Research Article

Application of Blockchain Technology Based on Privacy Data Protection in RMB Internationalization Path

Yang Yi

International Business School, Shaanxi Normal University, Xi’an 710119, Shaanxi Province, China

Correspondence should be addressed to Yang Yi; yangyi@snnu.edu.cn

Received 30 June 2022; Revised 29 July 2022; Accepted 6 August 2022; Published 7 September 2022

Academic Editor: Praveen Kumar Reddy Maddikunta

Copyright © 2022 Yang Yi. This is an open access article distributed under the Creative Commons Attribution License, which permits unrestricted use, distribution, and reproduction in any medium, provided the original work is properly cited.

With the integration of industrial Internet of Things technology and traditional industries, industrial Internet of Things has profoundly changed the production mode, organization mode, and business model of traditional industries. While people are enjoying the convenience brought by the Internet, their concerns about personal privacy are gradually increasing. Maintaining the value stability of RMB payment means and the security and efficiency of RMB settlement system are the key measures to promote the internationalization of RMB. Aiming at the problem of data insecurity and untrustworthiness in traditional information systems, this paper proposes a data protection technology for information systems based on blockchain. In the hierarchical authority information system, multichain structure is adopted to divide the authority of nodes in each layer, so that only the nodes with corresponding authority can access and operate data. Private digital currency, which is based on blockchain technology and represented by payment token and stable currency, helps to improve the defects of the agent banking model but increases additional market risks and trust risks. Blockchain technology adopts special networking technology and consensus mechanism. Therefore, in blockchain privacy protection, the focus of blockchain privacy protection is identity information and transaction information.

1. Introduction

At present, a new round of technological change and industrial revolution is booming. New technologies such as cloud computing, big data, artificial intelligence, and blockchain have emerged one after another. Emerging digital technologies are constantly developing and maturing, gradually changing the lifestyle and production mode of our society [1]. Blockchain is a distributed decentralized ledger that connects data blocks in time order in a form similar to a linked list, and then uses cryptography-related technologies to ensure that its transaction information is tamper proof and forgeable [2]. However, consensus algorithm is the core that affects the whole blockchain system. It can be said that the efficiency of consensus algorithm directly determines the performance of the blockchain system [3]. Therefore, research on the efficiency of blockchain consensus algorithms has a positive impact on promoting the development of blockchain technology. As an important means of personal data circulation, personal data transactions meet the needs of data buyers and allow data sellers to obtain economic benefits from them [4]. At the same time, personal data transaction promotes the open sharing of data and the integration of resources, so that personal data play an important role in social governance, scientific research, product development and marketing, and public life entertainment [5].

Currency internationalization is a very important and complex phenomenon in the international monetary field. The internationalization of a country’s currency is the result of the joint action of market demand and government supply [6]. When a currency has the conditions for internationalization, internationalization is an inevitable trend. The role of the government is to accelerate or slow down the process of currency internationalization [7]. To become an international currency, a country needs the political stability, strong economy, strong scientific and technological strength, developed financial market, stable currency value, and large market share and influence in international trade.
and investment [8]. Usually, the security and trustworthiness of data depend on trusted entities such as the system center or a third party. Once a trusted entity is no longer trusted, such as administrators being bought off, databases being invaded and tampered with, the security and reliability of data will be reduced. Credibility will not be guaranteed [9]. Under the existing rights management mechanism, third-party service providers can obtain the same user privacy information of their host applications, while the services of the same service provider are often integrated into multiple applications to collect the multidimensional information of the same user in different applications, and then draw a complete user portrait. However, in the blockchain, all transaction data must be fully disclosed to the distributed nodes for legitimacy verification to ensure that the distributed nodes can reach agreement on the block data on the peer-to-peer network. However, when the transaction data are publicly verifiable, the transaction data will disclose sensitive information such as transaction rules and identity privacy information [10].

The main innovations in this paper are as follows:

1. The original permanent nodes with resources and the right to vote in DDPOS algorithm can become the selected nodes, and the nodes with certain computing power can be selected by PoW to participate in the election. This can reduce the influence of ownership on becoming the selected node.

2. The original DDPOSalgorithm voted according to the number of blockchain resources a node has, and each node has only one vote for random voting. In this way, the impact of rights and interests on becoming a witness node can be weakened, the rights and interests of blocks can be decentralized as much as possible, and the node activity of the entire blockchain system can be mobilized.

3. In order to deal with the problem of malicious damage to the system by witness nodes in the DDPOS algorithm, the promotion system similar to that in modern sports leagues is introduced to quickly eliminate the malicious nodes, so as to maintain the good operation of the system.

This paper constructs a research model from two aspects: blockchain infrastructure based on privacy data protection and RMB internationalization technology based on DDPOS algorithm, and proposes RMB internationalization model based on blockchain technology. Then, an experimental environment is set up, and the effectiveness of the encryption algorithm in this paper and its role in RMB internationalization are verified through experimental analysis. Finally, the research and contribution of this paper are summarized, and the future development direction is put forward.

2. Related Work

With the rise of China’s economy, the internationalization of RMB has become an inevitable trend in the twenty-first century. At present, the internationalization of RMB and the development of offshore RMB business in Hong Kong are in the initial stage, which is about to be accelerated. In particular, it is necessary to have a big framework and a phased grasp, and a top-level design of the branch path of RMB internationalization is needed.

He believes that when a country’s currency is accepted by its individuals or institutions, the internationalization of its currency begins [11]. Zhang and Liu studied the transaction cost between domestic and foreign currencies and found that with the increase in transaction volume, the average transaction cost is decreasing, so the currency with the largest transaction volume and the lowest transaction cost will become the medium currency [12]. Hou established a model to analyze the research made by Krugman (1980) and theoretically proved the multiple equilibrium of the choice of media currency. He found that the preference of countries for commodity demand rather than the size of commodity demand determines the choice of media currency [13]. The idea of the algorithm proposed by Sambana is to infer the source node by using the time sequence of information forwarded by neighbor nodes. This attack method can also detect nodes hidden by Nat services [14]. Zhang proposed a malicious node detection method based on behavior pattern clustering, which can quickly locate and eliminate malicious nodes by analyzing the behavior patterns of distributed nodes, and greatly reduce the harm of malicious nodes to blockchain networks. With regard to data obfuscation methods, researchers suggest that blockchain applications should be used on private networks that can hide IP addresses, such as Onion Network [15]. Competing the computing resources of each blockchain node against Kapadia, so as to compete for the power to generate blocks, it consumes a lot of computer resources and power resources (the global Bitcoin network can consume 48.5 TW/h a year, or 485 TW/h). 100 million kWh, while Singapore’s annual electricity consumption is only 49.8 billion kWh, and the annual power consumption of the Bitcoin network is still increasing) [16]. Nasirov proposed a device management scheme for the Internet of things with privacy protection. In the scheme, the device information is shared among multiple organizations by taking advantage of the characteristics that blockchain data records cannot be tampered with, forged, and verified; Attribute-based encryption algorithm is adopted to ensure data privacy and provide fine-grained access control based on users’ roles and attributes; A time-limited key management mechanism is designed to realize the automatic revocation of keys [17]. Wu et al. pointed out that in the early stage of RMB internationalization, the Chinese currency circle can be launched in a coordinated manner so that the Chinese currency can compete with the Japanese yen and even the euro [18]. Wang et al. believe that the path of RMB internationalization has actually chosen the yen model, and this model is in line with China’s national conditions. With the complete reunification of the motherland, the mainland, Hong Kong, Macau, and Taiwan Province have become a unified economy, and four currencies can be merged into a single currency: the Chinese dollar; The single currency will adopt the internationalization path model of euro to realize internationalization [19].
3. Methodology

The blockchain is built on an open and interconnected computer network. It needs to use the communication ability of the network to transmit various information for it. Blockchain infrastructure is very similar to the Open System Interconnection (OSI) formulated by the International Organization for Standardization (ISO): the OSI model divides the work of network communication into seven layers, namely physical layer, data link layer, network layer, transport layer, session layer, presentation layer, and application layer; the blockchain system divides its infrastructure into six layers according to different functions, which are composed of data layer, network layer, consensus layer, incentive layer, contract layer, and application layer from low to high.

3.1. Infrastructure Analysis of Blockchain Based on Privacy Data Protection

3.1.1. Encryption Technology of Blockchain

(1) Alice and Bob do not know each other in advance, and there is no reliable and safe communication channel, but now Alice wants to send information to Bob through the insecure Internet.

(2) Alice writes the original text, which is called plaintext $X$ in the unencrypted state.

(3) Bob uses Cryptographic Secure Pseudorandom Number Generator (CSPRNG) to generate a pair of keys, one of which is $C$ as the public key and the other is $D$ as the private key.

(4) Bob can send the public key $C$ to Alice in any way, even if Eve eavesdrops on $C$ in the middle.

(5) Alice encrypts the plaintext $X$ with the public key $C$ to obtain the ciphertext $C(X)$.

(6) Alice can transmit the ciphertext $C(X)$ to Bob by any method, even if Eve eavesdrops on the ciphertext $C(X)$ in the middle, it is no problem.

(7) Bob receives the ciphertext and uses the private key $D$ to pair the ciphertext $C(X)$, $X$ decrypt $D(C(X))$ to obtain the plaintext $X$ written by Alice.

3.1.2. The Calculation Process of the Public Algorithm

(1) The client sends a request to wake up the service operation of the master node.

(2) The master node broadcasts the request to other nodes.

(3) Many secondary nodes perform operations and send replies to clients.

(4) The client waits for the same reply from different nodes, which is the result of the operation.

3.2. RMB Internationalization Technology Based on DDPOS Algorithm.

Marx discussed the issue of currency internationalization in the first article “Commodity and Currency” in the first volume of his Capital, which was embodied in his monetary theory. When a country’s currency plays the functions of value scale, circulation means, payment means, and storage means in a certain area, it is called regional currency, and once it plays the four basic functions of currency in the global scope, it becomes the world currency. The world currency serves as the general means of payment, the general means of purchase, and the absolute social materialization of wealth. In the era of the gold and silver standard, since gold and silver are commodities themselves, they have a certain value and can be used globally. It can be circulated and freely convertible, and has the function of automatically adjusting the amount of currency in circulation. Therefore, in the era of the gold standard and the silver standard, gold and silver are international currencies, that is, "the currency will be released as soon as it leaves the domestic circulation field. The local forms obtained there as price scales - coins, coins and symbols of value, return to the original bar form of precious metals". Marx also emphasized that if gold and silver removed the state form of natural value, it could serve as the world currency. Marx lived in the era of metal currency and convertible bank notes. Limited by the cognitive conditions at that time, he believed that only valuable precious metals such as gold and silver could serve as the world currency. In today's credit currency era, even if a country's currency has realized the advanced form of currency internationalization-globalization, it cannot be completely equal to the situation that gold is the world currency under the gold standard system. Blockchain-based distributed ledger technology can change the chain structure.
of cross-border payment. Transforming the one-to-one trust relationship into the sharing of capital information can improve the efficiency of payment and reduce the risks brought by cross-border. The use of RMB can also reduce the involvement of third-party organizations and cross-border payment costs. Because credit currency acts as a global currency, there is naturally an irreconcilable internal contradiction between confidence and liquidity, which will lead to the instability of the international monetary system. In this paper, the blockchain consensus environment of d DPOs algorithm is shown in Figure 1.

Transaction node $N_i^T$ is responsible for the creation, dissemination, and storage of transaction information. Witness node $N_i^W$ is responsible for packaging transactions into blocks and broadcasting the blocks. Consensus node $N_i^C$ is responsible for verifying the block. Each node in the blockchain network will add the verified block to its own blockchain.

Before starting the consensus block, this article defines a status bit in the block header with the value of GOOD, NORMAL, or ERROR: GOOD means good status, which is a successfully verified block; NORMAL means normal status, NORMAL is the default status of Value; ERROR indicates an error state, indicating that this is a block that failed to verify, and the node also becomes a malicious node. If the status bit is ERROR, the system enters the malicious node elimination mode.

Each blockchain network has only one system chain. If all data are public, the network will not need multiple virtual chains, and all data will be visible to members. Because the information system needs to ensure strong data privacy, it needs multiple chains to isolate data and provide confidentiality. According to the privacy protection requirements of information systems, this paper proposes a hierarchical Multi Chain blockchain structure, as shown in Figure 2. The primary information system participates in the primary information system chain, the secondary information system participates in the secondary information system chain, the tertiary information system participates in the tertiary information system chain, and the information unit does not participate in the blockchain.

Developing international credit business itself has great risks. The traditional transnational credit business with physical currency as the medium needs the intervention of third-party financial institutions, which increases the cost of credit business. Digital RMB supported by blockchain technology can make up for the shortage of traditional multinational bank credit. Consensus nodes: consensus nodes are connected with all nodes, and provide consensus services for the whole blockchain, and provide subscribed topics for nodes on the blockchain. Each topic is a channel, and consensus nodes do not store data, but are only responsible for generating blocks in time series and sending encapsulated blocks to each node through channels. The process of instruction issuance and block generation is shown in Figure 3.

The upper level node first sends instructions to the lower level nodes, and sends them to the lower level nodes in the form of instruction data packets. Consensus node. The consensus node encapsulates data packets into blocks and distributes them to upper level nodes through channels. The upper level nodes add new blocks to the local ledger and update the blockchain. Nodes with higher permissions can participate in more chains and have more ledgers in the blockchain. Therefore, nodes with higher permissions can monitor the behavior of nodes by reading blockchain data.
3.3. RMB Internationalization Model Based on Blockchain Technology. According to the difference in the number of payment and clearing operators, these settlement systems can be divided into “centralized system” which is currently dominant and “distributed system” represented by blockchain. In the former, a single network operator (such as the central bank) is responsible for verifying and storing settlement information, and at the same time providing users with services such as information query, sharing, and reconciliation. “Distributed system” distributes system operation functions such as verification and recording information, maintenance system to each subject entitled to participate in the operation of the system, namely “nodes” (hereinafter referred to as “operating participants”). The blockchain distributed settlement system can avoid the destruction of the clearing order caused by a single system operator’s suspension or random change of clearing information in the event of a technical failure, ensure the security and integrity of clearing information, and realize the trustworthiness of the clearing information in the absence of a centralized operator. This is mainly reflected in “no double flowers” for digital currency, that is, the settlement information cannot be copied.

Firstly, the algorithm of consensus node module is selected: from the system broadcast difficulty value \(d\) and random number nonce, to the output witness node and alternative node. The algorithm for selecting consensus node module is shown in formula (1). Where \(\xi\) represents the random number generated by the trading node, and \(V\) represents the number of votes obtained by the consensus node \(N_i^n\).

\[
N_i^n : \text{HASH(HASH(preBlockHead), nonce),}
\]
\[
\text{while (HASH(HASH(PreBlockHead), nonce) > } D),
\]
\[
\text{nonce} = \text{nonce} + 1,
\]
\[
\xi N_i^n \leftarrow \text{(int) (Math.random} \ast i),
\]
\[
N_i^n \leftarrow N_i^n (i \in (m, l - m)).
\]

Then there is the node consensus block module algorithm: starting from the witness node packaging the block, to the block being broadcast to all consensus nodes for verification, and finally outputting the successfully verified block or the failed verification block. The node consensus block module
algorithm is shown in formula (2). Among them, NUMBER represents the number of statistical blocks.

Output: BLOCK\textsubscript{GOOD} or BLOCK\textsubscript{ERROR}

\[ \begin{align*}
N_i^c \leftarrow \langle \text{MerkleTreeRoot}, \text{TimeStamp}, D, nonce, t, \text{txs} \rangle,
\end{align*} \]

\[ \begin{align*}
N_i^{W} & \leftarrow \sum \text{BLOCK}_{N_i}^{c}, \\
\text{NUMBER}_{\text{BLOCK}}^{N_i} & \leftarrow \sum \text{BLOCK}_{N_i}^{c}, \\
\text{if NUMBER}_{\text{BLOCK}}^{N_i} & > \text{NUMBER}_{\text{BLOCK}}^{N_i}.
\end{align*} \]

(2)

Finally, the algorithm of eliminating malicious node module: when a malicious node appears in the blockchain network, it means that a malicious node appears, all consensus nodes stop consensus, use the escalation mechanism to reduce the malicious node to the set of candidate nodes, and then promote the first candidate node to the witness node. The node consensus block module algorithm is shown in formula (3).

\[ \begin{align*}
N_i^{W} & \rightarrow \langle \text{BLOCKERROR} \rangle, \\
N_{i-m}^{W} & \rightarrow \text{BLOCKERROR}.
\end{align*} \]

(3)

(4)

By analyzing and comparing the advantages and disadvantages of several mainstream consensus algorithms, the problems to be solved in this paper and the ideas to solve them are put forward. Then, it describes the idea and process of improved DDPOS algorithm. Finally, the design and implementation of the improved DDPOS algorithm are described in detail.

4. Result Analysis and Discussion

This paper adopts the method of simulation experiment: build the experimental environment in Eclipse; use Java language to simulate the DDPOS algorithm. This article uses the threading technology in the Java language to simulate a blockchain node with a thread (the problem that this brings is: all nodes have the same level of computing power. In order to ensure that the nodes in the experiment are closer to the reality, this paper gives different priorities to different nodes in the experiment to ensure that the computing power of different nodes is different). In the experiment, the blockchain nodes of different sizes are given by changing the parameters of the number of nodes, such as 500, 1000, 2000, 3000, 4000, and 5000, and the corresponding number of nodes in the blockchain environment is simulated. By controlling the running time of DDPOS algorithm (10, 20, 30, 40, 50, and 60 minutes), the running results of DDPOS algorithm are observed, and the experimental data are statistically analyzed. In order to improve the persuasiveness of the experimental data, this paper also simulates the traditional PoW, PoS, and DPoS consensus algorithms in the experimental environment of this paper, and analyzes and compares them with the experimental results of the DDPOS algorithm. The software configuration parameters are shown in Table 1.

With the increase in time, the number of blocks generated by DDPOS consensus algorithm increases linearly, and the upward trend increases slightly. The possible reason
is that it takes a certain amount of time to select consensus node modules in DDPOS consensus algorithm. With the increase in consensus time, the proportion of time spent in selecting consensus node modules in the whole consensus time is decreasing, resulting in a slight increase in the number of generated blocks. Substituting the data in Figure 4 into (4) mentioned above, it can be concluded that the block generation efficiency SPB of the DDPOS consensus algorithm under the scale of 1000 nodes is approximately 9 seconds per block. As shown in Figure 4.

Next, the number of blocks generated by the DDPOS consensus algorithm for nodes of different sizes (500, 1000, 2000, 3000, 4000, and 5000) within 10 minutes is counted, and a line graph is drawn showing that the number of blocks generated varies with the size of the nodes, as shown in Figure 5. It is found from Figure 5 that when the node size is less than 3000, the blocking efficiency SPB of the DDPOS consensus algorithm is about 9 seconds/node; However, with the expansion of the node size, when the node size exceeds 4000, the blocking efficiency SPB of the DDPOS consensus algorithm will decrease; When the node size reaches 5000, the blocking efficiency SPB of the DDPOS consensus algorithm will be reduced to 10 seconds/node.

Then, we will show the line chart of the number of blocks generated by the three consensus algorithms of PoW, PoS, and d DPoS in different time periods (10, 20, 30, 40, 50, and 60 minutes) and nodes of different scales (500, 1000, 2000, 3000, 4000, and 5000), and analyze D DPO from it.

From the comprehensive analysis of Figures 6 and 7, it can be concluded that the consensus efficiency of the PoW consensus algorithm is 600 seconds/piece, while the consensus efficiency of the PoS consensus algorithm is about 61 seconds/piece, which is basically consistent with the data given in tables 2-3. Figure 6 comparison chart of block discount generated by three formula algorithms in 10 minutes. From these six line charts, it can be clearly seen that the d DPoS consensus algorithm, no matter in what time period (10, 20, 30, 40, 50, and 60 minutes) or in different node sizes (500, 1000, 2000, 3000, 4000, and 5000). Then, the consensus time is set to 20 minutes, 30 minutes, 40 minutes, 50 minutes, and 60 minutes, respectively, and the number of designated malicious nodes and the number of malicious nodes found are counted. The experimental results are shown in Table 2.

From Table 2, it is found that when the consensus time is 10 minutes, the number of designated malicious nodes is 8,
and the DDPOS algorithm finds 7 malicious nodes during operation and performs level up and down operations on them; When the consensus time exceeds 20 minutes, no matter how many malicious nodes are specified, the DDPOS algorithm can find them and perform ascending and descending operations. When the consensus time exceeds 20 minutes, the number of generated blocks is more than 101, and each witness node will have the power to generate blocks, so all designated malicious nodes will be found. It also proves that the promotion and demotion mechanism introduced in this paper can solve the problem of witness node destruction in DPoS algorithm.
5. Conclusions

In the era of digital economy, for sovereign countries, the best way to practice the issuing right of monetary countries is for the state to issue and control digital currency. Maintaining the value stability of RMB payment means and the security and efficiency of RMB settlement system are the key measures to promote the internationalization of RMB. Try not to let third parties store and master personal data and sensitive data, because these data can be easily attacked or misused. On the contrary, users need to control their data from security threats, and cannot be restricted by enterprises or authorities to provide personalized services. After experimental verification, it is found that the consistency efficiency of the improved algorithm is obviously higher than that of PoW and PoS. Although it is slightly inferior to DPoS, it is better than DPoS in the centralization of block generation nodes, and the introduced upgrade and upgrade mechanism can also be very effective. It makes up for the problem that the witness nodes of the original DPoS consensus algorithm are destroyed. In the future, the block structure will be improved, and the multisignature technology will be used to sign the block, so as to further improve the information security of the information system and the information security protection level of the information system.

Table 2: Fault tolerance analysis statistics table.

| Test results/time (minutes) | 10 | 20 | 30 | 40 | 50 | 60 |
|-----------------------------|----|----|----|----|----|----|
| Specify the number of malicious nodes (pieces) | 8  | 8  | 8  | 9  | 10 | 10 |
| The number of malicious nodes found (pieces) | 7  | 8  | 10 | 9  | 10 | 12 |

Data Availability

The data used to support the findings of this study are included within the article.

Conflicts of Interest

The author declares that there are no conflicts of interest.

References

[1] M. H. Au, J. Han, Q. Wu, and C. Boyd, Special issue on cryptographic currency and blockchain technology,” Future Generation Computer Systems, vol. 107, pp. 758-759, 2020.
[2] Surjandy, Meyliana, and H. Leslie, “The recent trend of organization development influenced by blockchain technology,” ICIC Express Letters, vol. 15, no. 4, pp. 389–396, 2021.
[3] S. Youn and H. C. Cho, “Blockchain technology in finance industry,” The Transactions of the Korean Institute of Electrical Engineers, vol. 68, no. 12, pp. 1601–1606, 2019.
[4] A. Esmat, P. Palensky, D. Epema, M. de Vos, and Y. Ghiassi-Farrokhi, “A novel decentralized platform for peer-to-peer energy trading market with blockchain technology,” Applied Energy, vol. 282, no. 22, Article ID 116123, 2021.
[5] S. Peng, L. Zhu, Z. Cai, W. Liu, C. He, and W. Tang, “Dynamic optimization of government data transmission based on blockchain technology,” Mobile Information Systems, pp. 1–8, 2021.
[6] Z. Xue, Y. Zhang, P. Liu, M. Wang, and Q. Zhang, “A regulatable blockchain transaction model with privacy protection,” International Journal of Computational Intelligence Systems, vol. 14, no. 1, p. 1642, 2021.
[7] K. O’Hara, “The digital citizen: authority printed upon emptiness: the prospects for Bitcoin,” IEEE Internet Computing, vol. 19, no. 6, pp. 72–76, 2015.
[8] Z. Bao, W. Shi, S. Kumari, Z. Y. Kong, and C. M. Chen, “Lockmix: a secure and privacy-preserving mix service for Bitcoin anonymity,” *International Journal of Information Security*, vol. 19, no. 3, pp. 311–321, 2019.

[9] M. H. Ibrahim, “SecureCoin: a robust secure and efficient protocol for anonymous Bitcoin ecosystem,” *International Journal on Network Security*, vol. 19, no. 2, pp. 295–312, 2017.

[10] D. He, A. Castiglione, K. K. R. Choo, and N. Kumar, “IEEE access special section editorial: research challenges and opportunities in security and privacy of blockchain technologies,” *IEEE Access*, vol. 6, Article ID 72033, 2018.

[11] C. Li, X. Sun, and Z. Zhang, “Effective methods and performance analysis of a satellite network security mechanism based on blockchain technology,” *IEEE Access*, vol. 9, no. 12, Article ID 113558, 2021.

[12] Z. Zhang and J. Liu, “Application of blockchain technology in international trade[,]” *Logistics Sci-Tech*, 2019.

[13] H. Si, C. Sun, Y. Li, H. Qiao, and L. Shi, “IoT information sharing security mechanism based on blockchain technology,” *Future Generation Computer Systems*, vol. 101, pp. 1028–1040, 2019.

[14] B. Sambana, “Blockchain Technology: Bitcoins, Cryptocurrency and Applications,” 2021, https://arxiv.org/abs/2107.07964.

[15] J. Zhang, “Analysis on the Status and Trends of Patent Application of Blockchain Technology in China,” *China Invention & Patent*, 2018.

[16] J. M. Kapadia, “Blockchain Technology: Application in the financial industry,” *Scholeje International Journal of Management & Development ISSN*, vol. 2394-3378, no. 8, 2021.

[17] S. Nasirov, I. Gokh, and F. Filippaios, “Technological radicalness, R&D internationalization, and the moderating effect of intellectual property protection,” *Journal of Business Research*, vol. 145, no. 20, pp. 215–227, 2022.

[18] Z. Wu, C. Lu, Y. Zhao, J. Xie, D. Zou, and X. Su, “The protection of user preference privacy in personalized information retrieval: challenges and overviews,” *Libri - International Journal of Libraries and Information Services*, vol. 71, no. 3, pp. 227–237, 2021.

[19] D. Wang, J. Zhao, and Y. Wang, “A survey on privacy protection of blockchain: the technology and application,” *IEEE Access*, vol. 8, no. 99, Article ID 108766, 2020.

[20] H. Wang, Ma S, and H. N. Dai, “Blockchain-based data privacy management with Nudge theory in open banking,” *Future Generation Computer Systems*, vol. 2019, no. 23, pp. 110–123, 2019.

[21] L. Xu, X. Zhou, X. Li, R. H. Jhaveri, T. R. Gadekallu, and Y. Ding, “Mobile collaborative secrecy performance prediction for artificial IoT networks,” *IEEE Transactions on Industrial Informatics*, vol. 18, no. 8, pp. 5403–5411, 2022.

[22] R. Durga, E. Poovammal, K. Ramana, R. H. Jhaveri, S. Singh, and B. Yoon, “CES blocks—a novel chaotic encryption schemes-based blockchain system for an IoT environment,” *IEEE Access*, vol. 10, Article ID 11354, 2022.

[23] A. R. Khan, M. Kashif, R. H. Jhaveri, R. Raut, T. Saba, and S. A. Bahaj, “Deep learning for intrusion detection and security of Internet of things (IoT): current analysis, challenges, and possible solutions,” *Security and Communication Networks*, pp. 1–13, 2022.