Aptisi Transactions on Technopreneurship (ATT)
Vol. 5 No. 1 March 2023

P-ISSN: 2655-8807
E-ISSN: 2656-8888

Transformation of Payment in Education Use Bitcoin with Reduced Confirmation Times

Henderi[1], Qurotul Aini[2], Danny Manongga[3], Irwan Sembiring[4], Dwi Apriliasari[5]
University of Raharja[1,2,5], Universitas Kristen Satya Wacana[3,4]
Jl. Jenderal Sudirman No.40, Cikokol, Kec. Tangerang, Kota Tangerang, Indonesia[1,2,5]
Jl. Diponegoro No.52-60, Salatiga, Kec. Sidorejo, Kota Salatiga, Indonesia[3,4]
e-mail: henderi@raharja.info[1], aini@raharja.info[2], danny.manongga@uksw.edu[3], irwan@staff.uksw.edu[4], dwi.apriliasari@raharja.info[5]

Author Notification
25 October 2022
Final Revised
24 November 2022
Published
08 December 2022

Henderi, Aini, Q., Manongga, D., Sembiring, I., & Apriliasari, D. (2022). Transformation of Payment in Education Use Bitcoin with Reduced Confirmation Times. Aptisi Transactions on Technopreneurship (ATT), 5(1), 1–8.

DOI: https://doi.org/10.34306/att.v5i1.285

Abstract

Significant changes in the financial system are prompted by the growth of the national economy, particularly as a form of payment. The means evolved from barter to things or commodities to metal and paper as the base materials for money before arriving at barter. With such significant changes, there is also a need for a transformation in the world of education in order to welcome technological advancements and one way to survive the changes in the increasingly rapid digital era. As the economic need increases, trade transaction methods shift from traditional to internet-based. One of the necessary international online payment options is bitcoin. For many applications where payments are modest and instantaneous approval is required, Bitcoin is inappropriate because of the high transaction fees and long confirmation periods. As a result, despite the introduction of numerous rival cryptocurrencies to address these problems, the Bitcoin network continues to be the most extensively used payment method. Unquestionably, ***new finding of this research*** *that effectively address the problems of high transaction costs and transaction verification times are needed if the company is to benefit from its user network. The Lightning Network (LN), which makes use of off-chain bidirectional payment channels between participants, is one of the most recent payment network concepts to be proposed.*

Keywords: *Bitcoin, Payment, Education.*

1. Introduction

The nation's economy has experienced significant changes as a result of its rapid expansion in the areas of finance, investment, and trade. One of the biggest disruptions to the economy has come from the use of Bitcoins in financial transactions. Both a national and global financial innovation, bitcoin represents both. The legality of Bitcoin as money is still a driving force behind its development. Given that bitcoin is a brand-new, entirely digital payment system with a supported conventional network, the study's objective is to use it in education. Another way to think of bitcoin is as electronic money that operates on a peer-to-peer (or user-to-user) network system. Although pure peer-to-peer (P2P) money transfers and transparency against censorship have been made possible by Bitcoin, it has long been criticized for its sluggish transaction confirmation times and expensive transaction fees.

As is generally known, manual transaction processes are no longer open and trusted in the field of education. Through this challenge, we will experience a revolution in Bitcoin

technology [1]. Transactions in bitcoin are kept in blocks, which are then typically verified by nodes known as miners. It takes an average of 60 minutes for a transaction to be accepted as authentic when it is 6 blocks old, according to a common heuristic. The Bitcoin block creation time is predicted to be around 10 minutes. Normal transactions, however, will take longer to be approved during busy periods since miners prefer transactions with higher fees.In that situation, the sender has two options: accept a steep fee or wait until a miner accepts the transaction request [2] [3]. Payees had to wait an average of 1188 minutes or pay more than $20 in transaction fees during one such extreme event, the 2017 Bitcoin boom. As a result, apps expecting timely payment evidence cannot use such transaction confirmation timings. Transaction fees are also inappropriate. Bitcoin simplifies payments by removing the need for a middleman, credit card, or bank account. Digital money known as Bitcoin can be used in place of traditional money when making purchases and sales online. It is stored electronically [4] [5]. Unlike other forms of virtual currency that are linked to banks and employ payment methods like Paypal [6]. In this essay, we suggest utilizing bitcoin as a transparent payment method in the field of education. Bitcoins are directly traded thanks to their special characteristics. The book Bitcoin: A Practical Guide to Understanding, Mining, and Earning can be read without the involvement of middlemen. Users receive bitcoin in different amounts. The resulting virtual currency is called cryptography, and it is predicted that it will grow in the future [7] [8]. The concept of a cryptocurrency is quite innovative because it is indistinguishable from the accepted form of payment in terms of uniqueness and resistance to harm.

Bitcoin provides a simpler method of payment that does not require a bank account, credit card, or middleman. Bitcoin is money that is kept on a computer and can be used in place of traditional currency for buying and selling things online. Unlike other online currencies, which are linked to banks and use a payment mechanism like Paypal. The concept of Bitcoin is the resulting virtual money, and it is highly likely that cryptography (crypto-currency) will continue to flourish in the future. The idea of a cryptocurrency is actually very similar to the characteristics of a recognized, durable, and freely agreed-upon legal medium of trade. 2 Therefore, Bitcoin has the potential to become a global medium of trade.

Therefore, payment routing, attack/privacy protection, and the reduction or removal of potentially unjust transaction charges all require a highly decentralized topology [9] [10]. **For this research have novelty** to development of a private payment channel network in the educational sector that will bring together businesses to form a consortium and contribute to this payment network rather than relying on the dubious public network. Customers will be able to make micropayments using this approach, and businesses will get precise guarantees regarding their reliability, privacy, and monopoly. In this study, we propose constructing a private payment channel network architecture for educational transactions from scratch by utilizing the off-chain Bitcoin concept. In order to lessen the overall fee cost of network construction, our goal is to evenly distribute forwarding loads among all nodes while reducing the number of off-chain channels [11]. We start with an optimization model, inspired by the multi-commodity flow problem, that will optimally disperse the flow within an initial network topology. With the intention of offering a design framework for transaction payments with a decentralized and open Bitcoin system, this paper will contribute to the global development of the field.

The structure of this essay is as follows: The following part outlines the relevant research, and in Section 3 we describe the methodology. The discussion's outcome is explained in Section 4, and the paper's conclusion is provided in Section 5.

2. Related Work

2.1 Bitcoin

One of the numerous virtual currencies based on an algorithm that employs the essential ideas to develop a direct peer-to-peer transaction mechanism is Bitcoin [12]. The address propagation technique is implemented by the Bitcoin protocol to help peers find other peers in the P2P network. Each peer in the Bitcoin network maintains a list of the addresses of other peers, and each address is given a timestamp to indicate how recent it is [13] [14]. Peers can communicate using the GETADDR and ADDR protocols to seek addresses from this list and to advertise addresses that they already know. Each address in an ADDR message is evaluated by a Bitcoin node to determine whether or not it should be sent to its neighbors.

The Bitcoin blockchain is a hash chain of blocks, each of which starts with the first or "genesis" block and contains an ordered collection of transactions as well as a hash of the preceding block [15] [16]. A Bitcoin block contains nonces that a Bitcoin miner (i.e., a node trying to add a block to the chain) must set in such a way that the hash of the entire block is less than a specified target, which is normally a very tiny amount. This is the main feature of the hash chain, known as Proof-of-Work (PoW):

2.2 Solution for Communication between Bitcoin and DLCC Blockchains

Changing the BTC blockchain is a nearly hard and impossible process, despite the fact that Bitcoin is an open source system built on mathematical formulas [17] This is as a result of the system's initial design, which layers transactions on top of one another. As a result, it is challenging to track down modifications to the blockchain once they have been made. Therefore, it would be most practical to make the changes to a different blockchain, which would then be connected to the current and reliable Bitcoin blockchain [18].

Making a DLCC blockchain would offer a cutting-edge solution that could be applied to education. This new blockchain would initially make it possible to sign Smart Contracts. The Ethereum system has so far been the only one to support smart contracts. Tens of thousands of contracts and millions of dollars' worth of virtual currency are supported by the Smart Contract system, which was developed in 2015 and became popular in 2016 [19] [20]. Therefore, Smart Contracts would be the DLC's underlying technology. The benefits and drawbacks of smart contracts can be determined based on our observations.

- Rich contract rules expressible in programmable logic that allow for a fair transaction amongst parties who are skeptical of one another.
- By terminating an exchange protocol, this feature stops parties from cheating while doing away with actual meetings and (perhaps dishonest) third-party middlemen.
- Reduced potential for unauthorized monitoring and tracking due to little contact between parties for a wide range of contracts expressible in programmable logic.

2.3 Payment Channel Networks

In both the corporate and academic worlds, numerous recent initiatives have been made to solve the high transaction fees, slow confirmation times, and scalability issues with cryptocurrencies, particularly Bitcoin. Making a Payment Channel Network (PCN), as was done in this study, is one of these endeavors. The Bitcoin community first proposed the off-chain payment channel technique [21]. The community is actively improving the concept and developing new concepts, such as channel factories, watchtowers, macaroons, and so on [22] [11] [23], to increase network efficiency.

Our research in this paper falls under the first category, but it is distinct because none of the participants are well-known figures like LN or Raiden. We support the creation of a private PCN to serve the requirements of participants in an application-based business consortium.

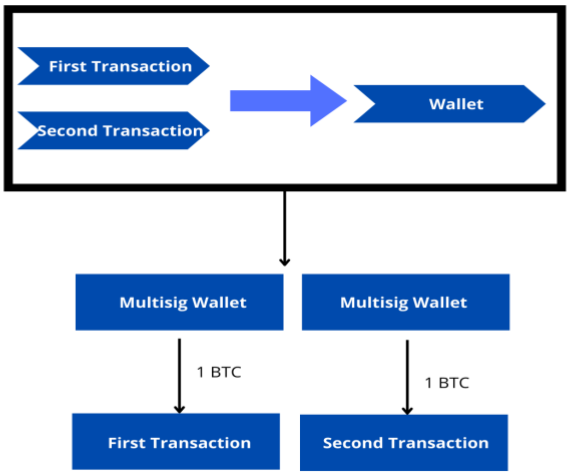

Figure 1. Illustrate Payment Network

3. Method

3.1 Deterrence by the Collapse of Credibility

An alternative strategy for preventing attacks through the decline in coin prices is necessary to tackle the problem. Our suggested substitute is a credibility crisis. To establish credibility and confidence, contractors need to be well acquainted with one another. A contractor's trustworthiness increases with the number of contracts he has with different parties. He thereby gains the respect of numerous individuals and establishes a solid reputation among numerous other parties.

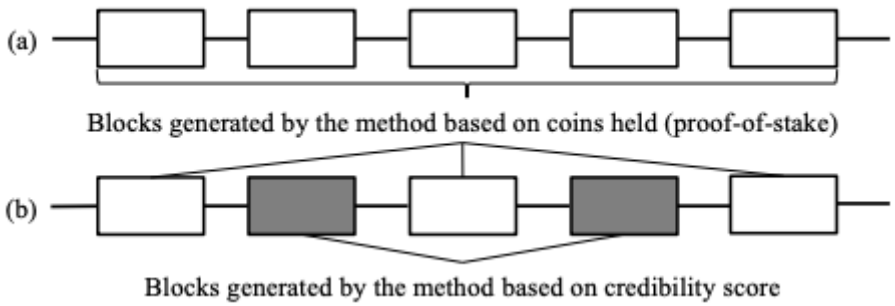

Figure 2. Generate Block in Transaction System

If he assaults it, the system risks losing faith not only in the blockchain network but also in society at large. Therefore, having a lot of credibilities rather than a lot of money serves as a deterrent. The number of parties the contractor engages into contracts with is one way we gauge their credibility. A credibility score is what we're talking about here. We suggest that a miner who creates a block produces evidence that he has a high enough credibility score to reach consensus in the blockchain network rather than utilizing proof-of-stake.

3.2 A proposal for a hybrid blockchain

However, when an illusory contract is involved, using a believability score rather than a stake poses a challenge. Regardless of whether a contract is real or not, a credit score is added. An attacker can simply raise his credibility rating by creating phony contracts with bogus party addresses. Because of this, an attacker with a high false credibility score may succeed in a 51% attack, and if he works with a node that has real contracts, they may be able to renew the contracts unlawfully.

Making a 51% attack cost more than it did previously is one solution. As a result, we suggest a novel mechanism for building a blockchain that is based on the aforementioned

credibility score method as well as proof-of-stake, another form of consensus technique. The consensus technique based on credibility score requires enough coins to be utilized in order to create contracts, but the proof-of-stake approach only requires enough coins to be kept. It is more challenging to increase both because keeping and using coins are two completely different ideas. The solution we provide uses both credibility score and proof of stake techniques to create a hybrid blockchain.

4. Result & Discussion

4.1 Problem motivation and definition

Although the LN concept is a great way to introduce Bitcoin to the micropayments market, the current structure of LN makes the deployment of relay nodes, which serve as a link between consumers and merchants, necessary. This brings up two significant issues: First off, the purpose of the payment network to reduce transaction prices is broken by the forwarding fees charged by these relay nodes. Second, when these relay nodes grow into significant hubs in the network, there is a greater chance that DDoS attacks will interrupt network payments at any time. Customer privacy is the third risk. The privacy of the clients is exposed if these relay nodes are compromised because it is simple for them to evaluate the payments that are traveling through them.

Due to these risks, any company may decide against adapting its payments to the current LN. Due to the following observations/problems with the current LN structure, this article makes the case that the creation of a private payment network necessitates a planned approach to creating a network topology from scratch: suggests that when customers and retailers haphazardly create payment channels over time, the simple payment mechanism in Fig. 2 will eventually evolve in a full payment network. Therefore, all payments are accepted inside LN. The main argument of this study is that, in the absence of a well-considered strategy, this assumption would not remain true over a substantial network size due to the following issues:

- For each channel, the following investment is needed: The cost of building a network will be high. Two on-chain transactions are required as a result of each channel setup. Because of this, a node should only create as many channels as necessary to maintain the flow of essential transactions.
- Partial use of the existing payment capacity: A node may decide that it needs 100 Bitcoins' worth of transactions per day to run. However, other nodes that rely on this node as a relay will often use up that capacity. Because of this, only a part of the capacity will ever be used. The node has the option to accept transactions from its own clients. This suggests that enterprises should invest far more than their anticipated transaction volume when joining forces to create a private payment network.

We propose to use the concept of creating payment channels among a consortium's retailers, assuming that each node in this network will create in-advance payment channels (i.e., links with specific transaction capacities) with some other nodes as needed. as shown in Figure 3. The participants' network is an overlay network built on top of the Bitcoin network that relies on channel establishment rather than the physical proximity of nodes. It is critical the nodes come to an understanding. However, in order to accomplish the advertised scalability, micropayment, and rapid confirmation capabilities, establishing such a network demands careful design in order to both guarantee fairness among collaborating nodes and to Share the associated costs.

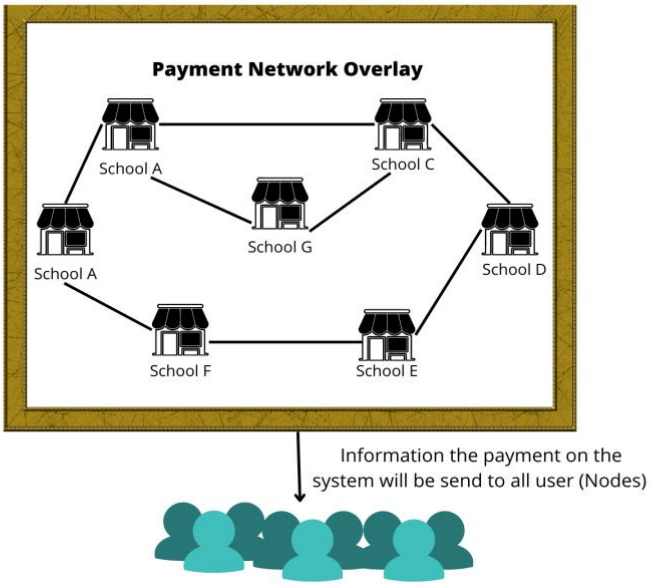

Figure 3. Payment Network Overlay

4.2 Flow and Network Optimization model

The PCN proposed in this work will provide virtual topology on top of on-chain operations, providing a beneficial infrastructure that can ensure P2P payment service without necessitating any on-chain transactions [24] [25]. When the network is designed, the payment channels connecting the stores should be able to send and receive payments meant for themselves. Additionally, it is important to build channel capacity amongst shops in a way that permits equal contributions to the network from business owners with comparable opportunities and intentions (i.e., business capacity). All of these issues are addressed by our approach, which is based on a mixed integer programming paradigm driven by multi-commodity network flow challenges.

5. Conclusion

In this study, we used IN technology to build a private Bitcoin payment network from the ground up for a marketplace with merchants and customers. We achieved a number of objectives while creating this payment network: **The contribution of this research** to get rid of expensive transaction fees and lengthy confirmation periods, we first used the offchain idea of LN. Second, we make sure that a connected payment network is created that can move any payments between customers and merchants while ensuring fairness among participating merchants so that the associated expenses are shared. Finally, by creating a pure P2P topology, we decreased the likelihood of privacy leaks as well as the success of DDoS attacks on the network.

References

[1] S. Watini, Q. Aini, U. Rahardja, N. P. L. Santoso, and D. Apriliasari, “Class DojoLMS in the Interactive Learning of PAUD Educators in the Disruption Era 4.0,” *J. Innov. Educ. Cult. Res.*, vol. 3, no. 2, pp. 215–225, 2022.

[2] D. Reijsbergen, S. Sridhar, B. Monnot, S. Leonardos, S. Skoulakis, and G. Piliouras, “Transaction Fees on a Honeymoon: Ethereum’s EIP-1559 One Month Later,” in *2021 IEEE International Conference on Blockchain (Blockchain)*, 2021, pp. 196–204.

[3] M. I. Sanni and D. Apriliasari, “Blockchain Technology Application: Authentication System in Digital Education,” *Aptisi Trans. Technopreneursh.*, vol. 3, no. 2, pp. 37–48, 2021.

[4] U. Rahardja, Q. Aini, E. P. Harahap, and R. Raihan, “GOOD, bad and dark bitcoin: a

systematic literature review," *Aptisi Trans. Technopreneursh.*, vol. 3, no. 2, pp. 115–119, 2021.

[5] R. Widhawati, A. Khoirunisa, N. P. L. Santoso, and D. Apriliasari, "Secure System Medical Record with Blockchain System: Recchain Framework," in *2022 International Conference on Science and Technology (ICOSTECH)*, 2022, pp. 1–8.

[6] S. Darwish, A. A. Abdul Rahman, and A. Meero, "Libra Currency and its Global Financial and Economic Impact," in *The International Conference On Global Economic Revolutions*, 2021, pp. 20–31.

[7] P. R. Cunha, P. Melo, and H. Sebastião, "From bitcoin to central bank digital currencies: Making sense of the digital money revolution," *Futur. Internet*, vol. 13, no. 7, p. 165, 2021.

[8] B. Rawat, A. S. Bist, U. Rahardja, C. Lukita, and D. Apriliasari, "The Impact Of Online System on Health During Covid 19: A Comprehensive Study," *ADI J. Recent Innov.*, vol. 3, no. 2, pp. 195–201, 2022.

[9] R. Widayanti, Q. Aini, H. Haryani, N. Lutfiani, and D. Apriliasari, "Decentralized Electronic Vote Based on Blockchain P2P," in *2021 9th International Conference on Cyber and IT Service Management (CITSM)*, 2021, pp. 1–7.

[10] H. Latifah and Z. Fauziah, "Blockchain Teaching Simulation Using Gamification," *Aptisi Trans. Technopreneursh.*, vol. 4, no. 2, pp. 184–191, 2022.

[11] A. Parsa and N. Moghim, "QoS-aware routing and traffic management in multi-flow opportunistic routing," *Comput. Electr. Eng.*, vol. 94, p. 107330, 2021.

[12] S. Ahamad, P. Gupta, P. B. Acharjee, K. P. Kiran, Z. Khan, and M. F. Hasan, "The role of block chain technology and Internet of Things (IoT) to protect financial transactions in crypto currency market," *Mater. Today Proc.*, vol. 56, pp. 2070–2074, 2022.

[13] E. Retnaningtyas, E. Kartikawati, and D. Nilawati, "Upaya Peningkatan Pengetahuan Ibu Hamil Melalui Edukasi Mengenai Kebutuhan Nutrisi Ibu Hamil," *ADI Pengabdi. Kpd. Masy.*, vol. 2, no. 2, pp. 19–24, 2022.

[14] P. Hillmann, M. Knüpfer, E. Heiland, and A. Karcher, "Selective Deletion in a Blockchain," in *2020 IEEE 40th International Conference on Distributed Computing Systems (ICDCS)*, 2020, pp. 1249–1256.

[15] D. Immaniar, A. A. Aryani, and S. Z. Ula, "Challenges Smart Grid in Blockchain Applications," *Blockchain Front. Technol.*, vol. 2, no. 2, pp. 1–9, 2023.

[16] G. Kaur and C. Gandhi, "Scalability in blockchain: Challenges and solutions," in *Handbook of Research on Blockchain Technology*, Elsevier, 2020, pp. 373–406.

[17] P. A. Sunarya, U. Rahardja, L. Sunarya, and M. Hardini, "The Role Of Blockchain As A Security Support For Student Profiles In Technology Education Systems," *InfoTekJar J. Nas. Inform. dan Teknol. Jar.*, vol. 4, no. 2, pp. 13–17, 2020.

[18] A. Kolluri, I. Nikolic, I. Sergey, A. Hobor, and P. Saxena, "Exploiting the laws of order in smart contracts," in *Proceedings of the 28th ACM SIGSOFT international symposium on software testing and analysis*, 2019, pp. 363–373.

[19] E. Guustaaf, U. Rahardja, Q. Aini, H. W. Maharani, and N. A. Santoso, "Blockchain-based education project," *Aptisi Trans. Manag.*, vol. 5, no. 1, pp. 46–61, 2021.

[20] Q. Aini, S. Santoso, R. Supriati, A. Badrianto, and T. Ramadhan, "Analysis of the potential context of Blockchain on the usability of Gamification with Game-Based Learning," 2021.

[21] N. Septiani, N. Lutfiani, F. P. Oganda, R. Salam, and V. T. Devana, "Blockchain Technology in the Public Sector by Leveraging the Triumvirate of Security," in *2022 International Conference on Science and Technology (ICOSTECH)*, 2022, pp. 1–5.

[22] V. Sivaraman *et al.*, "High throughput cryptocurrency routing in payment channel networks," in *17th USENIX Symposium on Networked Systems Design and Implementation (NSDI 20)*, 2020, pp. 777–796.

[23] Y. Zhu, J. He, K. Yuan, and Y. Yang, "Research on Modify Protection of Metrology Electronic Certificate Based on Blockchain Technology," in *2019 14th International Conference on Computer Science & Education (ICCSE)*, 2019, pp. 1020–1024.

[24] A. Alwiyah, S. Sayyida, P. A. Sunarya, and D. Apriliasari, "Inovasi Manajemen Pengajuan Judul Kuliah Kerja Praktek (KKP) berbasis Laravel Framework,"

Technomedia J., vol. 7, no. 2, pp. 168–180, 2022.
[25] S. A. Faaroek, A. S. Panjaitan, Z. Fauziah, and N. Septiani, “Design and Build Academic Website with Digital Certificate Storage Using Blockchain Technology,” *IAIC Trans. Sustain. Digit. Innov.*, vol. 3, no. 2, pp. 175–184, 2022.