Hindawi
Mobile Information Systems
Volume 2022, Article ID 1356480, 10 pages
https://doi.org/10.1155/2022/1356480

Research Article

Financial Risk Evaluation of Digital Currency Based on CART Algorithm Blockchain

Aping Zhao

Nanchang Jiaotong Institute, Nanchang 330010, China

Correspondence should be addressed to Aping Zhao; 05033@ncjti.edu.cn

Received 13 April 2022; Accepted 13 June 2022; Published 28 June 2022

Academic Editor: Yajuan Tang

In recent years, digital currencies based on blockchain technology have brought about a boom in the research of encrypted digital currencies with the design concept of peer-to-peer trading and decentralization, but due to the lack of supervision and obvious speculative characteristics of the digital currency market, the sharp fluctuations in the market can easily trigger investor sentiment fluctuations, which in turn will lead to social instability and even financial system risks. In this paper, through the analysis of the financial risk source factors of blockchain digital currency, the evaluation index is established, the risk evaluation index system is constructed, and then the CART classification algorithm is used to analyze it and evaluate and test the model. The characteristic factor structure obtained by the CART algorithm in this paper better explains the financial risk characteristics of blockchain digital currency and gives relatively reliable identification results. The results show that the CART decision tree classification method is effective and has a high accuracy rate, which classifies the financial risks of blockchain digital currency, and the method has excellent adaptability and matchability for the classification of risk problems.

1. Introduction

Blockchain digital currency (hereinafter referred to as "digital currency") refers to a digital representation issued by a nonstate (central bank), based on a distributed ledger or blockchain technology, and representing a certain value or contractual right, including payment tokens, utility tokens, and stable coins. With the continuous development of the digital economy, the application scenarios and scope of digital currency will gradually expand, and the impact on the economy, finance, and society will also increase. Digital currencies originate from the Internet, and development also depends on the Internet, which makes the various risks and hazards in the digital currency and financial system more contagious and amplified [1]. At the same time, the technical complexity and transaction privacy of digital currencies also make it more difficult to identify and assess various risks in digital currencies and have serious unpredictability.

Wang explores the current situation of digital currency and its impact on the existing financial system and reflects on the existing defects and development measures of digital currency [2]. Scott and Loihio consider digital currencies from a traditional asset pricing perspective, putting aside the risk of seller fraud or currency theft, assessing the volatility and systemic risk of Bitcoin's price [3]. In this paper, Xie and Shi analyze the risks and ICO phenomena of nonsovereign digital currencies and also analyze the main reasons for the regulatory problems caused by digital currencies, which lie in the decentralized "peer-to-peer" distributed architecture of public chain technology [4]. Yu-Dong and Chu proposed to balance technological innovation and technological risks, improve relevant laws and regulations and regulatory systems, and improve the digital currency legal system [5]. From the perspective of the digital economy, strengthen the research and development of digital technologies, build the application scenarios of legal digital currencies, and promote the sharing of legal digital currencies. On the basis of sorting out the regulatory measures and legal digital currency issuance mechanism of the United Kingdom, the United States, the European Union, and other economies on digital currency, Liu further explored the legal digital currency issuance mechanism and the corresponding risk prevention

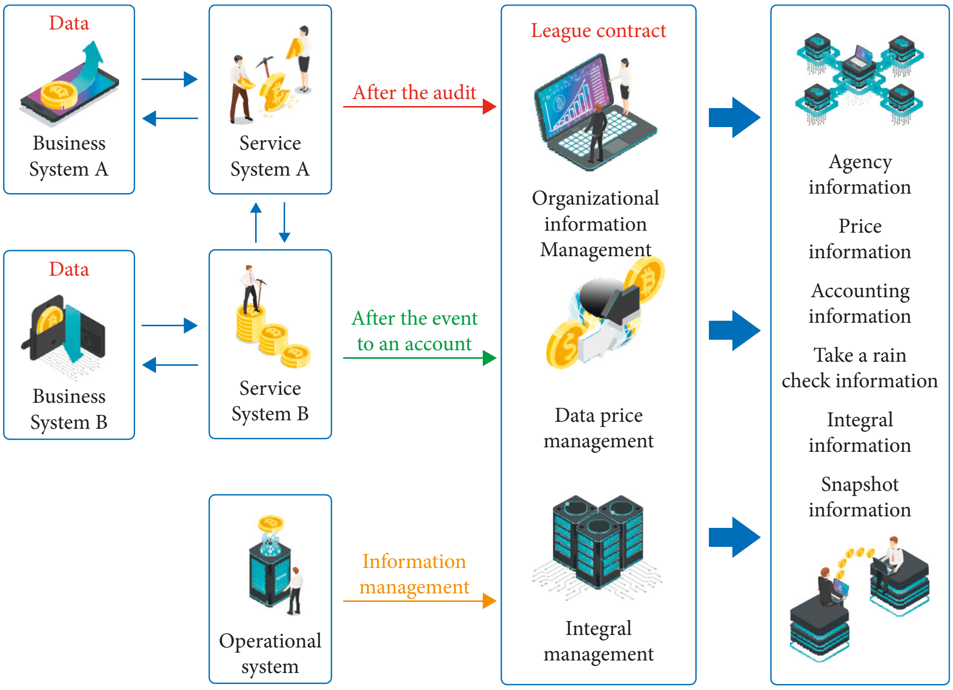

Figure 1: Application practice of blockchain in digital currency financial risk data sharing.

mechanism, elaborated on the regulatory deficiencies in the issuance of legal digital currency, lagged technological development, and increased pressure on antimoney laundering supervision, and put forward corresponding suggestions and preventive measures [6]. Therefore, it is of great practical significance that this paper analyzes the financial risk factors according to the technical characteristics of the blockchain digital currency based on the CART algorithm and proposes corresponding preventive measures according to the risk. Figure 1 shows the application practice of blockchain in digital currency financial risk data sharing.

2. CART Decision Tree Models and Algorithms

2.1. Introduction to CART Decision Tree Generation Algorithm. CART (ASSIFICATION AND REGRESSION TREES, CART) is an algorithm invented in 1970 by the United States by four statisticians to analyze the shortcomings of various statistical analysis methods at that time, proposed a new statistical analysis method that can not only contain the advantages of these statistical analysis methods but also overcome their defects classification and regression tree, until 1984 CART's theoretical model research is basically perfect [7].

CART models can handle highly skewed or polymorphic numeric data, as well as sequential or unordered generic data. The CART algorithm uses a technique of fractional recursive segmentation, which always divides the current sample set into two subsets, so that each nonleaf node of the generated decision tree has two branches. Therefore, the decision tree generated by the CART algorithm is a binary tree with a concise structure. The CART algorithm cart form *n* tree (T) is described as follows: (where, T represents the current sample set, and the current candidate property set is represented by T_attribute list), as shown Figure 2, the process step of the cart algorithm.

(1) Create root node N;

(2) Assign categories to N;

(3) If Tall belongs to the simple category or there is only one sample left in r, the IN is returned as a leaf node and assigned a category to it;

(4) For each attribute in the T attribute list, perform a division on that attribute and calculate the Gini coefficient for the secondary division;

(5) N's test attribute test. attribute = T attribute list with the smallest Gini coefficient;

(6) Divide T into two subsets of T and T;

(7) Call cart form tree ($T1$);

(8) Call cart form tree ($T2$).

The CART algorithm calculates the Gini coefficient for the division of each sample set, and the smaller the Gini coefficient, the more reasonable the division. For the sample set T, $\text{Gini}(T) = 1 - \sum_{j=1}^{n} p_j^2$, where is the probability that T contains the class J. If T is divided into two subset sums, the Gini coefficient for this division is as follows:

$$\text{Ginisplit}(T) = \frac{S_1}{S}\text{Gini}(T_1) + \frac{S_2}{S}\text{Gini}(T_2). \qquad (1)$$

2.1.1. Feature Selection Process

(1) Classification Tree. The classification tree uses the Gini index to select the optimal feature and, at the same time, determines the optimal binary segmentation point of the feature.

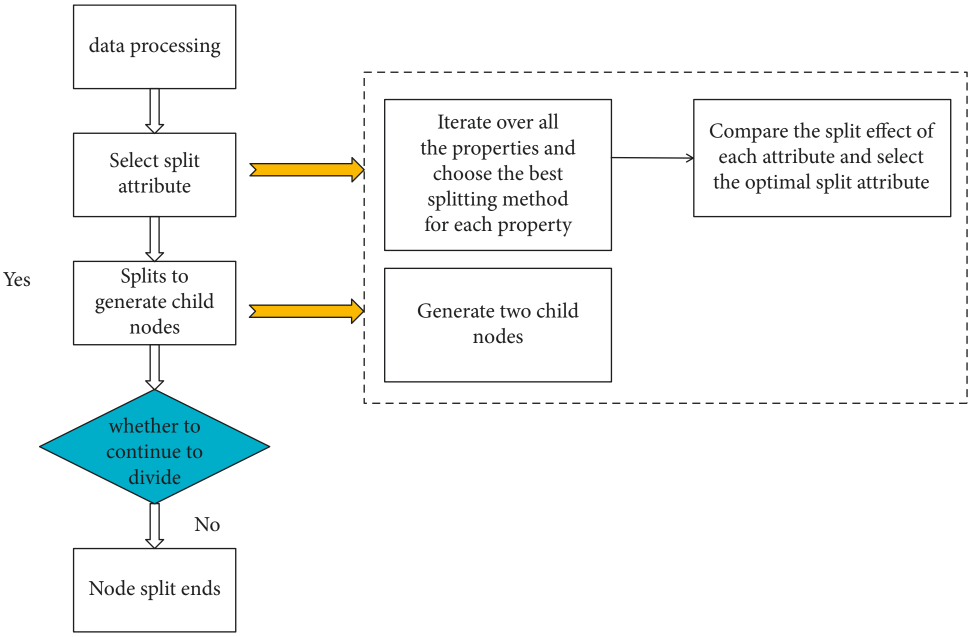
data processing
Select split attribute
Yes
Splits to generate child nodes
whether to continue to divide
No
Node split ends
Iterate over all the properties and choose the best splitting method for each property
Compare the split effect of each attribute and select the optimal split attribute
Generate two child nodes

Figure 2: Cart algorithm flowchart.

[Definition: Gini index] In the classification problem, assuming that there are K classes and the probability pk of the sample point belonging to the kth class, the Gini index of the probability distribution is defined as follows:

$$\mathrm{Gini}(p) = \sum_{k=1}^{k} p_k (1 - p_k) = 1 - \sum_{k=1}^{k} p_k^2. \qquad (2)$$

For the binary classification problem, if the probability that the sample point belongs to the first class is p, then the Gini index of the probability distribution is follows:

$$\mathrm{Gini}(p) = 2p(1 - p). \qquad (3)$$

For a given sample set D, its Gini index is: (C_k is the subset of samples in D that belong to the kth class, and K is the number of classes.)

$$\mathrm{Gini}(D)1 - \sum_{k=1}^{k} \left(\frac{|C_k|}{d} \right)^2. \qquad (4)$$

[Feature selection process] If the sample set D is divided into two parts $D1$ and $D2$ according to whether the feature A takes a certain possible value a, namely:

$$D_1 = \{(x, y) \in D | A(x) = a\} D_2 = D - D_1, \qquad (5)$$

The Gini index Gini(D) represents the uncertainty of set D, and the Gini index Gini(D, A) represents the uncertainty of set D after dividing by $A = a$. The larger the Gini index, the greater the uncertainty of the sample set.

2.1.2. Regression Tree.

2.1.2. Regression Tree. Suppose X and Y are input and output variables, respectively, and Y is a continuous variable, given a training dataset $D = \{(x_1, y_1), (x_2, y_2), \ldots, (x_N, y_N)\}$.

A regression tree corresponds to a partition of the input space (ie, the feature space) and the output values on the partitioned units. Assuming that the input space has been divided into M units $R_1, R_2, \ldots, R_M$, and each unit Rm has a fixed output value cm, then the regression tree model can be expressed as follows:

$$f(x) = \sum_{m=1}^{M} c_m I(x \in R_m). \qquad (6)$$

When the partition of the input space is determined, the optimal output value on each cell is solved using the criterion with the smallest squared error, which is as follows:

$$c_m = \mathit{average}(y_i | x_i \in R_m). \qquad (7)$$

Using a heuristic method, the input space is divided. Select the jth variable $x(j)$ and its value s as the cut variable and cut point, and define two regions:

$$\begin{aligned} R_1(j, s) &= \{x | x^{(j)} \le s\}, \\ R_2(j, s) &= \{x | x^{(j)} > s\}. \end{aligned} \qquad (8)$$

The optimal cut-off point s can be found for the fixed input variable j.

$$\begin{aligned} c_1 &= \mathit{average}(y_i | x_i \in R_1(j, s)), \\ c_2 &= \mathit{average}(y_i | x_i \in R_2(j, s)). \end{aligned} \qquad (9)$$

Traverse all input variables to find the optimal segmentation variable j, forming a pair (j, s). This divides the input space into two regions. That is, a feature selection process is completed.

2.2. Pruning Algorithm. The training of the CART decision tree model relies entirely on sample data, so the CART tree will fit perfectly from the training samples. If test data are put into a trained model, a higher error rate may occur, a situation known as overfitting. Therefore, the complex CART tree needs to be cut down, that is, some nodes are deleted, and the process is pruning [8].

There are two main types of pruning methods: front pruning and postpruning. Prepruning is performed during the decision tree split, and the method participates in the decision tree generation process, so too many nodes are generated. However, since it is not easy to accurately determine the end point of tree growth, the practicality is not very good. The postpruning method is currently used more methods, this method is to replace those node subtrees with leaf nodes that are not highly confident, and the most frequent class in the child node tree is marked as the class label of the leaf node. There are two types of postpruning methods, one of which is a growth set of pruning sets consisting of training set data, and the other algorithm of decision tree production and pruning is performed in the same data set. Common postpruning methods are CCP (cost complexity pruning), REP (reduced error pruning), PEP (pessimistic error pruning), and MEP (minimum error pruning) [9].

CCP is the most used pruning algorithm in CART classification regression trees. The two steps of CCP are (1) starting from T_0, that is, the most primitive tree, to produce some leaf tree sequences $\{T_0, T_1, \ldots, T_n\}$. In it, from the generation, T_i is generated by T_{i+1}, T_n is the root node. (2) The optimal decision tree is selected from the subtree sequence generated in the previous step, based on the true error estimate.

3. Blockchain Digital Currency Risk Evaluation Index Construction

3.1. Principles of Risk Indicator Construction

3.1.1. Principle of Purposefulness. In the Big Data environment, the data dimension is often wide, and the amount of data is large, so data selection and data cleaning become a complex project. How to build an effective indicator system lies in the determination of the characteristics of the research target. If the indicator chosen is vaguely correlated with the target being studied and the definition is unclear, the presence of too much of this type of data will only affect the speed of the operation.

3.1.2. Systematic Principles. The construction of the indicator system is not based on the more indicators, the more appropriate, in actual operation, often pay more attention to the relevance, constraint, and comprehensiveness of each indicator. If the target outcome can be predicted more systematically and accurately with fewer indicators, such an indicator system can often enhance the implementation efficiency of the research project model.

3.1.3. Principles of Feasibility. Feasibility mainly considers the applicability of indicators from two aspects:

① Whether indicators are easily available. If the index logic structure of the research target is good, but the indicator data are not easy to obtain, or the acquisition cost is high (capital cost and time cost), it is necessary to analyze the pros and cons to re-plan the project period and adjust the benefit expectations achieved by the project. The feasibility of data acquisition is the cornerstone of the project, so the actual situation must be fully taken into account when setting up the project.

② Whether the indicator representation can meet the actual analysis needs. Some indicators can be interpreted in qualitative analysis, but in quantitative analysis, there may be functions that cannot be adapted to operations or quantitative discussions. Therefore, when encountering such problems, try to change the form of this type of indicator to meet the quantitative operation, if you cannot do it, you can only delete similar indicators.

3.1.4. Scientific Principles. In empirical research, the selection of indicators needs to be supported by scientific theories. If the findings are not supported by scientific theories, this phenomenon may be only a phased, unsustainable incidental manifestation. Therefore, if the amount of data is not large enough, there is no data performance supported by scientific theories, it will not have typical performance, and the construction of this model needs to be continuously improved and tracked.

3.1.5. Principle of Comparability. The selection of indicators should be universal to solve problems in the project field, so as to ensure that the established indicator system is universal and can reflect the effectiveness of the evaluation indicators.

3.2. Analysis of Financial Risk Source Factors of Blockchain Digital Currency. Financial innovation contains risks, and the current digital currency system has caused various social problems and risks due to its technical characteristics. In the two decades since the advent and adoption of digital currencies, the types of risks have varied [10]. From the perspective of major historical events, there are such as the use of digital currency features for extortion, drug trading, gambling, money laundering, and tax evasion, and then such as the threat of policy regulation to its legal status and the impact of trading platforms on the digital currency security system. This paper discusses the risk of digital currency as a financial asset, refers to the classification of bank financial risk and discusses the financial risk of digital currency according to market risk, credit risk, liquidity risk, operational risk, and legal compliance risk.

3.2.1. Market Risk. Price risk is the main risk of digital currency, digital currency price fluctuations are large, investors face greater market risk, due to changes in macroeconomic variables such as interest rates caused by the price decline of digital currency investors suffer losses.

3.2.2. Credit Risk. On one hand, in the digital currency system, the issuance standard of currency is based on national credit, and the reputation of digital currency represents the credibility of the country. Owing to the particularity of the existence form, the anticounterfeiting technology of digital currency and the encryption measures of the banking system must be extremely strict and confidential, and once leaked, it will cause huge financial, economic, and even social disasters [11].

On the other hand, the public's holding of digital currency is based on cards, account numbers and even identities, and with the corresponding passwords, fingerprints, and other payment methods, if misappropriation occurs, it will not only cause harm to personal economic interests, but also lead to a systematic monetary credit crisis. Therefore, we need to strictly control risks with powerful technical means.

3.2.3. Liquidity Risk. Liquidity risk refers to the sharp price fluctuations caused by supply restrictions and trading volume changes of digital currencies, which make the market unable to operate effectively. On one hand, the digital currency system does not have the characteristics of a legal tender mechanism, and the total amount of digital currencies such as Bitcoin is almost rigid supply, which is easy to cause liquidity crunch. On the other hand, although the digital currency adopts the "$T+0$" trading model, the turnover rate is lower than that of the stock market in the same period, and the liquidity of the digital currency is seriously insufficient compared with the stock market. Most countries and regions cannot directly buy digital currency through legal tender, exchange legal tender for some platform currency such as TETC and Bitcoin, or purchase other digital currencies through platform currency, which makes it more difficult to manage digital currency liquidity. If there is a problem with the liquidity management of the exchanger, the holder cannot convert the digital currency into legal tender. Note that the digital currency system does not bear the public institution of last resort lender, and once a risk event occurs, the exchanger is vulnerable to a run, and the consumer or investor faces direct economic losses [12].

3.2.4. Operational Risks. Operational risk, also known as technical risk, refers to the difficulties that digital currency cannot foresee and solve due to the limitation of the existing level of technology. Technical risks stem from two aspects: the blockchain system and the currency trading platform. Digital currency is closely related to blockchain technology, and the blockchain itself has two technical risks: one is the internal risk of the blockchain's own technical defects, such as some unknown vulnerabilities, the system cannot be centrally closed and upgraded, the difficulty of repairing security loopholes, once 51% of the computing power is mastered, the blockchain data can be rewritten; the second is the external risk of blockchain applications brought about by the rapid development of quantum computing and artificial intelligence, such as the collapse of the consensus mechanism and the failure of the incentive mechanism.

3.2.5. Legal Compliance Risks. Legal compliance risk refers to the use of digital currency by some organizations or individuals to circumvent existing regulations or obtain certain benefits through noncompliant behavior. First, the crime of money laundering: The anonymity and ease of cross-border payments of digital currencies facilitate cross-border money laundering and terrorist criminal activities if poorly regulated. The second is illegal financing and the third is data breache. With the popularity of smart devices, individuals have become the carrier of data information; digital currency suppliers collect users' personal information or transaction data for specific business purposes, and over-centralized data face the risk of intrusion and leakage; however, the legal and regulatory mechanisms in many countries are not clear in this regard.

3.3. Indicator Construction

3.3.1. Indicator Selection. Through the analysis of the financial risk source factors of blockchain digital currency, it can be seen that the technical characteristics of digital currency have led to the diversity of risk sources, and the overall impact level of various risks is also different. On the basis of the analysis of its source factors, the following indicator system was established using the Delphi method and inviting a number of experienced experts to guide. There are five categories of first-level indicators: market risk, credit risk, liquidity risk, operational risk, and legal compliance risk; the first-level indicators are subdivided below the second-level indicators, as shown in Table 1, and the values of the secondary indicators are shown in Table 2:

4. CART Algorithm Modeling and Result Analysis

4.1. CART Tree Model and Result Analysis. The data in this article are from the Cathay Pacific CSMAR and Wind databases, and a total of 200 blockchain digital currency financial risk-related information cross-section data information fields were collected. The decision tree model is then built using SPSS Clementine 12.0, as shown in Figure 3. According to the aforementioned 10 characteristic factors, 70% of the sampling data are used as the training number, and 30% of the sampling data are imported into SPSS Clementine12 as the test data.

According to the analysis results of the CART tree, it can be seen that the proportion of high risk in the root node is 27.4%, and then the first layer of the model is split according to the interest rate of macroeconomic conditions, the split point is whether the interest rate is greater than 0.586, in the 76 pieces of data less than 0.586, 44.4% is high risk, and the second to fifth layers of the model are analyzed according to the split point. From the perspective of the entire decision tree model, the first financial risk of blockchain digital currency is reflected in the price market, price risk is the main risk of digital currency, digital currency price fluctuations are large, investors face greater market risk, due to changes in macroeconomic variables such as interest rates,

Table 1: Risk indicator construction.

Indicator order	Risk indicator category	Select the metric content	
Credit risk	The completeness of the trading platform products	The trading platform reserves traffic	
Market risk	Interest rate		
Technical and operational risks	Consensus mechanism security	Ability to fix security vulnerabilities in the trading platform	Operational prescriptiveness
Liquidity risk	The amount of money supply	Number of trading platforms	
Legal compliance risks	Contract standardization	Processing accuracy	

Table 2: Indicator variable names and values.

Indicator variables	Value
The completeness of the trading platform products	High; low
The trading plat form reserves traffic	High; low
Interest rate	Continuous numeric value
Consensus mechanism security	Yes; no
Ability to fix security vulnerabilities in the trading platform	High; low
Operational prescriptiveness	Yes; no
Number of trading platforms	Continuous numeric value
The amount of money supply	Continuous numeric value
Contract standardization	Yes; no
Processing accuracy	Yes; no

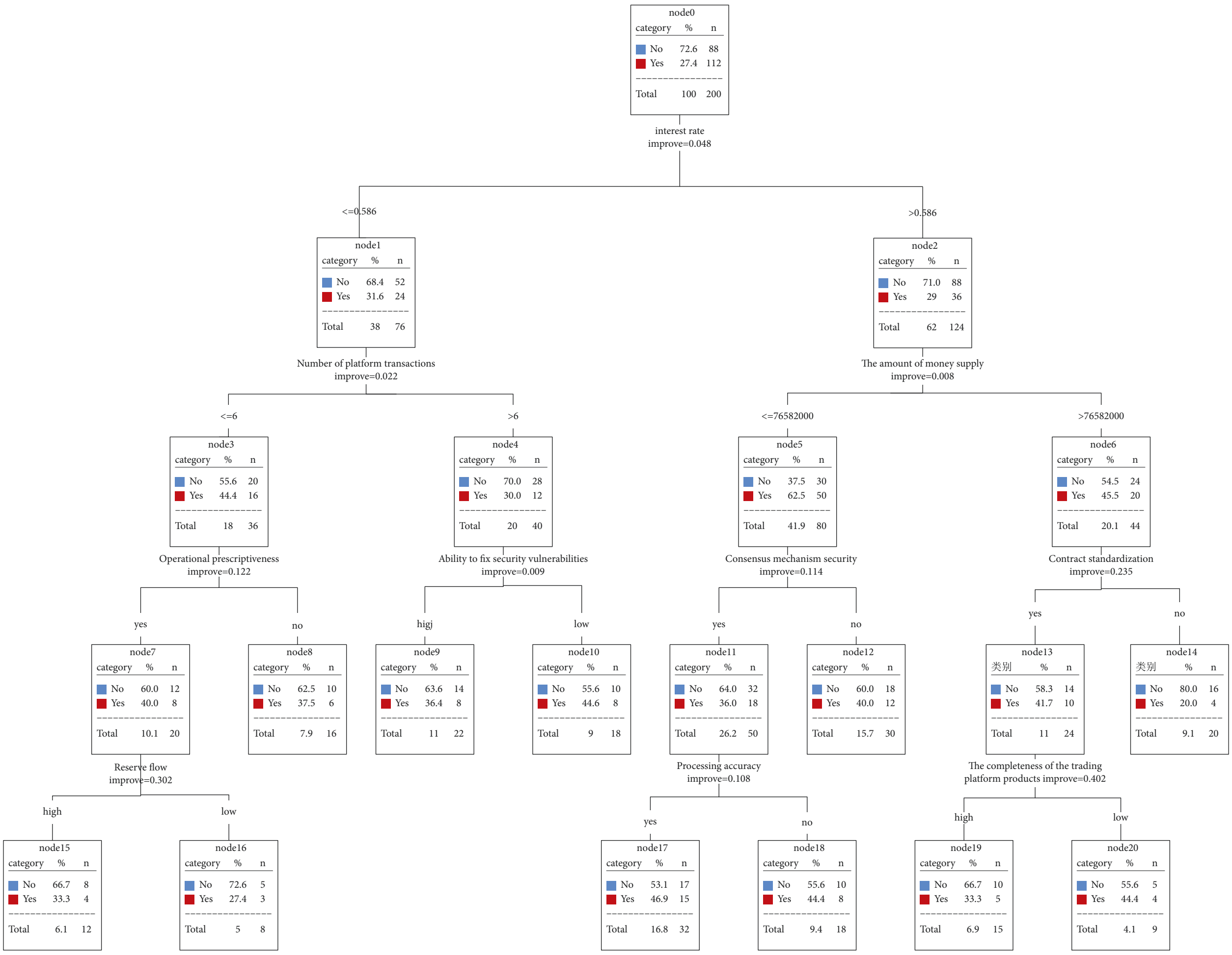

Figure 3: Blockchain digital currency financial risk decision tree.

Table 3: Confusion matrix.

Actual results	Predict the outcome	
	Positive example	Counter example
Positive example	TP (true-positive example)	FP (false-counter example)
Counter example	FP (false-positive example)	YN (true-counter example)

the price of digital currency falls so that investors suffer losses. The second is the amount of money supply and the volume of digital currency trading platforms, digital currencies due to supply restrictions and trading volume changes caused by sharp price fluctuations, making the market unable to operate effectively [13]. The third is technology and operation, mainly stemming from the two aspects of the blockchain system and the currency trading platform. Digital currency is closely related to blockchain technology, and the blockchain itself has two technical risks: one is the internal risk of the blockchain's own technical defects, such as some unknown vulnerabilities, the system cannot be centrally closed and upgraded, the difficulty of repairing security loopholes, once 51% of the computing power is mastered, the blockchain data can be rewritten; the second is the external risk of blockchain applications brought about by the rapid development of quantum computing and artificial intelligence, such as the collapse of the consensus mechanism and the failure of the incentive mechanism [14]. The aforementioned layers of indicators reflect the current situation of blockchain digital currency, exposing its risk points. From the aforementioned decision tree model, it can be seen that the amount of computation is relatively not large, not only can it handle continuous and categorical fields, but also the decision tree can clearly show which fields are more important.

4.2. Model Evaluation. From the theory of classification methods, it is known that when evaluating the performance of various classification models, the accuracy rate is one of the indicators for evaluating the prediction effect [15]. On this basis, the probability of classifying confusion matrices was introduced, as shown in Table 3.

Based on the listed confusion matrices, the FPR and TPR indicator values can be derived, which are calculated as follows:

$$\mathrm{FPR} = \frac{\mathrm{FP}}{(\mathrm{FP} + \mathrm{FN})}, \tag{10}$$

$$\mathrm{TPR} = \frac{\mathrm{TP}}{(\mathrm{TP} + \mathrm{FN})}. \tag{11}$$

As shown in formula (1), the case of a negative sample in the sample but judged to be a positive sample is represented by the indicator FPR, that is, the risk classification is wrong due to a prediction error. In general, the higher the value of FPR, the higher the rate of error judgment generated by the model, and it is easy to obtain undesirable prediction results. As shown in equation (2), the TPR indicates that the proportion Table 4 of the original positive sample that happens to be judged to be a positive sample, and when the TPR value increases, the prediction accuracy is rising. When evaluating the effectiveness of classifiers, the aforementioned indicators can effectively reflect the correct classification. After pruning the decision tree, the classification results listed in the following table are obtained, as shown in Tables 4 and 5.

Table 4: Training set confusion matrix.

Confusion matrix		Forecast			Total	Accuracy rate (%)	Error rate (%)
		I	II	III			
Actual	I	30	7	0	37	81.08	18.02
	II	8	49	8	65	75.38	24.62
	III	0	9	29	38	76.32	23.68
Total					140	79.51	20.49

Table 5: Test set confusion matrix.

Confusion matrix		Forecast			Total	Accuracy rate (%)	Error rate (%)
		I	II	III			
Actual	I	14	4	4	22	63.63	36.36
	II	4	15	2	65	71.42	28.57
	III	0	2	15	17	88.24	11.76
Total					60	73.33	26.66

Based on the data results obtained from the actual operation of the decision tree model, the study finally lists the confusion matrices for training and testing different sets [16]. Comparing the actual results of the two, the correct rate of model training is generally better, and the numerical results can reach the ideal level. The accuracy rate of the training samples reached 79.51%, and the accuracy rate of the test samples reached 73.33%, which can effectively classify the risk situation. Through the analysis of the obtained data results, it can be seen that the difference in classification accuracy between the two types of samples is small, and the false-positive rate of decision trees is low. In summary, by constructing a confusion matrix, it is possible to see the specific classification of the model.

5. Risk Prevention and Control Countermeasures Suggestions

5.1. Operational Risk Management. Third-party network security technology companies have a close business relationship with digital currency platforms and digital financial operators and should optimize transaction and production business processes in many links [17]. At the management level, the operational ability of the network security module is the most important to the degree of risk impact. Third-party network security technology enterprises should operate prudently in each process of their business and strictly implement management in accordance with the unified standards of relevant departments and carry out management supervision to prevent the risk of loss caused by the mistakes of regulatory personnel [18].

As far as operational risks in digital finance are concerned, there are differences between risks under different business models and business process risks. At present, multiple digital financial models have emerged in the market, which vary by region and platform business. On the basis of multimodel, the standardized management method is used to update the standardized process of the digital finance industry. Based on the decision tree method, the digital financial risk comprehensive evaluation model is studied, and the multimode digital financial business is standardized, gridded, and dynamically monitored, and the risk is effectively intervened [19].

First of all, contract management and audit in the business process need to be further improved to consolidate the foundation for business development. At present, the third network security technology company is a regulatory agency, and its scope of responsibility is only supervision and protection, and it lacks the responsibility of relevant legal entities. Based on such circumstances, in the signing of a contract treaty, the scope of responsibility should be clearly defined in the contract to ensure the standardized management of the digital financial industry. Under these conditions, after optimizing the normative nature of documents, the review and supervision of document contracts is further strengthened. In the management of business personnel, strict training is adopted for the personnel involved in the work, the scope of work of the personnel is clarified, and the obligations and responsibilities of the workers are clarified. After the aforementioned improvement, the dynamic monitoring of business processes is added to the business links, so that the probability of risks brought about in management operations is reduced.

5.2. Policy and Legal Risk Management. Digital finance is the product of the birth of the information age, and the prevention and management of digital financial risks, from a global perspective, has neither experience nor reference. With the close combination of blockchain technology and digital finance, digital finance is entering the "blockchain +" era, and blockchain continues to penetrate in banking, securities, insurance, and other fields [20].

While blockchain brings great opportunities to digital finance, it also generates a series of legal issues. The first is the contradiction between the "decentralized" nature of blockchain and the current application of law and jurisdiction. "Decentralization" is the most important feature of blockchain technology. As the blockchain does not have a specific physical address, there are certain legal loopholes in the application of law and jurisdiction. The second is the contradiction between the "anonymization" characteristics of the blockchain and the real-name system of the current legal network. China's Cybersecurity Law stipulates: Network operators implement a real-name system in their business activities. Owners, managers, and service providers of blockchains should comply with the requirements of the network real-name system. But in fact, blockchain technology has the characteristics of nonreal-name or anonymization, which contradicts the real-name provisions in the current law. The third is the contradiction between the "trustless" nature of blockchain and personal data protection. Blockchain has the characteristics of "de-trusting," the operation rules of the system and related data are completely open and transparent, and there is no need to establish a mutual trust relationship when exchanging data between each node. Although the blockchain also has relevant regulations to protect transaction data, its business activities need to combine the virtual world and the traditional physical world, comply with the rules of entity laws, and disclose relevant data and information, which makes it difficult to truly achieve personal data and information protection.

Therefore, the management of digital financial risks has been continuously explored and practiced, and in this process, it is inevitable that due to the updating of technology and changes in the financial ecology, digital finance will breed risks. For example, in digital finance, criminals will target the blank or gray areas of the law, exploit loopholes, wipe the edges, and use the regulatory gaps to make profits. For the construction of the relevant system of digital financial management and the formulation of the regulatory system, it not only takes time to improve, but also needs to go through multiple links of hearing, review and approval.

5.3. Prescriptive Risk Management. In recent years, virtual currency and blockchain have become hot topics in the industry. Virtual currencies and blockchains have created great wealth for a small number of people but also caused a large number of investors to suffer huge losses in their property. The reason is mainly because the blockchain digital finance industry is not standardized.

On one hand, the blockchain digital finance industry is out of order. At present, although the state has introduced some relevant specifications for blockchain, the blockchain application specifications in the field of digital finance are still not perfect. The capital market "chain speculation" behavior is serious, and individual merchants have maliciously induced and embezzled investors' assets, which has also stained the blockchain industry. Some merchants engage in pyramid schemes under the guise of blockchain and illegally absorb funds. On the other hand, the illegal cost of the blockchain digital finance industry is too low, and the crackdown on it is not enough.

At present, the threshold for blockchain access is low, and some merchants register multiple blockchain companies at one time for personal gain, maliciously arbitrage other people's funds, resulting in industry chaos such as "cutting leeks" and "running away." During the period, although the relevant departments took measures to crack down, due to insufficient punishment and low illegal costs, illegal blockchain companies will use other platforms in disguise to continue to engage in illegal trading activities.

5.4. Risk Monitoring and Management Measures. When working with top logistics companies, digital currency financial services must conduct a detailed investigation of third-party cybersecurity technology companies in the early stage. In order to ensure that they are in the process of supervision and have sufficient risk control capabilities, we need to choose large professional and technical companies with a high level of security management, a high degree of management informatization, a large scale of assets, and a certain solvency, such as Network Security Companies such as Qianxin, Xinxinfu, and Tianrongxin, to ensure that they have a greater advantage in digital financial additional services [21].

In optimizing the enterprise supervision and management mechanism, the third-party network security technology enterprises need to build their own organizational structure according to the development advantages of their own enterprises. In order to standardize the division of responsibilities to the greatest extent, different departments within the organization also need unified supervision and incentive guarantees. Identify and define the responsibilities of supervisors and project managers in various situations. Conduct efficient supervision in the form of supervision rotation to prevent supervisors from colluding with enterprises and adversely affecting the company.

It is necessary to vigorously build an information platform, strengthen the construction of an information collaboration platform for multiparty cooperation among participants, facilitate logistics enterprises to quickly and effectively form regulatory responsibilities and improve regulatory efficiency. At the same time, the information platform can implement a variety of functions, including querying the number and status of financial products at any time, monitoring security vulnerabilities, visual transactions, and so on.

In terms of inquiries, inquiries can be made from the public open windows of banks and financial enterprises. In terms of information, it also optimizes and facilitates communication and sharing among the various participants in the financial business.

6. Conclusion

The study first analyzes and sorts out the categories of the sources of blockchain digital currency financial risk indicators; second, constructs the risk indicator system that is in line with the actual research; and finally selects the digital financial business information data of listed companies in the financial information database. Combined with the multiparty sources and risk categories of blockchain digital currency financial risks, the CART decision tree method in the machine-learning method is used to classify and assess the degree of risk. The results show that the CART decision tree classification method is effective and has a high accuracy to classify the financial risks of blockchain digital currency, and the method has excellent adaptability and matching for the classification of risk problems. The research hotspots on blockchain digital currency are currently mainly concentrated in the research on the impact and role of digital currency, the theoretical basis and operation mechanism, the legal regulation research, the privatization and legalization, the monitoring system and the regulatory countermeasures, and so on, and there is less research on its risk assessment and prediction model, so the combination of Big Data mining technology and risk assessment will be a research direction in the future.

Data Availability

The labeled data set used to support the findings of this study is available from the corresponding author upon request.

Conflicts of Interest

The author declares that there are no conflicts of interest.

Acknowledgments

This study was supported by the Humanities and Social Sciences Research Project of Colleges and Universities in Jiangxi Province. Project name: Research on the impact of RMB exchange rate change on real estate after joining SDR (Grant no. JJ18227).

References

[1] A. Tobias and M. G. Tommaso, “The rise of digital money,” *Annual Review of Financial Economics*, vol. 13, 2021.

[2] Y. Wang, “Explore the Current Situation of Digital Currency and its Impact on the Existing Financial System, and reflect on the Existing Defects and Development Measures of Digital Currency,” 2021, https://www.coursehero.com/file/99414174/Pluto-3-pdf.

[3] G. Scott and LoiHio, “Digital currency risk,” *International Journal of Economics and Finance*, vol. 10, no. 2, 2018.

[4] P. Xie and W. Shi, “Digital Currency: Risk, Regulation and Policy Recommendations,” *New Finance Review*, 2018.

[5] Q. I. Yu-Dong and X. Chu, “Economic Benefits and Risk Prevention of Legal Digital Currency under the Perspective of Digital Economy,” *Reform*.

[6] W. Liu, “Exploration and risk prevention of digital currency issuance mechanism based on international experience,” *Southwest Finance*, no. 11, pp. 51–58, 2017.

[7] S. Yu, W. H. LiXiongfei, C. S. ZhangXiaoli, X. Zhang, and S. Chen, “C_CART: an instance confidence-based decision tree algorithm for classification,” *Intelligent Data Analysis*, vol. 25, no. 4, pp. 929–948, 2021.

[8] L. Chen, Q. Sun, and S. Fang, “Analysis of application trend of digital currency blockchain technology,” *World Scientific Research Journal*, vol. 7, no. 10, 2021.

[9] “Getting the balance right: crypto, stablecoin and central bank digital currency,” *Journal of Payments Strategy & Systems*, vol. 16, no. 1, 2022.

[10] Y. Lin, “Optimization analysis of the regulatory path of China’s legal digital currency,” *Frontiers in Economics and Management*, vol. 3, no. 1, 2022.

[11] M. Bie and Y. Chen, “Malicious mining behavior detection system of encrypted digital currency based on machine learning,” *Mathematical Problems in Engineering*, vol. 2021, pp. 2021–2030, 2021.

[12] M. khalidsalman, A. khalidsalmanMohammed, and I. Abdullahi, “Price prediction of different cryptocurrencies using technical trade indicators and machine learning,” *IOP Conference Series: Materials Science and Engineering*, vol. 928, no. 3, Article ID 032007, 2020.

[13] S. Chan, Z. Y. ChuJeffrey, Y. Zhang, and S. Nadarajah, "Blockchain and cryptocurrencies," *Journal of Risk and Financial Management*, vol. 13, no. 10, p. 227, 2020.

[14] M. H. Shou, X. Zheng, D. D. Li, and Yi. T. Zhou, "Forecasting the price Trends of Digital Currency: A Hybrid Model Integrating the Stochastic index and Grey Markov Chain methods," *Grey Systems Theory and Application*, 2020.

[15] H. LIU, "Prospects and challenges of blockchain technology in digital currency application," *Theory and practice of science and technology*, vol. 1, no. 3, 2020.

[16] O. I. Larina and O. M. Akimov, "Digital money at the present stage: key risks and development direction," *Financial Theory and Practice*, vol. 24, no. 4, pp. 18–30, 2020.

[17] C. Zhu and Z. Fu, "Regulatory issues of digital currencies," *Asian Research Journal of Mathematics*, 2020.

[18] K. Saito and M. Iwamura, "How to make a digital currency on a blockchain stable," *Future Generation Computer Systems*, vol. 100, pp. 58–69, 2019.

[19] V. Rastogi and P. Kushwaha, "Success and failure of digital money and virtual money: case of cryptocurrency-bitcoin," *IME Journal*, vol. 13, no. 1, 2019.

[20] M. A. Naheem, "Exploring the links between AML, digital currencies and blockchain technology," *Journal of Money Laundering Control*, vol. 22, no. 3, pp. 515–526, 2019.

[21] P. Latimer and M. Duffy, "Deconstructing digital currency and its risks: why ASIC must rise to the regulatory challenge," *Federal Law Review*, vol. 47, no. 1, pp. 121–150, 2019.