UNIVERSITI PUTRA MALAYSIA

ZCHAIN4U BASED ON BLOCKCHAIN TECHNOLOGY

NURUL NADIA BINTI ABDOL RAHMAN

FSKTM 2018 28

UPM

UNIVERSITI PUTRA MALAYSIA

BERILMU BERBAKTI

ZCHAIN4U BASED ON BLOCKCHAIN TECHNOLOGY

By

NURUL NADIA BINTI ABDOL RAHMAN

**Thesis Submitted to the School of Graduate Studies,
Universiti Putra Malaysia, in Fulfilment of the
Requirements for the Degree of Master of Information Security**

January 2018

Dedications

"In dedication to the lecturer I have respect for as my supervisor of this project. Also helpful friends and loving family"

ABSTRACT

Abstract of thesis presented to the Senate of Universiti Putra Malaysia in fulfilment of the requirement for the degree of Master of Information Security

ZCHAIN4U BASED ON BLOCKCHAIN TECHNOLOGY

By

NURUL NADIA BINTI ABDOL RAHMAN

JANUARY 2018

Chair: Assoc. Prof. Dr. Zuriati Ahmad Zukarnain, PhD

Faculty: Faculty of Computer Science and Information Technology

The growth of technology nowadays become a higher demand due to the fact of the era as from a manual system to an automatic machine. A lot of other changes affect in our world comes from a technology, mostly it comes to the digital communication also digital transmission. Digital transmission always is a platform for a hacker to hack another user, especially when the transmission is involved with financial. This project proposes a higher secure of digital transmission platform. This transmission is involved peer-to-peer network and decentralized consensus technique which to make all nodes using the transmission without a third party or dedicated server, to increased the anonymous of the user. The methodology used in this project is Merkle tree technology. Moreover, the platform is committed to cryptography technique, such as SHA256 and PKI. This technology is been proved to increase the integrity of the transmission and increased the trust of the sender and receiver of Zwallet user. A Zchain4u project has been concluding to be higher secure chain product to transmit Zcoin transactions.

ABSTRAK

Abstrak tesis yang dikemukakan kepada Senat Universiti Putra Malaysia Sebagai memenuhi keperluan untuk ijazah Sarjana Keselamatan Maklumat

ZCHAIN4U BERDASARKAN TEKNOLOGI BLOCKCHAIN

Oleh

NURUL NADIA BINTI ABDOL RAHMAN

JANUARI 2018

Pengerusi: Prof. Madya. Dr. Zuriati Ahmad Zukarnain
Fakulti: Fakulti Sains Komputer dan Teknologi Maklumat

Pertumbuhan teknologi saat ini menjadi permintaan yang lebih tinggi disebabkan oleh fakta zaman dari sistem manual ke mesin otomatis. Banyak perubahan lain yang mempengaruhi dunia kita datang dari teknologi, kebanyakannya ia berkaitan dengan komunikasi digital dan penghantaran digital. Penghantaran digital sentiasa menjadi platform bagi penggodam untuk menggodam pengguna lain, terutamanya penghantaran yang melibatkan kewangan. Projek ini mencadangkan platform penghantaran digital yang lebih selamat. Penghantaran ini melibatkan rangkaian peer-to-peer dan teknik konsensus terdesentralisasi yang menjadikan semua nod menggunakan penghantaran tanpa pihak ketiga atau server yang berdedikasi, untuk meningkatkan pengguna tanpa nama atau tidak dikenali. Metodologi yang digunakan dalam projek ini ialah teknologi merkel. Selain itu, platform ini melakukan teknik kriptografi, seperti SHA256 dan PKI. Tteknologi ini telah terbukti meningkatkan integriti penghantaran dan meningkatkan kepercayaan pengirim dan penerima pengguna Zwallet. Projek Zchain4u telah

disimpulkan sebagai produk rantaian selamat yang lebih tinggi untuk menghantar transaksi Zcoin.

ACKNOWLEDGEMENTS

In the name of God, the Most Gracious, the Most Merciful, the project was running well and done successfully. I would like to extend my sincere appreciation to everyone who gave me the opportunity to complete this project. My special appreciation to my project supervisor Assoc. Prof. Dr. Zuriati Ahmad Zukarnain, who contributed in simulating proposals and encouragement, helped me streamline my project especially in writing this project and focused on achieving the goal. Moreover, I would like to acknowledge the importance of the essential UPM staff role, which gives permission to use all the necessary equipment and materials needed to complete coding in HPC lab, special thanks to my classmates who helped me to assemble parts and gave suggestions on the project's LR task. Finally, many thanks to my family who support me the time and space to complete the report as well. I need to appreciate guidance from the panel especially Dr. Sharifah Md. Yasin who has improved me for her comments and advice.

APPROVAL

This thesis was submitted to the Senate of Universiti Putra Malaysia and has been accepted as fulfillment of the requirement for the degree of Master of Information Security. The members of the Supervisory Committee were as follows:

Signature: ____________________________________
ASSOC. PROF. DR. ZURIATI AHMAD ZUKARNAIN
Faculty of Computer Science and Information Technology
Universiti Putra Malaysia
(Supervisor)
Date:______________

Declaration Form

I hereby confirm that:

This thesis is my original work; except for the quotations and citations which have been duly acknowledged. I declare that it has not been previously submitted for any other degree at Universiti Putra Malaysia or at any other institutions.

Signature:____________________ Date:__________________

Name and Matric No.: Nurul Nadia Binti Abdol Rahman (GS46551)

TABLE OF CONTENTS

List of Tables

List of Figures

CHAPTER 1
INTRODUCTION

1.1 Purpose and significance of the study

The world at this time is convenient with the technology, including data transmission via online, also persistent existing of digital currency till the today year 2017. Digital currency is the most technology that has been used and upgrades from time to time then become cryptocurrency. Cryptocurrency is used cryptography technique to running digital currency, indeed becomes a phenomenon in business finance. Cryptocurrency exists since the year 2008, the first cryptocurrency was named as Bitcoin, it has been known until now because of its stability. Bitcoin was created by Satoshi Nakamoto and had been active in the year 2009. The Bitcoin has been attached financial item in verities of organizations in many industries since that, the Bitcoin technology has become known in the whole world.

The organizations involving business such as IT company, hotel, and accommodation, also a breakfast food restaurant is using Bitcoin as payment. Life of business for who are using Bitcoin technology is more efficient than who are not because the Bitcoin user believes there are benefits of it. The benefits include less time transfer money to the receiver, prevent from double spending. Since the sale and purchase used this kind of technology, the normal user like us can also become buyer via Bitcoin. We believe in the future, the position of Bitcoin is depending on its controller such as Blockchain, previously it was called as Genesis Block.

The blockchain is based or database of the secure online transaction, which plays in Peer-to-Peer (P2P) network. It works with cryptography ways that involve techniques of hash function SHA-256, public and private keys, which is to run the transactions by using Bitcoin as a cryptocurrency, plus it consists of the block by block so those blocks are known as data in Blockchain. Those blocks are holding the hash function and other data which is transactions. These transactions have been created such as by online business. The blockchain is the technology behind Bitcoin, that means just to be sure Blockchain and Bitcoin both are the difference. Bitcoin is used in the transaction and being transferred using the P2P network, while Blockchain is the technology which to maintain the Bitcoin transaction.

To be a user of Bitcoin, the user needs to create an e-wallet. This kind of wallet is known as Bitcoin or other cryptocurrency user account, this account is connected to Blockchain. It is not just a normal user as a peer, but there are also include peer as miner could sign up an e-wallet.

E-Wallet is available from many types, including Wallet Software, Mobile Wallet, Web Wallet and Hardware Wallet. These types of wallets depend on the user level, to their new users are encouraged to use Web Wallet / Online Wallet because from here they can learn from an easy interface. Web Wallet keeps Bitcoin storage on the server, no matter how Wallet is stored Bitcoin into the PC. Wallet Software is a wallet plugged into the PC, which can be online for connecting with other peer networks. Mobile Wallet can be installed on smartphones and other gadgets like tablets, etc. The creation of Mobile Wallet is to enhance the convenience of the users to enjoy Bitcoin functionality. The whole e-wallet is the user key to starting small foot movements to big and beyond. Once users get a digital wallet, they should not share their password with anyone including their best friends. Our proposed e-wallet is focused on Web Wallet as it is the starter to create e-wallet with a friendly user interface.

Normal user mostly only used Bitcoin to purchase things and buy cryptocurrency by changing the traditional currency to cryptocurrency, whereas miner is buying Bitcoin by mining, so basically, there are two ways to fill Bitcoin in e-wallet. Since Bitcoin is decentralized, the miner must complete mine Bitcoins.

Mining means a maintainer or a miner is creating a block in 10 minutes to its limited time given, the block is made by keeping the transaction in it. Once the block is ready it then sent to the blockchain, well at this time all miners is check then transfer the valid block to other miner and achieve the consensus to validate that there is only one block can be rewarded Bitcoin in his/her wallet. Essentially, this is how the Bitcoin is working with Blockchain:

a) The transaction is involved sender(peer) sent a request to purchase with a receiver, or sender sent cryptocurrency (Bitcoin) to another peer.

b) The transaction cannot be transmitted yet until the miner starts to mining, transactions are stored in miner's block.

c) Then, all miners verify and validate the block, with SHA256, and the public, private keys included.

d) Once the consensus is accepted, the reward (cryptocurrency) is active also all of the transactions in the block then now can be transmitted successfully.

Sometimes, the receiver as the online business seller can request more than one validation of the transaction from the buyer, so sender needs to wait if there are more than one miner are choosing his/her transaction to put in the miners' blocks and need to be validated more than one time.

e) Because different blocks can have same transactions, if three blocks have validated, then the transactions are valid three times already.

f) So, if the receiver is requested three validations of that transaction, for the transaction is then validated three times already, by that time the transaction is successfully submitted to the receiver, as a result of the sale and purchase online is run profitably.

Here shows that miner is so much important for the transaction to be submitted from sender to receiver, there are like give and take system. Miner can mine anytime. The fact said the average value of cryptocurrency is increased and decreased in certain time. If the average is increased then it would be lucky for the miner to sell back their Bitcoin to another peer.

The blockchain is used the decentralized system. The decentralized system is different with centralized. The centralized system is normally used in Banks, where it a single server that leads single point of failure, centralized system is also controlled by one center operation. The system is easy to publish however it is difficult to scale. Decentralized means a system that involved multiple servers, which the process is no node(peer) can tell another node what to do, that affect better handled of demand and failures. Although the ledger of Blockchain is used distributed ledger which means it is public for all miners or nodes to access. This shows the Blockchain technology is used both distributed and decentralized. It is distributed due to the timestamped public ledger and resides on multiple computers, whereas it is decentralized due to if one node is going down, other nodes will not be affected down too, it still has the ability to operate in a chain.

Merkle tree is the main method present which relates with anchor paper [21], this method is implemented using hash-based data structure. The generalization of the hash list is present as a leaf node (hash block). This method is also efficiently used to verify the blockchain system. It is efficient because it uses a hash rather than files, well that is how blockchain is used, in fact, this method is used in the p2p network.

This project has proposed the e-wallet called Zwallet which run the cryptocurrency of Zcoin to be transmitted the transaction via Zchain4u that act as blockchain in the network. These then will be explained starting with Chapter 3.

1.2 Problem Statements

The studied of this project, has found that verities disadvantage of conventional e-banking which can be distinguished and improved when using Blockchain. Disadvantage such problem as there are third-party in the process of common e-banking which functions to verify or regulate the transactions between clients. This problem shows that there is no privacy between sender and receiver on the value of transmitting while doing a transaction. Another problem statement includes the conventional e-banking system requires a charge known as transaction fee which is still employed by modern internet banking procedures. This happens is actually unfair to customers to send their money to the receiver at the same time their account balances also taken by central and decreased their balance even a bit. The last disadvantage that has been covered is downtime limitation. The standard e-banking systems usually have times in which the clients cannot access the system, due to maintenance, improvised downtime, system failure, etc., which render the verification mechanism inoperable thereby denying clients successful transactions.

1.3 Research Objectives

The project objectives are covered against the problem statements, including to propose a possible solution to create a new blockchain infrastructure (Zchain4u), with e-wallet and to enable secure authentication without a third party or any regulations because the technology of Blockchain is no need for a financial intermediary like a bank. Other is to create a framework process that will enable transaction of the Blockchain without the need for a transaction fee. For the last of the research, the objective is to be working on the technique of a cryptography hash functions that are used in to verify the Proof-of-Work (POW) of the all peers in the chain of a peer-to-peer network, which also giving users ability to use the service transaction anytime without a doubt. So, parties with access to quantum computation would have an unfair advantage in procuring mining rewards.

1.4 Research Scope

The scope of this project is to reimplement UI e-wallet called Naivecoin will be designed. This project is done in two (2) parts;

- Questioning information about blocks and transactions.
- Questioning information about a specific address.

Create a flow process for transactions and this project will be done in Zchain4u.

This will be used to design and propose a new cryptocurrency Zcoin and a digital account/e-wallet called Zwallet which will aid transactions on the aforementioned platform.

The scope also covered the limitation of this project which includes an inability to access the blockchain community. The blockchain community is highly secretive in its operation, transaction details and operational framework thereby making it an ardent task to understand its nitty-gritty.

1.5 Report Structures

As there are six chapters in this report, Chapter 1 is explained about introduction, meaning of Blockchain and Bitcoin, how are both are related in this era, what the function of e-wallet, problem statements which are related to the differentiation of conventional e-banking, research objectives that have been covered to opposite of research problems, and research scopes was explained on the requirements before start the method used, also discussed on limitations of this project. Next, Chapter 2 focuses on the literature review, which included varieties of existed e-wallet application with their own upgraded technologies. The methodology is presented in Chapter 3, include research design with flowchart, frameworks and project requirements. Then for Chapter 4 is explained on results and findings discussion part contained with a screenshot to analyze more clear, to be added the differences of proposed method and existing application in the table. For the Chapter 5 is the chapter that concluded from the overall project has been done. The last chapter would be Chapter 6 is determined the future work of this project.

BIBLIOGRAPHY

[1] http://slideplayer.com/slide/6913406/

[2] https://bitcoin.stackexchange.com/questions/4974/what-is-a-double-spend

[3] https://en.wikipedia.org/wiki/Systems_development_life_cycle

[4] http://molebit.com/blog/bitcoin-a-simple-explanation/intro-to-bitcoin-more-in-depth/

[5] https://en.wikipedia.org/wiki/Quantum_key_distribution

[6] Nakamoto, S. , Bitcoin: A Peer-to-Peer Electronic Cash System, 2008, 2016-01-06 (https://bitcoin.org/bitcoin.pdf)

[7] Kiktenko, E. O., Pozhar, N. O., Anufriev, M. N., Trushechkin, A. S., Yunusov, R. R., Kurochkin, Y. V., … Fedorov, A. K. (2017). *Quantum-secured blockchain*, 1–6. Retrieved from http://arxiv.org/abs/1705.09258

[8] Valenta, L., & Rowan, B. (2015). Blindcoin: Blinded, accountable mixes for bitcoin. *Lecture Notes in Computer Science (Including Subseries Lecture Notes in Artificial Intelligence and Lecture Notes in Bioinformatics)*, *8976*, 112–126. http://doi.org/10.1007/978-3-662-48051-9_9

[9] Ziegeldorf, J. H., Grossmann, F., Henze, M., Inden, N., & Wehrle, K. (2015). CoinParty. *Proceedings of the 5th ACM Conference on Data and Application Security and Privacy - CODASPY '15*, 75–86. http://doi.org/10.1145/2699026.2699100

[10] Ruffing, T., Moreno-Sanchez, P., & Kate, A. (n.d.). CoinShuffle: Practical Decentralized Coin Mixing for Bitcoin, 1–15. Retrieved from https://petsymposium.org/2014/papers/Ruffing.pdf

[11] Androulaki, E., & Karame, G. O. (2014). Hiding transaction amounts and balances in Bitcoin. *Lecture Notes in Computer Science (Including Subseries Lecture Notes in Artificial Intelligence and Lecture Notes in Bioinformatics), 8564 LNCS*, 161–178. http://doi.org/10.1007/978-3-319-08593-7_11

[12] Zhang, Y. , Wen, J. / 2015 , An IoT electric business: Extracting Intellingence in Next Generation Networks (ICIN)

[13] Moser, M., Bohme, R., & Breuker, D. (2013). An inquiry into money laundering tools in the Bitcoin ecosystem. *eCrime Researchers Summit, eCrime*. http://doi.org/10.1109/eCRS.2013.6805780

[14] https://wiki.namecoin.org/index.php?title=FAQ#What_is_the_relationship_of_this_
project_to_Bitcoin

[15] Stan, S. (2017, August 28) *Here's how to deal with those terribly high Bitcoin transaction fees*. Retrieved from http://mashable.com/2017/08/28/bitcoin-transaction-fees/#vwpRu501KkqF [Accessed 05 12 2017].

[16] Saxena, A., Misra, J., & Dhar, A. (2014). Increasing anonymity in bitcoin. *Lecture Notes in Computer Science (Including Subseries Lecture*

Notes in Artificial Intelligence and Lecture Notes in Bioinformatics), 8438, 122–139. http://doi.org/10.1007/978-3-662-44774-1_9

[17] Wilson, D., & Ateniese, G. (2015). From pretty good to great: Enhancing PGP using bitcoin and the blockchain. *Lecture Notes in Computer Science (Including Subseries Lecture Notes in Artificial Intelligence and Lecture Notes in Bioinformatics)*, *9408*, 368–375. http://doi.org/10.1007/978-3-319-25645-0_25

[18] Bonneau, J., Narayanan, A., Miller, A., Clark, J., Kroll, J.A., Felten, E. W. Anonymity for Bitcoin with Accountable Mixes. https://eprint.iacr.org/2014/077.pdf

[19] https://www.investopedia.com/tech/6-most-important-cryptocurrencies-other-bitcoin/

[20] http://jalan-gw.blogspot.my/2014/09/jenis-jenis-wallet-bitcoin.html

[21] Kiktenko, E.O., Pozhar, N.O., Anufriev, M.N., Trushechkin, A.S., Yunusov, R.R., Kurochkin, Y.V., Lvovsky, A.I., Fedorov, A.K. (2017). Quantum-secured blockchain. *Cornell University Library*, 1705.09258. https://arxiv.org/abs/1705.09258

[22] https://medium.com/@lhartikk/a-blockchain-in-200-lines-of-code-963cc1cc0e54

[23] S. Nakamoto, "*Bitcoin: A Peer-to-Peer Electronic Cash System,* bitcoin.org/bitcoin.pdf

[24] Lov K. Grover, *"A fast quantum mechanical algorithm for database search,"* Proceedings of the twenty-eighth annual ACM symposium on Theory of computing 212–219. ACM. doi:10.1145/237814.237866 arXiv:quant-ph/9605043

[25] Peter W. Shor, *"Polynomial-Time Algorithms for Prime Factorization and Discrete Logarithms on a Quantum Computer,"* SIAM J. Comput., 26 (5): 1484–1509. doi:10.1137/S0036144598347011

[26] *"Report on Post-Quantum Cryptography,"* National Institute of Standards and Technology, Chen et al., NISTIR 8105. doi:10.6028/NIST.IR.8105

[27] *"CNSA Suite and Quantum Computing FAQ*," Information Assurance Directorate of the NSA, Document MFQ-U-OO-815099-15 (2016).

[28] DJ Bernstein, J Buchmann, and E Dahmen, "*Post-Quantum Cryptography"* eds. (Springer Berlin Heidelberg, 2009) doi:10.1007/978-3-540-88702-7

[29] Bentogoa. (2014). *Electronic Money: Wikipedia.* Retrieved from Wikipedia website: http://www.en.wikipedia.org

[30] Clarke R. (2001) *Authentication: A Sufficiently Rich Model to Enable e-Business*. Xamax

[31] Consultancy Pty Ltd, 26 December 2001, at

http://www.anu.edu.au/people/Roger.Clarke/EC/AuthModel.html

[32] *Digital Wallet: Wikipedia. (2008).* Retrieved from Wikipedia website: http://www.en.wikipedia.org

[33] Dragt, B., 2012. *Universal Commerce: A Seamless, Personalized, Purchase Experience for Today's Connected Consumers*, s.l.: First Data Corporation.

[34] *Google, 2015. Google Wallet: How it works.* [Online] Available at: http://www.google.com/wallet/how-it-works/index.html.

[35] Gutman, J., Beach, B., Wright, J., Springs, C., & Puhl, L. (2000). *Electronic Wallet. Chicago.*

[36] Handa, R., Maheshwari, K. & Saraf, M., 2011. *Google Wallet - A Glimpse into the future of*

[37] *mobile payments*, s.l.: GRIN Publish & Find Knowledge.

[38] Hun, P. P. (2008). *Design and Implementation of Secure Electronic Payment System*

[39] *(Client)*. World Academy of Science, Engineering and Technology, Vol. 48, pp. 60-67.

[40] *ISIS Project* (2012). Available at http://www.paywithisis.com.

[41] Izhar, A. (2011). *Designing and Implementation of Electronic Payment Gateway for Developing Countries.* Journal of Theoretical and Applied Information Technology, Vol. 26, no. 2.

[42] Lahiri, S. (2003). *System And Method For Electronic Wallet Transaction.* Austin,

[43] Law, E. C., & Yam, L. M. (Jun. 7, 2007). *EXTENDED ELECTRONIC WALLET* United States.

[44] Lee, I. (2011). *Electronic Commerce Systems*, available at http://www.cis.upenn.edu/~lee/01emtm553/.

[45] Rutter, J., 2012. *What is Universal Commerce?* [Interview] (26 October 2012).

[46] Tang, B. (2009). *Innovations in China's e-Payment Market, available* at http://iisdb.stanford.edu/docs/189/epayment_bin_tang.pdf.

[47] Xu, W. (2000). *E-commerce online payment security issues*. Joint Hefei University Journal, vol 3.

[48] [1] SET Secure Electronic Transaction (TM) LLC. SETCo website: http://www.setco.org/.

[49] CyberCash. CyberCash Home Page. CyberCash website: http://www.cybercash.com/.

[50] DigiCash. DigiCash: Solutions for Security and Privacy. DigiCash website:
http://www.digicash.com/

[51] Digital Equipment Corporation. MilliCent. MilliCent website: http://www.millicent.digital.com/.

[52] Sun Microsystems. Java Commerce Home Page. JavaSoft website: http://java.sun.com/commerce/.

[53] Microsoft Corporation. Microsoft Wallet. Microsoft wallet website: http://www.microsoft.com/wallet/

[54] Alireza Bahreman. Generic Electronic Payment Services. In *The Second USENIX Workshopon Electronic Commerce Proceedings*, 1996.

[55] Alireza Bahreman and Rajkumar Narayanaswamy. Payment Method Negotiation Service. In *The Second USENIX Workshop on Electronic Commerce Proceedings*, 1996.

[56] Java Commerce Messages White Paper. Sun Microsystems website: http://java.sun.com/products/commerce/docs/whitepapers/jcm_whitepaper/jcm_whitepaper.html.

[57] Steven P. Ketchpel, Hector Garcia-Molina, and Andreas Paepcke. Shopping Models: A Flexible Architecture for Information Commerce. In *Proceedings of the Fourth Annual Conference on the Theory and Practice of Digital Libraries*, 1997. At http://www-diglib.stanford.edu/cgi-bin/WP/get/SIDLWP-1996-0052.

[58] Steven Ketchpel, Hector Garcia-Molina, Andreas Paepcke, Scott Hassan, and Steve Cousins. UPAI: A Universal Payment Application Interface. In *USENIX 2nd Electronic Commerce workshop*, 1996.

[59] W3C Joint Electronic Payments Initiative (JEPI). W3C website: http://www.w3.org/ECommerce/Overview-JEPI.html.

[60] [13] D. Eastlake. Universal Payment Preamble Specification. W3C website: http://www.w3.org/ECommerce/specs/upp.txt.

[61] B. Cox, D. Tygar, and M. Sirbu. NetBill Security and Transaction Protocol. In *First USENIX Workshop of Electronic Commerce Proceedings*, 1995.

[62] J.L. Abad-Peiro, N. Asokan, M. Steiner, M. Waidner. Designing a Generic Payment Service. *IBM Systems Journal Vol. 37 No. 1*, 1998.

[63] T. Goldstein. The Gateway Security Model in the Java Electronic Commerce Framework. In *Proceedings of the Financial Cryptography First International Conference, FC '97, 1997.*

[64] N. Daswani, D. Boneh. Experimenting with Electronic Commerce on the PalmPilot. [*preprint*].