

See discussions, stats, and author profiles for this publication at: <https://www.researchgate.net/publication/337935793>


NFC Pure Wallet (PW): An Offline and Real-time Blockchain transaction Architecture


Preprint · December 2019

DOI: 10.13140/RG.2.2.33806.31048


CITATIONS
0

3 authors:

 **Ikechi Saviour Igboanusi**
Kumoh National Institute of Technology
24 PUBLICATIONS 121 CITATIONS
[SEE PROFILE](#)

 **Dong-Seong Kim**
Kumoh National Institute of Technology
921 PUBLICATIONS 10,741 CITATIONS
[SEE PROFILE](#)

READS
5,597

 **Jae Min Lee**
Kumoh National Institute of Technology
412 PUBLICATIONS 3,700 CITATIONS
[SEE PROFILE](#)

NFC Pure Wallet (PW): An Offline and Real-time Blockchain transaction Architecture

Ikechi Saviour Igboanusi *IEEE Student Member*, Jae-Min Lee *IEEE Member*,
Dong-Seong Kim *IEEE Senior Member*

Networked System Laboratory, School of Electronics Engineering,
Kumoh National Institute of Technology, Gumi, South Korea.
ikechisaviour@ieee.org (ljmpaul, dskim)@kumoh.ac.kr

Abstract—This article proposes an electronic payment architecture named Pure Wallet (PW), which extends the concept of blockchain cryptocurrency for real-time and offline transaction. The first stage in this process requires the use of Internet connection, to convert cryptocurrency into a token. Then offline transactions are performed between electronic devices like mobile phones through a secure Near Field Communication (NFC) using the token in senders device. The financial value in form of a token is encrypted by the sender and sent with a key for decoding the value at the receiver's device via NFC. The receiver converts the received token into cryptocurrency in the presence of Internet connection. The major idea is to propose an electronic payment architecture utilizing cryptocurrency, which will enable financial transactions without instant connection to the Internet. Hence will be equivalent to cash transaction.

Index Terms—Blockchain, cryptocurrency, e-wallet, near field communication (NFC), offline transaction, pure wallet (PW)

I. INTRODUCTION

The need for daily financial transaction has lead to the development of several electronic payment systems that have made exchange of values relatively easier than the traditions means, but require financial institutions and presence of heavy communication equipment to be done efficiently. The transactions using payment cards exposes a lot of personal information to all the entities that participate in the transaction [1]. As mobile phones are taking most of the function like complimentary card, identification, credit/debit card, and so no, it still has many limitations in its current form for global adoption. The beauty of traditional cash transaction is the freedom to spend money anywhere, at anytime, with whoever wants the legal tender. 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 transaction but has also become popular for non-financial purpose.

Cryptocurrency has emerged to create a decentralized banking system, where no financial institution will control the money. It is a virtual currency that uses cryptography system to protect transaction [2]. 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 before a blockchain transaction can be done between two people is still a limitation of the current architecture. The existing blockchain methods has two major limitations for everyday use:

- Long transaction time [3] and,
- requires Internet connection at the moment of transaction.

As all transaction 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 scope of this work is to propose a payment architecture that will mitigate the above listed limitations of cryptocurrency. This article will use the concept of cryptocurrency payment systems to explain the proposed Pure Wallet (PW) algorithm. This algorithm can also be applied in other blockchain application. It is a combination of three stages; the online, the offline, and the online. Internet connection is required during the two online stages and NFC is required for the offline stage 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.

The rest of this article is arranged as follows: in section II, Papers that motivated this current work are summarized in Related Works. Section III presents the proposed system model. The expected benefit of this approach is presented in section IV, and finally the conclusion and future work is in section V.

II. RELATED WORKS

Researchers have made effort to create an offline cryptocurrency. Though cryptocurrency is protected with cryptographic encryption, a blockchain device is prone to unauthorized hacking. [4] proposed BlueWallet which 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 blockchain network to make transaction. 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 minutes to complete this process.

In [5], the authors proposed the use blockchain in card payment system. This is to reduce charges from financial institutions incurred by merchants for using payment card 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, save and encrypts transaction details, removes the need for a trusted middle man and limits exposure of information. A merchant local payment machine is able to determine at once if a card from customer can complete a transaction within limits of the payment card terms. The available amount saved to the blockchain ledger and the last information time update is obtainable. The system will refresh if the available information are outdated. Despite the contributions of this work, the authors did not consider their blockchain solution for offline transactions.

[6] explored the use of hardware to create a wireless mesh connection, with other device user to overcome the problem of poor or no Internet connection, for Bitcoin transaction. In this case, the several equipment are need 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 extent 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 will be required. This approach succeeded in extending connection to fixed areas without internet access. But 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 considerably bulky for mobile use.

The works in [7] explore the use of NFC enabled android mobile for Bitcoin transaction. In there work the receiver sends its 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.

Some papers have made contributions that served as motivation for this work, which is to overcome the above listed limitations itemized in the introduction. The authors of [8] compared cryptocurrency and fiat currency, and their role in the economy. It attempts to figure out how cryptocurrency improves fiat currency in terms of its performance of peer-to-peer network transaction. It pointed out the pros and cons of cryptocurrency. Authors of [9] proposed the combination of Ethereum and IoT to shorten the transaction time in IIoT. In [10], privacy and security of cryptocurrency mobile applications are considered. 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)

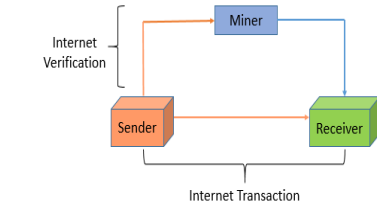


Fig. 1. Conventional blockchain architecture showing what happen when a sender sends money a receiver, and what happens at the back-end from the sender through the miner to the receiver. It also shows activities requiring Internet access.

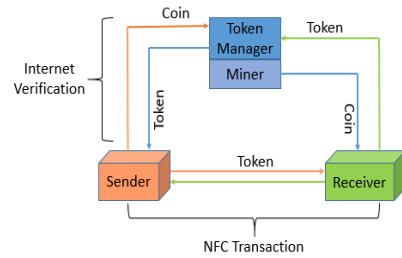


Fig. 2. shows the block diagram of the proposed Pure Wallet Blockchain architecture. The sender sends token through NFC connection to the receiver. The verification process happens over the Internet connection through the token manager and the miner.

than cryptocurrency in terms security provisions. Authors of [11] Proposed multi-factor authentication (MFA) which tries to improve cryptocurrency security. MFA approach is hinged on time-based onetime based password (TOTP), which is found to provide a more secure transaction. The authors in [12] demonstrated security-enabled near field communication tag using flexible architecture supporting cryptography. This is to solve the security problem of NFC by using symmetric and asymmetric cryptocurrency architecture.

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.

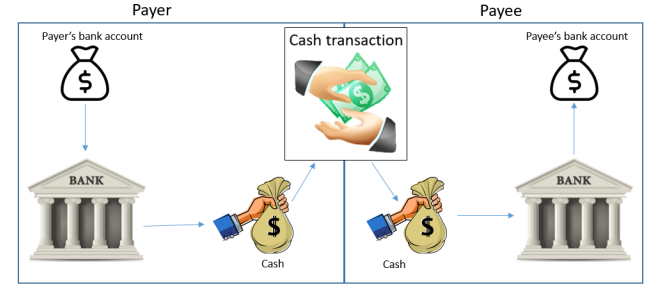


Fig. 3. The process of making cash transaction involving withdrawal of money from the payer's bank account. The physical cash is used for transaction and the payee deposits the money in a bank account.

III. SYSTEM MODEL

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 must be a sort of value that is transferable in an offline situation. To achieve a secure transaction, a digital cash in form of a trusted secret token is needed.

A. PW Digital Cash architecture

To achieve offline electronic transaction, it is necessary to create a form of value transfer system which work efficiently without instant connection to 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 takes place when there is Internet connection. The token manager resides in the network before the miner. Any transactions through the token manager is seen in the network as a transaction that has been initiated but is yet to be mined. The token is transferred from a sender to a receiver over an NFC connection. The receiver uses that token to retrieve the coin value from the token manager following the standard mining process. 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 can not send it to a new account. A time T_r is given for the receiver to claim the value of the received token. If the sender 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.

$$T_s + T_r \leq T_t \quad (1)$$

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 payers coin account. This is meant to prevent the chance of double redemption by the payee.

Algorithm 1: Pure Wallet (PW) processes

- 1 Sender sends coin to Token Manager (TM) via Internet access
- 2 sender receives token via Internet access
- 3 **while** Transaction is in offline **do**
- 4 hands shake
- 5 sender sends encryption key to receiver
- 6 sender sends amount embedded in token
- 7 receiver confirms amount
- 8 sender sends the token
- 9 receiver checks value and authorization on token
- 10 receiver removes any duplicate of sent token from the senders account
- 11 receiver confirms receipt and terminate transaction
- 12 **end**
- 13 Receiver sends token to TM
- 14 TM forwards the transaction to miners for mining
- 15 Receiver receives the coin

B. Real cash versus PW Digital cash

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

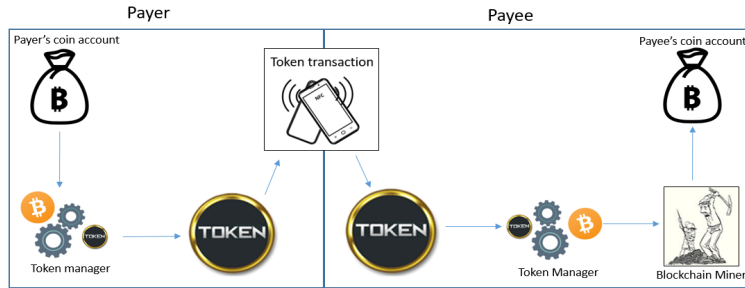


Fig. 4. Proposed Pure Wallet Blockchain architecture showing the process of payment from the payer to the payee using a token over an NFC connection. The token mimics the role of cash in cash transactions.

processes are illustrated in Fig. 4, to show its similarity with cash transaction as show in Fig. 3.

C. 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 Near Field Communication (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 [13], all that has recently changed. Near field communication is a wireless technology with short range (about 4cm) usually consisting of two portable device, 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 secured 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) [14]. A token is created by a cloud base Trusted Certifies Authority (TCA) and 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 hand shake. An acknowledgement shows the profile of the receiver and is used to confirm 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.

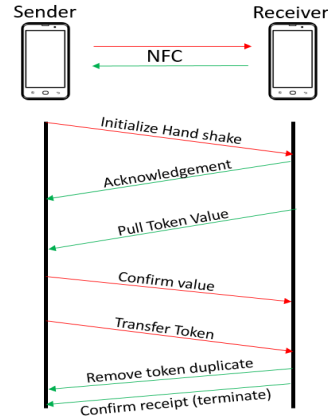


Fig. 5. Interaction between sender and receiver in pure wallet transaction during NFC exchange of token. The process is initiated by sender and is terminated by receiver. The acknowledgement and encryption is for security between sender and receiver.

IV. EVALUATION/BENEFITS OF PW

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

- **Real time transaction**

A regular block-transaction takes about 10min to be added into a block. The amount of time spent to com-

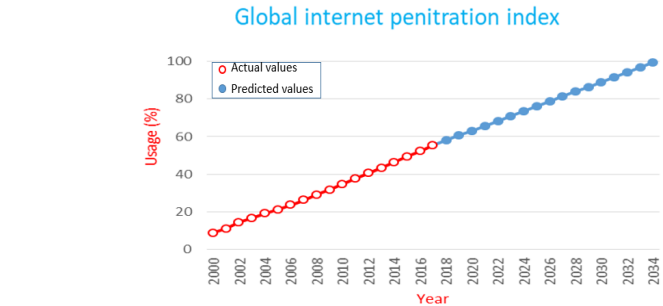


Fig. 6. The Internet usage penetration index in % from 2000-2017, according to the International Telecommunication Union, and the predicted predicted penetration index from 2018-2034.

plete a transaction can even take days based on certain reason. 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 [3]. With PW, real-time transaction 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, 0.0023, and 0.0047 seconds respectively. The token manager completes the transfer to the receivers 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 miner who take the advantage of excess waiting time by concentrating on transaction with high fee [2]. With PW transactions, can go on at anytime independent of the immediate average transaction fee, and the token manager will complete the transfer at a time with low average transaction fee.

- **Rural area adoption**

The concept of cryptocurrency is to provide financial services to all include those in the rural area, where there are no banking infrastructure. But in such rural areas, the possibility of making cryptocurrency transaction is slim because of poor or no Internet connection. According to the data from International Telecommunication Union, [15] in 2017 some countries have less than 15(%) Internet usage, thus making it unlikely to adopt cryptocurrency in such area.

In Fig.6 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 in urban area, areas with poor or no Internet connectivity are considered as part of potential beneficiaries of our proposed blockchain algorithm.

V. CONCLUSION AND FUTURE WORKS

This article has proposed a new payment technique for cryptocurrency introducing pure wallet (PW). This involves conversion of cryptocurrency into digital token which is used for transaction over a secure NFC connection. Some of the benefits of this new technique are listed. Although this paper considers payment system, this algorithm can be useful in other areas of blockchain transaction.

The application of this proposed algorithm to other areas of blockchain such as IoT systems, notary and digital identity will be the future of this work. A method of detecting falsified token and the behavior of the PW in a large environment are still open issue.

REFERENCES

- [1] A. N. Mian, A. Hameed, M. U. Khayyam, F. Ahmed and R. Beraldi, "Enhancing communication adaptability between payment card processing networks, in "IEEE Communications Magazine, vol. 53, no. 3, pp. 58-64, March 2015.
- [2] B. A. Ramadhan, and B. M. Iqbal, "User Experience Evaluation on the Cryptocurrency Website by Trust Aspect," *International Conference on Intelligent Informatics and Biomedical Sciences 2018. (ICIIBMS)*, pp. 274-279.
- [3] J. Fawkes, "Seven Reasons Behind a Delayed Crypto Transaction Confirmation" *CoolBitX*, Oct. 16, 2018.
- [4] T. Bamert, C. Decker, R. Wattenhofer, and S. Welten, "BlueWallet: The Secure Bitcoin Wallet " *Security and Trust Management*, 2014, pp. 65-80.
- [5] D. Godfrey-Welch, R. Lagrois, J. Law, and R. S. Anderwald, "Blockchain in Payment Card Systems," *SMU Data Science Review, Vol. 1, No. 1, Article 3*, pp. 1-44, 2018.

- [6] Hackernoon, "Completely Offline Bitcoin Transactions," <https://hackernoon.com/completely-offline-bitcoin-transactions-4e58324637bd>, February 4th, 2019
- [7] D.A. Bronleewe, "Bitcoin NFC. Technical report, "University of Texas Aug. 2011, pp. 1-26
- [8] M. R. Islam, I. F. Al-Shaikhli, R. M. Nor, and K. S. Mohamad, "Cryptocurrency vs Fiat Currency: Architecture, Algorithm, Cash-flow and Ledger Technology on Emerging Economy," *2018 International Conference on Information and Communication Technology for the Muslim World*, pp. 69-73.
- [9] K. P. Dirgantoro, J. M. Lee, D. S. Kim, "Private Ethereum Blockchain for Industrial Internet of Things (IIoT)," *KICS-Winter 2019*, pp. 1416-1417.
- [10] A. R. Sai, J. Buckley and A. L. Gear, "Privacy and Security analysis of cryptocurrency mobile applications," *2019 Fifth Conference on Mobile and Secure Services (MobiSecServ)*, pp 1-6.
- [11] K. A. Taher, T. Nahar, and S. A. Hossain, "Enhanced Cryptocurrency Security by Time-Based Token Multi-Factor Authentication Algorithm," *2019 International Conference on Robotics, Electrical and Signal Processing Techniques (ICREST)*, pp. 308-312.
- [12] T. Plos, M. Hutter, M. Feldhofer, M. Stiglic and F. Cavaliere, "Security-Enabled Near-Field Communication Tag With Flexible Architecture Supporting Asymmetric Cryptography," *IEEE Transactions on Very Large Scale Integration (VLSI) Systems*, vol. 21, no. 11, pp. 1965-1974, Nov. 2013.
- [13] R. Jin, and K. Zeng, "Secure Inductive-Coupled Near Field Communication at Physical Layer," *IEEE Transaction on Information Forensics and Security*, Vol. 13, No. 12, pp. 3078-3093 Dec. 2018.
- [14] D. Sethia, D. Gupta, and H. Saran, "NFC Secure Element-Based Mutual Authentication and Attestation for IoT Access," *IEEE Transaction on consumer electronics*, Vol. 64, No. 4, pp 470-479, Nov. 2018.
- [15] International Telecommunication Union (ITU), "Proportion of households with Internet access, 2017" *ICT Facts and Figures 2017*, Jul. 2017. <https://www.itu.int/en/ITU-D/Statistics/Pages/stat/default.aspx>

BIOGRAPHIES

Igboanusi Ikechi Saviour received his B. Tech degree in Physics from Federal University of Technology Owerri, Nigeria in 2013. He is currently working towards his M.S. degree in IT Convergence Engineering, at Kumoh National Institute of Technology, Gumi, South Korea. His interest research area include Network load balancing, real-time networks, machine learning, and blockchain.

Jae-Min Lee received the Ph. D degree in electrical and computer engineering from the Seoul National University, Seoul, Korea, in 2005. From 2005 to 2014, he was a Senior Engineer with Samsung Electronics, Suwon, Korea. From 2015 to 2016, he was a Principle Engineer in Samsung Electronics, Suwon, Korea. Since 2017, he has been an assistant professor with School of Electronic Engineering and Department of IT-Convergence Engineering, Kumoh National Institute of Technology, Gyeongbuk, Korea. He is a member of IEEE. His current main research interests are industrial wireless control network, performance analysis of wireless networks, and TRIZ.

Dong-Seong Kim received his Ph.D. degree in Electrical and Computer Engineering from the Seoul National University, Seoul, Korea, in 2003. From 1994 to 2003, he worked as a full-time researcher in ERC-ACI at Seoul National University, Seoul, Korea. From March 2003 to February 2005, he worked as a postdoctoral researcher at the Wireless Network Laboratory in the School of Electrical and Computer Engineering

at Cornell University, NY. From 2007 to 2009, he was a visiting professor with Department of Computer Science, University of California, Davis, CA. He is currently a director of kit Convergence Research Institute and ICT Convergence Research Center (ITRC and NRF advanced research center program) supported by Korean government at Kumoh National Institute of Technology. He is a senior member of IEEE and ACM. His current main research interests are real-time IoT and smart platform, industrial wireless control network, networked embedded system and Fieldbus.