KICS The Korean Institute of Communications and Information Sciences

Available online at www.sciencedirect.com

ScienceDirect

ICT Express 7 (2021) 327–334

www.elsevier.com/locate/icte

Blockchain side implementation of Pure Wallet (PW): An offline transaction architecture

Ikechi Saviour Igboanusi, Kevin Putra Dirgantoro, Jae-Min Lee, Dong-Seong Kim*

Networked System Laboratory, Department of IT Convergence Engineering, Kumoh National Institute of Technology, Gumi, South Korea

Received 19 January 2021; received in revised form 22 June 2021; accepted 2 August 2021
Available online 20 August 2021

Abstract

This article proposes an electronic payment architecture named Pure Wallet (PW), which extends the concept of Blockchain cryptocurrency for offline transactions. The process is divided into three steps. The first step requires the use of Internet connection, to convert cryptocurrency into a token at the token manager. The token manager initiates a transaction that requires the information in the token to complete. Then offline transactions step is performed between electronic devices like mobile phones through a secure Near Field Communication (NFC) using the token in senders device. The financial value in the form of a token is encrypted by the sender and sent to the receiver's device via NFC. In the third step, the receiver converts the received token into cryptocurrency in the presence of Internet connection by sending the information required to complete the transaction to the token manager. The goal is to propose an electronic payment architecture utilizing Blockchain, which will enable financial transactions without instant connection to the Internet. The Blockchain implementation in this work utilizes smart contract in Ethereum Blockchain. The result shows a successful transfer of value without instant Internet connection. The open issues related to Blockchain in offline transactions are listed for further research works.

Keywords: Blockchain; Cryptocurrency; e-wallet; Near Field Communication (NFC); Offline transaction; Pure Wallet (PW); Smart contract

1. Introduction

The need for daily financial transactions has led to the development of several electronic payment systems that have made exchange of values relatively easier compared to the traditional means. But, doing so requires financial institutions and presence of heavy communication equipment to do this efficiently. The transactions using payment cards expose a lot of personal information to all the entities that participate in the transaction [1]. As mobile phones are taking most of the functions like complimentary card, identification, and credit/debit card to name a few, it still has many limitations in its current form for global adoption. The beauty of traditional cash transactions is the freedom to spend money anywhere, at any time, with whoever wants the legal tender, and this is something the phone is yet to achieve.

The concept of Blockchain has been invented to remove restrictions posed on financial transactions by financial institutions. This Blockchain paradigm is especially popular for financial transactions, but is also becoming popular for non-financial purposes, popularly for wireless networks [2]. Cryptocurrency has emerged to create a decentralized banking system, where no financial institution controls the money. Cryptocurrency is a kind of virtual currency that uses cryptography to protect transactions [3]. Before the introduction of cryptocurrency, two factors determine the success of an electronic transaction namely; financial institution and Internet connection. With the introduction of cryptographic payment like Bitcoin and Ethereum, the role of financial institutions has been successfully eliminated. But the need for instantaneous connection to Internet to enable Blockchain transaction is still a limitation of the current architecture. The existing Blockchain methods require Internet connection at the moment of transaction, limiting for global adoption.

Researchers have made efforts to create an offline cryptocurrency. Though cryptocurrency is protected with cryptographic encryption, a Blockchain device is prone to unauthorized hacking. In [4] authors proposed BlueWallet which

* Corresponding author.
E-mail addresses: ikechisaviour@gmail.com, dskim@kumoh.ac.kr (D.-S. Kim).

Peer review under responsibility of The Korean Institute of Communications and Information Sciences (KICS).

https://doi.org/10.1016/j.icte.2021.08.004

uses hardware token for completing transactions. This approach succeeded in keeping the private key (in hardware) offline, making the wallet secure, but it still requires point of sale (POS) Internet connection to the Blockchain network to make transactions. This approach uses Elliptic Curve Digital Signature Algorithm (ECDSA) for verification and signing of transactions. The transaction is introduced into the Bitcoin network if observed as valid by the POS. Other peers in the network in due course will verify and confirm the transaction before it is added to the Bitcoin network. The ledger of a Bitcoin network is the end point of every confirmed Blockchain transaction. It takes between 10 and 40 min to complete this process.

In [5], the authors proposed the use of Blockchain in the card payment system. This is to reduce charges from financial institutions incurred by merchants for using payment cards and to protect sensitive information especially personal identification details of the participants during transaction. The Blockchain has a centralized virtual ledger which controls access of participants, saves and encrypts transaction details, removes the need for a trusted middleman, and limits exposure of information. A merchant local payment machine is able to determine at once if a card from a customer can complete a transaction within limits of the payment card terms. The available amount is saved to the Blockchain ledger and the last information time update is obtainable, otherwise the system will refresh if the available information is outdated. Despite the contributions of this work, the authors did not consider their Blockchain solution for offline transactions.

Authors in [6] explored the use of hardware to create a wireless mesh connection, with other device users to overcome the problem of poor or no Internet connection, for Bitcoin transactions. In this case, several equipments are needed to complete the setup. A block stream satellite receiver is installed to download block chain data from the satellite. This device is bulky and mostly stationary. To extend the connection from the receiver, a GoTenna mesh is used to create a mobile connection within a limited range. A device with a wallet is also required to read the downloaded information. To create a means for up-link, other sets of equipment are required. This approach succeeded in extending connection to fixed areas without internet access. However it has the limitation of cost and mobility, because the hardware is costly, must be at a certain range from other users to function, and is considerably bulky for mobile use.

The works in [7] explore the use of NFC enabled android mobile for Bitcoin transactions. In their work, the receiver sends its account address to the sender using an NFC connection. The transfer of Bitcoin follows the conventional process requiring an Internet connection, and takes the same length of time as regular transaction.

Authors in [8] explore the opportunities of blockchain for banking and other financial institutions. The authors of [9] compared cryptocurrency and fiat currency, and their role in the economy. Their attempt is to figure out how cryptocurrency improves fiat currency in terms of its performance of peer-to-peer network transactions. It pointed out the pros and cons of cryptocurrency. Authors of [10] proposed the combination of Ethereum and IoTeX miner to shorten the transaction time in IIoT. The same authors proposed the use of non difficulty proof in [11] to reduce the transaction time. Works in IIoT as presented in [12] focused on privacy and security of cryptocurrency mobile applications. It examines Android cryptocurrency and financial services applications and the underlying security profile. After examining the common vulnerability, they reported that in terms of privacy, the financial service applications are better and are still better (though marginally) than cryptocurrency in terms of security provisions. Authors of [13] proposed Multi-Factor Authentication (MFA) which tries to improve cryptocurrency security. MFA approach is hinged on time-based one-time based password (TOTP), which is found to provide a more secure transaction. The authors in [14] demonstrated security-enabled near field communication tags using flexible architecture supporting cryptography. This is to solve the security problem of NFC by using symmetric and asymmetric cryptocurrency architecture.

The motivation of this work is to propose an architecture that will function without instant connection to the internet. As all transactions must be made with Internet connection, it renders cryptocurrency unfit for transactions in places like rural areas, in aeroplanes (on flight) and even in case of sudden disconnection by Internet providers. The concept of offline crypto transaction was introduced in [15] as Pure Wallet (PW). The scope of this work is to implement the Blockchain aspect of PW. This article will use the concept of cryptocurrency payment systems to explain the proposed algorithm. This algorithm can also be applied in other Blockchain applications such as in IoT and conducting electronic elections. It is a combination of three steps; first is an online step, then an offline, and finally another online step. Internet connection is required during the two online steps and NFC is required for the offline step of the transaction. Pure wallet (PW) proposes a solution not as a replacement to the existing Internet based architecture, but as an extension to enable offline cryptocurrency transaction, for a more rapid adoption and users convenience.

As a brief summary, the innovation and contributions of this work include the following:

1 PW introduces Blockchain for offline use cases.
2 A new token capable of offline transfer is introduced.
3 Token is time sensitive for security and avoidance of double spending.
4 Introduces the concept of token manager.
5 We implemented the blockchain aspect of PW to validate the proposed idea.

The rest of this article is arranged as follows: Section 2 presents the proposed Pure Wallet system model. Section 3 shows the Blockchain side implementation of the Pure Wallet and the results are shown in Section 4. The expected benefit of the proposed approach is presented in Section 5. And finally the conclusion and future work are in Section 6.

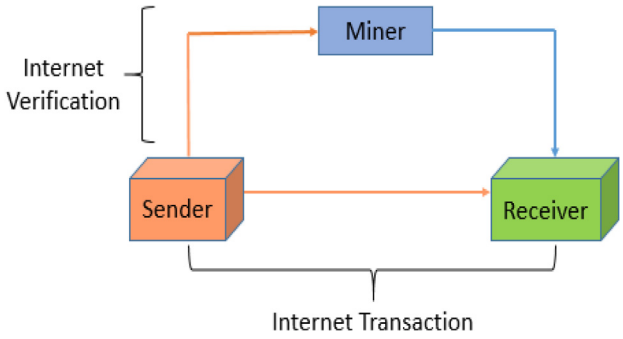

Fig. 1. Conventional Blockchain architecture showing what happens when a sender sends money to a receiver, and what happens at the back-end from the sender through the miner to the receiver. It also shows activities requiring Internet access.

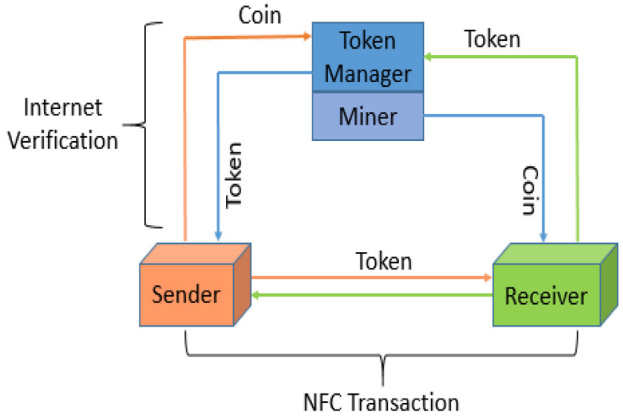

Fig. 2. Shows the block diagram of the proposed PW Blockchain architecture. The sender sends a token through NFC connection to the receiver. The verification process happens over the Internet connection through the token manager and the miner.

2. System model

Using the insight of the above discussed works, this article proposes Pure Wallet, an architecture to perform offline and real-time cryptocurrency transaction. The coin in the presence of Internet connection is converted into a token transferable over an NFC mobile connection. The receiver device retrieves the token value in the presence of an Internet connection. We assumed that the mobile application has the capacity to identify if a co-transacting device is legitimate or not. Consider a need to make payment on-board an aeroplane, the only possible payment is using cash, which has no equivalent in cryptocurrency following its current form. To make this kind of transaction possible there has to be a sort of value that is transferable during an offline situation. To achieve a secure transaction, digital cash in the form of a trusted secret token is needed.

2.1. PW Digital Cash architecture

To achieve offline electronic transactions, it is necessary to create a form of value transfer system which works efficiently without instant connection to the Internet. Fig. 1 illustrates a conventional Blockchain architecture. Fig. 2 shows the configuration of PW Blockchain architecture including the conversion process from crypto coins to electronic token at the sender (payer) account and vice versa at the receivers (payee) end. This conversion process at token manager can only take place when there is Internet connection. The token manager resides in the network. Any transactions through the token manager is seen in the network as a transaction that has been initiated but is yet to be completed. The token is transferred from a sender to a receiver over an Near Field Communication (NFC). The receiver uses that token to retrieve the coin value from the token manager. The PW algorithm is represented in Algorithm 1. A token is valid for transfer at the senders device within a certain time T_s, and for only one transaction. Received token can only be sent to the Token Manager, which implies that a receiver cannot send it into a new account. A time T_r is given for the receiver to claim the value of the received token. If the sender device does not make any transaction before T_s, it will have to wait for T_t before the token can be reconverted to crypto coins. After T_t the unclaimed coins will return to the sender's account.

$$T_s + T_r \leq T_t \tag{1}$$

The token manager holds all the token submitted by all payees until time T_t. The token manager completes all transactions associated with a token generated during one coin-token conversion, before returning the balance of unused token to the sender's coin account. This is meant to prevent the chance of double redemption by the payee.

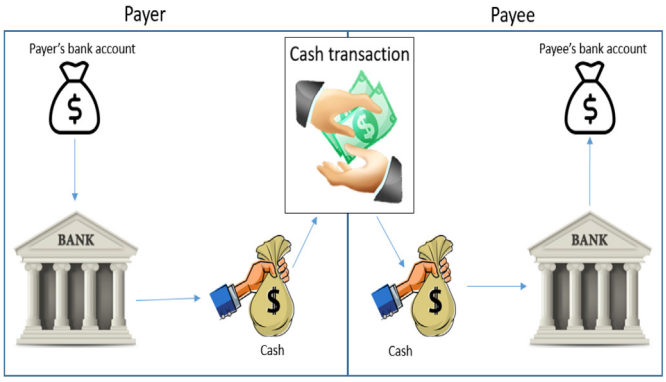

Fig. 3. The process of making a cash transaction involving withdrawal of money from the payer's bank account. The physical cash is used for transactions and the payee deposits the money in a bank account.

2.2. Real cash versus PW Digital cash

The process of using cash for transactions is a traditional means as illustrated in Fig. 3. Before a transaction is made, the payer withdraws cash from a bank account. During the transaction, the cash is handed over in exchange for a good or service. The cash is taken to the bank and deposited into an account by the payee. A similar process is mimicked in PW for offline transactions, but instead of physical cash a token is used. PW processes are illustrated in Fig. 4, to show its similarity with cash transaction as shown in Fig. 3.

Algorithm 1: Pure Wallet (PW) processes

```
Sender sends coin to Token Manager (TM) via Internet access
sender receives token via Internet access
while Transaction is in offline do
    Sender initiates a hands shake
    receiver sends acknowledgment
    receiver pulls token from sender
    sender confirms amount
    sender transfers the token
    receiver checks value and authorization on token
    receiver removes any duplicate of sent token from the sender's account
    receiver confirms receipt and terminate transaction
end
Receiver sends token to TM
TM forwards the transaction to miners for mining
Receiver receives the coin
```

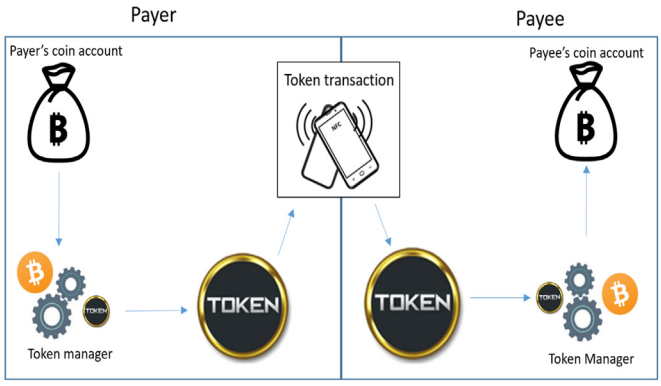

Fig. 4. Proposed PW Blockchain architecture showing the process of payment from the payer to the payee using a token over an NFC connection. The token mimics the role of cash in cash transactions.

2.3. Near Field Communication (NFC)

To transfer the token without Internet connection, there must be a close range communication between the receiver and sender. It is important for this transfer of token to happen under a secure condition capable of preventing cyber attacks, which makes NFC a viable candidate. Legacy NFC devices often are weakly encrypted or even lack encryption due to power and computational requirement, making them vulnerable to attacks [16], all that has recently changed. NFC is a wireless technology with short range (about 4 cm) usually consisting of two portable devices, connected in a peer-to-peer configuration as illustrated in Fig. 5. Using higher layer cryptographic protocols such as secure socket layer (SSL), NFC connections are secure from eavesdropping. An NFC Secure Element (SE) complimentary attestation and validation for mobile devices is capable of providing a secure on demand access, by utilizing NFC-based Host Card Emulation (HCE) [17]. A token is created by a cloud base Trusted Certified Authority (TCA) and

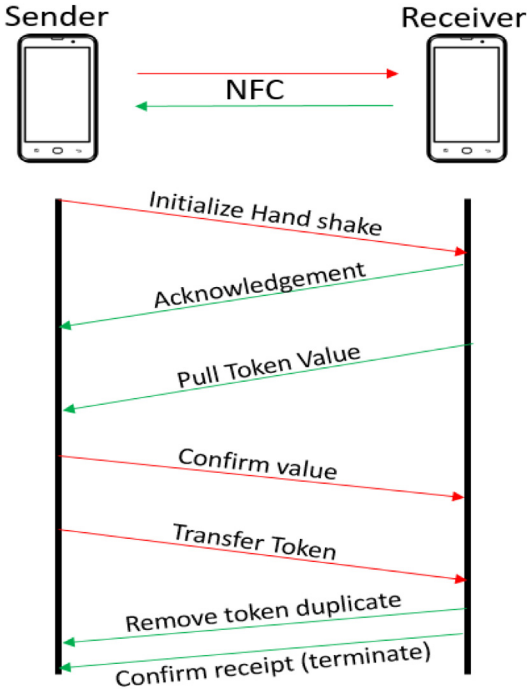

Fig. 5. Interaction between sender and receiver in PW transaction during NFC exchange of token. The process is initiated by the sender and is terminated by the receiver. The acknowledgment and encryption is for security between sender and receiver.

stored in a tamper resistant SE and Trusted Platform Module (TPM)-based attestation modules on the devices.

The token is used for transactions as shown in Fig. 5 between NFC devices even without connection to Internet. The NFC process is initiated by the sender with a handshake. An acknowledgment shows the profile of the receiver and is used to confirm if the token is sent to the right device. The receiver device pulls the value of token to be transferred. The sender device transfers token after confirming the value of transfer. The receiver device removes the used tokens from senders device and terminate transaction. The removal of used token is the first precautionary measure to prevent double spending.

3. Implementation

The pure wallet transaction is divided into three main steps.

1 In the first step the sender converts some coins to token from the token manager (TM). This process is represented in Fig. 6 as (A) and (B) Internet connection is required to complete this step. The pseudo code for this process is shown in Algorithm 2.
2 In the second step, the token information is transferred from the sender to the receiver. This step does not require the connection to the internet to be successful. It can be transferred through Bluetooth, WiFi, NFC etc. In this paper, this step was done manually by typing the information into the receiver device and is represented as (C) in Fig. 6.

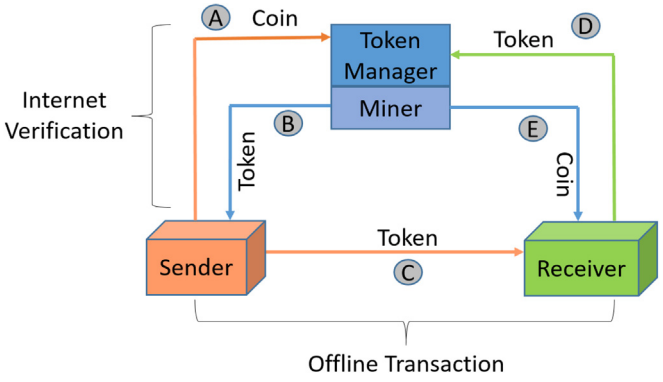

Fig. 6. Pure Wallet implementation architecture.

3 The last step as shown in Fig. 6 as (D) and (E). In this step, the token in the receiver's device is transmitted over the Internet to the TM, which in response transfers the appropriate coin value to the receiver's account. The pseudo code for this process is shown in Algorithm 3.

While Smart Contract (SC) is not listed as one of the steps, it plays an important role in the transaction process. The SC is a piece of transaction code that executes a set of instructions according to the terms of agreement of a contract. The SC resides in the ledger on the Blockchain network. Whenever a transaction is made between any sender and the TM, a process for another transfer is initiated at the TM. The new transfer process can only be completed with information contained in the token associated with the transaction. This process is represented in Algorithm 4.

Algorithm 2: Sender to the token manager

1 Sender sends coin to TM
2 mining process
3 TM sends token to sender
4 TM initiates a new transaction

Algorithm 3: Receiver from the token manager

1 Send token to TM
2 TM completes pending transaction
3 mining process
4 TM sends coin value to receiver

There are five implementation codes for this work. They are used to facilitate the desired behavior of the units of the architecture. They are listed below.

- The code executed by the sender's device.
- The code executed by the token manager.
- The code executed by the receiver's device.
- The code executed on the SC.
- The code executed by the miner to ensure automatic transaction mining.

Algorithm 4: SC process at token manager

1 receive coin from sender.
2 combine senders address and transaction hash information create token (T_1).
3 send a token to sender's device.
4 initiate a transact that requires T_1 to send coin.
5 send coin to any address that provides T_1 information within time (T_r)
6 else return the coin value to the sender after time T_t
7 end transaction

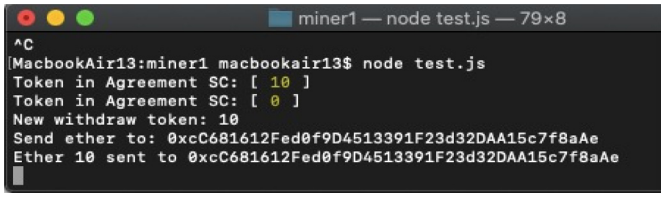

Fig. 7. A request to retrieve 10 tokens from TM by receiver device. The SC token reserve change from 10 (before the transaction) to 0 (after token all token has been claimed).

Table 1
Specification of used device.

Item	Specification
Computer	Mac air 2015
Memory	4Gb ram
Storage	256 Gb
Processor	1.6 GHz dual core Intel core i5
Operating system	Mac OS Sierra

In this implementation, the sender, the receiver, and the token manager are all different accounts on the same device. There is only a single miner in the network. Table 1 shows the specification of the used device. All the implementation codes for this paper have been uploaded in the Networked Systems Lab website; its URL is in Ref. [18].

4. Experimental evaluation

We conducted experimental evaluation to demonstrate the result of PW implementation. Specifically our demonstrations were conducted to show the Blockchain implementation of PW architecture, using the smart contract feature of Ethereum Blockchain. We discuss these experiments and results below.

The architecture utilizes token as the unit for offline transaction. The token resides in the sender's or the receiver's device, which is transferable over any short range connection (example NFC, Bluetooth, WiFi etc.). A token with a value of 10 is transacted in this evaluation. Fig. 7 shows a request message to claim a 10 token value from the token manager.

The process uses Internet connection to connect to the Blockchain network. The token manager utilizes the information contained in the token to complete the pending transaction initiated in Algorithm 2, which requires the information

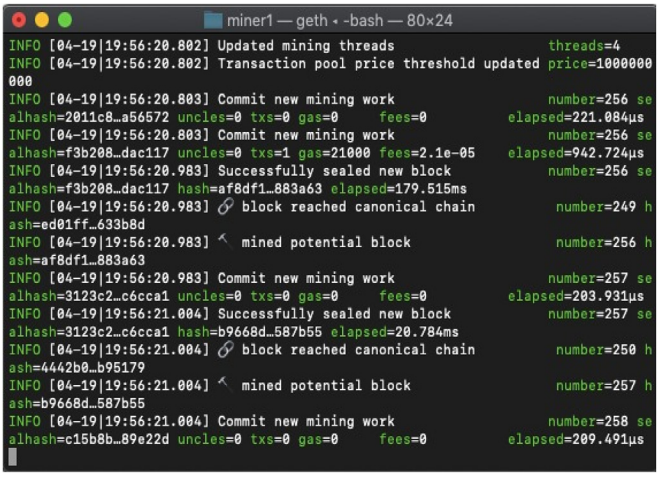

Fig. 8. Block mining process in a PW architecture using an auto mining activation protocol for energy efficiency.

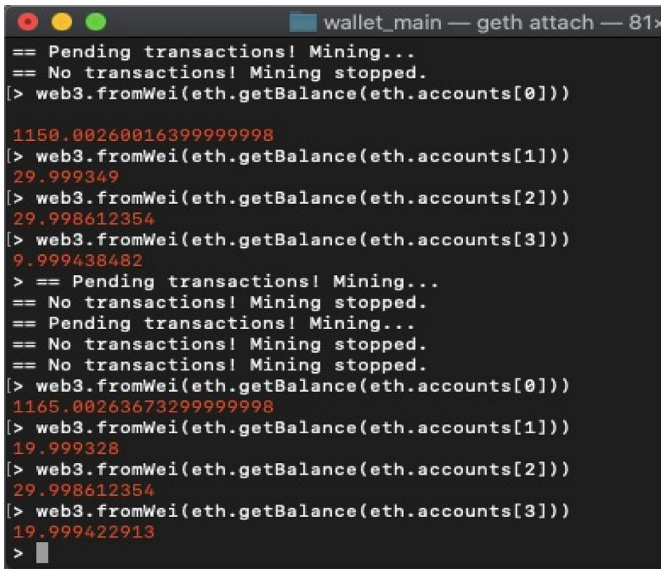

Fig. 9. The record of transaction history for account[1–4] showing balance values before and after transaction. It also shows the activation and deactivation of the mining process.

from the token. The TM commits the transaction into the Blockchain as the miner mines the transaction as shown in Fig. 8. It is the same as the mining operation that processes an online Blockchain transaction.

The account balance in the various accounts verifies the success of the transaction. Fig. 9 shows the balance in the four accounts, namely; the miner's account (accounts[0]), the token manager or bank (accounts[1]), the senders (accounts[2]), and the receiver (account[3]). The first set of account balance displays at the upper half of Fig. 9 is before the request and the balance displayed at the lower half of the figure shows the balance after withdrawal. It is seen that 10 token withdrawal is executed successfully, as the balance in accounts[1] changed from 29.999 to 19.999 indicating withdrawal from the TM and accounts[3] changed from 9.999 to 19.999 indicating a deposit into the receiver's account.

5. Strengths/benefits of PW

This proposed pure wallet system is necessary to improve the experience of using cryptocurrency in four major areas namely Real time transaction, rural adoption, reduced transaction fees, and Internet blind spot.

- **Real time transaction**
  A regular block-transaction takes about 10 min to be added into a block. The amount of time spent to complete a transaction can even take days based on certain reasons. For examples: Block Propagation Time, Number of Miners in the Network, Transaction Fee Set by the User, Speed of the Web, Spam on the Network and so on [15]. With PW, real-time transactions can be successfully done at any time. An NFC phone operating at 13.56 MHz frequency delivers a data rate of 424 kbit/s. A token of 64 characters encoded with UTF-8, UTF-16, or UTF-32 is delivered in 0.0012 s, 0.0023 s, and 0.0047 s respectively. The token manager completes the transfer to the receiver's crypto coin account at time T_t after receipt of the token from the payee.
- **Reduced transaction fee**
  With the growing popularity of cryptocurrency, users are exploited by miners who take advantage of excess waiting time by concentrating on transactions with high fees [11]. With PW, transactions can go on at any time independent of the immediate average transaction fee, and the token manager will complete the transfer at a time with a low average transaction fee.
- **Rural area adoption**
  The concept of cryptocurrency is to provide financial services to all including those in the rural area, where there is no banking infrastructure. However in such rural areas, the possibility of making cryptocurrency transactions is slim because of poor or no Internet connection. According to the data from International Telecommunication Union, [19] in 2017 some countries have less than 15% Internet usage, thus making it unlikely to adopt cryptocurrency in such areas.
  In Fig. 10 the actual value from year 2000 to 2017 shows continuous growth in Internet penetration trend. Prediction made using the actual value shows it will take about 15 years to achieve near 100% adoption worldwide. With PW, the goal of banking the unbanked will be achieved faster.
- **Internet blind spot**
  Passengers during flight can buy products sold by air hostesses through PW without having physical cash. Also, urban areas with poor or no Internet connectivity are considered as part of potential beneficiaries of our proposed Blockchain algorithm.

6. Conclusion

While the awareness and adoption of Blockchain growing globally, it is still limited to people who have internet connection. This article has presented a Blockchain architecture that

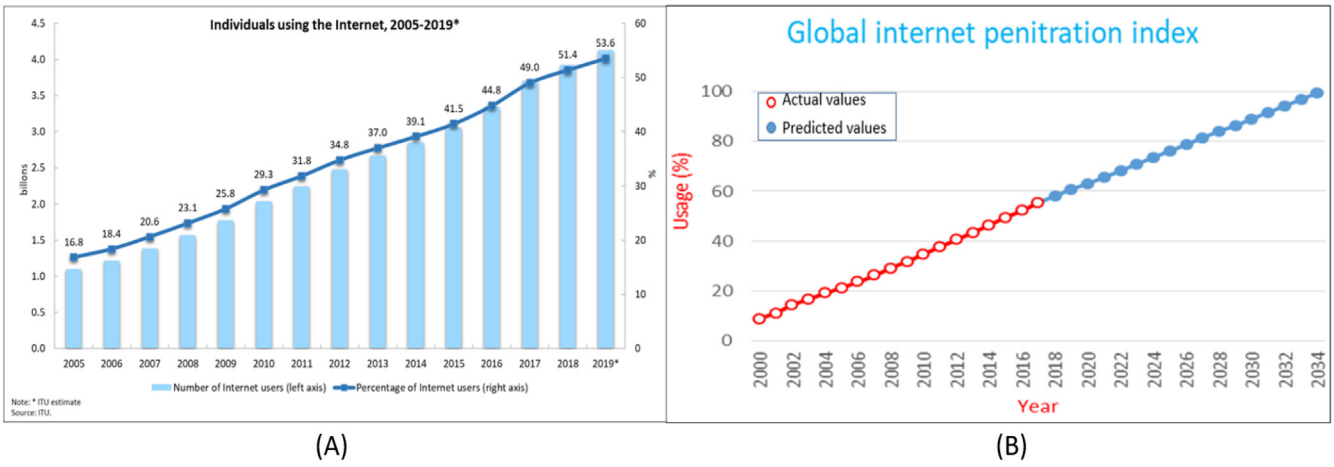

Fig. 10. (A) Represents the number and % of individuals using the Internet, 2005–2019. (B) Represents the Internet usage penetration index in % from 2000–2017, according to the International Telecommunication Union [17], and the predicted penetration index from 2018–2034.

enables offline transactions by introducing a token manager into the blockchain network, and applying the token and smart contract features. It elaborated and implemented the Blockchain aspect of a new payment technique for cryptocurrency termed Pure Wallet (PW). This involves conversion of cryptocurrency into digital token which is used for transaction during an offline state. The blockchain side implementation of the PW architecture was successfully implemented using Ethereum enabled smart contract. An offline transaction of 10 token was done, hence proving that the PW architecture has successfully enabled Blockchain for offline transactions. This work will positively impact the adoption of Blockchain, also it provides a pointer to other researchers on the possibility of offline Blockchain transaction.

Our work has limitations which include token divisibility i.e. our token must be sent as a whole. In addition, the proposed technique has no mechanism of detecting falsified tokens. Finally the behavior of the PW in a large adoption environment is also areas for further research. In the future, we hope work on the these limitations and apply this proposed algorithm to voting systems to improve the works in [20], by adding offline features to their proposed Blockchain voting technique.

Declaration of competing interest

The authors declare that they have no known competing financial interests or personal relationships that could have appeared to influence the work reported in this paper.

Acknowledgment

This research was supported by the MSIT (Ministry of Science and ICT), Korea, under the Grand Information Technology Research Center support program (IITP-2021-2020-0-01612) supervised by the IITP (Institute for Information & communications Technology Planning & Evaluation).

References

[1] A.N. Mian, A. Hameed, M.U. Khayyam, F. Ahmed, R. Beraldi, Enhancing communication adaptability between payment card processing networks, IEEE Commun. Mag. 53 (3) (2015) 58–64.

[2] A.A. Brincat, A. Lombardo, G. Morabito, S. Quattropani, On the use of blockchain technologies in WiFi networks, Comput. Netw. (ISSN: 1389-1286) 162 (2019) http://dx.doi.org/10.1016/j.comnet.2019.07.011.

[3] B.A. Ramadhan, B.M. Iqbal, User Experience Evaluation on the Cryptocurrency Website by Trust Aspect, in: International Conference on Intelligent Informatics and Biomedical Sciences 2018 (ICIIBMS), pp. 274-279.

[4] T. Bamert, C. Decker, R. Wattenhofer, S. Welten, Bluewallet: The secure bitcoin wallet, Secur. Trust Manag. (2014) 65–80.

[5] D. Godfrey-Welch, R. Lagrois, J. Law, R.S. Anderwald, Blockchain in payment card systems, SMU Data Sci. Rev. 1 (1) (2018) 1–44, Article 3.

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

[7] D.A. Bronleewe, Bitcoin NFC (M.S. thesis), Dept. Elect. and Comp. Eng., The University of Texas at Austin, USA, 2011, [Online] Available: https://repositories.lib.utexas.edu/bitstream/h{and}le/2152/ETD-UT-2011-08-4150/BRONLEEWE-MASTERS-REPORT.pdf?sequence=1&isAllowed=y.

[8] D. Unal, M. Hammoudeh, M.S. Kiraz, Policy specification and verification for blockchain and smart contracts in 5G networks, ICT Express (ISSN: 2405-9595) 6 (1) (2020) 43–47, http://dx.doi.org/10.1016/j.icte.2019.07.002.

[9] M.R. Islam, I.F. Al-Shaikhli, R.M. Nor, K.S. Mohammad, Cryptocurrency vs fiat currency: architecture, algorithm, cashflow and ledger technology on emerging economy, in: 2018 International Conference on Information and Communication Technology for the Muslim World, 2018, pp. 69-73.

[10] K.P. Dirgantoro, J.M. Lee, D.S. Kim, Private ethereum blockchain for industrial internet of things (IIoT), in: KICS-Winter 2019, 2019, pp. 1416–1417.

[11] K.P. Dirgantoro, Jae-Min Lee, Dong Seong Kim, None difficulty proof-of-work blockchain algorithm for industrial IoT, in: Proceedings of Symposium of the Korean Institute of communications and Information Sciences, 2019.6, pp. 1473-1474.

[12] A.R. Sai, J. Buckley, A.L. Gear, Privacy and security analysis of cryptocurrency mobile applications, in: 2019 Fifth Conference on Mobile and Secure Services (MobiSecServ), 2019, pp. 1-6.

[13] K.A. Taher, T. Nahar, S.A. Hossain, Enhanced cryptocurrency security by time-based token multi-factor authentication algorithm, in: 2019 International Conference on Robotics, Electrical and Signal Processing Techniques (ICREST), 2019, pp. 308-312.

[14] T. Plos, M. Hutter, M. Feldhofer, M. Stiglic, F. Cavaliere, Security-enabled near-field communication tag with flexible architecture supporting asymmetric cryptography, IEEE Trans. Very Large Scale Integr. (VLSI) Syst. 21 (11) (2013) 1965–1974.

[15] I.S. Igboanusi, J.M. Lee, D.S. Kim, Blockchain adoption in rural area: The role of internet penetration, in: Proceedings of Symposium of the Korean Institute of communications and Information Sciences, 2020, pp. 1207–1210.

[16] R. Jin, K. Zeng, Secure inductive-coupled near field communication at physical layer, IEEE Trans. Inf. Forensics Secur. 13 (12) (2018) 3078–3093.

[17] D. Sethia, D. Gupta, H. Saran, NFC secure element-based mutual authentication and attestation for IoT access, IEEE Trans. Consum. Electron. 64 (4) (2018) 470–479.

[18] I.S. Igboanusi, K.P. Dirgantoro, J.-M. Lee, D.-S. Kim, Pure wallet code, networked systems lab, 2020, posted 03.09.2020, accessed 03.09.2020, http://nsl.kumoh.ac.kr/include/sub.php?m=134&mode=Read&serial_no=202009030001&com_id=bi0001&menu_cd=30&class_cd=106&Page_Num=&left=&item=&find=&m=134.

[19] Proportion of households with Internet access, ICT Facts and Figures, International Telecommunication Union (ITU, 2017, [Online]. Available, https://www.itu.int/en/ITU-D/Statistics/Pages/stat/default.aspx.

[20] T. Dimitriou, Efficient, coercion-free and universally verifiable blockchain-based voting, Comput. Netw. (ISSN: 1389-1286) 174 (2020) http://dx.doi.org/10.1016/j.comnet.2020.107234.