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

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

A Comparison of Blockchain Application and Security Issues from Bitcoin to Cyber Security

Novandio Fahmi [1], Diki Edwin Hastasakti[2], Diaz Zaspiagi[3], Septi Wijayanti[4]
Information Systems, University of Raharja[1,2,3]
Informatics Management, University of Raharja[4]
Indonesia
e-mail: novandio@raharja.info, diki.edwin@raharja.info, diaz@raharja.info, septi.wijayanti@raharja.info

Author Notification
10 Desember 2022
Final Revised
15 January 2023
Published
25 January 2023

Fahmi, N., Hastasakti, D. E., Zaspiagi, D., Saputra, R. K., & Wijayanti, S. (2022). A comparison of blockchain application and security issues from Bitcoin to Cybersecurity. Blockchain Frontier Technology, 2(2), 81–88.
DOI: https://doi.org/10.34306/bfront.v2i2.231

Abstract

Blockchain has quickly emerged as one of the trendiest Internet technologies in recent years due to the fast pace of technological advancement. With its integrated cryptography and consensus process, blockchain has redefined trust as a decentralized and distributed data management solution, ensuring security, privacy, and data integrity without the involvement of a third party. However, there are still certain technical difficulties and restrictions with blockchain. This essay has studied the present blockchain applications in cybersecurity in a methodical manner. The paper evaluates the benefits that blockchain has brought to cybersecurity and provides a summary of recent studies and blockchain applications in cybersecurity-related fields in order to address security challenges. The paper presents four key security challenges of blockchain through in-depth research and an overview of the existing work and then conducts a more detailed investigation of each issue. The research also proposes an improved access control scheme using an attribute-based encryption technique.

Keywords: *Tamper-Proofing, Cyber Security, Privacy-Protection, Blockchain, Bitcoin*

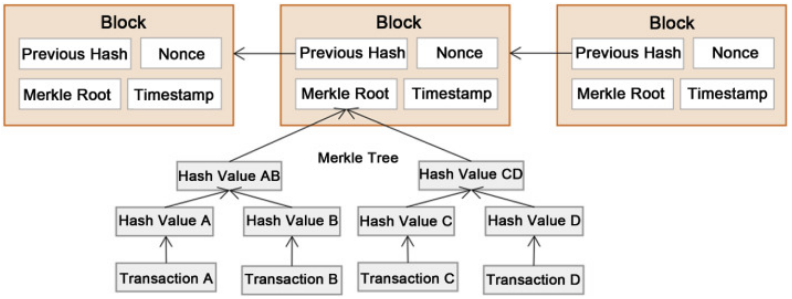
1. Introduction

At first, blockchain was proposed as the technical foundation of Bitcoin [1]. Although Bitcoin was formerly banned or limited to varying degrees in China, Russia, Europe, and several other nations due to excessive value fluctuation and supervisory management reasons. The general public is aware of the confidentiality, security, and dependability of blockchain technology [2]. Because it enables secure data and value transfer in a decentralized manner without the need for any third-party organizations, blockchain is regarded as a brand-new method of data storage, transmission, and management [3]. Blockchain began with cryptocurrencies, developed in the assets and credit space, and over time found usage in the information and communication sector as a technical solution that allows users to collaborate on data computation, storage, authenticity verification, and database maintenance [4]. Various industries are gradually realizing the technological superiority and practical utility of blockchain thanks to the technology's rapid development [5]. In the meantime, issues and security threats with blockchain applications, like the 51% attack, the constrained block size, and transaction latency, are becoming more and more obvious. This article does a thorough analysis of blockchain's technical principles, security mechanisms, typical uses, security threats, etc. in order to pinpoint the key security difficulties it faces [6]. The remainder of this essay is structured as follows. The benefits of blockchain technology for security are introduced in Section II. Section III elaborates on recent research

and blockchain applications in sectors relevant to cybersecurity. The blockchain's main security concerns and difficulties are examined in Section IV. The paper is concluded with Section 5 [7].

2. A Summary Of Blockchain Security Benefits

Blockchain is essentially a technical foundation. a system that enables users to jointly maintain a decentralized, trustworthy database [8]. The picture shows As seen in Figure 1, data is produced in a typical blockchain system. then arranged into blocks for storage. Blocks are connected in succession [9]. creating a linked data structure by arranging them chronologically. Each user Nodes take part in evaluating, storing, and maintaining data. Typically, a new block should get approval before being created. broadcast to all users, and more than half of the users, synchronization over the entire network using nodes. Once synchronized, neither modifying nor deleting is permitted optionally [10].



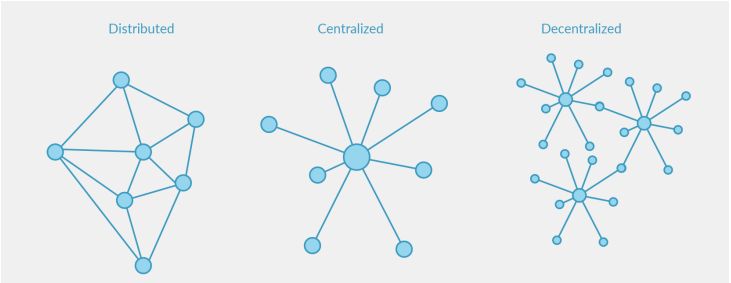
Source: Sciencedirect

Figure 1. Framework Blockchain Technical

Due to its incorporation of technological advances from P2P networks, distributed data storage, cryptography, and blockchain sacrifices the consensus mechanism and correct processing power, storage, and bandwidth for the increase in security [11]. The key benefits that blockchain has given to security are outlined below [12].

a. Disaster Recovery

By developing open-source sharing protocols, blockchain conducts data recording and saving synchronously at all users' ends [13]. As opposed to the conventional centralized database, which keeps data in one or more locations. Every user in a blockchain-based application has the ability to create data and retain a complete copy of that data [14]. Although some redundancy may result from this approach, the network's fault tolerance and dependability are increased. due to the fact that arbitrary attacks on one or more nodes won't completely destroy the network [14].

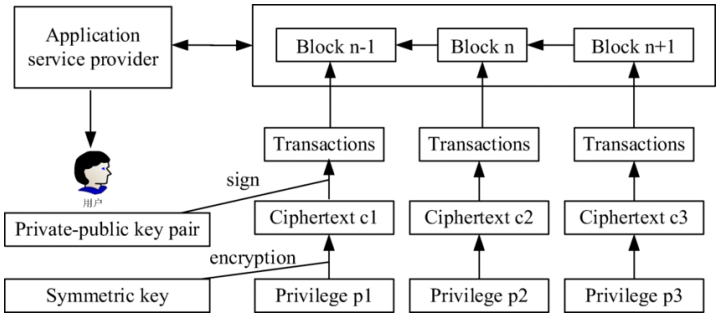


Source: Plesk

Figure 2. Decentralized and Distributed Storage of Blockchain.

b. Privacy Protection

The asymmetric encryption technology used by blockchain enables users to encrypt data using their private keys [15]. Additionally, the hash value of a user's public key is computed and used as the user's ID indicator. On the one hand, the hash value is unrelated to the user's true identity, protecting the user's personal information [16]. On the other side, the calculation of the hash value is invertible, making it difficult for an enemy to determine a user's public key from their public user address and for them to determine their private key from their public key. Blockchain succeeds in maintaining user privacy and anonymity [17].



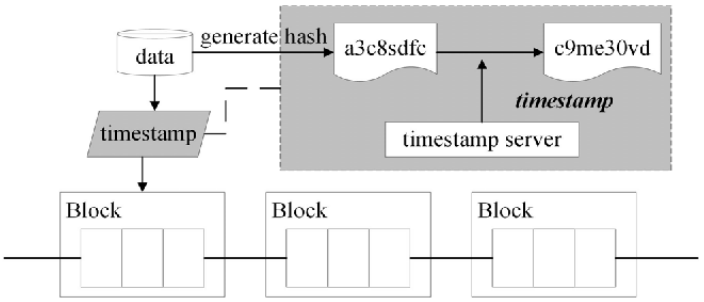
Source: Research Gate

Figure 3. Privacy Protection of Blockchain.

c. Tamper-Proofing

Because of its distinctive data format and data writing method, blockchain has the benefit of being tamper-proof [18]. A new timestamp will be recorded concurrently with the creation of a record, or "transaction," in the chained data structure of the blockchain, as shown in Figure 4. And after that timestamp, it will no longer be possible to modify data that has already been created. Additionally, a consensus method should decide if a new transaction can be recorded. In other words, it requires the consent of a certain number of users—usually set at more than 50%—to write data in blocks [19]. Because of the consensus mechanism, it is impossible for adversaries to tamper with data being recorded unless they control more than half of the network nodes or have more processing power [20].

recording process.

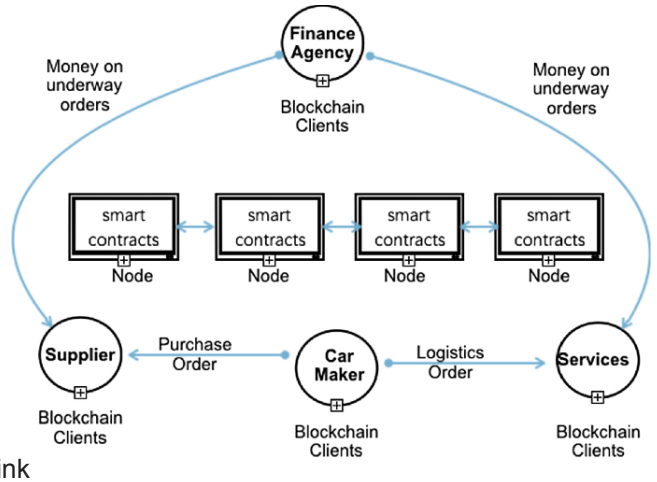


Source: Semantic Scholar

Figure 4. Tamper-Proofing Mechanism of Blockchain.

3. Current Blockchain Research and Application in Cybersecurity

As was previously noted, blockchain was first proposed as a base technology to build Bitcoin. Openness, transparency, and sharing are the guiding principles of blockchain technology [21]. Instead of employing a third-party middleman, blockchain uses mathematical and cryptographic techniques to ensure trust [22]. Blockchain is starting to replace other technologies as the technical foundation for cryptocurrencies, asset management, credit control, etc. by effectively guaranteeing the validity and originality of transactions. and gradually investigating its use in the domains of finance, medicine, energy, and ICT. Figure 5 compiles the common application scenario examples [23].



Source: Springer Link

Figure 5. Typical Application Scenarios of Blockchain

Blockchain can enable clearing and cross-border payment, for instance, in the financial industry by being introduced at the level of company operations, without altering the current oversight structure [23]. The deployment of blockchain also improved the effectiveness of company interactions and operational procedure optimization [24]. Blockchain technology is being used in the medical area by hospitals and security firms to store medical data and allow the transmission of electronic patient records between hospitals. Likewise, consider a solution to the issue of information sharing among several medical pillars [25]. Blockchain has been used in the smart grid to exchange decentralized power resources in the energy sector. In other words, the technical and security advantages gave the creation of blockchain a ton of room for innovation. Additionally, the blockchain's novel privacy and trust mechanisms have created the prospect of using it to effectively address some of the most pressing cybersecurity issues. The following are some examples of blockchain application scenarios in cybersecurity.

a. Keyless Signature Infrastructure

Key publication, update, and revocation issues arise in big data environments due to the explosion of data and equipment, which poses a challenge for authentication and signature techniques that rely on keys. The likelihood of breaking conventional asymmetric encryption techniques rises with the development of quantum computers. Security experts propose a Keyless Signature Infrastructure (KSI) to address the aforementioned security risks. The blockchain timestamp in KSI is fully utilized. In the KSI scenario, a block contains both the hash value and the current state of the data, system, or network. Then, KSI will continuously check these hash values against a timestamp to see if any files, operating systems, or applications have experienced unwanted access. Key management, distribution, or revocation

by KSI are not necessary thanks to the timestamp mechanism's adaptation as a monitor object. This makes it simple for KSI to increase protection of an EB data volume. Critical information infrastructures like nuclear power plants and flood-control systems in Indonesia have implemented security protection systems employing KSI.

b. Secure Data Storage

Large-scale user data leakage incidents have been common for a while. regularly because of the consolidated data storage, particularly in significant domains that are directly related to the national economy and people's means of subsistence, including financial, health, etc. In these circumstances, confidential information that leaks will bring up severe effects. looked into managing the hash value of medical data using blockchain, including identification, disease state, and treatment plan of patients. By creating distinct, individualized access rules requirements for security in specific business scenarios using Utilizing a multi-signature approach, users can only edit a clinical case using blockchain authorization network. In this approach, the healthcare sector becomes more transparent and the numerous privileges, including those of doctors, nurses, and patients, can be handled appropriately and successfully. Along with the aforementioned use cases, blockchain technology is also being investigated as an application mode in the fields of secure data transmission, IoT equipment verification, and cloud data desensitization.

c. Decentralized Distributed Secure Domain Name Service

Traditional domain name systems use a hierarchical resolution method, with the DNS server serving as the primary hub for all essential operations. The vulnerability of DNS servers to assaults like DDoS, DNS hijacking, and cache poisoning is therefore very high. Develop thorough research on blockchain-based DNS and build domain name infrastructures on the Bitcoin blockchain to overcome the aforementioned issues. Users can register, transmit, and update domain name data in any system node by creating a mapping between DNS and hash. A node is in charge of keeping the public and private keys of the domain name holder and keeping track of the resolved domain names. Domain owners can encrypt the operation process in the blockchain thanks to the integration of the blockchain and domain name service. Adversaries are unable to locate a central record to attack or manipulate as the previously centralized domain name service becomes decentralized. In a DNS system built on the blockchain, any system node can function as a DNS server, so attacks like DNS hijacking and cache poisoning that target one or more servers won't affect the entire system.

4. Security Issues of Blockchain

The study of blockchain technology is gaining momentum as awareness of it increases on a global scale. However, from the application layer's perspective, blockchain is still in the exploring phase. Till the technology is perfected and applications are fully developed, there is still a considerable integration and development process to be completed. Although blockchain technology has undergone revolutionary developments, there are still certain inherent security issues. Additionally, blockchain's revolutionary decentralization and self-organization have already resulted in minor security issues.

a. Open Source Blockchain Platforms Attract Intensive Attacks

The blockchain platform facilitates interoperability between various applications and consumers as the foundation technology of upper-layer applications. For instance, using a blockchain platform, industrial data in the medical, financial, and communication fields can be

created, saved, updated, and sent. Hackers are drawn to the open source blockchain platform's security flaws because of the enormous economic benefit.

b. Security Management of Self-organization and Anonymity

- Attack backtrack issues could be caused by anonymity mechanisms. Blockchain determines a user's public key's hash value to identify that specific user. In network attack backtracking and cybersecurity legislation, it is impossible to verify and trace a user's genuine identity due to this privacy-preserving operation.
- In blockchain use cases, distributed data storage may result in autonomous and frequent data cross-border transactions. Due to the distributed data storage model that blockchain uses and the maintenance of a complete copy of the data at each user's location. Once a new transaction is added to a block, all copies of the data should synchronously update. The difficulties of monitoring will increase when more people from different nations join the blockchain, taking initiative and frequently transferring data across borders.

c. Technical Limitations

- A cooperative attack might be started through a consensus process. Blockchain's consensus algorithm is predicated on the idea that the vast majority of nodes will be truthful in managing and maintaining the system. One or 978 more nodes can team up to start an attack to tamper with the content in blocks and carry out disruptive attacks like DDoS once they have more than 51% of the system's computational power.
- The limited block size severely limits the widespread use of blockchain technology. Initially, 1MB was chosen as the maximum size for a single block in order to fend off any DDoS assaults. Additionally, the debate over larger versus smaller block sizes has long existed. Because a larger block can hold more records, the criterion of development can be satisfied. However, larger blocks can make it more challenging to run and control blockchain nodes. However, despite the fact that smaller blocks are simpler to manage and more dependable for a third-party payment solution, there is a severe lack of available capacity, particularly in complicated big data environments.
- Blockchain's distributed storage architecture increases the attack surface. A blockchain system opts to retain an exact duplicate of every data on each user's computer. This implies that an attacker will have additional options to get those data. Although it is forbidden to alter content in a blockchain, attackers can nevertheless employ methods like data mining and correlation analysis to extract useful information about blockchain applications, users, network architecture, etc.

d. Potential Risk of Cryptography Application

- Widespread use of cryptographic algorithms could result in the introduction of unforeseen backdoors or weaknesses. Blockchain technology has widely adopted cryptography techniques like RSA and ECC. Security flaws and backdoors could appear in the algorithms themselves or in the methods used to implement them. then hurt the blockchain applications and the system as a whole. The likelihood of breaking asymmetric encryption schemes will also rise with the development of new computing capabilities like the quantum computer.
- The blockchain does not provide a solution to the private key management issue. Private keys are typically used by existing blockchain applications to verify a user's identity and execute a transaction. Therefore, the security of the private key is a need for the non-falsification of information. Users of blockchains are accountable for their

own private keys, in contrast to traditional public key cryptography, which relies on a third party to generate and manage private keys. It will be hard for a user to access his digital assets on blockchain if they lose their private key.

5. Conclusions

In recent years, blockchain has been the subject of enormous expectations. The use of blockchain has already branched out from finance into the realms of ICT and network security. Additionally, the topic of blockchain security is discussed. As a ground-breaking new technology in the age of the Internet, blockchain is quickly integrating with current technologies and creating new business models. In the meantime, maintaining network security regulation mode is growing more difficult. This essay investigates blockchain's use in cybersecurity in depth and examines the ongoing security concerns. More work will be put into addressing blockchain security issues in the future and investigating better solutions, such as standards for technology testing and blockchain security requirements, mechanisms for securing business flow, and clarification of security operations in blockchain, among other things.

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] 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.

[3] Y. Durachman, A. S. Bein, E. P. Harahap, T. Ramadhan, and F. P. Oganda, “Technological and Islamic environments: Selection from Literature Review Resources,” *Int. J. Cyber IT Serv. Manag.*, vol. 1, no. 1, pp. 37–47, 2021.

[4] 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.

[5] Q. Aini, W. Febriani, C. Lukita, S. Kosasi, and U. Rahardja, “New normal regulation with face recognition technology using attendx for student attendance algorithm,” in *2022 International Conference on Science and Technology (ICOSTECH)*, 2022, pp. 1–7.

[6] 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.

[7] K. D. Nusandari, R. Widayanti, Y. F. Achmad, A. H. Azizah, and N. A. Santoso, “Analisis Kesuksesan Pengguna Tangerang Live menggunakan Information System Success Model (ISSM),” *J. MENTARI Manajemen, Pendidik. dan Teknol. Inf.*, vol. 1, no. 1, pp. 77–88, 2022.

[8] U. Rahardja, M. A. Ngad, S. Millah, E. P. Harahap, and Q. Aini, “Blockchain Application in Educational Certificates and Verification Compliant with General Data Protection Regulations,” in *2022 10th International Conference on Cyber and IT Service Management (CITSM)*, 2022, pp. 1–7.

[9] 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.

[10] U. Rahardja, N. Lutfiani, A. S. Rafika, and E. P. Harahap, “Determinants of Lecturer Performance to Enhance Accreditation in Higher Education,” in *2020 8th International Conference on Cyber and IT Service Management (CITSM)*, 2020, pp. 1–7.

[11] 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.

[12] U. Rahardja, C. Lukita, F. Andriyani, and Masaeni, "Optimization of marketing workforce scheduling using metaheuristic genetic algorithms," *Int. J. Adv. Trends Comput. Sci. Eng.*, vol. 9, no. 1.2 Special Issue, pp. 243–249, 2020, doi: 10.30534/IJATCSE/2020/3691.22020.

[13] Q. Aini, U. Rahardja, I. Handayani, M. Hardini, and A. Ali, "Utilization of google spreadsheets as activity information media at the official site alphabet incubator," *Proc. Int. Conf. Ind. Eng. Oper. Manag.*, no. 7, pp. 1330–1341, 2019.

[14] U. Rahardja, Q. Aini, and E. P. Harahap, "Manajemen Sistem Gamifikasi Sebagai Inovasi Pembelajaran," in *Seminar Nasional APTIKOM (SEMNASTIKOM)*, 2016, vol. 3, no. 1, pp. 190–197.

[15] A. S. Bist, B. Rawat, Q. Aini, N. Lutfiani, and M. Hardini, "COVID-19 Wave Pattern Analysis: An Exhaustive Survey," in *2021 9th International Conference on Cyber and IT Service Management (CITSM)*, 2021, pp. 1–4.

[16] F. Fukuyama, B. Richman, and A. Goel, "How to save democracy from technology: ending big tech's information monopoly," *Foreign Aff.*, vol. 100, p. 98, 2021.

[17] R. Yunita, M. S. Shihab, D. Jonas, H. Haryani, and Y. A. Terah, "Analysis of The Effect of Servicescape and Service Quality on Customer Satisfaction at Post Shop Coffee Tofee in Bogor City," *Aptisi Trans. Technopreneursh.*, vol. 4, no. 1, pp. 66–74, 2022.

[18] 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.

[19] N. Sari, W. A. Gunawan, P. K. Sari, I. Zikri, and A. Syahputra, "Analisis Algoritma Bubble Sort Secara Ascending Dan Descending Serta Implementasinya Dengan Menggunakan Bahasa Pemrograman Java," *ADI Bisnis Digit. Interdisiplin J.*, vol. 3, no. 1, pp. 16–23, 2022.

[20] B. S. Riza, "Blockchain Dalam Pendidikan: Lapisan Logis di Bawahnya," *ADI Bisnis Digit. Interdisiplin J.*, vol. 1, no. 1, pp. 41–47, Jun. 2020, doi: 10.34306/abdi.v1i1.112.

[21] S. Purnama, Q. Aini, U. Rahardja, N. P. L. Santoso, and S. Millah, "Design of Educational Learning Management Cloud Process with Blockchain 4.0 based E-Portfolio," *J. Educ. Technol.*, vol. 5, no. 4, pp. 628–635, 2021.

[22] T. Wahyuningsih, F. P. Oganda, and M. Anggraeni, "Design and Implementation of Digital Education Resources Blockchain-Based Authentication System," *Blockchain Front. Technol.*, vol. 1, no. 01, pp. 74–86, 2021.

[23] 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.

[24] U. Rahardja, Q. Aini, and S. R. Zuliana, "Metode Learning Management System (LMS) iDu Untuk Mendukung Kegiatan Belajar Mengajar MIT Pada Perguruan Tinggi Raharja," *Cyberpreneursh. Innov. Creat. Exact Soc. Sci.*, vol. 2, no. 2, pp. 156–172, 2016.

[25] S. Azizah *et al.*, "Quantum Computing and AI: Impacts & Possibilities," *ADI J. Recent Innov.*, vol. 3, no. 2, pp. 121–138, 2022.