Hindawi
Mobile Information Systems
Volume 2022, Article ID 7908625, 13 pages
https://doi.org/10.1155/2022/7908625

Research Article

The Current Situation and Trend of Blockchain Technology in the Financial Field

Weixuan Zhang

College of Arts and Science, Vanderbilt University, Nashville 003535, Tennessee, USA

Correspondence should be addressed to Weixuan Zhang; weixuan.zhang@vanderbilt.edu

Received 24 May 2022; Revised 5 July 2022; Accepted 14 July 2022; Published 8 August 2022

Academic Editor: Yanyi Rao

In the Internet era, with the development and application of information technology, the financial environment is becoming more and more complex, and traditional financial business products and service models are gradually unable to meet people's daily needs. In response to this problem, it is important to iteratively upgrade the traditional business products by rationally applying the existing information technology in the entire financial market and realize the adjustment of the organizational structure of financial institutions and the optimization of products and services. With the development of network technology, the research on the application of blockchain technology in the financial field is gradually carried out, and its advantages and characteristics are of great significance to the optimization and upgrading of the traditional financial system. The purpose of this paper is to analyze the research status and trends of blockchain technology in the financial field. Through CiteSpace to analyze all relevant researches on blockchain technology in the financial field, we can grasp the research status and trends of blockchain technology in the financial field as a whole, coping with financial issues in the new environment. This article explains the basic theory of blockchain technology and conducts an overall visual analysis of related research on blockchain technology in the financial field based on CiteSpace. The results showed that the research keywords of blockchain technology in the financial field at home and abroad are concentrated in "supply chain finance," and China's research on this keyword accounts for 59.5%. Foreign research on this keyword accounts for 26.5%. The difference is 33%, and the overall popularity is on the rise.

1. Introduction

With the continuous progress of the times, the rapid development of the national economy and the process of urbanization have promoted the rapid development of Internet technology. At the same time, the Internet finance industry continues to mature. In order to solve the current business pain points of serious centralization, opaque transaction information, and difficulty in establishing customer credit in the financial industry, scholars have actively explored the Internet transformation in the traditional financial field. Blockchain technology is a brand-new distributed infrastructure and computing paradigm. Blockchain technology has successfully solved a series of problems such as serious centralization and information opacity in the financial field and achieved good optimization results.

At a time when traditional finance is being impacted by the new model of emerging Internet financial applications characterized by lightweight and online services, in the entire financial market, how to reasonably apply existing information and new technologies, fully grasp the role of blockchain technology in finance, study the status quo and trends in this field, realize the structural adjustment of financial institutions, and optimize products and services for the financial industry has far-reaching significance for the development and growth of the financial industry. However, CiteSpace has few restrictions on the problem to be solved, so its application range is wide. In recent years, scholars have used CiteSpace to solve problems in the financial field, but there is little overall research on blockchain technology in the financial field. Therefore, this paper uses CiteSpace to analyze the research status and trends of blockchain

technology in the financial field to solve problems in the financial field, which has both theoretical and practical significance.

The innovations of this paper: (1) the theoretical knowledge of blockchain technology is introduced, and how blockchain technology plays a role in the financial field is analyzed using blockchain technology and CiteSpace. (2) The overall grasp of the research status and development trend of blockchain technology in the financial field is carried out. Through CiteSpace analysis, it is found that the research on blockchain technology in the financial field at home and abroad is on the rise in recent years. The research keywords mainly focus on "supply chain finance."

2. Related Work

With the continuous development of network technology, more and more people have studied the blockchain. Sikorski et al. explored the application of blockchain technology in relation to the Fourth Industrial Revolution (Industry 4.0); they showed an example of using blockchain to facilitate machine-to-machine (M2M) interaction and established an M2M electricity market in China. While this technology has significant understudied potential to support and enhance the efficiency gains of the revolution and to identify areas for future research, no research has been done on cryptocurrencies [1]. With this, Ittay explored how blockchain research beyond Bitcoin could bridge the gap from transaction throughput to security primitives and privacy and some of the challenges that remained. Although it provided a reference for the development of cryptocurrencies, there was insufficient research on the regulatory field of blockchain [2]. Based on this, Yeoh examined the key regulatory challenges affecting blockchain of the European Union (EU) and the United States, and innovative distributed technologies. Although this research expands financial inclusion in the financial field, research on privacy aspects of user information has not been carried out [3]. Therefore, Engelhardt described specific examples of the application of blockchain technology in the health sector and expanded the application of blockchain technology in this field but did not solve the problem of blockchain application in digital asset transfer [4]. Eze P identified the problems of existing attempts to implement an all-inclusive smart contract platform and proposed a new framework. Although this framework answered some of the ongoing questions about the current implementation of smart contracts involving blockchain, there was no in-depth study on the philosophy of blockchain technology and the issue of blockchain ontology [5]. With scholars' in-depth research, blockchain technology continues to develop, but new problems also appear.

CiteSpace can be used to analyze the research status and trend of blockchain technology in the financial field because of its advantages in data analysis. Yi et al. quantitatively studied the knowledge structure, development, and evolution of social commerce using CiteSpace to systematically review the current state of the social commerce literature [6]. Ming uses the Scientometric software CiteSpace to visually analyze the English test in China from 1995 to 2020 by drawing a map of keyword co-occurrence, time zone, author cooperation network, and scientific research institution cooperation network [7]. Chen et al. used the information visualization analysis software CiteSpace to analyze institutions, authors, cited references, and keywords [8]. However, although these studies have applied CiteSpace to different degrees and angles, the disadvantage is that there is no overall grasp of the research on the application of blockchain technology in the financial field, and there is no application of blockchain technology in the financial field.

3. Current Situation and Trend Method of Blockchain Technology in the Financial Field

3.1. Blockchain-Related Technical Methods

3.1.1. Blockchain Structure. A blockchain is a chain consisting of one block after another. Each block stores a certain amount of information, and they are connected into a chain according to the time sequence of their generation. This chain is kept in all servers, and as long as one server in the entire system can work, the entire block chain is secure.

The top-level block structure of the blockchain is a structure designed to be tamper proof, and its structure is shown in the following formula:

$$(H(C_{n-1}), H(C_n), X_d). \tag{1}$$

$H\ (Ci-1)$ is the hash value of the previous block, $H\ (Ci)$ is the hash value of the block, and X_d is the information in the block. Each block has a hash value pointing to the previous block, so if the block information on the blockchain changes, the hash value of the new block is modified, and all subsequent blocks are modified. This structurally guarantees the immutability of the blockchain. In various interlocking systems, the information recorded can be called a general ledger. The Merkle trusted tree is generated to solve the authentication problem in multiple one-time signatures. The Merkle trusted tree structure has the advantage of a large number of authentications for one signature and has significant advantages in authentication. The bottom layer of the blockchain uses Merkle tree to store transaction data for fast calculation, fast rollback, lightweight nodes, and other operations. When performing P2P transmission, RLP is used to serialize, encode, and decode the block data [9]. In terms of data structure, the blockchain is a chain structure that is linked by hashes to protect the recorded content. The blockchain can be regarded as a state transition system in general, and its state change form can be formally described by the formula as follows:

$$\begin{cases} \delta_{t+1} = \eta(\delta_t, X_t), \\ C = (X_0, X_1, \ldots, X_n), \\ \delta_{t+1} = \eta(\ldots \eta(\eta(\delta_0, X_0), X_1)\ldots). \end{cases} \tag{2}$$

Among them, blockchain B is the sum of the confirmed records of T_i within a period of time, and δ_{t+1} represents all

the information of the confirmed records in the blockchain network. After adding a new block C, it needs to perform a state transition with the previous δ_t to finally confirm δ_{t+1}. η is called the state transition function, which converts δ_t to δ_{t+1}. The consensus mechanism on the blockchain can ensure the consistency of data information between servers. Common consensus mechanisms include Pow, PBFT, Raft, and so on. The so-called "consensus mechanism" is to complete the verification and confirmation of transactions in a short period of time through the voting of special nodes. For a transaction, if several nodes with unrelated interests can reach a consensus, it can be considered that the entire network can also reach a consensus on this. Smart contracts ensure the operation logic on the blockchain. Smart contracts are not a concept unique to blockchain [10]. The essence of a smart contract is a set of distributed computer programs that perform a series of operations according to predetermined events. Once the smart contract is deployed on the blockchain, it is difficult to change the smart contract, but it is generally possible to "change in disguise" by upgrading or terminating the smart contract [11]. A smart contract is a computer protocol designed to inform, verify, or execute a contract. Smart contracts allow for trusted transactions without third parties that are traceable and irreversible. Generally speaking, smart contract development is carried out after the blockchain development is basically perfected. Using smart contracts allows nodes on the blockchain to do things in a unified way. The nodes on the blockchain only need to determine the content of the agreement with each other, and the smart contract can run effectively. With the further improvement of blockchain and smart contracts, smart contracts can gradually handle complex system logic such as transaction settlement, resource allocation, and privacy protection. Some key processes that required human and material costs in the past can rely on smart contracts to reduce the investment of human and material resources, improve efficiency, and reduce costs [12].

According to the application scenarios and the historical development of the blockchain, there are about three types of blockchains as shown in Table 1.

3.1.2. Blockchain Architecture. The starting point of the blockchain is to maintain trust between participants that do not trust each other through the blockchain to establish virtual currency. There are three stages in the development of blockchain. In the blockchain 1.0 virtual currency stage, a large number of virtual currencies represented by Bitcoin entered the capital market. In the stage of blockchain 2.0 intelligent architecture, intelligent architecture appears on the blockchain, and many decentralized applications are applied to the market. A sign of maturity is building a distributed platform. With the continuous deepening of future blockchain technology and applications, blockchain is the trust stage of blockchain 3.0, such as the Internet of Things, big data, cloud computing, and so on. Each blockchain development stage has its architecture changed [13]. For example, in the blockchain 1.0 virtual currency stage, there are basically no concepts such as smart contracts and DAPPs. It also means that general virtual currencies do not have a Turing-complete language. In the blockchain trust stage of blockchain 3.0, the general technical architecture of blockchain has not been fully formed. The technical architecture of the current blockchain is basically in the blockchain 2.0 smart contract period, and specific types of blockchains will also have a partial impact on the technical architecture of the blockchain, which can be generally represented by Figure 1.

3.1.3. Supply Chain Finance Relying on Blockchain. Supply chain finance based on block chain is developing rapidly. The following steps are generally carried out to complete the accounts receivable mode: small- and medium-sized enterprises generate accounts receivable after trade with core enterprises. Small- and medium-sized enterprises apply for financing to the blockchain supply chain finance platform by means of documents and upload the transaction history information to the chain. Core enterprises will trade information, credit upstream and downstream small- and medium-sized enterprises supplier list chain. After the bank makes a loan, the loan information will be on the chain. Small- and medium-sized enterprises will send goods to core enterprises, i.e., goods information chain. After the core enterprise pays the payment information, the payment information will be linked. Small- and medium-sized enterprises repay to financial institutions and link up the repayment information [14]. Supply chain finance relying on blockchain is shown in Figure 2.

As shown in Figure 2, an enterprise user indirectly interacts with blockchain nodes through the integration of supply chain financial platform logic, financing application, financing credential confirmation, and other operations. The essence is that each enterprise integrates information on the blockchain. After relying on the blockchain, it can be seen that many things have become transparent in the whole process. In blockchain supply chain finance, members of various institutions jointly maintain the transaction information of data books on multiple chains. It not only greatly helps financial institutions to strengthen the review of the specific flow and use of funds but also core enterprises to improve corporate security and reduce corporate financial risks. More importantly, due to the decentralization of the blockchain, it can balance the disparity between SMEs and core enterprises in the supply chain and reduce the financing cost of SMEs [15].

3.1.4. Coinjoin. Blockchain privacy protection is to solve the problem of account privacy leakage caused by public transaction information. Currently, it is mainly achieved by directly or indirectly hiding key user information. Typical privacy protection technologies include CoinJoin, Stealth Address, Ring Signature, and zkSNARKs. Coinjoin is a widely used privacy-preserving technology on the blockchain. The completely public transaction information on the blockchain will leak the privacy of transaction information. More precisely, even if the attacker intercepts the company's

Table 1: Three mainstream types of blockchain.

	Public chain	Alliance chain	Private chain
Degree of centralization	Decentralization	Weak centralization	Strong centralization
Participant	Everyone can enter	Members of the alliance	Chain owner
Consensus mechanism	Pow et al.	PBFT etc.	Raft et al.
Openness	Public	Semipublic	Private
Typical scene	Cryptocurrency	Supply chain finance, banking	Database management, auditing.
Representative project	Bitcoin	Hyperledger fabric	No

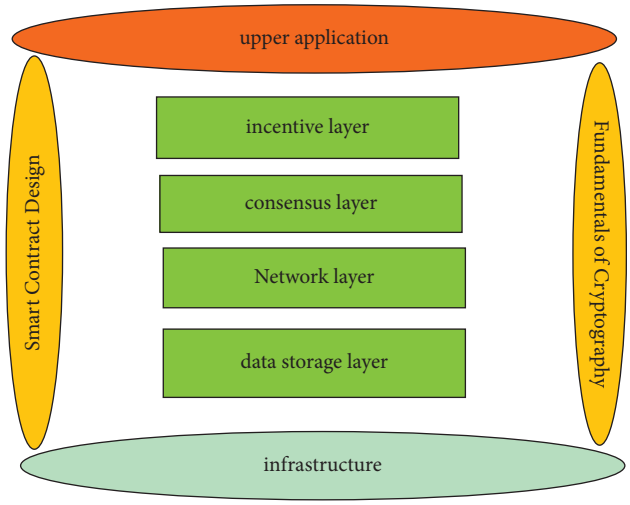

Figure 1: Blockchain technology architecture.

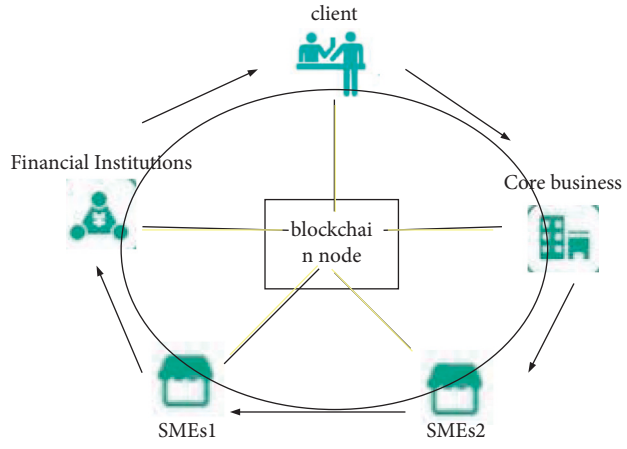

Figure 2: Supply chain finance relying on blockchain.

private information, the attacker cannot determine who sent it and to whom it is sent. This technique makes it impossible for the attacker to obtain the complete information of the transaction, thus protecting the privacy of the transaction [16]. Its main idea can be expressed by the formula:

$$G_N(t_1, G_A(T_0, n), A) \longrightarrow G_A(T_0, n), A. \quad (3)$$

Among them, X_0 and n are the messages that the sender wants to send to the receiver. $G_A(x)$ represents the encryption using the public key of the receiver. A represents the address of the receiver, t_1 represents the verification message generated after using the signature, and $G_N(x)$ is the process in which the so-called intermediary uses its public key N to encrypt.

If it is a message sent from the sender to the middleman, the sender encrypts X_0 and n with the recipient's public key, and after wrapping t_1, $G_A(X_0, n)$ together, $G_N(x)$ processes the wrapped data packet to encrypt. After receiving the information, the intermediary uses the secret key to decrypt the information to obtain t_1, $G_A(X_0, n)$, A. The intermediary cannot decrypt $G_A(X_0, n)$ without the recipient's private key, so the signature information will be sent to the recipient after t_1 verification. The recipient decrypts with his own private key to complete the Coinjoin process. The relationship between the receiver, the middleman, the sender, and the attacker can be intuitively explained with Figure 3.

3.2. Cryptography-Related Methods. Blockchain is a new technology based on cryptography.

3.2.1. Hash Function. Hash function is also called hashing function. A hash function refers to a function that maps the key value of an element in the hash table to the storage location of the element. Its definition is shown in the following formula:

$$H: \{0,1\}^* \longrightarrow Q | h = H(w). \quad (4)$$

When the hash function is used for signature, its properties are shown in Table 2:

When the hash function is used for signature, its characteristic points are mainly compressed mappability, many-to-one mapping, irreversible in calculation, avalanche effect, weak anticollision ability, strong impact resistance, and evenly distributed mapping. There are many implementation methods in the general implementation of hash functions, but many hash functions have the following basic structure. The basic structure of the hash function is shown in Figure 4.

In Figure 4, R is the input string, SC_i is the output string, f is the compression algorithm, y_m is the intermediate input grouping variable, and SC is the intermediate output string. After entering the hash function, the input string is divided into $y_1, y_2, \ldots, y_n$ input grouping variables. When the length of the input string is not enough, random padding is performed. One is the input grouping variable, and the other is the value of SC_{i-1} after the last f-function. Initially, $SC_o = R$ will be set. Its basic structure expression is shown in the following formulas:

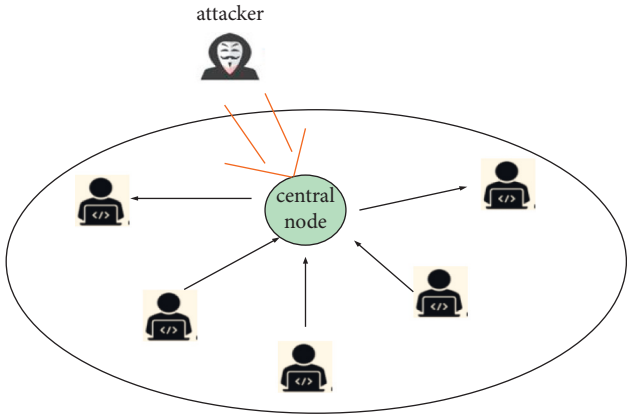

Figure 3: Process diagram of coinjoin.

Table 2: Hash function properties.

Serial number	Feature
1	Compression mappability
2	Many-to-one mapping
3	Computationally irreversible
4	Avalanche effect
5	Weak collision resistance
6	Strong impact resistance
7	Mapping is evenly distributed

$$SC_x = f\left(SC_{x-1}, y_{x-1}\right); \quad 1 \le x \le i, \tag{5}$$

$$h(w) = SC_i. \tag{6}$$

Now commonly used password hash functions are as follows: MD5, SHA, RIPEMD, and so on. Hash function has become an essential tool for digital signature, file verification, password management, and many other information security aspects [17].

3.2.2. Symmetric Cryptography and Public-Private Key System. The encryption and decryption stages of the symmetric cryptosystem are shown in the following formulas:

$$M' = E(z, f), \tag{7}$$

$$M = D\left(z', f\right). \tag{8}$$

The encryption process is a process in which the message z performs a certain encryption operation E through the encryption function f to generate M'. The decryption process is a process in which the encrypted ciphertext z' performs a certain decryption operation D through the encryption function f to generate M. Commonly used symmetric encryption algorithms include DES (insecure), AES, ChaCha20, and so on. Public–private key cryptosystems are also called asymmetric cryptosystems. Compared with the symmetric key system, the public–private key system is more difficult to understand. In a public key encryption system, the encryption key is different from the decryption key, and

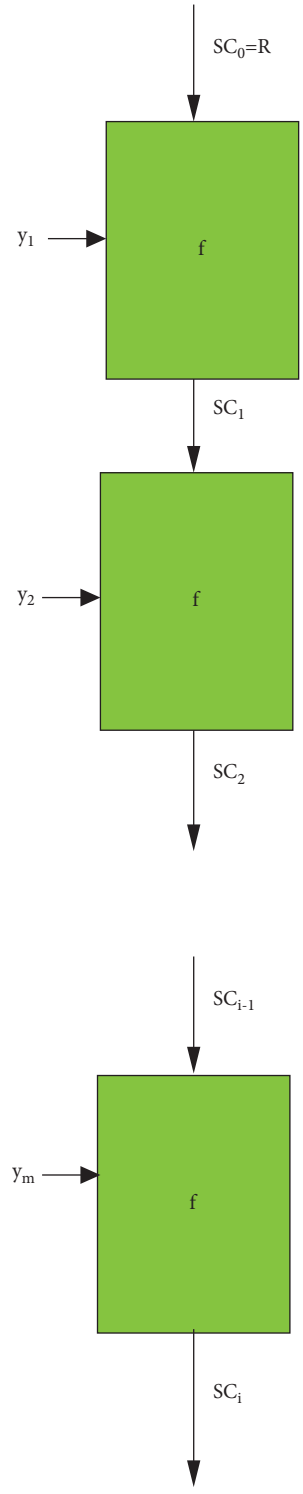

Figure 4: Hash function basic structure.

the public key refers to the public key that anyone can obtain and use. The top secret key is not disclosed to the public, and only the encryptor can know it. The private key cannot be inferred from the public key [18]. Under the public–private key cryptosystem, $Jk_g(M)$ is generally used to represent the process of encrypting J with the public key g; $Jk_s(M)$ is used to represent the process of decrypting M with the private key s.

Taking the widely used RSA public and private key cryptographic mechanism as an example, the security of RSA is based on a basic difficult problem in number theory: the product of two large prime numbers is easy to obtain, but the factorization of the product of two large prime numbers is extremely difficult. The specific description of RSA key generation is as follows:

Y and U are the two prime numbers selected, and the product $c = Y * U$ and $\text{ø}(c) = (Y-1) * (U-1)$ is calculated. Any integer z is chosen so that it satisfies $\gcd(z, \text{ø}(c)) = 1$. t is determined so that it satisfies $(tz) \bmod \text{ø}(c) = 1$, that is, $tz = k\text{ø}(c) + 1$, $k \geq 1$ is an arbitrary integer. Public integers c and z are used as public keys, and t will be secretly stored as the private key.

The RSA encryption algorithm is shown in the following formula:

$$\begin{aligned} S &= E(z) \\ &= z^z \bmod c. \end{aligned} \tag{9}$$

The RSA decryption algorithm is shown in formula:

$$\begin{aligned} M &= D(S) \\ &= S^t \bmod c. \end{aligned} \tag{10}$$

For RSA, the strength of the secret increases with the length of the key. Generally used RSA keys require at least 1024 bits. However, the longer the key, the more time the encryption and decryption algorithms need. The main comparison between the symmetric key system and the public–private key system is shown in Table 3.

Symmetric cryptosystem and public–private key cryptosystem are the basic concepts in cryptography. Symmetric ciphers are relative to public–private key ciphers. In today's cryptographic techniques or schemes, symmetric cryptography and public–private key cryptosystems have their own advantages and disadvantages, so often in the same cryptographic technique or scheme, symmetric cryptography, and public–private key will appear in the same cryptographic technique or scheme at the same time [19].

3.2.3. ECC Elliptic Curve Cryptography Mechanism. Elliptic curve cryptography (ECC) is a public key cryptography technique based on elliptic curve theory that allows for faster, smaller, and more efficient key creation. ECC uses the properties of elliptic curve equations to generate keys rather than use the traditional method of using the product of large prime numbers to generate keys. In some difficult problems, the discrete logarithm problem on elliptic curves is often used. Compared to RSA, ECC requires only a shorter key length and takes less time for encryption and decryption operations [20]. Overall, ECC can be an order of magnitude faster than RSA.

According to the Riemman-Roch theorem, any curve in the plane can be represented by the Weierstrass equation (a cubic equation). On the finite field Yt modulo T, the elliptic curve is the plane determined by the equation $i^2 + a_1 io + a_3 o = i^3 + a^2 i^2 + a_4 i + a_6$, and the commonly used simplified Weierstrass equation such as formula (11) can be obtained by coordinate simplification:

$$\left\{a, b \in Y_t : o^2 \equiv i^3 + ai + b \,(\bmod t) \,\&\, 4a^3 + 27b^2 \neq 0 \,(\bmod t)\right\} \cup \{W\}, \tag{11}$$

where W represents the point at infinity, and a and b are two elements on the finite field Y_t. The operation rules of the group can be further constructed at the time of concrete construction. Generally, the following definition method is used to define the addition operation on the elliptic curve. For any $k = (i_1, o_1) \in Y_t$, $j = (i_2, o_2) \in Y_t$, k and j are connected as a straight line $ki + jo + R \equiv 0 \,(\bmod \mathrm{T})$. The definition of the algorithm is shown in the following formula:

$$k + j = \begin{cases} W, & i_1 = i_2 \,\&\, o_1 = -o_2, \\ -R = (i_3, o_3), & \text{other}. \end{cases} \tag{12}$$

The slope λ of the straight line is shown in the following formula:

$$\eta = \begin{cases} \dfrac{o_2 - o_1}{i_2 - i_1} \,(\bmod t), t \neq j, \\ \dfrac{3i_1^2 + a}{2o_1} \,(\bmod t), t \neq j. \end{cases} \tag{13}$$

Therefore, when $i_1 \neq i_2$ and $o_1 \neq -o_2$, as shown in the following formula:

$$\begin{aligned} -R &= (i_3, o_3) \\ &= \left(\left(\eta^2 - i_1 - i_2 \,(\bmod t)\right), \eta(i_1 - i_3) - o_1\right) (\bmod t)). \end{aligned} \tag{14}$$

Further, the following construction rules are given below to construct the elliptic curve additive exchange group $A(Y_t)$: (1) Closure: from the definition of addition, $A(Y_t)$ satisfies the closure. (2) Unit element: $k + W = W + k = k$, the point at infinity is its additive unit element. (3) Inverse element: $\forall k \epsilon A(Y_t)$, $\exists j \epsilon A(Y_t)$ makes $k + j = W$. It can be easily verified that $A(Y_t)$ satisfies the commutative law and the associative law, thus an Abelian group is constructed.

If the order of $k \epsilon Y_t$, k will satisfy the operation of dot product as shown in the following formula:

$$nk = \underbrace{\{k + k + \cdots + k\}}_{n * k} = W, \tag{15}$$

where nk is called a multiple of k. When B is a point on $A(Y_t)$ and the order of B is prime n, then {0B, B, 2B, 3B, . . ., $(n-1)$

Table 3: The main comparison between symmetric key system and public–private key system.

	Symmetric key system	Public–private key system
Principle	Use the same key	Use a different key
Speed	Generally faster	Generally slower
Key management	Difficulty in key management	Simple key management
Key distribution	The key distribution is complex and requires a dedicated or complex communication protocols	Simple key distribution, no dedicated Channels or complex communication protocols
Applicable environment	Encrypted data	Encryption key, digital signature

$B\}$ is obviously a cyclic subgroup, and the base point B is considered as a group generator. is denoted as the order of element k in the group. The definition of the elliptic curve cofactor $\forall k \epsilon A\ (Y_t)$, ord (k) is shown in formula :

$$v = \frac{\#A(Y_t)}{\mathrm{ord}(k)}. \tag{16}$$

$\#A\ (Y_t)$ is the number of elliptic curve points. The cofactor v can be used to judge the pros and cons of elliptic curve cryptography. Generally speaking, the smaller the v is, the larger the order of the base point in the group and the key space are. The problem of computing the magnitude of k in $Q = \mathrm{kG}$ given Q and G is known as the discrete logarithm problem on elliptic curves, which is now generally regarded as a "hard" problem. For security reasons, in general, ECC requires a large p value, and the p value is generally 256 bits or more. Based on this intractable problem, many cryptographic public–private key cryptosystems have made good technical solutions for encryption, decryption, signature, and so on. The SM2 algorithm used in this paper is one of them.

3.3. Use CiteSpace to Visually Analyze the Research Status and Trends of Blockchain Technology in the Financial Field

(1) Literature search strategy

This article uses CiteSpace to visually analyze the research status and trends of blockchain technology in the financial field and search for research on blockchain technology in the financial field until January 1, 2022. The language of the literature is limited to Chinese and English.

(2) Search terms

Searches are carried out using the following keywords in combination with their synonyms: "blockchain technology," "financial field," "supply chain finance," "risk factors," etc.

(3) Literature selection

Read the titles and abstracts of the retrieved articles, read the full text of studies that may meet the selection criteria, cross-check the screening results of the articles, and resolve inconsistencies through group discussions.

(4) Inclusion standard as shown in Table 4.

(5) Exclusion standard as shown in Table 5.

The screening process is as follows: first, total the number of searched items, then delete duplicates, then read the title and abstract of the remaining literature and delete irrelevant studies. Then, after reading the rest of the literature, irrelevant studies were excluded, and finally, the articles included in this study were obtained. The flow chart of literature search and screening is shown in Figure 5.

(6) Coword cluster analysis

Coword cluster analysis is a commonly used literature research method [21]. Coword analysis takes the keywords or subject headings of related documents as the research object, by counting and summarizing the frequency of the co-occurrence of any two keywords in the same document and then constructing keyword cowords based on the frequency between these keywords. Then, clustering or coordinate visualization analysis is carried out according to the coword matrix, and the relationship between keywords is analyzed quantitatively, so as to discuss the hot topic or research structure or hotspot of a certain research field. Coword analysis focuses on the calculation of word frequency and coword frequency. The formulas are as follows:

$$\begin{aligned} Q_w(e_r) &= \sum_{y=1}^{T} U_y(e_r), \\ U_y(e_r) &= \begin{cases} 0, e_r \notin U_y, \\ 1, e_r \notin U_y, \end{cases} \end{aligned} \tag{17}$$

$$\begin{aligned} Q_w(e_i{:}\ e_o) &= \sum_{y=1}^{T} U_y(e_i{:}\ e_o), \\ U_y(e_i{:}\ e_o) &= \begin{cases} 0(e_i{:}\ e_o) \notin U_y, \\ 1(e_i{:}\ e_o) \notin U_y. \end{cases} \end{aligned} \tag{18}$$

Among them, $Q_w\ (e_r)$ represents the statistical accumulation degree of the keyword er of the related topic document data, and w represents the number of documents included in the sample document. When the keyword er belongs to the document U_y, the value of $U_y\ (e_r)$ is 1. Otherwise, the value is 0. Q_w $(e_\mathrm{i}{:}\ e_\mathrm{o})$ represents the relative reference cumulative frequency of a two-dimensional common word pair $(e_\mathrm{i}{:}\ e_\mathrm{o})$. If the keywords kq and kr both belong to the

Table 4: Literature inclusion standard.

Serial number	Standard
1	The research object is a system based on blockchain technology
2	Using blockchain technology to upgrade and optimize the traditional financial field
3	Report at least one of the following results: Degree of decentralization, security performance, accuracy, and information transparency
4	The study design type is a performance study or a system comparison study.

Table 5: Literature exclusion standard.

Serial number	Standard
1	Nonfinancial research
2	Studies with duplicate publications or overlapping data
3	Test reports, meeting summaries, letters and comments
4	Studies not available in full text

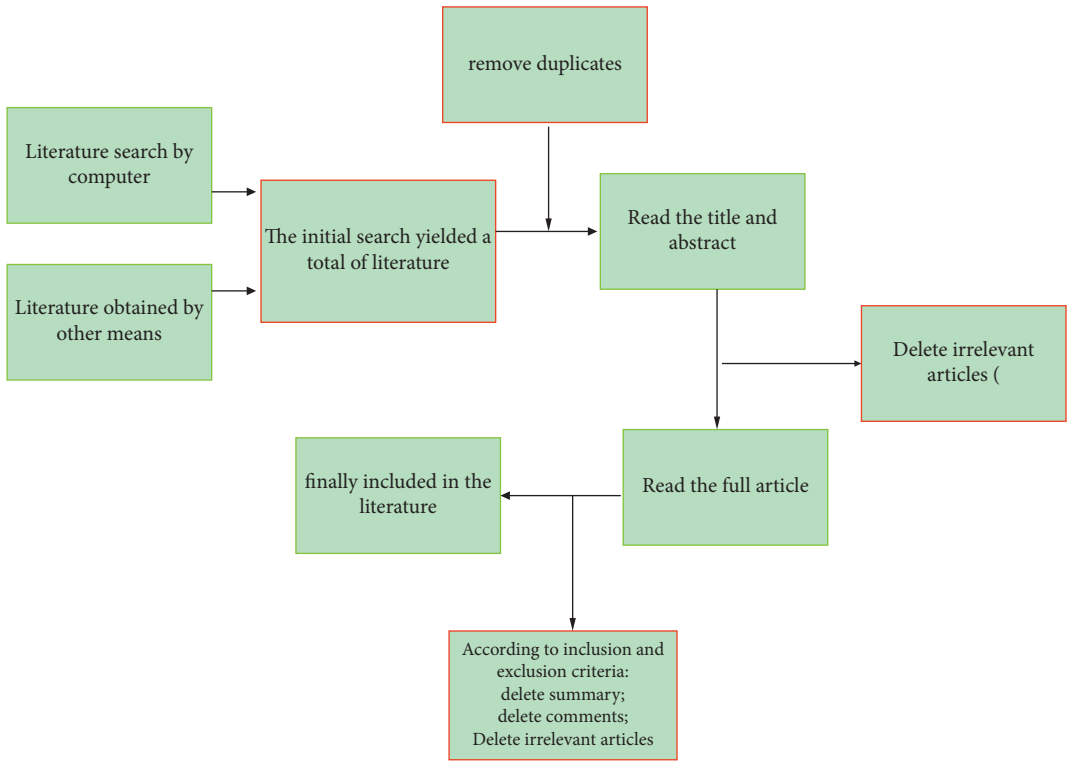

Figure 5: Flowchart of literature search and screening.

document PJ, the binary word pair takes the value 1, otherwise it is 0.

(7) Multidimensional scaling analysis

Two-dimensional Euclidean space distance calculation is to use vector coordinates to represent points. The coordinates of the keyword G_1 are represented by $G_1 = (a_1, a_2)$, the coordinates of the keyword G_2 are represented by $G_2 = (b_1, b_2)$, and the Euclidean distance between G_1 and G_2 is represented by the following formula:

$$S = \text{sqrt}\left((a_{1\_} b_1)^2 + (a_2 - b_2)^2 \right). \tag{19}$$

The formula for calculating the three-dimensional Euclidean space distance is shown in the following formula:

$$S = \text{sqrt}\left((a_1 - a_2)^2 + (b_1 - b_2)^2 (c_1 - c_2)^2 \right). \tag{20}$$

Extended to the x-dimensional space, the Euclidean distance calculation formula is as follows:

$$S = \text{sqrt}\left(\sum (a_{i1} - a_{i2})^2 \right), \quad i = 1, 2, \ldots, x. \tag{21}$$

S is the Euclidean distance in the x-dimensional space.

4. Experiments and Analysis of the Research Status and Trends of Blockchain Technology in the Financial Field Based on CiteSpace Knowledge Graph Visualization

4.1. Results of Literature Screening on Blockchain Technology in the Financial Field. A total of 864 Chinese documents were obtained in this search, 733 English documents were obtained, and all of which were between 2010 and 2020. The sources of the documents were journals, and the search theme was "blockchain finance," which were retrieved in CNKI and web of science, respectively. According to the statistics of CNKI and Web of Science, the annual changes of literature related to blockchain financing from 2010 to 2020 are shown in Figure 6.

As can be seen from Figure 6, during the past 10 years from 2010 to 2020, the number of blockchain finance research literature at home and abroad generally showed an upward trend, and the trend was obvious, indicating that the research heat of blockchain finance was increasing year by year both at home and abroad. In terms of quantity, since 2012, the number of domestic literature on blockchain finance has been higher than the number of foreign literature in the same year. The difference between the two is 32, and in 2020, it reached a maximum of 68, which further shows that domestic scholars have gradually strengthened their efforts in recent years. Research in this field also shows that compared with foreign scholars, domestic scholars have paid more attention to blockchain finance in recent years [22].

The industry research situation can be better understood through statistical results, and the top 10 journals with the most frequent occurrences are presented in pie chart as shown in Figure 7 for details.

It can be seen from Figure 7 that the distribution of journals of literature included in blockchain finance. It is calculated that the share of the above-mentioned journals in CNKI and Web of Science reaches 33.4% and 19.8%, respectively. It can be seen that the main source journals of CNKI sample documents are logistics technology, accounting for 15%. The main source of foreign sample literature is International journal of production economics, accounting for 30%. From the distribution of journals, the journals published by blockchain finance at home and abroad are all distributed in the fields of finance, economic production, and logistics. Both at home and abroad, the influence of published journals is at the upper middle level, which further indicates that blockchain finance is increasingly becoming an important research direction in the field of finance or blockchain [23].

4.2. Data Processing. Through the use of Mysql statistical screening, there are 2018 English keywords and 2024 Chinese keywords.

In the process of statistics, it was found that the word frequency statistics table of Chinese and English keywords is finally obtained. The word frequency of "supply chain" with the highest foreign word frequency is 78, while the word frequency of "supply chain finance" with the highest Chinese word frequency is 419. There is a certain gap between them. Therefore, in this paper, the frequency of word frequency statistics is normalized, and the zero-average normalization method is adopted, that is, the Z-score normalization method. Z-values are calculated, and normalized Z-values follow a standard normal distribution. The mean is 0 and the standard deviation is 1. Therefore, the larger the Z value, the higher the hotspot of the keyword. After calculation, the standardized Chinese and English keyword word frequency map is obtained, and the top five keywords of each selected word frequency are summarized into a high-frequency keyword map, as shown in Figure 8:

As can be seen from Figure 8, the Chinese keyword high-frequency word supply chain finance has the highest Z value, reaching 28.5; the English keyword high-frequency word supply chain finance has the highest Z value, reaching 21.5. It can be seen that the research hotspot focuses on the research on supply chain finance.

This article collects statistics from the number of domestic and foreign blockchain finance annual literature publications and the number of keywords from 2010 to 2020, and the summary is shown in Figure 9.

From the comparison of the two figures, it can be seen that China's research on blockchain finance shows a steady upward trend both in terms of literature quantity and word frequency quantity, and the trend is obvious, indicating that the publication of blockchain finance literature is stable, and the research in this field is gradually deepening. Foreign research on blockchain finance has fluctuated in terms of the number of publications and the frequency of keywords, but since 2010, the research attention has increased, which also shows that the research topic of blockchain finance has increasingly entered the international academic research field.

4.3. High-Frequency Keyword. This paper makes statistics on the annual frequency of high-frequency keywords in Chinese and English and then understands the annual hot words and development trends as shown in Figure 10:

As can be seen from Figure 10, the annual trend of high-frequency keywords supply chain finance of CNKI is on the rise. The number of articles has risen from 10 articles in 2010 to the highest point of 63 articles in 2018, while the annual trend of high-frequency keywords of web of science has some changes. This year, the research focus has turned to Supply chain, reaching a peak of 13 in 2020. The growth trend of Web of Science high-frequency keywords can be divided into stable, growing, and fluctuating. The stable type includes risk management, risk, financing, and so on. The annual trend of these keywords is stable, which also shows that these keywords are mature and have a certain degree of research attention. Growing types include inventory strategies, financing constraints, and so on. These keywords are emerging topics, and the trend of popularity is rising, which further shows that the subtopics of supply chain finance research are constantly enriched and developed. The volatility type includes supply chain management, supply chain finance, and so on. These keywords have common

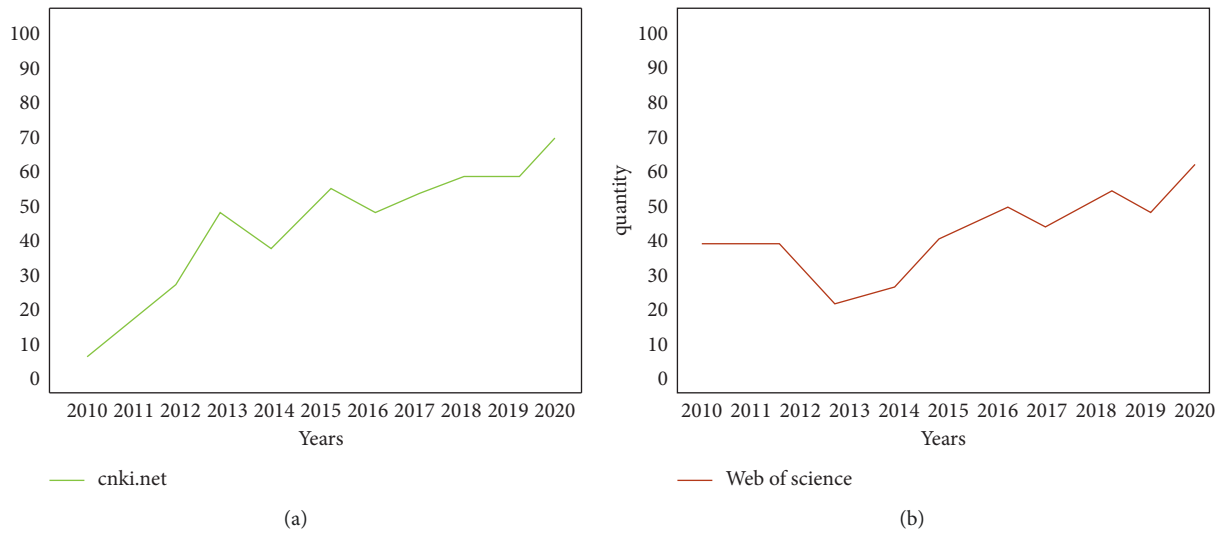

Figure 6: Annual changes in blockchain finance-related literature. (a) Annual changes of relevant documents on CNKI. (b) Annual changes in Web of Science-related literature.

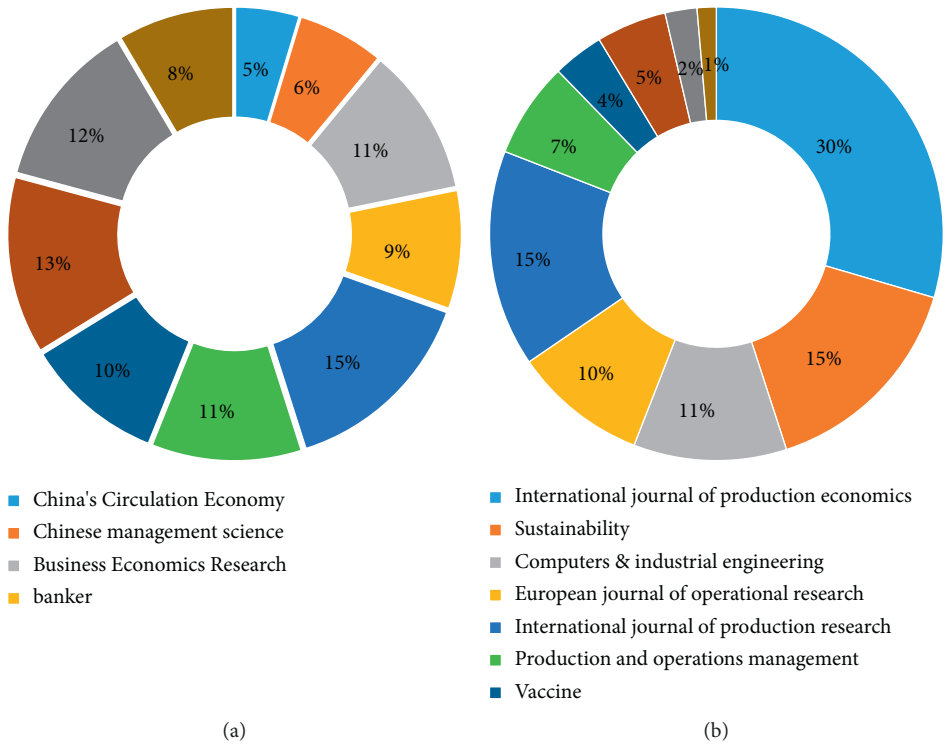

Figure 7: Top source journals for blockchain finance literature. (a) Major source journals of CNKI sample literature. (b) The main source of Web of Science sample literature.

characteristics and all belong to the main disciplines. In the past 10 years, the trend of keywords has a certain volatility, but on the whole, it belongs to the rising trend of volatility.

Through a comprehensive comparative analysis, it can be seen that in the research of blockchain in the financial field at home and abroad, the research in the financial field of blockchain technology at home and abroad is on the rise as a whole, mainly focusing on the keyword "supply chain finance." China's research on this keyword accounted for 59.5%, and foreign research on this keyword accounted for 26.5%, with a difference of 33%. This kind of research that focuses on combining national conditions and starting from the general environment is in line with the needs of relevant problems in the reality of the national economy. There may be some uncertain factors, such as the instability of the retrieval environment and the difference of operators, so that

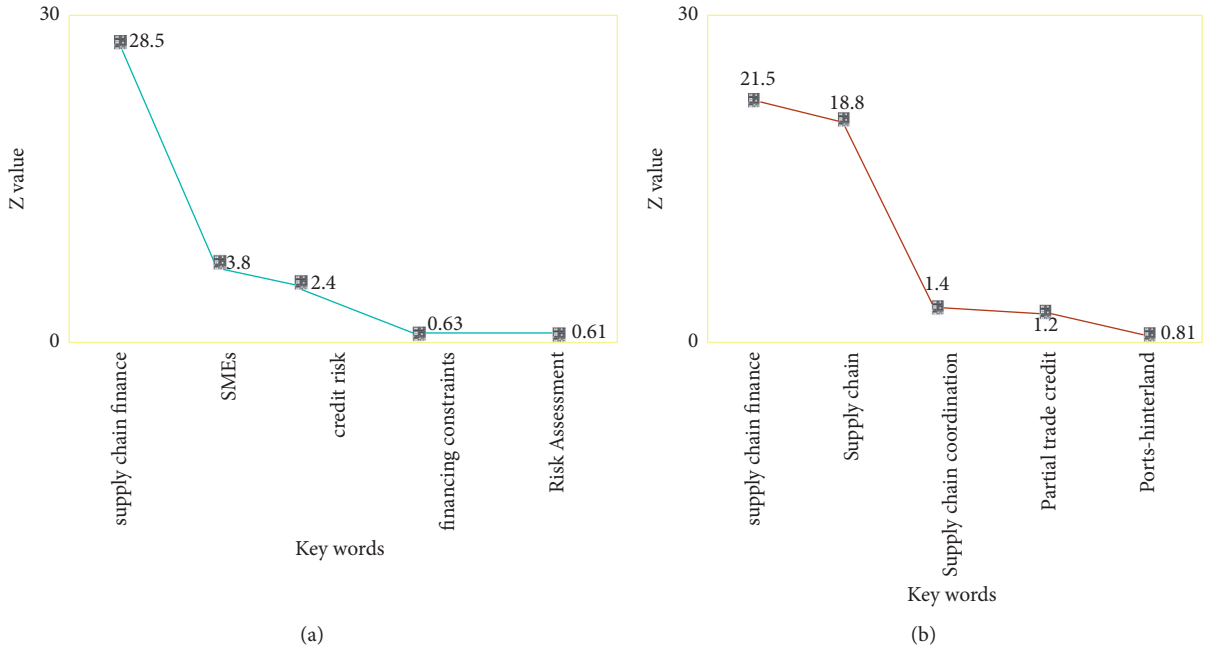

Figure 8: Keyword high-frequency word Z value. (a) Z-value of high-frequency words of Chinese keywords. (b) Z-value of high-frequency words of English keywords.

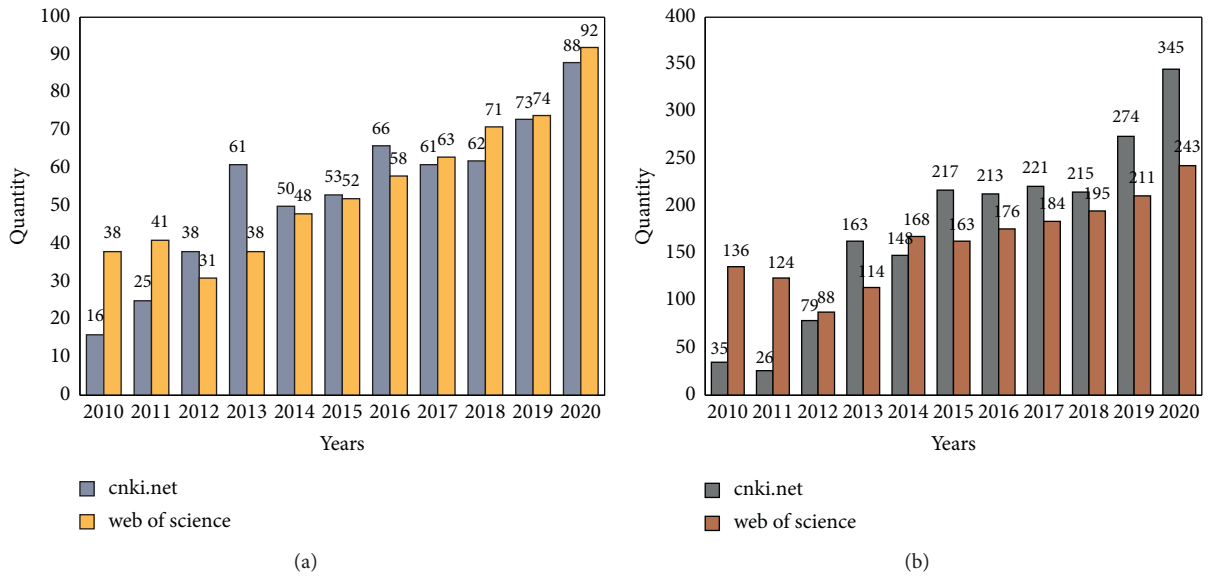

Figure 9: Annual statistics of blockchain finance at home and abroad. (a) Annual statistics on the number of blockchain financial literature at home and abroad. (b)Annual statistics of blockchain financial keywords at home and abroad.

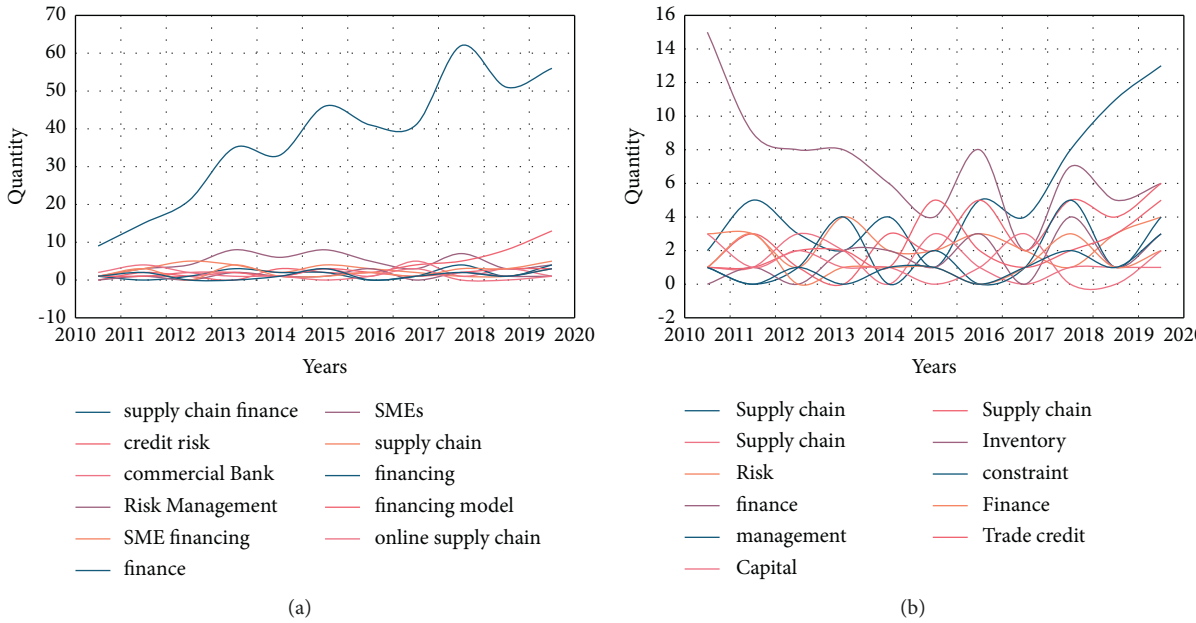

Figure 10: Annual trend of high-frequency keywords. (a) Annual trend of high-frequency keywords in CNKI. (b) Annual trend graph of high-frequency keywords in Web of Science.

the results of this experiment are not completely accurate and reliable, and there are certain differences.

5. Conclusions

With the rise of Internet finance, people have higher and higher requirements for financial services. The development of the financial field cannot be separated from the contribution of the Internet. Due to its technical advantages, blockchain technology has been widely applied in many fields. This article first gives a general introduction to blockchain technology, so that people can understand its functions and principles and then use relevant principle formulas to analyze its function. In the experimental part, this article used CiteSpace to analyze the current research status of blockchain in the financial field, conducted a search and analysis on the development of blockchain technology, and concluded that in the research on blockchain technology at home and abroad in the financial field, the research in the field of blockchain finance at home and abroad is extensive, but the main focus is on the keyword "supply chain finance" showing an overall upward trend. This provided ideas for the development and research of blockchain technology in the financial field in the future, so it is necessary to study the status quo and trend of blockchain technology in the financial field.

Data Availability

No data were used to support this study.

Conflicts of Interest

The author declares that there are no conflicts of interest regarding the publication of this article.

References

[1] J. J. Sikorski, J. Haughton, and M. Kraft, "Blockchain technology in the chemical industry: machine-to-machine electricity market," *Applied Energy*, vol. 195, pp. 234–246, 2017.

[2] E. Ittay, "Blockchain technology: transforming libertarian cryptocurrency dreams to finance and banking realities[J]," *Computer*, vol. 50, no. 9, pp. 38–49, 2017.

[3] P. Yeoh, "Regulatory issues in blockchain technology," *Journal of Financial Regulation and Compliance*, vol. 25, no. 2, pp. 196–208, 2017.

[4] M. A. Engelhardt, "Hitching healthcare to the chain: an introduction to blockchain technology in the healthcare sector," *Technology Innovation Management Review*, vol. 7, no. 10, pp. 22–34, 2017.

[5] P. Eze, T. Eziokwu, and C. Okpara, "A triplicate smart contract model using blockchain technology," *Circulation in Computer Science*, vol. 2017, no. 1, pp. 1–10, 2017.

[6] C. Yi, M. Jian, and Y. Liu, "Knowledge mapping of social commerce research: a visual analysis using CiteSpace[J]," *Electronic Commerce Research*, vol. 18, no. 4, pp. 837–868, 2018.

[7] N. Ming, "Characteristics and trends of English testing research in China: visual analysis based on CiteSpace," *Region - Educational Research and Reviews*, vol. 3, no. 3, p. 1, 2021.

[8] Y. Chen, X. Y. Zeng, F. W. Yang, and F. Sun, "Visual analysis of knowledge map of network Meta-analysis in traditional Chinese medicine based on CiteSpace," *Zhongguo Zhong yao za zhi = Zhongguo zhongyao zazhi = China journal of Chinese materia medica*, vol. 45, no. 18, pp. 4500–4509, 2020.

[9] F. Adoma, "Big data, machine learning and the BlockChain technology: an overview," *International Journal of Computer Application*, vol. 180, no. 28, pp. 1–4, 2018.

[10] C. L. Rinaudo, S. Lee, and K. Hali, "How securitization can benefit from blockchain technology," *Journal of Structured Finance*, vol. 23, no. 2, pp. 51–54, 2017.

[11] C. Koch and G. C. Pieters, "Blockchain technology disrupting traditional records systems," *Economic Review*, vol. 6, no. 2, pp. 1–3, 2017.
[12] V. Raju, "Economic dimensions of blockchain technology: in the context of extention of cryptocurrencies," *International Journal of Psychosocial Rehabilitation*, vol. 24, no. 2, pp. 29–39, 2020.
[13] E. Hemalatha, "Monitoring and securing the healthcare data harnessing IOT and blockchain technology[J]," *Turkish Journal of Computer and Mathematics Education (TURCOMAT)*, vol. 12, no. 2, pp. 2554–2561, 2021.
[14] I. A. Kurniawan, D. Yusman, and I. O. Aprilia, "Utilization of blockchain technology revolution in electronic ID card data integrity," *Aptisi Transactions on Management (ATM)*, vol. 5, no. 2, pp. 137–142, 2021.
[15] R. Vikaliana, Z. Raja, M. Rasi, N. Pujawan, and R. Sham, "The application of blockchain technology in agribusiness supply chain management in Indonesia[J]," *Solid State Technology*, vol. 63, no. 6, pp. 16522–16533, 2021.
[16] M. Surjandy, H. Leslie, H. Spits, and E. Abdurachman, "The recent trend of organization development influenced by blockchain technology[j]," *ICIC Express Letters*, vol. 15, no. 4, pp. 389–396, 2021.
[17] Y. Tribis, A. E. Bouchti, and H. Bouayad, "Blockchain technology-based supply chain: state-of-the-art and future prospects[J]," *International Journal of Innovative Technology and Exploring Engineering*, vol. 10, no. 3, pp. 125–136, 2021.
[18] X. Guo, M. A. Khalid, I. Domingos et al., "Smartphone-based DNA diagnostics for malaria detection using deep learning for local decision support and blockchain technology for security," *Nature Electronics*, vol. 4, no. 8, pp. 615–624, 2021.
[19] A. Pal, C. K. Tiwari, and A. Behl, "Blockchain technology in financial services: a comprehensive review of the literature," *Journal of Global Operations and Strategic Sourcing*, vol. 14, no. 1, pp. 61–80, 2021.
[20] D. Vervoort, "Re: Part 2: blockchain technology in health care," *ANZ Journal of Surgery*, vol. 91, no. 4, p. 763, 2021.
[21] D. Ahmad, N. Lutfiani, A. D. A. Rizki Ahmad, U. Rahardja, and Q. Aini, "Blockchain technology immutability framework design in E-government," *Jurnal Administrasi Publik Public Administration Journal*, vol. 11, no. 1, pp. 32–41, 2021.
[22] B. Sokolov and A. Kolosov, "Blockchain technology as a platform for integrating corporate systems," *Automatic Control and Computer Sciences*, vol. 55, no. 3, pp. 234–242, 2021.
[23] P. Wang and S. Qiao, "Emerging applications of blockchain technology on a virtual platform for English teaching and learning," *Wireless Communications and Mobile Computing*, vol. 2020, no. 2, 10 pages, Article ID 6623466, 2020.