Computers, Materials & Continua

Tech Science Press

DOI: 10.32604/cmc.2023.036691
Article

Blockchain Mobile Wallet with Secure Offline Transactions

Raed Saeed Rasheed[1], Khalil Hamdi Ateyeh Al-Shqeerat[2,*], Ahmed Salah Ghorab[3], Fuad Salama AbuOwaimer[4] and Aiman Ahmed AbuSamra[1]

[1]Faculty of Engineering, Islamic University of Gaza, P.O. Box 108, Gaza, Palestine
[2]Department of Computer Science, College of Computer, Qassim University, P.O. Box 52211, Buraydah, Saudi Arabia
[3]University College of Applied Sciences, P.O. Box 1415, Gaza, Palestine
[4]Palestine Technical College, P.O. Box 6037, Deir ElBalah, Palestine
*Corresponding Author: Khalil Hamdi Ateyeh Al-Shqeerat. Email: kh.alshqeerat@qu.edu.sa

Received: 09 October 2022; Accepted: 29 December 2022

Abstract: There has been an increase in the adoption of mobile payment systems worldwide in the past few years. However, poor Internet connection in rural regions continues to be an obstacle to the widespread use of such technologies. On top of that, there are significant problems with the currently available offline wallets; for instance, the payee cannot verify the number of coins received without access to the Internet. Additionally, it has been demonstrated that some existing systems are susceptible to false token generation, and some do not even permit the user to divide the offline token into smaller portions to be used as change. This paper proposes a blockchain-based wallet system that provides a secure mobile payment service even if a user cannot access a reliable Internet connection. Our approach relies on Bluetooth and digital signatures to establish and build a trust connection between the parties. The proposed solution overcomes the main limitations of existing systems that use offline transactions, such as the generation of fake offline tokens and the indivisibility of offline tokens. The user buys Offline Tokens (OTs) from a server called an Offline Token Manager (OTM) to use them later to perform offline transactions. Each mobile device must store a single, signed offline token transaction to prevent fake tokens. On the other hand, all offline transactions will be kept as a history in a particular local database. Finally, when the receiver becomes online, it will send a convert request to the OTM to change the value of the OTs to the appropriate amount in real coins. This step requires a connection to the Internet. To evaluate the effectiveness of the system, the Solidity programming language was used to develop a smart contract on the Ethereum blockchain with a backend application programming interface (API) and an android mobile application. The proposed method has an advantage over other prominent wallets.

Keywords: Mobile wallet; blockchain; smart contracts; digital signature

1 Introduction

Electronic payment using mobile wallets has spread widely in the last decade. However, it still faces difficulties in areas where people suffer from poor Internet coverage [1], particularly in rural areas and third-world countries. In addition, electronic payment methods are hard to use for day-to-day shopping and selling because they require a stable Internet connection.

There are numerous forms of E-Payment, such as credit cards, web wallets, and mobile wallets. These E-Payment forms need extensive personal information to complete payment transactions, which require an effective communications network infrastructure [2]. Mobile wallets have a broader appeal as they provide instantaneous access and have more significant potential for growth in consumers and suppliers [3]. However, mobile payment still has limitations that prevent it from being superior to a traditional cash payment in rural areas and third-world countries, most notably due to the lack of communication infrastructure. Conventional cash payment is still the prevalent payment method as it has the freedom of payment anytime and anywhere, which current mobile payment systems cannot achieve yet in rural areas.

This problem has been discussed in other papers, and multiple workarounds have been proposed; some suggested solutions based on the connectivity to satellite Internet, while others offered to complete the mobile payment through a cellular connection. But these solutions are expensive or unreliable. Others have suggested making the mobile payment when there is no connection and then completing and registering the transaction when the connection is back. However, these solutions were either not complete or not convincing.

The system proposed in this paper relies on blockchain technology to achieve mutability and non-repudiation. Furthermore, it provides secure mobile payment service even in the absence of a stable Internet connection. In such cases, the two parties to the payment will use Bluetooth for direct device connection and exchange digital content to carry offline transactions [4].

The system supposes that the buyer should obtain Offline Tokens (OT) in advance while they are online by contacting an Offline Token Manager (OTM). These OTs can be used to facilitate mobile payments by establishing a Bluetooth connection between the two parties involved in the transaction. The buyer will send the required amount of OTs to the seller, and the amount of OTs will be deducted from the buyer by the system and added to the seller once a connection has been restored.

Blockchain with Decentralized Ledger Technology (DLT) is used for storing transactions, as this technology's data integrity is a crucial advantage [5]. The system's core is a smart contract, a program stored in the blockchain [6] and used for a decentralized application paradigm. The smart contract will control the mobile payment process and check for completion conditions. An up-to-date list of all participants' public keys is kept in a local database on each user's mobile device, and each participant in the system has a unique pair of public and private keys. In addition, the two parties using the system will utilize digital signatures to verify the integrity of messages [7]. More details will provide about blockchain, smart contracts, Bluetooth, and digital signature technologies in Section 2.

The main contributions of this paper are as follows:

1. Provide a thorough introduction to the history of blockchain mobile wallet strategies for securing Offline Transactions.

2. Allows customers to make safe, convenient mobile payments even if they can't always connect to the Internet. Give an idea of how the offline token division problem can be fixed.

3. Propose Token forgery is a problem in the cryptocurrency industry. Thus, this research proposes a method for detecting forged tokens.

The rest of this paper is organized as follows: Section 2 describes the background of this research. Section 3 presents a review of some related works in the literature. Section 4 elaborates on the research problem and presents the proposed method. Finally, Section 5 offers the implementation and shows the experimental results.

2 Background

This section presents background information about the technologies used in this research, such as Bluetooth, Blockchain, Smart Contracts, and Digital Signatures.

2.1 Bluetooth

Bluetooth technology is a short-range radio link technology that allows neighboring users to exchange data. It is the most commonly used in proximity range for digital contact tracing apps [8]. Bluetooth provides low price, low power, ease of control, and invisible distance limitations [9]. If users are next to each other, they can exchange digital content without accessing the Internet; they want to use Bluetooth for that purpose. There is no license needed to use the Bluetooth operating frequency band. When Bluetooth turns on, it searches for other devices in the proximity range and sends signals [10]. Bluetooth is an alternative to data cables that lets nearby devices send and receive data over radio waves. It is also designed for connecting portable or fixed electronic devices. The range can cover approximately ten to twenty meters in length. Mainly, Bluetooth connections are used for Personal Area Networks (PANs) [11]. Ericsson started replacing the cables connecting mobile phone accessories with Bluetooth wireless connections in 1994 [9].

Several Bluetooth connections are used, such as point-to-point, Piconet, and ad-hoc or "scatternet" networks. The point-to-point connection enables two devices to connect. In contrast, the Piconet connection forms a small personal area network consisting of a master and, at most, seven active slaves [11]. Fig. 1 illustrates a Bluetooth Piconet Network connection in the manner of one master device with several slave devices. Finally, an ad-hoc or scatternet network consists of two or more Piconet networks connected using one of the bridge slaves. Fig. 2 depicts how two Piconet networks are combined to form a new network.

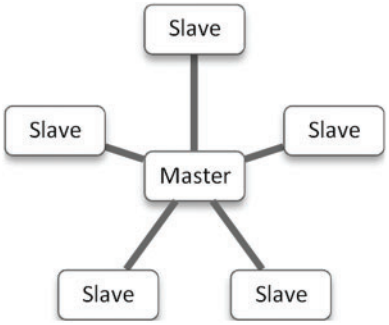


Figure 1: Bluetooth piconet network

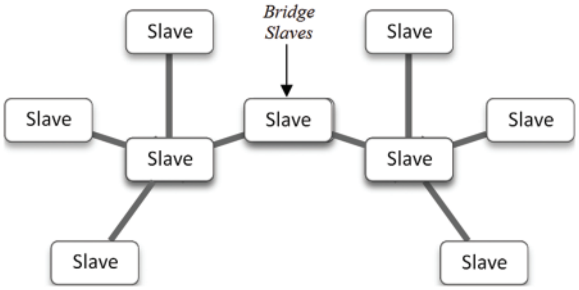


Figure 2: Bluetooth scatternet network

2.2 *Smart Contract*

The blockchain is a sequence of blocks that holds an entire list of transaction records, like a conventional public ledger. Fig. 3 illustrates an example of a blockchain structure. Each block points to the immediately previous block via a reference, essentially a hash value of the last block called the "parent block." It is worth noting that uncle block hashes (the children of the block's ancestors) would even be stored in the blockchain. The primary block of a blockchain is named the "genesis block," which has no parent block [12].

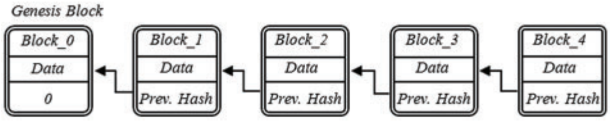


Figure 3: Bluetooth scatternet network

In 2008, Satoshi Nakamoto showed the first use of blockchain by presenting a peer-to-peer cash system with a cryptography-based distributed ledger [13–15]. This ledger contains all transactions done by the system users [6].

Blockchains can be categorized into different types according to their consensus mechanisms, such as public, private, and consortium. Public blockchains are open source and permit anybody to join as a client or network individual. Private blockchains, or permissioned blockchains, are chains for which membership approval is required to join the network [3]. A consortium blockchain is a hybrid blockchain in which two or more organizations govern the identical blockchain. It is not a public blockchain but rather a permissioned blockchain.

A small computer program stored on a blockchain, called a "smart contract," introduced by Nick Szabo, will execute a transaction under specified conditions [16]. Self-executing and transparent code is stored in the Ethereum blockchain's immutable ledger, which makes smart contract code impossible to modify. Furthermore, the smart contract guarantees that transactions between parties satisfy both parties' needs; otherwise, the transaction will not occur.

Blockchain systems serve as the basic platform for smart contracts, which automate the execution of software programs in a verifiable manner. One noteworthy example is Ethereum [17], the second most popular cryptocurrency after Bitcoin, which has grown in popularity due to its sophisticated smart contract capability [17].

A smart contract's life cycle begins with the parties writing the conditions of a contract on a distributed ledger. Next, the contract waits for preset criteria to be evaluated by external factors. Finally, the contract self-executes when criteria are met via triggers.

In a nutshell, smart contracts function as self-contained agents whose actions are predictable. As a result, smart contracts can assist parties that do not trust each other in entering into a contract without the assistance of a third party. Fig. 4 summarizes the essential features of smart contracts.

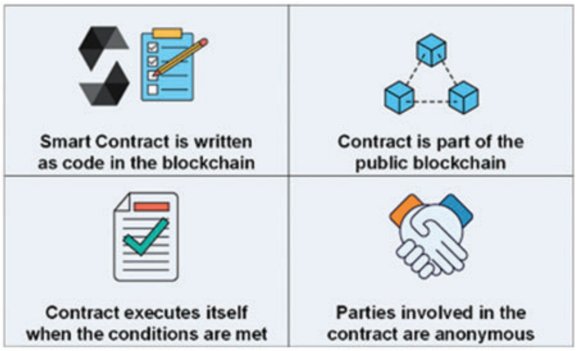

Smart Contract is written as code in the blockchain
Contract is part of the public blockchain
Contract executes itself when the conditions are met
Parties involved in the contract are anonymous

Figure 4: Smart contracts

2.3 Digital Signature

A digital signature is used to verify the data source and data integrity in a communication process (e.g., an email, a credit card transaction, or a digital document). During the verification process, a public, mutually-owned key is extracted from the signature and used to verify the signer's identity via the trusted certificate authority. In addition, it confirms that no changes have been made to the signed document since signing. The signer's public key, which is used to decrypt the signature, is also given to the document recipient. If the recipient cannot open the document using the signer's public key, it indicates something wrong with the document or the signature. Finally, the signature is created with the signer's private key, which is always kept securely with the signer [18].

3 Literature Review

Several types of research have been presented to discuss or create electronic wallets; some of these studies attempt to figure out the electronic wallet through offline transactions.

Authors in [19] offered a Pure Wallet architecture to use blockchain for offline transactions successfully. The primary addition that they have made to the architecture is the introduction of a token manager in the form of a smart contract responsible for managing offline tokens. Unfortunately, the Pure Wallet is built in a way that makes it impossible to split tokens and notify if a token is changed.

Authors in [20] proposed the use of hardware tokens to complete bitcoin transactions using Bluetooth technology and called it BlueWallet. They protect the private key inside the hardware token. An Internet connection is required to connect the blockchain network to conduct transactions. The proposed BlueWallet uses Elliptic Curve Digital Signature Algorithm (ECDSA) for transaction verification and signing. The Bitcoin network receives the transaction if it is observed as valid by the point of sale (POS). This process takes about 40 min to complete.

Authors in [21] proposed a card payment system using blockchain that reduces fees and protects the participants' privacy, especially personal identification details within the transaction. They used a centralized virtual ledger to control participants' access and encrypt transaction details and remove the need for a trusted middleman. An Internet connection is required to connect to the blockchain network and complete transactions.

The authors in [22] proposed a solution using a satellite receiver to solve problems with poor or nonexistent Internet connections. Unfortunately, this apparatus is cumbersome and stays put for the most part. Instead, a GoTenna is used to establish a mobile connection within a specific range to extend the connection established by the receiver. A device with a wallet is required to read the downloaded information. With this strategy, connections were made to fixed places that didn't have Internet access before.

Authors in [23] investigated the potential blockchain technology benefits for many types of financial institutions, such as banks, and presented a method for the policy specification and verification of financial transactions that are based on smart contracts. In [24], authors examined the similarities and differences between cryptocurrency and fiat currency and their function within the economy. They tried to figure out how the performance of peer-to-peer network transactions can be improved by using cryptocurrency as an alternative to fiat currency. Finally, they discussed the benefits and drawbacks of using cryptocurrency.

4 Proposed System

In areas with limited Internet access, mobile payments are still uncommon. Moreover, they are encountering many difficulties in performing Internet payments due to the lack of equipment and poor infrastructure of Internet networks. The best choice for overcoming this situation is to use Personal Area Networks (PAN) and direct communication through mobile devices. As mentioned in Section 3, the inability to create offline tokens and the indivisibility of offline tokens, which means they can only be sent as a whole, are two of the most significant obstacles that stand in the way of offline transactions. This paper presents a solution that will successfully overcome these two restrictions. As seen in Fig. 5, the architecture of the offline transaction can be broken down into four distinct parts. Four steps must be followed to perform offline transactions.

1. Client1 (sender) sends its real coins to the OTM in the online mode. Then, the OTM sends the same value to client1 as OTs to be used later in the offline mode.

2. Client1 sends the OTs to client2 (receiver) using the offline mode (i.e., Bluetooth or any peer-to-peer communication channel).

3. After the end of the offline mode, client2 sends the OTs to the OTM.

4. The OTM re-sends the value of OTs as real coins to the client2.

A preparation stage is added to the proposed system. In this stage, each client sends a connection request to OTM to obtain an updated public key database from OTM for all network participants. This stage would keep the database of public keys updated locally in the client's mobile device storage. This stage is mandatory to check the token's transfer identity during the offline mode. Fig. 6 depicts the preparation stage.

The proposed solution suggests four steps to achieve the offline transaction using a digital signature with a direct network connection:

1. Requesting OTs from OTM by the sender.

2. Requesting OTs from the sender by the receiver.
3. Offline Token Division.
4. Divided Offline Token Exchange.

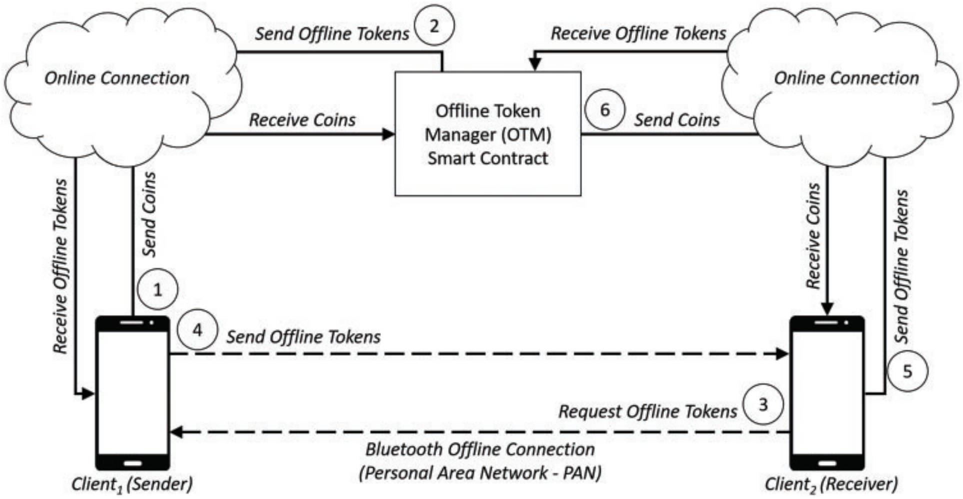


Figure 5: The architecture of the whole system used for e-wallet

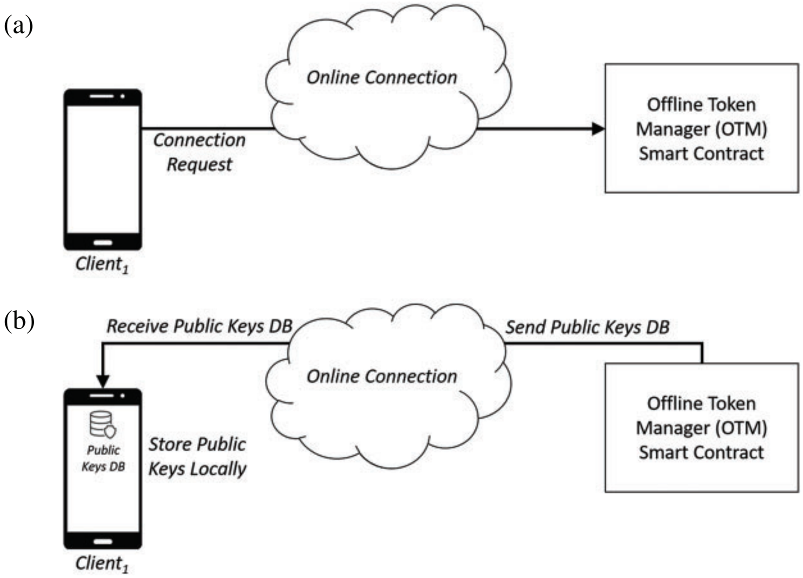


Figure 6: The preparation stage of the proposed system. (a) The client sends a connection request to OTM. (b) The client stores the public key database locally on the mobile device

4.1 Requesting OTs from OTM by the Sender

The first step starts with the client, who sends a request for some OTs from the OTM. The token manager responds to the request by transferring the requested tokens in a signed transaction using the OTM private key as in (1) through an Internet connection. The OTM's signed transaction must be stored locally on the sender's mobile in the OT's storage area. This transaction should be kept as a single transaction to prevent deleting the last transaction without detecting that in the case of using multiple transactions. The signed transaction is depicted in Fig. 7.

$$OTM_{priv}\,(from\colon\, OTM, to\colon\, Client_1, amount\colon\, NOTs) \tag{1}$$

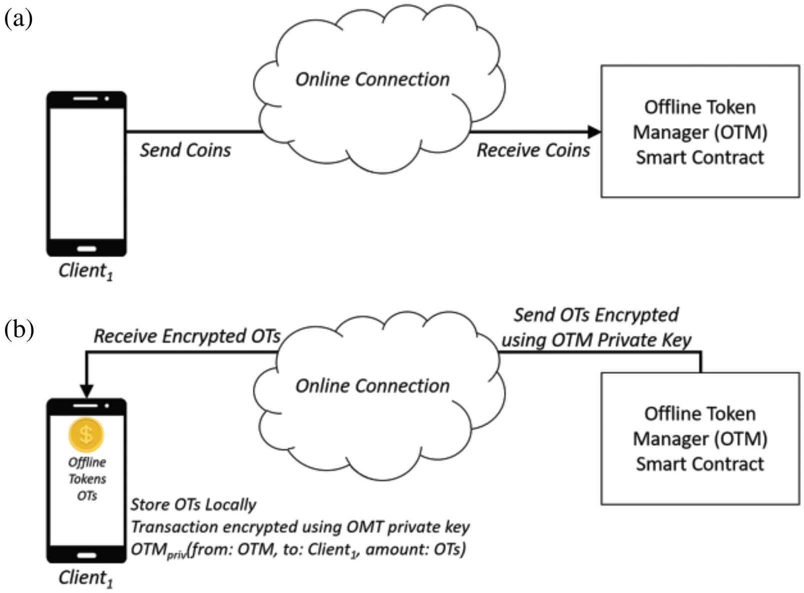

(a)
Online Connection
Send Coins
Receive Coins
Offline Token Manager (OTM) Smart Contract
$Client_1$
(b)
Receive Encrypted OTs
Send OTs Encrypted using OTM Private Key
Online Connection
Offline Token Manager (OTM) Smart Contract
$
Offline Tokens OTs
Store OTs Locally
Transaction encrypted using OMT private key
OTM_{priv}(from: OTM, to: $Client_1$, amount: OTs)
$Client_1$

Figure 7: (a) The client sends real coins to the OTM. (b) The client receives the signed OTs and stores them locally on the mobile device

4.2 Requesting OTs from the Sender by the Receiver

In this stage, the receiver requests some OTs from the sender. Then the sender sends the OTs transaction signed using the OTM private key to the receiver. After that, the receiver decrypts the OTs transaction using the OTM public key to identify the transaction identity and prevent the OTs fabrication as shown in Fig. 8. A peer-to-peer connection is established in this stage without an Internet connection.

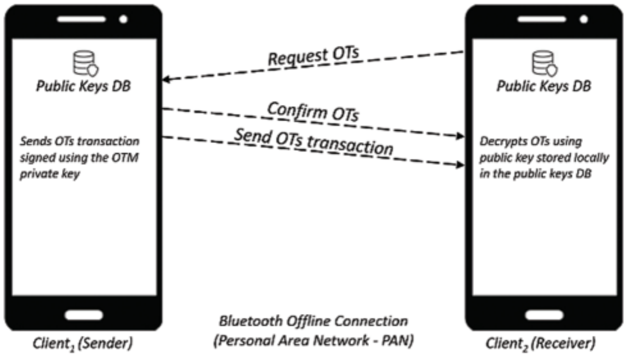

Public Keys DB
Sends OTs transaction signed using the OTM private key
Request OTs
Confirm OTs
Send OTs transaction
Public Keys DB
Decrypts OTs using public key stored locally in the public keys DB
$Client_1$ (Sender)
Bluetooth Offline Connection (Personal Area Network - PAN)
$Client_2$ (Receiver)

Figure 8: Requesting OTs from the sender by the receiver

4.3 Offline Token Division

In the third stage, the receiver divides the offline tokens according to the payment amount and sends a pull-token value request to the sender. Then, the sender sends confirmation for this request, as depicted in Fig. 9.

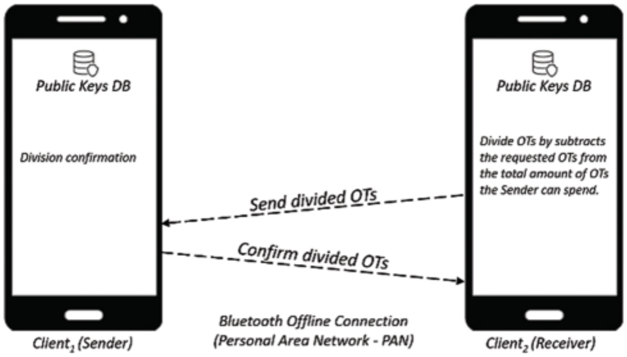

Public Keys DB
Division confirmation
Public Keys DB
Divide OTs by subtracts the requested OTs from the total amount of OTs the Sender can spend.
Send divided OTs
Confirm divided OTs
Bluetooth Offline Connection
(Personal Area Network - PAN)
Client1 (Sender)
Client2 (Receiver)

Figure 9: The offline mode between the sender and the receiver

4.4 Divided Offline Token Exchange

In the fourth step, the sender and the receiver exchange the signed offline tokens transactions. The receiver decrypts the new transaction using a private key in Eq. (2). On the other hand, the sender signs the transaction using the private key in Eq. (3), where N is the number of OTs, which will be divided into M1 and M2, so N = M1 + M2. Fig. 10 depicts the new transactions exchange in the fourth step.

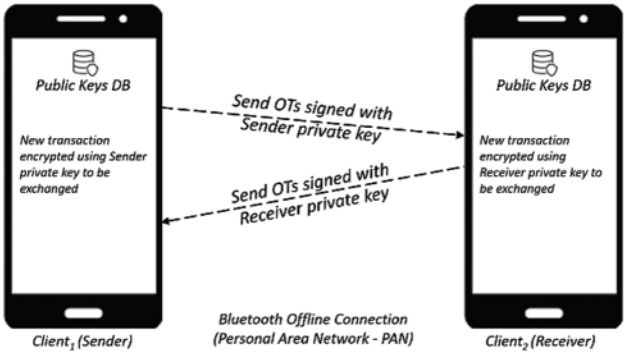

Public Keys DB
New transaction encrypted using Sender private key to be exchanged
Public Keys DB
New transaction encrypted using Receiver private key to be exchanged
Send OTs signed with Sender private key
Send OTs signed with Receiver private key
Bluetooth Offline Connection
(Personal Area Network - PAN)
Client1 (Sender)
Client2 (Receiver)

Figure 10: The new transactions exchanged in the fourth step

As mentioned, a single signed offline token transaction must be stored in each mobile device to prevent falsified tokens. But all offline transactions will be stored locally in a particular database as transaction history. Fig. 11 depicts the structure of the single signed offline token transaction.

$$Client_{2_{priv}}(OTM_{priv}(from\colon\ OTM, to\colon\ Client_1, amount\colon\ NOTs)+(from\colon\ Client_2, to\colon\ Client_1, amount\colon\ M_1 OTs)) \tag{2}$$

$$Client_{1_{priv}}(OTM_{priv}(from: OTM, to: Client_1, amount: NOTs) + (from: Client_1, to: Client_2, amount: M_2OTs)) \quad (3)$$

Finally, when the receiver becomes online, it will send a convert request to the token manager to change the value of the OTs to the appropriate amount in actual coins. At this stage, an Internet connection is required.

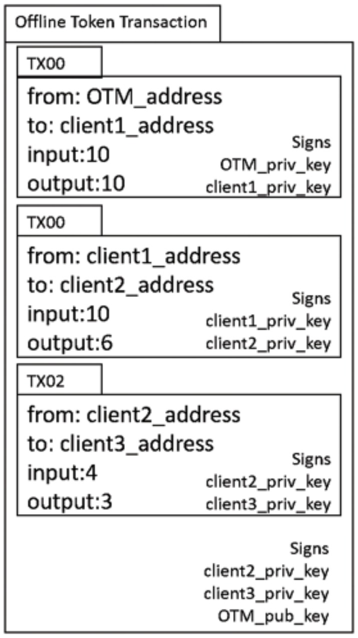


Figure 11: Exchange transactions in the fourth step

4.5 System's Key Algorithm

In this section, the algorithm is presented for the preparation stage and each of the four stages of the proposed solution, as shown in Algorithm 1.

The sender submits a connection request to OTM. OTM accepts the connection request and updates the public key database. The sender receives an up-to-date copy of OTM's database and maintains its database on its local machine. Then, the sender sends actual coins to the receiving wallet. OTM signs the OTs transaction using its private key. When the sender receives the signed OTs transaction, it keeps a copy. While the receiver has no Internet connection, it contacts the sender to obtain the signed OTs. Then, the receiver decrypt the OTs transaction using the OTM public key. The OTs are partitioned by the receiver based on the total amount of the payment. The pull OTs value request is transmitted from the receiver to the sender. The request made by the receiver is met with a confirmation from the sender. The new OTs transaction is decrypted by the receiver using its private key. The sender used its private key to decrypt the new OTs transaction. The new signed OTs transaction is sent to the recipient by the sender. In turn, the receiver transfers the new signed OTs transaction to the sender. If the Internet connection is lost, the receiver sends signed OTs transaction to OTM, which checks the OTs transaction and sends actual coins back to the receiver.

5 Implementation

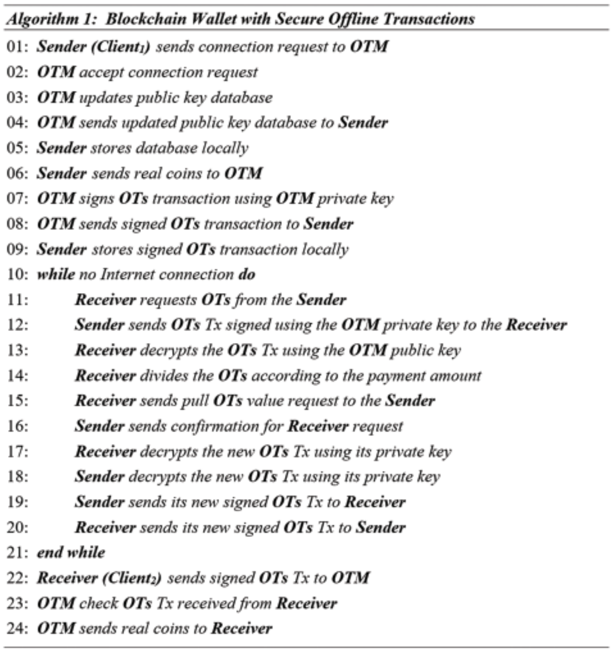
This section discusses the three main components that make up the system's implementation: the smart contract TokenManager, the mobile wallet implemented as an Android application, and the backend API the source code of the system is available in [25]. A comprehensive mobile wallet was developed as a mobile application to validate the suggested method. The mobile wallet connects to the Ethereum smart contract on the Ropsten test network.

5.1 Token Manager Smart Contract

The $TokenManager$ was built component in Solidity with the help of the Ethereum Remix, and it was then deployed on the Ropsten Ethereum test net. The smart contract contains a constructor and three functions, referred to as $transferToClient$, $transferToOTM$, and $_transfer$. In the constructor, the complete supply of OT will be deposited into the account of the contract owner, who also created the contract. Two distinct transferring functions was constructed: the first one is called $transferToClient$, and it is used to move tokens from the Token Manager to the clients. The second function, $transferToOTM$, is used to move tokens from the clients to the Token Manager. The final function, $_transfer$, is responsible for updating the account balances whenever tokens are transferred.

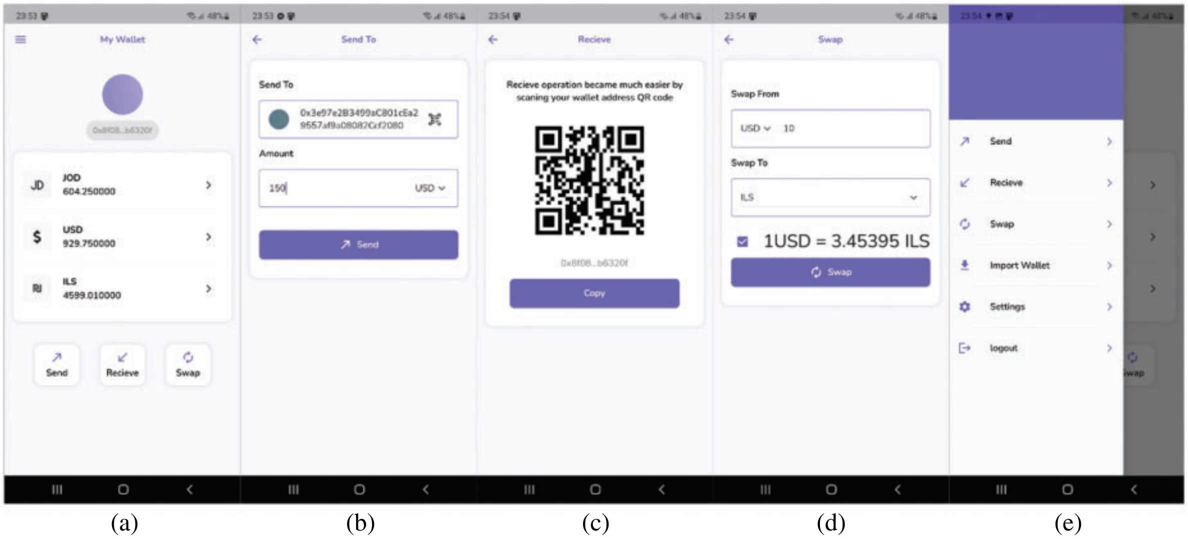
5.2 Mobile Wallet

A straightforward mobile application is developed with Android Studio to carry out the primary functions of a mobile wallet. This included displaying the account balances in various currencies, such as the United States dollar and the Saudi Riyal. Another set of functions is added to mobile wallets, including the ability to send and receive money and exchange currency amounts. The user interface of the mobile wallet is shown in Fig. 12.



```
Algorithm 1: Blockchain Wallet with Secure Offline Transactions
Sender (Client$_1$) sends connection request to OTM
OTM accept connection request
OTM updates public key database
OTM sends updated public key database to Sender
Sender stores database locally
Sender sends real coins to OTM
OTM signs OTs transaction using OTM private key
OTM sends signed OTs transaction to Sender
Sender stores signed OTs transaction locally
while no Internet connection do
    Receiver requests OTs from the Sender
    Sender sends OTs Tx signed using the OTM private key to the Receiver
    Receiver decrypts the OTs Tx using the OTM public key
    Receiver divides the OTs according to the payment amount
    Receiver sends pull OTs value request to the Sender
    Sender sends confirmation for Receiver request
    Receiver decrypts the new OTs Tx using its private key
    Sender decrypts the new OTs Tx using its private key
    Sender sends its new signed OTs Tx to Receiver
    Receiver sends its new signed OTs Tx to Sender
end while
Receiver (Client$_2$) sends signed OTs Tx to OTM
OTM check OTs Tx received from Receiver
OTM sends real coins to Receiver
```

The screen in Fig. 12a is the primary screen that displays the account balances. The screen in Fig. 12b is used to send any amount of existing currencies to another wallet address. In the third screen, Fig. 12c, the account address and the QR code for the amount received used to be displayed. The interface for exchanging currencies can be found on the fourth screen, as in Fig. 12d. Finally, the mobile wallet application menu is on the screen's extreme right, as shown in Fig. 12e.



Send To: 0x3e97e2B3499aC801cEa29557af9a08082Ccf2080

Amount: 150 USD

Recieve operation became much easier by scaning your wallet address QR code

0x8f08...b6320f

Swap From: USD 10

Swap To: ILS

☑ 1USD = 3.45395 ILS

(a) (b) (c) (d) (e)

Figure 12: Graphical user interface of the mobile wallet application

The mobile wallet uses the Internet connection to perform the essential wallet functions, and it uses the Bluetooth direct connection to complete the offline token exchange. In addition, the public key database is stored as a JavaScript Object Notation (JSON) file locally on the mobile device.

As described in Section 4, a single transaction is saved locally on the mobile device in the form of a JSON file. The JSON file is made up of an array called "transactions" that stores the history of all transactions, a hash of the transactions array, and a signed hash that is signed with the private key of the sender, the private key of the receiver, and the public key of the offline token manager. The following components make up each transaction in the transaction history:

1. The moment the transaction was initially created (timestamp).
2. The tokens are sent from the address associated with the account (from).
3. The tokens are sent to the address of the account receiving them (to).
4. The amount of the sender's account's remaining token balance at the time of the transaction (input).
5. The total number of tokens the receiver has drawn (output).
6. The transaction's unique identifier or hash (hash).
7. A hash signed in 6 using the sender's private key (sign hash using private key "from").
8. A hash value that has been signed using the receiver's private key (sign hash using private key "to").

5.3 Backend API

The backend implementation is carried out with the assistance of Node.js, which serves as an asynchronous, event-driven JavaScript runtime. The Node.js web server is an intermediary between the mobile wallet application and the smart contract [26]. The primary objective of this implementation component is to make it easier for the various parts of the system to communicate with one another. API is implemented so that HTTP requests can be called from within the mobile application. The backend implementation relies heavily on the package's ethers, web3, and express as its key components. This backend was used to link the deployed smart contract. The smart contract features include the Application Binary Interface, often known as ABI [27].

5.4 Results Discussion

In this subsection, this paper outlines the key distinctions between numerous systems stated in the literature and the system suggested. Offline, token divisibility, cost, mobility, and multi-offline transactions are used in this comparison as advantageous features, whereas token tampering is used as an unfavorable attribute. Offline refers to the absence of an Internet connection during the transaction process. Token divisibility is the ability to divide tokens. The cost is the cost of the hardware, if required. Multi-offline transactions are the ability to conduct multiple transactions in offline mode with multiple peers at the same time. Finally, token tampering is the capability of modifying tokens during the offline transaction process.

After analyzing the four solutions described in the literature and our proposed system, we have determined that Pure Wallet is capable of offline operation, has no hardware requirements, and is mobile but cannot prevent token tampering. BlueWallet and Card Payment support token divisibility and are portable, but they cannot function offline and incur hardware expenses. The Hackernoon can work offline and perform several transactions without an Internet connection, but it is not movable and challenging to maneuver. The proposed system has the advantage over all others since it can operate offline, allows token divisibility, requires no hardware, is mobile, can complete many offline transactions, and prevents token tampering. The advantages of the proposed system compared to other systems are shown in Table 1.

Table 1: Comparison of different eWallet systems

System	Hardware needed	Block chain-based	Offline	Token divisibility	Cost	Mobility	Multi offline Tx	Token tampering
Pure wallet [19]	No	Yes	Yes	No	No	Yes	No	Yes
Bluewallet [20]	Yes	Yes	No	Yes	Low	Yes	No	No
Card payment [21]	Yes	Yes	No	Yes	Low	Yes	No	No
Hackernoon [22]	Yes	Yes	Yes	Yes	Very high	No	Yes	No
Proposed system	No	Yes	Yes	Yes	No	Yes	Yes	No

6 Conclusion

Mobile payments are still tricky to use in places with limited Internet access due to a lack of equipment and a poor Internet network architecture.

This paper proposes an offline blockchain-based mobile wallet to provide a secure mobile payment service. It was developed to solve the limitations of several surveyed systems, like the ability to produce fake offline tokens and the indivisibility of offline tokens. Our system provides a secure mobile payment service to users without access to a reliable Internet connection. It makes a suggestion for how the divisibility of offline tokens can be resolved and makes a suggestion for a technique that can identify fake tokens. Using Ethereum smart contract, Bluetooth, and digital signature technologies to build the wallet.

The proposed offline transaction is divided into five steps: the sender sends the real coins to the OTM in the online mode, then the OTM sends the same value to the sender as OTs to be used later in the offline mode. After that, the sender sends the OTs to the receiver offline. Finally, when the offline mode ends, the receiver sends the OTs to the OTM, which resent the value of the OTs as real coins to the receiver.

An Android application has been implemented to verify the concept of the proposed offline wallet. Comparisons with other systems showed that our system performed the offline transactions in a better and more secure manner and overcame the two previously mentioned limitations of the other methods.

Funding Statement: The researchers would like to thank the Deanship of Scientific Research, Qassim University, for funding the publication of this project.

Conflicts of Interest: The authors declare that they have no conflicts of interest to report regarding the present study.

References

[1] A. AbuSamra, K. Elbatsh and A. Hassan, “Gaza wallet: A simple and efficient blockchain application,” in *Proc. 1st Int. Conf. on Information Technology & Business ICITB2020*, Gaza, Palestine, pp. 1–7, 2020.

[2] A. N. Mian, A. Hameed, M. U. Khayyam, F. Ahmed and R. Beraldi, “Enhancing communication adaptability between payment card processing networks,” *IEEE Communications Magazine*, vol. 53, no. 3, pp. 58–64, 2015.

[3] T. A. Khan, A. T. Hasan, Q. Jiang and Q. Qu, “A hybrid blockchain-based zero reconciliation approach for an effective mobile wallet,” in *Proc. 2nd Int. Conf. on Sustainable Technologies for Industry 4.0 (STI)*, Dhaka, Bangladesh, pp. 1–6, 2020.

[4] S. Sudin, R. B. Ahmad and S. Z. S. Idrus, “A model of virus infection dynamics in mobile personal area network,” *Journal of Telecommunication, Electronic and Computer Engineering (JTEC)*, vol. 10, no. 2, pp. 197–201, 2018.

[5] P. Urien, “Innovative countermeasures to defeat cyber attacks against blockchain wallets,” in *Proc. 5th Cyber Security in Networking Conf. (CSNet)*, Abu Dhabi, United Arab Emirates, pp. 49–54, 2021.

[6] B. K. Mohanta, S. S. Panda and D. Jena, “An overview of smart contract and use cases in blockchain technology,” in *Proc. 9th Int. Conf. on Computing, Communication and Networking Technologies (ICCCNT)*, Bengaluru, India, pp. 1–4, 2018.

[7] W. Fang, W. Chen, W. Zhang, J. Pei, W. Gao *et al.,* “Digital signature scheme for information non-repudiation in blockchain: A state-of-the-art review,” *Journal on Wireless Communications and Networking*, vol. 56, no. 1, pp. 1–15, 2020.

[8] S. M. Idrees, M. Nowostawski and R. Jameel, "Blockchain-based digital contact tracing apps for COVID-19 pandemic management: Issues, challenges, solutions, and future directions," *Medical Informatics*, vol. 9, no. 2, pp. 1–29, 2021.

[9] M. Mahajan, G. Verma, G. Erale, S. Bonde and D. Arya, "Design of chatting application based on android bluetooth," *International Journal of Computer Science and Mobile Computing (IJCSMC)*, vol. 3, no. 3, pp. 712–717, 2014.

[10] R. Verma, R. Gupta, M. Gupta and R. Singh, "A complete study of chatting room system based on android bluetooth," *International Journal of Emerging Technology and Advanced Engineering*, vol. 4, no. 1, pp. 135–141, 2014.

[11] A. Bhat and A. Jain, "Bluetooth network security," *Journal of Analysis and Computation (JAC)*, vol. 14, no. 6, pp. 1–7, 2020.

[12] Z. Zheng, S. Xie, H. N. Dai, X. Chen and H. Wang, "Blockchain challenges and opportunities: A survey," *International Journal of Web and Grid Services*, vol. 14, no. 4, pp. 352–375, 2018.

[13] S. Nakamoto, "Bitcoin: A peer-to-peer electronic cash system," Technical Report, 2009. [online]. Available: https://bitcoin.org/bitcoin.pdf

[14] R. Rasheed, R. Bulbul and M. Mikki, "Bluetooth Text Messages Integrity Security (BTMIS) based on blockchain," *American Journal of Electrical and Computer Engineering*, vol. 6, no. 2, pp. 54–60, 2022.

[15] M. Obaid, M. Aqel and M. S. Obaid, "Mobile payment using blockchain security," *Journal of Applied Science and Engineering*, vol. 24, no. 4, pp. 687–692, 2021.

[16] N. Szabo, "Formalizing and securing relationships on public networks," *First Monday*, vol. 2, no. 9, pp. 1–21, 1997.

[17] V. Buterin, "A next-generation smart contract and decentralized application platform," Technical Report, 2014. [Online]. Available: https://ethereum.org/669c9e2e2027310b6b3cdce6e1c52962/Ethereum_Whitepaper_-_Buterin_2014.pdf

[18] J. Katz and Y. Lindell, *Introduction to Modern Cryptography*. CRC press: Boca Raton, Florida, USA, pp. 107–120, 2020.

[19] I. S. Igboanusi, K. P. Dirgantoro, J. M. Lee and D. S. Kim, "Blockchain side implementation of Pure Wallet (PW): An offline transaction architecture," *ICT Express*, vol. 7, no. 3, pp. 327–334, 2021.

[20] T. Bamert, C. Decker, R. Wattenhofer and S. Welten, "Bluewallet: The secure bitcoin wallet," in *Proc. Int. Workshop on Security and Trust Management*, Wroclaw, Poland, pp. 65–80, 2014.

[21] S. Anderwald, D. Godfrey-Welch, R. Lagrois, J. Law and D. Engels, "Blockchain in payment card systems," *SMU Data Science Review*, vol. 1, no. 1, pp. 1–44, 2018.

[22] Hackernoon, "Completely offline bitcoin transactions," 2019. [Online]. Available: https://hackernoon.com/completely-offline-bitcoin-transactions-4e58324637bd

[23] D. Unal, M. Hammoudeh and M. S. Kiraz, "Policy specification and verification for blockchain and smart contracts in 5G networks," *ICT Express*, vol. 6, no. 1, pp. 43–47, 2020.

[24] M. R. Islam, R. M. Nor, I. F. Al-Shaikhli and K. S. Mohammad, "Cryptocurrency *vs.* Fiat currency: Architecture, algorithm, cashflow & ledger technology on emerging economy: The influential facts of cryptocurrency and fiat currency," in *Proc. Int. Conf. on Information and Communication Technology for the Muslim World (ICT4M)*, Kuala Lumpur, Malaysia, pp. 69–73, 2018.

[25] R. Rasheed, "eWalletOfflineTx," [Online]. Available: https://github.com/raedrasheed/eWalletOfflineTx Accessed 3-June, 2022.

[26] G. Saldamli, V. Reddy, K. S. Bojja, M. K. Gururaja, Y. Doddaveerappa *et al.,* "Health care insurance fraud detection using blockchain," in *Proc. Seventh Int. Conf. on Software Defined Systems (SDS)*, Paris, France, pp. 145–152, 2020.

[27] L. Nimer and A. Tahat, "Implementation of a peer-to-peer network using blockchain to manage and secure electronic medical records," in *Proc. IEEE Jordan Int. Joint Conf. on Electrical Engineering and Information Technology (JEEIT)*, Amman, Jordan, pp. 187–192, 2021.