International Journal of Information, Control and Computer Sciences
ISSN: 2517-9942
Vol:12, No:12, 2018

Cryptocurrency-Based Mobile Payments with Near-Field Communication-Enabled Devices

Marko Niinimaki

***Abstract*—**Cryptocurrencies are getting increasingly popular, but very few of them can be conveniently used in daily mobile phone purchases. To solve this problem, we demonstrate how to build a functional prototype of a mobile cryptocurrency-based e-commerce application the communicates with Near-Field Communication (NFC) tags. Using the system, users are able to purchase physical items with an NFC tag that contains an e-commerce URL. The payment is done simply by touching the tag with a mobile device and accepting the payment. Our method is constructive: we describe the design and technologies used in the implementation and evaluate the security and performance of the solution. Our main finding is that the analysis and measurements show that our solution is feasible for e-commerce.

***Keywords*—**Cryptocurrency, e-commerce, NFC, mobile devices.

I. Introduction

CRYPTOCURRENCIES like Bitcoin [1] have been the focus of both technical and economical discussion in the 2010s. It has been estimated that, in 2017, people used $190.2 million worth of Bitcoin monthly on merchant services [2]. Yet, this is minor amount compared with estimated $1.35 trillion spent using mobile wallets during the same year [3]. With a few exceptions like GraftCoin [4], we lack a method of making a payment with an NFC-enabled[1] mobile device as with ApplePay [5]. The aim of this paper is to provide a simple but working prototype that integrates a cryptocurrency, an NFC reader, and web-based payments.

The rest of the paper is organized as follows. In Section II, we explain the basic concepts of cryptocurrency, NFC, and a web interface with a cryptocurrency wallet. Section III describes our implementation in more detail. Finally, Section IV contains a summary and conclusions.

II. Basic Concepts

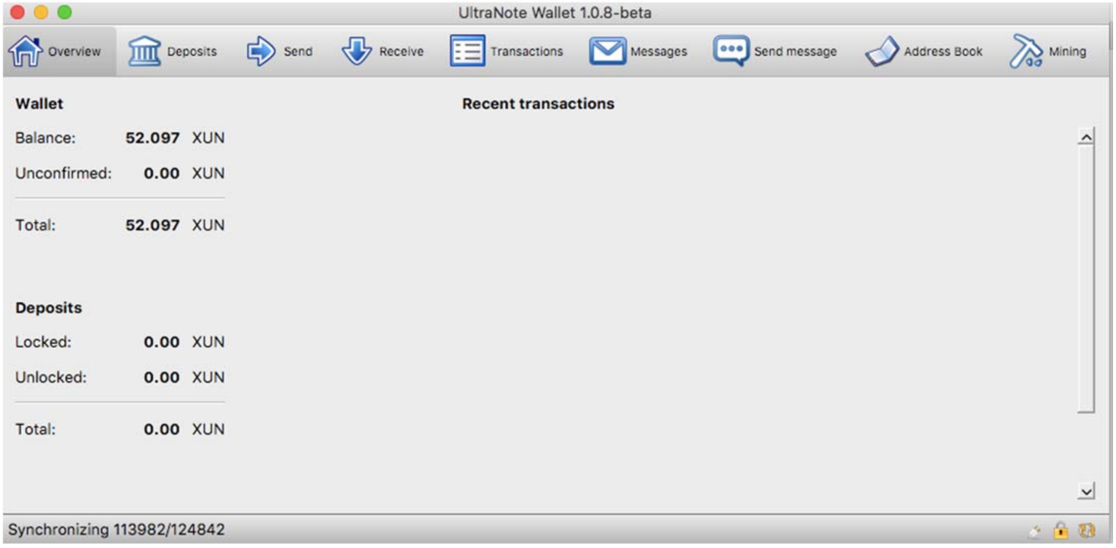
A cryptocurrency can be loosely defined as a medium of exchange using cryptography to secure the transactions and to control the creation of new units. Cryptocurrencies are decentralized systems; they do not have a central authority like a national bank to supply the currency. Rather, they use cryptography to control transactions, increase the supply, and prevent fraud [6]. Transactions are recorded in a blockchain that is essentially a distributed database of records, or public ledger of all transactions or digital events that have been executed and shared among participating parties. Each transaction in the public ledger is verified by consensus of a majority of the participants in the system. Once entered, information can never be erased. The blockchain thus contains a certain and verifiable record of every single transaction ever made [7]. The verification process of transactions is called mining. Anyone (with sufficient hardware, software and network resources) can become a miner, and successful verifications are rewarded with cryptocurrency (for details, see [8]).

A transaction record contains the identifiers of the sender, the receiver, and the transaction itself as well as the amount of currency transferred. Since the blockchain contains all the transactions, we could call sender/receiver identifiers simply “wallets” (holders of currency). The balance of a wallet at any time can be computed by traversing the blockchain transactions. In practice, it is more common to use the term “wallet” for a wallet file managed by a program. A wallet program secures the owner’s access to his/her funds by cryptography. Moreover, a wallet program does not store the entire blockchain, rather it downloads the block headers of the blockchain, and the transactions that represent payments to the owner’s identifier [8]. There is no link between a person’s actual identity and his/her wallet(s). With a wallet software available for most popular operating systems, anyone can create a wallet. A cryptocurrency exchange like the now infamous Mt.Gox exchange [6] lets a user convert fiat currency into a cryptocurrency and send it to his/her wallet. Another way of gaining cryptocurrency is mining (since successful verifications are rewarded). Most cryptocurrency wallet programs contain a mining function. An example of a wallet program (UltraNote cryptocurrency) is shown in Fig. 1. The “synchronizing” process shown at the bottom illustrates that the program is loading blockchain headers from the network. The mining button on the right will make the program launch a sub-process that verifies transactions.

Though BitCoin is the best known cryptocurrency, many other similar currencies have been introduced, often in order to remedy weaknesses in BitCoin’s architecture (notably: long transaction times [9]) or intended to a particular group (like Venezuela’s Petro [10]). UltraNote [11] is a cryptocurrency based on Bitcoin, but with an emphasis on privacy. Moreover, the UltraNote platform supports messaging and storing data like documents [11].

Marko Niinimaki (Dr.) is with the Webster University Thailand, 1 Empire Tower, South Sathorn Rd., Bangkok 10120, Thailand (phone: +66 21066599; e-mail: niinimakim@ webster.ac.th).

[1] NFC stands for Near-field communication. This contactless communication/data exchange method is standardized in ECMA-340 and ISO/IEC 18092.



Wallet

Balance: 52.097 XUN

Unconfirmed: 0.00 XUN

Total: 52.097 XUN

Deposits

Locked: 0.00 XUN

Unlocked: 0.00 XUN

Total: 0.00 XUN

Recent transactions

Synchronizing 113982/124842

Fig. 1 A cryptocurrency (UltraNote) wallet program running on OSX

Near Field Communication (NFC) is a short range (4..10 cm) low-cost, low-energy wireless communication technology jointly developed by Philips and Sony in late 2002 [12]. With an NFC enabled mobile phone, the user first touches a smart object (either an NFC tag, NFC reader, or another NFC enabled mobile phone). After touching, the NFC phone may further make use of received data, or it may use mobile services such as opening a web page or making a web service connection [12]. An NFC tag and a phone application for writing data in the tag are shown in Fig. 2.

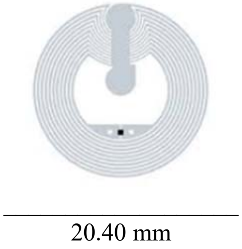
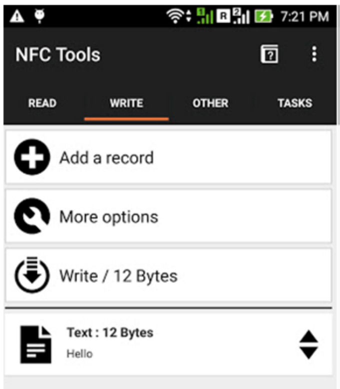


Fig. 2 (a) An NFC tag



Add a record

More options

Write / 12 Bytes

Text : 12 Bytes
Hello

Fig. 2 (b) A phone application for writing data (here just "Hello") on the tag

NFC tags are inexpensive (currently about $0.03) but can hold relatively small amounts of information (up to 888 bytes). However, they work without expensive hardware terminals that are required by many other payment schemes (like the Rabbit Card that is popular in Thailand [13]).

After a brief downturn during the "dot com bust" in the early 2000's, online shopping has enjoyed steady growth [14]. In 2017, users spent $453.46 billion on the web for retail purchases in the U.S. alone [15]. We loosely define a business-to-consumer based online shopping as a system where a user utilises his or her web browser or mobile application to browse and buy products and services from a seller. Many shop operators use standard e-commerce applications to run their sites [16], among them Magento.

III. System Design

The goal of the design is to provide a method by which users can purchase a physical item by scanning the NFC tag attached to it and paying it with a cryptocurrency. Our solution relies on (i) coding information in the NFC tag as a URL (web address) and (ii) making cryptocurrency wallets available by a web application.

Technically, the only piece of information that needs to be coded in the NFC tag is the address (URL) of a web application with a parameter that identifies the product that carries the tag, like the device (power bank for mobile phones, our product id 10345678) in Fig. 3. However, in our design, the parameter consists of the product id and the seller id. Thus, our database can have a clear distinction of products and sellers (and multiple sellers can sell the same product).

When a mobile device with an NFC reader is brought in contact with the tag, the phone's NFC application activates a web browser with the URL it reads from the tag. This is shown in Fig. 4 (a) where the web application invoked by the URL authorizes the user, checks his/her balance and if it is sufficient, displays the "Buy" button for the item. Fig. 4 (b) shows that the payment was accepted. The seller receives a notification of the payment in a few seconds. In our design, the product id (10345678 padded with zeros since it needs to be 64 characters long) is stored as a payment id as shown in Fig. 4 (c). The payment id is recorded in the blockchain and thus works as a proof of the payment of the product. A small transaction fee (0.001 units) is collected by the the UltraNote system.

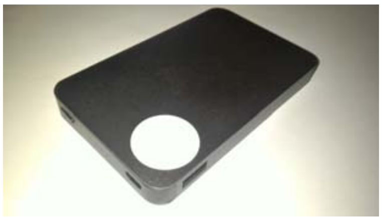
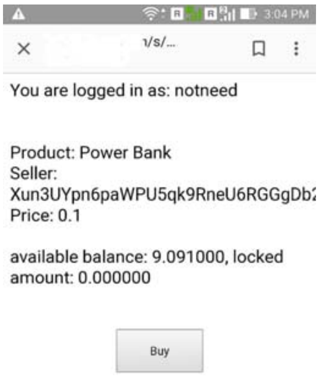


Fig. 3 A product with an NFC tag attached. The tag contains a URL and a parameter identifying the product and its seller

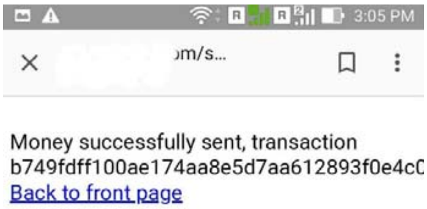


You are logged in as: notneed

Product: Power Bank
Seller:
Xun3UYpn6paWPU5qk9RneU6RGGgDb
Price: 0.1

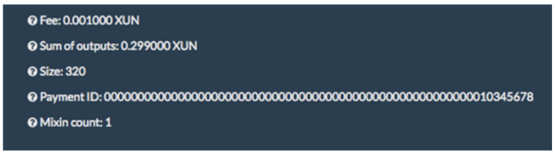
available balance: 9.091000, locked amount: 0.000000

Fig. 4 (a) Product and seller data with a “buy” option



Money successfully sent, transaction b749fdff100ae174aa8e5d7aa612893f0e4cC
Back to front page

Fig. 4 (b) A successful transaction



Fee: 0.001000 XUN
Sum of outputs: 0.299000 XUN
Size: 320
Payment ID: 0000000000000000000000000000000000000000000000000000000010345678
Mixin count: 1

Fig. 4 (c) A transaction record: product id as the payment id

There are still some functions needed for usability and security. The web application of Fig. 4 requires authentication and authorization so that only the owner of each wallet can issue payments from it. This can be easily provided since wallet files can be protected by a password. Thus, upon registration, a user can upload his/her wallet file into the web application and type its password. User authentication and authorization is done by the digest method (see [17] for details) using the wallet file name and wallet password as username and password.

Our implementation relies on command-line UltraNote programs with relatively few modifications. The programs incorporate practically the same functionality as the graphical wallet program in Fig. 1: a program called *ultranoted* synchronizes the blockchain headers and *ultranotewallet* interacts with the user. *Ultranotewallet* was modified to support more command line options. We have added an option called NFC that encodes the product id, the seller’s wallet address and the price. Pressing the “Buy” button of Fig. 4 (a) will call *ultranotewallet* with parameters that identify the wallet, its password and the information encoded in the NFC tag (product id, seller id).

IV. Summary, Conclusions and Future Work

In this paper, we have presented a framework to integrate NFC based mobile payments with a cryptocurrency. Our design is simple, but it facilitates quick and easy payments with an internet-connected NFC-enabled mobile device. We consider it safe, too, since the authentication and authorization are based on wallet file names and passwords, and the communication between the mobile device and the web server uses the encrypted HTTPS protocol. The application is written in PHP, and the web server is Apache. The service can be run on a server with very limited resources, in our case a virtual machine with 512 MB memory, 6 GB disk space and a single QEMU Virtual CPU at 2 GHz. With this setup, querying the wallet balance (Fig. 4 (a)) takes about 5 seconds and submitting a payment likewise 5 seconds. The seller’s wallet software will get a notification of an unconfirmed transaction almost immediately but the full payment verification can take up to 27 minutes (due to blockchain processing).

In the future, we aim at improving the performance and the user experience of the system. So far, we have only concentrated on the buyer’s action and have not provided an interface for a seller to list and promote his/her products on the platform. To accomplish that provision, we hope to integrate our software with a shopping cart solution like Magento.

Acknowledgment

This research has been partially supported by Webster University Thailand grant “Big Data Integration” 19th June 2017.

References

[1] S. Nakamoto, "Bitcoin: A Peer-to-Peer Electronic Cash System," 2008. (Online). Available: https://bitcoin.org/bitcoin.pdf.

[2] A. Nova, "Spending Cryptocurrencies on Everyday Purchases," 2 3 2018. (Online). Available: https://www.cnbc.com/2018/03/02/spending-cryptocurrencies-on-everyday-purchases-is-getting-easier.html.

[3] Juniper Research, "Mobile Wallet Spending," 30 Jan 2017. (Online). Available: https://www.juniperresearch.com/press/press-releases/mobile-wallet-spend-to-rise-by-more-than-30-this.

[4] S. Gomzin and D. Itkis, "GRAFT: Decentralized, Real-Time Credit, Debit, and Crypto Payment Processing Blockchain," Graft.network, 2018.

[5] S. Ghosh, J. Goswami, A. Kumar and A. Majumder, "Issues in NFC as a form of contactless communication: A comprehensive survey.," in Smart Technologies and Management for Computing, Communication, Controls, Energy and Materials, 2015.

[6] N. Gandal and H. Halaburda, "Competition in the Cryptocurrency Market," Bank of Canada Working Paper 2014-33, Ottawa, Canada, 2014.

[7] M. Crosby, P. Pattanayak, S. Verma and V. Kalyanaraman, "Blockchain technology: Beyond bitcoin," Applied Innovation, no. 2, Jun 2016.

[8] A. Narayanan, J. Bonneau, E. Felten, A. Miller and S. Goldfeder, Bitcoin and Cryptocurrency Technologies, Princeton University Press, 2016.

[9] N. T. Courtois, P. Emirdag and D. A. Nagy, "Could bitcoin transactions be 100x faster?," in Proc SECRYPT, 11th International Conference on Security and Cryptography (SECRYPT), 2014.

[10] M. O'Brien, "Venezuela's cryptocurrency is one of the worst investments ever," The Washington Post, 5 March 2018.

[11] UltraNote.org, "UltraNote White Paper 2.0," 2017. (Online). Available: https://ultranote.org/WHITEPAPER_ULTRANOTE2.0.pdf. (Accessed 20 May 2018).

[12] V. Coskun, B. Ozdenizci and K. Ok, " A Survey on Near Field Communication (NFC) Technology," Wireless personal communications, vol. 71, no. 3, pp. 2259-2294, 2013.

[13] Rabbit Card, "Where to use?," 2018. (Online). Available: https://card.rabbit.co.th/en/where-use-top-rabbit.

[14] M. Chang, W. Cheung and V. Lai, "Literature derived reference models for the adoption of online shopping," Information & Management, vol. 42, p. 543–559, 2004.

[15] Digital Commerce 360, "U.S. e-commerce sales grow 16.0% in 2017," 16 Feb 2018. (Online). Available: https://www.digitalcommerce360.com/article/us-ecommerce-sales/.

[16] K. Stoll, M. Ge and M. Hepp, "Understanding the Impact of E-Commerce Software on the Adoption of Structured Data on the Web," in LNBIP, 2013.

[17] G. Apostolopoulos, V. Peris and D. Saha, "Transport Layer Security: How much does it really cost?," in INFOCOM'99. Eighteenth Annual Joint Conference of the IEEE Computer and Communications Societies, New York, 1999.