INTERNET FINANCIAL RISK MANAGEMENT STUDY

A Thesis submitted by

Guansan Du

For the award of

Doctor of Philosophy

2023

ABSTRACT

Driven by technological change, the Internet has rapidly integrated with the traditional financial sector of the economy, and has continued to advance and develop new features. The Internet is no longer simply providing support and services to traditional finance in terms of technology and operation mode, but has continuously penetrated the traditional financial field, resulting in an emerging financial system that breaks the traditional model of financial intermediation, eliminates information asymmetry, reduces transaction costs and improves payment efficiency. This new financial model enables information sharing, resources sharing, economic activities facilitation and scale effect formation. Internet finance can play an important role in areas that traditional finance can not, and thus can better serve the economy and promote the development of human society. However, Internet finance as a new financial model in the process of rapid development will certainly be accompanied by hidden risks of various kinds, and has a huge impact on the traditional financial industry, financial markets and financial regulators. Therefore, this thesis raises the important issue of risk management research in Internet finance. The development of the financial industry under the Internet technology revolution is studied. Based on the characteristics of Internet finance, the types of risks that are different from those of traditional finance are identified. Based on the qualitative analysis of the identification of the types of Internet financial risks, the quantitative analysis method is used to establish the evaluation index system and do quantitative evaluation analysis of Internet financial risks. The use of BP (Back Propagation) neural network expands the application of BP neural network in the field of Internet finance, and provides a new development direction for the early warning and assessment of Internet credit risk. Comparative analysis of ML (Machine Learning) and DL (Deep Learning) algorithms in Internet credit risk assessment is used and explored to improve the accuracy of financial prediction. The exploration of edge computing and blockchain technology intends to solve the great security risks in the financial network transaction process and the certain restrictions on the current use of blockchain technology in mobile terminal equipment. The research object of this thesis is Internet financial risk management. Under the current social, economic and financial environment, it explores the theoretical basis of Internet financial risk management, and analyses the risk management framework and methods of Internet financial risk assessment, risk warning and risk control. The aim is to achieve healthy and stable development of the Internet finance industry, thus contributing to the real economy and the promotion of human social progress.

CERTIFICATION OF THESIS

I, Guansan Du, declare that the PhD Thesis entitled Internet Financial Risk Management Study is not more than 100,000 words in length including quotes and exclusive of tables, figures, appendices, bibliography, references, and footnotes.

This thesis is the work of Guansan Du except where otherwise acknowledged, with the majority of the authorship of the papers presented as a Thesis by Publication undertaken by the student. The work is original and has not previously been submitted for any other award, except where acknowledged.

Date: 30 Jan 2023

Endorsed by: Guansan Du

Principal Supervisor: Dr Frank Elston

Associate Supervisor: Professor Shane Zhang

Student and supervisor signatures of endorsement are held at the University of Southern Queensland.

ACKNOWLEDGEMENTS

First and foremost, I would like to express my deep and sincere gratitude to my supervisor Dr Frank Elston for his generous guidance and helpful comments during the writing of my thesis. With his patience and encouragement, I would continue my PhD study at USQ without stress. In many instances, his guidance has helped me to become more disciplined and logical in my thesis.

I also would like to convey my heartfelt gratitude towards my associate supervisor Professor Yahua (Shane) Zhang for helping me in valuable discussions and for his continuous encouragement and endless patient. I have been blessed to have a professional and knowledgeable supervisor who is passionate about research.

To be honest, even I did not expect that I would have the opportunity to study for PhD at USQ. This is a very important experience for me, and it changed the path of my life. Thus, I would like to David Dukes, International Office, Graduate Research Office, Christopher Droney and USQ. Thanks for them offering me a chance to study at USQ and for their generosity, help and support during my study.

In addition, I would like to thank my friends in Australia and China and Benjamin Eban. Their care and company make me less stressful.

Finally, I would like to thank my family, my parents and my sister. They are like a light that forever shines in front of me. Although they are far away in China, they always support me with their love and cheer me on. They always give me selfless support and love, making me more fearless in my exploration of the world. I wish them good health, peace and joy.

Once again, thank you so much for all your continued support through the good times and the bad.

May I continue to strive to live up to my dreams in the years to come.

STATEMENT OF CONTRIBUTION

Du, G., Liu, Z., & Lu, H. (2021). Application of Innovative Risk Early Warning Mode under Big Data Technology in Internet Credit Financial Risk Assessment. *Journal of Computational and Applied Mathematics,* 386.

The overall contribution of Guansan Du was 80 per cent to the concept development, analysis, drafting and revising of the final submission. Zixian Liu and Haifeng Lu contributed the other 20 per cent to analysis, editing and providing important technical inputs.

Du, G., & Elston, F. (2022). Financial risk assessment to improve the accuracy of financial prediction in the internet financial industry using data analytics models. *Operations Management Research*.

The overall contribution of Guansan Du was 80 per cent to the concept development, analysis, drafting and revising of the final submission. Frank Elston contributed the other 20 per cent to analysis, editing and providing important technical inputs.

Du, G., & Elston, F. (2022). Financial Network Transaction Risk Control based on Edge Computing and Blockchain Technology. *IEEE Transactions on Engineering Management.* Under Review.

The overall contribution of Guansan Du was 80 per cent to the concept development, analysis, drafting and revising of the final submission. Frank Elston contributed the other 20 per cent to analysis, editing and providing important technical inputs.

TABLE OF CONTENTS

LIST OF ABBREVIATIONS

AHP	Analytic Hierarchy Process
AUC	Area Under Curve
BCGWO-KNN	Basic Change Grey Wolf Optimizer-K Nearest Neighbors
BFWO-KNN	Basic Grey Wolf Optimizer-K Nearest Neighbors
BP	Back Propagation
BTS-PD	Base Transceiver Station-Power Device
CNN	Convolutional Neural Network
CPU	Central Processing Unit
CP-ABE	Ciphertext Policy Attribute Based Encryption
DCN	Deep & Cross Network
DID	Decentralized Identity
DL	Deep Learning
DNN	Deep Neural Network
EC	Edge Computing
ECP	Edge Computing Platform
GA	Genetic Algorithm
GWO	Grey Wolf Optimizer
HMM	Hidden Markov Model
HTTP	Hyper Text Transfer Protocol
IoT	Internet of things
IPFS	Inter Planetary File System
IFTF	International Financial Action Task Force
IT	Internet Technology
ML	Machine Learning
MSE	Micro Small Enterprises
MSE	Mean Square Error
NBS	National Bureau of Statistics
NN	Neural Network
OS	Operating System
P2P	Peer to Peer

RAM	Random Access Memory
ROC	Receiver Operating Characteristic
RTT	Round-Trip Time
SME	Small and Medium-sized Enterprise
SRDF	Semantic Robot Description Format
UCI	University of California Irvine
VC	Verifiable Credential

CHAPTER 1: AN INTRODUCTION OF THE INTERNET FINANCIAL RISK

1.1. Background

As we enter the 21st century, the Internet and new mobile communication technologies are gradually becoming a strategic infrastructure for the development of human society in the information age, changing the way human society operates and consumer behaviour, and driving prosperity and profound changes in the entire social economy. The integration of the Internet and finance has not only changed the operation of traditional finance but also led to the development of a new financial industry. The Internet finance industry, represented by Peer to Peer (P2P) network lending, third-party payment, crowdfunding and mobile finance, has increasingly had a widespread impact on internet finance. Internet finance has developed rapidly, and has revealed many new features including new risk characteristics. Due to the time cost and time lag in the construction of the regulatory system, the regulation of Internet finance has not kept pace with the development of its business-level innovation. There are a series of potential risks in the development of Internet finance, and even some of them have caused serious risk exposure problems, which have aroused widespread concern in society and academia. Given the above problems, it is necessary to conduct timely academic analysis and in-depth research on risk management in the Internet finance industry from identification, and early warning to prevention and disposal.

1.2. Research Aim and Objects

With the combination of financial assets with Internet technology and information technology, Internet finance has emerged and developed rapidly, becoming a new type of financial industry that relies on Internet information technology to form businesses such as investment and financing, payment and lending. The rise of Internet finance has not only changed the financing mode of the traditional financial system represented by commercial banks, but it also has optimised the function of financial resource allocation, alleviated the financing constraints of small and medium-sized enterprises, and promoted the rapid development of inclusive finance. Furthermore, the rise of Internet finance has greatly improved the efficiency of payment clearing through innovative third-party payment and digital currency, providing faster payment services to society and bringing great convenience to life.

Notwithstanding the rapid development of Internet finance, its risk problems are also increasingly prominent. On the one hand, the use of a large number of technologies in Internet finance has given rise to new and specific risks, such as technology risk, information security risk, and information security risk. On the other hand, the integration of Internet technology and financial business has changed the risks in the traditional financial market, adding new characteristics to traditional financial risks. Different types of risks are superimposed on each other, and the impact on the financial system and even the whole national economic system is further expanded. Therefore, how to effectively measure and warn about the risks of the Internet financial market has become a hot issue of concern for scholars.

Throughout its compilation, the thesis is sought to provide new insights into several research questions.

Firstly, conventional risk assessment methods include logistic regression discriminant analysis and multiple discriminant method, which can accurately assess credit risk. However, the disadvantage is that it requires a large amount of real data as the premise, it relies too much on historical data, and the dynamic early warning capability is reduced. In chapter 2, The neural network model can solve complex nonlinear problems. Therefore, by building a Back Propagation (BP) neural network credit warning model to combine big data technology with Internet credit risk warning, early Internet credit risk can be quickly identified and analysed.

Secondly, what could be used to assess risks for Internet financial enterprises systematically? In chapter 3, Machine learning (ML) technology can greatly improve financial processing and decision-making ability. Deep Learning (DL) technology can analyse and model financial data and help enterprises and regulators make decisions through a systematic financial industry learning environment. ML and DL methods can measure the system indexes with strong data analysis and processing capabilities, providing solutions for the risk assessment of the Internet financial industry.

Finally, present blockchain technology research in network security has been relatively mature. However, due to the functional defects of the intelligent terminal device itself, there are still some restrictions on the use of blockchain. In chapter 4, an anonymous storage protocol for financial network transaction data based on blockchain technology and EC (Edge Computing) is proposed. The protocol can generate a false identity for the terminal equipment and use the false identity to protect the real identity to protect the corresponding relationship between identity and data and improve the privacy protection of financial network transactions.

1.3. Methodology

Quantitative analysis is used in the thesis to study the management of Internet financial risks in a comprehensive and systematic manner. This thesis adopts BP neural network, machine learning, deep learning, edge computing and blockchain in an attempt to more accurately portray the risks of Internet finance and to more scientifically and rationally manage the risks of Internet finance.

1.4. Thesis structure

As an emerging industry, Internet finance has experienced rapid growth since 2013, and has been accompanied by a significant accumulation of industry risks. Internet finance risk has become increasingly important. It is important to accurately identify the types and impacts of risks in Internet finance, to correctly deal with the relationship between Internet finance and traditional financial risks, and to identify, evaluate and measure risks with scientific means. Therefore, in the background of the rapid development of Internet finance, with the frequent risks, this thesis conducts theoretical research on Internet financial risk management issues theoretically.

Chapter 1 and 2 present the relevant research background and significance of this paper, and provides an objective combing, review and critique of domestic and international literature, forming a literature review of Internet financial risk. It presents the main theories involved in this paper and their guiding significance in the paper are presented. Moreover, the thesis explains the research methods used in this paper, the structure of the paper, and the innovation points are explained.

In chapter 3, the paper proposes the problems in the current Internet financial risk assessment. It collects data of Micro small Enterprises (MSE) for analysis. And it explores the role of ML and DL algorithms in Internet credit risk assessment to improve the accuracy of financial prediction. A feature extraction method based on ML is proposed to solve data redundancy and interference in enterprise credit risk assessment. To solve the data imbalance problem in the credit risk assessment system, a credit risk assessment system based on the DL algorithm is introduced. The proposed credit risk assessment system is verified through a fusion algorithm in different models with specific enterprise data.

To continue the study of internet financial risk assessment, in chapter 4, the paper uses big data technology to form an effective early warning and prevention of Internet credit in the era of big data. The BP neural network algorithm is applied to determine the number of nodes, activation function, learning rate, and other parameters of each layer of the BP neural network. Also, many data samples are used to build an early warning model of Internet credit risk. The constructed model is trained and tested. Finally, the genetic algorithm (GA) is used to optimise the neural network to improve the accuracy of early warning.

In chapter 5, a final journal article intends to solve the great security risks in the Internet financial network transaction process and the certain restrictions on the current use of blockchain technology in mobile terminal equipment. An anonymous storage protocol for financial network transaction data and a trusted data synchronisation system based on blockchain technology and EC (Edge Computing) are proposed. It is expected that these two methods can improve the security of financial network transactions to a certain extent. This exploration provides a reference for the research of multi-node trusted data synchronisation across multiple security domains and the risk control methods of Internet financial transactions.

In Chapter 6, a concluding discussion of the main findings, limitations and future recommendations is presented to promote discussion. It may perhaps provide a springboard from which other more worthy researchers might find solutions to assess internet financial risk.

CHAPTER 2: LITERATURE REVIEW

2.1. Financial innovation based on technological changes in the Internet

Financial innovation based on the changes wrought by Internet technology and Internet Finance is a new development field resulting from the integration of traditional financial operation methods with the spirit of the Internet. Therefore, Internet finance cannot be simply regarded as the operation of Internet technology in the financial industry. In essence, it is a finance based on the idea of Internet operation with technology as the main support (Allen, 2002).

In terms of the concept and connotation of Internet finance, it is not a unified and comprehensive concept. The earliest concept of Internet finance can be traced back to the application of computer and communication technology in the financial field, i.e., the early stage of electronic finance. With the continuous innovation of electronic payment system innovation and the rapid development of the financial industry, the connotation of e-finance and internet finance has arisen. In 2001, banks proposed a definition of e-finance, that is, e-finance refers to the provision of financial services to the public through the Internet or other public-type electronic communication media, mainly including money services, banking services, payment services, trading venues, etc., which can also be generally called digital finance. In most developed countries, some concepts of finance are interchangeable. For example, e-finance can be interchanged with online finance, virtual finance, Internet finance and cyberfinance. Whether it is online finance or e-finance, in the initial application, the essence is that the traditional financial organisations or traditional financial services are gradually developed in the direction of the Internet, the most important feature of which is that through the Internet as a trading platform, the transaction costs of financial transactions are greatly reduced, thus enhancing the availability and accessibility of financial services. In the previous 15 years, many companies began to enter the Internet finance industry, and some companies have made good achievements.

However, due to the fierce competition in the market, many enterprises were eliminated from the market. The successful companies responded to the development needs of the financial market and made full use of their strengths in the Internet, big data, and cloud computing to build an efficient operating market (Sven Seuken, 2012). The important thing is not the mere use of Internet technology, rather, the birth of the Internet has allowed financial organisations to overcome information asymmetry and adverse selection behaviour of financial organizations, creating a new marketplace where transactions can be conducted without intermediaries. Burstein(2008) proposed that mobile finance could transcend the constraints of time and space, enabling customers to receive effective services from "intermediaries" at any point in time. Given the increasing reliance on financial services on the Internet, the unique scale of the network economy will also play an important role in the overall competitive environment of the financial industry (Claessens, Dobos, Klingebiel & Laeven, 2003). Companies that choose to operate on the Internet will no longer be subject to the monopoly of banks in terms of user information; they will be able to create a complete chain of services for their customers and provide a variety of financial services, thus reducing their costs and adopting intelligent systems to provide high-quality services to their customers (Sato & Hawkins, 2001). Shahrokhi(2008) suggested that the development of e-finance has many positive effects on the financial industry, including a significant reduction in transaction costs, a significant improvement in the quality of services enjoyed by customers, and a qualitative development in the availability of financial services. He also argued that e-finance is likely to be the third type of operation after the emergence of traditional financial intermediation and capital markets. He also argues that e-finance is likely to be the third mode of operation after the emergence of traditional financial intermediation and capital markets. In terms of empirical research, in 2003, Nagurney and Ke constructed a mathematical model of the e-finance trading platform and conducted a study on the equilibrium operation and the coordinated development of the model.

In terms of development models, Paul Timmers (1998), based on the analysis of value chain decomposition and reconstruction, and combining the characteristics of the degree of functional integration development and innovation methods of e-commerce type companies, classifies e-commerce types into 11 types, specifically including e-auction, e-mall, e-type shopping centre, virtual type community, service operator of value chain, integrator of the value chain, trading platforms, information brokers, third-party trading markets, and trust-based services. Paul Bambury(1998) found the differences between the operational models of e-commerce and traditional commerce by comparing them and divided e-commerce into two main categories: the transplantation model, which includes operational methods, financing methods, and incentives embedded in the Internet; and the endowment model, which includes all barter transactions. Peter Weill(2001) also proposed that there are eight types of e-commerce operation models, specifically including content providers. Crystal Dreisbach and Staff Writer (2000) have divided the business functions of the Internet into three major categories based on several business functions, including the business operation mode based on product sales. The business operation mode based on The Internet has been divided into three major categories based on several business functions, including business operations based on selling products, business operations based on providing services, and business operations based on providing information.

2.2. Research related to the risk of Internet finance

Studies about the risk of Internet finance divide it into two types, which are liquidity risk and credit risk. Kim (2005) suggests that online transactions conducted in e-commerce include services provided by several third-party credit organisations, such as banking institutions, institutions authorised to issue credit cards, and online information protection agencies for purchasers. The article also describes the third-party payment methods provided by eBay. In 2013, the International Financial Action Task Force (IFTF) studied the impact and risk factors of various payment methods, such as prepaid cards, Internet payments and mobile payments, and completed a report on the analysis, based on which it proposed a methodology to assess the risks, and proposed to strengthen regulation and improve regulation from the perspective of money laundering risks. Haizheng Li, Richard Ward and Han Zhang (2003) used two models, Prohibit and Nested Logit, to investigate the selection behaviour of online payment methods for eBay transactions, and constructed a payment selection system based on risk, convenience and cost indicators. Michael Klafft (2008) analysed the problem of revenue recovery for inexperienced lenders in a virtual network with information imbalance and studied the case of Prosper.com. In the same year, Harpreet Singh, Ram Gopal, and Xinxin Li (2008) used a decision tree study to analyse the different returns and risks associated with Prosper.com multiple loans and risk, concluding that no credit level is immune to subgroups in making positive returns, and that returns are associated with risk in general. The study also found that lower credit tiers were more efficient than higher credit tiers in terms of the consistency of returns with risk.

In terms of risk management and macro regulation, Karne Furst (2002) conducted a study on all commercial banks in the U.S. financial industry and found that commercial banks offering e-finance products or services have more diversified sources of liabilities. Their income has shifted from an general spread income to income from intermediate business, and their profitability and asset quality are higher than other commercial banks. Anait K. Pemlhatur (2001) argued that banks may face operational risks, as well as security, legal, and reputational risks, if they want to launch online services. Because the evolution from traditional banking to online banking has entered a new mode of operation and development, the mechanisms and methods of risk control have to be re-worked to meet the relevant market needs and trends. Mann and Ronald (2004) studied the current legal system and policy system of the new online payment forms represented by PayPal in the U.S. and proposed a feasible idea to improve the regulatory law given the difficulty of protecting the interests of consumers in the new online payment medium. RJ Sullivan (2006) analysed the opportunities and risks of third-party payments in the retail payment system and reflected on the regulatory system of the operating third-party payment providers, suggesting that the regulatory policies are largely designed to control the risks of the retail payment system of third-party payments overcoming information asymmetry and externalities. Andrew Verstein (2011) argued that P2P lending has been successful in connecting borrowers to investors through technological and financial innovations, examined regulatory issues on the platform, and suggested that P2P lending be introduced into consumer financial protection organizations. In the same year, Akindemowo and Eniola (2011) explored the regulatory history of the Federal Deposit Insurance Corporation, the Federal Reserve Board, and the instrumental products that govern online stored value, arguing that regulators need to set aside disagreements about whether stored value instruments can become deposits and focus on building an efficient, flexible payment system that can target regulation of different types of stored value products. Claxton (2011) conducted a comparative study of U.S. and EU anti-money laundering laws for stored value cards, concluding that the EU has more robust laws on electronic money than the U.S., resulting in more rational and regulated use of stored value cards, and stricter regulation of both illegal money laundering and suspicious transactions. Eric C. Chaffee and Geoffrey C. Rapp (2012) analysed the problems with the regulation of P2P lending after Dodd-Frank, examined the current regulatory regime for lending platforms at the federal and state levels, and presented a report on "Person-to-Person Lending: New Regulatory Challenges Could Emerge as Industry Grows". In 2013, the Wolfsburg Group took a stand on the self-regulation of the payments industry and proposed specific requirements for its risk characteristics and industry self-regulation.

2.3. Studies in China

The early research on the nature of Internet finance in China was conducted by Xie et al (2012), who think that Internet finance will form a new market that is different from both the indirect financing model of commercial banks and the direct financing model of the capital market. This new market can be called the direct financing market in the Internet field, or the

Internet finance operation model. Zeng (2012) agrees with the above view and believes that Internet finance does have many characteristics different from traditional finance, including strong innovation and competition, and compares the relevant characteristics of traditional finance and Internet finance from multiple perspectives such as function and institution. Wu (2014) analysed the nature of Internet finance from the perspective of financial functions, and argued that the Internet is a source of genetic change and systemic pressure on traditional finance, finance with the Internet as a platform. He suggests that the development of Internet finance is disruptive and alternative, and will eventually be replaced by a new financial industry. Wu (2015) further studies the growth logic of Internet finance and agrees with the judgment of Xie and Ping that Internet finance is the third financial industry (the new financial industry).

Wang Shuguang et al. (2014) argue that in a broad sense, Internet finance is the organic combination of modern information technology, network technology and various financial businesses. And it is a new form of finance that the Internet and mobile Internet virtual space carry out financial activities. Gong (2014) argues that this new form of financial operation, Internet finance, has perfected the defects of traditional financial operation methods and has the characteristics of universality, digitalization and convenience, which have positive promotion significance for serving the real economy. Cao (2015) proposes that Internet finance is the integration of the Internet with finance, a new financial operation model that enables the financing of funds, online payment, and access to various types of information through the development of modern technology in the field of Internet and mobile communication. He points out that Internet finance is a new development field formed by the integration of traditional financial operation methods with the Internet, and the most prominent performance is represented by modern digital technology, especially various search engines, cloud computing technology, mobile payment, data analysis and network coverage development in various fields such as society. Zhang (2014) argues that Internet finance has enriched the temporal path of financial development theories, and its innovation is not only reflected in the service technology, but also the transformation of the business model. Therefore, Xie and Ping (2014) define Internet finance broadly. They argue that Internet finance points to a forward-looking and systematic concept that encompasses any financial organization and transaction model influenced by the technology and spirit of the Internet, from multiple financial intermediaries and markets, to non-financial intermediaries and markets corresponding to the universal equilibrium of Varas, which is a highly flexible and spatial definition.

2.3.1. Causes of Internet financial risks

He et al. (2014) analysed the risk causes of Internet finance from both institutional and non-institutional factors, among which institutional factors include inadequate laws and regulations, the lack of regulators, and the failure of Internet financial institutions to establish a sound risk internal control system. Non-institutional factors include information security risks and operational risks brought about by big data application technology and operational risks, the uneven endowment of possessing resources, divergent regulatory understanding and regulatory philosophy, and immature credit mechanisms. Yao et al. (2015) analysed the risk causes of Internet finance that are different from traditional finance, including the lack of corresponding standard norms, the inability of the regulatory system to adapt to the new business development, the complexity of the technical architecture and its rapid evolution. Peng (2015) takes P2P network lending companies as the research object and believes that the reasons for their risk formation mainly include the lack of legal regulation, an imperfect credit system and an unhealthy competition environment. Xue (2016) analysed the liquidity risk of Internet finance and considers that the causes of risk are divided into the financial environment and the general environment. etc. The financial environment mainly includes three aspects: the government's financial policies and the amount of monetary input, the government's regulatory policies and laws and regulations, and the operating conditions of financing enterprises. Zhou (2016) believes that the causes of Internet finance risks include the lack of government regulation, the weak operation level of enterprises in the industry, and the lack of basic investment knowledge of investors. Peng (2016) analysed the causes mainly from the perspective of the systemic risk of Internet finance, dividing them into external and internal causes. The external causes mainly include the excessive penetration of information technology, the prominent irrational behaviour of market subjects, the strong control of public opinion of Internet enterprises, and the lag of regulatory regulations and policies; the internal causes include the fragility of the Internet financial market, the pro-cyclicality of the financial system, the segmentation of the regulatory model, and the segmentation of the regulatory mechanism. Although the analysis of the existing literature is relatively comprehensive, there is a lack of comparison between the causes of traditional financial risks and the causes of Internet financial risks. At the same time, there are few academic achievements based on the theories of economics and finance to analyse the causes of Internet financial risks.

2.3.2. Internet financial risk transmission

Liu (2015) analysed the transmission conditions (transmission threshold, transmission vector, transmission object), transmission mode (contact-induced transmission, non-contact-induced transmission) and transmission scope (traditional financial system, real trading area) of Internet finance risk. Yuan (2016) analysed the risk transmission system of traditional finance and Internet finance comparatively, and the data of capital flow and flow in Internet finance, and the transmission paths of various risks from seven aspects, including risk transfer, institutionalised risk, information imbalance risk, flow-related risk, credit-related risk, information technology-related risk and monetary policy-related risk. He argued that the number of Internet financial users is higher than that of other financial institutions. He also believed that due to the greater number of users of Internet finance, once substantial risks occur, they will be transmitted more rapidly than traditional finance. Chen et al. (2017) believe that there are two types of transmission paths in Internet finance, the first type is the network creditability risk originating among Internet financial organizations, and the second type is the network financial risk originating from customers in the Internet financial sector. Based on the perspective of Internet finance, a principal-agent model and a dynamic game analysis model are established to study the risk transmission of credit in the network domain. The study is based on a principal-agent model and a dynamic game analysis model. Some of these papers analyses the transmission paths of different risks from the perspective of risk classification, and the other mainly uses models to analyse the risk transmission in Internet finance.

2.3.3. Identification of risk types in Internet finance

Yan (2013) proposed that Internet finance itself has many risks of specificity, mainly including risks in the field of legal policies, risks in the field of business management, risks in the field of network technology, risks in monetary policies and risks in money laundering crimes. Zheng (2014) summarised the risks of Internet finance into two aspects: on the one hand, there are risks related to the technical field of Internet finance, and on the other hand, the industry does not transcend the essential attributes of finance, and thus significant financial risks may occur, here mainly referring to the risks of information imbalance, risks in the field of credit, risks arising from liquidity, legal and policy. The main risks here are information imbalance risk, credit area risk, liquidity-induced risk, legal and policy risks, etc. Yao et al. (2015) identify in detail the categories of Internet finance risks, which are classified as operational risks (risks arising from technical and user operation irregularities), technical risks (risks in technology development, risks in technology security), credit risks (risks arising from default, risks of individual credit and information theft, fraud-type risks), operational risks (risks arising from liquidity, risks arising from market selection, risks arising from maturity mismatch, risks arising from capital balance, risks arising from correlation, risks arising from imperfect coordination of interests), legal and regulatory risks (risks arising from imperfect laws and regulations, risks arising from inadequate supervision, risks arising from legal qualification of subjects, risks arising from money laundering), other risks (risks arising from perception, moral risks, risks inhibited by traditional financial institutions, risks arising from public opinion). Liu (2016) classifies Internet finance risks as risks encountered in the financial system before the use of the Internet, mainly including systemic risks, circulation-type risks, moral risks, and operational risks, as well as new risks that have emerged with the emergence of Internet finance, including technology risks, policy risks, and crisis expansion risks, etc. E (2016) divides Internet finance risks into systemic and non-systemic risks, where systemic risks are divided into risks arising from information technology dimension risks (technical security, technical support risks), risks arising from macro environment and policy dimensions (macro environment, industry system, and monetary policy risks). The non-systematic risks are divided into risks arising from the operational dimension (business process, legal compliance, specific operational risks), and risks arising from the participant dimension (strategic, credit and reputation risks). The above literature shows that there are various types of Internet financial risks, which generally include legal and regulatory risks, credit risks, technical risks, liquidity risks, information security risks, etc. Meanwhile, some of the literature also compares traditional financial risks with Internet financial risks.

2.3.4. Risk assessment of Internet finance

Yao et al. (2015) proposed that Internet finance risk assessment can take three methods: qualitative, qualitative, and comprehensive analysis assessment. Among them, qualitative assessment methods include expert interviews, questionnaire surveys, and collective discussion methods; quantitative assessment methods include decision tree analysis, sensitivity analysis, and computer simulation methods; and comprehensive analysis assessment methods combine qualitative and quantitative methods and use fuzzy hierarchical analysis to conduct assessments, including establishing a hierarchical model of risk factors, determining the weights of sub-risk factor values, solving fuzzy matrices, and deriving overall risk value. Shen et al. (2016), Lu (2016) and Xu (2017) all three authors used fuzzy hierarchical analysis to conduct risk assessment research on Internet finance. Based on the daily return data of the Internet finance index and the SSE Composite Index, Ouyang et al. (2016) discussed and developed the Pareto extreme value distribution model and the historical simulation method model under the parametric, semi-parametric, and non-parametric VaR methods, to measure the risk value of Internet finance, and used the return test to determine the merits of the models. The results show that the Pareto extreme value distribution model can reflect the risk of Internet finance more accurately, and the risk of Internet finance is higher than that of the stock market as a whole. Li et al. (2016) assessed the risk of Internet finance by building a CVaR model based on the daily return per 10,000 of Tianhong Balance Money data, including CVaR model and estimation method, selecting and processing data, calculating VaR and CVaR, etc.. Based on the results of the model analysis, they concluded that the risk of Internet finance is more explosive and contagious, and its risk is in a positive accumulation and rising state. Jiang et al. (2016) took P2P network lending as an example and assessed the credit risk of Internet finance based on the Logistic regression model, and found that lenders on P2P platforms attach more importance to factors such as whether the borrower has a car, whether the property is verified, and whether field authentication is performed. From the above literature analysis, it can be seen that the Internet finance industry is still in the development stage. Corresponding real industry data are difficult to obtain. Therefore, when evaluating Internet financial risks, combining qualitative and quantitative methods, using fuzzy analytic hierarchy process, and combining risk type identification are currently more feasible methods for evaluating Internet financial risks.

2.3.5. Internet finance risk warning

From the perspective of big data, Yang (2014) follows the data-centred system design principles for the characteristics of Internet finance, classifies the system hierarchically according to the processing of data, and constructs a risk warning system in the field of Internet finance. In this system, the data-centred system design principles include the principles of systematicity, timeliness, operability, scientificity, and flexibility. The data-centred system layers include the data management layer, data integration layer, data analysis layer, and data interpretation layer. Peng et al. (2016) used the fuzzy comprehensive evaluation method to quantify the risk assessment indexes. Based on the selected weight coefficients for measuring the early warning comprehensive score value of Internet financial risks, they determined the Internet financial risk early warning area. Then according to the set early warning area range, the authors propose the corresponding risk response strategy. This approach is consistent with the risk assessment method described above. Zhu et al. (2016)

used principal component analysis for dimensionality reduction and a binary logistic regression model to construct an early warning model for 40 private P2P platforms of Internet finance. Liu et al. (2017) proposed to establish a risk early warning system for the Internet financial service industry with multiple functions such as dynamic monitoring, forecasting and warning, and regulation and standardization. The system should be built according to the principles of scientificity, objectivity, practicality, and operability, and the system generally contains information collection, immediate detection, risk perception, risk prediction, early warning decision, forecasting and warning, risk prevention and control, early warning evaluation, and early warning feedback. The above literature has qualitative analysis of risk early warning design principles, hierarchy, etc., as well as quantitative analysis using the fuzzy synthesis method and principal component analysis.

2.3.6. Internet finance risk prevention

Xiong et al. (2014) proposed measures to strengthen risk prevention by analyzing the risks of Internet finance, firstly, to build a security system for Internet finance, including improving the operating environment of Internet finance and strengthening data management; secondly, to improve the business risk control system in the field of Internet finance; thirdly, to further strengthen the construction of regulations and institutions for risk prevention in the field of Internet finance. Chen et al. (2015) proposed risk control methods in terms of information security in the Internet financial field, specifically including firstly, improving the regulations in the Internet financial field and building a more complete regulatory system; secondly, making Internet financial companies improve their information management level and enhance the protection of information security; third, improve the construction of internal control system of Internet financial companies and enhance the concept of consumer and investor rights protection.

Zhao (2015) gave suggestions for Internet finance risk prevention from the perspective of legal risk prevention: first, standardize the existing financial regulations and improve the legal regulation of Internet finance in innovative business, so that the level of regulations in the field of Internet finance can be upgraded. Secondly, to absorb the scientific legislative experience of European and American countries in the Internet finance industry, improve the regulatory regulations of several Internet finance operation modes such as third-party payment, P2P network credit and electronic banking, and make some new regulations to adapt to the development of the industry. Third, improve legislation on consumer rights protection in the field of Internet finance. Fourth, build a coordinated protection mechanism for Internet finance.

Song et al. (2016) analysed the main risks of Internet finance and evaluated them according to the hierarchical analysis method, and concluded that the risk prevention countermeasures of Internet finance include these measures: establishing and improving the legal supervision and management system; promoting the construction of the real-name system in the field of Internet finance; constructing the industry customer rights protection system; strengthening the management of network platforms; strengthening the management of computer software and hardware systems, etc.

Wang (2013) argues that preventing Internet financial risks should include these measures: establishing sound policies and regulations and standardizing the management model; creating a high-quality environment and improving the quality of services; improving the construction of the credit system and protecting the rights and interests of consumers.

He (2014) argues from the case of BalancePay that the measures to prevent the risks of Internet finance should highlight the following points: the emerging things should be viewed critically from an objective and scientific perspective to protect and promote innovation in Internet finance; the relevant laws and regulations should be improved to make the development of the Internet finance industry more standardised; the financial regulatory system should be improved to adopt a comprehensive, integrated and dynamic regulation in the field of Internet finance; the internal risk management and risk control of BalancePay and the industry should be enhanced; risk publicity and education should be conducted for users of BalancePay. Bao (2013) makes the following suggestions for Internet finance risk prevention: establish an effective multi-party cooperative regulatory system; gradually build up a more complete regulatory system; improve access requirements and capital management; strengthen computer software and hardware system management; establish a sound consumer rights protection system.

Tong (2014) believes that Internet finance risk prevention should implement the following measures: strengthen the management of Internet finance and implement a strict market access system; clarify that the industry is against money laundering according to the universal and targeted principle, and any financial organization; focus on customer identification as the key point of supervision of the Internet financial industry; establish a suspicious transaction reporting system based on "reasonable suspicion"; establish an incentive and restraint mechanism to strengthen the enthusiasm of anti-money laundering work.

Wang (2014) proposes these specific measures to prevent risks in the Internet financial sector include: establishing a security system in the Internet financial sector; improving the risk control system in the Internet financial sector; promoting the construction of a risk regulation system in the Internet financial sector; improving the regulatory system in the Internet financial sector.

From the above-mentioned literature, we can categorise the recommended measures for preventing or minimising risks implemented in the Internet financial sector mainly through three aspects: one is the government level, mainly through the construction of regulatory institutions and laws and regulations, etc.; the second is the institutional level, mainly through their compliance operation and management, internal security system construction, and increased investment in advanced technology; the third is the investor level, mainly through strengthening investor education, investors' own risk awareness, investors to improve the skills of using the Internet, consumer and investor rights protection, etc.

2.3.7. Internet financial risk disposal

Yuan and He (2015) studied the disposal of non-performing assets in the banking industry under the model innovation based on the Internet. They argue that "Internet+" should be used as a guide to strengthen the construction of a professional network trading platform for non-performing assets, to give play to the platform effect, to connect the resources and demands of various parties, and to improve the efficiency of non-performing asset disposal. Li (2016) made a typological analysis of the main industry and endogenous criminal legal risks of Internet finance, and from the perspective of the legislative system of Internet finance, the design logic of the legal liability system, the orientation of the criminal law system, the fault of the victim, the legal measures for the disposal of Internet financial risks are proposed The problem of Internet financial risk disposal has both theoretical and practical significance, and it is necessary to study it in depth and propose feasible solutions.

2.3.8. Regulation of Internet finance

Wu (2013) argues that the regulation implemented in the field of Internet finance, as long as it involves the interests of the general public, must be licensed, and according to these licenses, they should be strictly regulated, and the other parts should be properly controlled and targeted.

Xie and Ping (2014) put forward the necessity, generality, specificity, consistency and difference of the regulation of Internet finance. Although its development is not mature, the regulation of Internet finance should not be lax and should promote the development of the industry through regulation, and should promote industry innovation under the constraints of bottom-line thinking and regulatory ceiling. The universality of regulation shows that traditional financial risks and externalities still appear intensively in the Internet finance field at present, and the problems of damaged legitimate rights and interests of consumers in the Internet finance industry are still occurring. Therefore, the regulation of Internet finance is different from that of traditional finance in terms of underlying principles. Macro-prudential and behavioural regulation, as well as the protection of consumers' interests are still applicable at present. Because the Internet finance sector is riskier in terms of information technology, and the possible long-tail risks are more likely to put the legitimate rights and interests of consumers at greater risk, it is necessary to provide better and more targeted protection. This is the specificity of regulation. The consistency of regulation is that if an Internet financial enterprise has a certain function in traditional finance, it can be regulated by applying the regulatory measures of traditional finance. If different types of Internet financial enterprises operate the same type of business and raise the same type of risk, theoretically, a consistent regulatory approach can be adopted. The variability in the regulatory field is manifested in the different categories of Internet financial organizations. Different measures are applied to different risks based on the classification principle of risk identification, but if the business approached is mixed, there is a need to enhance the coordination within the regulatory system.

Zhang (2014) proposes several principles for Internet finance regulation: appropriate risk tolerance limits should be reflected; dynamic weighting controls should be adopted; a combination of normative and institutionalised regulation; regulatory arbitrage should be avoided and the overall nature of regulation should be emphasised; systemic risks should be emphasised and predicted; a comprehensive data monitoring and analysis system should be constructed; violations in the field should be strictly punished; information disclosure should be improved to enhance the market; the Internet financial companies need to maintain smooth, good and meaningful communication with the regulatory organisations in the financial sector; enhance consumer education and strengthen consumer protection; enhance industry self-regulation; and strengthen regulatory coordination.

Ba et al. (2012) conducted a comparative study on the international regulation of third-party payments and made suggestions to improve the regulation of third-party payments in China. These suggestions are improving third-party payment regulatory legislation, establishing a classification and dynamic regulatory system, striking a balance between scale and development, establishing a relatively flexible reserve fund regulatory system and protecting the legitimate rights and interests of consumers, etc.

Li et al. (2014) set out the main regulatory ideas of Internet finance are: localisation of regulatory bodies, guideline-oriented control instruments, and establishment of a "safe harbour" system including a membership invitation system, third-party management of funds system, information disclosure system and information security protection system, etc.

Zheng (2014) proposes specific regulatory opinions in the field of Internet finance: strengthen the prevention of risks specific to the Internet finance industry; pay attention to the risk spillover consequences of the industry on the traditional financial system; adhere to the risk management bottom line of no systemic or local risks; recognise the systemic mismatch of the regulatory model; protect the consumer rights and interests and information security; comprehensively deepen the reform; and gradually build a more comprehensive and scientific financial market mechanism.

Gao (2014) puts forward suggestions related to the construction of the regulatory legal system in the field of Internet finance: establishing a credit collection system for Internet finance enterprises; implementing a business license system for Internet financial enterprises; establishing a dispute redress system; formulating regulatory rules and self-regulatory guidelines for the Internet finance industry.

Wu (2014) points to the preferred direction of Internet finance regulation: achieving moderately innovative financial regulatory instruments; highlighting security and coordination as well as stable regulation; enhancing self-regulation of the whole industry; enhancing the protection of market participants. He also suggests the following regulatory paths: building an orderly and effective regulatory system; establishing a sound system of laws and regulations; strengthening industry self-regulation and standardising industry behaviour; strengthening financial monitoring and macro-control, and improving the anti-money laundering system; establishing and improving the credit collection system, and the allocation efficiency of scarce financial resources; strengthening the protection of the rights and interests of market participants, and enhancing the intensity of social supervision; improving the tax collection and management system; strengthening international exchanges and cooperation.

Feng (2013) proposed several measures in the field of regulation: improve the regulatory system in the field of Internet finance; establish multiple levels within the Internet finance regulatory system; strengthen the protection of the rights and interests of Internet finance consumers.

Zhang (2016) proposes to build a regulatory system that adapts to the development characteristics of the Internet finance industry. It includes upholding the principle of targeted regulation, enhancing the functional regulation of the Internet finance industry, and strengthening the role of industry associations, so that they can perform more self-regulatory duties.

There are still some gaps in the current research, which should be improved. First, the application of economics and financial theories needs to be further improved. Most of the contents in terms of risk causes, risk transmission, risk type identification and supervision are summarized based on the development phenomenon of Internet finance, not based on economic theories, financial theories and management theories. As a result, the research lacks theoretical foundation, comprehensiveness and systematicness. Second, few scholars have made a comparative analysis of the differences between the risks in the Internet finance field and the traditional finance field. Although Internet finance is a new thing, its development is based on traditional finance. For the analysis of Internet financial risk management, by comparing with traditional financial risks it can be found the core of the problem and analyze the essence. Third, most of the research content is normative analysis, and there are very few empirical studies. The main reason is the lack of industry statistics and cases. However, risk assessment, risk early warning, risk disposal, etc. belong to the category of quantitative analysis, and need to used by empirical analysis. Fourth, the view of research is relatively single. Most of the research literature is analyzed from a certain aspect, mostly focusing on independent aspects such as risk causes, type identification, prevention and supervision, lack of research on risk transmission, early warning and disposal.

CHAPTER 3: APPLICATION OF INNOVATIVE RISK EARLY WARNING MODE UNDER BIG DATA TECHNOLOGY IN INTERNET CREDIT FINANCIAL RISK ASSESSMENT

Preface

In the era of big data, it is aimed to use big data technology to form an effective early warning and prevention of Internet credit. The BP neural network algorithm is applied to determine the number of nodes, activation function, learning rate, and other parameters of each layer of the BP neural network. Also, many data samples are used to build an early warning model of Internet credit risk. The constructed model is trained and tested. Finally, the genetic algorithm (GA) is used to optimise the neural network to improve the accuracy of early warning. The results show that based on 450 data samples from 90 enterprises over five years and the risk interval divided by the "3σ" rule, the Internet credit risk level is initially determined. Then, the neural network is trained and tested. The network output rate is as high as 85%. To avoid the defect of the BP neural network falling into local extreme value, GA is used to optimise the neural network. The warning is more accurate, and the error is smaller. The accuracy rate can reach 97%. Therefore, the use of BP neural network for early warning and assessment of Internet credit risk has good accuracy and computing efficiency, which expands the application of BP neural network in the field of Internet finance, and provides a new development direction for the early warning and assessment of Internet credit risk.

CHAPTER 4: FINANCIAL RISK ASSESSMENT TO IMPROVE THE ACCURACY OF FINANCIAL PREDICTION IN THE INTERNET FINANCIAL INDUSTRY USING DATA ANALYTICS MODELS

Preface

The purpose is to explore the role of ML and DL algorithms in Internet credit risk assessment and improve the accuracy of financial prediction. First, the problems in the current Internet financial risk assessment are understood, and data from MSE are chosen for analysis. Then, a feature extraction method based on ML is proposed to solve data redundancy and interference in enterprise credit risk assessment. Finally, to solve the data imbalance problem in the credit risk assessment system, a credit risk assessment system based on the DL algorithm is introduced, and the proposed credit risk assessment system is verified through a fusion algorithm in different models with specific enterprise data. The results show that the credit risk assessment model based on the ML algorithm optimises the standard algorithm through the global optimal solution. The credit risk assessment model based on DL can effectively solve imbalanced data. The algorithm generalisation is improved through layer-by-layer learning. Comparison analysis shows that the accuracy of the proposed fusion algorithm is 25% higher than that of the latest Convolutional Neural Network(CNN) algorithm. The results can provide a new research idea for the assessment of Internet financial risk, which has important reference value for preventing financial systemic risk.

CHAPTER 5: FINANCIAL NETWORK TRANSACTION RISK CONTROL BASED ON EDGE COMPUTING AND BLOCKCHAIN TECHNOLOGY

Preface

This exploration intends to solve the great security risks in the financial network transaction process and the certain restrictions on the current use of blockchain technology in mobile terminal equipment. First, the concepts of blockchain technology and Edge Computing (EC) are described. Next, an anonymous storage protocol for financial network transaction data and a trusted data synchronization system based on blockchain technology and EC are proposed. It is expected that these two methods can improve the security of financial network transactions to a certain extent. Finally, the experiment is designed to verify the protocol and the system's performance. The experimental results show that the anonymous storage protocol of financial network transaction data greatly reduces the time cost for information encryption transmission. Besides, it can effectively resist external attacks, EC device attacks, Man-in-the-Middle attacks and replay attacks, with high security. The system's Round-Trip Time (RTT) is lower than the average human response time, and the system has no obvious delay, showing good performance. Both full data synchronization and incremental synchronization are better than the file distribution function module based on Peer to Peer (P2P) network, which is suitable for data synchronization with a small sampling rate. This exploration provides a reference for the research of multi-node trusted data synchronization across multiple security domains and the risk control methods of Internet financial transactions.

5.1. Introduction

The progress of Internet finance has a diversified trend. The development modes in China mainly include Peer to Peer (P2P) online lending, public financing, third-party payment, big data finance and information-based financial institutions. They are still in the embryonic stage. Their potential risks gradually emerge with the blowout development . The potential risks of Internet finance are divided into internal risks and external risks. Internal risk mainly refers to the enterprise's own operational risk, and external risk mainly includes legal risk, credit risk, network technology risk and market risk . The technical risks of Internet financial services mainly focus on data transmission, financial application systems and viruses. If the data transmission system is damaged, massive personal information of users will be leaked, which will threaten the security of funds. The previous identity authentication in financial network transactions mainly depended on the storage and authentication of a third party, and there were hidden dangers of information disclosure caused by a third party. Blockchain technology is a technical scheme that does not rely on a third party and carries out network data storage, verification, transmission and exchange through its own distributed nodes, which provides a new idea for improving the security of financial network transactions. There have been many research results combining blockchain technology with network security.

Gupta et al. (2019) pointed out that the adaptability of cloud computing grew rapidly at this stage, but the concerns about information security were not fully addressed. The information security problem still hinders the development of cloud computing to a certain extent and needs to be solved. Besides, blockchain has become a key technology to provide security, especially in terms of integrity, authenticity and confidentiality. Adiyanto and Febrianto (2020) pointed out that the trading process turned into a digital trading process through the Internet. The digital transaction process requires accuracy, security and good trust between the buyer and the seller. Blockchain technology can maintain transaction process, maintain management efficiency, identify identity, track system implementation, identify product authenticity, and synchronously record data of all parties. It is expected to increase the trust and relationship between buyers and sellers. Hosen et al. (2020) proposed a verification protocol for secure distributed Internet of things (IoT) transactions based on blockchain technology. In addition, the software-defined networking gateway was used as the middleware between the IoT and blockchain network to ensure the control operation and security of large-scale networks. Yu and Wu (2018) believed that blockchain technology was actually a distributed database technology. It adopts a series of security technologies such as P2P network technology, asymmetric encryption technology and smart contract technology to ensure the security and reliability of transactions. It has the advantages of decentralization, anonymity and traceability. Given the problems existing in the current centralized network transaction mode, they proposed a design scheme of "network transaction system based on blockchain technology", and proposed a safe and feasible network transaction system model to ensure the security of transactions in network data transmission and data processing. Perez et al. (2018) proposed an improved sha256 security protocol for the blockchain mechanism, which protected the online transaction process based on the blockchain mechanism through the smart contract. It focuses on optimizing security protocols specially designed for the practical application of blockchain, especially privacy and trust. With the increasing number of smartphones and other terminal devices, more and more people choose to carry out financial transactions on portable terminal devices. However, the computing power of these devices is relatively weak and cannot perform complex encryption and decryption operations. Therefore, Edge Computing (EC) technology comes into being. It refers to an open platform integrating network, computing, storage and application core capabilities on the side close to the terminal equipment to provide the nearest end services. Its application program is initiated on the edge side to produce faster network service response and meet the basic needs of the industry in real-time business, application intelligence, security and privacy protection. Yang et al. (2019) proposed that the introduction of EC was to expand cloud resources and services to be distributed at the edge of the network. However, it faces challenges in its decentralized management and security. Integrating blockchain and EC into one system can realize reliable access and control of the network, storage and computing distributed at the edge to provide large-scale network server, data storage and validity calculation near the end in a secure way .

The above existing research shows that present blockchain technology research in network security has been relatively mature. However, due to the functional defects of the intelligent terminal device itself, there are still some restrictions on the use of blockchain. Moreover, the feasibility of the combination of blockchain technology and EC technology has not been further analyzed and studied. Based on the above problems, an anonymous storage protocol for financial network transaction data based on blockchain technology and EC is proposed. The protocol can generate a false identity for the terminal equipment and use the false identity to protect the real identity to protect the corresponding relationship between identity and data and improve the privacy protection of financial network transactions. Next, a trusted data synchronization system based on blockchain technology and EC is proposed to enhance terminal data security, improve data synchronization efficiency, and strengthen the channel's credibility to prevent information leakage in data transmission. Finally, the experiment is designed to analyze the security of the anonymous storage protocol for financial network transaction data based on blockchain technology and EC in detail. The performance of the trusted data synchronization system based on blockchain technology and EC is tested. This exploration provides a certain reference for the secure storage of real information of mobile terminals and the technical risk control of financial network trading business.

5.2. Anonymous storage protocol design and construction method of the data

synchronization system

The information network itself has multiple unsafe factors of data tampering and destruction. It is necessary to enhance the security credentials of the transactions' operating system, customer information database and transaction communication protocol, and manage network security to reduce Internet financial risks. Data encryption transmission of client devices, EC devices and blockchain is studied to improve the safety of Internet financial transactions. Figure 5.1 displays the research route.

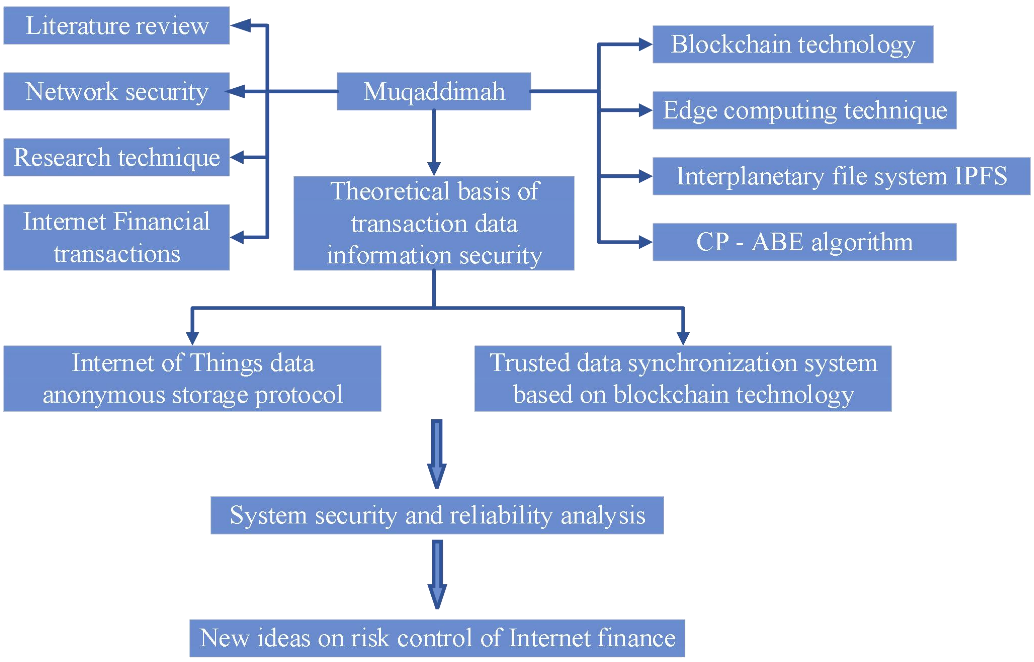

Figure. 5.1 Research roadmap

5.2.1. Overview of blockchain and EC

(1) Blockchain technology

Blockchain is essentially a public distributed database, in which data can be accessed and shared by nodes. However, new blocks need to be linked to the end of the blockchain through the consensus mechanism, and any single node cannot control the blockchain data . Figure 5.2 is the infrastructure diagram of blockchain, which is composed of three layers: basic network layer, intermediate protocol layer and application service layer.

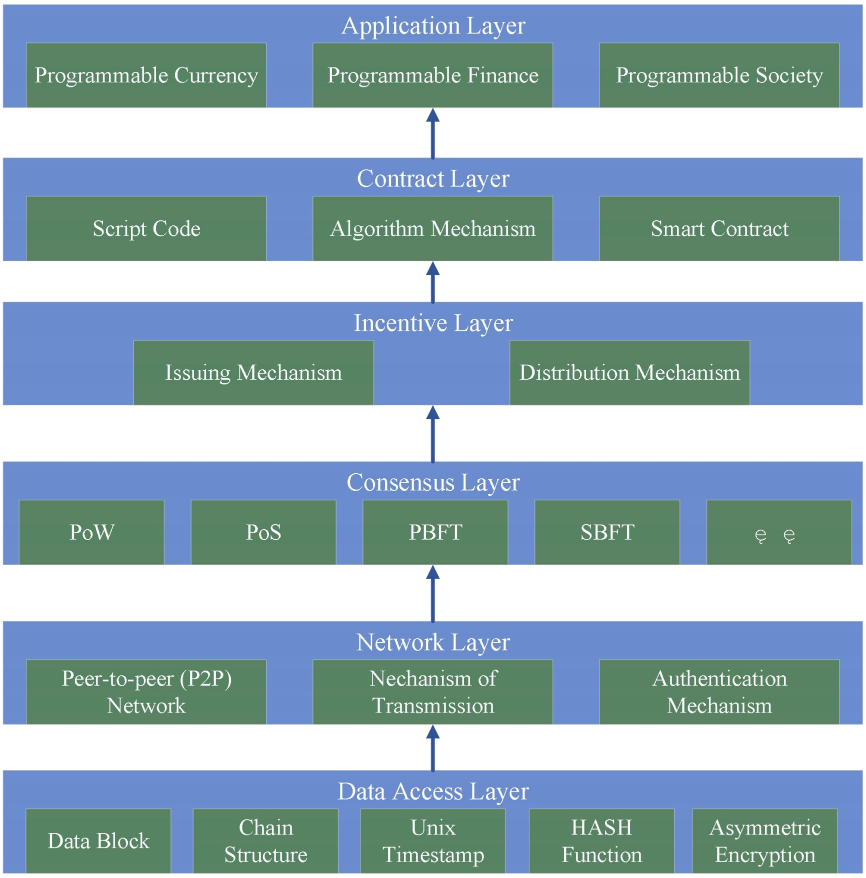

Figure. 5.2 Infrastructure of blockchain

(2) EC technology

The data generated by the client device shows an exponential growth trend. The Edge Computing Platform (ECP) can quickly expand the cloud computing capabilities such as stored big data, artificial intelligence and privacy processing to the edge node closest to the data source of the client device to ensure real-time task processing . Figure 5.3 is the framework of ECP.

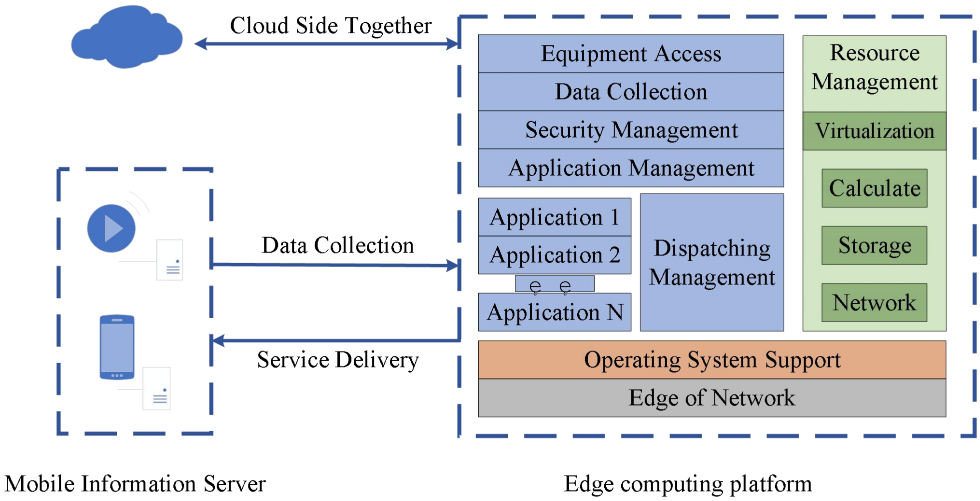

Figure. 5.3 The framework of ECP

In the ECP framework, the resource management module mainly carries out the calculation of edge networks and the management of stored data. The device access and data acquisition module functions provide a data source for relevant data processing of subsequent EC devices. The platform management module manages the EC device itself, and detects and controls the clients running on it.

5.2.2. Design of anonymous storage protocol for financial network transaction data based on blockchain technology and EC

An anonymous storage protocol combined with EC and the cryptographic algorithm of blockchain is set up to protect the real information of customer terminals and their corresponding data in Internet financial transactions. This protocol can generate corresponding false information according to the customer terminal information to protect the customer, which can hide the relationship between the customer's real information and the corresponding relevant data. Figure 4 shows the protocol model.

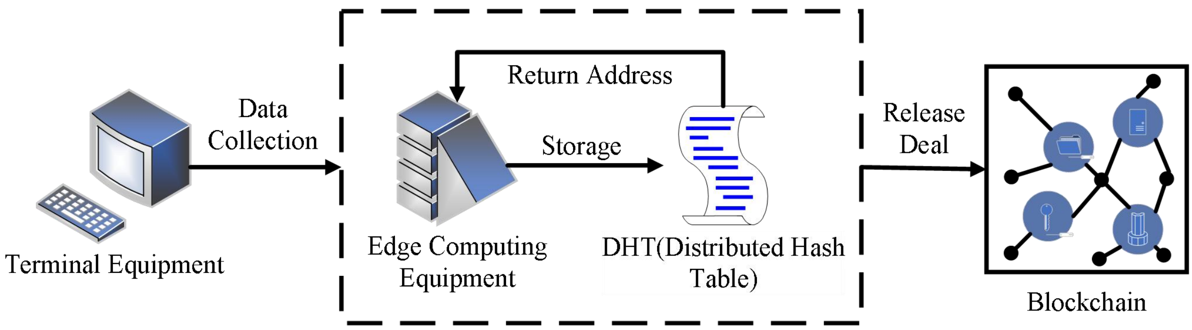

Figure. 5.4 Data anonymous storage protocol model

Figure 5.4 displays that the anonymous protocol comprises terminal equipment, EC equipment, and blockchain . Among them, blockchain technology mainly uses Ethereum open-source platform. As the data generator, the terminal device can be some sensors or intelligent devices with a data collection function. The computing power of these devices is relatively weak and cannot perform complex encryption and decryption operations. The protocol introduces the EC device to solve this problem. The EC device has strong computing power, low transmission delay, and high real-time performance and is closer to the terminal device in position. It is suitable to help the terminal device generate a false identity. The protocol assumes that there is a secure channel between the terminal device and the EC device for communication between both parties, and the EC device is trusted. After the EC device generates a false identity for the terminal device, the false identity will replace the real identity to be stored in the local database with the data. Each data's address in the local database will be stored on the blockchain because of the advantages of the decentralized, tamper-proof and traceable blockchain. Meanwhile, the corresponding relationship between false identity and real identity is also saved and stored on the blockchain for later proof and traceability.

The anonymous storage protocol proposed realizes anonymous storage by generating a false identity for the terminal device. The starting point of constructing the false identity generation algorithm is that the false identity can protect the real identity and reverse it through the false identity when necessary. Therefore, the mapping relationship between false identity and real identity is also the focus of the protocol to be protected. In addition, the data generated by the terminal device also need to be encrypted and stored. According to the requirements, the data anonymous storage protocol designed includes three algorithms:

(1) False information generation algorithm:

The specific algorithm is designed based on the ElGamal signature algorithm [16], and the process is as follows.

1) The EC device randomly selects a single hash coefficient $H()$ and a prime number p that meets the security requirements to generate a generator $g \in Z_p$ of the group Z_p of order p. The parameters p and g are disclosed. A public-private key pair PK_X/SK_X is generated, which is used to encrypt the subsequently generated random number X.

2) The client device generates a unique identity $Xid_i(1 \leq i \leq n)$. i is the current device

identity and n is the number of client devices. The client and EC devices jointly negotiate to generate two random numbers X and Y ($X \in Z_p$, $Y \in Z_p$). The client device sends Xid_i and random number Y together to the EC device, and the latter encrypts the random number X and returns it to the client device.

3) After receiving Xid_i and Y, the EC device calculates $g^{H(X)\cdot Y}$.

The public-private key pair of false information generated by the client device is:

$$PK_{pse} \equiv g^{H(Xid)} \cdot g^{H\left(g^{H(X)\cdot Y}\right)} mod\, p = g^{H(Xid)+H\left(g^{H(X)\cdot Y}\right)} mod\, p \tag{1}$$

$$SK_{pse} \equiv H(Xid) + H\left(g^{H(X)\cdot Y}\right) \tag{2}$$

4) The EC device divides the identity Xid of the client device into n groups, and the length of each group is l:

$$Xid = Xid_1 Xid_2 ... Xid_n \tag{3}$$

The EC device selects the random number y_i ($1 \le i \le n$, $1 \le y_i \le p$-1) for each group of Xid_i of the client device and calculates the corresponding ciphertext $e_i/e_i^{'}$.

$$e_i \equiv g^{y_i} mod\, p \tag{4}$$

$$e_i^{'} \equiv Xid_i \cdot {PK_{pse}}^{y_i} mod\, p \tag{5}$$

5) The false information $PseID$ of the client device is:

$$PseID = \left(e_1, e_1^{'}\right)\left(e_2, e_2^{'}\right)...\left(e_n, e_n^{'}\right) \tag{6}$$

6) The process of tracing real information through false information is:

SK_{pse} is adopted for calculation:

$$Xid_i = \left(\frac{e_i^{'}}{e_i^{SK_{pse}}}\right) mod\, p \tag{7}$$

The obtained Xid_i is combined into a complete Xid:

$$Xid = Xid_1\, Xid_2 ...\, Xid_i \tag{8}$$

After the traceability phase is completed, the EC device stores the mapping relationship between $PseID$ and Xid in the blockchain as:

$$Mapping = \langle\, PseID, Xid \,\rangle \tag{9}$$

(2) Symmetric key design algorithm:

After the client device generates false information, the symmetric encryption algorithm is adopted to encrypt the original data O generated by the client to reduce the computing pressure of the EC device. Part of SK_{pse} is selected as encryption key C:

$$C = H\left(g^{H(X)\cdot Y}\right) \tag{10}$$

In the subsequent transaction protocol, the client device can use the encryption of the solution of C value to verify the authenticity of the output data of the edge device.

(3) Data encryption algorithm:

After generating the encryption key, O, $PseID$ and timestamp Ts are input, and ciphertext E is output:

$$E = En_C(O, PseID, Ts) \tag{11}$$

En_C is a symmetric encryption algorithm. The encrypted ciphertext E will be marked by $label$ to identify its data type.

Each group of data will be stored in the database, and the storage object reads:

$$Storage\ Object = \langle E, PseID, label, Ts \rangle \tag{12}$$

The data will return the $Address$ to the edge device, and the edge device will sign and transmit it to the blockchain for storage. In subsequent transaction protocols, the $Address$ can quickly obtain data through addressing. Transaction format T_{Edge} is:

$$T_{Edge} = (Address, Ts, label) \parallel Sign_{sk}\left(T_{Edge}\right) \tag{13}$$

sk is the private key of the EC device itself, and $Sign_{sk}$ refers to signing data transactions with the private key sk.

5.2.3. Construction of trusted data synchronization system based on blockchain technology and EC

In information transmission, a trusted data synchronous transmission system based on blockchain technology is designed to ensure the safety and reliability of communication channels of client devices, EC devices, and blockchain during interworking. First, blockchain technology, EC technology, Inter Planetary File System (IPFS) and Ciphertext Policy Attribute Based Encryption (CP-ABE) are briefly introduced.

(1) IPFS

The centralization efficiency of the Hyper Text Transfer Protocol (HTTP) is low and the running cost of the protocol is high. It defines the content-based addressing file system. Common technologies include distributed hash, P2P transmission, and version management systems, which store and access files, websites, applications and data . IPFS addresses the file through the content in the file, which can verify the required data content. Figure 5.5 shows the related technologies of the IPFS protocol.

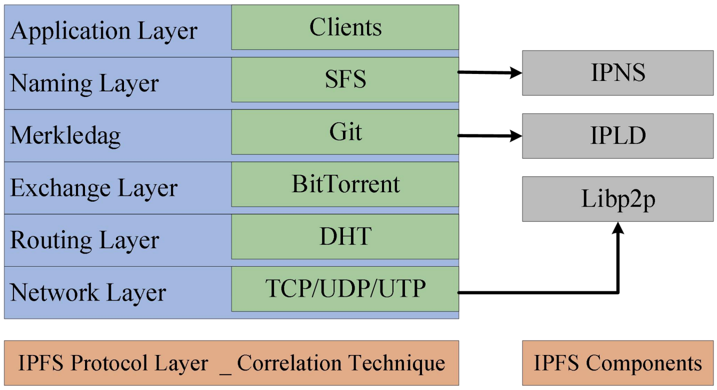

Figure. 5.5 IPFS protocol related technologies

The basic idea of IPFS is to change the communication mode between human and computer networks. It has multiple characteristics, such as a standardized data model, independent protocol, upgrade with multi-format support, cross-format interoperability, backward compatibility, and protocol space disclosure.

(2) CP-ABE algorithm

In practical application, ciphertext encryption can be understood as that the client obtains the key from the attribute organization according to its own characteristics or attributes. Then, the encryptor formulates the access control of the message. Decryption can only be performed if and only if the attributes in the attribute set can meet the access structure. The CP-ABE algorithm process includes setting, encryption, key generation, and decryption . The specific process is as follows:

1) Initialization setting: the hidden security parameter a is input. The public parameter PK and master key MSK are output.

2) Encryption steps: the message m to be encrypted, the access control structure T and the public parameter PK are input. The ciphertext E of m is output. Only the client that meets the requirements of access control structure T can decrypt E and obtain the corresponding real information m.

$$Encrypt\ (PK, m, T) \rightarrow E \tag{14}$$

3) Key generation: public parameter PK, master key MSK and User Attribute Set (UAS) are input. The client's private key USK is calculated and output.

4) Decryption steps: the public parameter PK, ciphertext E and client private key USK are input. If $UAS \in T$ is satisfied, the algorithm outputs E corresponding to the real information m.

$$Decrypt(PK, E, USK) \rightarrow m \tag{15}$$

(3) Basic framework of the trusted data synchronization system

The system selects rsync command and Decentralized Identity (DID) technology to assist the system construction and solve the synchronous data transmission between edge nodes of multiple security domains and the existing security risks . The rsync command can mirror-save the entire directory tree, file system, permissions and links of source files and other information for cross-platform data synchronous transmission, such as between Windows system and Linux system. The blockchain and rsync commands build a data synchronization system. The blockchain and DID perform edge service identity authentication across multiple security domains. Figure 5.6 displays the basic structure of the trusted data synchronization system.

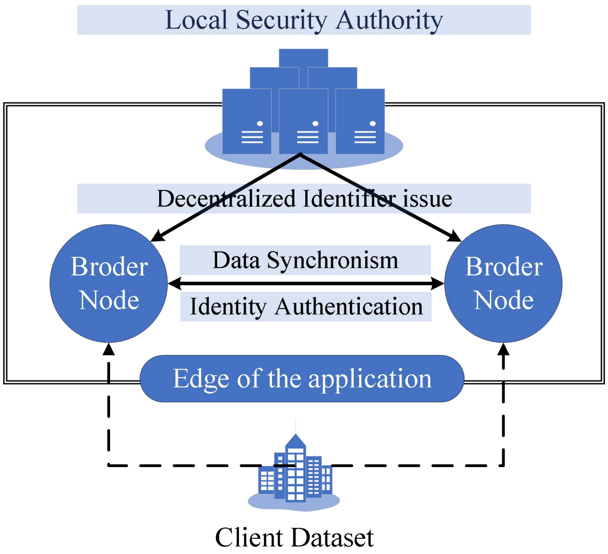

Figure. 5.6 Basic structure of trusted data synchronization system

The system mainly includes four levels: application entity, function module, network encryption protocol and blockchain database. CP-ABE algorithm, DID authentication algorithm, and rsync tool support the protocol's operation. It relies on the existing mature Hyperledger Fabric ultra-long ledger framework to form a blockchain, allowing the various modular functional structures' insertion and extraction . Only DID documents, Verifiable Credential (VC) and corresponding IPFS storage addresses are stored. Figure 5.7 displays the specific hierarchical structure of the system.

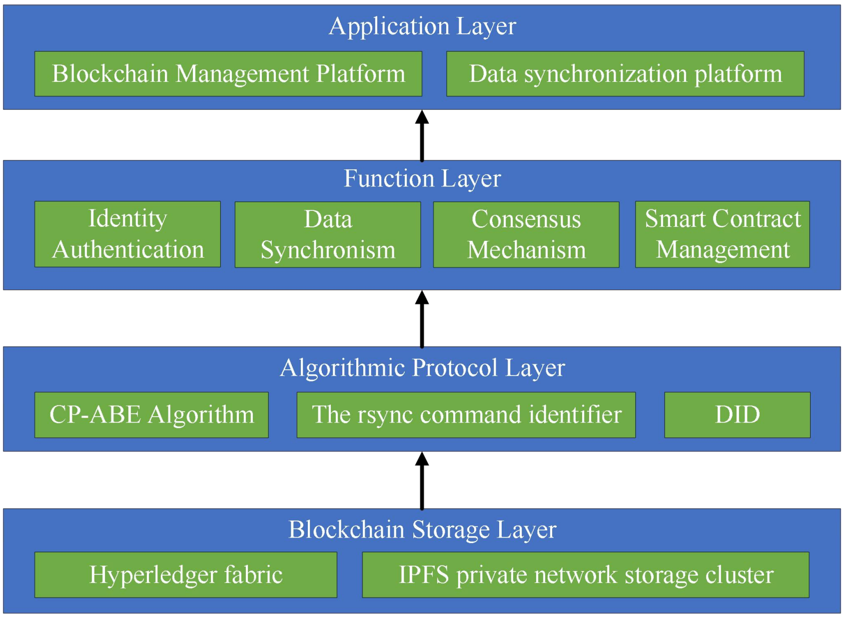

Figure. 5.7 Trusted data synchronization system hierarchy

(4) Workflow of the trusted data synchronization system

The workflow is divided into identity registration, authentication, and data synchronization.

1) DID registration:

The Setup() method is executed to provide resource support for subsequent tests and generate *PK* and *MSK*. The key generation method is used to generate the private key of the EC device . When the EC device applies for DID, the authorized gateway makes attribute judgment. If the application conditions are met, it will generate its own DID, service certificate and public key of authorization gateway, and call the server interface to generate DID document. Documents and vouchers are stored on IPFS, and their own IDs and corresponding hash addresses are stored in the blockchain.

2) Identity authentication: the client device provides its own DID documents, credentials and other authentication expressions to the EC device. The EC device verifies its attributes, obtains the IPFS address of the client, downloads the corresponding copy file, converts the original file, and verifies the expression according to the public key. After verification, the EC device provides services for the client device. The structure of identity authentication smart contract mainly includes EsDiddoc structure and EsDidvc structure:

Table 5.1 introduces the attributes, data types and other information of the EsDiddoc structure:

Table. 5.1 EsDiddoc structure

Attribute	Types	Introduction
EsDiddoc_Dids	String	ID of user DID document
EsDiddoc_ Ipfsaddr	String	The address where the DID document is stored in the IPFS private cluster

Table 5.2 introduces the attributes, data types and other information of EsDidvc structure.

Table. 5.2 EsDidvc structure

Attribute	Types	Introduction
EsDidvc_Id	String	ID of the user edge service verifiable credential
EsDidvc_ Ipfsaddr	String	The address where the edge service verifiable credentials are stored in the IPFS private cluster

3) Data synchronization: the edge node publishes the data synchronization task and stores the task information in the blockchain. The EC device terminal receives the task, and rsync command sends the checksum list of old files to the data synchronization terminal. The data synchronization end obtains the difference data. The synchronization terminal calls the difference data interface at the data synchronization source end to obtain the matching information and difference data of the old and new files at both ends, and stores the call log of the difference data of the service interface in the blockchain. The data synchronization end calls the terminal reorganization interface to complete data synchronization. Figure 5.8 presents the workflow of the system.

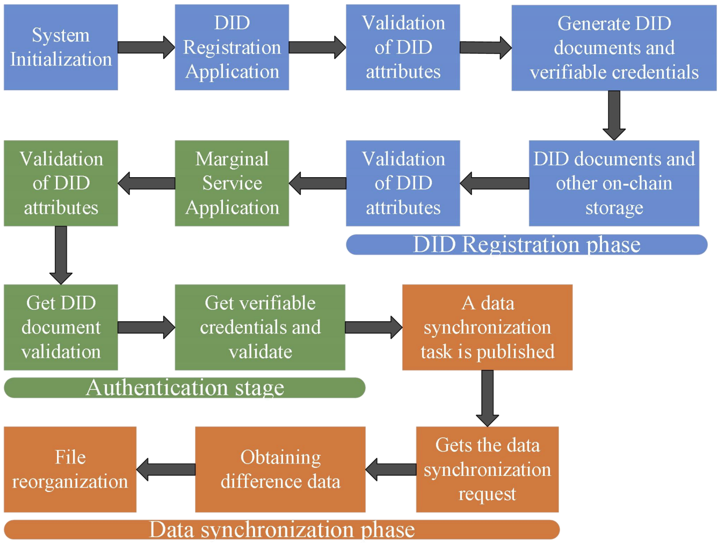

Figure. 5.8 Workflow of the trusted data synchronization system

5.2.4. Experimental design

(1) Security analysis of anonymous storage protocol for IoT data

The computational cost and complexity of the proposed protocol are evaluated and analyzed in two parts. $Cost_{add}$, $Cost_{mui}$ and $Cost_{index}$ are used to represent the cost of one-time modular addition, modular multiplication and modular exponentiation. $Cost_{hash}$ indicates the time required to operate the hash function once.

(2) Time cost analysis and operation test of the trusted data synchronization system

1) Test results of workflow Round-Trip Time (RTT) of the trusted data synchronization system

Round-Trip Time (RTT) is used to evaluate the system's availability in practical applications. Two hardware platforms, desktop of Windows system and Rsapberry Pi 4 of Linux system, are selected for testing, and compared with human reaction time.

2) Multi-node cooperative experiment

A multi-node cooperation experiment is conducted under the condition of a stable network. The experiment selects two platforms: a multi-node edge environment and a cloud computing center to detect the time required to complete the task process under the experimental condition that the camera acquisition frequency increases linearly from 1 frame per second to 10 frames per second.

(3) Performance test of the trusted data synchronization system

1) Performance test of blockchain

Hyperledger caliper, a blockchain performance testing framework, is used to test the performance of the Hyperledger fabric framework. During the test, Tx Number is set to 1000, 2000, 5000, 10000 and 15000, respectively.

2) Performance test of full data synchronization (one-time synchronization of all data)

The unified network conditions are controlled. The test scenario is that one data synchronization source is synchronized to three data synchronization terminals. The file sizes are 1M, 5M, 10M, 50M, 100M, 200M, 250M and 500M, respectively. The system data synchronization module proposed and the file distribution function module, Base Transceiver Station-Power Device (BTS-PD) based on the P2P network, are selected for the data synchronization test.

3) Incremental synchronization performance test of data

The specified test scenario is that one data synchronization source is synchronized to one data synchronization terminal. The experimental simulation background is the incremental synchronization of folders and files between edge nodes across multiple security domains. First, the performance of folder incremental synchronization is tested. The file sizes contained in the folder are 100K, 1M, 10M, 100M, 500M and 1G, respectively. rsync synchronization and BTS-PD synchronization are used to synchronize the folder to the terminal, respectively, and 10K files are added for the second time to synchronize again. Then, the performance of file incremental synchronization is tested. Under the same experimental conditions and background, 10M, 50M, 100M, 250M and 500M files are synchronized to the terminal. The subsequent operations are the same as above.

(4) Development environment

Table 5.3 shows the specific development environment required for this experiment.

Table. 5.3 Development environment

Items	Tool
System environment	Windows 10 x64
Blockchain dependency	Ethereum geth v1.8.3
Database	MySql 5.6
Smart contract development language	Solidity v0.4.24&Web3j v4.2.0
Cryptography development library	Bouncycastle v1.45
Web development language	Java Development Kit 8
Web service framework	Spring-Boot 2.0.6-REALEASE

The system is developed in the windows system environment. The system is portable, so it can also be transplanted to the Linux system. Meanwhile, the Web framework uses Java language to develop applications.

5.3. Results and discussion

5.3.1. Security analysis results of anonymous storage protocol for IoT data

(1) Cost analysis results of anonymous storage protocol for IoT data

The running cost of the anonymous storage protocol of IoT data is $3Cost_{hash}+Cost_{add}+2Cost_{mui}+4Cost_{index}$ in the false information generation stage. In the symmetric key generation stage, it is $2Cost_{hash}+Cost_{mui}+Cost_{index}$. The comparison reveals that in the symmetric key, the modular addition operation is reduced, and the cost of modular multiplication, modular power and performing a hash function is lower than that in the false information generation stage, which significantly reduces the time cost. The reason should be that the symmetric key is generated based on false information and key extraction.

(2) Safety analysis

The data anonymous storage protocol proposed can generate false identities for terminal equipment to protect the corresponding relationship between real identity and data. It can safely and continuously protect the device data generated by the terminal device. This section lists several possible attack modes in the scenarios where this protocol is applicable, and analyzes the security attributes of the protocol.

1) Resist external attacks

An external attack is that the attacker obtains the device data generated by the terminal device and the identity of the terminal device by eavesdropping on the communication channel. In the protocol proposed, the identity of the terminal device is replaced by a false identity, and the device data collected by the edge device are encrypted. Hence, it can effectively resist external attacks.

2) Resist attacks from the EC devices

This attack means that an attacker forges an EC device and uses it to imitate a legal EC device to obtain the data and real identity of the terminal device and trade with the blockchain. In the proposed protocol, the EC device attaches its own signature when sending transactions to the blockchain, preventing external attackers from counterfeiting their identity to trade with the blockchain.

3) Resist Man-in-the-Middle attacks

The man-in-the-Middle attack is to cheat the receiver of the message by imitating the legitimate sender of the message. In the encryption key generation stage, it is assumed that the attacker imitates the EC device and generates an encryption key to encrypt the device data and send it to the blockchain. The terminal device can check its authenticity at this time, because the edge device has previously obtained the random number constituting the encryption key. Therefore, the edge device can use the correct encryption key to decrypt its encrypted data to resist Man-in-the-Middle attacks.

4) Resist replay attacks

Replay attack means that the attacker deliberately sends a packet that the destination host has received to deceive the host. In the protocol proposed, when the data address is published to the blockchain, a timestamp will be attached to prevent the attacker from replay attacks. If the attacker wants to modify the timestamp in the transaction, the attacker must obtain the private key of the EC device, which the attacker cannot do. Therefore, this protocol can resist replay attacks. To sum up, the anonymous storage protocol of financial network transaction data based on blockchain technology and EC proposed has high security and is suitable for use in financial network transactions.

5.3.2. Time cost analysis and operation test results of the trusted data synchronization system

Figure 5.9 and Figure 5.10 are RTT results and multi-node cooperation experiment results. According to the test records of the background of the Human Benchmark website, the statistical analysis shows that the average human response time is 215ms. If the RTT of the experimental result is less than 215ms, the trusted data synchronization system has no obvious delay in the actual function operation, and the system has certain availability.

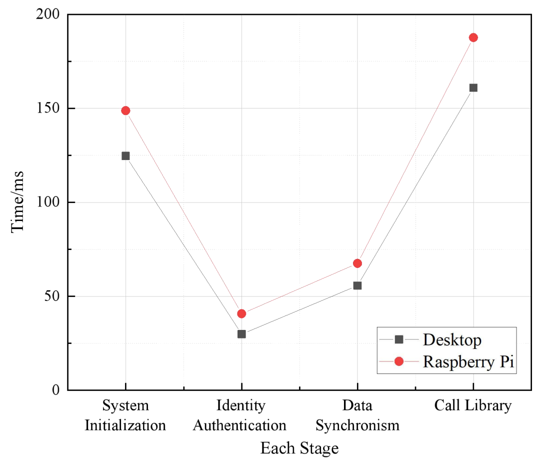

Figure. 5.9 Statistical diagram of average time consumption of each step of the system on

different hardware platforms

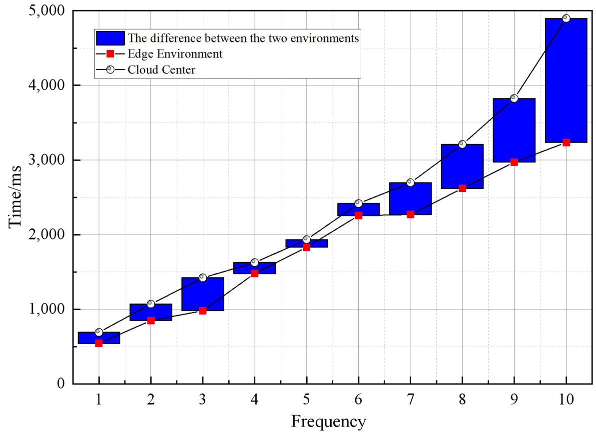

Figure. 5.10 A statistical chart of average time consumption of multi-node cooperation

Figure 9 shows that the average time of each step of the trusted data synchronization system proposed on the two hardware platforms is between 26ms-184ms, which is lower than the average human response time of 215ms. The system delay is within an acceptable range and has a low impact on the use effect of the client. Figure 10 suggests that when the camera sampling rate is below six frames per second, there is little time difference between the operation mode based on ECP multi-node cooperation and the operation mode based on cloud computing center in performing a task. When the camera sampling rate is higher than six frames per second, the time cost of the two calculation methods increases gradually, and the gap increases gradually. When the acquisition frequency increases, the transmission volume of source data increases, the communication delay increases, and EC is less affected. However, the cloud computing center needs to spend more time processing data, so the time cost increase is higher than that of EC.

5.3.3. Performance test results of the trusted data synchronization system

(1) Performance test results of blockchain

When Tx Number is 10000, the data transmission volume of the blockchain can reach $1.69*10^2$ when data are written (Open). During data query, the data transmission volume of blockchain can reach $3.50*10^2$. Each index can meet the basic operational requirements of the client in practical application. Meanwhile, it can also improve the Central Processing Unit (CPU), memory, disk and other configurations of edge nodes to improve performance.

(2) Performance test results of full data synchronization (one-time synchronization of all data)

The full data synchronization is conducted in the system based on the rsync command and the BTS-PD file distribution module. Figure 5.11 shows the test results.

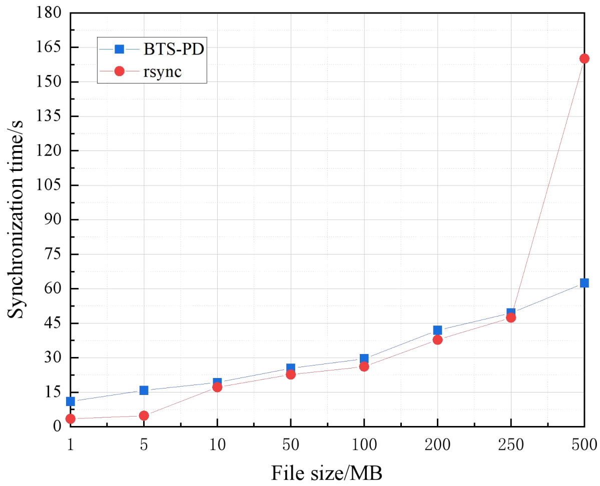

Figure. 5.11 Full file synchronization performance

Figure 11 reveals that the maximum synchronization speed of the rsync command can reach 7.93M/s. When the synchronized file size is less than 250MB, the rsync command synchronization time is lower than PTS-PD, and the time requirement is lower. When the file is a small file, PTS-PD takes more time for additional redundancy in the synchronization process, so it takes more time than rsync command. When the file is large, the data synchronization time of PTS-PD is significantly lower than that of the rsync command, which has outstanding advantages. The reason is that P2P nodes in BTS-PD share data with other P2P nodes while downloading data, so the download speed increases gradually. The data synchronization between edge nodes is mainly small files, and BTS-PD cannot realize incremental data synchronization. Therefore, BTS-PD synchronization has limitations, and rsync command is more suitable for data synchronization of edge nodes.

(3) Incremental synchronization performance test results of data

Figure 5.12 and Figure 5.13 present the experimental results of folder/file incremental synchronization.

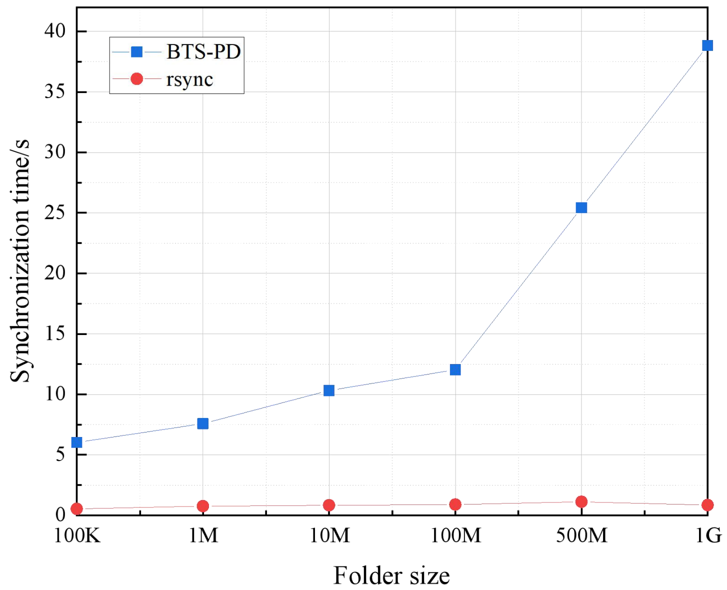

Figure. 5.12 Incremental folder synchronization performance

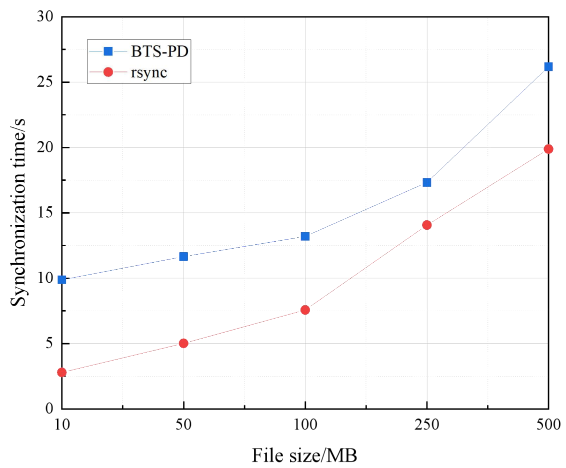

Figure. 5.13 Incremental file synchronization performance

Figure 5.12 suggests that the BTS-PD synchronization time gradually increases with the synchronization folder size increase. rsync synchronization time is basically stable, and the time gap between the two synchronization methods increases gradually. When the size of the synchronization folder is 1G, the time consumption difference between the two synchronization methods is about 38s. According to the trend prediction, with the increase of transmission folders, their synchronization time will continue to increase under certain conditions. The reason may be that when BTS-PD synchronizes folders, it needs to re-synchronize the original files and the newly added 10K files in batches, while rsync synchronization only needs to transfer 10K incremental files in the second incremental transfer. Figure 5.13 reveals that rsync synchronization is faster than BTS-PD synchronization and takes less time in file synchronization. rsync only synchronizes the matching information and incremental part, reducing redundant data transmission in traditional data synchronization and improving bandwidth utilization.

5.4. Conclusion

The Internet financial market widens the financing channels for small and medium-sized enterprises and individual entrepreneurs. However, it also increases the risk of financial transactions. The improvement of business security of online transactions can better control internet financial risks. User information storage and transaction system security are critical risk concentration dimensions in business security. Therefore, for information network security, based on EC and blockchain technology, the encrypted transmission and trusted data synchronization among client equipment, EC equipment and blockchain database in financial transactions are studied. The anonymous storage protocol for IoT data is proposed, and the trusted data synchronization system based on blockchain technology is constructed. The protocol cost analysis shows that the protocol greatly reduces the time cost for information encryption transmission. The system workflow RTT results show that the RTT is less than 215ms, and the system will not have an obvious delay. The time difference between ECP and cloud computing centers is small at a low sampling rate. As the sampling rate increases, the time consumption increases. The cloud computing center is greatly affected when the sampling rate is high. The data synchronization between edge nodes is mainly small files. The performance test results of a trusted data synchronization system show that the system's full synchronization and incremental synchronization based on the rsync command are better than the file distribution function module based on the P2P network, BTS-PD. rsync only synchronizes the matching information and incremental part, while BTS-PD cannot realize incremental data synchronization. Therefore, BTS-PD synchronization has limitations, and the rsync command is more suitable for data synchronization of edge nodes. However, due to the limited energy, this exploration only briefly puts forward the protocol and makes a theoretical analysis. Besides, the system established is only briefly introduced, and only one data synchronization method is selected for experimental comparison. These aspects can be supplemented and optimized to refine the details in the follow-up study. Besides, various data synchronization methods can be selected for comparison to explore better solutions, provide a reference for the design of financial network transaction security and customer privacy security system, and provide ideas for the research of risk control.

CHAPTER 6: DISSCUSSION AND CONCLUSION

6.1. Conclusions

Based on a detailed review of the literature on Internet finance, the thesis analysed the conventional and special forms of risks in Internet finance with reference to traditional financial risk management theories and practices, explore the internal and external mechanisms of Internet financial risks, and study the identification, assessment and measurement, internal control and external supervision of Internet financial risks. This will be a useful supplement and reference for the development of Internet financial risk management and related theories.

The new risk management idea of "using big data to control the internal risk of Internet financial enterprises" is proposed, and how to use big data to control the internal risk of Internet financial enterprises from different perspectives is demonstrated and analysed. By comparing the analysis of Machine Learning and Deep Learning Algorithms in Internet financial risk assessment, the results provide a new research idea for the assessment of Internet financial risk, which has important reference value for preventing financial systemic risk. In the internet financial network transaction process, blockchain technology and Edge Computing are introduced and these two methods can improve the security of financial network transactions to a certain extent. This exploration provides a reference for the research of multi-node trusted data synchronisation across multiple security domains and the risk control methods of Internet financial transactions.

At the outset, three research questions framed the research inquiry.

Firstly, the disadvantage of conventional risk assessment methods is that it requires a large amount of real data as the premise, and it relies too much on historical data, and the dynamic early warning capability is reduced. Is there any better way? In chapter 2, based on the analysis of the financial risk performance and causes of Internet credit, the BP neural network algorithm is used to construct an Internet credit risk early warning model. In terms of the neural network training, the data fitting effect is good, but the accuracy rate needs to be improved. Based on this, GA is used to optimise the neural network so that the model error is small, and the accuracy of early warning can reach more than 90%. Therefore, the early warning model based on big data can effectively pre-warn and assess Internet credit risk.

Secondly, what could be used to assess risks for Internet financial enterprises systematically? In Chapter 3, ML and DL are introduced to collect, process, and analyse data. And different credit risk measurement analysis models are constructed. The performance of different models is verified through the public data sets of MSE to prove the effectiveness of the proposed credit risk assessment model. The ML algorithm is verified through experiments to improve the processing accuracy and solve data feature redundancy and noise interference. The DL algorithm enhances the feature extraction ability of the model, and the fusion model improves the generalisation ability of the model in layer-by-layer learning.

Finally, due to the functional defects of the intelligent terminal device itself, there are still some restrictions on the use of blockchain. In chapter 4, based on EC and blockchain technology, the encrypted transmission and trusted data synchronisation among client equipment, EC equipment and blockchain database in financial transactions are studied. The experiment is designed to verify the protocol and the system's performance. The experimental results show that the anonymous storage protocol of financial network transaction data greatly reduces the time cost for information encryption transmission.

6.2. Limits of the Study

This study focuses on the risk management of Internet finance, and analyses the risk identification of Internet finance. However, due to the existence models of Internet finance and continuous innovation, it is not possible to fully develop each model, and the risk management of each model is not studied in depth. Therefore, on the basis of this study, the risk management of each specific Internet finance model can be refined in the future.

In Chapter 2, as the BP neural network model must require a certain number of data samples. The number and authenticity of data samples significantly affect the learning performance and final assessment results of neural network models. Therefore, the authenticity, reliability, and extensiveness of the data sources should be ensured as much as possible in the future investigation to provide a guarantee for the accuracy and practicality of the analysis results.

In Chapter 3, although a suitable analysis model is constructed, there are still some shortcomings. First, the data of MSE are all from financial credit companies, so the sample resources are limited. Meanwhile, some key enterprise information is not available due to confidentiality, making it difficult to analyse data comprehensively. Second, although the proposed algorithm has been optimised, it still needs improvement on feature selection through multi-objective optimisation to construct the corresponding objective function. It is hoped that these problems can be further analysed in the follow-up research to improve the proposed Internet financial credit risk assessment model.

In Chapter 4, due to the limited energy, this exploration only briefly puts forward the protocol and makes a theoretical analysis. Besides, the system established is only briefly introduced, and only one data synchronisation method is selected for experimental comparison. These aspects can be supplemented and optimized to refine the details in the follow-up study. Besides, various data synchronisation methods can be selected for comparison to explore better solutions, provide a reference for the design of financial network transaction security and customer privacy security system, and provide ideas for the research of risk control.

6.3. Policy Imperatives

As Internet finance gradually reveals many security issues and risk hazards, the need for Internet finance regulation is becoming more and more important. The purpose of this endeavour was to better inform future policy initiatives.

Firstly, the system of laws and regulations should be improved to regulate the behavior of Internet finance. Existing financial laws and regulations are formulated for traditional finance, and rarely involve Internet finance. And even if they do, they are only supplements and additions based on certain risk phenomena, and cannot become a system. The basic laws and regulations for the protection of consumer rights and interests in the development of Internet finance, technical information network security, and the construction of a positive new system also need to be further developed and improved. The lag of the current legal and regulatory system makes the development of Internet finance to be regulated. In the face of the diverse and ever-changing models of Internet finance innovation, laws and regulations are urgently needed to regulate it. However, the development of laws and regulations requires in-depth research, comprehensive and integrated consideration, which has resulted in the development and introduction of laws and regulations lagging behind the innovation of Internet finance. Therefore, it is necessary to revise and improve the existing laws and regulations related to Internet finance in a timely manner.

Secondly, new regulatory mechanism should be innovated and a regulatory sandbox should be introduced. Regulators can set up regulatory sandboxes for Internet finance innovation as a complementary regulatory mechanism to provide corresponding safety controls for innovation in Internet financial institutions. Setting up innovation centers in Internet finance institutions can improve the overall level of innovation in the financial industry, especially in financial technology. Setting up such institutions means providing a space for testing services and products designed by financial or non-Internet finance institutions, and improving their security and reliability. Internet financial institutions do not need to bear the burden of regulation on the formation of innovation, but only to test the business model of products and services based on real and effective situations. Regulators should protect consumers' rights and interests as the basis for appropriate liberalisation.

Based on the protection of consumers' rights and interests, it is appropriate to relax the scope of regulation, remove the obstacles in the rules for financial technology innovation, and increase the control and management of risks to achieve financial technology innovation. The current development of Internet finance has formed a challenge for innovation and regulation, so the regulatory sandbox was born, which is in line with the policy direction, aiming to stimulate innovation and avoid harming the legitimate rights and interests of consumers. It can be seen that the regulatory sandbox can better balance the relationship between financial innovation and financial regulation.

Finally, although a number of regulations, documents and reports have been issued by many countries on the risk management of Internet finance, the construction of a real regulatory system and regulatory measures still need a relatively long process. In the process of the gradual construction of the Internet financial regulatory system, industry self-regulation can be strengthened to promote and protect the continued healthy development of the Internet financial industry. On the one hand, industry self-regulation expands the scope and extends the role of space, achieving significant results and enhancing the degree of self-awareness of institutions. On the other hand, the development experience of industry self-regulation can provide an important reference and basis for the development of laws and regulations and regulatory system. The degree of self-regulation of the Internet finance industry and the development of the industry has a direct and important impact on the government's regulatory attitude and degree, thus affecting the whole development direction of the industry.

REFERENCES

Abdel-Basset, M., El-Shahat, D., El-henawy, I., de Albuquerque, VHC., & Mirjalili, S.(2020). A new fusion of grey wolf optimizer algorithm with a two-phase mutation for feature selection. *Expert Systems with Applications*, 139112824-139112829.

Adiyanto, A., & Febrianto, R. (2020). Authentication Of Transaction Process In E-marketplace Based on Blockchain?? technology. *Aptisi Transactions on Technopreneurship (ATT)*, 2(1), 68-74.

Ai, Q. (2019). Research on Systemic Risk of Banking Industry from the Perspective of Internet. 2*019 Annual Conference of the Society for Management and Economics*, 328-334. doi: https://doi.org/10.35532/JSSS.V4.068.

Allen, F., McAndrews, J., & Strahan, P. (2002). E-finance: A Introduction. *Journal of Financial Services Research*, 22, 130-141.

Anait, K. (2001). E-risk Management for Banks in the Age of the Internet. *Journal of Banking &Finance*,25(40), 143- 165.

Anderson, C.(2006). The Long Tail: Why the Future of Business is Selling Less or More. I*nformation Processing & Management*,43(4), 1147–1148.

Ba, S., & Yang, B. (2012). Research on the international regulation of third-party payment. *Fiscal Research*, 4, 72-75.

Bambury, P. (1998). A taxonomy of Internet commerce.*First Monday*,10(3).

Banks, E. (2001). E-Finance: The Electronic Revolution in Financial Services, *John Wiley & Sons*.

Bao, A. (2013). The challenge of Internet finance to traditional finance and risk prevention. *Inner Mongolia Financial Research,* 12, 36-38.

Banerjee, S., Bera B., Das, A., Chattopadhyay, S., Khan, M., & Rodrigues, J. (2021). Private blockchain-envisioned multi-authority CP-ABE-based user access control scheme in IIoT. *Computer Communications*,169(6), 99-113.

Benaim， M. (2018). From symbolic values to symbolic innovation: Internet-memes and innovation. *Research Policy*, 47(5), 901-910.

Berger, A., & Deyong, R. (2001). The Effects of Geographic Expansion on Bank Efficiency.*Journal of Financial Services Research*,19,163-184.

Beque, A., & Lessmann, S. (2017). Extreme learning machines for credit scoring: An empirical evaluation. *Expert Systems with Applications*, 86, 42-53.

Bureš, V. (2017). A method for simplification of complex group causal loop diagrams based on endogenization, encapsulation, and order-oriented reduction. *Systems*, 5(3), 46-52.

Cai, S., & Zhang, J. (2020). Exploration of the credit risk of P2P platform based on data mining technology. *Journal of Computational and Applied Mathematics,* 372112718-372112726.

Cao, F. (2015). The challenge of Internet finance to traditional finance. *Financial Forum*, 01, 3-6.

Chaffee, E., & Rapp, G. (2012). Regulating Online Peer-to-Peer Lending in the Aftermath of Dodd–Frank： In Search of an Evolving Regulatory Regime for an Evolving Industry.*Washington and Lee Law Review*，1, 485-533.

Chen, J. (2019). Big data boosts commercial bank credit business and risk management innovation. *Investment and Financing,*12, 62-64.

Chen, X., & Li Z. (2017). Research on the transmission mechanism of network credit risk based on the perspective of Internet finance. *Innovation,* 01, 80-90.

Chen, Y., & Qiao, G. (2015). Research on information security risk prevention in the mode of "Internet+Finance". *Journal of Suzhou University (Philosophy Social Science Edition)*, 06, 124-130.

Chen, Z. (2014). How new is Internet finance. *New Finance*, 4, 9-13.

Chen, Z., Zhang, L., & Zhang, S. (2021). Access control scheme on blockchain and decentralized attributed-based algorithm with identity. *Scientia Sinica Informationis*, 51(8), 1345-1359.

Chen, Z., Li, Y., Wu, Y., & Luo, J. (2017). The transition from traditional banking to mobile internet finance: an organizational innovation perspective-a comparative study of Citibank and ICBC. *Financial Innovation*, 3(1), 1-16.

Chi, G., Ding, S., & Peng, X. (2019). Data-Driven Robust Credit Portfolio Optimization for Investment Decisions in P2P Lending. *Mathematical Problems in Engineering*, 1, 1-10.

Claessens, S., Dobos, G., Klingebiel, D., & Laeven, L. (2003). The Growing Importance of Networks in Finance and its Effects on Competition, *Edward Elgar Publishing.*

Claxton, N. (2011). Progress, Privacy, and Preemption: a Study of the RegulatoryHistory of Stored-Value Cards in the United States and The European Union. *Arizona Journal of International & Comparative Law*, 2, 501-538.

Craig, A., Zabala., Jeremy.,& Marc, J. (2018). Shadow credit in the middle market: the decade after the financial collapse. *The Journal of Risk Finance,*19, 120-123.

Cui, D. (2015). Financial Credit Risk Warning Based on Big Data Analysis. *Metallurgical & Mining Industry*, 6, 133-142.

Cui, Z., Kirkby, JL., & Nguyen, D. (2021). A data-driven framework for consistent financial valuation and risk measurement. *European Journal of Operational Research*, 289(1), 381-398.

Dai, X. (2014). The authenticity of Internet finance. *Finance and Economics*,07.

David, J., Gonsalvez., & Robert, R. (2016). Supply chain shared risk self-financing for incremental sales. *The Engineering Economist*, 1, 250-253.

Dendramis, F., Tzavalis, E.,& Adraktas, G. (2018). Credit risk modelling under recessionary and financially distressed conditions. *Journal of Banking and Finance*, 91, 23-25.

Du, G., Liu, Z., & Lu, H. (2021). Application of innovative risk early warning mode under big data technology in Internet credit financial risk assessment. *Journal of Computational and Applied Mathematics*, 386113260-386113268.

E, Y., Qiao, Y., & Liu, Z. (2016). Research on the evolution of Internet finance model and risk identification based on system science perspective. *East China Economic Management*, 03, 91-96.

Eniola, A. (2011). Recalibrating Abstract Payments Regulatory Policy: A Retrospective Post Dodd-Frank Act. *Kansas Journal of Law and Public Policy*, 21(1), 86-120.

Feng, J. (2013). Research on the regulation of Internet finance in China. *Time Finance*, 29, 20-21.

Firdous, S., & Farooqi, R.(2017). Impact of internet banking service quality on customer satisfaction. *The Journal of Internet Banking and Commerce*, 22(1), 1-17.

Franklin, A.(2002). E-Finance: An Introduction. *Journal of Financial Services*

Research, 22(2), 5-27.

Gao, H. (2014). The development of Internet finance and its legal regulation. *Zhongzhou Journal*, 02, 57-61.

Gong, M. (2014). Internet finance: characteristics, impact and risk prevention. *New Finance*, 02, 8-10.

Guo, J., & Du, Y. (2021). A secure three-factor anonymous roaming authentication protocol using ECC for space information networks. *Peer-to-Peer Networking and Applications*, 9(14), 898-916.

Guo, J., & Zhu, Z. (2018). When deep learning meets inter-data center optical network management: Advantages and vulnerabilities. *Journal of Lightwave Technology*, 36(20), 4761-4773.

Gupta, A., Siddiqui, S., & Alam, S. (2019). Cloud computing security using blockchain. *Journal of Emerging Technologies and Innovative Research*, 6(6), 791-794.

Hasan, M., Popp, J., & Olh, J. (2020). Current landscape and influence of big data on finance. *Journal of Big Data*, 7(1),1-17.

He, Q. (2014). Pay attention to the prevention of financial risks to promote the healthy development of Internet finance. *Price theory and practice*, 03, 10-12.

He, W., & Yang, Y. (2014). Research on the regulation of Internet financial risks in China based on the perspective of institutional and non-institutional factors. *Financial Development Research*, 08, 48-54.

Hosen, A., Singh, S., & Sharma, P. (2020). Blockchain-based transaction validation protocol for a secure distributed IoT network. *IEEE Access*, 8,117266-117277.

Hu, J. (2018). Brief Analysis on the Application of Big Data in Internet Financial Risk Control. *2018 5th International Conference on Business, Economics and Management, 154-159.*

Huang, X., Li, X., & Yu, Y. (2019). Integration of Bricolage and Institutional Entrepreneurship for Internet Finance: Alibaba's Yu'E Bao. *Journal of Global Information Management*, 27(2),1-23.

Huang, Y., He, N., Chen, Y., Chen, Z., & Li, L. (2018). BERMP: a cross-species classifier for predicting m6A sites by integrating a deep learning algorithm and a random forest approach.

International journal of biological sciences,14(12), 1669-1673.

Hou, W., Wang, X., Zhang, H., Wang, J., & Li, L. (2020). A novel dynamic ensemble selection classifier for an imbalanced data set: An application for credit risk assessment. *Knowledge-Based Systems*, 208106462-208106469.

Imakura, A., Inoue, Y., & Sakurai, T. (2018). Parallel Implementation of the Nonlinear Semi-NMF Based Alternating Optimization Method for Deep Neural Networks. *Neural processing letters*,47(3), 815-827.

Jiang, S. (2016). Big data technology application and development trend. *Value Engineering,* 33, 166-168.

Jiang, Z., Zhang, H., Shen, C., Cheng, D., & Wu, H. (2016). Credit risk assessment of Internet finance based on logistic regression model. *Heilongjiang Science and Technology Information*, 29, 147.

Kang, Q. (2019). Financial risk assessment model based on big data. *International Journal of Modeling Simulation & Scientific Computing*, 10(04), 106-113.

Karne, F., Lang, W., & Nolle, D.(2002). Internet Banking: Developments and Prospects.*Program on Information Resources Policy*.

Kim, D., Song, Y., & Braynov, S. (2005). A Multidimensional and content Analyses of Academia Practitioner Perspectives. *Decision Support Systems*.

Klafft, M. (2008). Online Peer-to-Peer Lending: A Lenders'Perspective. *CSREA Press*, 371-375.

Li, H., & Song, L. (2016). The classification and assessment of Internet financial risks. *E-commerce*, 12, 50-53.

Li, L., Zhu, F., Sun, H., Hu, Y., Yang, Y., & Jin, D. (2021). Multi-source information fusion and deep-learning-based characteristics measurement for exploring the effects of peer engagement on stock price synchronicity. *Information Fusion*, 691-621.

Li, R. (2016). The reasonable boundary of criminal law intervention in Internet financial innovation in Shanghai Pilot Free Trade Zone. *Foreign Economics and Management,* 02, 101-112.

Li, Y., & Zhang, C. (2019). Research on Internet Credit Interest Rate Risk under Asymmetric Information. *Journal of Baoji University of Arts and Sciences (Natural Science Edition)*, 39(1), 16-20.

Li, Y., Chen, F., & Jin, Y. (2014). An analysis of the regulation of Internet finance. *Journal of Zhejiang University (Humanities and Social Sciences Edition)*, 04, 87-97.

Li, Z., Cai, Y., & Hu, S. (2021). Research on Systemic Financial Risk Measurement Based on HMM and Text Mining: A Case of China Financial Market. *IEEE Access*, 922171-922185.

Liao, M., Zheng, S., & Pan, S.(2021). Deep-learning-based ciphertext-only attack on optical double random phase encryption. *Opto-Electronic Advances*,4(5), 12-23.

Liu, C. (2016). The function, operation mode, risk identification and institutional design of the development of Internet finance. *Modern economic information,* 03, 265-266.

Liu, D., & Liu, Y. (2017). Research on risk early warning of Internet financial service industry. *Contemporary Economy*, 01, 48-49.

Liu, S. (2014). Adhering to the concept of tolerance and innovation to correctly handle the relationship between the development of Internet finance and regulation. *Tsinghua Financial Review*, 02, 20-23.

Liu, X. (2020). A Visualization Analysis on Researches of Internet Finance Credit Risk in Coastal Area. *Journal of Coastal Research*, 103(SI), 85-89.

Liu, X. (2015). Research on the prevention and regulation of Internet financial risks. *Central Party School of the Communist Party of China.*

Lu, B., & Mei, P. (2016). Research on operational risk assessment of Internet supply chain finance based on fuzzy hierarchical analysis. *Times Finance,* 35, 333-334.

Luo, C., Li, M., Peng, P., & Fan, S. (2018). How Does Internet Finance Influence the Interest Rate? Evidence from Chinese Financial Markets. *Dutch Journal of Finance and Management*, 2(1), 1-8.

Kim, A., Yang, Y., Lessmann, S., Ma, T., Sung, M-C., & Johnson, JE. (2020). Can deep learning predict risky retail investors? A case study in financial risk behavior forecasting. *European Journal of Operational Research*, 283(1), 217-234.

Kwon, H., Do, T., & Kim, J. (2020). Comprehensive Decision Framework Combining Price Prediction and Production-Planning Models for Strategic Operation of a Petrochemical Industry. *Industrial And Engineering Chemistry Research*, 59(25),11610-11620.

Ma, Z., Zhang, C., & Zhang, L. (2021). Energy saving strategy and Nash equilibrium of hybrid P2P networks. *Journal of Parallel and Distributed Computing*, 157(10), 145-156.

Mann, R. (2004). Regulating Internet Payment Intermediaries.*Texas LawReview*, 3, 681-716.
Masmoudi, K., Abid, L., & Masmoudi, A. (2019. Credit risk modeling using Bayesian Network with a latent variable. *Expert Systems with Applications*, 127, 157-166.
Mazumdar, S., & Ruj, S. (2021). Design of Anonymous Endorsement System in Hyperledger Fabric. *IEEE Transactions on Emerging Topics in Computing,* 9(4), 1780-1791.
Mohammadi, S., & Nazemi, A. (2020). On portfolio management with value at risk and uncertain returns via an artificial neural network scheme. *Cognitive Systems Research*, 59, 247-263.
Mollick, E. (2013). The Dynamics of Crowdfunding:Determinants of Success and Failure. S*SRN Scholarly Paper.*
Nagurney, A., & Ke, K. (2003). Financial Networks with Electronic Transactions: Modelling, Analysis and Computations. *Quantitative Finance*, 3, 71-87.
Ouyang, Z., & Mo, T. (2016). Research on risk measurement and assessment of Internet finance. *Journal of Hunan University of Science and Technology (Social Science Edition)*, 03, 173-178.
Peng, S. (2015). Analysis of risks and causes of P2P lending companies in the context of Internet finance. *Time Finance*, 23, 207-209.
Peng, J., & Zhuo, W. (2016). Characteristics, causes and regulation of systemic risks of Internet finance in China. *Southwest Financial*, 10, 3-7.
Peng, Y., & Zhang, Y. (2016). Research on the early warning model of Internet finance business risk under the threshold of cloud finance. *Accounting*, 13, 103-108.
Perez, M., Gerardo, B., &Medina, R. (2018). Modified sha256 for securing online transactions based on blockchain mechanism. *2018 IEEE 10th International Conference on Humanoid, Nanotechnology, Information Technology, Communication and Control, Environment and Management (HNICEM),* 1-5.
Pignolet,Y., Schmid, S., & Tochner, S. (2021). Survey on Blockchain Networking: Context, State-of-the-Art, Challenges. *ACM Computing Surveys*,54(5),1-34.
Qu, Y., Quan, P., Lei, M., & Shi, Y. (2019). Review of bankruptcy prediction using machine learning and deep learning techniques. *Procedia Computer Science*, 162895-162899.
Rahardja, U., Hidayanto, A., & Lutfiani, N. (2021). Immutability of Distributed Hash Model on Blockchain Node Storage. *Scientific Journal of Informatics*,8(1), 137-143.
Rappa, M. (2003). Business Models on the Web. *Managing the Digital Enterprise*.
Rappa, M. (2004). The Utility BusinessModel and the Future of Computing Services. *IBM*

Systems Journal.

Raschka, S. (2018). MLxtend: Providing machine learning and data science utilities and extensions to Python's scientific computing stack. *Journal of open-source software*, 3(24), 638-641.

Reegan, A., & Kabila, V. (2021). Highly Secured Cluster Based WSN Using Novel FCM and Enhanced ECC-ElGamal Encryption in IoT. *Wireless Personal Communications,* 118(1), 1313-1329.

Sato, S., & Hawkins, J. (2001). Electronic Finance: An Overview of the Issues, Bank for International Settlements Information. *Press & Library Services CH—4002.*

Shahrokhi, M. (2008). E-finance: Status, innovation, resources and future challenges. *Finance*.34(6), 365-398.

Sharma, D., Prinja, S., & Aggarwal, K. (2017). Out-of-pocket expenditure for hospitalization in Haryana State of India: Extent, determinants & financial risk protection. *The Indian Journal of Medical Research*, 146(6), 759.

Shen, C., Cheng, D., Jiang, Z., & Zhang, H. (2016). Application of fuzzy hierarchical analysis in Internet financial risk assessment. *Heilongjiang Science and Technology Information*, 05, 135.

Shen, F., Ma, X., Li, Z., Xu, Z., & Cai, D. (2018). An extended intuitionistic fuzzy TOPSIS method based on a new distance measure with an application to credit risk evaluation. *Information Sciences*, 428105-428119.

Shen, F., Zhao, X., Li, Z., Li, K., & Meng, Z. (2019). A novel ensemble classification model based on neural networks and a classifier optimisation technique for imbalanced credit risk evaluation. *Physica A: Statistical Mechanics and its Applications*, 526121073-526121081.

Shi, J. (2015). Theoretical basis, market foundation and prospect analysis of Internet finance development. *Contemporary Economy,* 13, 14-15.

Shi, P., Olshevsky, A., & Paschalidis, I. (2020). Asymptotic Network Independence in Distributed Stochastic Optimization for Machine Learning: Examining Distributed and Centralized Stochastic Gradient Descent. *IEEE Signal Processing Magazine*, 37(3), 114-122.

Singha, N., & Singh, Y. (2021). New incentive mechanism to enhance cooperation in wireless P2P networks. *Peer-to-Peer Networking and Applications*, 14(4), 1-11.

Singh, H.，Gopal, R. & Li, X．(2008). Risk and Return of Investments in Online Peer-to-Peer Lending.*University of Texas.* 1-5.

Soler-Dominguez, A., Juan, A., & Kizys, R. (2017). A Survey on Financial Applications of

Metaheuristics. *ACM Computing Surveys*, 50(1), 1-23.

Song, T., & Gao, J. (2015). Evaluation of Internet finance risk and preventive measures based on hierarchical analysis. *Financial Economy*, 16, 60-63.

Stehlík, M., Helperstorfer, C., & Hermann, P. (2017). Financial and risk modelling with semicontinuous covariances. *Information Sciences*, 394-395, 246-272.

Sullivan, R. (2000). How has the adoption of internet banking affected performance and risk in banks? *Financial Industry Perspectives*, 1-16.

Seuken, S Z.(2012). Improved Memory-Bounded Dynamic Programming for Decentralized POMDPs. *Co RR*,5, 3-35.

Talal, M., Zaidan, A., Zaidan. B., Albahri, A., Alamoodi, A., Albahri, O., Alsalem, M., Lim, C., Tan, KL., & Shir, W. (2019). Smart home-based IoT for real-time and secure remote health monitoring of triage and priority system using body sensors: Multi-driven systematic review. *Journal of medical systems*, 43(3), 42-49.

Tao, N. (2019). Analysis of Credit Risk of Internet Credit. *Time Finance*, 15, 145-149.

The Wolfsberg Group. (2013). Wolfsberg Guidance on Mobile and Internet Payment Services. *The Wolfsberg Group*.

Timers, P.(1999). Electronic Commerce: strategies and models for business-to-business trading. *New York: Wiley* .

Tong, W. (2014). Research on money laundering risk and prevention countermeasures of Internet finance. *Financial Accounting,* 08, 71-76.

Tu, C., Chang, C., Chang, S., Lee, C., & Chan, C. (2018). A Decision for Predicting Successful Extubation of Patients in Intensive Care Unit. *BioMed Research International*, 1-11.

Valaskova, K., Kliestik, T., Svabova, L., & Adamko, P.(2018). Financial risk measurement and prediction modeling for sustainable development of business entities using regression analysis. *Sustainability*, 10(7), 2144-2149.

Verstein, A.(2001). The Misregulation of Person-to-person lending. *U.C.Davis Law Review.*

Walton, R.(2005). Low-cost Assurance for B2C E-commerce.*Computer Fraud & Security,*(10), 4-6.

Wang, C. (2013). Internet financial model innovation and risk prevention. *Qinghai Finance*, 12, 36-38.

Wang, D., Xue, X., & Wang, Y. (2021). Overcapacity Risk of China's Coal Power Industry: A Comprehensive Assessment and Driving Factors. *Sustainability*, 13(3), 1426-1431.

Wang, F. (2018). Research on Application of Big Data in Internet Financial Credit Investigation Based on Improved GA-BP Neural Network. *Complexity*, 1-16.

Wang, G. (2014). New trends in the reform of China's financial system from Internet finance. *Red Flag Manuscript*, 0, 9-13.

Wang, L. (2016). On the construction of Internet financial risk warning system under the background of big data. *Economic and Trade Practice*, 004,38-40.

Wang, L., Mo, T., Wang, X., Chen, W., He, Q., Li, X., Zhang, S., Yang, R., Wu, J., & Gu, X.(2021). A hierarchical fusion framework to integrate homogeneous and heterogeneous classifiers for medical decision-making. *Knowledge-Based Systems*, 212106517-212106523.

Wang, S., & Zhang, C. (2014). The Chinese model of Internet finance development and financial innovation. *Changbai Journal*, 01, 80-87.

Wang, Z. (2014). Risk analysis and preventive measures of China's Internet finance. *Times Finance*, 8, 82-83.

Wu, F., Su, X., & Ock, Y. (2021). Personal Credit Risk Evaluation Model of P2P Online Lending Based on AHP. *Symmetry*,13(1),83-103.

Wu, L., Yang, Y., & Maheshwari, M. (2019). Parameter optimization for FPSO design using an improved FOA and IFOA-BP neural network. *Ocean Engineering*, 175(1), 50-61.

Wu, W., Zhou, F., & Hu, R. (2020). Energy-Efficient Resource Allocation for Secure NOMA-Enabled Mobile Edge Computing Networks. *IEEE Transactions on Communications,* 68(1), 493-505.

Wu, X. (2014). Research on the direction and path of Internet finance regulation. *Jilin Financial Research*, 09, 1-8.

Wu, X. (2013). Internet finance should be regulated differently. *IT Times*, 21, 14.

Wu, X. (2014). The logic of Internet finance. *China Finance*, 03, 29-31.

Wu, X. (2015). Internet finance:The logic of growth. *Finance and trade economy,* 02, 5-15.

Wu, Z. (2017). The Legal Application and Resolving Mechanism of "Campus Naked Loans" Threat. *DEStech Transactions on Social Science, Education, and Human Science*, 252-263.

Xia, Y., Liu, C., Da, B., & Xie, F. (2018). A novel heterogeneous ensemble credit scoring

model based on stacking approach. *Expert Systems with Applications*, 93182-931899.
Xie, P., & Zou, C. (2012). Research on internet finance model. *Financial Research*, 12, 11-22.
Xie, P., Zou, C., & Liu, H. (2014). The necessity and core principles of Internet finance regulation. *International Financial Research*, 8, 3-9.
Xiong, H., & Liu, C.(2014). Research on the risk of Internet finance and risk prevention. *China Trade*, 31, 97-98.
Xu, D., Tang, S., & Guttman, D. (2019). China’s campaign-style Internet finance governance: Causes, effects, and lessons learned for new information-based approaches to governance. *Computer Law & Security Review*, 35(1),3-14.
Xu, G., & Gao, W. (2019). Financial Risk Contagion in Stock Markets: Causality and Measurement Aspects. *Sustainability,* 11(5), 1402-1411.
Xu, X. (2017). Research on the risk assessment of Internet finance based on consumer perspective. *Northern Economic and Trade*, 02, 123-124.
Xue, Z. (2016). Causes and prevention of liquidity risk in Internet finance. *China Development Observation*, 12. 26-28.
Yan, Z. (2013). Some thoughts on the current risk of Internet finance. *Zhejiang Finance*, 12, 40-42.
Yang, A. (2020). Analysis on Internet Financial Business and Construction of Credit System. *Business Economics Research*,3(2),1-4.
Yang, D., Chen, P., Shi, F., & Wen, C. (2018). Internet finance: Its uncertain legal foundations and the role of big data in its development. *Emerging Markets Finance and Trade*, 54(4), 721-732.
Yang, H., Yi, D., & Xiao, H. (2014). Research on early warning of Internet finance risk based on big data analysis. *Modern Management Science,* 04, 3-5.
Yang, L. (2018). Research on the Present Situation and Countermeasures of Credit Risk Management of Rural Small and Medium Financial Institutions. *Financial and Economic*, 31, 210.
Yang, Q., Wang, Y., & Ren, Y. (2019). Research on financial risk management model of internet supply chain based on data science. *Cognitive Systems Research*, 5650-5655.

Yang, R., Yu, F., & Si, P. (2019). Integrated blockchain and edge computing systems: A survey, some research issues and challenges. *IEEE Communications Surveys & Tutorials,* 21(2), 1508-1532.

Yao, G., & Zhao, Gang. (2015). Research on Internet finance and its risks. *Journal of Nanjing University of Posts and Telecommunications (Natural Science Edition)*, 02, 8-21.

Yin, J. (2014). The myth and reality of "Internet finance". *Shanghai Securities News*.

Yu, W., & Wu, Y. (2018). Research on network trading system using blockchain technology. *2018 International Conference on Intelligent Informatics and Biomedical Sciences (ICIIBMS). IEEE*,3: 93-97.

Yuan, M., & He, L. (2015). Disposal of non-performing assets in the banking industry: model innovation based on the Internet platform. *Nanfang Finance*, 12, 92-97.

Yuan, Y. (2016). Analysis and comparison of risk transmission mechanism of traditional finance and Internet finance. *Times Financial*, 18, 53-54.

Zeng, G. (2014). Comparison of Internet finance and traditional banking industry. *Internet World*, 01, 74-76.

Zhang, B., Waqas, M., & Tu, S. (2021). Power Allocation Strategy for Secret Key Generation Method in Wireless Communications. *Comtech Science Press*, 68(4),2179-2188.

Zhang, C. (2016). The regulation and development of Internet finance in China. *Financial Forum*, 10, 13-17.

Zhang, J., & Wei, Y. (2017). The Institutional Guarantee of Internet Financial Consumer's Security Right. *DEStech Transactions on Social Science, Education, and Human Science* , 1124-1132.

Zhang, J., Zhu, S., & Cao, X.(2020). Application of Animal Food Management in Internet Financial Growth System. *Revista Científica de la Facultad de Ciencias Veterinarias*, 30(3), 1459-1469.

Zhang, Q., Luo, Y., Fu, S., Xu, Z., & Xiao Y. (2015) Research on Internet-Finance Risk Warning based on Big Data. *International Conference on Social Science, Education Management and Sports Education.* Atlantis Press.

Zhang, S., Mao, D., & Wang, B. (2016). Application of Big Data Processing Technology in Fault Diagnosis and Early Warning of Wind Turbine Gearbox.*Automation of Electric Power Systems*, 40(14), 129-145.

Zhang, X. (2014). Principles of Internet finance regulation: exploring a new financial regulatory paradigm. *Financial regulation research,* 02, 6-17.

Zhang, X. (2014). Internet finance will promote innovation in financial theory development. *IMI Research Update*, 6.

Zhang, Y. (2018). Research on Credit Risk Prevention of Large and Medium-sized Enterprises in Commercial Banks. *Market Modernization*, 20, 122.

Zhang Y. (2019). Research on the Risk Management of Internet Credit Business of Commercial Banks. *Finance and Economics (Academic Edition)*,20, 24-25.

Zhao, B., Zhang, X., Li, H., & Yang, Z. (2020). Intelligent fault diagnosis of rolling bearings based on normalized CNN considering data imbalance and variable working conditions. *Knowledge-Based Systems*, 199105971-199105982.

Zhao, C. (2015). The risk of China's Internet finance industry and the construction of legal prevention system. *Social Science Line,* 10, 224-231.

Zhao, Z. (2017). Neural network algorithm based on combined classifier. *Electronic Technology,* 12, 43-46.

Zheng, L. (2014). Internet finance in China: model, impact, nature and risks. *International Economic Review*, 05, 103-118.

Zheng, L., Liu, L., & Xu, J. (2014). The current situation, models and risks of Internet finance: an analysis based on the U.S. experience. *Financial Market Research,* 02, 41-49.

Zhou, H. (2016). A preliminary study on the causes of China's Internet financial risks and its prevention mechanism. *Financial Economics*, 24, 45-47.

Zhou, Y. (2013). Internet finance: an epoch-making financial change. *Exploration and contention*, 09, 67-71.

Zhu, Q., & Wang, Li. (2016). Risk warning of private P2P lending platform of Internet finance. *Journal of Hebei University (Philosophy and Social Science Edition),* 04, 123-130.

Zhu, X. (2018). Research on Credit Risk Management of China’s Commercial Banks under the Background of Interest Rate Marketization. *Financial community*, 9, 9.

Ziar, R., Irfanullah, S., & Khan, W. (2021). Privacy Preservation for On-Chain Data in the Permission less Blockchain using Symmetric Key Encryption and Smart Contract. *Mehran University Research Journal of Engineering and Technology*,40(2), 305-313.