Blockchain Frontier Technology (B-Front)
Vol. 2 No. 2 January 2023

P-ISSN: 2808-0831
E-ISSN: 2808-0009

Challenges of Bitcoin Blockchain Technology in Real-World Apps

Rizky Amien Fauzi[1], Indrawan Nugroho[2], Janu Ilham Saputro[3], Dimas Mahesa[4], Muhammad Daffa Fadhillah[5]
Information Systems, University of Raharja[1,2]
Master in Management, University of Raharja[3]
Accounting Computer, University of Raharja[4,5]

e-mail: rizky.amien@raharja.info, indrawan@raharja.info, janu@raharja.info, dimas.mahesa@raharja.info, daffa.fadhillah@raharja.info

Author Notification
01 January 2023
Final Revised
04 January 2023
Published
05 January 2023

Fauzi, R. A., Nugroho, I., Saputro, J. I., Mahesa, D., & Fadhillah, M. D. (2023). Challenges of Bitcoin Blockchain Technology in Real-World Apps. Blockchain Frontier Technology, 2(2).
DOI: https://doi.org/10.34306/bfront.v2i2.207

Abstract

Blockchain is the newest innovation in the fields of internet of things, social media, and cloud computing. Blockchain has quickly become a force to be reckoned with thanks to its reputable uses and rapid development. However, the application of blockchain is not just restricted to bitcoin or other cryptocurrencies. This paper clarifies blockchain requirements outside of bitcoin. In addition, this study offers insights into the mechanics, problems, and evolution of blockchain technology based on a literature review. The difficulties or difficulties in applying blockchain technology to real-world applications were identified in this study. The main issue that needs to be solved is how to securely utilize blockchain technology on small-scale applications.For the secure deployment of the blockchain on small-scale applications or projects, the proposed consensus mechanism might be helpful.

Keywords: *Smart Contracts, Blockchain Technology, Bitcoin, P2P (peer to peer), Lightning Network, POS (Proof of Stake)*

1. Introduction

As the name suggests, a blockchain is a single linked list of blocks, where each block contains many transactions or other types of information. It gives users access to a decentralized, immutable data format that they may use to generate assets, record transactions, and use throughout a network of users [1]. Each type of data is accessible and allows for better transparency and trust amongst all stakeholders. Introducing a decentralized solution without the need for third-party transactions is the goal of blockchain technology [2]. Blockchain has demonstrated to be a more than suitable answer to a number of problems, including:

1. Data sharing between organizations.
2. Registration of digital assets (using bitcoin coins as an example).
3. Identity management and integrity (using cryptographic identification, for example).

The blockchain protocol uses a peer-to-peer (P2P) network of computers to run on top of the internet. Every user has a copy of the transaction ledger that is exact. Through machine consensus, enabling P2P value provides us with the means to trade information without the use of an intermediary [3]. Blockchain is merely a file that is kept on your computer and broadcast to other users on the network in order to share information and the most recent update of the data. Because the blockchain is based on a distributed consensus system, or DCS, it guarantees both integrity and security. "If everyone could agree, it would work." The remainder of the essay is structured as follows. The literature on bitcoin and blockchain

technology is detailed in Section 2. The issues with blockchain technology are clarified in Section 3. The answer to the main problems with blockchain application is presented in Section 4. Section 5 brings the paper to a close [4].

2. Literature Review

Stuart Haber and W. Scott Stornetta introduced the idea of a secured chain of blocks in 1991. Bayer, Haber, and Stornetta included the "Merkle trees" method to the system's design, which increased efficiency overall by allowing several documents or pieces of information to be combined into a single block [5]. The initial research report on bitcoin, which was published in 2008 by Satoshi Nakamoto, whose identity is still unknown, outlined a P2P system that can be used to securely move funds from one location to another and is also known as bitcoin. One of today's most revolutionary technologies, the blockchain has grown over the past ten years.The 2.0 version of blockchain, which started to take shape in 2016, allows users to access external data or events at any moment as dictated by market conditions [6]. Midway through 2016, IBM opened a blockchain research facility in Indonesia for a World Economic Forum working group to create blockchain models for usage in governmental and other institutions. According to the findings of that research center's study, the use of the blockchain by financial services and institutions reached about 14% in 2016. Given the openness of the blockchain mechanism, hostile attacks were also partly possible, which led to the development of new strategies for implementing blockchains as private, permissioned networks [7]. In the working world today, there are three primary varieties of blockchain, which are mentioned as follows:

Public blockchain: This class of blockchain applications allows anybody to join the network, such as bitcoin and ICO networks, without any access restrictions. The network is open to anyone with an internet connection. Additionally, the user can take part in task completion by either approving transactions (mining) or by just making transactions [8].

Blockchain that is private and has permissions: A private blockchain has permissions. A single person cannot join on their own without the network's invitation. A set of requirements that must be satisfied before a user can join under user authentication, access control, and privileges can be used to create the invitation system [9]. For businesses looking to integrate blockchain technology into their infrastructures, this kind of blockchain might be seen as a medium ground. Banks, the real estate industry, and file distribution networks are a few examples. Examples of this kind of blockchain include FedEx, Walmart, and Multichain. Without user interference from the general public, these applications use the private blockchain implementation to securely distribute information across their network [10].

Blockchain Consortium: A blockchain consortium is a type of semi-decentralized data structure. It is governed by a single entity, just like a permissioned blockchain. The nodes, which are dispersed throughout the network, can function as a consensus system for any new data or blocks handled by the network [11] . The transaction of records is contained in a 20GB-sized bitcoin file. The size of the file has increased from 50 to 100 GB. The second iteration of the blockchain, known as blockchain 2.0, which first surfaced in 2014, featured programmable contracts and addressed several scalability difficulties [12].

A. Ethereum Blockchain Consensus Mechanism

The most recent blockchain applications go beyond just cryptocurrencies and a transactional ledger. The Proof of Stake (POS) Algorithm's implementation serves as the basis for this notion. This algorithm made sure that inefficient use of mining equipment was taken into account. Some terminology was changed, such as validators becoming miners and mining becoming minting or forging [13]. The Proof of Work (POW) algorithm, used in conventional currencies, determined who mined a block with the greatest amount of processing power and

who received the reward. When a new block is mined, the reward is paid, but in the POS algorithm, the validators are chosen at random based on their stake in the system, which is a certain amount of coins deposited as a security. As a result, less mining equipment is being used by each network node [14].

B. Blockchain 2.0

The blockchain technology served as a transactional ledger and stored the account values of the coins in bitcoin and other cryptocurrencies [15]. The community subsequently began developing additional blockchain applications that went beyond only financial ones. Blockchain that is "programmable" is a brand-new idea introduced by computer programmers. The authors present many methods for saving and viewing data saved on a blockchain, often known as smart contracts [16] . Similar to real-world contracts, smart contracts also carry out their obligations when predetermined criteria are satisfied. However, the contract itself uses a tiny computer software, which distinguishes it from a typical contract [17]. A blockchain is the foundation for smart contracts, which take on some of its characteristics like immutability. A smart contract's immutability makes it tamper-proof since once it has been created by any party, it cannot be modified [18]. Additionally, a blockchain smart contract inherits some of its traits, including:

Immutable: means that once a smart contract is made, it cannot be altered or changed for any reason, meaning that no one can secretly change the terms or code of the contracts you have produced.

Distributed: Being distributed means that your contract is made available to the public and that everyone on the network validates the results. Therefore, a single person cannot force the release of the funds; other network users can detect this and stop the attempt. It's possible that professional associations like banks, lawyers, brokerage services, and public administrators won't be deemed necessary for bitcoin transactions. With no friction and a small fraction of the present transaction costs, people, businesses, robots, algorithms, and programs might easily engage and transact with one another. Smart contracts can be used by organizations like banks or financial institutions to release payments automatically when particular conditions are met, reducing the chance of human error in the process.

3. Blockchain Challenges

Smart contracts and smart property are two components that make up blockchain technology. Due to the qualities and decentralized nature of blockchain, it can be utilized in a wide range of industries, such as private securities, insurance, internet finance, the internet of things, decentralized data storage, notary documents, and anti-counterfeit solutions [19]. The following list of existential issues with the use of blockchain technology is determined by this paper:

A. Blockchain Scalability Implications

Regarding the problems with the bitcoin blockchain, where a block took an average of 10 minutes to process. Due to this block creation time restriction, the blockchain for bitcoin could only process 7 transactions per second. While the majority of other transactions were put on hold while they awaited the mining of the following blockchain[20]. The Bitcoin network currently processes 10 million transactions each month, the majority of which are held in pending transactions [21]. While the majority of transactions can take up to 30 minutes or longer. Additionally, the cryptocurrency's viability started to be affected by the inflation-oriented coin supply limit. As there won't be any more coins produced after the original 21-million coin cap. This had an impact on the miners who verified the transaction in exchange for a reward

for building the blockchain [22]. Once this cap has been reached, miners will only receive transactional payments as compensation, which will be provided by the users carrying out the transactions. This restriction was put out to keep the network in check, much as banks are constrained in how much money they can produce, however it has had a significant negative impact on the "Demand and Supply" law of economics. Due to the limited availability of bitcoin, individuals have overstated its value; at the time this paper was written, one bitcoin (BTC) was worth nearly 7500 US dollars [23].

B. Blockchain Implementation In Small-Scale Applications

The security and integrity of the blocks were not an issue while taking into account larger-scale blockchain applications on cryptocurrencies [24]. Because the attacker would have to match the network's overall mining power. Additionally, the attackers would have to compute the hashes of each and every child block where the original block was modified, which is thought to be nearly hard. At the time of the survey on May 28, 2018, the overall bitcoin mining hash rate was estimated to be at 33 million TH/sec. That is practically impossible for any adversary to catch. According to our review of the relevant literature, the researcher has determined that the difficulty of securely implementing blockchain technology on current small-scale projects is a concern. When the network's hash rate is low, it would be simple for an attacker to mine a malicious block because they could equal the network's overall mining power [25].

5. Proposed Solution

The following are some strategies and techniques that are used in this section of the study to address the issues with the implementation of blockchain in real-time applications that have been uncovered by this research:

A. Using Segwit & Lightening Network Mechanisms, scalability issues are addressed

When addressing the scalability problem in blockchain, which has dogged the blockchain community since the invention of blockchain, the community working around bitcoin ran into a problem that is the enormous number of pending transactions due to blockchain's limit that could only handle 7 Transaction/sec. Segregated witness (Segwit) and the lightning network have been identified by this research's literature assessment as two innovative solutions that can address scalability problems.

i. Electric Network

The off-chain method is another name for the lightning network. This method is designed to reduce the burden on the primary blockchain and speed up the number of transactions that can be processed in a second. Payment Channels are a mechanism layer used by the Lightning Network, which is a mechanism layer constructed on top of blockchain. A balance sheet is stored in the payment channels. Both parties can use the balances recorded on the balance sheet to conduct transactions based on those balances. The primary blockchain experiences a decrease in workload, and transaction speeds significantly increase. Moreover, since the signatures and transactions won't be kept on the main blockchain, this approach is more advantageous than the Merkle tree. Parallel to the main blockchain, there is a payment channel that enables multiple transactions between two or more parties without broadcasting them to the entire network. The balances placed by both parties are combined into a single balance sheet when the payment channel is launched, though. This balance sheet is a digital ledger with the digital signatures of two or more parties. The balance sheet is updated and signed each time a user conducts a transaction, and the payment channel can be shut down at any time. To determine how

money should be transferred, the blockchain will verify the most recent version of the balance sheet. By using this technique, users can carry out thousands of transactions without having to save the majority of them on the main blockchain. Only two transactions will be recorded on the blockchain: one when a payment channel is formed and another when it closes. Furthermore, not everyone requires a payment channel to conduct transactions. Trades can be completed more quickly, more affordably, and with greater security when using one of the other payment channels as a middleman between two parties. This study offers a distinct viewpoint on the application of blockchain technology for small-scale projects as a quick and secure means of handling data. Users are able to build a network of swift and safe blockchains on both lower and higher network levels by utilizing all the mechanisms discussed in this paper.

ii. Mechanism of Segwit

Segwit employs a method to strip digital signature information from bitcoin transactions. More transactions can be added to the ledger when specific informational components of a transaction are removed. Signatures are included in a block of transactions as part of the input. A block's digital signature may occupy as much as 60% of the available space. Given that segwit removes the hash from the digital signature and stores it as a witness on the blockchain, its implementation may be more advantageous than the Merkle tree strategy. With this method, the "transaction malleability" issue that frequently arises in the Bitcoin blockchain system is resolved while also expanding block size.

B. Block Maturity Level Mechanism proposed to addressing modest projects

Relating to the problem of using blockchain technology to modest-scale projects. Due to security concerns, applying blockchain technology to small-scale projects might be risky. Due to the nature of the blockchain's consensus mechanism, which makes networks with fewer nodes more susceptible to manipulation, security vulnerabilities arise. This research suggests a consensus technique termed block maturity level to address the issue raised (BML).The short block is marked as "pending" by the proposed BML method, but all transactions contained within it will be approved by the miners. When six to eight new blocks have been prematurely mined, the status of that block will be changed from "pending" to "approved." Once at least 6 further blocks have been prematurely mined, the block will be put to the network. The BML method operates similarly to how a transaction is stored pending until a block is mined to add it to the ledger. By simply matching the total network hash power, the proposed BML technique will help to ensure that an attacker cannot intentionally alter the blockchain. Currently, the last block on the blockchain is the one that is most susceptible to attack and manipulation. An attacker only needs to add a new block and recalculate the hash to change the blockchain, but the implementation of the proposed BML mechanism will significantly lower the risk of any sort of alteration. As a result of having to calculate all the succeeding child blocks, the attacker and any other hostile network invader will have difficulties. Additionally, the BML process will make sure that the validation of a certain blockchain entails the least amount of risk possible without relying solely on the prior consensus algorithm. The "non matured" blocks can be utilized to identify any type of data modification or even invalidate the malicious blocks that are being added in by the attacker if any attempt is made to nullify the blockchain that is used in an institution. One aspect of this approach is to employ a high level of maturity, as the blockchain ecosystem will become increasingly inactive and congested the longer blocks are held waiting.

6. Conclusions

Blockchain is a ground-breaking technology that is bringing about revolutionary changes throughout all of our businesses, including the public and private sectors. This study has illustrated the use and consequences of blockchain technology in many scenarios. The features extend beyond the segments, with reference to the implementation of the consensus method, and do not merely relate to the immediate notion of cryptocurrencies and payments (Blockchain 1.0), or to contracts, property, and all financial markets (Blockchain 2.0). The security and scalability issues are probably of concern to the businesses. Every industry, including government, healthcare, science, literacy, the arts, and culture, can use blockchain technology. similar to any advanced technology. However, it must also be handled very carefully when it comes to handling people's funds because doing so will encourage the growth of larger, smarter ecosystems that could contain new ideas. The main difficulties that the blockchain community has encountered while implementing blockchain in practical applications have been identified in this article. The two primary issues that this research has found are the scalability issue and the use of blockchain in small-scale projects. One of the major issues this study identifies is scalability. The scalability problem is addressed by Segwit and lightning techniques. In this research article, another issue that has been brought up is the security concerns associated with applying blockchain technology to small-scale applications. In order to overcome the security concerns of using blockchain on small scale applications, this research has developed the BML consensus mechanism. The ideas offered in this paper can offer a fresh viewpoint on data handling efficiency, robustness, security, and deployment of blockchain in practical applications.

7. Future Directions

Many current issues can be solved with blockchain technology. The supply-chain and logistics sector is one of the prospective industries. Both small-scale and higher-level network implementations are made viable by the solution offered in this study. Beyond the effects that blockchain will have on the sector, the majority of business entities are still unwilling to integrate blockchain into their infrastructure. The proposed consensus approach will significantly enhance the system's security and data handling. Additionally, it will offer a fresh viewpoint on the consequences and application of blockchain technology in other sectors.

References

[1] A. Suryadi, “The Implementation Of Turbine Ventilator As An Alternative Power Plant,” *ADI J. Recent Innov.*, vol. 2, no. 1, pp. 1–6, 2020.

[2] S. F. Meilana, “Development Professionalism Strategy In Lecturers Improve The Competitiveness Of The Nation Through The Development Of Science And Technology,” *ADI J. Recent Innov.*, vol. 2, no. 1 Sept, pp. 222–226, 2020.

[3] N. L. P. G. S. Kusuma, P. E. T. Dewi, and N. P. R. K. Sari, “Regulation of Copyright Certificate as a Material Guarantee and Bankrupt Estate/Beodel in Indonesia,” *ADI J. Recent Innov.*, vol. 2, no. 2, pp. 290–303, 2020.

[4] K. Khasanah, “The Effect of Lecturer Professionalism and Teaching Motivation on Lecturers Strengthening the Nation’s Competitiveness (Survey on XYZ College Lecturers in Central Jakarta City),” *ADI J. Recent Innov.*, vol. 2, no. 1 Sept, pp. 243–249, 2020.

[5] D. Apriani, T. Ramadhan, and E. Astriyani, “Kerja Lapangan Berbasis Website Untuk Sistem Informasi Manajemen Praktek (Studi Sistem Informasi Program Studi Kasus Merdeka Belajar Kampus Merdeka (MBKM) Universitas Raharja,” *ADI Bisnis Digit. Interdisiplin J.*, vol. 3, no. 1, pp. 24–29, 2022.

[6] T. Ramadhan and R. D. Destiani, "Pengetahuan Manajemen Keuangan Bisnis Terhadap Niat Mahasiswa Bisnis Digital dalam Berwirausaha," *ADI Bisnis Digit. Interdisiplin J.*, vol. 3, no. 1, pp. 59–62, 2022.
[7] T. C. Husnadi, T. Marianti, and T. Ramadhan, "Determination of shareholders' welfare with financing quality as a moderating variable," *APTISI Trans. Manag.*, vol. 6, no. 2, pp. 191–208, 2022.
[8] P. Hendriyati, F. Agustin, U. Rahardja, and T. Ramadhan, "Management Information Systems on Integrated Student and Lecturer Data," *APTISI Trans. Manag.*, vol. 6, no. 1, pp. 1–9, 2022.
[9] A. G. Prawiyogi, A. S. Anwar, M. Yusup, N. Lutfiani, and T. Ramadhan, "Pengembangan Program Studi Bisnis digital bagi pengusaha dengan perangkat lunak lean," *ADI Bisnis Digit. Interdisiplin J.*, vol. 2, no. 2, pp. 52–59, 2021.
[10] N. N. Halisa, "Peran Manajemen Sumber Daya Manusia" Sistem Rekrutmen, Seleksi, Kompetensi dan Pelatihan" Terhadap Keunggulan Kompetitif: Literature Review," *ADI Bisnis Digit. Interdisiplin J.*, vol. 1, no. 2, pp. 14–22, 2020.
[11] M. F. Wahyutama and N. Natasyah, "Perancangan Sistem Informasi Platform Pencarian Kerja Pada PT. Wira Karya Indonesia," *ADI Bisnis Digit. Interdisiplin J.*, vol. 1, no. 2, pp. 46–59, 2020.
[12] B. S. Riza, "Blockchain Dalam Pendidikan: Lapisan Logis di Bawahnya," *ADI Bisnis Digit. Interdisiplin J.*, vol. 1, no. 1, pp. 41–47, 2020.
[13] E. Retnaningtyas, E. Kartikawati, and D. Nilawati, "erma 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] R. Hardjosubroto, U. Raharja, N. Anggraini, and W. Yestina, "PENGGALANGAN DANA DIGITAL UNTUK YAYASAN DISABILITAS MELALUI PRODUK UMKM DI ERA 4.0," *ADI Pengabdi. Kpd. Masy.*, vol. 1, no. 1, 2020.
[15] A. Moeins, S. Sudaryono, and A. Khoirunisa, "Utilization of Management of Writing Scientific in the Learning Process in Higher Education," *Aptisi Trans. Manag.*, vol. 2, no. 1, pp. 1–8, 2018.
[16] K. Arora, A. S. Bist, R. Prakash, and S. Chaurasia, "Custom OCR for Identity Documents: OCRXNet," *Aptisi Trans. Technopreneursh.*, vol. 2, no. 2, pp. 112–119, 2020.
[17] S. Saryani, H. Harfizar, and J. F. Maulana, "Design Of Inventory Data Information Systems In PT. Matahari Putra Prima. Tbk," *Aptisi Trans. Manag.*, vol. 3, no. 2, pp. 99–108, 2019.
[18] E. S. Aisyah, E. P. Harahap, and N. Salsabila, "The Effect Requirements Selling In The Marketplace For Security Against Buyer Trust," *Aptisi Trans. Manag.*, vol. 4, no. 1, pp. 67–75, 2019.
[19] Q. Aini, S. Riza Bob, N. P. L. Santoso, A. Faturahman, and U. Rahardja, "Digitalization of Smart Student Assessment Quality in Era 4.0," *Int. J. Adv. Trends Comput. Sci. Eng.*, vol. 9, no. 1.2, pp. 257–265, Apr. 2020, doi: 10.30534/ijatcse/2020/3891.22020.
[20] P. A. Sunarya, F. Andriyani, Henderi, and U. Rahardja, "Algorithm automatic full time equivalent, case study of health service," *Int. J. Adv. Trends Comput. Sci. Eng.*, vol. 8, no. 1.5 Special Issue, pp. 387–391, 2019, doi: 10.30534/ijatcse/2019/6281.52019.
[21] U. Rahardja, Q. Aini, F. P. Oganda, and V. T. Devana, "Secure Framework Based on Blockchain for E-Learning During COVID-19," in *2021 9th International Conference on Cyber and IT Service Management (CITSM)*, 2021, pp. 1–7.
[22] Q. Aini, R. Simbolon, and S. R. Dewi, "Effects of Credit Memos on Performance Accountant on Uncollectible Receivables," *Aptisi Trans. Manag.*, vol. 3, no. 2, pp. 149–158, 2019.
[23] N. Lutfiani, F. P. Oganda, C. Lukita, Q. Aini, and U. Rahardja, "Desain dan Metodologi Teknologi Blockchain Untuk Monitoring Manajemen Rantai Pasokan Makanan yang Terdesentralisasi," *InfoTekJar J. Nas. Inform. dan Teknol. Jar.*, vol. 5, no. 1, pp. 18–25, 2020.
[24] R. Widayanti, U. Rahardja, F. P. Oganda, M. Hardini, and V. T. Devana, "Students Formative Assessment Framework (Faus) Using the Blockchain," in *2021 3rd International Conference on Cybernetics and Intelligent System (ICORIS)*, 2021, pp. 1–6.
[25] T. Ramadhan, Q. Aini, S. Santoso, A. Badrianto, and R. Supriati, "Analysis of the potential

context of Blockchain on the usability of Gamification with Game-Based Learning," *Int. J. Cyber IT Serv. Manag.*, vol. 1, no. 1, pp. 84–100, 2021.