Blockchain Frontier Technology (B-Front)
Vol. 3 No. 1 July 2023

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

Position Paper on Applications of Smart Contracts and Blockchain Technology

Penny Wells[1], Georgia Probert[2], Daniel Marke[3], Claudia Konopka[4]
Information Technology, Nanyang Technological University[1,2]
Computer Science and Information Technology, Nanyang Technological University[3,4]
Singapore
e-mail: penny.wells@yahoo.com, georgiapro123@gmail.com, daniel12marke@gmail.com, claudia_konopka@yahoo.com

Author Notification
24 June 2023
Final Revised
26 June 2023
Published
01 July 2023

Wells, P., Probert, G., Marke, D., & Konopka, C. (2022). Position Paper on Applications Of Smart Contracts and Blockchain Technology. Blockchain Frontier Technology, 3(1).
DOI: https://doi.org/10.34306/bfront.v3i1.362

Abstract

Decentralized transaction management is made possible by blockchain technology. In this position paper, we'll cover some recent applications of blockchain technology in the cryptocurrency, financial services, risk management, and Internet of Things sectors, as well as its history and one of its main elements, the smart contract.

Keywords: *Applications, Blockchain, Smart Contracts*

1. Introduction

Digital currencies known as cryptocurrencies use cryptographic methods to safeguard its transactions and manage the creation of new currency units. Research on cryptocurrencies began in the 1980s. The first electronic cash system was proposed by Chaum [1]. The usage of cryptocurrencies in the real world has had little success despite extensive investigation. The situation has changed substantially as a result of Bitcoin [2]. It is now the cryptocurrency that is utilized the most. The fact that early cryptocurrencies were not decentralized was their main drawback [3]. Bitcoin addresses this problem by utilizing blockchain, a distributed ledger technology. Each and every Bitcoin transaction is specifically recorded on the blockchain, which is supported by a distributed consensus mechanism that can only be hacked if the attacker has complete control over all of the world's computing resources [4]. Double spending can be detected at the time of expenditure by utilizing the blockchain. Bitcoin is distinct from some of the other cryptocurrencies now in use since it does not support offline transactions. Peers can conduct transactions directly within the network, however, without the need for a centralized party like a bank, as the Bitcoin network is entirely decentralized. According to CoinMarketCap1, there are over 1700 cryptocurrencies with a total market value of over 267 billion US dollars. The blockchain industry is expected to grow from 411 million USD in 2017 to 7683 million USD over the next five years, according to recent Markets research [5].

Both the industry and academia have given blockchain a lot of attention. In summary, blockchain provides a promising foundation for applications that were previously only known to work with (offline) infrastructure. a reliable third party [6]. Blockchain technologies find uses outside of electronic currencies, financial applications like trading, and other FinTech applications since they are a decentralized, append-only distributed ledger. It enables the recording, management, and tracking of goods or replacement components, or more generally, complex procedures in the logistics process, when integrated with other approaches. The second-largest cryptocurrency, Ethereum2, introduces the blockchain platform's compatibility. This broadens the scope of blockchain-based applications [7].

1.1 Different Blockchain Layers

Multiple layers can be found in blockchain applications, including consensus, ledger and data structure, as well as application [8]. The consensus layer makes certain that various nodes in the network have the same understanding of the live blockchain and who is allowed to add a new block to the present blockchain is controlled by this. While the application layer determines the format and meaning of the recorded data, the data structure layer describes how data are recorded and organized. In the sections below, we go through how crucial a part cryptography plays in each of these layers of the Bitcoin blockchain [9].

Consensus. The Nakamoto consensus, which refers to Nakamoto's initial Bitcoin proposal, is the name given to the consensus mechanism that underpins Bitcoin. The longest chain rule states that nodes must use the longest chain to determine their local view of the blockchain. This layer also specifies the guidelines for determining who has the right to create the subsequent block that will be added to the existing blockchain. This is upheld in Bitcoin through proof-of-work [10].

Data Architecture. Blocks are collections of data items that make up the Bitcoin blockchain. A cryptographic hash function is used to connect each block to the one before it. Each block specifically contains the previous block's hash. The word "blockchain" comes from the fact that this structure forms a chain [11].

Applied Layer. Supporting Bitcoin transactions was the blockchain's original goal. Records in each block's original data type follow a straightforward structure. The first transaction that is recorded on each blockchain does not need an output, therefore each record is just a Bitcoin transaction with an input and an output [12]. This unique transaction, sometimes referred to as the coinbase transaction, acts as a method to incentivize nodes to produce new blocks as well as to facilitate the generation of additional Bitcoin units [13].

1.2 Privacy Aspects of Blockchain-Enabled Cryptocurrencies

Since their inception, cryptocurrencies have been designed with the dual objectives of achieving security and anonymity. Despite being highly anonymous in the eyes of the general public, Bitcoin's privacy guarantee remains subpar [14]. To conventional encrypted electronic money. In particular, Bit-coin transactions can be linked. One analysis example is the correlation between Bitcoin. In the Bitcoin blockchain, including IP address [15].

Several new coins have been proposed to overcome the privacy issue. Monero is a decentralized cryptocurrency that was created in 2014. It uses linkable ring signatures to conceal the transaction's sender [16]. A ring signature technique is a type of digital signature that can convince a verifier that the signature was generated by one of several plausible signers without revealing who it is [17]. As more individuals consider using blockchain for uses other than cryptocurrency, the privacy problem is gaining traction. To deal with these novel use cases in an effective manner, improved cryptographic approaches are required.

2. Smart Contract

In 1994, Szabo proposed the idea of smart contracts. With Bitcoin's enormous success, Blockchain 2.0 now includes smart contract functionality for a variety of non-crypto applications. More particular, Ethereum, the second-largest blockchain, supports Turing-complete smart contracts [18]. There are currently more than 4 million smart contracts on Ethereum. Other blockchain platforms that support smart contracts besides Ethereum include Counterparty, Stellar, Lisk, Monax, and others [19]. The logic of the specified programme can be automatically applied to an autonomous programme, which is what is meant by a smart contract. Developers often utilize high-level programming languages to design and deploy smart contracts. such as Solidity, Serpent, LLL, etc. The smart contract will then be developed and implemented in the Ethereum virtual machine [20]. Blockchain. As soon as a user or another smart contract triggers the smart contract, it will execute in the EVM

on each Ethereum node. A specification paper for the register-based virtual machine EVM may be found in the Ethereum yellow paper. Because EVM is sandboxed for security purposes, the smart contract running in it cannot access any of each Ethereum node's essential resources, such as its network and file system [21]. Unlike conventional virtual machines. Ethereum introduces the gas mechanism in such a way that the cost of doing each EVM operation is determined by multiplying the gas price by the operation's gas cost. This infers that a smart contract's execution will eventually come to an end [22]. A symbolic execution technique that found four different types of security flaws:

Due to the fact that the current execution of an Ethereum smart contract waits till the other one has finished, this vulnerability is known as reentrancy [23]. If the caller is malicious, the callee may use the caller's interim state as a springboard for assaults. This weakness allowed for the theft of 60 million dollars' worth of ether [24]. When one smart contract makes a call to another one, the improperly handled exceptions may occur. The execution logic of the caller will be impacted, in particular, if the exception in the callee is not propagated to the caller or the caller does not handle the return value from the callee. The potential assaults brought on by the unexpected order of transactions are referred to as the transaction-ordering reliance. Keep in mind that the order of the transactions can be chosen by the miner who creates the block [25].

The term "timestamp dependence" describes a potential weakness in intelligent programmes that require the block timestamp to regulate the execution of some crucial processes. The block timestamp could be altered by an evil miner to have an impact. the carrying out of such crucial procedures. Recently, Kalra et al. proposed a tool called Zeus that leverages limited horn clauses, symbolic model testing, and abstract interpretation to find security flaws in smart contracts rapidly. In addition to the aforementioned four security flaws, they also looked at ways to find other vulnerabilities such unchecked send, unsuccessful send, integer overflow/underflow, etc. To increase the accuracy of vulnerability detection and reduce false positive rates, more research is required.

Along with security concerns, Ethereum suffers from a number of performance problems. In terms of throughput, latency, scalability, and fault-tolerance, Dinh et al. provided the first evaluation framework to gauge the performance of private blockchains. A lightweight performance monitoring framework for blockchain systems was created by Zheng et al., and it can display detailed and real-time performance statistics. Because it costs money to execute smart contracts, Chen et al. Discovered that gas-inefficient patterns are common in already-existing smart contracts. To put it another way, a smart contract with inefficient gas patterns is expensive and extra petrol is needed. They also created GasReducer, a programme that automatically removes smart contract patterns that waste gas. Further to automatically detect and eliminate more gas-inefficient patterns, study is required.

3. Applications of Blockchain Besides Cryptocurrencies

Bitcoin was the first blockchain to be used. It has numerous use cases in the areas of finance, the Internet, and more as adoptions raise risks, the Internet of Things, etc. The applications or the inspiration behind some of these are highlighted below.

3.1 Financial Sector

Blockchain technology is expected to enhance the global financial system and provide a successful economic foundation. To promote economic growth and speed the development of green technologies, many institutions are investing heavily in blockchain technology. In other words, when using blockchains, consumers value the effort done to conserve energy. In addition, the de facto central bank of Hong Kong intended to set up an innovation hub to evaluate blockchain distributed ledger concepts. The Hong Kong Monetary Authority (HKMA) and the Hong Kong Applied Science and Technology Research Institute (ASTRI) are working together to enhance this hub's capabilities as a blockchain testbed. They believe that this

innovation hub can act as a "neutral ground" where financial technology can be tested before it is eventually deployed.

3.2 Internet of Things (IoT)

What is meant by a smart contract is an independent programme that can automatically apply the logic of the given programme. To create and implement smart contracts, developers frequently use high-level programming languages. for instance, LLL, Serpent, Solidity, etc. After that, the smart contract will be created and put into use in the Ethereum virtual machine. Blockchain. Each Ethereum node's EVM will execute the smart contract as soon as a user or another smart contract activates it. The Ethereum Yellow Paper contains the specification document for the register-based virtual machine (EVM). The smart contract operating in the EVM is sandboxed for security reasons, so it is unable to access any of each Ethereum node's crucial resources, including its network and file system.

The IoT network. Novo introduced an IoT architecture based on blockchain technology for arbitrating roles and permissions as a completely distributed access control system for IoT. Their method can be applied in a single smart contract, speeding the operation of the entire blockchain network and reducing communication costs between nodes. IoT could entail a lot of monetary factors. Through the Bitcoin protocol, Zhang and Wen presented an E-business architecture created exclusively for the Internet of Things.

3.3 Management of Risk

A central authority or a reliable third party are not required for verification thanks to blockchain technology. It may be beneficial to improve the current risk management, which includes intrusion detection and trust computation.mThanks to blockchain technology, verification does not require a centralized authority or a trustworthy third party. The present risk management, which includes intrusion detection and trust computation, might benefit from improvement. A multi-feature detection system using blockchain technology to compile a fact-base of reported Android malicious programmes is a method for identifying and categorizing malware. Specifically, they proposed an architecture for malware detection and evidence extraction termed "consortium blockchain," which is made up of two mixed-chain parts: a consortium chain for testing by test members, and a public chain for users.

Evaluating the reliability of nodes in a distributed IDS network environment is a crucial and vital task. Traditionally, trust computation required a third party with certification or a central server, both of which are vulnerable to several assaults, particularly insider attacks where the intruders have permission to access the network. With the development of blockchains, it is now possible to conduct a trust assessment without the assistance of a reliable third party. According to Alexopoulos Et Al et al. 's description of a blockchain-based CIDS system, each IDS node's raw alerts are treated as a transaction on a blockchain.

4. Conclusion

There are more and more blockchain uses in a variety of industries. This position paper provides a brief overview of blockchain technology and smart contracts, as well as some of their most recent uses in the fields of risk management, IoT, and finance. To further understand how to create a reliable, effective, and privacy-preserving blockchain-based security mechanism, more study is still required.

References

[1] 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.

[2] F. P. Oganda, N. Lutfiani, Q. Aini, U. Rahardja, and A. Faturahman, "Blockchain education smart courses of massive online open course using business model canvas," in *2020 2nd International Conference on Cybernetics and Intelligent System (ICORIS)*, 2020, pp. 1–6.
[3] F. P. Oganda, "PEMANFAATAN SISTEM IJC (iLearning Journal Center) SEBAGAI MEDIA E-JOURNAL PADA PERGURUAN TINGGI DAN ASOSIASI," *CSRID (Computer Sci. Res. Its Dev. Journal)*, vol. 11, no. 1, pp. 23–33, 2020.
[4] 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.
[5] N. Putri and L. Meria, "The Effect of Transformational Leadership on Employee Performance Through Job Satisfaction and Organizational Commitment," *IAIC Trans. Sustain. Digit. Innov.*, vol. 4, no. 1, pp. 8–21, 2022.
[6] E. Astriyani, D. Paramitha, Y. Destiany, A. Baihaqi, and R. Setiawan, "Perancangan Sistem Informasi Pengelolaan Biaya Perawatan Truck Hebel Pada PT Maju Sukses Mandiri Blok," *ADI Bisnis Digit. Interdisiplin J.*, vol. 1, no. 2, pp. 90–104, 2020.
[7] 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.
[8] A. Argani and W. Taraka, "Pemanfaatan Teknologi Blockchain Untuk Mengoptimalkan Keamanan Sertifikat Pada Perguruan Tinggi," *ADI Bisnis Digit. Interdisiplin J.*, vol. 1, no. 1, pp. 10–21, 2020.
[9] H. Haris and N. Priliasari, "THE DESIGN OF WEB-BASED TRAINING MANAGEMENT INFORMATION SYSTEMS AT PT. SINTECH BERKAH ABADI," *ADI J. Recent Innov.*, vol. 2, no. 2, pp. 269–274, 2020.
[10] M. Handayani, I. K. Mandiyasa, and I. Arini, "Marketing Mix Analisys Business Success Ceremonial Means Fiber-Based In Bresela Village, Gianyar," *ADI J. Recent Innov.*, vol. 1, no. 2, pp. 130–135, 2020.
[11] Sudaryono, U. Rahardja, and E. P. Harahap, "Implementation of Information Planning and Strategies Industrial Technology 4.0 to Improve Business Intelligence Performance on Official Site APTISI," *J. Phys. Conf. Ser.*, vol. 1179, no. 1, pp. 0–7, 2019, doi: 10.1088/1742-6596/1179/1/012111.
[12] B. P. K. Bintoro, N. Lutfiani, and D. Julianingsih, "Analysis of the Effect of Service Quality on Company Reputation on Purchase Decisions for Professional Recruitment Services," *APTISI Trans. Manag.*, vol. 7, no. 1, pp. 35–41, 2023.
[13] D. Zarasky and N. Septiani, "Analisis Faktor Kepuasan dan Minat Penggunaan E-Money Flazz BCA di Kota Tangerang," *J. MENTARI Manajemen, Pendidik. dan Teknol. Inf.*, vol. 1, no. 1, pp. 89–99, 2022.
[14] C. S. Bangun and N. A. Santoso, "Inovasi Pengembangan Kartu Ujian Online pada Web Portal dengan Metode Waterfall," *J. MENTARI Manajemen, Pendidik. dan Teknol. Inf.*, vol. 1, no. 1, pp. 1–8, 2022.
[15] 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.
[16] 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.
[17] P. Sokibi, "LTAI Management Based on Blockchain Technology to Increase Alexa Rank," *Int. J. Adv. Trends Comput. Sci. Eng.*, vol. 9, no. 4, pp. 4798–4802, 2020, doi: 10.30534/ijatcse/2020/88942020.
[18] L. A. Faza, P. M. Agustini, S. Maesaroh, A. C. Purnomo, and E. A. Nabila, "Motives For Purchase of Skin Care Product Users (Phenomenology Study on Women in DKI Jakarta)," *ADI J. Recent Innov.*, vol. 3, no. 2, pp. 139–152, 2022.

[19] Q. Aini, E. P. Harahap, and F. Faradilla, “The Effects of Sales Reports Business Intelligence on Employee Performance,” *Aptisi Trans. Manag.*, vol. 4, no. 1, pp. 83–91, 2019.
[20] M. Saraswati, N. Lutfiani, and T. Ramadhan, “Kolaborasi Integrasi Inkubator Bersama Perguruan Tinggi Sebagai Bentuk Pengabdian Terhadap Masyarakat Dalam Perkembangan Iptek,” *ADI Pengabdi. Kpd. Masy.*, vol. 1, no. 2, pp. 23–31, 2021.
[21] P. Abas Sunarya, Henderi, Sulistiawati, A. Khoirunisa, and P. Nursaputri, “Blockchain family deed certificate for privacy and data security,” *2020 5th Int. Conf. Informatics Comput. ICIC 2020*, no. November, 2020, doi: 10.1109/ICIC50835.2020.9288528.
[22] B. Mardisentosa, U. Rahardja, K. Zelina, F. P. Oganda, and M. Hardini, “Sustainable Learning Micro-Credential using Blockchain for Student Achievement Records,” in *2021 Sixth International Conference on Informatics and Computing (ICIC)*, 2021, pp. 1–6.
[23] F. P. Oganda, M. Hardini, and T. Ramadhan, “Pengaruh Penggunaan kontrak cerdas pada Cyberpreneurship Sebagai Media Pemasaran dalam Dunia Bisnis,” *ADI Bisnis Digit. Interdisiplin J.*, vol. 2, no. 1, pp. 55–64, 2021.
[24] N. Lutfiani, E. P. Harahap, Q. Aini, A. D. A. R. Ahmad, and U. Rahardja, “Inovasi Manajemen Proyek I-Learning Menggunakan Metode Agile Scrumban,” *InfoTekJar J. Nas. Inform. dan Teknol. Jar.*, vol. 5, no. 1, pp. 96–101, 2020.
[25] Sudaryono, U. Rahardja, Q. Aini, Y. Isma Graha, and N. Lutfiani, “Validity of Test Instruments,” *J. Phys. Conf. Ser.*, vol. 1364, no. 1, 2019, doi: 10.1088/1742-6596/1364/1/012050.