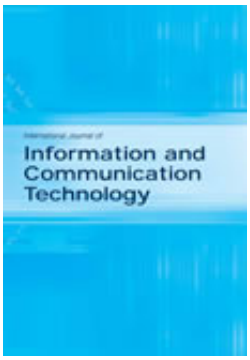
INDERSCIENCE PUBLISHERS
Linking academia, business and industry through research



International Journal of Information and Communication Technology

ISSN online: 1741-8070 - ISSN print: 1466-6642
https://www.inderscience.com/ijict

Risk assessment of e-commerce finance development based on blockchain algorithm in digital economy

Libo Zhao, Hongwei Xu, Wangyuan Xi

Article History:

Received:	27 October 2024
Last revised:	25 November 2024
Accepted:	25 November 2024
Published online:	02 January 2025

Risk assessment of e-commerce finance development based on blockchain algorithm in digital economy

Libo Zhao*, Hongwei Xu and Wangyuan Xi

School of Computer and Mathematics,
Harbin Finance University,
Harbin, 150000, China
Email: zhaolibo_jlu@126.com
Email: 13936090146@163.com
Email: 15545971689@163.com
*Corresponding author

Abstract: With the rapid development of the digital economy, the application of blockchain technology in the field of e-commerce finance is becoming increasingly widespread, but its potential risks are also increasing. This article aims to use blockchain algorithms to conduct risk assessment on the development of e-commerce finance. Firstly, build a smart contract based on Ethereum to monitor abnormal behaviour in real-time during the transaction process; Secondly, utilising the pluggable consensus mechanism of the super ledger, evaluate the efficiency and security of different consensus algorithms in processing transactions, and analyse their impact on compliance risks. The found risk components are quantitatively investigated to build a risk assessment model by using real instances and merging fuzzy comprehensive evaluation approach. The findings of the research show that the suggested approach can support pertinent judgments, clearly identify and measure any hazards in e-commerce finance, and encourage its sustainable development.

Keywords: blockchain; electronic commerce; financial risk.

Reference to this paper should be made as follows: Zhao, L., Xu, H. and Xi, W. (2024) 'Risk assessment of e-commerce finance development based on blockchain algorithm in digital economy', *Int. J. Information and Communication Technology*, Vol. 25, No. 12, pp.16–28.

Biographical notes: Libo Zhao received her Master's degree at Jlin University in 2008. She is currently a Lecturer in Harbin Finance University. Her research interests include blockchain technology.

Hongwei Xu received her Master's degree at Shenyang University of Technology in 2007. She is currently a Lecturer in Harbin Finance University. Her research interests include computer application technology.

Wangyuan Xi received her Master's degree at Harbin University of Commerce in 2009. She is currently a Lecturer in Harbin Finance University. Her research interests include e-commerce and electronic finance.

1 Introduction

As the digital economy develops quickly, e-commerce finance – a crucial component – is changing significantly. With its distributed, transparent, tamper proof properties, blockchain technology has progressively become a major instrument for enhancing the security and efficiency of e-commerce financing. The broad use of blockchain technology, however, also carries possible hazards including technical, compliance, and market risks that can endanger the sustainable growth of e-commerce finance.

Scholars have investigated the use of blockchain technology in related studies somewhat intensively. Zohar (2015) underlined, for instance, the technical dangers presented by code vulnerabilities and unanticipated behaviour even if smart contracts provide great benefits in automating transactions and lowering middleman costs.

Scholars of e-commerce finance have also started to focus on blockchain technology's risk assessment. For instance, Ioannou and Demirel (2022) investigated its possible compliance and technological hazards, examined the use of blockchain in supply chain finance, and suggested related risk management techniques. Furthermore, Kaur et al. (2023) statistically assessed the dangers of blockchain technology in financial services using the fuzzy comprehensive evaluation (FCE) technique, therefore offering theoretical justification for pertinent decisions. Ante (2021) looked examined how smart contracts were applied in financial services, especially with regard to derivatives trading and settlement and how they can lower financial risk. Lewis et al. (2017) discussed how blockchain and smart contracts can be applied in financial market infrastructure, particularly in improving risk management processes and reducing credit and operational risks. Through smart contracts on blockchain networks, Le Quoc et al. (2022) investigated the real-time assessment and management mechanism of credit risk and suggested a credit risk management system based on smart contracts.

Though studies have given blockchain technology in e-commerce finance a theoretical framework, comprehensive assessment of its possible hazards is still lacking. With an eye toward smart contracts and consensus methods based on Ethereum and hyperledger fabric, this paper seeks to employ blockchain algorithms to do risk analyses on the evolution of e-commerce finance. First, this paper will build a smart contract based on Ethereum, which uses on chain data recording and transparency tools to track unusual behaviour during the transaction process in real-time and so uncover technical hazards; Second, assess the security and efficiency of several consensus algorithms (such as Kafka and Raft) in handling transactions by using the pluggable consensus mechanism of the super ledger and investigate their influence on compliance risks.

By applying practical cases and combining FCE method, this article will quantitatively analyse the identified risk factors and construct a risk assessment model. The research results will provide support for relevant decisions in the field of e-commerce finance and promote its sustainable development. Through in-depth exploration of the application of blockchain technology in e-commerce finance, this article hopes to provide theoretical basis for industry practice and indicate direction for future research. The main contribution of this article is to systematically explore the application of blockchain technology in the field of e-commerce finance and its potential risk assessment, which is reflected in the following aspects:

1 Construction of risk assessment framework: This article proposes a risk assessment framework based on blockchain algorithms, which combines smart contracts and consensus mechanisms of Ethereum and hyperledger to systematically identify and quantify technical and compliance risks in e-commerce finance. This framework provides a theoretical foundation and practical guidance for subsequent research.

2 Real-time monitoring mechanism for smart contracts: By constructing a smart contract based on Ethereum, this article achieves real-time monitoring of abnormal behaviour during the transaction process, utilising on chain data recording and transparency features to enhance the ability to identify technical risks. This method provides new ideas for risk management in e-commerce finance.

3 Efficiency and security evaluation of consensus mechanism: This article deeply analyses the pluggable consensus mechanism of the super ledger, evaluates the efficiency and security of different consensus algorithms (such as Kafka and Raft) in transaction processing, and explores their impact on compliance risks. This analysis provides empirical evidence for selecting appropriate consensus mechanisms.

4 Application of FCE method: combining the FCE method, this article quantitatively analyses the identified risk factors and constructs a risk assessment model. The application of this method not only improves the scientificity and accuracy of risk assessment, but also provides data support for relevant decisions.

5 Verification of actual cases: Through the application of actual cases, this article verifies the effectiveness of the proposed risk assessment method and demonstrates the practical potential of blockchain technology in e-commerce finance. This empirical study provides reference for industry practice and promotes the sustainable development of blockchain technology.

In summary, this article not only provides theoretical support for the application of blockchain technology in the field of e-commerce finance, but also offers practical solutions for related risk management practices, which has important academic value and practical significance.

2 Relevant technologies

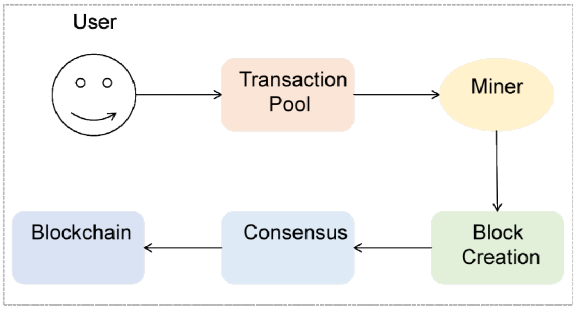
2.1 Ethereum

Ethereum is an open-source blockchain platform designed to support the development of smart contracts and decentralised applications (DApps) (Buterin, 2023; Chen et al., 2020). It is not only a cryptocurrency (Ethereum, ETH), but also an infrastructure on which various applications can be built (Metcalfe, 2020; Wood, 2014). The design of Ethereum allows developers to automatically execute contract terms through smart contracts, thereby reducing the need for intermediaries and improving efficiency and transparency. The workflow of Ethereum is shown in Figure 1.

Ethereum is also a type of blockchain, which is a decentralised and distributed ledger technology. Each blockchain is composed of a chain like structure of blocks. Each block contains transaction information and the hash value of the previous block, ensuring the immutability of the blockchain (Jani, 2017). Smart contract is an automatically executed

protocol written on the Ethereum virtual machine (EVM) and running on a decentralised network (Kushwaha et al., 2022). They automatically perform actions when specific conditions are triggered, based entirely on rules specified by code, without the need for intermediaries. The native token of Ethereum is Ethereum (ETH), which is mainly used to pay transaction fees on the network and incentivise miners. There are two types of Ethereum accounts: externally owned accounts (EOA), which are controlled by users and operated through private keys. Contract account: controlled by smart contract code, the contract account can interact with EOA or other contract accounts.

Figure 1 Ethereum workflow diagram (see online version for colours)



Ethereum initially used the proof of work (PoW) mechanism, similar to Bitcoin, where miners compete to compute complex mathematical problems to package transactions and generate new blocks. The formula for PoW mainly involves hash operations:

$$H(block\_header) \leq target \tag{1}$$

where *block_header* is the hash value of the block header, *target* is a difficulty target value. Miners must find a random number (nonce) that satisfies this condition, so that the hash value of the block header is smaller than the difficulty target. However, Ethereum has currently shifted towards proof of stake mechanism. PoS selects block validators based on the amount of ETH held. The theoretical core of PoS is to obtain block rights by staking ETH. The more ETH staked, the higher the probability of becoming a block validator.

On the Ethereum network, every transaction requires a *Gas Fee*, which is a unit used to measure computing resources. Different operations (such as sending ETH, calling smart contracts, etc.) consume different computing resources and corresponding gas fees.

The equation for calculating transaction costs is:

$$Transaction\ Fee = Gas\ Used \times Gas\ Price \tag{2}$$

where *Gas Used* represents the amount of gas consumed during the execution of the transaction, and *Gas Price* represents the fee (in ETH) that the user is willing to pay per unit of gas.

On the PoS Ethereum network, each validator can set a base fee and a priority fee, where the base fee is the basic network fee and the priority fee is the additional fee charged by the validator.

A hash function is a function that converts data of any length into a fixed length output. SHA-256 and Keccak-256 are extensively used as hash functions in Ethereum. The hash value formula can generally be expressed as:

$$H(x) = Hash\ Function(x) \tag{3}$$

where x is the input data, and $H(x)$ is the output hash value.

Ethereum uses elliptic curve digital signature algorithm (ECDSA) for asymmetric encryption. The public key and private key pairs are generated through the formula of elliptic curves, with the commonly used curve being secp256k1, whose mathematical definition is as follows:

$$y^2 = x^3 + ax + b \tag{4}$$

The Ethereum blockchain is a state machine, where each block represents a transition of state. Each transaction will cause changes in account balance, storage, and smart contract status. The state transition function can be expressed as:

$$State_{t+1} = Apply\left(Transaction, State_t\right) \tag{5}$$

where $State_t$ is the current state, $Transaction$ is the input transaction, and $State_{t+1}$ is the new state after executing the transaction.

2.2 Hyperledger

Under direction by the Linux Foundation, Hyperledger is an open-source blockchain initiative meant to offer infrastructure for applications at the corporate level. Hyperledger is a permissioned chain unlike public blockchains like Ethereum and Bitcoin whereby only authorised players may access the network (Dhillon et al., 2017; Benhamouda et al., 2019). The hyperledger architecture lets one be tailored depending on various business demands by supporting several modular components. The core components of a hyperledger include chaincode, smart contracts, consensus mechanisms, privacy protection, and scalability.

Comprising several transactions, a block is a structure in a super ledger used to store transaction records (Andola et al., 2019; Yuan et al., 2018). Changing the status of a transaction record account has this equation:

$$B_i = \left(T_1, T_2, ..., T_n\right) + H\left(B_{i-1}\right) \tag{6}$$

where using B_i for the i^{th} block, T_1, T_2, …, T_n for the transactions housed in that block, $H(B_{i-1})$ for the hash value of the preceding block helps to preserve the blockchain's chain structure. Every block in a blockchain comprises the hash value of the one before it, therefore attaining its immutability.

Through the 'world state', the hyperledger retains the most recent status of accounts. Each transaction will update these statuses using the following equation:

$$S_{t+1} = Apply\left(T_i, S_t\right) \tag{7}$$

where S_t is the state before the transaction is executed; T_i and S_{t+1} is the new state following the transaction execution. Representing the state in a super ledger as a key value pair database will help one to understand it as an account or asset with the matching state data.

A smart contract in the super ledger, chain codes specify read and write actions on the ledger. Usually made of specified business logic, chain codes update the state on the blockchain when run. The equation runs as follows:

$$C(T) = Invoke(T, S) \tag{8}$$

where S is the input state and $C(T)$ is the chain code used by transaction T. The block will record the chain code's execution results, hence creating the blockchain's state transition.

The super ledger uses a modular consensus mechanism so that users may select several consensus techniques based on their usage situation. Common consensus methods comprise Raft with the following equation and Practical Byzantine Fault Tolerant Algorithm (PBFT):

$$C(T) = Invoke(T, S) \tag{9}$$

where T_1, T_2, …, T_n is the transaction to be checked; V is the list of confirmed transactions. A super ledger provides major processing efficiency and scalability since its consensus mechanism does not depend on PoW or proof of stake.

Transactions in a hyperledger have to be verified by an Endorser node to be regarded as valid. Using the following equation, the endorsement node checks the chain code execution result:

$$E(T_i) = Validate(T_i) \tag{10}$$

where $E(T_i)$ represents endorsement of transaction T_i. Based on the chain code execution result, the Validate function ascertains the validity of the transaction. A vital step for transactions to find their way on the blockchain is the signature of endorsement nodes.

Participants of the licensed hyperledger network must be authenticated. The equation is as follows: the access control list (ACL) specifies which users can conduct which operations.

$$A(u, p) = Permission(u, p) \tag{11}$$

where $A(u, p)$ determine whether user u has permission p. ACL policies define access rights. Hyperledger's privacy protection system guarantees that particular specified transactions and data can be accessed only by authorised users.

Execution time and resource use help one to gauge the complexity of chain code running. Similar to Gas in Ethereum, Hyperledger Chain Code also has the concept of resource consumption, with the following equation:

$$Cost = Compute\ Time \times Resource\ Usage \tag{12}$$

where *Cost* is the cost of chain code execution, *Compute Time* is the computation time, and *Resource Usage* is the amount of resources used. Different chain code operations require different computing resources, which affect the efficiency and cost of the network.

Hyperledger's idea of a channel separates data. Every channel stands for a particular set of people who can do secret transactions inside the channel – that which cannot be accessed from other channels. The formula runs as follows:

$$T_i \in C_j \tag{13}$$

where T_i is the transaction in channel C_j. The transactions and data of each channel are isolated from each other, enhancing privacy.

Channels allow multiple business processes to run in parallel while maintaining data confidentiality.

Ledger snapshot is a mechanism for recording the network state at a certain moment. By regularly creating snapshots, the computational burden of queries can be reduced and efficiency can be improved. The equation is as follows:

$$S_{snapshot} = S_t \tag{14}$$

where $S_{snapshot}$ is a snapshot of the world state recorded at time point t. Through snapshots, the ledger state can be quickly restored, especially when the data size is large, which can improve performance.

Hyperledger improves network scalability by supporting sharding and sidechains, as follows:

$$N = S_1 + S_2 + ... + S_k \tag{15}$$

where N is the total network capacity, and S_1, S_2, …, S_k is the processing capacity of each shard or sidechain. By introducing multiple sidechains or shards, the throughput and processing speed of the super ledger can be significantly improved.

3 Risk assessment model for the development of e-commerce finance based on blockchain algorithm

Smart contracts are an automation protocol running on Ethereum that can execute preset rules in real-time and record transaction data (Zou et al., 2019; Giancaspro, 2017). Through the on chain data transparency of smart contracts, we can monitor abnormal behaviour during the transaction process and identify potential technical risks. The framework of this method is shown in Figure 2.

Smart contracts enable real-time monitoring and verification of transactions by deploying contract code on the blockchain. The formula for creating a smart contract is as follows:

$$C = Deploy(Code, Inputs) \tag{16}$$

where C is the smart contract, *Deploy* represents the deployment process, *Code* is the smart contract code, and inputs are the initial parameters of the smart contract

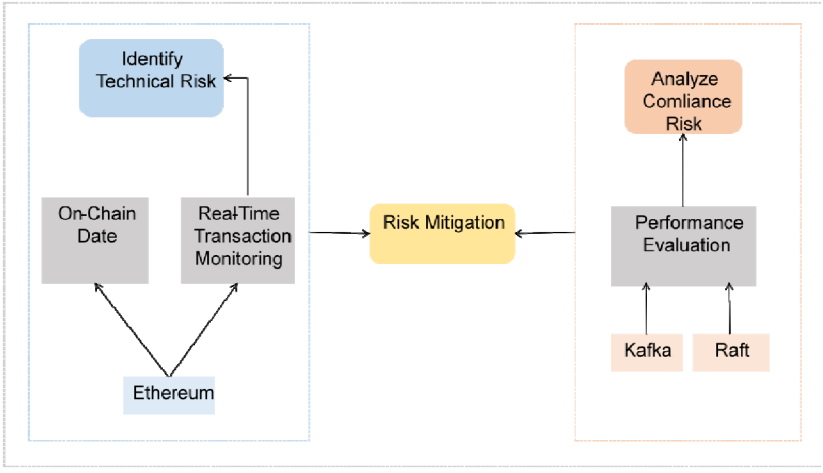
Smart contracts detect abnormal behaviour through on chain data such as transaction time, amount, account, etc.

The transaction monitoring equation is as follows:

$$A(t) = Monitor\left(T_i, t\right) \tag{17}$$

where D represents the monitoring of transaction T_i at time t, and *Monitor* is the monitoring function of the smart contract.

Figure 2 Method framework diagram of this article (see online version for colours)



Smart contracts can detect abnormal behaviour through preset rules, such as timeout transactions or operations that do not conform to business logic. The equation for anomaly detection is as follows:

$$D = Detect(T_i, R) \tag{18}$$

where D represents whether an anomaly has been detected, T_i is the transaction, and R is the set of detection rules.

The modular design of Hyperledger supports pluggable consensus mechanisms, such as Kafka and Raft, allowing for the selection of different consensus algorithms based on business needs. Evaluating the performance and security of these algorithms can help measure compliance risks during the transaction process.

Hyperledger supports multiple consensus algorithms, and users can choose consensus mechanisms such as Kafka and Raft based on their transaction needs. The consensus mechanism selection equation is as follows:

$$C_M = Select(Algorithm, Criteria) \tag{19}$$

where C_M is the chosen consensus mechanism, $Algorithm$ is the available consensus algorithm (such as Kafka, Raft, etc.), and Criteria is the standard for selecting algorithms based on efficiency and security

Evaluate the efficiency of different consensus mechanisms, with main indicators including transactions per second (TPS) and latency. The consensus efficiency equation is as follows:

$$E(C_M) = \frac{T}{L} \tag{20}$$

where $E(C_M)$ is the efficiency of consensus mechanism C_M, T is the number of transactions processed per unit time, and L is the average delay time for transaction confirmation

The security of consensus mechanism refers to its ability to resist Byzantine errors or malicious node attacks. Security can be evaluated through fault tolerance.

$$S(C_M) = f(n, t) \tag{21}$$

where $S(C_M)$ is the security of consensus mechanism C_M, n is the total number of nodes in the network, and t is the number of Byzantine nodes tolerated. $f(n, t)$ is a security function defined according to different algorithms.

Based on the evaluation results of efficiency and security, analyse the degree of compliance of the consensus mechanism with compliance requirements. The compliance risk equation is as follows:

$$R = Assess\left(E(C_M), S(C_M), R_c\right) \tag{22}$$

where R stands for compliance risk; R_c is compliance standard; the *Assess* function ranks compliance depending on the efficiency and security outcome of the consensus method.

At last, a complete risk management system results from merging the technical risk monitoring of smart contracts with the compliance risk assessment of the super ledger consensus mechanism.

Comprehensive evaluation equation:

$$R_{total} = R_{tech} + R_{compliance} \tag{23}$$

where R_{total} is overall risk assessment, R_{tech} is technical risk, and $R_{compliance}$ is compliance risk.

Optimisation formula:

$$Opt = Minimise\left(R_{total}\right) \tag{24}$$

where *Opt* is a choice for optimisation, and the *Minimise* function helps to reduce the overall risk.

This approach examines compliance risks utilising the pluggable consensus mechanism of the super ledger, therefore forming a dual risk assessment and optimisation framework for technology and compliance. It also monitors the technical risks during the transaction process in real-time through Ethereum smart contracts.

4 Experimental results and analysis

4.1 FCE method

Appropriate for handling multidimensional elements with great ambiguity, FCE is a good approach for measuring complicated risk factors. The approach consists on the following actions:

1 Build an evaluation indicator system depending on found risk factors. For every risk dimension, define secondary and tertiary risk factors. For example, primary indicators include technical risk, compliance risk, market risk, and operational risk. Secondary indicators: smart contract vulnerabilities, regulatory compliance, market volatility, system maintenance issues, etc.

2 Establish a fuzzy evaluation set: Set fuzzy levels (such as ‘low, medium, high, very high’) for each indicator, with each level corresponding to a fuzzy value. Let the fuzzy evaluation set be

$$V = \{v_1, v_2, v_3, v_4\} \tag{25}$$

3 Determine weight matrix: Determine the weight matrix of each risk factor based on expert ratings or historical data. Assuming the weight vector is $A = \{a_1, a_2, \ldots, a_n\}$, where a_i represents the weight of the i^{th} risk factor.

4 Build a fuzzy evaluation set: Based on the scores of experts or users for each risk factor, establish a fuzzy evaluation set R:

$$R = \begin{bmatrix} r_{11} & r_{12} & \ldots & r_{1n} \\ r_{21} & r_{22} & \ldots & r_{2n} \\ \ldots & \ldots & \ldots & \ldots \\ r_{m1} & r_{n2} & \ldots & r_{mn} \end{bmatrix} \tag{26}$$

where r_{ij} represents the fuzzy rating of the j^{th} risk factor by the i^{th} expert or historical data.

5 Calculate the risk assessment result: By using the weighted sum method, combined with the weight vector and fuzzy evaluation matrix, the risk assessment result B is obtained:

$$B = A \times R \tag{27}$$

where $B = \{b_1, b_2, \ldots, b_m\}$ is the final risk assessment result.

4.2 Dataset

The dataset used in this experiment includes blockchain transaction data, performance data of super ledger consensus mechanism, expert scoring data, and historical risk event data, aiming to evaluate potential risks in e-commerce finance. Firstly, Ethereum transaction data includes 10,000 transactions, including transaction numbers, timestamps, transaction amounts, consumed gas, and smart contract execution status fields, used to identify technical and compliance risks. Secondly, the transaction data of the hyperledger Fabric platform comes from two consensus mechanisms, Kafka and Raft, and records 8000 transactions, including performance indicators such as throughput and confirmation delay, to evaluate the impact of consensus mechanisms on transaction processing efficiency and security. In addition, the expert rating data is based on the ratings of 10 experts on four types of risk factors: technology, compliance, market, and operation, with a rating range of 1-5, used to quantify the impact of different risk factors. Finally, the experiment also introduced 50 historical risk event data, including technical failures, compliance violations, market fluctuations, etc., to verify the risk identification ability of the model.

4.3 Comparative analysis of experimental results

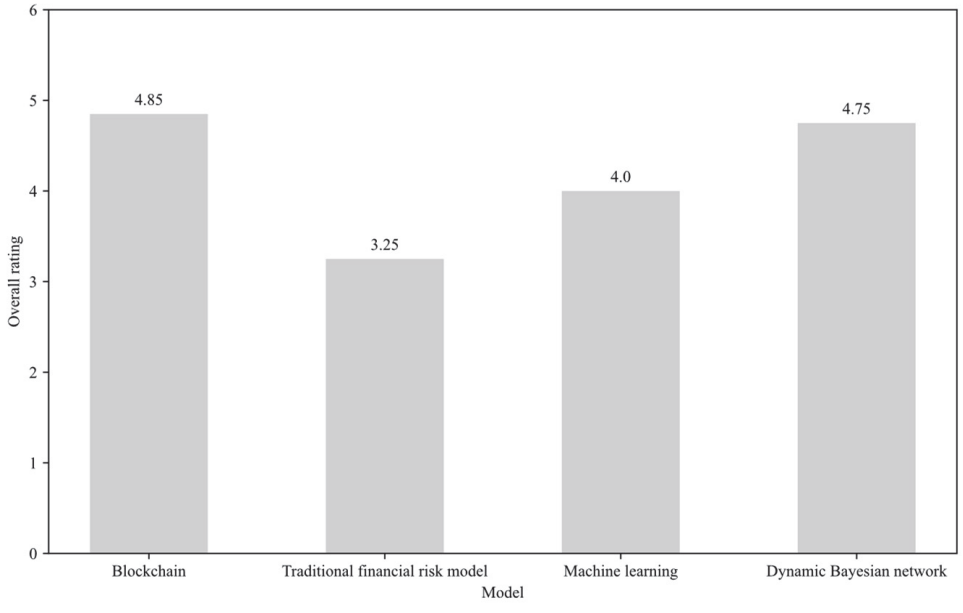
In this experiment, a comprehensive comparative analysis was conducted between the blockchain based risk assessment model and other traditional risk assessment models, mainly evaluating from multiple dimensions such as risk identification accuracy, transaction processing performance, real-time performance, risk quantification ability, and model adaptability. The experiment used data from two blockchain platforms,

Ethereum and hyperledger fabric, combined with FCE method to quantitatively analyse risk factors such as technology, compliance, market, and operation. Meanwhile, traditional financial risk assessment models, machine learning models, and dynamic Bayesian network models were also introduced in the experiment as comparative models to evaluate their performance differences in risk identification and quantification. Table 1 compares the overall risk assessment results. Figure 3 shows the experimental results.

Table 1 Comparison of overall risk assessment results

Model	*Accuracy of risk identification*	*Real-time rating*	*Risk quantification capability*	*Model adaptability*	*Overall rating*
Blockchain	89%	5/5	4.5/5	5/5	4.85
Traditional financial risk model	76%	2/5	3/5	3/5	3.25
Machine learning	82.5%	3.5/5	4/5	4/5	4.0
Dynamic Bayesian network	81.25%	3/5	4/5	3/5	4.75

Figure 3 Experimental result chart



The comparative analysis of experimental results shows that the risk assessment model based on blockchain technology has significant advantages in identifying and quantifying financial risks in e-commerce. Compared with traditional financial risk assessment models and other common algorithms such as machine learning models and dynamic Bayesian network models, blockchain models perform superior in risk identification accuracy, real-time performance, and transparency. Firstly, in terms of risk identification

accuracy, the blockchain based model achieved an accuracy of 89%, higher than the 76% of traditional models and the 81.25% of dynamic Bayesian network models. Especially in identifying technical and compliance risks, the blockchain model utilises the transparency of smart contracts and on chain data, achieving recognition rates of 95% and 92%, respectively. Secondly, in the comparison of transaction processing performance, the Kafka consensus mechanism of the hyperledger exhibits high throughput (1,200 TPS) and low confirmation latency (80 ms), which has significant advantages in handling large-scale transactions. Although the Raft consensus mechanism has a slightly lower throughput (950 TPS), it still maintains good performance. Finally, blockchain based models also score the highest in risk quantification ability and adaptability, thanks to the immutability and real-time data monitoring capabilities of blockchain, providing decision-makers with more timely and accurate risk assessment results. This indicates that blockchain technology has broad potential for application in risk management in the financial sector.

5 Conclusions

This article studies the application of blockchain technology in e-commerce financial risk assessment, with a focus on analysing the smart contracts and consensus mechanisms of two major platforms, Ethereum and hyperledger fabric. By constructing smart contracts based on Ethereum, this article achieves real-time monitoring of technical risks during the transaction process; At the same time, through the pluggable consensus mechanism of the super ledger, the efficiency and security of different consensus algorithms (such as Kafka and Raft) in processing transactions were evaluated, and compliance risks were further identified and analysed. Combining the FCE method, this article constructs a comprehensive risk assessment model, which quantitatively analyses various risk factors such as technology, compliance, market, and operation. The experimental results show that the risk assessment model based on blockchain is significantly better than traditional methods in terms of accuracy, efficiency, and real-time risk identification, and can effectively identify and quantify potential risks in e-commerce finance. Ultimately, the model provides decision-makers with accurate risk assessment information, promoting the sustainable development of the e-commerce finance industry. The research results of this article demonstrate that blockchain technology has the potential to enhance financial risk management, especially in terms of improving transparency, data integrity, and real-time monitoring, providing strong support for the security and stability of future e-commerce financial systems.

References

Andola, N., Gogoi, M., Venkatesan, S. et al. (2019) ‘Vulnerabilities on hyperledger fabric’, *Pervasive and Mobile Computing*, Vol. 59, p.101050.

Ante, L. (2021) ‘Smart contracts on the blockchain – a bibliometric analysis and review’, *Telematics and Informatics*, Vol. 57, p.101519.

Benhamouda, F., Halevi, S. and Halevi, T. (2019) ‘Supporting private data on hyperledger fabric with secure multiparty computation’, *IBM Journal of Research and Development*, Vol. 63, Nos. 2/3, pp. 3:1–3:8.

Buterin, V. (2013) ‘Ethereum white paper’, *GitHub Repository*, Vol. 1, pp.22–23.

Chen, H., Pendleton, M., Njilla, L. et al. (2020) 'A survey on ethereum systems security: Vulnerabilities, attacks, and defenses', *ACM Computing Surveys (CSUR)*, Vol. 53, No. 3, pp.1–43.

Dhillon, V., Metcalf, D., Hooper, M. et al. (2017) 'The hyperledger project', *Blockchain Enabled Applications: Understand the Blockchain Ecosystem and How to Make It Work for You*, pp.139–149.

Giancaspro, M. (2017) 'Is a 'smart contract' really a smart idea? Insights from a legal perspective', *Computer Law & Security Review*, Vol. 33, No. 6, pp.825–835.

Ioannou, I. and Demirel, G. (2022) 'Blockchain and supply chain finance: a critical literature review at the intersection of operations, finance and law', *Journal of Banking and Financial Technology*, Vol. 6, No. 1, pp.83–107.

Jani, S. (2017) 'An overview of ethereum & its comparison with bitcoin', *Int. J. Sci. Eng. Res*., Vol. 10, No. 8, pp.1–6.

Kaur, S., Singh, S., Gupta, S. et al. (2023) 'Risk analysis in decentralized finance (DeFi): a fuzzy-AHP approach', *Risk Management*, Vol. 25, No. 2, pp.14–20.

Kushwaha, S.S., Joshi, S., Singh, D. et al. (2022) 'Ethereum smart contract analysis tools: a systematic review', *IEEE Access*, Vol. 10, pp.57037–57062.

Le Quoc, K., Trong, P.N., Le Van, H. et al. (2022) 'Letter-of-credit chain: cross-border exchange based on blockchain and smart contracts', *International Journal of Advanced Computer Science and Applications*, Vol. 13, No. 8, pp.38–45.

Lewis, R., McPartland, J. and Ranjan, R. (2017) 'Blockchain and financial market innovation', *Economic Perspectives*, Vol. 41, No. 7, pp.1–17.

Metcalfe, W. (2020) 'Ethereum, smart contracts, DApps', *Blockchain and Crypt Currency*, Vol. 77, pp.77–93.

Wood, G. (2014) 'Ethereum: a secure decentralised generalised transaction ledger', *Ethereum Project Yellow Paper*, Vol. 151, No. 2014, pp.1–32.

Yuan, P., Xiong, X., Lei, L. et al. (2018) 'Design and implementation on hyperledger-based emission trading system', *IEEE Access*, Vol. 7, pp.6109–6116.

Zohar, A. (2015) 'Bitcoin: under the hood', *Communications of the ACM*, Vol. 58, No. 9, pp.104–113.

Zou, W., Lo, D., Kochhar, P.S. et al. (2019) 'Smart contract development: challenges and opportunities', *IEEE Transactions on Software Engineering*, Vol. 47, No. 10, pp.2084–2106.