Jurnal Ilmiah Teknik Elektro Komputer dan Informatika (JITEKI)
Vol. 8, No. 2, June 2022, pp. 199-205
ISSN: 2338-3070, DOI: 10.26555/jiteki.v8i2.24327

Blockchain Technology

Purwono Purwono [1], Alfian Ma'arif [2], Wahyu Rahmaniar [3], Qazi Mazhar ul Haq [3], Dimas Herjuno [4], Muchammad Naseer [5]
[1] Universitas Harapan Bangsa, Jl. Raden Patah No. 100 Kedunglongsir Ledug Kembaran, Banyumas 53182, Indonesia
[2] Universitas Ahmad Dahlan, Yogyakarta, Indonesia
[3] National Taipei University of Technology, Taipei 10608, Taiwan
[4] Kyushu Institute of Technology, Japan
[5] Sekolah Tinggi Teknologi Bandung, Bandung 40235, Indonesia

ARTICLE INFO

Article history:

Received May 30, 2022
Revised July 16, 2022
Accepted July 21, 2022

Keywords:

Blockchain;
Smart Contract;
Security

ABSTRACT

Blockchain came because of the occurrence of incredulity to single authorities by introducing the concept of network decentralization and data distribution saved in a ledger. Decentralization is used to validate discrepancies in the majority of data. The consensus mechanism collectively maintains the consistency of the ledger. A blockchain is a set of blocks containing transaction data interconnected to each other using the concept of cryptography. A mining process is an effort to add new blocks to the blockchain. The mining computer carries out the process after passing several complex mathematical problems. The fastest miner is rewarded with crypto coins. Some consensus mechanisms commonly used in blockchain are proof of work, proof of stake, practical byzantine fault tolerance, and proof of elapsed time. Blockchain network is designed and implemented in such a way that it can guarantee the security of its data, is easy to be audited, is robust to denial of service and majority attacks, and is private and confidential. The application of blockchain is not limited to finance systems; it can also be applied in health, education, supply chain, and state democracy systems.

Corresponding Author:

Purwono, Universitas Harapan Bangsa, Address, City and Postcode, Indonesia
Email: purwono@uhb.ac.id

1. THE CONCEPT OF BLOCKCHAIN

Blockchain technology has become one of the popular technologies aside from the Internet of Things (IoT) [1]. The technology has been well-accepted by society and has begun to be adopted in various fields over the last few years [2][3]. Blockchain became the most preferred due to the technological innovation initiated by Satoshi Nakamoto [4] in his white papers: bitcoin, decentralized cryptocurrency [5]. Aside from bitcoins, another popular blockchain product is Ethereum [6], which is characterized by its concept of smart contracts [7].

The origin of blockchain is the occurrence of incredulity in single authorities [8]. There is a potential risk of unilateral data manipulation by a single authority. For instance, when data is stored in a rented server, the data can be altered unilaterally by the server's owner. Single authorities, which is the server's owner, have full control of the stored data. A similar example is in banking services; there is distrust by a group of people who save their money on banks using a centralized finance system.

A solution for the incredulity issue to single authorities is to synthesize a decentralization. Contrary to centralization, a decentralized system has no exclusive right to decide any system status by itself. Any decision-making in the system must pass the consensus collectively, and each system's data should be able to be mutually validated by each other [9]. Decentralization has entirely changed today's concept of centralization [3]. It became the primary concept of Blockchain technology where there is no centralized directory server and no reference of file placement, which determines data location [10]. Blockchain eliminates the need for central

authority, so verification from the third party is unnecessary [11]. Moreover, blockchain uses a peer-to-peer network; all members use private/public keys to interact with the network [12]. Private keys are used to sign transactions, while public keys are used for network addresses [12].

Blockchain stores transaction data, in the form of ledgers, in blocks of data that will be distributed to all network members [13] that are unalterable [14]. In the blockchain, the concept of decentralization is employed to validate any discrepancy in majority data. The validation process is held with a consensus mechanism that collectively maintains the ledger's consistency [15]. The consensus mechanism is accountable for the security and integrity of the whole data network in a blockchain system, where all network members are interconnected to reach a particular agreement [16].

2. TECHNICALITY OF BLOCKCHAIN

2.1. Block Interconnection

Technically, a blockchain is a set of blocks containing transaction data interconnected with each other using the concept of cryptography to ensure the integrity of information within its blocks [17][18]. A cryptographic hash function is an algorithm that maps arbitrary-sized data to a fixed-size string [19]. The first block in a blockchain is called the genesis block. It is a special block called the 0-th block, the first block ever mined by its creator. Genesis block became a basis for additional blocks of transactions [20].

Information regarding the transaction is stored in different blocks, which later will be batched and form a verified data chain [21]. The content in each block is hashed and then will be saved in the subsequent block. Any altered block will cancel the current block's hash using this way [21]. When a new transaction is added to the subsequent block, there will always be a validation regarding the previously-saved hash blocks.

In a particular timestamp, there is a possibility that more than one transaction occurs, which is up to 10.457 transactions per second [22]. Storing data in hash aims to maintain the integrity of data transactions that occurred in previous blocks [23]. If there is an attempt to modify a block, then the hash in the block will be invalid, damaging the other hash blocks in the blockchain. When a hacker tries to alter only one data transaction in a block, the hacker must modify all blocks in the blockchain. Moreover, synchronization needs to be done to all other computers in the distributed network.

2.2. Mining

Mining is an effort to add new blocks to the blockchain. In well-known blockchain products, such as Bitcoin or Ethereum, several computers are known as nodes. Some computers in blockchain can add additional blocks, known as mining computers or mining nodes (miners). Mining nodes (also known as miners) in Bitcoin always receive new problems every 10 minutes, and the fastest node to solve the problem will be rewarded with the cryptocurrency [24].

When a transaction occurs, the transaction is broadcasted to all networks in the blockchain [25]. The consensus mechanism is necessary for the integrity of stored information and defense against various attacks [26][27]. All mining computers (miners) can receive the information at different times. As the node can receive the transaction, the node will add the information into a block. Every node is free to input any desired transaction into a block.

A protocol is needed to slow down the rate of adding newer blocks to the blockchain; consensus is a mutual agreement to determine targetted network difficulty [28][29]. Every mining node must hash its block's content and fulfill requirements made by the targetted network difficulty before adding new blocks to a blockchain.

For instance, each hash needs to be started with 0 in its first five bits. Therefore, the mining node must repeatedly make a hashing code of the block's content, ensuring that there are five 0 in its first five bits. The difficulty level will increase when there are many miners joining the network. For example, the difficulty level mentioned earlier is for a network with 50 miners; when there are 400 miners in the same network, the hash code must have ten 0 in the first ten bits.

There may be issues when the network difficulty is consistent; after a miner finds a hash code that meets the difficulty criteria, the particular hash code may be used continuously for mining. Thus, a new rule must be made. Aside from only making a hash code for the next block, miners need to add a nonce (number only used once). Nonce will be added to the block's hash to preserve the network difficulty.

The nonce is obtained when the miner hash the block's content [30]. It can be obtained as the number of computations made by miners to make a hash code that meets the network difficulty. For example, a miner successfully creates a hash code, which meets the difficulty criteria of hash code with 0 in the first five bits, at the 1235-th iteration. The obtained nonce for the example is 1235. This number, 1235, will be added to the subsequent block's hash information along with the hash code. Therefore, the network difficulty can be maintained.

Adding block to a blockchain, a mining, can occur when a miner succeed to solve the network difficulty for the first time, which is finding the nonce to the next hash. The successful miner will be rewarded in a cryptocurrency from the blockchain network for solving the network difficulty. Information regarding the success of mining nodes in solving this network difficulty level will be broadcasted to all members of the blockchain network. Then, all these members will validate whether new blocks are actually added to the network. Other miners will stop mining immediately and look for other transactions that can be mined.

2.3. Consensus Mechanisms

The mining process in blockchain requires a consensus algorithm. Several popular consensus algorithms are as follows [31][32][33]:

- Proof of Work (PoW) is a consensus that demands counting nonce to qualify a particular mathematical problem of a hash block. PoW is the first consensus used in bitcoin to prevent spam attacks and distributed denial of service (DDoS) attacks [34].
- Proof of Stake (PoS) is a consensus with a basic stake of nodes in the network. Node with the highest bet can validate the new block in the chain. This approach is used to reduce the complexity of counting conditions in PoW consensus.
- Practical Byzantine Fault Tolerance (PBFT) is a consensus that is used in asynchronous (no upper bound on when the response to the request will be received) system where the network assumes some nodes are false. Using this assumption, a node requires consensus from the remaining nodes to create a new block in the chain.
- Proof of Elapsed Time (PoET) is a consensus that is run in private networks. The consensus requires the node to wait in a random time period before achieving consensus in a new block.

2.4. Blockchain Security

Blockchain network is designed and implemented to ensure data security, easy to be audited, robust to denial of service, robust to majority attacks, and maintain privacy and confidentiality [35]. Data consistency in the network refers to a concept where data is confirmed to be copied accurately and precisely for every network member in time dots [36][37]. Blockchain is robust to data corruption or tampering, which means it can withstanding any damage or tampering to data, system, or product, whether done intentionally or unintentionally [38]. This also means that all data stored in a blockchain cannot be altered or modified by anyone. Therefore, a blockchain network ensures the data integrity of its users. This is done by disguising the identity of its users in a hash [39]. Meanwhile, a decentralized peer-to-peer connection is a solution to maintain blockchain networks, ensuring that the transaction process is done fairly when several nodes fail to make new blocks. Koneksi peer to peer yang terdesentralisasi adalah solusi yang digunakan untuk memelihara blockchain, yang memastikan bahwa proses transaksi dilakukan secara merata ketika beberapa node dalam jaringan gagal. Hacking attempts on a blockchain are challenging since hackers must block more than half of the total nodes [40]. Blockchain also ensures the confidentiality of the transactions by using pseudo identities. The purpose of using pseudo identities is to ensure no dangerous attack on data stored in the blockchain can be performed and make the nodes hardly recognized by hackers [41].

3. BLOCKCHAIN AND SMART CONTRACT

3.1. History of Smart Contract

The history of smart contracts began in 1991 when S. Haber dan W. S. Strornetta proposed a system that is hard to be altered in storing digital documents [42]. The system is schemed to have a certificate that contains the date when the documents were made and information regarding previously published certificates of other digital documents [43]. Satoshi had an idea to make blocks containing sets of transactions, a nonce, timestamp, and hash of previous blocks [42], later used as a foundation for developing blockchain technology. In 1994, Nick Szabo introduced a smart contract, a computer program that replicates actions commonly explained in physical or traditional contracts [44]. Then, in 1996, Szabo defined the purpose of making smart contracts: observability, verifiability, privity, and enforceability. Szabo assessed that smart contracts are suitable for blockchain; smart contracts that have been made should not be altered, should be easily observed and verified, and can run autonomously [42]. In 2015, Vitalik Buterin created Ethereum, an open-source blockchain platform that supports decentralized payments, which rapidly increases smart contract developments [45].

3.2. Smart Contracts Developments

Smart contracts are continuously developed to fix issues in implementing them in bitcoin [46]. Ethereum was then presented as a platform that tries to develop the concept of smart contracts. The main idea of Ethereum is to run programs specified by users in a blockchain, creating special and expressive smart contracts with a

particular programming language [47]. Codes are written with Solidity, a programming language, and are run in an Ethereum Virtual Machine (EVM) [48]. Source codes are then compiled to be EVM bytecode to be run. With complex intelligence, Ethereum is considered the most popular blockchain platform for developing smart contracts, marking the start of the Blockchain 2.0 era [49]. Other platforms that can be used to develop smart contracts are Corda, Hyperledger Fabric, and BigChain DB [50]. The benefit of using smart contracts is a compatible protocol implementation with the consensus. Smart contracts work by encoding rules that have been specified and performing related operations when an agreement is met [47].

4. APPLYING BLOCKCHAIN

Blockchain technology can be applied to wide applications, such as health systems, and is not limited to cryptocurrency. For instance, research by Haleem [51] implemented the technology in the medical care system, in which patient information is shared carefully to identify severe and hazardous medical issues. One health product running with blockchain technology is the Medicalchain [52], an application of health technology that utilizes patient-centered blockchain. Patients were given special control to share their medical records. Another research held by Riadi [20] utilized blockchain to secure patients' medical private records, especially records of those who were diagnosed with Covid19 and the vaccine certificates.

Blockchain was also applied to the agricultural supply chain during the pandemic era [53]. Blockchain was proven to be a solution to track deliveries during the Covid19 pandemic era, and a solution to collect and monitor data, as well as product scams and other transactions. Products related to the supply chain were also developed by IBM, which was the IBM Food Trust [54]. Research by Firedman proved that blockchain contributed to a fair, sustainable, and traceable food supply chain [21][55].

Applying blockchain to education systems can be done by maintaining transactions of students' records from the beginning of education to graduating universities. Blockchain can ensure data availability so that those data are traceable to see each student's academic history. Applying blockchain also avoids data manipulation from the central administrator, potentially altering academic histories [56].

Blockchain can also be applied to voting during an election, which supports democracy to be held properly, and peace can be maintained in countries worldwide [57]. Transparency in blockchain can also reduce concerns regarding centralized e-voting, which is vulnerable to data alteration by irresponsible parties. Trust and confidentiality to tools and systems are keys to successful blockchain-based e-voting.

5. CONCLUSIONS

Blockchain is a popular technology nowadays. The technology emerges rapidly due to the incredulity of single authorities. Blockchain presents a solution by applying a decentralized network as its concept, where each member has the authority to validate data from each other. It is regarded as a peer-to-peer network that is supported by a consensus algorithm to maintain data security. Private keys are used to sign transactions, while public keys are used as network addresses. Blockchain stores all data in a distributed ledger, which means all network members have identical copies of the stored data. Consensus becomes a way to validate any discrepancy in majority data. The validation is done collectively to preserve the consistency of the ledger. Adding transaction data to the blockchain, commonly called mining, is done by passing some consensus chains in the blockchain network. Each block is interconnected with a chain in hash codes. Blocks of transactions are continuously hashed, and the hash codes are stored in the next block. Therefore, if there is a block containing different data from the data stored in most network members, the block will be easily traced and ignored by other members in the network. Several consensus algorithms that are popularly used are PoW, PoS, PBFT, and PoET. In the perspective of data security, blockchain is considered tough and robust since blockchain networks are built and implemented to have excellent data security, easy to be audited, robust to denial of service, robust to majority attacks, and private and confidential. The application of blockchain is not limited to banking services but can also be applied to many systems: healthcare, education, supply chain, and also democracy of a state or country.

REFERENCES

[1] R. L. Kumar, F. Khan, S. Kadry, and S. Rho, "A Survey on blockchain for industrial Internet of Things," *Alexandria Eng. J.*, vol. 61, no. 8, pp. 6001–6022, Aug. 2022, https://doi.org/10.1016/j.aej.2021.11.023.

[2] M. A. N. Agi and A. K. Jha, "Blockchain technology in the supply chain: An integrated theoretical perspective of organizational adoption," *Int. J. Prod. Econ.*, vol. 247, p. 108458, May 2022, https://doi.org/10.1016/j.ijpe.2022.108458.

[3] A. S. Rajasekaran, M. Azees, and F. Al-Turjman, "A comprehensive survey on blockchain technology," *Sustain. Energy Technol. Assessments*, vol. 52, p. 102039, Aug. 2022, https://doi.org/10.1016/j.seta.2022.102039.

[4] H. H. Khan, M. N. Malik, Z. Konečná, A. G. Chofreh, F. A. Goni, and J. J. Klemeš, "Blockchain technology for agricultural supply chains during the COVID-19 pandemic: Benefits and cleaner solutions," *J. Clean. Prod.*, p.

131268, Mar. 2022, https://doi.org/10.1016/j.jclepro.2022.131268.
[5] N. Six, N. Herbaut, and C. Salinesi, "Blockchain software patterns for the design of decentralized applications: A systematic literature review," *Blockchain Res. Appl.*, p. 100061, 2022, https://doi.org/10.1016/j.bcra.2022.100061.
[6] Q. T. Thai, N. Ko, S. H. Byun, and S. M. Kim, "Design and implementation of NDN-based Ethereum blockchain," *J. Netw. Comput. Appl.*, vol. 200, p. 103329, Apr. 2022, https://doi.org/10.1016/j.jnca.2021.103329.
[7] S. J. Aquilina, F. Casino, M. Vella, J. Ellul, and C. Patsakis, "EtherClue: Digital investigation of attacks on Ethereum smart contracts," *Blockchain Res. Appl.*, vol. 2, no. 4, p. 100028, 2021, https://doi.org/10.1016/j.bcra.2021.100028.
[8] W.-M. Lee, *Beginning Ethereum Smart Contracts Programming*. Berkeley: Apress, 2019, https://doi.org/10.1007/978-1-4842-5086-0.
[9] J. Lee, B. Lee, J. Jung, H. Shim, and H. Kim, "DQ: Two approaches to measure the degree of decentralization of blockchain," *ICT Express*, vol. 7, no. 3, pp. 278–282, Sep. 2021, https://doi.org/10.1016/j.icte.2021.08.008.
[10] E. M. Adere, "Blockchain in healthcare and IoT: A systematic literature review," *Array*, p. 100139, Mar. 2022, https://doi.org/10.1016/j.array.2022.100139.
[11] H. Ritchi, A. Bandana, Z. Adrianto, and A. Alfian, "Permissioned blockchain for business process visibility: A case of expenditure cycle," *Procedia Comput. Sci.*, vol. 197, no. 2021, pp. 336–343, 2021, https://doi.org/10.1016/j.procs.2021.12.148.
[12] M. Šarac, N. Pavlović, N. Bacanin, F. Al-Turjman, and S. Adamović, "Increasing privacy and security by integrating a Blockchain Secure Interface into an IoT Device Security Gateway Architecture," *Energy Reports*, vol. 7, pp. 8075–8082, 2021, https://doi.org/10.1016/j.egyr.2021.07.078.
[13] Y. Yang, T. Lin, P. Liu, P. Zeng, and S. Xiao, "UCBIS: An improved consortium blockchain information system based on UBCCSP," *Blockchain Res. Appl.*, p. 100064, Jan. 2022, https://doi.org/10.1016/j.bcra.2022.100064.
[14] N. Singh and M. Vardhan, "Computing Optimal Block Size for Blockchain based Applications with Contradictory Objectives," *Procedia Comput. Sci.*, vol. 171, no. 2019, pp. 1389–1398, 2020, https://doi.org/10.1016/j.procs.2020.04.149.
[15] Y. Liu, Y. Lan, B. Li, C. Miao, and Z. Tian, "Proof of Learning (PoLe): Empowering neural network training with consensus building on blockchains," *Comput. Networks*, vol. 201, p. 108594, Dec. 2021, https://doi.org/10.1016/j.comnet.2021.108594.
[16] H. Samy, A. Tammam, A. Fahmy, and B. Hasan, "Enhancing the performance of the blockchain consensus algorithm using multithreading technology," *Ain Shams Eng. J.*, vol. 12, no. 3, pp. 2709–2716, Sep. 2021, https://doi.org/10.1016/j.asej.2021.01.019.
[17] R. L. Kumar, F. Khan, S. Kadry, and S. Rho, "A Survey on blockchain for industrial Internet of Things: Blockchain for Internet of Things," *Alexandria Eng. J.*, vol. 61, no. 8, pp. 6001–6022, 2022, https://doi.org/10.1016/j.aej.2021.11.023.
[18] J. Wan, J. Li, M. Imran, D. Li, and Fazal-e-Amin, "A Blockchain-Based Solution for Enhancing Security and Privacy in Smart Factory," *IEEE Trans. Ind. Informatics*, vol. 15, no. 6, pp. 3652–3660, 2019, https://doi.org/10.1109/TII.2019.2894573.
[19] L. Wang, X. Shen, J. Li, J. Shao, and Y. Yang, "Cryptographic primitives in blockchains," *J. Netw. Comput. Appl.*, vol. 127, no. June 2018, pp. 43–58, 2019, https://doi.org/10.1016/j.jnca.2018.11.003.
[20] I. Riadi, T. Ahmad, R. Sarno, P. Purwono, and A. Ma'arif, "Developing Data Integrity in an Electronic Health Record System using Blockchain and InterPlanetary File System (Case Study: COVID-19 Data)," *Emerg. Sci. J.*, vol. 4, no. Special issue, pp. 190–206, 2020, https://doi.org/10.28991/esj-2021-SP1-013.
[21] N. Friedman and J. Ormiston, "Blockchain as a sustainability-oriented innovation?: Opportunities for and resistance to Blockchain technology as a driver of sustainability in global food supply chains," *Technol. Forecast. Soc. Change*, vol. 175, no. December 2021, p. 121403, 2022, https://doi.org/10.1016/j.techfore.2021.121403.
[22] S. S. Hazari and Q. H. Mahmoud, "Improving transaction speed and scalability of blockchain systems via parallel proof of work," *Futur. Internet*, vol. 12, no. 8, 2020, https://doi.org/10.3390/fi12080125.
[23] J. Fu, S. Qiao, Y. Huang, X. Si, B. Li, and C. Yuan, "A Study on the Optimization of Blockchain Hashing Algorithm Based on PRCA," *Secur. Commun. Networks*, vol. 2020, 2020, https://doi.org/10.1155/2020/8876317.
[24] S. L. Náñez Alonso, J. Jorge-vázquez, M. Á. Echarte Fernández, and R. F. Reier Forradellas, "Cryptocurrency mining from an economic and environmental perspective. Analysis of the most and least sustainable countries," *Energies*, vol. 14, no. 14, 2021, https://doi.org/10.3390/en14144254.
[25] C. N. Truong, M. Schimpe, U. Bürger, H. C. Hesse, and A. Jossen, "Multi-use of stationary battery storage systems with blockchain based markets," *Energy Procedia*, vol. 155, pp. 3–16, 2018, https://doi.org/10.1016/j.egypro.2018.11.070.
[26] A. Abdelmaboud, A. I. A. Ahmed, M. Abaker, T. A. E. Eisa, H. Albasheer, S. A. Ghorashi, and F. K. Karim, "Blockchain for IoT Applications: Taxonomy, Platforms, Recent Advances, Challenges and Future Research Directions," *Electronics*, vol. 11, no. 4, p. 630, 2022, https://doi.org/10.3390/electronics11040630.
[27] A. Reyna, C. Martín, J. Chen, E. Soler, and M. Díaz, "On blockchain and its integration with IoT. Challenges and opportunities," *Futur. Gener. Comput. Syst.*, vol. 88, no. 2018, pp. 173–190, 2018, https://doi.org/10.1016/j.future.2018.05.046.
[28] B. Shrimali and H. B. Patel, "Blockchain state-of-the-art: architecture, use cases, consensus, challenges and opportunities," *J. King Saud Univ. - Comput. Inf. Sci.*, 2021, https://doi.org/10.1016/j.jksuci.2021.08.005.
[29] C. Hsueh and C.-T. Chin, "Toward Blockchain Realization," *Fintech*, vol. 1, pp. 81–99, 2022, https://doi.org/10.3390/fintech1010007.
[30] T.-T. Kuo, H. Kim, and L. Ohno-Machado, "Blockchain distributed ledger technologies for biomedical and health

care applications," *J. Am. Med. Informatics Assoc.*, vol. 26, no. 6, pp. 1211–1220, 2017, https://doi.org/10.1093/jamia/ocx068.
[31] M. T. Al Ahmed, F. Hashim, S. Jahari Hashim, and A. Abdullah, "Hierarchical blockchain structure for node authentication in IoT networks," *Egypt. Informatics J.*, 2022, https://doi.org/10.1016/j.eij.2022.02.005.
[32] Mohamed Tahar Hammi, B. Hammi, P. Bellot, and A. Serhrouchni, "Bubbles of Trust: A decentralized blockchain-based authentication system for IoT," *Comput. Secur.*, vol. 78, pp. 126–142, 2018, https://doi.org/10.1016/j.cose.2018.06.004.
[33] B. Cao, Z. Zhang, D. Feng, S. Zhang, L. Zhang, M. Peng, and Y. Li "Performance analysis and comparison of PoW, PoS and DAG based blockchains," *Digit. Commun. Networks*, vol. 6, no. 4, pp. 480–485, 2020, https://doi.org/10.1016/j.dcan.2019.12.001.
[34] I. G. A. K. Gemeliarana and R. F. Sari, "Evaluation of Proof of Work (POW) Blockchains Security Network on Selfish Mining," *2018 International Seminar on Research of Information Technology and Intelligent Systems (ISRITI)*, pp. 126-130, 2018, https://doi.org/10.1109/ISRITI.2018.8864381.
[35] S. M. Idrees, M. Nowostawski, R. Jameel, and A. K. Mourya, "Security Aspects of Blockchain Technology Intended for," *Electronics*, vol. 10, no. 951, pp. 2–24, 2021, https://doi.org/10.3390/electronics10080951.
[36] J. Vora, P. Italiya, S. Tanwar, S. Tyagi, N. Kumar, M. S. Obaidat, and K-F. Hsiao, "Ensuring Privacy and Security in E- Health Records," in *2018 International Conference on Computer, Information and Telecommunication Systems (CITS)*, 2018, pp. 1–5, https://doi.org/10.1109/CITS.2018.8440164.
[37] N. M. Kumar and P. K. Mallick, "Blockchain technology for security issues and challenges in IoT," in *Procedia Computer Science*, 2018, vol. 132, pp. 1815–1823, https://doi.org/10.1016/j.procs.2018.05.140.
[38] D. Ichikawa, M. Kashiyama, and T. Ueno, "Tamper-Resistant Mobile Health Using Blockchain Technology," *JMIR mhealth uhealth*, vol. 5, no. 7, 2017, https://doi.org/10.2196/mhealth.7938.
[39] A. AlOmara, M. Z. A. Bhuiyan, A. Basuc, S. Kiyomoto, and M. S. Rahman, "Privacy-friendly platform for healthcare data in cloud based on blockchain environment," *Futur. Gener. Comput. Syst.*, vol. 95, pp. 511–521, 2019, https://doi.org/10.1016/j.future.2018.12.044.
[40] R. Singh, S. Tanwar, and T. P. Sharma, "Utilization of blockchain for mitigating the distributed denial of service attacks," *Security and Privacy*, vol. 3, no. 3, 2019, https://doi.org/10.1002/spy2.96.
[41] D. Tapscott, A. Tapscott, and J. Pilgrim, *How Blockchain Will Change Organizations*, MIT Sloan Management Review, 2017, https://sloanreview.mit.edu/article/how-blockchain-will-change-organizations/.
[42] V. Y. Kemmoe, W. Stone, J. Kim, D. Kim, and J. Son, "Recent Advances in Smart Contracts: A Technical Overview and State of the Art," *IEEE Access*, vol. 8, pp. 117782–117801, 2020, https://doi.org/10.1109/ACCESS.2020.3005020.
[43] S. Nakamoto, "Bitcoin: A Peer-to-Peer Electronic Cash System," 2008, https://bitcoin.org/bitcoin.pdf.
[44] M. G. Vigliotti, "What Do We Mean by Smart Contracts? Open Challenges in Smart Contracts," Frontiers in Blockchain, vol. 3, Feb. 2021, https://doi.org/10.3389/fbloc.2020.553671.
[45] "Ethereum Whitepaper," https://ethereum.org/en/whitepaper/.
[46] E. S. Negara, A. N. Hidayanto, R. Andryani, and R. Syaputra, "Survey of smart contract framework and its application," *Inf.*, vol. 12, no. 7, pp. 1–10, 2021, https://doi.org/10.3390/info12070257.
[47] S. Wang, Y. Yuan, X. Wang, J. Li, R. Qin, and F.-Y. Wang, "An Overview of Smart Contract: Architecture, Applications, and Future Trends," *2018 IEEE Intelligent Vehicles Symposium (IV)*, 2018, pp. 108-113, https://doi.org/10.1109/IVS.2018.8500488.
[48] E. Hildenbrandt *et al.*, "KEVM: A complete formal semantics of the ethereum virtual machine," in *Proceedings - IEEE Computer Security Foundations Symposium*, 2018, vol. 2018-July, pp. 204–217, https://doi.org/10.1109/CSF.2018.00022.
[49] I. Bashir, *Mastering Blockchain: Distributed ledger technology, decentralization, and smart contracts explained*. Birmingham, UK: Packt Publishing Ltd, 2018, https://books.google.co.id/books?id=3ZlUDwAAQBAJ.
[50] K. Salah, M. H. U. Rehman, N. Nizamuddin, and A. Al-Fuqaha, "Blockchain for AI: Review and open research challenges," *IEEE Access*, vol. 7, pp. 10127–10149, 2019, https://doi.org/10.1109/ACCESS.2018.2890507.
[51] A. Haleem, M. Javaid, R. P. Singh, R. Suman, and S. Rab, "Blockchain technology applications in healthcare: An overview," *Int. J. Intell. Networks*, vol. 2, no. September, pp. 130–139, 2021, https://doi.org/10.1016/j.ijin.2021.09.005.
[52] "Medicalchain," https://medicalchain.com/en/.
[53] H. H. Khan, M. N. Malik, Z. Konečná, A. G. Chofreh, F. A. Goni, and J. J. Klemeš, "Blockchain technology for agricultural supply chains during the COVID-19 pandemic: Benefits and cleaner solutions," *J. Clean. Prod.*, p. 131268, 2022, https://doi.org/10.1016/j.jclepro.2022.131268.
[54] "IBM Food Trust: A New Era In The World's Food Supplt," https://www.ibm.com/blockchain/solutions/food-trust.
[55] F. Casino, V. Kanakaris, T. K. Dasaklis, S. Moschuris, and N. P. Rachaniotis, "Modeling food supply chain traceability based on blockchain technology," *IFAC-PapersOnLine*, vol. 52, no. 13, pp. 2728–2733, 2019, https://doi.org/10.1016/j.ifacol.2019.11.620.
[56] S. I. M. Ali, H. Farouk, and H. Sharaf, "A blockchain-based models for student information systems," *Egypt. Informatics J.*, vol. 23, no. 2, pp. 187-196, 2021, https://doi.org/10.1016/j.eij.2021.12.002.
[57] P. Baudier, G. Kondrateva, C. Ammi, and E. Seulliet, "Peace engineering: The contribution of blockchain systems to the e-voting process," *Technol. Forecast. Soc. Change*, vol. 162, no. October 2020, p. 120397, 2021, https://doi.org/10.1016/j.techfore.2020.120397.

BIOGRAPHY OF AUTHORS

Purwono was Born on May 16, 1989 in Banyumas Indonesia. He is a graduate of the Information Systems College of Computer Science (STIKOM) Yos Sudarso in 2019. His postgraduate education is a master's program in Informatics Engineering at Universitas Ahmad Dahlan (UAD). Currently, he is a lecturer in the informatics study program at Harapan Bangsa University (UHB) Purwokerto. Areas of interest are Data Science, Blockchain, Internet of Things. Email: purwono@uhb.ac.id

Alfian Ma'arif was born in Klaten, Central Java, Indonesia, in 1991. He received the bachelor's degree from the Department of Electrical Engineering, Universitas Islam Indonesia, in 2014, and the master's degree from the Department of Electrical Engineering, Universitas Gadjah Mada, in 2017. Since 2018, he has been a Lecturer with the Department of Electrical Engineering, Universitas Ahmad Dahlan. He is currently an Assistant Professor, since 2020. His research interest includes control systems. He is a member of IEEE and ASCEE. He is the Editor in Chief of International Journal of Robotics and Control Systems. Email: alfianmaarif@ee.uad.ac.id

Wahyu Rahmaniar received the B.S. degree in Electronics and Instrumentation from the Universitas Gadjah Mada, Yogyakarta, Indonesia, in 2009 and the Ph.D. degree in Electrical Engineering from the National Central University, Taiwan, in 2020. She is currently a Postdoctoral researcher with the National Taipei University of Technology, Taiwan. Her research interests include artificial intelligence, computer vision, medical imaging, and robotics. Email: wahyu.rahmaniar@gmail.com

Qazi Mazhar ul Haq received the M.S. degree in Electrical Engineering from the National University of Sciences and Technology Islamabad, Pakistan, in 2016 and the Ph.D. from the National Taiwan University of Science and Technology, Taiwan, in 2021. He is currently a postdoctoral researcher in the Intelligent Control Lab of Electrical engineering at the National Taipei University of Technology. His research interests include object detection, classification, life-long learning, and medical image processing. Email: q.mazhar876@gmail.com

Dimas Herjuno currently pursue a doctoral degree at Kyushu Institute of Technology. He received a bachelor's degree in electrical engineering from Sepuluh Nopember Institute of Technology Surabaya in 2012 and a master's degree in electronics engineering from National Taiwan University of Science and Technology in 2017. His research interests include computer vision, deep learning, and robotics. Email: herjuno.dimas478@mail.kyutech.jp

Muchammad Naseer received a bachelor degree in Computer System from the ITB STIKOM Bali, Bali, Indonesia, in 2008 and the Master degree in Electrical Engineering from the Universitas Indonesia, Indonesia, in 2013. He is currently a Ph.D. student in Universitas Indonesia and also a Lecturer in Informatics from Sekolah Tinggi Teknologi Bandung. His research interests include artificial intelligence, natural language processing, and computer vision. Email: naseer@sttbandung.ac.id