytm wallets and transfer money from Paytm wallets to bank accounts (Joshi et al., 2019).

PayPal is one of the most accepted payment services in the world. PayPal allows any business or individual to send and receive payments online, in-store or on mobile securely, conveniently, and cost-effectively. PayPal deducts the funds from whatever bank account or credit card the consumer has linked (Pandy and Crowe, 2017). PayPal uses public key cryptography to encrypt communication between the consumer and merchant. Public key cryptography is a popular technique used to encrypt data which are transmitted over the Internet from one location to another and to ensure that the sender's identity is guaranteed. It operates by using public keys and private keys, which are bits of data mathematically connected to each other by means of an algorithm (Williams, 2007).

Google Wallet lets a consumer save all their loyalty cards in once place. A consumer can also make payments online and make contactless payments with their mobile phone. Google Wallet offers tap-to-pay for near field communication (NFC) enabled devices. If a consumer needs to send money to someone, a consumer can do so without any transaction charges if they're using Google Wallet as well. Google Wallet allows users to store their debit cards, credit cards, gift cards and loyalty cards on a smartphone, transforming it into a virtual wallet (Ghag and Hegde, 2012). Google. It consists of an Android app with a user interface. The user interface is used to protect the wallet with a PIN code, to manage the payment, gift, and reward cards, to select the currently active card, to find specific offers, and to view the transaction history. The secure element of the wallet is used to store sensitive information of the payment, gift, and reward cards, and to interact with existing POS reader infrastructures (Roland, et al., 2013).

Apple Pay is a mobile payment system that lets iPhone (iPhone 6 and higher versions) users pay for goods and services using Touch ID. As compared to entering or confirming payment card information (credit or debit card) every time they make a purchase, users can authorize payment for items securely by touching the home button of the iPhone. A payment token stores all the information needed to process the payment all the way from authorization to settlement. During an Apple Pay transaction, payment card information never leaves the user's iPhone; this information is stored securely in the device (Bruce, 2016). To set up Apple Pay, users simply add a debit or credit card to the wallet app. The card information can be imported from iTunes, entered manually, or added by taking a picture of a debit or credit card using an iPhone. To tap-and-pay in stores, users need to hold their iPhone close to an NFC reader. Users then place a finger on Touch ID (fingerprint scanner) to authenticate themselves and complete the payment process. The wallet app immediately notifies users about confirmed transactions (Huh, 2017).

Samsung Pay is a method to make purchases over the latest line of Samsung smartphones devices. Leveraging a proprietary technology called magnetic secure transmission (MST) and NFC, Samsung Pay makes mobile payment more accessible to both merchants and customers. Samsung implemented a sophisticated alphanumeric algorithm called tokenization. In addition, Samsung partnered with payment card providers such as Visa and MasterCard, and embraced the VTS framework (Visa Token Service) to push its ambitious project. When a user adds a card to their Samsung Pay, the system generates a new "virtual random" CC (a new card number with some parameters) implementing the framework which assigns a token to each card. That token is saved in a token vault relating the original primary account number (PAN) information. Therefore, in each transaction instead of using the original CC's data, the mobile device sends a tokenized number (Choi and Lee, 2018). Samsung Pay works with traditional point-of-sale (POS) devices that allow the use of magnetic card swipes. The key technology that gives Samsung Pay such a superior position is called MST. Under this technology, devices using the Samsung Pay app can generate a magnetic signal that contains the same payment information as that generated by swiping a magnetic card in the POS card reader. Thus, the POS device can recognize the Samsung Pay signal if the mobile device is sufficiently close, even though nothing is swiped on the card reader. Unlike Apple Pay, Samsung Pay supports MST alongside NFC, which means it works with any payment terminal that accepts contactless payments or the more traditional method of swiping a card through the reader (Choi and Lee, 2018).

2.2 Block chain Technologies

A blockchain can be defined as an immutable transaction recording ledger, held within a distributed network of mutually untrusting peers. A consensus protocol is used by the peers to verify transactions, group them into blocks, and construct a hash chain over the blocks (Mvula et al., 2020). A blockchain can be considered as a data structure, that is, a blockchain contains a connected list of blocks, each containing a collection of transactions. Furthermore, a blockchain can considered as a network, that is, a blockchain is a combination of peer-to-peer networks (Hussein et al., 2018). Blockchain from a software engineering perspective enables the development of a new distributed and decentralized system software architecture, where a sensitive transaction or confidential transaction agreements may be made with untrusted individuals across the chain (Muhamad et al., 2020). In addition, Blockchain is a distributed system that operates without the use of a central authority or third-party intermediaries (Labrador and Hou, 2019).

Public and private blockchains are the two primary types of blockchains. In a public or permission-less blockchain, without a particular identity, any device can participate. Usually, public blockchains provide a native cryptocurrency, use consensus based on Proof of Work (PoW) and financial rewards. Permissioned blockchains, on the other hand, runs a blockchain among a collection of known, identified devices. A permissioned blockchain provides a way for a group of organizations that have a common purpose but do not fully trust each other to secure interactions, such as businesses that share money, products, or information (Mvula et al., 2020).

Blockchain as an emerging technology became popular in 2008. It was first used as a peer-to-peer ledger for registering the transactions of Bitcoin cryptocurrency (Nakamoto, 2008). The aim was to eliminate any third-party intermediary and allow users to make their transactions directly. Thus, blockchain was designed as a decentralized network of peer nodes. Each node in the network: (1) Holds a replica of the transaction's ledger; (2) writes an entry to its own ledger when it receives consensus from the other nodes in the network; (3) broadcasts any transaction made by its user to the other nodes in the network; (4) checks, on a regular basis, that the ledger it holds is identical to the ones across the network (Grech, 2017). As Bitcoin continues to grow in popularity, researchers and practitioners have realized the enormous potential of its underlying technology (Collins, 2016). The unique capabilities of blockchain, which include immutability, transparency and trustworthiness, were found to be useful not only in cryptocurrencies, but also in many other fields. Therefore, an increasing number of blockchain-based applications have been developed in various fields (Memon et al., 2018). Furthermore, the various features of Blockchain technology, such as decentralization, immutability, robustness, privacy, consensus and cryptographic algorithms have the ability to alleviate reliance on a single centralized authority which is more susceptible to inaccuracy, insecurity, lack of complete trust and single point of failure (Yaqoob et al., 2019). This would lead to a reduction in the reliance on traditional central ledger managed by a trusted entity for holding and transferring funds (Mvula et al., 2020).

According to Gatteschi et al. (2018), the development of blockchain-based applications could be divided into three main stages: Blockchain 1.0, 2.0, and 3.0. Blockchain 1.0 was used for cryptocurrencies, and its focus was to facilitate simple cash transactions. Subsequently, Blockchain 2.0 was introduced for properties and smart contracts. These smart contracts impose specific conditions and criteria to be met before registering them in the blockchain.

Registration takes place without the intervention of a third party. In Blockchain 3.0, many applications were developed in various sectors, such as government, education, health and science. The application of blockchain to education is still in its early stages. Only a small number of educational institutions have started to utilize blockchain technology.

Since Diffie and Hellman introduced public-key cryptography in 1976, there has been awareness of the potential for the use of the discrete logarithm problem in public-key cryptosystems. Although the discrete logarithm problem as first used by Diffie and Hellman was specifically defined as the problem of finding logarithms in relation to a generator in the multiplicative group of the integer modulo a prime, this concept can be generalized to arbitrary groups, and to elliptic curve groups. The resulting public-key systems provide relatively small block size, high speed and high security. Koblitz et al. (2000) conducted a survey to investigate the development of elliptic curve cryptosystems from Koblitz and Miller's invention in 1985 to present-day implementations.

Singh and Singh (2015) implemented text encryption using elliptic curve cryptography. They introduced a new technique, in which the authors omitted the classic technique of mapping characters to affine points in the elliptic curve. The respective plain text ASCII values are paired up. The paired values serve as input for the cryptography of the elliptic curve. This new technique eliminated the expensive mapping process and the need to share the standard lookup table between the sender and the recipient. The algorithm was built in such a way that any kind of script with specified ASCII values can be encrypted or decrypted.

In order to realize safe and fair payment of outsourcing services in general without depending on any third party, trusted or not, Zhang et al. (2018) introduced a solution called BCPay. BCPay is a blockchain-based fair payment system for outsourcing services in cloud computing. Security review showed that BCPay achieved soundness and immunity to attacks of eavesdropping and malleability. Performance review showed that BCPay was very effective in terms of the number of transactions and the cost of computation.

Lusetti, Salsi, and Dallatana (2020) proposed a blockchain-based solution for the custody of digital files in forensic medicine. The authors suggested addressing the problem through a hybrid operating model using a consensus framework to maintain a transparent access history and prevent unauthorized users from changing the access history. The digital evidence was encrypted and stored electronically, while the file properties were stored on a private blockchain implementation of the Hyperledger Fabric. The nodes to the blockchain would allow access to the data by means of a dynamic consensus process and any operations (e.g., uploads, images, or deletions) were registered on the blockchain, continuously and indefinitely. All information was accepted and exchanged amongst the blockchain nodes to prevent single points of failure, and safe access to digital proof was achieved by combining cryptography and the blockchain consensus mechanism.

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 software 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 subsections outline some of the key phases the authors used in this study.

3.1 Requirements Specifications

This phase is critical to the success of the project. Expectations need to be looked at and recorded in great detail. 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 mobile e-wallet application:

1. A user should be able to create a mobile wallet account using his/her registered student number, mobile number and PIN.
2. A user should be able to login his/her mobile wallet account using his/her mobile number and PIN.
3. A user should be able to reset his/her forgotten PIN.
4. A user should be able to view his/her current mobile wallet balance and private and public keys.
5. A user should be able to load funds into his/her mobile wallet from either his/her bank account or mobile money account.
6. A user should be able to input necessary information in order to perform a transaction.
7. A user should be able to view payment information before committing a transaction.
8. A user should be able to receive feedback that relates to the transaction.
9. A user should be able to pay for various student fees and other merchant fees.
10. A user should be able to send funds from his/her mobile wallet to another registered mobile wallet.
11. A user should be able to request transfer of funds from another registered mobile e-wallet to his/her mobile e-wallet.
12. A user should be able to view his/her transaction history.

3.2 Design Specification:

Fundamental in the implementation of the proposed block chain-based payment system was the use of elliptic curve public-key encryption and signature scheme. Cryptography is the transformation of plain message 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). The authors adopted Eq. 1, 2, 3, and 4 as outlined by Hankerson et al. (2004) as essential components in the algorithms used in the proposed system. An elliptic curve E is defined by an equation over a field K:

$$E : y^2 + a_1xy + a_3y = x^3 + a_2x^2 + a_4x + a_6 \tag{1}$$

Where a1, a2, a3, a4, a6 ∈ K and Δ ≠ 0, where Δ is the discriminate of E and is defined as follows:

$$\begin{gathered} \Delta = -d\frac{2}{2}d_8 - 8d\frac{3}{4} - 27d\frac{2}{6} + 9d_2d_4d_6 \\ d_2 = a\frac{2}{1} + 4a_2 \\ d_4 = 2a_4 + a_1a_3 \\ d_6 = a\frac{2}{3} + 4a_6 \\ d_8 = a\frac{2}{1}a_6 + 4a_2a_6 - a_1a_3a_4 + a_2a\frac{2}{3} - a\frac{2}{4} \end{gathered} \tag{2}$$

If L is any extension field of K, then the set of L-rational points on E is as follows:

$$E(L) = \{(x, y) \in L \; x \; L: y^2 + a_1xy + a_3y - x^3 - a_2x^2 - a_4x - a_6 = 0\} \cup \{\infty\} \tag{3}$$

where ∞ is the point at infinity.

For the generation of the key pair, this study utilized Eq. 4:

$$\langle P \rangle = \{\infty, P, 2P, 3P, \dots, (n-1)P\} \tag{4}$$

Let E define an elliptic curve over a finite field F_p. Let P be a point in $E(\mathrm{F}_p)$ and assume P has prime order n. The cyclic subgroup of $E(\mathrm{F}_p)$ generated by P is Eq. **Error! Reference source not found.**, where prime p, the equation of the elliptic curve E and the point P and its order n are the public domain parameters. A private key is an integer d that is generated randomly from the interval [1, n-1] and the respective public key is $Q = dP$.

The elliptic curve key pair generation used in the proposed system can be represented as follows:

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).

For the encryption scheme, in this study the authors adopted the following algorithm:

INPUT: Plain transactional data denoted as m, public key Q and elliptic curve domain parameters (p, E, P, n).

OUTPUT: Cipher text (C_1, C_2).

1. Represent the plain transactional data m as a point M in $E(\mathrm{F}_p)$.
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.

For the decryption scheme, in this study the authors adopted the following algorithm:

INPUT: Cipher text (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 $M = C_2 - dC_1$

Based on the design specification, the authors implemented a prototype of the proposed blockchain-based mobile payment system. The implementation stage of software development is the process of converting design specification to an executable software system. The authors implemented the blockchain mobile payment system using the following programming languages and tools: Flutter version 1.6, JavaScript Object Notation (JSON), Node.js version 12.18.1, Express.js version 4.17.1, Visual Studio Code version 1.48.2, Postman version 7.31.1 and GitHub.

3.3 Blockchain API

The authors implemented a RESTful API using Express.js, which is a web framework for Node.js. The researchers used JavaScript, particularly Express.js as the programming language, to implement the API, while Visual Studio Code was the development tool the authors used to construct the API. The API used JSON as the data-interchange format. The authors used Postman to test the API. Furthermore, Postman was used to view the various responses from the endpoints of the API. The complete API was hosted on Ubuntu 18.04 LTS powered virtual server provisioned from Amazon Web Services. At the core of the API, the authors implemented blockchain using JavaScript, particularly using Node.js and Express.js as the programming language. Visual Studio Code was the development tool the authors used to implement the blockchain.

3.4 Mobile Application

The authors implemented an Android-based and iOS-based e-wallet mobile application using Flutter which is a tool that enabled the authors to build a native cross-platform (Android and iOS) application with one programming language and codebase. The user interface (UI), business and application logic were implemented using dart as the programming language. Overall, the mobile application was developed using Visual Studio Code as the development tool. The mobile wallet application was installed on an Android device running Android Marshmallow for testing purposes.

3.6 Code Versioning

The researchers used GitHub as a code version and backup tool while developing the blockchain-based mobile payment system.

4. RESULTS

4.1 Blockchain API

The RESTful API was the communication and data sharing mechanism between the numerous nodes and mobile e-wallet. Fig. 4 shows an overview of the client server communication of the API.

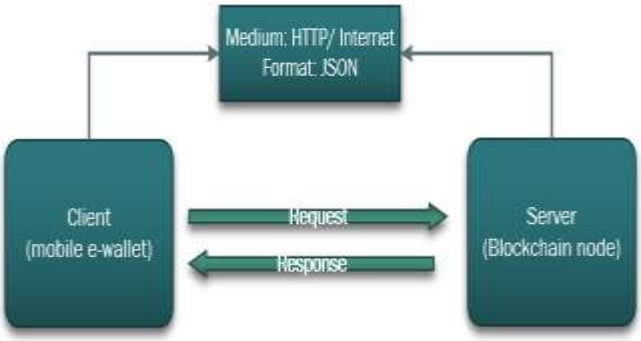
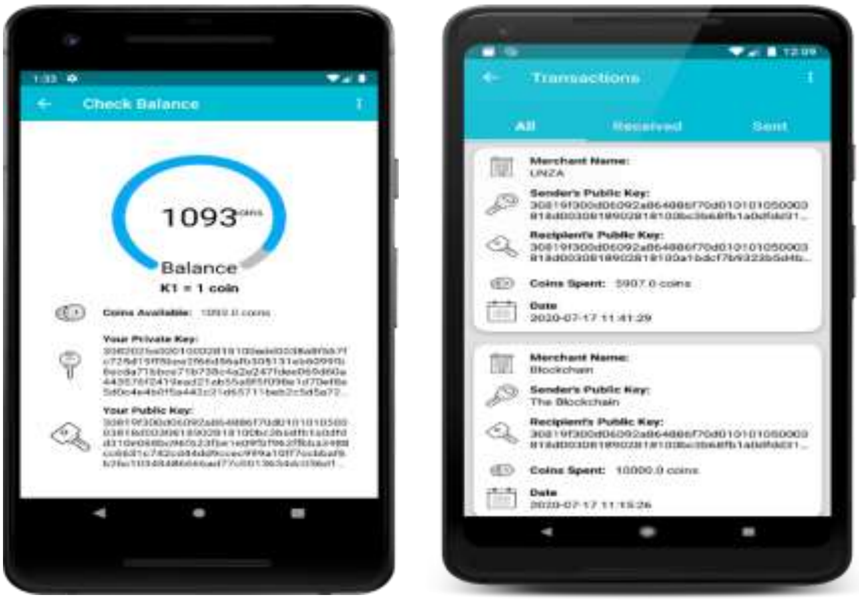


Figure 1 : Client Server Communication

The API leverages the block chain as the core component. It does so in order to keep a database of transactions. As a ledger, the block chain serves the purpose of storing transactional data. The immutable ledger is used to refer to block chains to describe the way in which blocks cannot be changed after they are recorded. Block chain is the underlying technology and data structure of the API. Fig. 5 shows the JSON formatted output obtained from consuming one the API's endpoint using Postman.

A block chain contains a connected list of blocks, each containing a collection of transactions, and is considered one of the data structures (Hussein et al., 2018). The first JSON object in the JSON array shows the first block called the genesis block. This is the block that is generated after initializing of the block chain. The genesis block has meta-data such as the nonce which increases for every hash calculation, timestamp in seconds which refers to the time the block was created and the difficulty which is the existing hashing target. In addition, the genesis block does not have a previous or last hash. Conventionally the last hash for the genesis block is represented with all zeros. Nevertheless, the genesis block has its own harsh. The second JSON object in the JSON array shows the second block that proceeds the genesis block. Like the genesis, the second block contains its own meta-data such as nonce, timestamp and difficulty. The last hash of the second block is identical to the hash for the genesis block. Therefore, genesis block and the second are cryptographically linked with each other through the hashes. Furthermore, the second block has its own hash which is generated based on the block's meta-data and data to store. As shown in Fig. 5, transactions consist of an input (where funds came from) and output (where funds are going) objects. Information about the sender is generated by the input of a transaction. Input information includes a timestamp, sender's public key, the sender's balance, as well as the signature (digital signature) of the sender which is generated using the sender's private key. Digital signatures are like unique handwritten signatures, but with far more inherent security, so as to solve the problem of impersonation and tampering. The output object includes recipient public key and a JSON array of fees being paid. The output object also includes a transaction that specifies the public key of the sender as the recipient key. This transaction is called Unspent Transaction Output (UTXO). UTXO refers to the amount of digital currency left after executing a transaction.

4.2 Mobile Application



Coins Available: 1093.0 coins

Your Private Key:
[illegible]

Your Public Key:
[illegible]

Merchant Name:
UNZA
Sender's Public Key:
30819f300d06092a864886f70d010101050003
818d0030818902818100bc3b68fb1a0dfdd31...
Recipient's Public Key:
30819f300d06092a864886f70d010101050003
818d0030818902818100a1bdcf7b9323b5d4b...
Coins Spent: 5907.0 coins
Date
2020-07-17 11:41:29

Merchant Name:
Blockchain
Sender's Public Key:
The Blockchain
Recipient's Public Key:
30819f300d06092a864886f70d010101050003
818d0030818902818100bc3b68fb1a0dfdd31...
Coins Spent: 10000.0 coins
Date
2020-07-17 11:15:26

Figure 2 :Implementation Mobile E-Wallet Android Application

AS the Figure 2 Shows the implemented e-wallet Android application. Like a physical wallet, the mobile e-wallet Android application will help a student track to how much digital currency he/she is entitled. Furthermore, the e-wallet application will store the student's private and public keys. The private key allows the student to generate a unique digital signature to sign very exchange of digital currency between the student and the institution. The institution may use the student's public key to verify the student's signature. A wallet's public key allows other nodes or individuals to verify digital signature generated by the private key of the wallet in the blockchain network. Using the student public key, the institution will decrypt the data presented by the signature. If the decrypted data does not match the data suggested, then the signature is deemed invalid. Likewise, the signature is valid if the decrypted data matches the proposed data. It is required that the signature undergoes a verification to check whether the underlying transactional data is being sent by the allegedly student to prevent system fraud. The public key also serves as the public address of the wallet and is what other nodes or people use to send digital currency to a wallet. The public key is generated from the private key. The public key is a 2D point coordinate on an elliptic curve. In addition, the Fig. 6 shows the transaction history of the wallet.

Discussion:

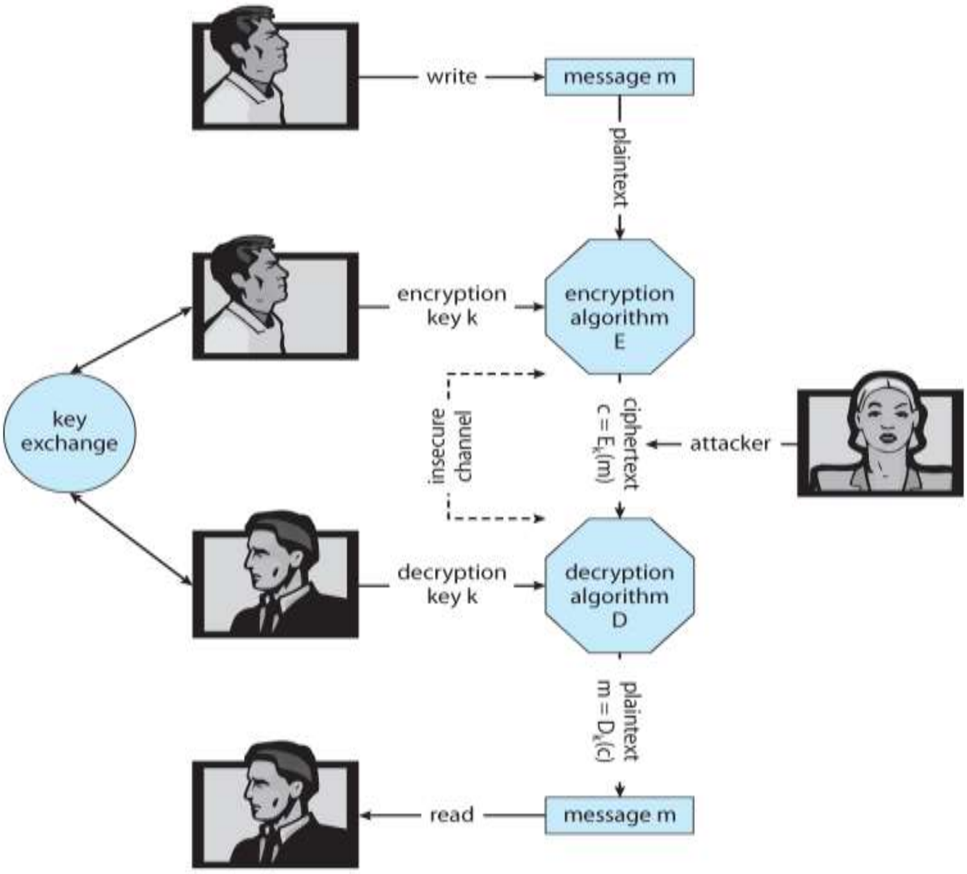


Figure 3: Communication process over unsecured channel

Fig. 3, tells about communicate via an unsecured channel. In this study, the communication channel is the Internet. All communication occurs in the presence of an attacker whose aim is the defeat of any security services provided to the student and institution. The attacker could attempt to read the traffic from the student to the institution, therefore learning the student's personal identifiable information as well as bank card or account information. In addition, the attacker could attempt to impersonate either the student or institution.

Careful analysis of the aforementioned scenarios shows the following underlying factors that required to be addressed in the implementation of the proposed payment system:

1. Confidentiality: Keeping data secret from everyone, but those authorized to view it. Transactional data sent by the student using the mobile e-wallet to the intuition should not be readable by the attacker.
2. Data Integrity: Ensuring that the transactional data sent through the unsecured channel is not altered by the attacker. The institution should be able to detect when the transactional data sent by the student using the mobile e-wallet have been modified by the attacker.
3. Data Origin Authentication: The institution should be able to check and verify that the transactional data supposedly sent by the student using the mobile e-wallet did actually originate from the student.
4. Entity Authentication: The institution should be convinced of the identity of the student.
5. Non-Repudiation: Preventing the student from denying transactions previously made. When the institution supposedly receives transactional data from the student, it should not only be convinced that the transaction came from the student, but it should be able to convince a neutral third party that the transaction came from the student. Therefore, the student should not be able to deny having made the transaction.

The authors addressed the highlighted fundamental security factors by the use of elliptic curve public-key encryption and signature in the implementation of the proposed system. With the help of the blockchain, both the student and institution generate a pair of keys (e, d) consisting of a public key e and associated private key d. Each entity keeps its private key a secret. Fig. 8 illustrates an overview of the wallet public and private key.

When a student want to send transactional data /process from wallet to the end user, the mobile e-wallet obtains a copy of the institution's public key $e_{institution}$. The mobile e-wallet uses the encryption function ENCRYPT of elliptic curve public key encryption scheme to compute the cipher text c= ENCRYPT $e_{institution}$(transactional data).

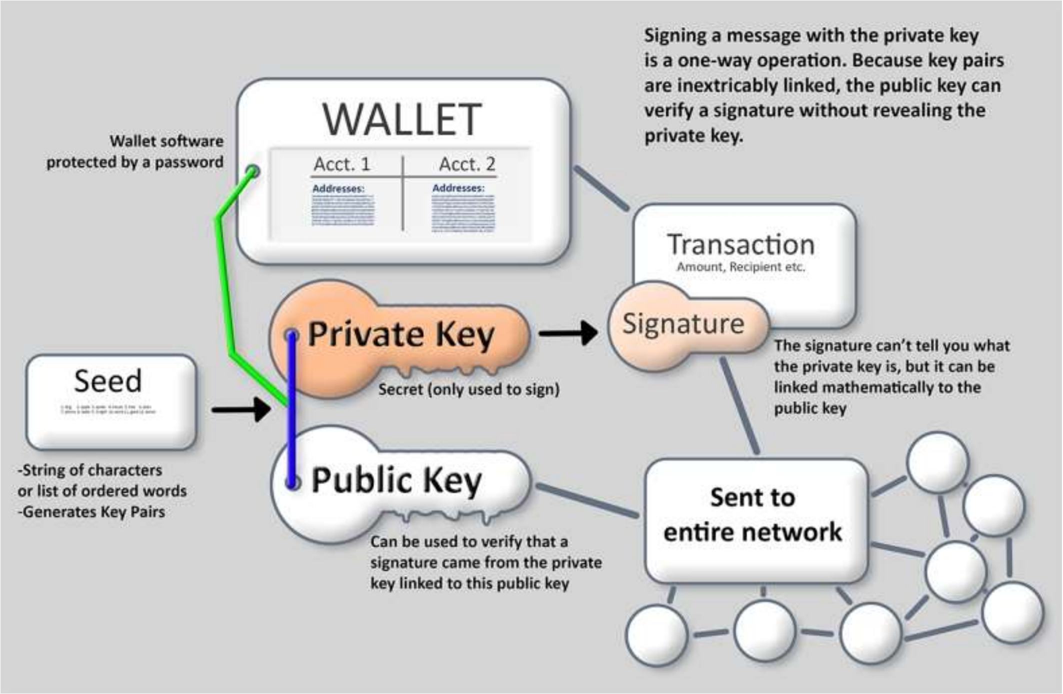

Signing a message with the private key is a one-way operation. Because key pairs are inextricably linked, the public key can verify a signature without revealing the private key.
WALLET
Acct. 1
Acct. 2
Addresses:
Addresses:
Wallet software protected by a password
Transaction
Amount, Recipient etc.
Private Key
Secret (only used to sign)
Signature
The signature can't tell you what the private key is, but it can be linked mathematically to the public key
Seed
-String of characters or list of ordered words
-Generates Key Pairs
Public Key
Can be used to verify that a signature came from the private key linked to this public key
Sent to entire network

Figure 4: Wallet Public and Private key

The mobile e-wallet then sends c to the institution. The institution uses the decryption function DECRYPT and its private key $d_{institution}$ to recover the plaintext format of the transactional data, which are represented by m = DECRYPT $d_{institution}$(c), where c is the cipher text that was received. An attacker with access to the copy of the institution's public cannot use the public key to decrypt the cipher text sent from the student to the institution. The key pair has a property that is not computationally feasible to determine the private key only from the information of the public key.

A student using the mobile e-wallet uses the signature generation algorithm SIGN of the digital signature scheme of the elliptic curve cryptography and their private key $d_{student}$ to compute the signature of the transactional data s = SIGN $d_{student}$(transactional data). The mobile e-wallet sends the signed transactional data in ciphertext format to the institution. The institution obtains a copy of the student's public key $e_{student}$ and uses a signature verification algorithm to confirm that *s* was indeed generated from m and $d_{student}$. Since $d_{student}$ is only known by the student, the institution is assured that the transactional data did indeed originate from the student. More importantly, since verification requires only the non-secret quantities m and $e_{student}$, the signature *s* for the transactional data can also be verified by a third party who could settle disputes if the student denies having signed the transactional data. Fig. 5 and 6 summaries the use of elliptic curve public-key encryption and signature in the implementation of the proposed system.

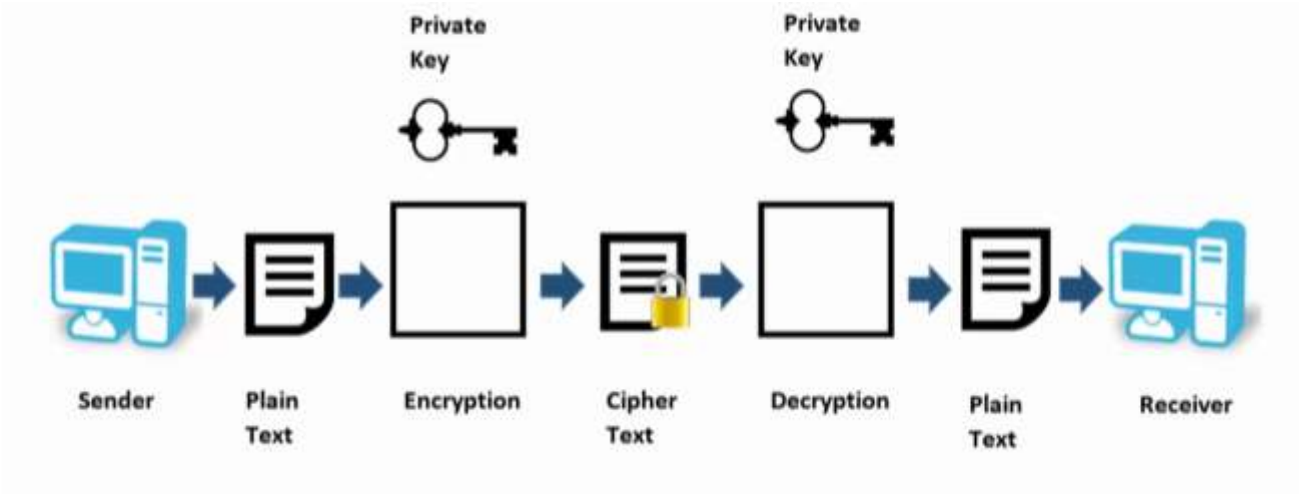


Figure 5: Summary of Elliptic curve public key encryption

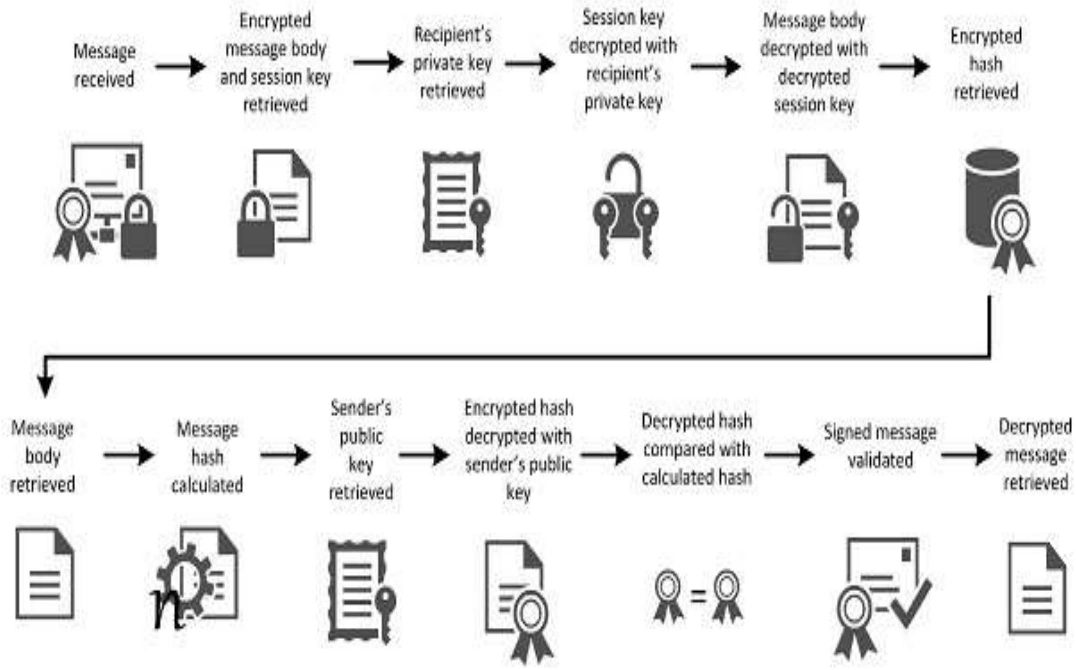

Message received
Encrypted message body and session key retrieved
Recipient's private key retrieved
Session key decrypted with recipient's private key
Message body decrypted with decrypted session key
Encrypted hash retrieved
Message body retrieved
Message hash calculated
Sender's public key retrieved
Encrypted hash decrypted with sender's public key
Decrypted hash compared with calculated hash
Signed message validated
Decrypted message retrieved

Figure 6 : Digital Signature Summary process

Public key cryptography is a popular technique used to encrypt data which are transmitted over the Internet from one location to another and to ensure that the sender's identity is guaranteed. It operates by using public keys and private keys, which are bits of data mathematically connected to each other by means of an algorithm. Their relationship is such that no knowledge of the public key can extract the private key. The private key must be kept confidential, while the public key can be made widely available. Transactional data is encrypted, so that it cannot be read or modified while in transit.

A block chain can be regarded as a digital distributed ledger that is used to store and exchange information over a peer-to-peer network (Alexander and Wang, 2019). Permissioned block chains were used in this research, which ran a block chain among a group of known and identified devices.

The concept of block chain emerged initially from two people: Stuart Haber and W. Scott Stornetta. They did not necessarily coin or introduce the term “block chain,” because it came much later after Satoshi Nakamoto's original paper. Nevertheless, Haber and Stornetta (1991) introduced the concepts of what is now called the block chain, and actually all or most of the features and ideas behind the block chain are present in the document. Block chain technology creatively blends cryptography with a decentralized database in a novel way, allowing a block chain to be decentralized, immutable and transparent all at once (Werapun et al., 2020).

Block chain is a distributed ledger that is tamper-proof and preserves the growing array of data records. There is no centralized approach and no master computer. The ledger comprises a chain of blocks linked to each other by cryptography (Muhamad et al., 2020). Furthermore, the block chain is a distributed and decentralized ledger that stores data such as transactions, and the ledger is publicly shared across all the nodes of its network. By implementing the proof-of-work consensus protocol, each node of the network checks the validation of the block. The validated block is appended to the chain and the modified ledger is replicated through the permitted nodes of the chain. The consensus protocol replaces the requirement trusted third party or the central authority (Yaqoob et al., 2019). This study made use of the Proof of Work as the consensus protocol.

The block chain consists of multiple blocks of data chained together like the links of a physical chain (Atlam and Wills, 2019). Blocks are a storage of data on the block chain network. Once a block is added to the chain of blocks that precedes it, it becomes irreversible. Every block is given a unique value that looks like a random string of characters. The random string of characters is called the hash since it is generated from a hash function that creates a unique output for every unique input that it receives (Nakamoto, 2008). The unique hash is generated based on the metadata about the block and the unique data that are in the block. There is also one more very crucial data point used to generate the hash of a new block, namely the unique hash of the previous block. The unique hash of the previous block is also used as part of the input that the new block uses to generate its hash. This means that the previous block is an integral part of creating the hash value of the new block.

6. Conclusion

The purpose of this study was to design and implement a mobile payment system for higher learning institutions in developing countries based on block chain. The initiative to implement a block chain-based mobile payment system was propelled by the awareness of how the payment of student fees is undeniably ineffective, expensive and time-consuming. In addition, the increase in the number of students studying in higher education institutions often results in long stressful queues and severe overcrowding when paying student fees in most financial institutions. Students are expected to use the proposed payment system to pay their respective higher educational institution tuition fees and other student fees. In addition, the proposed payment is to be used by students to pay for the goods and services offered by the institution and other vendors on the premises of the institution.

Acknowledgments

I would like to acknowledge the authors for the review of my paper and supporting the research and we would like to thank Dr. Y. Madhavee Latha ,Principal- Malla Reddy Engineering College for Women(UGC Autonomous Campus), Maisammaguda, Dhulapally, Kompally, Medchal (M), Secunderabad, Telangana , India . Furthermore, the authors would like to thank all colleagues and friends in the Computer Science Department for their support.

REFERENCES

[1] *Benson, C. N. (2016). The Digital Financial Services Ecosystem. ITU-T Focus Group On Digital Financial Services.*

[2] *Benson, C. N. (2017). Financial Inclusion. ITU-T Focus Group Digital Financial Services.*

[3] *Braniff, L. (2017). Schools Africa Aren't Taking Advantage Mobile Money Why.*

[4] *Bruce, S. (2016). Apple Pay Essentials. Packt Publishing.*

[5] *Choi, D. and Lee, Y. (2016). "Eavesdropping One-Time Tokens Over Magnetic Secure Transmission in Samsung Pay. 10th USENIX Workshop on Offensive Technologies (WOOT 16). USENIX Association. Retrieved from https://www.usenix.org/conference/woot16/workshop-program/presentation/choi*

[6] *Choi, D. and Lee, Y. (2018). Eavesdropping of Magnetic Secure Transmission Signals and Its Security Implications for a Mobile Payment Protocol. IEEE, 6, 42687-42701. doi:doi: 10.1109/ACCESS.2018.2859447*

[7] *Collins, R. (2016). Blockchain:A New Architecture for Digital Content. Retrieved from http://www.econtentmag.com/Articles/Editorial/Commentary/Blockchain-A-New-Architecture-for-Digital-Content-114161.htm*

[8] *Deloitte. (2014). Value of Connectivity Economics and Social Benefits of Expanding Internet Access.*

[9] *Gatteschi, V., Lamberti, F., Demartini, C., Pranteda, C. and Santamaría V. (2018). Blockchain and Smart Contracts for Insurance: Is the Technology Mature Enough? Future Internet, 10(20). doi:doi:https://doi.org/10.3390/fi10020020*

[10] *Ghag, O. and Hegde S. (2012). A Comprehensive Study of Google Wallet as an NFC Application. International Journal of Computer Applications, 58(16), 37-42.*

[11] *Grech, A. a. (2017). Blockchain in Education. Publications Office of the European Union. doi:doi:10.2760/60649*

[12] *Haber, S. and Stornetta, W.S. (1991). How to Time-Stamp a Digital Document. Journal of Cryptology, 3(2), 99-111.*

[13] *Hankerson, D., Menezes, A.J. and Vanstone, S. (2004). Guide to Elliptic Curve Cryptography. Springer. doi:https://doi.org/10.1007/b97644*

[14] *Hevner, A. R. (1992). Object-Oriented System Development Methods. Advances in Computers, 35, 135-198. doi:doi:https://doi.org/10.1016/S0065-2458(08)60595-1*

[15] *Hinz, M. (2014). M-PESA: The Best of Both Worlds. BBVA, 1-5.*

[16] *Hughes, N. and Lonie, S. (2007). M-PESA: Mobile Money for the "Unbanked" Turning Cellphones into 24-Hour Tellers in Kenya. Innovations: Technology, Governance, Globalization, 2(1-2), 64-81. doi:doi:https://doi.org/10.1162/itgg.2007.2.1-2.63*

[17] *Huh, J. (2017). I Don't Use Apple Pay Because It's Less Secure: Perception of Security and Usability in Mobile Tap-and-Pay. NDSS Symposium 2017. doi:doi:10.14722/usec.2017.23021*

[18] *Hussein, D. M. E. M., Taha, M.H.N. and Khalifa, N.E.M. (2018). A Blockchain Technology Evolution Between Business Process Management (BPM) and Internet-of-Things (IoT). International Journal of Advanced Computer Science and Applications (IJACSA), 9(8). doi:http://dx.doi.org/10.14569/IJACSA.2018.090856*

[19] *Joshi, T., Gupta, S.S. and Rangaswamy, N. (2019). Digital Wallets 'Turning a Corner' for Financial Inclusion: A Study of Everyday PayTM Practices in India. IFIP Advances in Information and Communication Technology, 552, 280-293. doi:doi:https://doi.org/10.1007/978-3-030-19115-3_23*

[20] *Koblitz, N., Menezes, A. and Vanstone, S. (2000). The State of Elliptic Curve Cryptography. Designs, Codes and Cryptography, 19(2), 173-193. doi:doi:10.1023/A:1008354106356*

[21] *Labrador, M. & Hou, W. (2019). Security Mechanism for Vehicle Identification and Transaction Authentication in the Internet of Vehicle (IoV) Scenario: A Blockchain Based Model. Journal of Computer Science, 15(2), 249-257. doi:https://doi.org/10.3844/jcssp.2019.249.257*

[22] *Maciaszek, L. A. (2007). Requirements Analysis and System Design. Addison-Wesley.*

[23] *Martin, R. and Mauree, V. (2016). Commonly Identified Consumer Protection Themes. Focus Group Technical Report.*

[24] *Memon, M., Hussain, S. S., Bajwa, U. A. and Ikhlas, A. (2018). Blockchain Beyond Bitcoin: Blockchain Technology Challenges and Real-World Applications. 2018 International Conference on Computing, Electronics & Communications Engineering (iCCECE), 29-34. doi:doi: 10.1109/iCCECOME.2018.8658518*

[25] *Muhamad, W. N. W., Razali, N. A. M., Wook, M., Ishak, K. K., Zainudin, N. M., Hasbullah, N. A. and Ramli, S. (2020). Evaluation of Blockchain-based Data Sharing Acceptance among Intelligence Community. International Journal of*

Advanced Computer Science and Applications(IJACSA), 11(12). doi:http://dx.doi.org/10.14569/IJACSA.2020.0111270

[26] *Nakamoto, J. (2008). Bitcoin: A peer-to-peer electronic cash system. Google Scholar.*

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

[28] *Pandy, S. M. and Crowe, M. (2017). Choosing a Mobile Wallet. The Consumer Perspective.*

[29] *Roland, M., Langer, J. and Scharinger, J. (2013). Applying Relay Attacks to Google Wallet. 1-6. doi:doi:10.1109/NFC.2013.6482441*

[30] *Singh, L.D. and Singh, K.M. (2015). Implementation of Text Encryption using Elliptic Curve Cryptography. Procedia Computer Science, 54, 73-82. doi:doi:https://doi.org/10.1016/j.procs.2015.06.009*

[31] *Werapun, W., Arpornthip, T., Sangiamkul, E., Wetprasit, R. & Karode, T. (2020). A Blockchain-based Renewable Energy Investment Management Platform: Decentralized Sustainable Development (DeSDev). Journal of Computer Science, 16(11), 1657-1668. doi:https://doi.org/10.3844/jcssp.2020.1657.1668*

[32] *Williams, D. (2007). Encrypted Website Payments. In Pro PayPal E-Commerce (pp. 55-57). doi:doi:https://doi.org/10.1007/978-1-4302-0353-7*