The Model of Evaluating Financial Transactions Involving Digital Currencies with Blockchain Technology

Supantana Jairak[1]
and Sooksawaddee Nattawuttisit[2]
Faculty of Information Technology,
Sripatum University, Bangkok, Thailand
[1]supantana@gmail.com
[2]sooksawaddee.na@spu.ac.th

Received: 2/7/2019
Accepted: 24/7/2019

***Abstract* - Nowadays, emerging technology such internet and mobile convergence ecosystems had changed the world. Blockchain was recently one of the most propitious and ingenious technologies that were disrupted in financial services. In this paper, we evaluated the model involving digital currency transactions with blockchain technology by using MyEtherwallet as a research tool. The evaluation criteria consisted of the accuracy, the security and privacy perspectives, the reliability, and Suitability of the model that finally were investigated by the experts. Finally, our findings were that the model created effective results because it increased the accuracy of any transaction. Moreover, it supported facilitate sharing, and log services transparently. As a result, the experts agreed that the evaluation results based on criteria were achieved at a high level (the average score was at 4.48 and standard deviation was 0.103).**

***Keywords* - Blockchain; Transactions; Finance; Currencies; Thailand**

I. INTRODUCTION

Generally, the financial institutions in Thailand have mostly utilized the centralized database as core banking systems. In fact, the centralized database might be easily hacked and losing data from its vulnerable. Unlike centralized databases, the emerging of the decentralized database with blockchain technology takes advantage of trailing auditing the data verifications, real-time, trust, confidentiality, and so on [1-7].

Blockchain technology has been a disruptive force within multiple industries. Blockchains have the potential to change almost every industry, especially of the system of financial institutions are revolutionizing and domains while bringing forward newer business models. Nowadays, IDC's latest Worldwide Semiannual Blockchain Spending Guide covers Gartner's irrational exuberance phase and forecasts a compound annual growth rate of 81.2 percent from 2016 with total spending of $9.7 billion in 2021 [8]. The biggest blockchain investments will increase over 40 percent of worldwide spending and will be made by the US during this period, followed by Western Europe, China, and Asia/Pacific [8].

As a result, Gowlings expert panel identified a wide range of sectors, that will be particularly benefited from the blockchain headed by banking and financial institutions [8]. Especially, Thailand is the beginning phase of blockchain technology development. However, the researchers currently reveal that transaction distributed ledger related to the digital currency in financial transactions still has the issue. Digital currency is not effectively

trusting and accepted in some governances of the central validation, as well as they are less insulated from the law's reach than it seems [9].

According to the issue, we came up with the problem statement "How users can trust the financial transaction, especially the transactions involving digital currencies?". Toward the phase the beginning to develop distributed ledger with blockchain technology to support the trust of financial based systems to confirm the legal and governance regulations.

In this paper, we propose the evaluating model of the transactions involving digital currencies with blockchain technology. We adopt foundationally concepts of blockchains and Ethereum platform by using MyEtherWallet as a research tool to verify the transaction of digital currencies as proof of concepts. Additionally, the research findings can be applied to support Thailand 4.0 development in the future.

Our paper is organized by followings: section 1 introduction, section 2 discusses literature reviews of related works. section 3 discusses the problem overview. Our model and the experimental results are provided in Section 4 and 5 respectively. Finally, a conclusion is given in section 6 with future works for the next generations.

II. LITERATURE REVIEW

A blockchain is essentially a decentralized distributed database or a ledger to support in financial services. The benefit of blockchain is to increase data transparency, security, asset management, and smart contracts, without the intermediary [10-14]. That to make the user's digital currency reduce time and cost [7, 15-18].

Recently, blockchain technology becomes in the Ethereum blockchain version 3 in the concepts of smart contracts allows users to write programs into the currencies [12]. An Ethereum blockchain network consists of multiple nodes belonging to miners and some nodes that to help in the execution of smart contracts and transactions as EVMs. Each node is connected to another node on the network and node use peer-to-peer protocol to contact to each other [2-5].

In theorem, a decentralized distributed database definitely defines as follow [2, 10-14]:

The Definition I: The blockchain - A set of transactions, blocks linked as a chain, validation of the block with timestamp, and consensus containing a hash of the previous blocks. It is shown as Eq. (1) [2-5].

$$\text{Blockchain} \in \{\text{Block, Chain, Validation, Consensus}\} \quad (1)$$

The Definition II: The validation - the security insides blockchain technology significantly are the public and private keys using the SHA256 hashing algorithm and function with any length of input will always generate 256-bits output data. The public key is the numbers generate and random by the network, called the user's address and is stored in the blockchain. Unlike a public key, the private key seems a virtual password in order to allow the user access to do transactions [10-14].

The Definition III: The consensus - every block contains a hash of the previous block, thus creating a chain of blocks linked with each other. Every node in the network holds a copy of the blockchain which is consensus in forms of proof-of-work (PoW) or proof-of-stake (POS) are various consensus protocols used to keep the blockchain secure? Depending on the consensus protocol, the blocks are created and added to the blockchain differently [10-14].

From the technical of distributed ledger processing is similarly as a state transition system. where is a "state" that consisting of the owner status of all Ether and a "state transition function" that showing a state, a transaction and outputs of the state which is the result in banking system [13-14].

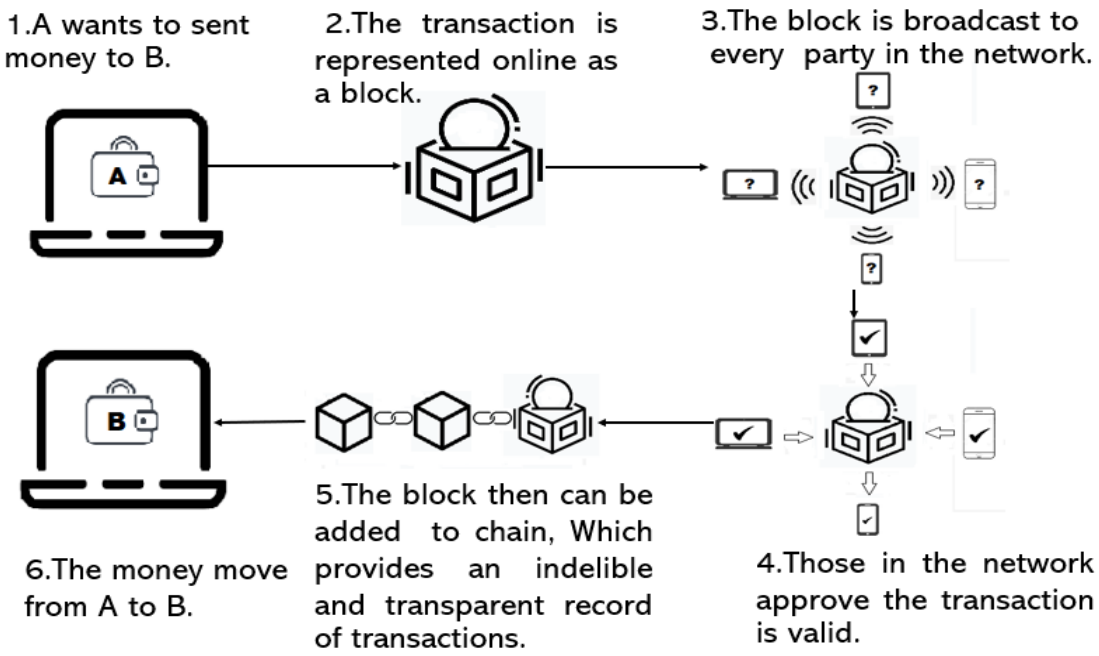

Figure 1. Digital Currency Transaction Processing [15].

The "state (S)" in ETH is the collection of all coins (technically, "unspent transaction outputs" or UTXO) that it has been minted and not yet spent, with each UTXO having a denomination and an owner (defined by 20-byte address which is essentially the cryptographic public key [14]). A transaction (TX) contains one or more inputs, with each input containing a reference to an existing UTXO and a cryptographic signature produced by the private key associated with the owner's address (S and S'), and one or more outputs, with each output containing a new UTXO to be added to the state. The state transition function APPLY(S, TX) -> S' can be defined roughly as follows [14]:

Begin:
For each input in TX:
{
If {the referenced UTXO =! in S} return ERROR;

If {the provided signature does not match the owner of the UTXO} return ERROR;

If the {the sum of the denominations of all input UTXO is less than the sum of the denominations of all output UTXO} return ERROR;

Return S and all input UTXO Removed;
Add all output UTXO;
}
End;

For example, the state is a balance sheet, a transaction is a request to move $X from Mrs. Alice (A) to Mr. Bob (B), and the state transition function reduces the value in A's account by $X and increases the value in B's account by $X. If A's account has less than $X in the first place, the state transition function returns an error [14]. Hence, the financial transaction in blockchain can formally process as followings:

Step 1: APPLY(S, TX) > S' or ERROR

Step 2: APPLY({ Alice: $50, Bob: $50 }, "send $20 from Alice to Bob") = { Alice: $30, Bob: $70 }

If APPLY({ Alice: $50, Bob: $50 },"send $70 from Alice to Bob") = ERROR

The first step prevents transaction senders send coins (ETH) that do not exist. The middle half's first step prevents transaction senders send coins to other user's coins and the second step control treat of value to use for payment is an example. Alice wants to send the total

amount of 11.7 ETH to Bob. Step 1st, Alice will check an available UTXO in her asset total balance of 11.7 ETH. Actuality, Alice will not be able to get exactly 11.7 ETH. Because at her asset can get is 6+4+2=12 [14]. Then Alice creates a transaction with 3 inputs and 2 outputs. But 1st step output will be 11.7 ETH with Bob's address as its owner, and the 2nd output will be the remaining 0.3 ETH "change", with the owner being Alice herself [14].

III. PROPOSED MODEL

The purposed model is developed by using MyEtherwallet (MEW) [19] as a research tool to evaluate the model and verify proof of concept. MEW is a wallet used to send and receive ETHER using ERC-20 Tokens to invoke smart contact to manage ETH, as well as helping in executing transactions on the Ethereum network. The network can be public or private. MEW is an opensource platform for crypto users to make financial transaction through their digital wallet accounts, such as to send and receive ETHER by using ERC20 Token [19].

In this section, we design the evaluating model of the financial transactions involving digital currency as shown in the activity diagram (Figure 2). The activities continue starting from state 1 (S01) to the final state (S06). Each state is in sequence for the mechanisms of the digital transactions following Eq. (1) below.

Begin:

S01 - sender send the amount payable to the receiver.

S02 - the transection creates in block that sender requests and broadcasts to a peer to peer transaction to all node in the network to check the validation of transactions.

S03 - then all nodes in network validate who send a request transaction by using the validation mechanism as private and public key cryptography to identify and verify ownership of transactions.

S04 - then nodes in network mining by using PoW of consensus mechanism as the agreement between nodes in a network. After finish consensus, the transactions and PoW are valid. The nodes in a network accept and update the copy of the transaction. Definitely, the transaction is verified and confirm of transaction successful.

S05 - the status of the validation of transactions is valid and processing to send money to the receiver. Then the chain added with a new block will be created.

S06 - the transaction is completed. The receiver receives the amount of payment from the sender.

End;

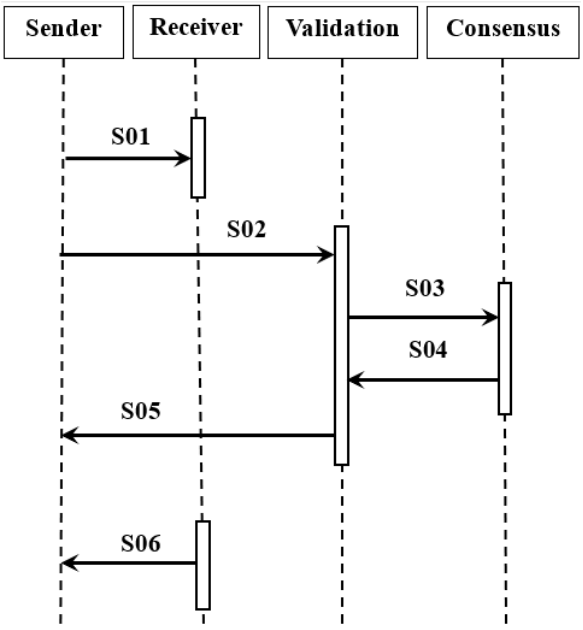

Figure 2. Flow to Verify the Transaction of Digital Currency.

IV. THE EXPERIMENT

In the experiment, we invite the experts to conduct the test and proof of our model using MyEhterwallet. In the evaluation, we conduct the steps of scenarios (S01 – S06) using Likert's scale [20] of quantitative measurement following the standard of the transactions involving digital currencies with the blockchain evaluation as follows: 4.50 – 5.00 is highest, 3.50 – 4.49 is high, 2.50 – 3.49 is medium, 1.50 – 2.49 is low and 0.00 – 1.49 is lowest shown in Table I.

TABLE I
THE CRITERIA OF THE EVALUATING TRANSACTIONS INVOLVING DIGITAL CURRENCIES WITH THE BLOCKCHAIN

Score	Levels	Description
4.50 to 5.00	The Highest	There has the system, mechanism, process, the procedure for maintenance and checking according to indicators, apparent, accurate for applying to follow operation guidelines of digital currency.
3.50 to 4.4.9	High	There has the system, mechanism, and process, that apply to support implementation, operation. Also, can be modified or developed of elements, new features or functions to properly support the operation and accuracy of digital currency.
2.50 to 3.49	Medium	There has lacked the system, mechanism, and some process, that can't apply to support implementation or operation. But can make modified or developed of elements, features or functions to properly support the operation and accuracy of digital currency.
1.50 to 2.49	Low	Low-level of criteria due to lack of system, mechanisms of digital currency as follow of indicators. Can't actual operation if want to apply to use must to modify a lot.
0.00 to 1.49	The Lowest	Minimum-level of criteria. There doesn't have the system, mechanism, and procedure of operation, monitoring, and improvement of indicators. Cannot apply digital currency to use.

V. THE FINDINGS

The result of our model evaluation regarding transactions involving digital currencies with the blockchain is gathered from the experts. We found that the result of the average score is at a high level. The standard deviation (S.D.) is between 0.201-0.213 which is represented as an appropriated 4.48 and S.D. is 0.103) as shown in Table II.

TABLE II
THE RESULTS OF EVALUATING THE TRANSACTIONS INVOLVING DIGITAL CURRENCIES WITH THE BLOCKCHAIN

No.	Description	Levels		
		$\bar{X}$	S.D.	Result
1	Accuracy of transactions involving digital currencies with the blockchain	4.76	0.139	The Highest
2	Security of transactions involving digital currencies with the blockchain	4.75	0.045	The Highest
3	Friendly to apply use, transactions involving digital currencies with the blockchain	4.13	0.125	High
4	Transparency and reliability of transactions involving digital currencies with the blockchain	4.63	0.098	The Highest
5	Suitability of transactions involving digital currencies with the blockchain	4.13	0.108	High
Average Score		**4.48**	**0.103**	**High**

In Table II, the researcher analyzed as followings:

1) Accuracy of transactions with digital currencies with the blockchain evolution is the highest level. With an average's score is 4.76 and S.D. is 0.139 by the opinion of most experts that the transaction is correct.

2) Security of transactions involving digital currencies with the blockchain evolution is the highest level. With an average's score is 4.75 and S.D. is 0.045 by the opinion of most experts that the functionality asymmetric encryption with SHA256 is security and distributed leader database to the node of each block (do not store user's computer). Cannot fraudulent.

3) Friendly to apply using is high level. With an average's score is 4.13 and S.D. is 0.125 by the opinion of most experts that

difficult of beginners. Therefore, beginners should have training in using to understand the concept and process.

4) Transparency and reliability of transactions involving digital currencies with the blockchain is the highest level. With an average's score is 4.63 and S.D. is 0.098 by the opinion of most experts that the verifying of checking and recording transaction is transparency and reliability. The transaction has been recorded will not be able to delete or modify.

5) Suitability of transactions involving digital currencies with the blockchain is high to apply to use with an average's score is 4.13 and S.D. is 0.108 by the opinion of most experts that Thailand is beginning of phase to apply using digital currencies with blockchain.

VI. CONCLUSIONS

In this paper, we aim to evaluate the model of financial transactions involving digital currencies with the blockchain. Our findings can proof our model such as Ethereum platform can create consensus, trust, security, and privacy, including the accuracy with reliability. Our result is similar to [1-7, 15-18] that found the distributed ledger can increase the accuracy by transparently monitor, keep traces of any asset, facilitate sharing, and exchange services effectively. As a result, the experts agree that the evaluation results based on criteria of the accuracy, the security perspectives, user-friendly, the transparency, the reliability, and Suitability of transactions are at a high level (the average score is at 4.48 and S.D. is 0.103). In the future, we continue to work to improve the model with smart contact development.

REFERENCES

(Arranged in the order of citation in the same fashion as the case of Footnotes.)

[1] Buatongjun, V. (2018). The Implement Prototype in Trusted Digital Cooperative Service System in Thailand using Blockchain Application.

[2] Crosby, M., Pattanayak, P., Verma, S., & Kalyanaraman, V. (2016). Blockchain technology: Beyond Bitcoin Applied Innovation, 2(6-10): 71.

[3] Geoffrey, G. & Aste, T. (2019). Can Cryptocurrencies Preserve Privacy and Comply with Regulations?. Frontiers in Blockchain, 2: 4.

[4] Pichada, S., Khunthi, S., & Chomsiri, T. (2019). Design of Blockchain Lottery for Thai Government. In 2019 Joint International Conference on Digital Arts, Media and Technology with ECTI Northern Section Conference on Electrical, Electronics, Computer and Telecommunications Engineering (ECTI DAMT-NCON), IEEE, 9-12.

[5] Nikola, B., Pujolle, G., & Secci, S. (2016). A tutorial on blockchain and applications to secure network control-planes. In 2016 3rd Smart Cloud Networks & Systems (SCNS), IEEE, 1-8.

[6] Trent, M., Marques, R., Müller, A., De Jonghe, D., McConaghy, T., McMullen, G., Henderson, R., Bellemare, S., & Granzotto, A. (2016). BigchainDB: a scalable blockchain database. White Paper, BigChainDB.

[7] Alexis, C. & Sok, K. (2016). Blockchain / distributed ledger technology (DLT): What impact on the financial sector?. Digiworld Economic Journal, 103.

[8] IDC. (2018). Worldwide Semiannual Blockchain Spending Guide. Retrieved from <https://www.idc.com/getdoc.jsp?containerId=prUS43526618>.

[9] Werbach, K. (2018). Trust, but verify: Why the blockchain needs the law. Berkeley Tech, LJ, 33: 487.

[10] Swan, M. (2015). Blockchain: Blueprint for a new economy. O'Reilly Media, Inc.

[11] Ritesh, M. (2018). Solidity Programming Essentials: A beginner's guide to build smart contracts for Ethereum and blockchain. Packt Publishing Ltd.

[12] Chris, D. (2017). Solidity programming. In Introducing Ethereum and Solidity. Apress, Berkeley, CA, 69-88.

[13] Satoshi, N. (2008). Bitcoin: A peer-to-peer electronic cash system.

[14] Vitalik, B. (2014). A next-generation smart contract and decentralized application platform white paper.
[15] Mamun, S.A. & Musa, S. (2017). BLOCKCHAIN. Cost Manag, 45(5): 2-8.
[16] Michael, N., Gomber, P., Hinz, O., & Schiereck, D. (2017). Blockchain Business & Information Systems Engineering, 59(3): 183-187.
[17] Zibin, Z., Xie, S., Dai, H.N., Chen, X., & Wang, H. (2018). Blockchain challenges and opportunities: a survey. International Journal of Web and Grid Services, 14(4): 352-375.
[18] Deepak, P., Malik, N., Mohanty, S.P., Kougianos, E., & Das, G. (2018). Everything you wanted to know about the blockchain: Its promise, components, processes, and problems. IEEE Consumer Electronics Magazine, 7(4): 6-14.
[19] MyEtherWallet Team. (2018). Myetherwallet. Retrieved from <https://www.myetherwallet.com/>.
[20] Allen, I.E. & Seaman, C.A. (2007). Likert scales and data analyses. Quality progress, 40(7): 64-65.