PERSONAL INFORMATION PROTECTION BASED ON BLOCKCHAIN TECHNOLOGY

YINGHONG ZHAO

MASTER OF SCIENCE

IN DIGITAL INNOVATION AND FINANCIAL TECHNOLOGY

CHIANG MAI UNIVERSITY

OCTOBER 2023

PERSONAL INFORMATION PROTECTION BASED ON BLOCKCHAIN TECHNOLOGY

YINGHONG ZHAO

AN INDEPENDENT STUDY SUBMITTED TO CHIANG MAI UNIVERSITY IN PARTIAL FULFILLMENT OF THE REQUREMENTS FOR THE DEGREE OF MASTER OF SCIENCE
IN DIGITAL INNOVATION AND FINANCIAL TECHNOLOGY

CHIANG MAI UNIVERSITY
OCTOBER 2023

PERSONAL INFORMATION PROTECTION BASED ON BLOCKCHAIN TECHNOLOGY

YINGHONG ZHAO

THIS INDEPENDENT STUDY HAS BEEN APPROVED TO BE A PARTIAL FULFILLMENT OF THE REQUIREMENTS FOR THE DEGREE OF MASTER OF SCIENCE
IN DIGITAL INNOVATION AND FINANCIAL TECHNOLOGY

Examination Committee: **Advisor:**

……. Chairman ……
(Asst.Prof.Dr.Kittawit Autchariyapanitkul) (Lect.Dr.Ahmad Yahya Dawod)

……. Member
(Lect.Dr.Somsak Chanaim)

……. Member
(Lect.Dr.Ahmad Yahya Dawod)

17 October 2023

To

Dr.Nopasit Chakpitak

Dr.Anukul Tamprasirt

Dr.Nathee Naktnasukanjn

Dr.Piyachat Udomwong

Dr.Piang-or Laohavilai

Lec.Kanya Hirunwattanapong

For my supervisors and Mentors who were the guiding light every step of the way as I researched for this dissertation.

ACKNOWLEDGEMENT

First and foremost, I would like to thank the almighty for blessing me with physical and mental strength for doing this thesis.

I express my sincere gratitude to my Guide, Dr. Ahmad Yahya Dawod, for giving me moral support and excellent guidance throughout the course of the development of this thesis.

I express my deep appreciation for the help and warm encouragement that I received from ICDI staff members for completing this thesis successfully.

Yinghong Zhao

หัวข้อการค้นคว้าอิสระ	การป้องกันการฝ่าฝืนข้อมูลส่วนบุคคลจากการถูกละเมิด โดยใช้เทคโนโลยีบล็อคเชน
ผู้เขียน	นางสาว ยิ่งฮง เจ้า
ปริญญา	วิทยาศาสตรมหาบัณฑิต (นวัตกรรมดิจิทัลและเทคโนโลยีการเงิน)
อาจารย์ที่ปรึกษา	ดร.อาหมัด ยาห์ยา ดาวูด

บทคัดย่อ

เทคโนโลยีบล็อกเชนได้พัฒนาจากบิทคอยน์ไปสู่การซื้อขายหลักทรัพย์การชำระเงินออนไลน์ โลจิสติกส์และการดูแลสุขภาพ บนพื้นฐานนี้ปัญหาความเป็นส่วนตัวที่เกี่ยวข้องมีความโดดเด่นมากขึ้น เนื่องจากการพัฒนาและความนิยมของเทคโนโลยีบล็อกเชน บทความนี้ เริ่มต้นด้วยรายละเอียดเกี่ยวกับบริบทการวิจัยและความสำคัญของการวิจัยในหัวข้อนี้และการตรวจสอบสถานะปัจจุบันของการรั่วไหลของข้อมูลส่วนบุคคล โดยกรณีข้อมูลรั่วไหล ได้มีการวิเคราะห์ถึงสาเหตุของการรั่วไหลของข้อมูล ประการที่สอง เราประเมินระดับความรู้ความเข้าใจเกี่ยวกับเทคโนโลยี บล็อกเชน ของผู้ใช้วีแชท และความเข้าใจของพวกเขาเกี่ยวกับการประยุกต์ใช้บล็อกเชนที่อาจเกิดขึ้นในการปกป้องข้อมูลส่วนบุคคลและความคิดเห็นเกี่ยวกับความเป็นไปได้และความน่าเชื่อถือของเทคโนโลยี ซึ่งรวมถึงการประเมินความปลอดภัย ความสามารถในการปกป้องความเป็นส่วนตัว ความพร้อมใช้งาน และด้านอื่นๆของโซลูชั่น เพื่อให้ทราบว่าผู้ใช้ยอมรับและยอมรับโซลูชั่นมากน้อยเพียงใด จากผลการวิจัยสามารถสรุปได้ว่า การจ่ายเงินจะเก็บข้อมูลการบันทึกวีแชทเพย์ ฟังก์ชั่นการชำระเงินจะเก็บข้อมูลที่เกี่ยวข้องกับบัตรธนาคาร อายุของผู้ใช้ และเก็บข้อมูลเสียงต่อข้อความ แต่ไม่ได้บันทึก ซึ่งมีผลกระทบมากที่สุดต่อความพึงพอใจของผู้ใช้วีแชทต่อการคุ้มครองข้อมูลส่วนบุคคล ตรวจสอบสาเหตุของการรั่วไหลของข้อมูลส่วนบุคคลของผู้ใช้วีแชท สัดส่วนของการรั่วไหลของข้อมูล และการเยียวยาการรั่วไหลของข้อมูล ในที่สุดบทความนี้ ได้นำเสนอข้อเสนอแนะและแนวทางการปรับปรุงที่ใช้เทคโนโลยี บล็อกเชน โดยอิงจากสถานการณ์ปัจจุบันของการรั่วไหลของข้อมูลส่วนบุคคลของผู้ใช้วีแชท ผลการวิจัยแสดงให้เห็นว่าการรับรู้และความพึงพอใจของผู้ใช้วีแชทเกี่ยวกับเทคโนโลยี บล็อกเชน สามารถบรรลุความปลอดภัยและความเป็นไปได้ของข้อมูลได้ดียิ่งขึ้น โดยการตรวจสอบจะสามารถยืนยันจุดแข็งของการประยุกต์ใช้บล็อกเชนในการปกป้องข้อมูลส่วนบุคคลได้ดีขึ้น การประยุกต์ใช้เทคโนโลยีบล็อกเชนในการปกป้องข้อมูลส่วนบุคคลมีแนวโน้มกว้างไกล

คำสำคัญ: บล็อกเชน การคุ้มครองข้อมูลส่วนบุคคล การรั่วไหลของข้อมูล ผู้ใช้วีแชท

Independent Study Title	Personal Information Protection Based on Blockchain Technology
Author	Miss Yinghong Zhao
Degree	Master of Science (Digital Innovation and Financial Technology)
Advisor	Dr.Ahmad Yahya Dawod

ABSTRACT

Blockchain technology has evolved from Bitcoin to fields such as securities trading, online payments, logistics, and healthcare. On this basis, due to the continuous development and popularization of blockchain technology, the privacy issues involved have become increasingly prominent. This article first provides a detailed introduction to the background and research significance of this topic and investigates the current situation of personal information leakage. Through information leakage cases, the reasons for information leakage were analyzed. Secondly, we evaluated the level of awareness and understanding among WeChat users of blockchain technology, as well as their understanding of the potential application of blockchain technology in personal information protection, as well as their views on the feasibility and credibility of the technology. This includes an evaluation of the security, privacy protection ability, availability, and other aspects of the solution to understand the user's recognition and acceptance of the solution. Based on the research findings, it can be concluded that Tenpay collects WeChat payment record information, the payment function collects bank card-related information, user age, and collects voice to text conversion information but does not save it, which has the strongest impact on WeChat user satisfaction with personal information protection. An investigation into the reasons for personal information leakage among WeChat users, the proportion of information leakage, and the remedial measures taken for information leakage. Finally, based on the current situation of personal information leakage among WeChat users, this article proposes suggestions and solutions for improvement based on blockchain technology. The results show that WeChat users'

awareness and satisfaction with blockchain technology can better achieve data security and feasibility. Through verification, the advantages of blockchain application in personal information protection can be better confirmed, which has broad prospects for the application of blockchain technology in personal information protection.

Keywords: Blockchain; Personal information protection; Information leakage; WeChat users

CONTENTS

LIST OF TABLES

LIST OF FIGURES

LIST OF ABBREVIATIONS

XSS	Cross-site scripting
DOS	Denial of Service
S	Services
C	Customer
TP	Third Party Services
DS	Data Subject
MQ	Memory Quotient
UTXO	Unused Transaction Output
IBC	Identity-Based Cryptography
ZKP	Zero Knowledge Proof
RSA	Sensing Services Association
IPFS	Interplanetary File System
PRC	People's Republic of China

CHAPTER 1

INTRODUCTION

1.1 Research Background

Personal privacy data leakage has become a major social issue in the internet age. In recent years, the application of big data has become increasingly frequent and the technology has become more mature. However, the issue of privacy data leakage is also worrying and frightening. Various cases of personal privacy breaches have repeatedly occurred, with incomplete statistics reaching approximately millions, and the number of people affected by privacy data breaches is also approaching billions. Based on this, it is necessary to study and analyze the use of blockchain technology for personal information protection to prevent the leakage of personal privacy data. The article uses methods such as survey questionnaires and mathematical statistics to investigate the leakage of personal privacy data of WeChat users in a certain region. WeChat is a popular communication platform owned by Chinese technology giant Tencent, where users can send text, make voice and video calls, and share files and social media. As of 2021, WeChat has over 1.2 billion monthly active users, mainly concentrated in China, but also used globally. However, the data privacy and security issues of WeChat have attracted the attention of users and experts, especially considering the strict regulation and censorship of the Internet by the Chinese government. In recent years, the rise of blockchain technology has provided potential solutions to address these privacy and security issues on WeChat and other platforms. Blockchain is a decentralized, encrypted, and tamper-resistant digital ledger that can store and validate transactions or data without the need for intermediaries or central institutions. By using blockchain, WeChat can enhance its personal information protection, identity authentication, and data-sharing mechanisms, while promoting transparency and trust among users.

With the advent of the era of online consumption, when consumers enjoy the various benefits brought by the rapid development of mobile internet, incidents of personal privacy information leakage, theft, and trafficking occur frequently. Harassment,

fraudulent phone calls, and emails continue to rage, becoming a common concern for the entire society and consumers. There are reports that Chinese netizens have suffered economic losses of over 100 billion yuan due to online fraud and other issues. According to the statistics on the acceptance of consumer complaints by the National Consumers' Association, the phenomenon of illegal collection of consumer personal information on e-commerce platforms, social media software, and other platforms became a new hot topic for complaints in the first half of 2022.

The protection of personal information in China is facing practical difficulties such as weakened security guarantees, virtualization of personal control, and insufficient information sharing. Limited to protecting personal information from a legal perspective. Without fundamental changes, the dilemma of personal information protection cannot be fundamentally improved, so we call for the use of blockchain technology to protect personal information. Scholars have further analyzed the definition of personal information under blockchain technology [2], the issue of personal data ownership [3], and the compatibility between blockchain technology and personal information protection [4]. From this perspective, blockchain technology has a natural fit with personal information protection. Blockchain technology is a decentralized distributed database technology that has the characteristics of low trust, open and transparent transactions, and data that cannot be tampered with. It can effectively reduce data management costs, improve work efficiency, and protect data security. At present, the application of blockchain technology to personal information protection is a way to further develop blockchain in the field of data security.

The awareness of personal information protection among WeChat users is weak. From a user's perspective, WeChat users mainly use WeChat for daily activities such as socializing and WeChat payments, with a high utilization rate of WeChat. WeChat has a large user base, with a wide age distribution range of users. Most users are not familiar with the personal information protection services provided by WeChat, and are not clear about the situations that may lead to information leakage. Young people's awareness of personal information protection is already weak, and they are more willing to try novel online products, which unintentionally brings security risks; For middle-aged and elderly users, there are various rapidly developing internet products, and these users are unable to quickly adapt to the challenges brought by the information age. Personal information

protection in the big data era has undergone significant changes compared to traditional personal information protection. Middle-aged and elderly users are not clear about the specific measures for personal information protection, and may unintentionally disclose personal information; For underage users, they should receive more protection from society. Most underage users are in the high school or below stage and have not yet entered society. Their awareness of personal information protection is weak, and they need external help to protect their personal information. Therefore, it is crucial to obtain the satisfaction of WeChat users with WeChat personal information protection services and apply them to improve WeChat services, and to provide more attractive quality services to enhance user satisfaction.

Therefore, this study aims to investigate the user satisfaction level of the WeChat personal information protection system and explore the potential impact of integrating blockchain technology into it. Specifically, we will study users' perceptions, attitudes, and behaviors towards WeChat data privacy and security, as well as their understanding and acceptance of blockchain technology. In order to improve the user satisfaction of the WeChat platform and make users feel more confident and secure when using it.

1.2 Objectives of the Study

WeChat is a popular communication platform with up to 1.2 billion monthly active users in China and globally. However, despite the convenience and user-friendliness of the platform, the protection and privacy security of users' personal data have been a compelling issue. WeChat's data privacy and security protection mechanisms are particularly vulnerable due to the PRC government's stringent Internet regulation, censorship, and filtering regime. Therefore, the current emergence of blockchain technology worldwide offers a potential solution for WeChat to address data privacy and security issues, as this technology can enhance the protection mechanisms for users' personal data, authentication, and data sharing mechanisms, while promoting transparency and trust among users. Therefore, the main objectives of this study are to:

(1) Understanding user satisfaction with WeChat's personal information protection system and assessing possible blockchain technologies used by WeChat's personal privacy problem resolution mechanism.

(2) Investigate the diverse attitudes of users and delve into any factors that might influence their attitudes towards this new protection measure.

(3) in-depth study of users' awareness and acceptance of blockchain technology, as well as their knowledge and opinions on WeChat's storage and sharing mechanisms.

(4) Provide WeChat users with some suggestions for blockchain technology interfaces that are actionable to help them better protect their data and privacy, thereby enhancing their trust in and use of WeChat.

1.3 Research Significance

1.3.1 Theoretical significance

(1) Empirical study of the mechanism of protection of WeChat users' personal privacy and the effect of blockchain technology. This study contributes to an in-depth study of the mechanisms of personal privacy protection for WeChat users and the effects of blockchain technology on user satisfaction and trust. The study can provide researchers with empirical evidence and reveal insights into the attitudes and circumstances of WeChat users regarding privacy and security, enhance the connection between social media platforms and blockchain technology, and improve the personal privacy protection and trust of social media users. This research result can provide strong support for the development and improvement of related measures in social media and blockchain.

(2) In-depth exploration of potential connections between blockchain technology and social media platforms. This study delves into the potential connections between social media platforms and blockchain technology. Our study will investigate users' attitudes, trust, and behaviors towards data privacy and security, understand the perception and acceptance of blockchain technology and its application potential, as well as their knowledge and opinions on the storage and sharing mechanism of WeChat. By clarifying users' perceptions of the relationship between social media and blockchain technology, we can provide blockchain developers and social media operators with comprehensive insights and actionable practical guidelines. This will enable them to provide more precise directions and goals in enhancing user personal data protection and privacy security.

(3) To provide support for the development of local areas and operational guidelines for data security and user privacy protection. This study can provide strong theoretical support for the development of bureaucratic domain and operational guidelines for personal data protection. Our data analysis results, interviews and survey results, discussions and recommendations summarized in this study are of significant reference value, which can be used as a joint pull of statutes and regulations within the norms of social media and blockchain-related platforms.

1.3.2 Practical implications

(1) Provide directions for WeChat and other social media platforms to improve user information protection mechanisms and establish blockchain protection mechanisms. As the privacy and security issues of users' personal data on social media platforms increase, more secure and scientific mechanisms are needed to protect personal privacy and data. The practical significance of this study is to provide guidance for WeChat and other social media platforms to improve personal data protection mechanisms. For such platforms, a more scientific approach to personal data protection, such as solutions that incorporate blockchain technology to improve the transparency and security of information, would be a guaranteed and welcome solution.

(2) Improving the skills and capabilities of researchers and technology developers in the social media industry. With the increased emphasis on information and privacy protection, the market demands for data privacy and security are increasing. For technical staff and researchers in the blockchain technology and social media industries, the practical implications of this study are to improve their skills and capabilities in order to more effectively drive research and development in the area of personal data privacy and security. The concepts and methods presented in this study can guide technology developers and researchers by providing them with more scientific and actionable guidelines for developing platforms with blockchain protection mechanisms, thus enabling the successful implementation of stronger information and privacy protection strategies.

(3) Increase people's understanding and acceptance of blockchain technology applications. Due to the novelty and complexity of blockchain technology, many people lack understanding and knowledge about its application and efficacy. The practical

significance of this study is to increase people's understanding and learning about the application of blockchain technology, so as to promote people's attention to the acceptance and development direction of this technology. And to make people aware of how blockchain technology can play a positive role in protecting personal data privacy and information security.

1.4 Problem Statement

In the context of global economic integration and internet informatization, personal information has become a very important strategic resource. Personal information includes citizens' family environment, personality, biometric information, education, work experience, etc. These information together constitute citizens' personal information. Personal information has strong identification functions, and many businesses provide targeted services by analyzing consumers' personal information. The chain of interests behind personal information is very large, which is also the main reason for personal information leakage. In addition, many illegal individuals can use citizens' personal information for criminal activities, seriously threatening the personal and property safety of citizens. In addition to the highly purposeful theft behavior mentioned above, many citizens' personal information is unintentionally leaked, such as personal information on express delivery forms. Many consumers do not properly keep the express delivery forms after receiving them, resulting in personal information leakage. With the rapid development of computer information technology, there are more and more ways for people to obtain information, which also poses huge risks to personal information. Information can be quickly disseminated through various online channels, such as common social media platforms such as Weibo, WeChat, forums, etc [6]. This information may involve commercial secrets or international secrets, and personal information, as the basic protection of citizens' privacy rights, is directly related to their immediate interests. However, the protection of personal information rights in the context of the Internet is very difficult. On the one hand, there are many ways of dissemination on online platforms, and personal power is difficult to prevent the spread of information; Secondly, many infringement behaviors do not have clear legal definitions, making it difficult for rights holders to protect their rights [7].

The emergence of blockchain technology has optimized many weaknesses in personal information protection, but any technology has two sides. The emergence of blockchain has also brought new challenges to personal information protection. In addition to the inherent poor carrying capacity of public chains and the inability to eliminate the use of tokens as incentive mechanisms, which make blockchain difficult to popularize, there are also issues of incompatibility with current laws and regulations. [8] It is worth further exploration whether blockchain technology can truly be implemented in various fields and play a significant role in personal information protection.

1.5 Research Questions

This study aims to explore the satisfaction of WeChat users with personal information protection based on blockchain technology, gain a deeper understanding of their needs and expectations for personal information protection, analyze the advantages and disadvantages of personal information protection solutions based on blockchain technology, and provide theoretical and practical support for further improving the satisfaction of WeChat users with personal information protection**.** Specifically, the research questions of this study are as follows**:**

(1**)** What is the level of attention and needs of WeChat users for personal information protection?

This study will investigate the level of concern among WeChat users regarding personal information protection, understand their level of concern about privacy leakage and abuse, and explore their needs and expectations for personal information protection**.**

(2**)** What is the level of awareness and understanding of blockchain technology among WeChat users?

This study will evaluate WeChat users' awareness and understanding of blockchain technology, understand their cognitive level of the potential application of blockchain technology in personal information protection, and their views on the feasibility and credibility of the technology**.**

(3**)** How satisfied are WeChat users with personal information protection solutions based on blockchain technology?

This study will explore the satisfaction of WeChat users with personal information protection solutions based on blockchain technology, including evaluations of the security, privacy protection capabilities, availability, and other aspects of the solution, in order to understand users' recognition and acceptance of the solution.

(4) What are the advantages and challenges faced by WeChat users when using personal information protection solutions based on blockchain technology?

The study will explore the advantages and challenges faced by WeChat users when using blockchain-based personal information protection solutions. By investigating the user experience and feedback in actual use, our aim to understand the specific advantages and problems of the solution from the user's perspective, such as the evaluation of operational convenience, performance performance, user privacy protection, data security, and other aspects.

(5) How to improve the satisfaction of WeChat users with personal information protection?

Based on the research results and analysis of WeChat users' satisfaction with personal information protection, this study will propose relevant suggestions and measures to improve WeChat users' satisfaction with personal information protection. These suggestions may include improvements at the technical level, formulation of policies and regulations, user education and awareness cultivation, etc., to promote the further development and improvement of personal information protection work.

1.6 Research Contributions

Since its inception, blockchain technology has become a research hotspot in academia and industry due to its characteristics of decentralization, traceability, and immutability. With the advent of the blockchain era, smart contracts have made it possible for blockchain to solve more practical application problems. However, due to the open and transparent design of blockchain technology ledgers, the information security of users has been affected. More seriously, due to the decentralized nature of blockchain, it cannot compensate for information leakage like centralized applications. In order to meet the protection needs of blockchain applications for user personal information, in recent years,

relevant researchers have analyzed the problems of blockchain personal information protection and proposed corresponding solutions, providing support for the secure implementation of blockchain applications. Some features of blockchain technology are beneficial for personal information protection. The Data Security Law (Draft) explicitly requires the establishment of a data traceability system to trace the direct or indirect sources of personal information. The Cybersecurity Law and the Personal Information Protection Law (Draft) stipulate that unauthorized access to information, encryption, deidentification, and prevention of information leakage should be prevented. Blockchain technology records the creation and operation of node information one by one, and ensures information accuracy through cross-validation such as timestamp and multi-party accounting. These technical features are conducive to personal information protection. In addition, blockchain technology can trace the entire process of information processing, which can enhance personal control over information.

This article will use a hybrid method of quantitative and qualitative data to comprehensively understand WeChat users' attitudes, trust, and behavior toward data privacy and security. We will conduct a series of questionnaires, and interviews, and adopt various methods to analyze the results, in order to gain a more comprehensive understanding and insight into the problem. The expected contributions of this study in this article include:

(1) Provide empirical data analysis on the potential of personal information protection and blockchain technology to address these issues for users of WeChat and other platforms.

(2) Identify factors that affect user satisfaction, trust, and willingness to use blockchain personal information protection features.

(3) Provide new and practical insights for operators, decision-makers, and researchers on WeChat and other similar platforms, promote better methods of providing privacy and security services, and enhance users' privacy protection and trust on the internet and social media platforms.

1.7 Conceptual Framework

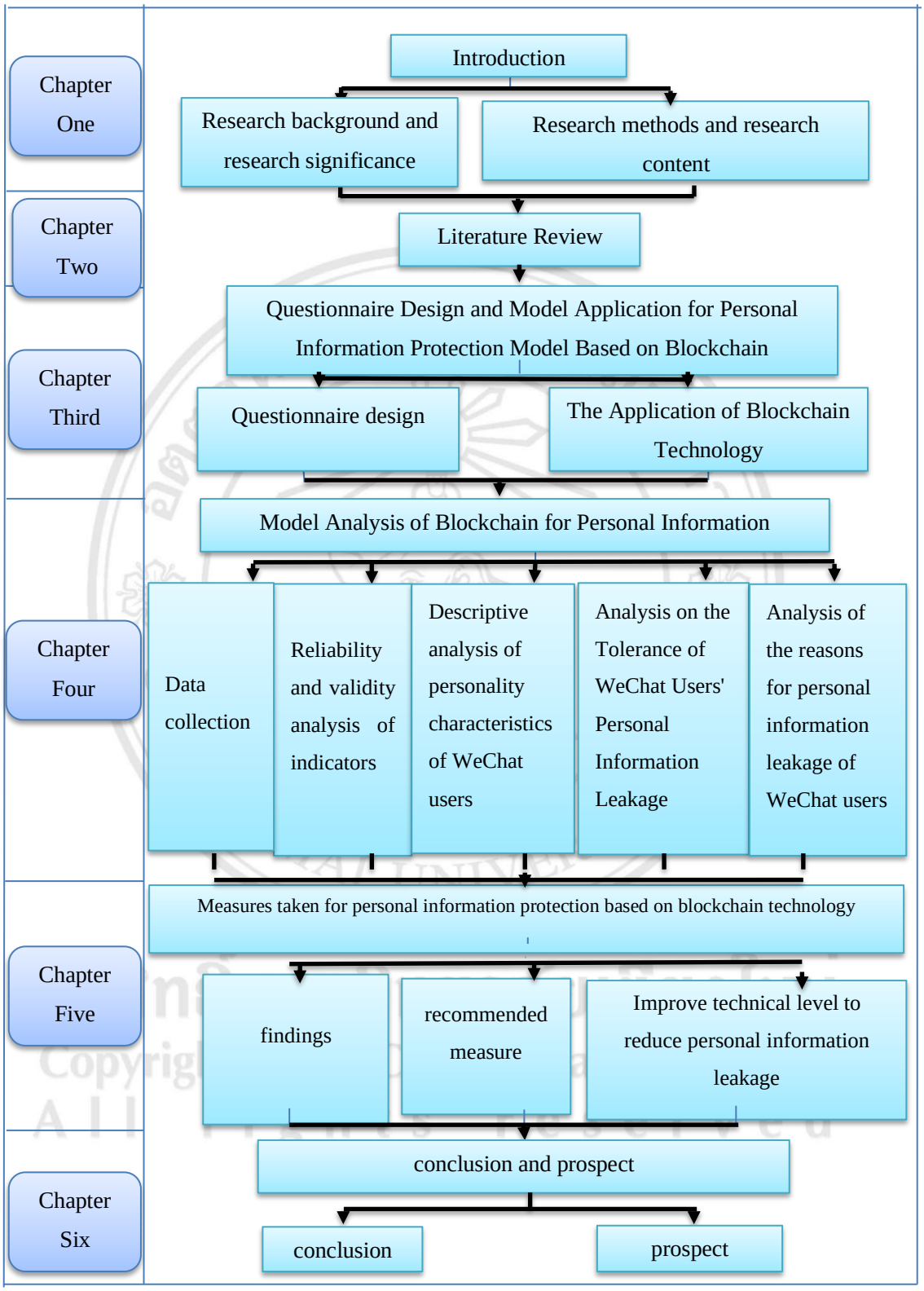


Figure 1.1 Conceptual framework

1.8 Thesis Outline

This thesis is mainly divided into six chapters.

The first chapter is an introduction. It mainly introduces the research background, significance, and methods. The main content of this section is to understand background information, and determine research objectives, research questions, and research directions through literature research methods and empirical research.

Chapter 2 is a literature review section, which mainly focuses on the advantages and disadvantages of similar technologies in the market, analyzes the application of blockchain technology in personal information protection, and conducts relevant research on the use of blockchain technology in data sharing and personal information protection in social media environments.

Chapter 3 collects the satisfaction of WeChat users with the amount of personal information protection through questionnaire design. By comprehensively using scientific methods such as investigation and observation to understand the phenomenon of information leakage before, during, and after the incident, it is concluded that the main cause of information leakage is data security issues, which can better improve the use of WeChat users.

Chapter 4 is data analysis, mainly analyzing the correlation between reliability and validity indicators to draw conclusions on the satisfaction of WeChat users with personal information protection. Through descriptive analysis, the individual characteristics of WeChat users for personal information protection are obtained, and better solutions for personal information protection are proposed.

Chapter 5 is the conclusion. Based on WeChat users' concerns about the integrity of blockchain data, starting from the core characteristics of data security, some improvement measures are proposed to enhance personal information protection. At the same time, the use of blockchain technology is more conducive to the protection of personal information and has a certain promoting effect.

Chapter 6 is the research conclusion and future prospects. It pointed out the shortcomings of this article and provided ideas and insights for other scholars to further analyze the application of blockchain technology in personal information protection. The

essence of applying it to personal information protection**.** Reflect on the governance ideas for personal information protection under blockchain technology, seek the integration of technology and law, and analyze its advantages, existing problems, and future improvement directions**.**

CHAPTER 2

LITERATURE REVIEW

The data sources selected in this article are all from Baidu Academic Search. Baidu Academic has fully integrated excellent data and application content on the internet. Based on this research approach, this article takes academic journal papers from the Chinese academic journal online publishing database as the research object, and researches the theme of "blockchain+personal information". More than 50,000 articles were retrieved. My research topic is "Personal Information Protection Based on Blockchain Technology". Among the more than 50,000 valid papers retrieved, I downloaded more than 30 papers that are highly relevant to this topic for research.

Although the research on personal information protection in China started relatively late, it has also sparked a research boom among scholars in recent years. Professor Qi Aimin is a pioneer and integrator of research on personal information protection in China. He has published articles such as "On Personal Data" [9], "On Legal Protection of Personal Information" [10], and "On the System of Personal Information Rights from a Balanced Perspective - Between Personal Interests and Freedom of Information" [11], systematically studying the personal information protection systems of developed countries and international organizations, This article provides a detailed introduction to the academic theories and legislative models of personal information protection, and proposes legislative principles and suggestions for future information legislation in China. Other scholars have explored the protection of personal information from various perspectives such as criminal law, civil law, and administrative law. Regarding the mechanism for protecting personal information, Wang Shaohui believes that the government should play a leading role in protecting personal information, establish a sound mechanism for pre, during, and post-supervision, a cross-border cooperation mechanism for personal information protection, and a diversified governance mechanism [12]. Wang Na and Minister Xu explore personal information security in mobile networks from four perspectives: users, social network enterprises, mobile terminal enterprises, and national legislation [13].

From existing literature, scholars' research on personal information protection mainly focuses on exploring the macro network environment and legal level, with very little research on personal information protection on WeChat platforms**.** This issue has important research significance for the improvement of the internet environment, the long**-**term healthy development of WeChat, and the protection of users' personal rights and interests**.**

2.1 Blockchain for Personal Information Protection

In the research on blockchain-based personal information management methods [14], a blockchain-based personal information management method was mainly proposed. This method stores personal information transaction records between users and service providers on the blockchain, allowing users to distinguish whether the service provider is legally or illegally acquiring users' personal information. After applying this method, if criminals obtain and use the user's personal information through illegal means, the user can easily obtain relevant evidence.

Li (2017) [15] proposed a conceptual model for managing personal health information (PHI) data to address the issues of decentralized management of personal health information data and patients' lack of authority to manage their own information. This model utilizes blockchain technology to manage data from multiple healthcare institutions, enabling patients and healthcare institutions to effectively collect personal health information data into a single view while ensuring data integrity. Although this method effectively solves the problem of fragmented personal health information, its concept can only be used to integrate personal information with comprehensive data sources. It is not feasible for more dispersed information stored in the hands of each user.

Yu (2019) [16] proposed a blockchain based personal information management system that can generate, modify, delete, and read personal information on the blockchain. In this system, only trusted institutions can participate in the construction of blockchain, and the operation of personal information is completed by trusted super nodes. The verification of transactions adopts consensus algorithms. The system only achieves the use of blockchain to obtain personal information, and does not provide a trusted storage

method related to personal information transactions. It only has the function of managing personal information, and cannot protect personal information.

Zhao (2018) [17] designed and implemented an off-chain personal data protection scheme based on blockchain. This scheme utilizes resource services to encrypt the address of personal data, thereby avoiding the problem of users revoking their permissions when authorizing third-party services, and provides an Ethereum-based solution implementation. In this method, although the user's personal data address can be encrypted, dishonest service providers may save the data after obtaining the data address for the first time, making the operation of the data address meaningless. The purpose of protecting personal information cannot be achieved.

Tseng (2017) [18] conducted research on the application of blockchain technology in personal information protection, mainly starting from the advantages of blockchain technology in personal information protection, and fully studied the existing shortcomings and improvement measures.

At present, the academic community and industry have high hopes for the development prospects of blockchain technology in personal information protection. Li (2018) [19] analyzed in the article "Exploration of Building a Blockchain Credit Management Platform for University Student Archives" that the application of blockchain technology in university student archives can prevent the leakage of student archive information and ensure the authenticity of academic information. It can provide convenient and reliable information authentication services for students. Fan (2021) [20] believes in the article "Blockchain Mode Analysis of Personal Credit Reporting System Alliance in the Internet Era" that blockchain technology can promote the establishment of Internet credit reporting systems and achieve effective and rapid analysis and application of credit information data. [21] Wang (2021) pointed out that within the industry, JD.com utilizes blockchain technology to record information from production to transactions to distribution, ensuring the authenticity and reliability of product information, and also providing a security umbrella for users' personal logistics information. Liu (2019) People's Daily, Weibo, and other media have also introduced blockchain technology to protect the copyright information of authors [22].

At present, personal information on the Internet is facing many threats. The platform collects and leaks personal information of users without permission. Due to the technological advantages of the platform, individual citizens are unable to obtain relevant evidence materials, so there is a problem and dilemma of insufficient proof ability in judicial practice. At present, blockchain technology is still in its infancy, immature, and there is no relevant legal system. Therefore, while blockchain technology brings certain advantages to personal information protection, it also faces some shortcomings, how to improve these shortcomings, and further exploration is needed on how to use blockchain technology to participate in personal information protection.

2.2 Research Related to The Protection of Personal Information in the Social Media Environment

Liang (2021) [23] explored the problems faced by social media applications in the context of Web 3.0. He introduced the concept of Web 3.0 and analyzed the problems in social media applications. The research mainly focuses on issues related to social media applications, such as personal information leakage and data privacy. The research conclusion points out that in the era of Web 3.0, social media applications need to pay more attention to personal information protection and privacy protection.

Liu Wenjie's (2021) [24] research focuses on personal information protection on social networks. His research method is a literature review. The research mainly discusses the importance and challenges of personal information protection on social networks. The research conclusion emphasizes the necessity of personal information protection in social networks and proposes some protective measures and suggestions.

Gao (2021) [25]'s research focuses on the challenges and solutions of online privacy in the era of social media. The research method was not explicitly mentioned. The research mainly explores the challenges faced by individual privacy rights in the era of social media, and explores possible solutions and ways out.

Liu's (2022) [26] research focuses on strategies for protecting the personal information of social media users. The research method was not explicitly mentioned, and the main focus of the study was to explore strategies and measures for protecting the personal information of social media users. The research conclusion emphasizes the

personal information protection strategies that users should adopt when using social media.

Yi (2021) [27]'s research analyzed the civil law protection of personal information in the era of social media. The research method is literature review and analysis. The research mainly explores the current situation and existing problems of civil law protection of personal information in the era of social media. The research conclusion points out that there are still some problems in the protection of personal information in the era of social media in China, and relevant legal protection and regulatory measures need to be strengthened.

Huang (2022) [28] studied the mechanism of personal privacy exposure and protection in social media from the perspective of privacy paradox. The research process focused on analyzing the reasons and influencing factors of personal privacy exposure in social media, and explored the mechanisms of personal privacy protection. The research conclusion points out that both social media platforms and individual users need to work together to strengthen the protection mechanism of personal privacy.

Chen's (2021) [29] research focuses on the mechanism and innovation of community information dissemination in the social media environment. The research involves observing and analyzing information dissemination behavior on social media. The research mainly explores the mechanism and innovation of community information dissemination in the social media environment, as well as its impact on personal information protection. The research conclusion emphasizes the diversity and innovation of information dissemination in social media, and puts forward some relevant suggestions.

Wu's (2021) [30] research explores the civil law protection of personal information from the perspective of social media. Research methods may include literature review and legal analysis. The research mainly explores the legal issues and challenges of personal information protection in the era of social media, as well as the relevant provisions on personal information protection in China's current civil law. The research conclusion points out that China's civil law protection measures need to be further improved to meet the personal information protection needs of the social media era.

Gu's (2022) [31] research explores the difficulties and breakthroughs in the legal protection of self-disclosure of personal information in social media. The research

involves analyzing the policies and user behavior of social media platforms. The research mainly focuses on the legal protection of individuals' self-disclosure of information. The research conclusion points out that although personal disclosure of information is widely used on social media, there are certain difficulties in its legal protection. To address this issue, it is necessary to strengthen the formulation of relevant laws and regulations and the self-discipline mechanism of social media platforms.

Li's (2021) [32] research is based on the perspective of "use and satisfaction" and investigates the application of parenting social media. The research involves observing and analyzing the functions and user behavior of parenting social media applications. The research mainly explores the characteristics, user satisfaction, and demand for personal information protection of parenting social media applications. The research conclusion emphasizes the importance of protecting personal information while meeting user needs in parenting social media applications.

Cheng’s (2021) [33] research is based on grounded theory and investigates the influencing factors of social media users' willingness to privacy settings. The research involves investigating and statistically analyzing the privacy setting behavior and related factors of social media users. The research mainly explores factors that affect users' willingness to set privacy settings, such as personal privacy awareness and social environment. The research conclusion points out that understanding the influencing factors of users' willingness to privacy settings is of great significance for designing better personal information protection mechanisms.

Yang's (2021) [34] research takes WeChat communication as an example to study the "privacy paradox" issue of social media. The research process involves observing and analyzing privacy issues in WeChat communication. The research mainly explores the privacy paradox in social media, where users face the risk of personal privacy leakage while enjoying the convenience brought by social media. The research conclusion emphasizes the need to balance the relationship between user experience and personal privacy protection in the development of social media.

Tan's (2021) [35] research focuses on privacy protection in nongovernment social media file archiving management. The research process involves investigating and analyzing the filing management system and practices of nongovernment social media

files. The research mainly explores privacy protection issues in nongovernment social media file archiving management, as well as current challenges and improvement directions. The research conclusion points out the need to strengthen privacy protection measures in nongovernment social media file archiving management to ensure the security of user personal information and respect for privacy rights.

Wang's (2022) [36] research explores the "human flesh search" and privacy protection in the new media era. The research methods include a literature review and case analysis. The research process involves the investigation and analysis of laws and regulations related to "human flesh search" behavior and privacy protection. The research mainly focuses on the impact of the "human flesh search" phenomenon on personal privacy rights in the new media era, as well as related privacy protection measures. The research conclusion emphasizes the importance of strengthening the regulation of "human flesh search" and protecting personal privacy rights.

Xiao's (2021) [37] research focuses on the compliance of personal information protection policies for social applications in China. The research methods include literature review and policy analysis. The research process involves collecting and analyzing relevant laws, regulations, and practical situations of personal information protection policies for social applications in China. The research mainly explores the compliance issues of personal information protection policies for social applications in China, as well as the areas that need to be strengthened. The research conclusion points out that China should further improve personal information protection policies for social applications and strengthen compliance supervision and supervision.

Wu's (2021) [38] research explores user privacy risks and protection in the context of social media development. The research methods include literature review and empirical research. The research involves investigating and analyzing the privacy risks of social media users. The research mainly focuses on the risks posed by the development of social media to user privacy, as well as related privacy protection measures.

2.3 Research Gaps

Based on the content of the provided text, it can be seen that there is a current research gap regarding the research on the satisfaction of personal information protection of WeChat users based on blockchain technology. Although blockchain technology has attracted extensive attention from academia and industry in terms of personal information protection, the current research is relatively limited, especially in terms of satisfaction with the personal information protection of WeChat users.

Through the review of related studies in the paper, it can be seen that the existing studies focus on the following aspects: blockchain-based personal information management methods, personal health information data management, personal information transaction management, and personal data protection schemes. These studies revolve around how blockchain technology can be used to protect the security, integrity, and privacy of personal information.

However, research on the satisfaction of personal information protection of WeChat users has not received sufficient attention. WeChat, as one of the largest social networking platforms in China, has a large user base and a huge amount of personal information data. However, with the frequent occurrence of information leakage and misuse, users' awareness of personal information protection and privacy is gradually increasing, and research on the satisfaction of personal information protection of WeChat users has become particularly important.

Among the current research gaps, the following aspects can be explored:

(1) What is WeChat users' awareness and satisfaction of personal information protection? How much do users recognize the personal information protection measures of the WeChat platform?

(2) How can blockchain technology be applied to the protection of the personal information of WeChat users? Can blockchain technology provide a higher level of security, privacy protection, and data integrity?

(3) How receptive are WeChat users to blockchain technology-based personal information protection solutions? What are their expectations and needs for using blockchain technology to manage and protect personal information?

(4) What are the advantages and shortcomings of blockchain technology in the protection of the personal information of WeChat users? How to improve and make up for these shortcomings?

By conducting a study on the satisfaction of personal information protection of WeChat users based on blockchain technology, we can gain insight into users' attitudes and needs for personal information protection, explore the potential of applying blockchain technology on the WeChat platform, and provide a reference basis for relevant policymakers and technology developers.

CHAPTER 3

METHODOLOGY

With the rapid development of network technology, social platforms have become an indispensable part of people's lives. While social networks bring convenience and opportunities to people, they also pose hidden dangers to personal information security. WeChat, the most active platform on the mobile internet, is a mobile instant messaging software launched by Tencent on January 21, 2011. Through continuous updates and development of new features, it has a large user base, covering over 90% of smartphones, gradually evolving from a social tool to a comprehensive life service tool. Meanwhile, as a brand new platform for information production and dissemination, WeChat has the characteristics of limited dissemination objects, quasi-real name dissemination content, and semi-closed dissemination methods. The WeChat user group tends to be younger and more educated, with 45.4% of users between the ages of 18 and 25, with college students accounting for an important share. Although college students have a high level of education and strong personal information protection literacy, they are often high-risk victims of WeChat crimes. Therefore, studying the current situation of personal information protection for WeChat users and analyzing their existing problems will contribute to the horizontal extension of research related to personal information protection.

3.1 Personal Information Protection Model

WeChat is a popular communication platform with up to 1.2 billion monthly active users in China and globally. However, despite the convenience and user-friendliness of the platform, the protection of user personal data and privacy security have always been prominent issues. Due to the strict internet regulation, censorship, and filtering system of the People's Republic of China's government, the protection mechanism for data privacy and security on WeChat is particularly fragile. Therefore, the emergence of blockchain technology worldwide provides potential solutions for WeChat to address data privacy

and security issues, as this technology can enhance the protection mechanism, authentication, and data sharing mechanism of user personal data, while promoting transparency and trust between users. The objectives of this study are:

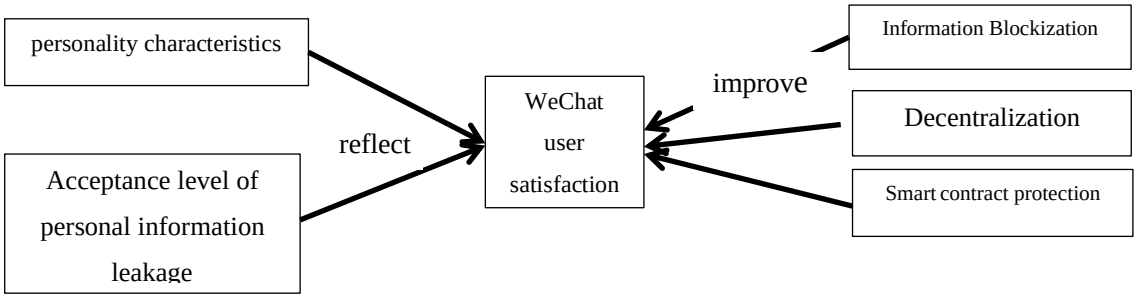
Objective 1: To the usage situation of WeChat users after applying blockchain technology to protect personal information?

Objective 2: To Analyze the impact of blockchain technology on the protection of personal information of WeChat users;

Objective 3: To Determine the satisfaction level of WeChat user personal information protection based on blockchain technology.

This article will use a hybrid method of quantitative and qualitative data to comprehensively understand WeChat users' attitudes, trust, and behavior toward data privacy and security. We will conduct a series of questionnaires, and interviews, and adopt various methods to analyze the results. Through questionnaire stars and interviews, we have collected quantitative data from participants using WeChat to gain a more comprehensive understanding and insight into the problem. This study aims to explore the satisfaction of WeChat users with personal information protection based on blockchain technology, gain a deeper understanding of their needs and expectations for personal information protection, analyze the advantages and disadvantages of personal information protection solutions based on blockchain technology, and provide theoretical and practical support for further improving the satisfaction of WeChat users with personal information protection. Based on the research results and analysis of WeChat users' satisfaction with personal information protection, this study will propose relevant suggestions and measures to improve WeChat users' satisfaction with personal information protection. These suggestions may include improvements at the technical level, formulation of policies and regulations, user education and awareness cultivation, etc., to promote the further development and improvement of personal information protection work.

Based on research hypotheses, an empirical model of WeChat user satisfaction with personal information protection based on blockchain technology is constructed from two aspects: individual characteristics and acceptance of personal information leakage,



The Application of Blockchain in Information Protection

Figure 3.1 Empirical Model of WeChat User Satisfaction with Personal Information Protection Based on Blockchain Technology

Based on surveys and interviews, analyze WeChat users from two aspects: personal characteristics and acceptance of personal information leakage, determine indicator independent variables and dependent variables, clarify the manifestation of WeChat user satisfaction, and analyze how blockchain technology can improve WeChat user satisfaction. By applying blockchain technology to personal information protection to improve WeChat user satisfaction, the characteristics of blockchain technology and the needs of WeChat users for personal information protection are utilized to transform the ways and methods of personal information protection. Applying blockchain technology to block information data, decentralize structure, level information, and manage smart contracts, establishing a three-dimensional and full lifecycle protection model, as well as a new management mechanism for de-trust, to address information protection needs such as preventing information leakage, tampering, and evidence tracing. By analyzing the personal characteristics and acceptance level of personal information leakage of WeChat users, we can better improve WeChat user satisfaction.

3.2 Application of Blockchain in Information Protection

Based on the characteristics of blockchain technology and the need for personal information protection to transform the way and method of personal Research on the application of blockchain technology to block information data, decentralize structure, hierarchize information and smart contract management, establish a three-dimensional

and full lifecycle protection model, and a new management mechanism of personal information protection. Research on the application of blockchain technology to block information data, decentralize structure, hierarchize information and smart contract management, establish a three-dimensional and full lifecycle protection model, and a new management mechanism of de- It proves the advantages and feasibility of blockchain in the field of information protection. It proves the advantages and feasibility of blockchain in personal information protection.

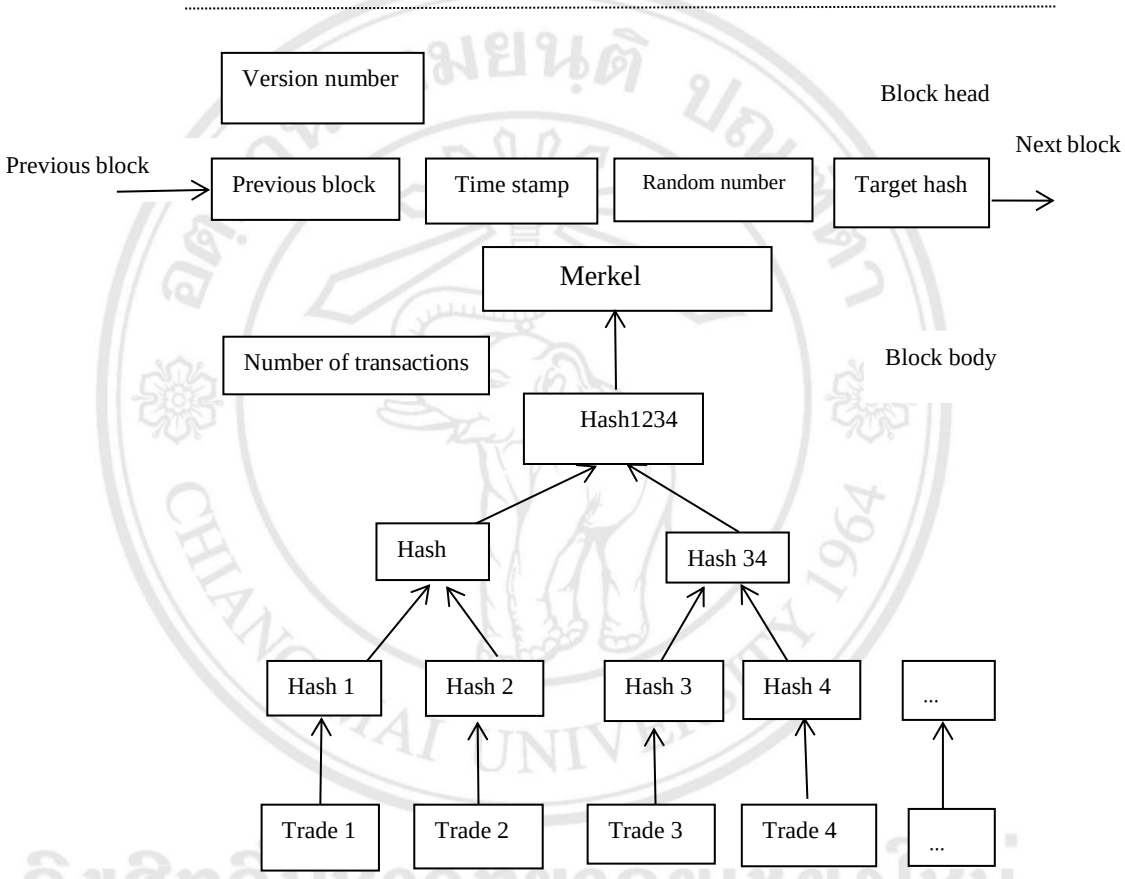


Figure 3.2 Blockchain structure model

(1) Information Blocking

Information is mainly streaming data, and the advantage of streaming data over batch data is that it is real-time and continuous. However, once the streaming data is attacked, intercepted, and analyzed by big data, it is easy to be stolen, and it is difficult to trace the flow of data [40]. The information is data blocked as shown in Figure 3.3. Each data block contains only a small part of the complete information and is asymmetrically

Each data block contains only a small part of the complete information and is asymmetrically encrypted with a hash function, and the integrity and consistency of the data is ensured by the chain structure and Byzantine, [41] MerK Tree, etc. It is easier Even under attack, a data block is difficult to break, let alone a data blockchain, and moreover, a data block is difficult to trace the time interception of the blockchain. Big data and other intelligent technologies are also difficult to reason intelligently to big data and other intelligent technologies are also difficult to reason intelligently to derive information, thus better ensuring the security of information. Blockchain adds a technical gap for information protection, and the information will have an additional guarantee.

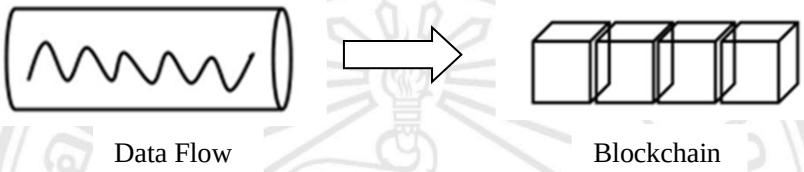


Figure 3.3 Blocking the Information Data Flow

(2) Decentralization of information

The centralized model is shown in Figure 3.4. A centralized system brings problems such as increased risk, increased costs, and limited node expansion. The central point of centralization has problems or crashes, which causes all nodes to fail and become unusable, increasing the risk of the system. The central point of centralization has problems or crashes, which not only causes all nodes to fail and become unusable, increasing the risk of system management, but also leads to overall and destructive information leakage once the central data is leaked. When there are more nodes at the same time, both the central computing and loading capabilities need to be large. If the capacity is insufficient, the risk of information leakage increases, so When there are a large number of nodes, centralization cannot establish the legitimacy and When there are a large number of nodes, centralization cannot establish the legitimacy and failure of nodes, and the risk of information leakage increases, so node expansion will inevitably be limited. These factors are not conducive to personal information protection.

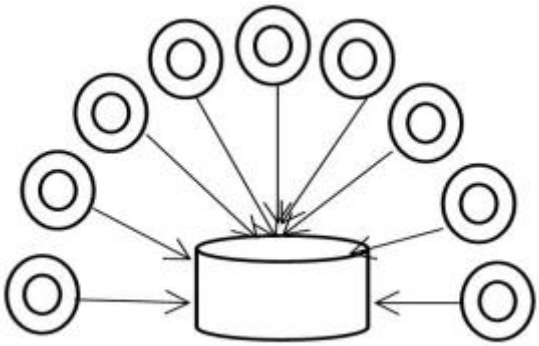


Figure 3.4 Centralization Model

Blockchain technology is also distributed, but its structure is weakly centered or decentralized, as shown in Figure 3.5. Decentralization is characterized by the fact that the information flow between nodes is not limited to the central point, and does not rely on a third party. Decentralization is characterized by the fact that the information flow between nodes is not limited to the central point, and does not rely on a third party [42]. The distributed nodes of the blockchain form P2P networks, verification mechanisms, and propagation mechanisms through open account books, consensus mechanisms, and distribution mechanisms. On the premise of security, reliability, and consistency among various nodes, point-to-point collection, and verification. On the premise of security, reliability, and consistency among various nodes, point-to-point collection, verification, storage, propagation, and management are carried out to avoid the high cost, high risk, and low efficiency issues of centralization. Decentralization of structure greatly reduces the risk of overall and significant information leakage.

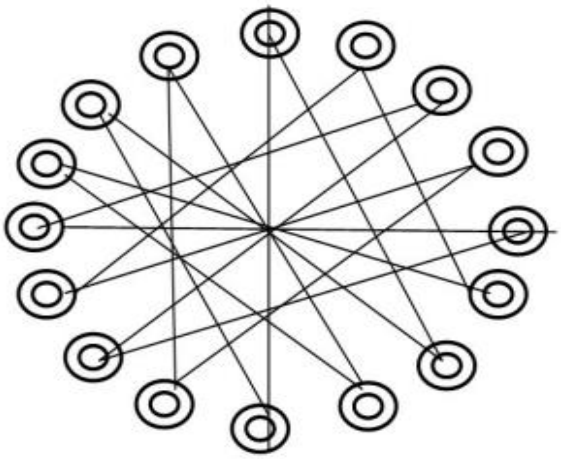


Figure 3.5 Decentralized Model

(3) Hierarchical smart contract protection for information

Transaction response or execution action must meet the established response conditions and response rules, and follow the process step by step to the transaction response or execution action must meet the established response conditions and response rules, and follow the process step by step to execute the operation, as shown in Figure 3.6. Each action must first verify its legality and condition satisfaction before executing the operation. Some operations require the state value of the previous operation to determine whether to proceed with the next step[43], making the operation complex Due to the step-by-step execution method, multiple operations cannot be executed continuously and automatically, resulting in low Due to the step-by-step execution method, multiple operations cannot be executed continuously and automatically, resulting in low efficiency.

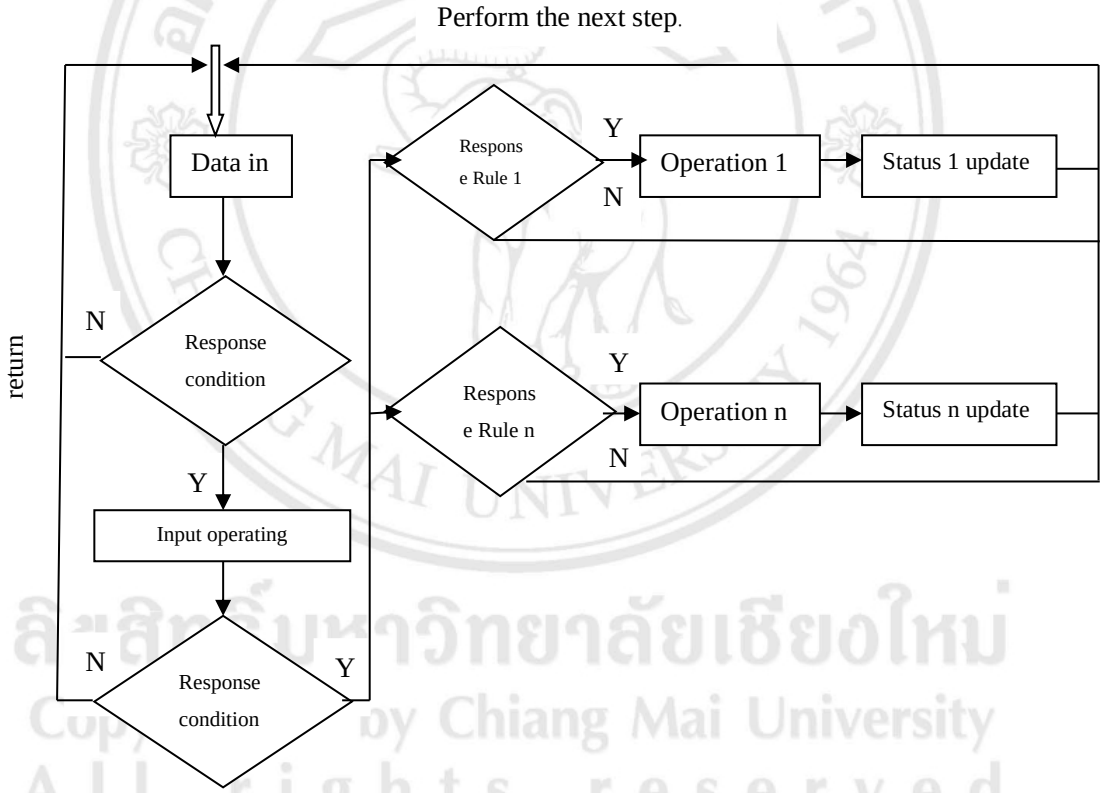


Figure 3.6 Traditional Transaction Execution Operation Mode

The smart contract of blockchain only needs to input data and events into the contract. If the original contract conditions are met, the on-chain code of If the original contract conditions are met, the on-chain code of the smart contract can continuously and

automatically perform multiple operations, as shown in Figure 3.7. For example, in smart homes, after signing an online rental payment for a house, the tenant obtains the identification code of the house's assets and can automatically open the door and use the house When the contract expires, the contract value is changed, automatically turning off the house, water and electricity switches, and checking the equipment. The status value of the asset is updated without the need for on-site confirmation. [44]Smart contracts automatically execute the business logic and legal rights and obligations of contracts, improve management efficiency, and provide a basis for information protection. According to the corresponding authorization or contract determined by the customer, the smart contract will automatically take different protection measures for According to the corresponding authorization or contract determined by the customer, the smart contract will automatically take different protection measures for information according to different levels.

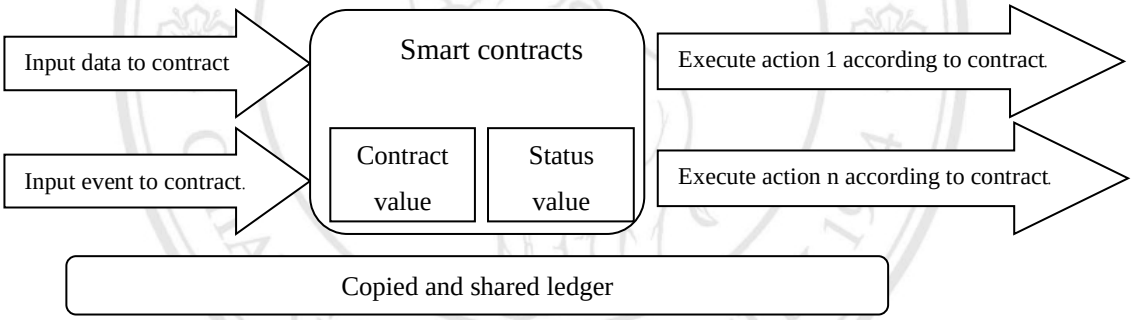


Figure 3.7 Smart Contract Model

(4) A three-dimensional protection model for information blockchain

The application of blockchain technology in information protection systems has inherent advantages of structural layers. The seven-layer structure of blockchain includes data layer, network layer, consensus layer, incentive layer, contract layer, and application layer, which can provide The seven-layer structure of blockchain includes data layer, network layer, consensus layer, incentive layer, contract layer, and application layer, which can provide comprehensive protection for the three-layer structure of information protection system perception layer, transmission layer [45], and application layer. With the big lock of smart contracts, blockchain protection of information is not limited to a

certain layer of protection, but rather a three-dimensional protection. Information is protected by blockchain technology throughout its entire lifecycle, from collection to storage, and use. Information is protected by blockchain technology throughout its entire lifecycle, from collection to storage, use, transfer, and deletion, making information protection more secure. The blockchain three-dimensional protection model is shown in Figure 3.8.

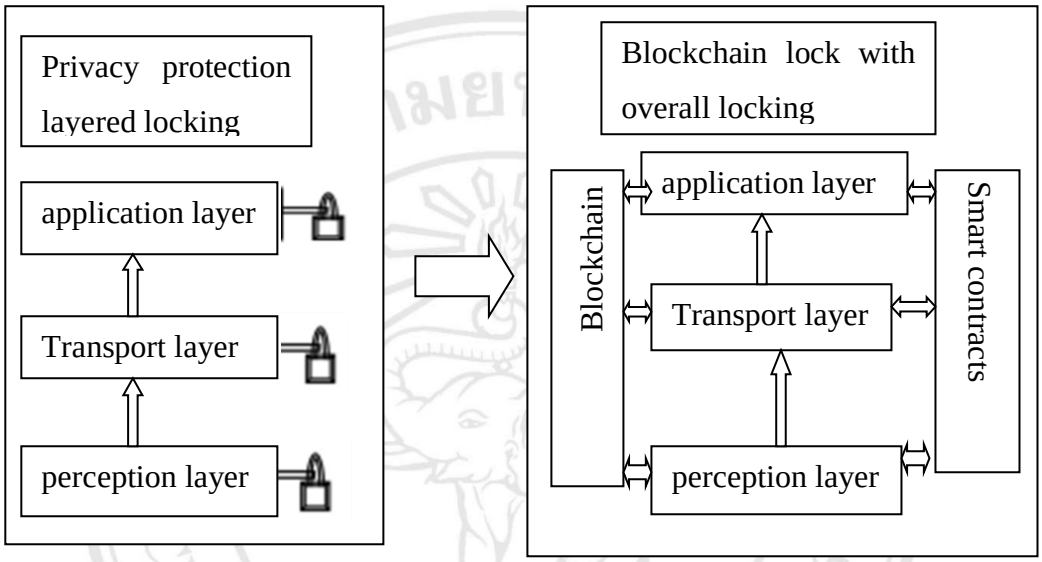


Figure 3.8 Blockchain Stereoscopic Protection Model

(5) A New Management Model for Removing Trust from Information

Blockchain technology is decentralized, and its application in information protection will inevitably lead to a change in management mechanisms, that is, from centralized management to decentralized or weakly centralized management[46], greatly reducing the chances of internal personnel such as system is, from centralized management to decentralized or weakly centralized management, greatly reducing the chances of internal personnel such as system At the same time, for any business operation and transaction behavior, blockchain will be recorded in chronological order. At the same time, for any business operation and transaction behavior, blockchain will be recorded in chronological order, and tamper proof, with traceable evidence, without the need for third-party supervision, reducing the opportunity for customers, enterprises, and In management, it is not about strengthening the restrictive measures of nodes, but

strengthening the design of consensus and incentive mechanisms to In management, it is not about strengthening the restrictive measures of nodes, but strengthening the design of consensus and incentive mechanisms to attract more nodes to join. While improving the mutual constraint and balance between nodes, it also While improving the mutual constraint and balance between nodes, it also enhances computing and storage capabilities, saving more costs.

3.3 Questionnaire Design

The questionnaire design mainly determines the questionnaire indicators through two forms. After preliminary surveys and comprehensive opinions from all parties, the survey questions are determined and divided into three parts: WeChat user demographic analysis, including gender, subject classification, and education level The basic information about using WeChat, including the duration of WeChat registration, the frequency of daily WeChat usage, and frequently used WeChat services The current situation of personal information security on WeChat platforms, including the willingness to disclose personal information on WeChat, whether personal information has been leaked, the content, channels, reasons for information leakage, and remedial measures after leakage. To understand the current situation of personal information protection for WeChat users, it is necessary to first determine the questionnaire indicators, and first determine the analysis indicators through in-depth interviews and the WeChat privacy system.

3.3.1 In-depth interviews

In-depth interview is a common and widely applicable survey method, through communication with the interviewees can understand the real needs of users, so that Microsoft users better understand the meaning of the problem, while the results of the survey are more reliable.

(1) Interview 18 WeChat users of different age levels for in-depth interviews, the interviewees must meet the following conditions:

① Using WeChat for more than 5 years

② Using WeChat as the main social networking software

③ Combined use of WeChat for more than 3 hours per day

④ Proficiency in using WeChat functions Since this research mainly analyzes WeChat personal information protection services, the research subjects are all ordinary WeChat users and do not cover WeChat platform staff, the interview locations are random, some interviews are conducted through WeChat videos, and the interview time for each respondent is controlled within 15-20 minutes.

(2) Design of interview questions This interview was an open-ended interview, in which a brief explanation was given to the interviewees before the interview to explain the concepts involved in the interview process, followed by questions about the protection of personal information in WeChat. The interview questions were as follows:

① Have you ever been concerned about the protection of personal information in WeChat?

② Do you authorize your personal information to other links?

③ Would you click on links like "Take a 2023 horoscope"?

④ What kind of content do you post in your circle of friends? What is the visible range?

⑤ Which features of WeChat do you think are more likely to leak personal information?

(3) How much do you know about the personal information protection measures provided by WeChat?

Since each respondent has a different background in life, the specific questions for each respondent will be modified from the above questions, and the questions will be expanded based on the respondent's answers after the questions are asked of the respondent. For example, respondents with minor children in the family were asked about their children's use of WeChat.

(4) Extraction of questionnaire indicators through in-depth interviews

During the interview process, these 18 WeChat users answered 100% of the questions, communicated with the respondents in a timely manner to reduce problems such as low data quality caused by the respondents' misunderstanding of the questions, and made

records of the interview content at any time to ensure the authenticity of the survey data. The questions answered by the respondents were summarized after the interviews, and 12 index elements were extracted through in-depth interviews (see Table 3.1).

Table 3.1 Indicator elements extracted through in-depth interviews

Number	Personal Information Protection Services	Number	Personal Information Protection Services
1	Real Name Authentication	7	Do not allow strangers to view the circle of friends
2	Login to the game requires authorization	8	You need to pass the verification when adding friends
3	Set access rights to your circle of friends	9	The applet requires authorized login
4	Device lock, sound lock	10	Other devices require my consent to log in
5	SMS verification code login WeChat	11	You can freeze WeChat when you lose your phone
6	The circle of friends "three days visible"	12	Refer a friend through your phone's address book

3.3.2 Literature combing to obtain indicators

By reviewing the WeChat Privacy Guidelines, a total of 30 indicators were extracted (see Table 3.2).

Table 3.2 Literature Review

Serial number	Name	Serial number	Name
1	Collect nicknames, cell phone numbers, and other basic information	16	National and defense-related unauthorized collection of information
2	Select whether to provide voice fingerprint-sensitive information	17	Unauthorized collection of information related to public safety, etc.

Table 3.2 Literature Review (Cont.)

Serial number	Name	Serial number	Name
3	Collect log information such as device model number	18	Unauthorized collection of information related to crime investigation, etc.
4	Friendship information will be stored on the server	19	Unauthorized collection of information for the safety of life and property
5	No personal information is provided to third-party software	20	Can collect information that users disclose to the community on their own
6	Nearby people, shake, etc. record location information	21	Collection of legally reported personal information without authorization
7	Using the WeChat Games to collect step-by-step information	22	May collect information on performance and contracting without authorization
8	Using Search, etc. will record search information, etc.	23	Information can be collected to maintain the security and stability of the product or service
9	Voice input collects voice information	24	Information needs to be gathered to conduct legitimate journalism
10	WeChat payment will collect bank card information	25	De-identification of information to be collected for academic purposes
11	Using WeChat Pay will collect transaction records	26	Other cases specified by law will collect personal information
12	Interoperability with other software with the option of public information	27	No unsolicited provision of user information to third parties

Table 3.2 Literature Review (Cont.)

Serial number	Name	Serial number	Name
13	WeChat moment video will be stored in the server	28	Use SSL encryption technology to protect user information
14	You can set whether to show game information to your friends	29	Protecting user information with anonymization processing
15	Access to location information after authorizing third-party services	30	Personal information can be deleted by yourself

3.3.3 Determination of Index Elements

The 12 indicators collected from the interviews were collated with the 30 indicators extracted from the WeChat Privacy Guidelines, such as "Table 3.1 (2) Authorization required to log in to games, Table 3.1 (9) Authorization required to log in to applets" and "Table 3.2 (15) Access to location information after authorizing third-party services". Table 3.2 (15) "Authorization of third-party services to obtain location information", etc. After sorting, we got a total of 28 indicators (see Table 3.3).

Table 3.3 Indicator Elements of the First Draft of the Questionnaire

Serial number	Name	Serial number	Name
Q1	Collect nicknames, cell phone numbers, and other basic information	Q15	CaiPay will collect WeChat payment record information
Q2	Select whether to provide voice fingerprint-sensitive information	Q16	Collects voice-to-text conversion information but does not save it
Q3	Collect log information such as device model number	Q17	You can freeze your own WeChat through your friends
Q4	Login to WeChat via SMS verification code	Q18	Delete all personal information when canceling your WeChat account

Table 3.3 Indicator Elements of the First Draft of the Questionnaire (Cont.)

Serial number	Name	Serial number	Name
Q5	Set your own access rights to your circle of friends	Q19	You can complain when you encounter infringement
Q6	The data for uploading friends is stored on the server	Q20	Use SSL encryption technology to protect user information
Q7	Authorization is required to log in to the applet and APP	Q21	Protecting user information with anonymization processing
Q8	Authorization is required to obtain geolocation information	Q22	National and defense-related unauthorized collection of information
Q9	Verified information required for "infrequently used devices" login	Q23	Unauthorized collection of information related to public safety, etc.
Q10	A customizable way for strangers to add friends	Q24	Unauthorized collection of information related to crime investigation, etc.
Q11	Step information will be collected when using WeChat Sports	Q25	Unauthorized collection of information for the safety of life and property
Q12	Search information is recorded when using functions such as "Search".	Q26	Can collect information that users disclose to the community on their own
Q13	The address book feature collects encrypted information	Q27	Collection of legally reported personal information without authorization
Q14	The payment function collects information about the bank card	Q28	Personal information can be collected when conducting legitimate journalism

3.3.4 Questionnaire composition

The questionnaire was designed based on the 28 indicators obtained from the above survey results and was divided into three parts:

(1) The first part is a general survey on the satisfaction of personal information protection of WeChat, divided into five levels, namely "very satisfied", "satisfied", "indifferent", "dissatisfied", "very dissatisfied", "dissatisfied", "very dissatisfied", dividing the options into five levels, avoiding low-quality answers caused by too absolute or too euphemistic emotions.

(2) The second part is a survey of personal information of WeChat users, including user gender, age range, and education, in which age is divided into four grades: below 18, 18-28, 28-50, and above 50, with a large age span, based on the following: the user group below 18 is almost in the student age of high school and below, the WeChat users aged 18-28 are basically in the university They are in the age group of light letter users, 28-50 years old users are in the working stage, and over 50 years old users are in the retirement stage, because of the short release time of WeChat, this part of the user group has a low acceptance and usage rate of WeChat;

(3) The third part is the WeChat personal information protection questionnaire, which is the main part of the questionnaire, and the questionnaire is designed by "Questionnaire Star". To investigate the satisfaction level of WeChat users, from "I like it a lot", "I should", "I don't care", "I can tolerate it", "I don't like it", and "I don't like it". "I like it a lot", "I deserve it", "I don't care", "I can stand it", "I don't like it", and "I don't like it", and assigning values to these five emotional levels, with scores of 1, 2, 3, 4, and 5.

3.3.5 Question item correction

In order to improve the quality of the questionnaire and the authenticity of the sample data, 10 WeChat users (mainly teachers and graduate students of related disciplines) were booked to fill in this questionnaire before the formal research was conducted to check whether the questions were clearly formulated and easy to understand, and whether the questions were set reasonably, etc. Based on the suggestions made by these 10 users, the questions were integrated and modified, and the questionnaire was further improved.

The situation of collecting users' personal information in accordance with legal requirements, as stated in the "WeChat Privacy Protection Guidelines," is considered an uncontrollable factor. Therefore, Questions 22 to 28 in Table 3.3 should be removed. Questions 21 and 20 in Table 3.3 should be integrated as "Protecting personal information using encryption technology." Due to the wide age range and diverse educational levels of the respondents, the questionnaire questions were formulated using simple and accessible language to ensure that the respondents could correctly understand the meaning conveyed by the questionnaire and patiently answer all the questions. This approach aimed to enhance the data quality of the sample. After compilation, a total of 20 items were determined for the questionnaire (refer to Table 3.4).

Table 3.4 Questionnaire Items

Serial number	Name	Serial number	Name
Q1	Collect basic user information when registering for WeChat	Q11	Step information will be collected when using WeChat Sports
Q2	Select whether to provide voice fingerprint information	Q12	Search information is recorded when using functions such as "Search".
Q3	Collect log information such as device model number	Q13	The address book feature collects encrypted information
Q4	Login to WeChat via SMS verification code	Q14	The payment function collects information about the bank card
Q5	Set your own access rights to your circle of friends	Q15	CaiPay will collect WeChat payment record information
Q6	The data for uploading friends is stored on the server	Q16	Collects voice-to-text conversion information but does not save it
Q7	Authorization is required to log in to the applet and APP	Q17	You can freeze your own WeChat through your friends
Q8	Authorization is required to obtain geolocation information	Q18	Delete all personal information when canceling your WeChat account
Q9	Verified information required for "infrequently used devices" login	Q19	You can complain when you encounter infringement
Q10	A customizable way for strangers to add friends	Q20	Use of encryption technology to protect personal information

3.4 Variable settings

In this thesis, we define, assign values to, and anticipate the direction of the independent variables influencing the dependent variable for each variable in the regression model of the satisfaction of personal information protection of WeChat users based on blockchain technology, as shown in Table 3.5.

Table 3.5 Definition, Type and Value Range of Each Variable

Title Number	Variable Name	Variable Type
A1	Villager satisfaction(Y)	Dependent variable
B2	Gender(X1)	Independent variable
B3	Age(X2)	Independent variable
B4	Marital status (X3)	Independent variable
B5	Education level (X4)	Independent variable
B6	WeChat usage time (X5)	Independent variable
C7	Collect basic user information when registering for WeChat (X6)	Independent variable
C8	Select whether to provide voice fingerprint information (X7)	Independent variable
C9	Collect log information such as device model (X8)	Independent variable
C10	Log in to WeChat (X9) via SMS verification code	Independent variable
C11	Set your own access rights to your circle of friends (X10)	Independent variable
C12	Data for uploading friends is stored on the server (X11)	Independent variable
C13	Login to the applet, APP requires authorization (X12)	Independent variable
C14	Authorization required to obtain geolocation information (X13)	Independent variable

Table 3.5 Definition, Type and Value Range of Each Variable (Cont.)

Title Number	Variable Name	Variable Type
C15	"Infrequently used devices" login requires verification information (X14)	Independent variable
C16	A customizable way for strangers to add friends (X15)	Independent variable
C17	Collect step information when using WeChat Sports (X16)	Independent variable
C18	Search information is recorded when using functions such as "Search" (X17)	Independent variable
C19	The address book function collects encrypted information (X18)	Independent variable
C20	The payment function collects information about the bank card (X19)	Independent variable
C21	CaiPay will collect WeChat payment record information (X20)	Independent variable
C22	Collects voice-to-text conversion information but does not save it (X21)	Independent variable
C23	You can freeze your own WeChat through your friends (X22)	Independent variable
C24	Delete all personal information when canceling a WeChat account (X23)	Independent variable
C25	You can complain when you encounter infringement (X24)	Independent variable
C26	Use of encryption technology to protect personal information (X25)	Independent variable

This article mainly focuses on the WeChat user group as the research object, and uses the questionnaire survey method to investigate the current situation of personal information security on the WeChat platform from four aspects: personal information disclosure willingness, personal information leakage content, personal information leakage channels, and relief measures. Research has found that the WeChat user group is a loyal follower of WeChat, but the security situation of their personal information on the WeChat platform is not optimistic. The design purpose of the variables is to draw conclusions and propose optimization suggestions based on the research results: to improve the legal system for personal information protection, improve the administrative supervision mechanism for personal information protection, strengthen the self-discipline of the WeChat platform industry, enhance users' personal information security literacy, and strengthen the construction of personal information ethics and morality.

CHAPTER 4

RESULT AND DISCUSSION

4.1 Data Collection

The questionnaire was collected from April to June 2023, lasting for 3 months. The sample sampling method was random sampling. Due to the survey group being WeChat users, most of the questionnaires were distributed through WeChat in the form of questionnaire stars, while a small portion were distributed in the form of paper questionnaires in the neighborhood. In order to avoid consistency in certain attributes brought about by social circles, such as education, academic background, living environment, age, etc., a portion of questionnaires are distributed through shopping groups to guide users to fill out paid forms, greatly ensuring the diversity of user basic information. When distributing questionnaires, the following principles should be followed: ① During WeChat group distribution, obtain the consent of the group owner before distributing the questionnaire; ② The sample age and educational level cover a comprehensive range; ③ Ensure the authenticity of the data filled in by users; ④ Declare that this data is only for academic research and will not pose any threat to the user's personal information.

This survey adopts non probability sampling method, and through channels such as the "Questionnaire Star" network platform and WeChat friend radiation, real-time monitoring is carried out during the survey questionnaire filling process. Multiple rounds of questionnaires are distributed to make the number of people filling out the questionnaire more reasonable. A total of 348 questionnaires were sent out, and 341 valid questionnaires were collected, with an effective recovery rate of 97.98%. There are 156 males (45.75%) and 185 females (54.25%) in the survey sample; There are 205 undergraduate students (60.12%), 136 graduate students or above (39.88%); There are 133 students (39%) majoring in humanities, 107 students (31.38%) majoring in science, and 101 students (29.62%) majoring in engineering. The proportion of respondents is basically balanced.

4.2 Data analysis (reliability and validity analysis)

4.2.1 Reliability analysis

In this thesis, the statistical software SPSS 20.0 was used to test the internal consistency of the scales, which was expressed as Cronbach's alpha coefficient. Reliability, introduced by Spearman in 1904 and used in psychological measurement [47], refers to the stability and consistency (homogeneity) of the results measured by a test, scale, or questionnaire constructed from several questions, and is generally expressed as a reliability coefficient. Reliability analysis can be used to test the reliability of a questionnaire measure by examining the degree of consistency of the user's answers to all questions on the same scale when completing the questionnaire. The commonly used reliability tests are fold-half reliability, Cronbach'sa coefficient, and retest reliability. Here, Cronbach'sa coefficient is used to test the reliability of the measurement. [48] L.J. Cronbach proposed this method of intrinsic reliability analysis in 1951 to test the homogeneity of questionnaire surveys, using the coefficient calculation formula to obtain a value between 0 and 1. The higher the value obtained, the higher the reliability, and the final result is influenced by the number of questions, and when the number of questionnaire questions is higher, a coefficient closer to 1, the higher the reliability will be.

If the reliability coefficient reaches 0.9 or above, it means that the questionnaire has high reliability; if the reliability coefficient is above 0.8 then the questionnaire is acceptable; if the reliability coefficient is above 0.7, it means that the questionnaire has some feasibility but should be modified more; if it is below 0.7, then the questionnaire basically loses its use value. The questionnaire data were imported into SPSS22.0 for reliability test, and the Cronbach'sa value of this questionnaire was 0.899 for the positive questions and 0.903 for the negative questions (see Table 4.1 and Table 4.2), which indicates that the reliability of the questionnaire is high, the test results of the questionnaire are more reliable, and the questionnaire has a good internal consistency.

Table 4.1 Reliability Analysis of Reverse Problem

Cronbach's Alpha	Number of projects
0.899	24

Table 4.2 Reliability analysis of the forward problem

Cronbach's Alpha	Number of projects
0.903	24

4.2.2 Validity Analysis

Scale validity is a measure of the truthfulness of a scale, and scale validity testing is the collection of theoretical and empirical evidence from a variety of sources by the user of the measurement scale to demonstrate that the scale can provide a valid analysis of the true situation. The questionnaire for this study was a paper-based field distribution questionnaire, which was filled out anonymously by the person completing the questionnaire, and was specifically stated and requested to be filled out based on intuitive impressions prior to answering the questionnaire. Although the researcher followed the whole survey process and tried to emphasize the objectivity of the completed questionnaire in order to reduce the error, the bias may still exist.

In order to reduce the impact of bias on the study results and mislead the findings, this study used the KMO [49] test and Bartlett's spherical test to test the validity of the organizational identity scale itself. In detail, the KMO statistic takes values from 0 to 1. If the squared simple coefficient within variables far exceeds the squared partial correlation coefficients, the KMO value is close to 1. The closer the KMO value is to 1, the closer the relationship between variables is and the more suitable the original variables are for factor analysis; if the squared correlation coefficients of different variables are much lower than the sum of squared correlation coefficients, the specific KMO value is infinitely close to 0. This status indicates that the independence of variables is maintained If the squared correlation coefficients of different variables are much lower than the sum of squared correlation coefficients, the specific value of KMO is infinitely close to 0. During the judgment work for Bartlett's spherical test, if it is a unit matrix, the different

variables remain independent, and the degree of fit for factor analysis is low. Most researchers use SPSS data statistical software to perform the test, and when Sig. < 0.05 (i.e., p < 0.05), it proves that the variables are correlated with each other, and factor analysis can be performed. In this thesis, we used SPSS 22.0 to conduct a factor analysis of the Kano questionnaire on the personal information protection satisfaction of WeChat users (see Table 4.3.) The KMO statistic values belong to the interval from 0 to 1, and when the value is closer to 1, it the more suitable for factor analysis. After the factor analysis of the data, KMO = 0.859, when the KMO value is greater than 0.5, it means that the factor analysis can be conducted; when the Bartlett's sphericity test is less than 0.001, it means that the factor analysis is suitable, and the significance of this data is 0.000, which means that the data is relevant and suitable for factor analysis.

Table 4.3 KMO Test and Sphericity Test

Kaiser-Meyer-Olkin test		0.859
Bartlett	Approximate cardinality	10465.764
The sphere of	df	946
Checking	Sig.	0

4.3 Descriptive Analysis

4.3.1 WeChat Personal Information Protection Satisfaction Analysis

Based on the questionnaire data, a descriptive analysis of satisfaction with the protection of personal information in WeChat can be conducted, and according to Table 4.4, the variables can be briefly analyzed as follows:

Table 4.4 WeChat Personal Information Protection Satisfaction Statistics

Variables	Categories	Frequency	Frequency	Mean	Interpretation
1. Are you satisfied with the current personal information protection services provided by WeChat?	Very satisfied	19	5.33%	3.453	Moderate Level
	Satisfaction	37	10.67%		
	Doesn't matter	161	47.33%		
	Dissatisfaction	104	30.67%		
	Very dissatisfied	20	6.00%		

The table presents the distribution of responses regarding the satisfaction level with the personal information protection services provided by WeChat. The variable Are you satisfied with the personal information protection services provided by WeChat? is divided into five categories: "Very The variable Are you satisfied with the personal information protection services provided by WeChat? is divided into five categories: "Very Satisfied", "Satisfied" "Indifferent", "Dissatisfied", and "Very Dissatisfied".

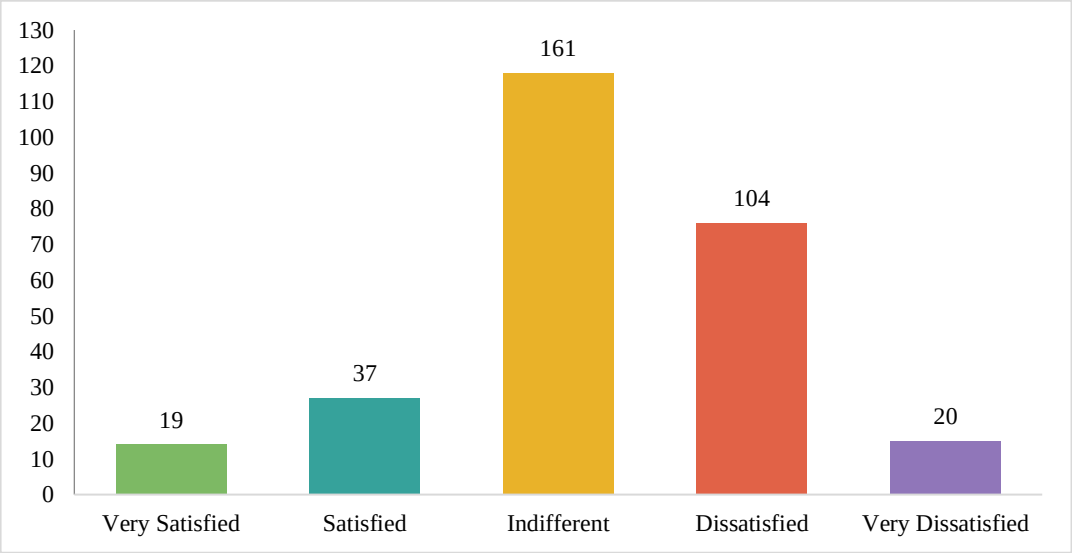


Figure 4.1 WeChat personal information protection satisfaction statistics

The frequencies and percentages of respondents falling into each category are provided in the table. For example, 8 respondents (5.33% of the total) expressed being "Very Satisfied", while 46 respondents (30.67%) reported being "Dissatisfied. For example, 8 respondents (5.33% of the total) expressed being "Very Satisfied", while 46 respondents (30.67%) reported being "Dissatisfied.

The mean score, calculated as 3.453, suggests a moderate level of satisfaction overall. This mean value indicates that the respondents, on average, expressed a moderate level of satisfaction with the personal information protection services provided by WeChat. This mean value indicates that the respondents, on average, expressed a moderate level of satisfaction with the personal information protection services provided by WeChat.

To determine the statistical significance of the findings, further analysis may be required. This could involve conducting hypothesis tests or performing inferential statistics to determine if the observed differences in satisfaction levels across the categories are statistically significant.

4.3.2 Descriptive analysis of individual characteristics

Based on the questionnaire data, descriptive analysis of individual characteristics, according to Table 4.5, a brief analysis of the frequency and percentage of each category in the sample for each of the different categories of each variable can be performed as follows:

Table 4.5 Descriptive analysis of individual characteristics

Variables	Categories	Frequency	Percentage
2. Gender	Male	156	45.75%
	Female	185	54.25%
3. Have you encountered any personal information leakage	Yes	211	61.88%
	No	130	38.12%
4. Education level	Below high school	66	19.35%
	Bachelor's degree	139	40.76%
	Master's degree	109	31.96%
	Ph.D. or above	27	7.92%

Table 4.5 Descriptive analysis of individual characteristics (Cont.)

Variables	Categories	Frequency	Percentage
5. User age	Below 18 years old	37	10.85%
	18-28 years old	92	26.98%
	28-50 years old	124	36.36%
	50-65 years old	63	18.48%
	Above 65 years old	25	7.33%
6. WeChat use time	Very rarely used	34	9.97%
	Infrequently used	51	14.96%
	Average	103	30.21%
	Frequently used	129	37.83%
	Very frequently used	24	7.04%

Through statistically significant analysis, researchers can further explore the degree of influence of different genders, marital statuses, education levels, ages and time of WeChat use on the satisfaction of WeChat users' personal information protection based on blockchain technology, in order to better understand users' needs and preferences and provide a basis for the design and improvement of personal information protection solutions.

The variables in the table include gender, marital status, education level, age, and time spent on WeChat. The following is a descriptive analysis of each variable:

(1) Gender of WeChat users: Male Number: 156, accounting for 45.75% of the total sample. Number of women: 185, accounting for 54.25% of the total sample. Exploring the impact of gender factors on satisfaction by comparing whether there is a significant difference in satisfaction between men and women with WeChat user personal information protection schemes based on blockchain technology, it was found that the distribution of gender factors is relatively balanced.

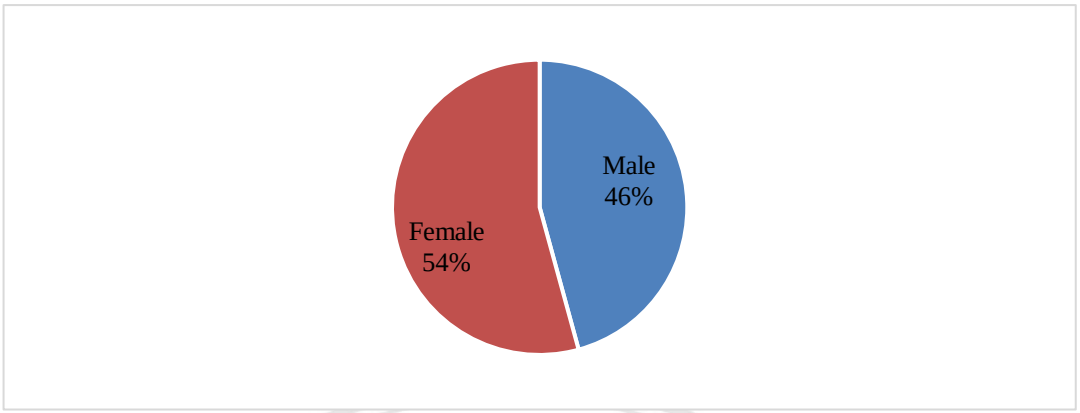


Figure 4.2 Gender status statistics of WeChat users

(2) Have you encountered personal information leakage? Yes, the number is 211, accounting for 62% of the total sample. No Quantity: 130, accounting for 38.00% of the total sample. Most of the people in the sample have experienced personal information leakage.

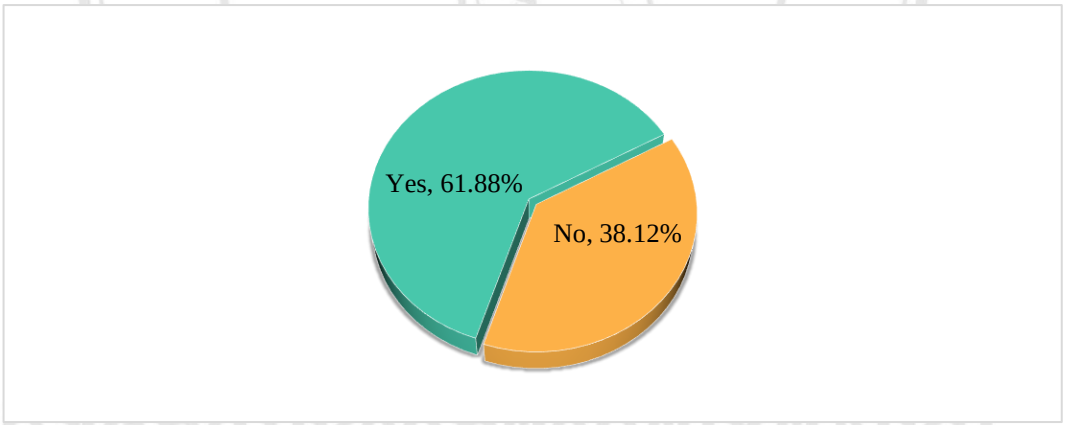


Figure 4.3 Have you encountered any personal information leakage statistics

(3) Education level: below high school: 66, accounting for 19% of the total sample. Number of undergraduate programs: 139, accounting for 41% of the total sample. Number of master's degrees: 109, accounting for 32% of the total sample. Number of PhDs and above 27, accounting for 8% of the total sample.

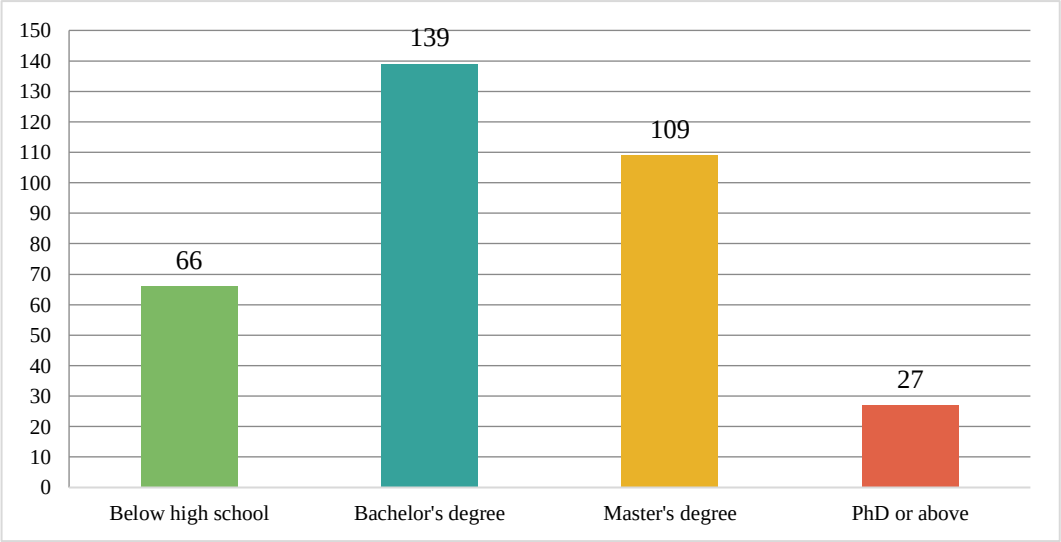


Figure 4.4 Statistics of Education Level

(4) User age: Under 18 years old Number: 37, accounting for 10.85% of the total sample. Number of 18-28 year olds: 92, accounting for 26.98% of the total sample. Number of people aged 28 to 50: 124, accounting for 36.36% of the total sample. Number of people aged 50-65: 63, accounting for 18.48% of the total sample. Number of people aged 65 and above: 25, accounting for 7.33% of the total sample

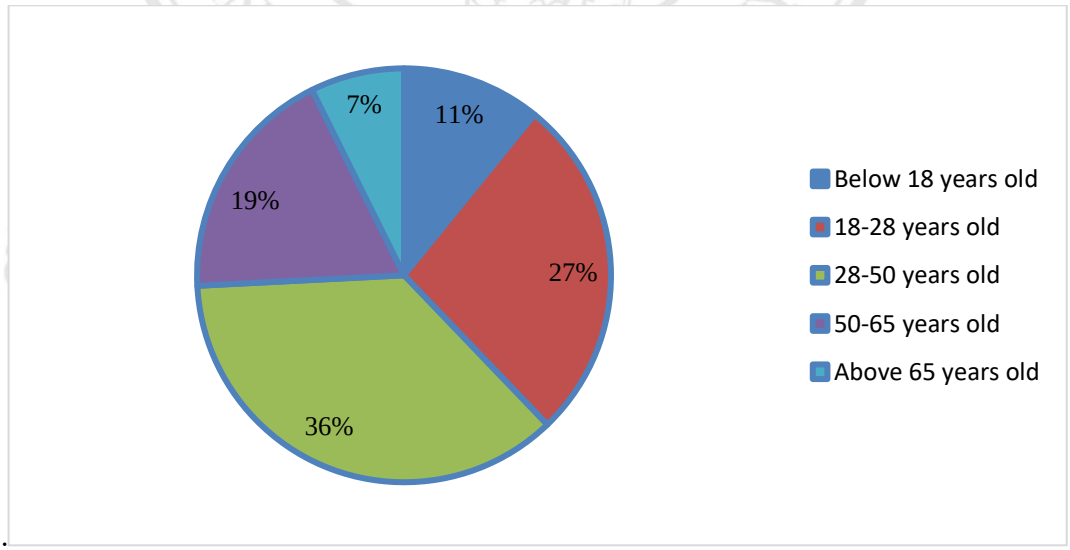


Figure 4.5 Statistics on the age status of WeChat users

(5) Daily WeChat usage frequency: Rare usage quantity: 34, accounting for 9.97% of the total sample. Not commonly used quantity: 103, accounting for 14.96% of the total sample. General quantity: 129, accounting for 30.21% of the total sample. The more commonly used quantity is 58, accounting for 37.83% of the total sample. Frequently used quantity: 24, accounting for 7.04% of the total sample.

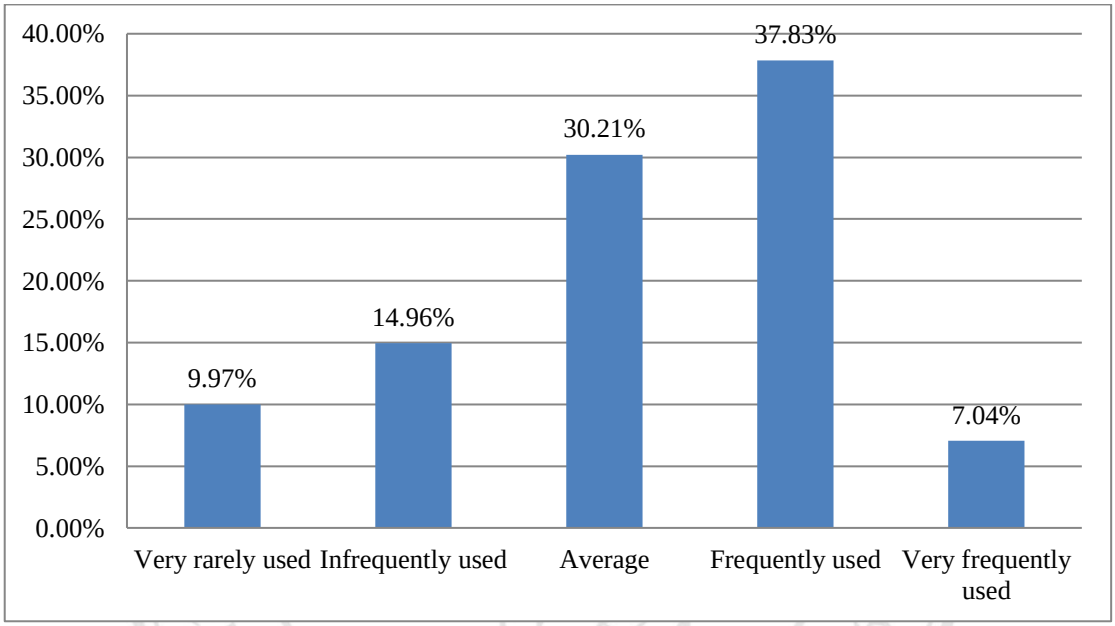


Figure 4.6 WeChat usage time status statistics

(6) User WeChat usage

According to Table 4.6, 42.82% of users have registered on WeChat for more than 3 years, 33.72% have registered for 2-3 years, and 23.46% have registered for less than 2 years. From this, it can be seen that the user group has been using WeChat for a long time and has a high loyalty to WeChat. In addition, out of 341 respondents, only 39 did not use WeChat every day, while the remaining 302 used WeChat more frequently, with nearly half of the users using WeChat more than 10 times a day. This indicates that WeChat applications have a strong allure for users and have become a "necessity" for some users.

Table 4.6 Time Profile of Users Using WeChat

problem	option	Number of people/person	Ratio/%
Registration duration	Less than 1 year	16	4.69
	1-2 years	64	18.77
	2-3 years	115	33.72
	Over 3 years	146	42.82
Frequency of use	Not used every day	39	11.43
	1-5 times	70	20.53
	5-10 times	74	21.70
	More than 10 times	158	46.33

Since its inception, WeChat has never stopped developing new features, as shown in Table 4.7. Social functions are the core function of WeChat applications. Among 341 respondents, 95.01% of users frequently use WeChat's messaging function (including sending text, voice, video, etc.), and 82.11% of users frequently use the Moments function. Other commonly used WeChat services for users are public platform (64.22%), WeChat payment (51.03%), QR code (33.43%), Yaoyiyao/nearby people (16.71%), Tencent games (15.54%), and WeChat shopping (11.43%). Users are relatively rational when using WeChat, but various WeChat services may leak their personal information, especially the use of functions such as shaking/nearby people, QR codes, etc., which puts users in unfamiliar external environments and increases the possibility of personal information leakage.

Table 4.7 Common WeChat Services for Users

Common WeChat services	Send a message	circle of friends	public platform	WeChat payment	QR code	Shake it/ People nearby	Tencent Games	Micro store shopping
Number of people/person	324	280	219	174	114	57	53	39
Ratio/%	95.01	82.11	64.22	51.03	33.43	16.71	15.54	11.43

4.3.2 Descriptive analysis of the degree of acceptance of personal information leakage

Based on the questionnaire data, a descriptive analysis of the degree of acceptance of personal information leakage, according to Table 4.8, a brief analysis of the frequency and percentage of each category in the sample for each of the different categories of each variable can be made as follows:

Table 4.8 Descriptive analysis of personal information Leakage acceptance level

Variables	Categories	Frequency	Mean	Interpretation
Collect basic user information when registering for WeChat (X6)	Dislike	11	3.473	Moderate Level
	Tolerable	9		
	Doesn't matter	155		
	As it should be	139		
	I like it very much	27		
Select whether to provide voice fingerprint information (X7)	Dislike	7	3.553	High Level
	Tolerable	55		
	Doesn't matter	106		
	As it should be	89		
	I like it very much	84		
Collect log information such as device model (X8)	Dislike	7	3.58	High Level
	Tolerable	14		
	Doesn't matter	127		
	As it should be	161		
	I like it very much	32		

Table 4.8 Descriptive analysis of personal information Leakage acceptance level (Cont.)

Variables	Categories	Frequency	Mean	Interpretation
Login to WeChat (X9) via SMS verification code	Dislike	102	3.767	High Level
	Tolerable	10		
	Doesn't matter	50		
	As it should be	88		
	I like it very much	91		
Set your own access rights to your circle of friends (X10)	Dislike	9	3.48	High Level
	Tolerable	25		
	Doesn't matter	136		
	As it should be	134		
	I like it very much	36		
Data for uploading friends is stored on the server (X11)	Dislike	9	3.453	Moderate Level
	Tolerable	34		
	Doesn't matter	111		
	As it should be	167		
	I like it very much	20		
Login to the applet, APP requires authorization (X12)	Dislike	5	3.52	High Level
	Tolerable	23		
	Doesn't matter	130		
	As it should be	158		
	I like it very much	25		
Authorization required to obtain geolocation information (X13)	Dislike	2	3.8	High Level
	Tolerable	14		
	Doesn't matter	98		
	As it should be	163		
	I like it very much	64		
"Infrequently used devices" login requires verification information (X14)	Dislike	2	3.787	High Level
	Tolerable	18		
	Doesn't matter	103		
	As it should be	145		
	I like it very much	73		

Table 4.8 Descriptive analysis of personal information Leakage acceptance level (Cont.)

Variables	Categories	Frequency	Mean	Interpretation
Customizable way for strangers to add friends (X15)	Dislike	2	3.787	High Level
	Tolerable	7		
	Doesn't matter	120		
	As it should be	144		
	I like it very much	68		
Collect step information when using WeChat Sports (X16)	Dislike	7	3.22	Moderate Level
	Tolerable	43		
	Doesn't matter	175		
	As it should be	100		
	I like it very much	16		
Search information is recorded when using functions such as "Search" (X17)	Dislike	7	3.16	Moderate Level
	Tolerable	43		
	Doesn't matter	191		
	As it should be	89		
	I like it very much	11		
The address book function collects encrypted information (X18)	Dislike	7	3.133	Moderate Level
	Tolerable	43		
	Doesn't matter	160		
	As it should be	7		
	I like it very much	124		
The payment function collects information about the bank card (X19)	Dislike	2	3.3	Moderate Level
	Tolerable	39		
	Doesn't matter	173		
	As it should be	109		
	I like it very much	18		
CaiPay will collect WeChat payment record information (X20)	Dislike	7	3.373	Moderate Level
	Tolerable	16		
	Doesn't matter	182		
	As it should be	116		
	I like it very much	20		

Table 4.8 Descriptive analysis of personal information Leakage acceptance level (Cont.)

Variables	Categories	Frequency	Mean	Interpretation
Collects voice to text conversion information but does not save it (X21)	Dislike	18	3.41	Moderate Level
	Tolerable	34		
	Doesn't matter	118		
	As it should be	132		
	I like it very much	39		
You can freeze your own WeChat through your friends (X22)	Dislike	25	3.29	Moderate Level
	Tolerable	36		
	Doesn't matter	118		
	As it should be	139		
	I like it very much	23		
Delete all personal information when canceling a WeChat account (X23)	Dislike	5	3.58	High Level
	Tolerable	30		
	Doesn't matter	95		
	As it should be	186		
	I like it very much	25		
You can complain when you encounter infringement (X24)	Dislike	11	3.52	High Level
	Tolerable	27		
	Doesn't matter	107		
	As it should be	164		
	I like it very much	32		
Use of encryption technology to protect personal information (X25)	Dislike	18	3.75	High Level
	Tolerable	27		
	Doesn't matter	85		
	As it should be	102		
	I like it very much	109		

Based on the data in the table, the lower-scoring option is

(1) X6: Basic user information is collected when registering for WeChat. A possible reason is that users have reservations about collecting personal information during the registration process. They may feel uneasy about providing personal details or think that too much information is collected.

(2) X16: Step count information is collected when using WeChat Sports. The lower score may be due to users' concerns about collecting and storing personal health data. Users may be reluctant to share their step information or have doubts about the use of the data.

(3) X17: Search information is recorded when using functions such as "search". A low score may indicate that users are concerned about their search history being recorded. Users may prefer to have more privacy and do not want their search activity to be tracked or recorded.

(4) X18: The Address Book feature collects encrypted information. A low score indicates that users have concerns about the collection and use of address book data, even if this data is encrypted. Users may be hesitant to share information about their contacts, due to privacy and security concerns.

These low scores indicate that users have reservations or concerns about the collection and use of personal information in specific areas. The importance of addressing users' privacy concerns and implementing transparent data protection measures to increase user satisfaction and trust in the WeChat platform is emphasized.

1. Willingness to disclose personal information of WeChat users

The root cause of information leakage lies in the conscious or unconscious disclosure of personal information by users. Therefore, exploring personal information protection in WeChat platforms inevitably requires understanding users' willingness to disclose personal information. Table 4.9 shows that 71.26% of users are unwilling to disclose personal information on WeChat, while 28.74% of users express their willingness to disclose it. Subsequently, a survey was conducted on the types of personal information disclosure among 98 respondents who were willing to disclose their personal information. 55 were willing to disclose their photos, while 60 were willing to disclose

their geographical location. The willingness to disclose information related to mobile phone numbers, family status, and other information was not strong.

Table 4.9 willingness of WeChat users to disclose personal information

problem	option	Number of people/person	Ratio/%
Are you willing to disclose personal information on WeChat platform?	Yes, because I believe that the WeChat platform can abide by its commitment to protecting users' personal information	55	16.13
	Yes, because I believe WeChat will consider my best interests when processing personal information	43	12.61
	Not willing, because I am worried that my personal information may be misused by others	243	71.26
What type of personal information are you willing to disclose on WeChat?	photo	55	56.12
	geographic location	60	61.22
	phone number	28	28.57
	Family situation	16	16.33
	other	13	13.27
What personal information have you authorized WeChat to access?	Read location information	238	69.79
	Accessing contacts	215	63.05
	Reading call logs	115	33.72
	Collect user usage behavior	83	24.34
	None of the above	22	6.45

In addition to actively disclosing information by users themselves, authorizing WeChat platforms to access user information can also indirectly disclose personal information. After investigation, it was found that only 6.45% of users have not authorized WeChat to access any information, while the remaining users have authorized the WeChat platform to access one or more personal information, such as location

information, contacts, call records, usage behavior, etc. Compared to direct disclosure, authorized access has concealment and paralysis, and most users are mistakenly guided to click authorization due to inertia. This also indirectly reflects that the information protection awareness of WeChat users needs to be strengthened.

2. The proportion and content of personal information leakage among WeChat users

In the information society, personal information is not only a distinctive symbol, but also an important strategic resource, used by enterprises for their hidden commercial value. It is precisely due to the value-added nature of information that transactions related to personal information are becoming increasingly profitable, leading to information leakage on social media platforms. As shown in Table 4, 42.52% of users have experienced personal privacy information leakage on the WeChat platform, with personal data being the most leaked information, followed by spatial information. Other personal information such as financial information and life information have been leaked to varying degrees. The current situation of personal information security for WeChat users is relatively severe.

Table 4.10 Proportion and Content of Personal Information Leakage of WeChat Users

problem	option	Number of people/person	Ratio/%
Have you ever encountered any personal information leakage during the use of WeChat?	Encountered	145	42.52
	Never encountered	196	57.48
Which personal information has been leaked?	Personal information (phone, email, address, etc.)	82	56.55
	Spatial information (location, activity trajectory, etc.)	80	55.17
	Communication information	53	36.55
	life information	48	33.10
	Financial Information	41	28.28

3. The ways and reasons for personal information leakage on user WeChat platforms

Due to the blind spots in personal information protection and hidden dangers in the use of various functions in WeChat software design, there are many ways for personal information leakage. This is a multiple-choice question. Respondents need to choose the most likely way to leak personal information from 3-5 WeChat platforms among the options. Among them, 58.94% of respondents choose to scan QR codes, 54.55% of users choose phishing website links, 52.20% of respondents choose software vulnerabilities, 43.69% of respondents believe that WeChat payment is also another major way to leak personal information, and 39.30% of respondents believe that location services will leak information, In addition, WeChat shopping, matching contacts, following WeChat public accounts, and testing games are all important ways for personal information leakage (see Table 4.11).

Table 4.11 Ways and Reasons for Personal Information Leakage on WeChat Platform

problem	option	Number of people/person	Ratio/%
The channels for personal information leakage	Scan QR code	201	58.94
	Phishing website link	186	54.55
	Software vulnerabilities	178	52.20
	WeChat payment	149	43.69
	Location Services	134	39.30
	Match Address Book	107	31.38
	WeChat public account	110	32.26
	Test Games	81	23.75
Reasons for personal information leakage	Incomplete legislation	166	48.54
	Lax enforcement by regulatory authorities	216	63.16
	Illegal collection by merchants	259	75.73
	Lack of personal protection awareness	237	69.30
	Lack of social information ethics and morality	157	45.91

From Table 4.11, it can be seen that 75.73% of respondents believe that the leakage of personal privacy information is driven by the interests of the merchant and illegally collected information; 69.30% of respondents believe that weak awareness of personal information protection is an important reason for privacy leakage; 63.16% of respondents believe that lax regulation is also a factor causing personal information leakage. In addition, imperfect legislation, lack of ethical ethics in information protection, and other factors, such as technological factors, are also important reasons for personal information leakage.

4. Reasons for failure to take measures after personal information leakage

After investigation, it was found that only 20% of respondents took remedial measures to defend their privacy rights when personal privacy information was leaked; The remaining 80% of respondents did not take remedial measures after experiencing personal privacy information leakage. From Table 6, it can be seen that 57.16% of users did not choose relief because they did not know who to seek it from, 31.86% of users believed that the leaked information did not have a significant impact on them, and 10.98% of users believed that the cost of relief was too high. From this, it can be seen that the current relief measures for personal information leakage in China are extremely lacking, and there are problems such as weak relief awareness and ineffective relief.

Table 4.12 Reasons for failure to take measures after personal information leakage

Reason options for failure to take remedial measures	Number of people/person	Ratio/%
Relief costs are too high	30	10.98
The leaked information did not cause significant losses to oneself	87	31.86
I don't know who to seek relief from	156	57.16

The impact of WeChat users' satisfaction with personal information protection can be determined through the analysis of personality description and acceptance level of personal information leakage. Based on the personal characteristics of WeChat users, the importance of using blockchain technology for the construction of personal information protection solutions can be analyzed based on the analysis of information data collected

by WeChat and the individual's tolerance for information leakage. The frequency of WeChat usage is increasing. With the development of mobile internet, WeChat builds a series of ecosystems, including social, entertainment, information, e-commerce, finance, and lifestyle platforms, produces content, establishes smart cities, and opens up the platform, allowing third parties to play a greater role in the WeChat ecosystem and jointly build the WeChat ecosystem. WeChat conducts comprehensive penetration around user needs, establishing fundamental high-frequency and vertical scenarios for users' mobile life, maximizing the attraction and retention of users, and increasing user stickiness. In addition, on the basis of WeChat payment, the WeChat ecosystem has formed its own unique e-commerce marketing method and transaction loop. These changes all benefit from the application of blockchain technology, making people's lives more convenient. By conducting a descriptive analysis of the acceptance level of personal information leakage, WeChat can be better optimized and technology can better protect personal information. Provide WeChat users with a better experience. In the past year, WeChat has driven a data traffic expenditure of 86.7 billion yuan, driving growth of 20% -25% in data traffic for the three major operators. The investigators stated that the use of WeChat accounts for the vast majority of smartphone usage time. Apart from social communication, the acquisition, forwarding, and forwarding of news and entertainment information are mostly generated on the WeChat platform. WeChat has become an important channel for the informatization of small and medium-sized enterprises. The proportion of companies or institutions using WeChat public platform accounts has reached 70%; Among them, 53% of users have already invested in informatization based on the WeChat platform. WeChat has also become an important entrepreneurial incubation platform, with over 600000 individual entrepreneurial activities driven by WeChat. WeChat has a significant driving effect on social employment. Currently, the number of employments driven by WeChat reaches 10.07 million people.

The application of blockchain technology for personal information protection revolves around key principles such as security, decentralization, transparency, and control. Security is a fundamental aspect of using blockchain for personal information protection. This technology provides a tamper-proof and immutable data storage method, ensuring that any attempt to modify information is detected by the network. By using encryption technology to protect data, individuals can be confident that their personal

information is protected from unauthorized access and network threats. Decentralization is another key principle for using blockchain for personal information protection. By storing data on distributed ledgers, the system avoids the need for central or intermediary institutions to manage data. This reduces the risk of single-point failures and provides greater resilience against attacks and data breaches. Transparency is also important for the protection of personal information on the blockchain. Individuals can choose which organizations can access their personal information and revoke access at any time. This gives individuals greater control over their data and ensures that they know how their personal information is used. Control is an important component of a blockchain-based personal information protection framework. By using their unique identity stored on the blockchain, individuals have greater control over their data and can manage their personal information without the need for third-party organizations to manage it on their behalf. This reduces the risk of data leakage and improves the efficiency of the system.

CHAPTER 5

CONCLUSION

5.1 Research Conclusion

Through a survey of the current situation of personal information protection among user groups on the WeChat platform, it was found that most users have a strong awareness of information protection, but the security situation of their personal information on the WeChat platform is not optimistic. With the continuous development of WeChat platform functions, the channels for personal information leakage are also increasing. The current weak protection of personal information on WeChat platforms is caused by various reasons, such as the macro legal system and supervision mechanism, the mid-level industry self-discipline and information ethics, and the micro-level personal literacy. The current situation of relief after personal information leakage is worrisome, with weak awareness of relief and a lack of access to relief.

5.2 Suggestions

The protection of personal information in WeChat platforms is a very complex system engineering, which can be achieved through multiple measures such as national legislation, administrative supervision, industry self-discipline, user literacy, and ethical construction, and comprehensive protection measures can be taken.

Information leakage brings many risks, even catastrophic consequences, but personal information protection awareness is still weak. Perhaps we should first clarify the path of the criminals' actions. Faced with the issue of information leakage, everyone may be a victim. To solve the problem, it requires the joint efforts of legislators, businesses, and individuals.

Table 5.1 Measures taken for personal information leakage

Projects	Measures
Legislators	Formulation of unified personal information protection laws
Enterprise	To comply with relevant laws and regulations. Respecting the user's right to information. Collecting the same type of information for the same kind of use, the user's consent must be obtained
Personal	Raise awareness of personal information protection by doing the following: Proper handling of courier orders, tickets, etc. timely removal of personal information data from old cell phones beware of phishing, luring personal information Cautiously link free WiFi; regularly change passwords; do not actively disclose personal information using security protection software

5.2.1 Improving the Legal System for Personal Information Protection

At present, in terms of personal information protection legislation in China, there are problems such as the lack of a unified "Personal Information Protection Law", and scattered and ineffective existing regulations, which are difficult to adapt to the needs of ensuring personal information security in the information age. Therefore, in order to establish a comprehensive legal system for personal information protection, the first step is to formulate a specialized "Personal Information Protection Law" [50], which defines the content of personal information, infringement methods, relief methods, punishment measures, etc., so that personal information protection has laws and regulations to follow. Secondly, after the promulgation of the Personal Information Protection Law, on the one hand, existing laws and regulations should be promptly modified and adjusted to address provisions related to personal information, maintaining consistency in the legal principles of personal information protection; On the other hand, it is also necessary to accelerate decentralized legislation, with the Personal Information Protection Law [51] as the center, and formulate personal information protection regulations targeting different industries. The legislation within the industry is more specific and operational, which can provide

detailed protection for personal information. The protection of personal information on WeChat platforms needs to accelerate legislation in the field of mobile internet, clearly stipulating the collection, processing, and use of user information by developers. Only by using rigid legal provisions to regulate possible infringement can personal information security be effectively protected.

5.2.2 Improving the Administrative Supervision Mechanism for Personal Information Protection

There are still many problems in the administrative supervision of personal information in China, which are inevitably related to the lack of compliance. The power of supervision comes from legal authorization. Therefore, in order to improve the administrative supervision mechanism for personal information protection, there is an urgent need for an independent regulatory body authorized by comprehensive laws to exercise the regulatory responsibilities for personal information protection. At present, the administrative supervision of personal information in China is mainly handled by the Ministry of Industry and Information Technology. [52] It is recommended to establish a national administrative supervision institution for personal information protection led by the Ministry of Industry and Information Technology. Secondly, after the establishment of an independent regulatory authority, a full process supervision mechanism for personal information should also be established. In advance supervision, it is necessary to establish a personal information sales license mechanism, control the channels of personal information outflow from the source, and allow information transactions to be legalized. In the process of supervision, establish a risk warning mechanism for personal information security, and regulatory authorities regularly inspect network service providers, issue risk warnings, and remind users to pay attention to security risks. In post supervision, establish a personal information reporting mechanism and a market exit mechanism. On the one hand, once a user's personal information is illegally leaked, they can seek relief through a reporting mechanism; On the other hand, businesses that have repeatedly encountered personal information security issues and information protection technologies that are not up to standard in the mobile internet will be subject to industry exit processing to urge mobile internet businesses to improve their information protection technologies.

5.2.3 Strengthen self-discipline in the WeChat platform industry

Under the premise of insufficient legal and regulatory power in the field of mobile internet, WeChat officials have the responsibility and obligation to provide users with a safe and clean information environment. Firstly, the WeChat platform should implement a user information disclosure system. On the one hand, when the information posted by a user is stored, reprinted, or shared by other users, the information publisher should be notified in a timely manner. Only after the publisher agrees can it be stored or disseminated. If the publisher refuses, it should be immediately stopped. On the other hand, when collecting and using user information, WeChat officials and merchants should also clearly inform users of the content of the collected information, the purpose and method of using their personal information, etc. Only with the user's consent can they collect and use it, and use technical means to protect the collected personal information. Secondly, pay attention to the effectiveness of privacy statements, refine the "WeChat Terms of Use and Privacy Policy" statement [53], and do not make the release statement mere formality, let alone use the privacy statement as an excuse to shirk responsibility. Finally, the WeChat platform simplifies the security settings steps, provides detailed explanations for various security settings in the software, and actively guides users to set up security settings.

5.2.4 Improving Users' Personal Information Security Literacy

Improving the current situation of personal information security on WeChat platforms and enhancing users' self-protection awareness is the fundamental solution to the problem. Firstly, users should maintain a sense of discrimination when using features that are prone to revealing personal information, and minimize the use of these features as much as possible. Secondly, be cautious when clicking on links with unknown sources, such as those related to name testing, constellation analysis, etc. that require input of name, date of birth, and phone number. Once again, in the face of various WeChat marketing activities such as sharing gifts and free lottery, one should withstand the temptation and not easily expose personal information. Finally, when personal information is infringed upon, do not condone the infringing behavior, and actively protect your own rights and interests.

5.2.5 Strengthen the construction of personal information ethics and morality

Unlike mandatory management methods such as information laws and policies, information ethics protect personal information through information values. Firstly, the government should increase publicity and education on the protection of personal information, enhance the protection awareness of information subjects and the protection quality of merchants, thereby promoting the formation of a social trend of protecting personal information and respecting the privacy of others. Then, incorporate personal information protection into the education system. The construction of information ethics and morality is a long and arduous task. To root information protection awareness in the national consciousness, it is necessary to pay close attention to the education of information ethics among young people and cultivate healthy information values.

5.3 Improving technical skills to reduce personal information leakage

Although strengthening personal information leakage from the above aspects can reduce some information leakage, it still faces the threat of information leakage due to various information technology reasons. With the advent of the blockchain era, smart contracts have brought the possibility of solving more practical application problems to blockchain. However, due to the open and transparent design of blockchain technology ledgers [54], the information security of users is affected. More seriously, due to the decentralized nature of blockchain, it cannot compensate for information leakage like centralized applications. In order to meet the protection needs of blockchain applications for user personal information, in recent years, relevant researchers have analyzed the problems in blockchain personal information protection and proposed corresponding solutions, providing guaranteed support for the safe implementation of blockchain applications.

In response to the issue of personal information leakage in blockchain, combined with the reasons and countermeasures for personal information leakage, a personal information protection system has been designed by introducing blockchain technology into the prevention and control of personal information leakage. By establishing solutions through blockchain technology, encryption technology, smart contracts, etc., [55] has constructed a blockchain sharing model in data security to more cost-effective and labor-

saving protect personal information. Play a key role in obtaining evidence after information leakage, analyze the advantages of blockchain technology in personal information protection, and use "technology+law" to prevent personal information leakage, thus bringing us a more harmonious society.

(1) The benefits of blockchain technology applied in different fields:

With the development of information technology and continuous innovation, blockchain technology has gradually deepened its application in fields such as digital recognition, financial transactions, data storage, and personal data management. Blockchain technology has also achieved many benefits in application fields (Table 5.2).

Table 5.2 The benefit of Blockchain by based on the different application areas

Application Areas	**Benefits of Using Blockchain Technology**
Digital Identification	1. Secure and reliable authentication. 2. Data privacy protection. 3. Data integrity and security. 4. Improved trust between parties.
Data Storage	1. Enhanced data security. 2. Increased data transparency. 3. Improved data traceability. 4. Cost savings due to reduced third-party involvement.
Personal Data Management	1. Increased user control over personal data; 2. Greater data privacy; 3. Improved identity management. 4. Reduced risk of data misuse.
Personal Finances	1. Improved financial security. 2. Reduced transaction costs. 3. Increased transparency. 4. Enhanced reliability of financial data

(2) Comparison of blockchain technology in application fields before and after

The application of blockchain technology has achieved certain results in different fields.

Table 5.3 Comparison of blockchain technology in application fields before and after

Main application areas	**Before application**	**After application**
finance	Complex process, centralized data storage, third-party guarantee	Simplify processes, improve data security, eliminate intermediaries, and reduce costs
network security	The central server stores data, transfers, and delivers	The information dissemination path has changed and cannot be intercepted
identity management	The identification process is cumbersome and prone to theft	Simplify the identification process and strengthen the protection of identity information
notarization	Require endorsement from third parties with strong credibility such as the government	Mathematical encryption for credit endorsement, permanently saving data
Supply Chain	Low efficiency, product fraud, low quality	Improve integrity assurance in all aspects, ensure product traceability, and ensure quality
vote	The counting of votes can be forged	The process is fully open and the votes can be traced back

(3) The application of blockchain in personal information protection targets (post monitoring and supervision)

The feasibility analysis of applying blockchain technology to personal information protection In the context of big data, the characteristics and advantages of blockchain technology can effectively compensate for the shortcomings of personal information protection, providing new ways to solve problems (Table 5.4).

Table 5.4 The working characteristics of blockchain applied in disciplinary inspection

Characteristics of blockchain	The application of blockchain in personal information protection targets (post monitoring and supervision)
Distributed architecture	1. Improved the efficiency of personal information protection, improved real-time verification and comparison 2. Decentralization ensures personal information sovereignty, and the OFID system implements real-name supervision 3. Provide a proof mechanism for judicial protection of personal information rights
Unmodifiable	Ensure the authenticity of evidence data during the case review process
Traceable	Being able to track and supervise the operational records of case handlers after information infringement
Timestamp	Clear case clues and investigation sequence

(4) The advantages of blockchain application for personal information protection

Decentralized blockchain has obvious advantages over traditional information storage methods in resisting external attacks. Blockchain also has the characteristic of anonymity, which still has a protective effect on directly recognized personal information. In any situation where identity verification is required, providing a public key self-certified virtual identity can replace directly providing sensitive identity information. This approach reduces the storage of personal information by social institutions for verification purposes and avoids illegal dissemination by insiders from the source.

When blockchain technology is introduced as the underlying data storage technology, even though the social status and transaction records posted by users are still open and transparent, different platforms have their own independent chains. Each blockchain adopts different anonymous technologies, and users have completely different virtual identities in different main chains.

The application of zero-knowledge proof has gradually shown the trend of decentralized databases surpassing centralized databases in personal information

protection [56]. For example, the electronic medical record cloud and other services provided by China's blockchain service platform Ping An One Account Chain have achieved accurate data sharing of user personal information in different occasions. The optimization of encryption technology enables more fields to use blockchain as the underlying technology to build distributed databases, strengthening users' control over personal information while also ensuring privacy.

Table 5.5 Main advantages of blockchain technology in network security

Blockchain technology	**Advantage**
Decentralization	Better transaction dispersion without third-party verification
Traceability	Adopting digital signatures and timestamps can more effectively obtain relevant information
Confidential	Using encryption algorithms for identity authentication
Sustainability	Distributed ledger and decentralized information storage
Integrity	Distributed ledger ensures that data is not modified or damaged
Quality	Encryption technology ensures the accuracy and quality of data
Smart contracts	Improving Security Standards and Verifying Conjugate Energy for Smart Contracts

The introduction of blockchain technology has provided new thinking for the improvement of personal information protection systems, which has also become a new attempt to promote legal systems through technology. The decentralized, encrypted, and tamper-resistant characteristics of blockchain can precisely meet the various needs of personal information protection. Of course, the personal information protection system is a complex system engineering, and there are still some risks in the implementation of technology. However, due to the high compatibility between blockchain technology and the personal information protection system, we should still give blockchain technology space to explore. We hope that blockchain technology can shine brightly in building a new trust mechanism, bringing true dawn to the construction of a personal information protection system.

CHAPTER 6

CONCLUSIONS AND FUTURE WORK

6.1 Conclusions

This article takes the WeChat user group as the research object and conducts a survey on personal information security on the WeChat platform through the distribution of questionnaires. On this basis, countermeasures and suggestions have been proposed to ensure the security of personal information on WeChat platforms, aiming to guide users to use WeChat reasonably and safely and promote the establishment of personal information protection mechanisms in the field of the Internet in China. However, there are still some shortcomings in this article, such as the lack of comprehensive and in-depth research on personal information protection on WeChat platforms, and the relevant suggestions proposed still need to be further improved in future research and practice.

The emergence of blockchain technology not only brings new technological advantages to personal information protection, but also potential risks to information protection. Faced with the current trend of blockchain technology, on the one hand, it is necessary to embrace technology and apply its advantages to personal information protection; On the other hand, it is also necessary to maintain a cautious attitude towards blockchain technology and address potential new issues that may arise in its application. As well as the legal challenges faced, it is necessary to combine technological and legal improvements with the development and application of technology to maximize technological advantages. This article mainly starts from the personal information leakage of WeChat users, explores the impact of WeChat user personal information leakage, and identifies the reasons for personal information leakage. It proposes some suggestions and measures that can be improved by using blockchain technology to prevent information leakage and find a way to prevent it. It is hoped that there will be new improvements in information protection and make some contributions to personal information protection. This article conducts research and discussion around the hot topic of "blockchain+personal information protection". In response to the current problem of

personal information leakage, a questionnaire survey is designed to understand the personality characteristics and willingness of WeChat users to disclose information, and provide solutions. The main work of this article is as follows:

(1) The background and research significance of this topic were introduced in detail, and the current situation of personal information leakage was investigated. Through a questionnaire, the reasons and characteristics of WeChat user information leakage were understood, and the reasons for information leakage were analyzed.

(2) We evaluated the level of awareness and understanding among WeChat users of blockchain technology, as well as their understanding of the potential application of blockchain technology in personal information protection, as well as their views on the feasibility and credibility of the technology. This includes an evaluation of the security, privacy protection ability, availability, and other aspects of the solution to understand the user's recognition and acceptance of the solution. Based on the research findings, it can be concluded that Tenpay collects WeChat payment record information, the payment function collects bank card-related information, user age, and collects voice to text conversion information but does not save it, which has the strongest impact on WeChat user satisfaction with personal information protection.

(3) Based on the current situation of personal information protection, suggestions and measures have been proposed. This method adopts blockchain technology, encryption technology, and zero-knowledge proof technology, and combines current legislative regulations in various countries to achieve more efficient, accurate, and low-cost results for personal information protection compared to traditional methods.

(4) Using blockchain for personal information protection, technology, and law develop together in the interaction. Technology can serve as an important tool to promote the construction of legal systems, while the law can provide macro direction for technological development.

6.2 Future Work

Blockchain technology conforms to the trend of technological development leading to the virtualization of production and life, and further weakens the use of blockchain in personal information protection proposed in this article, better achieving data security, and finding a new direction for the application of blockchain technology in personal information protection. The industrial era serves as a platform for credit endorsement and information intermediary, achieving personalized and peer-to-peer customized information processing for each node. However, blockchain technology is still developing, and many applications are in an unknown state. At the same time, the development of the internet has made it a reality to collect a large amount of personal information. Using personal information can deeply explore people's needs and achieve commercial value, which makes it necessary to specifically protect personal information through law. Blockchain technology and personal information protection laws are both in the process of development, so collisions at the border cannot be avoided. Blockchain technology is characterized by nodes using machines to decentralize data, while personal information protection law is based on data control and centralized processing of human information by processors. Personal information protection law is a system designed around people, while blockchain is centered around machines, programs, and algorithms. In real life, people are abstracted as nodes in cyberspace. Although the interaction between blockchain technology and personal information protection laws remains to be observed, the current development of blockchain technology still needs to consider and meet the requirements of personal information protection laws. In the era where the property value of personal information is infinitely expanded, the storage and sharing security of personal information should become a key aspect of personal information protection. The traditional legal single-system protection model has gradually been abandoned by the times. The introduction of blockchain technology has provided new thinking for the improvement of personal information protection systems, which has also become a new attempt to promote legal systems through technology. The decentralized, encrypted, and tamper-resistant characteristics of blockchain can precisely meet the various needs of personal information protection. Of course, the personal information protection system is a complex system engineering, and there are still some risks in the implementation of technology. However, due to the high compatibility between blockchain technology and

the personal information protection system, we should still give blockchain technology space to explore. We hope that blockchain technology can shine brightly in building a new trust mechanism, bringing true dawn to the construction of a personal information protection system.

REFERENCES

[1] Li, Q. (2022). Research on the Protection of Personal Information in Blockchain Technology. Discussion on Rule of Law Forum of World Artificial Intelligence Conference 2022.

[2] An Anthology (pp. 189-202). Shanghai Juridical Journal, No. 5, 2022.

[3] Regueiro, C., Seco, I., de Diego, S., Lage, O., & Etxebarria, L. (2021). Privacy-enhancing distributed protocol for data aggregation based on blockchain and homomorphic encryption. Information Processing & Management, 58(6), 102745.

[4] Xu, G., Qi, C., Dong, W., Gong, L., Liu, S., Chen, S., ... & Zheng, X. (2022). A Privacy-Preserving Medical Data Sharing Scheme Based on Blockchain. IEEE Journal of Biomedical and Health Informatics.

[5] Li, Y. (2022). Blockchain in IoT privacy, 335-337.

[6] Cao, X., Zhang, J., & Liu, B. (2021). A Review of Research on Blockchain Security, Privacy and Performance Issues. Computer Integrated Manufacturing Systems, 27(07), 2078-2094.

[7] Zhang, J., Gao, J., Wang, L., Li, Q., & Chen, Z. (2020). A review of blockchain privacy protection technologies. Security Science and Technology, (01), 26-29.

[8] Yu, X. (2019). Research and application of key technologies for blockchain privacy protection [Dissertation, Nanjing University of Posts and Telecommunications].

[9] Long H. Q., Hou J., Li Q. M., et al. (2021). Data privacy protection for industrial blockchain. Proceedings of the 10th International Conference on Cloud Computing, 83-99.

[10] Liang H., Hyung-Hyo L. A. (2020). Blockchain and cloud-based privacy protection scheme for medical data. Wireless Communication and Mobile Computing, 11.

[11] Cheng, L. (2021). Research on privacy protection of healthcare data based on blockchain [Master's thesis, Nanjing University of Posts and Telecommunications].

[12] Li, Y., Li, J., & Zhang, Y. (2017). Secure certificate-free signature scheme under standard model. Journal of Communications.

[13] Huifang Yu, Gao X. Z. (2019). A homomorphic ring signature scheme for multi-source network coding. Information Network Security, (2), 3642.

[14] Zhao, Y., Lai, Q., Yu, Y., (2018). Identity-based ring signature scheme in the standard model. Journal of Electronics, 46(4), 1019-1024.

[15] Tseng, Y. M., Huang, S. S., & Wu, J. D. (2017). Secure certificate-free signatures against persistent leakage attacks. In Proceedings of the International Conference on Applied System Innovation (ICASI 2017) (pp. 1263-1266).

[16] Li, K., Sun, Y., Zhang, J., Li, J., Zhou, J., & Li, Z. (2018). Technical challenges of applying zero-knowledge proofs in blockchain. Big Data, 4(01), 57-65.

[17] Fan, J., Zhang, Y., Nie, T., & Yu, G. (2021). Applications and prospects of blockchain technology in the Internet of Things. Computer and Digital Engineering, 49(12), 2407-2413.

[18] Wang, L., Guan, Z., Li, Q., Chen, Z., & Hu, M. S. (2021). A review of blockchain data security services. Journal of Software, 34(1), 1-32.

[19] Liu, J. L., Fu, Z. J., & Sun, X. M. (2019). A review of blockchain security. Journal of Nanjing University of Information Engineering: Natural Science Edition, 11(5), 513-522.

[20] Chen, J., & Xue, Y. (2017, June). Bootstrapping a blockchain based ecosystem for big data exchange. In 2017 IEEE international congress on big data (bigdata congress) (pp. 460-463). IEEE.

[21] Trikande, M., Kudale, S., Desai, A., & Kore, P. (2019). Integrating Blockchain for Data Sharing and Collaboration in Mobile Healthcare Applications. International Journal of Scientific Research in Science and Technology, 6(2), 520-525.

[22] Theodouli, A., Arakliotis, S., Moschou, K., Votis, K., & Tzovaras, D. (2018, August). On the design of a blockchain-based system to facilitate healthcare data sharing. In 2018 17th IEEE International Conference On Trust, Security And Privacy In Computing And Communications/12th IEEE International Conference On Big Data Science And Engineering (TrustCom/BigDataSE) (pp. 1374-1379). IEEE.

[23] Gordon, W. J., & Catalini, C. (2018). Blockchain technology for healthcare: facilitating the transition to patient-driven interoperability. Computational and Structural Biotechnology Journal, 16, 224-230.

[24] Azaria, A., Ekblaw, A., Vieira, T., & Lippman, A. (2016, August). Medrec: Using blockchain for medical data access and permission management. In 2016 2nd International Conference on Open and Big Data (OBD) (pp. 25-30). IEEE.

[25] Yang, H., & Yang, B. (2017, November). A blockchain-based approach to the secure sharing of healthcare data. In Proceedings of the Norwegian Information Security Conference (pp. 100-111). Oslo, Norway: Nisk J.

[26] Cao, S., Zhang, G., Liu, P., Zhang, X., & Neri, F. (2019). Cloud-assisted secure eHealth systems for tamper-proofing EHR via blockchain. Information Sciences, 485, 427-440.

[27] Liu, Y., Xia, Q., Li, C., Xia, H., Zhang, X., & Gao, J. (2020). Research on blockchain-based on-chain data security sharing system. Big Data, 6(5), 92-105.

[28] Yu, K., Tan, L., Aloqaily, M., Yang, H., & Jararweh, Y. (2021). Blockchain-enhanced data sharing with traceable and direct revocation in IIoT. IEEE Transactions on Industrial Informatics, 17(11), 7669-7678.

[29] He, K., Chen, X., Xie, S., Li, Y., Dollár, P., & Girshick, R. (2022). Masked autoencoders are scalable vision learners. in Proceedings of the IEEE/CVF Conference on Computer Vision and Pattern Recognition (pp. 16000-16009).

[30] Sward, A., Vecna, I., & Stonedahl, F. (2018). Data insertion in bitcoin's blockchain. ledger, 3.

[31] Gilder, G. (2018). Life after Google: the fall of big data and the rise of the blockchain economy. Simon and Schuster.

[32] Shafagh, H., Burkhalter, L., Hithnawi, A., & Duquennoy, S. (2017, November). Towards blockchain-based auditable storage and sharing of IoT data. in Proceedings of the 2017 on cloud computing security workshop (pp. 45-50).

[33] Pan, J., Wang, J., Hester, A., Alqerm, I., Liu, Y., & Zhao, Y. (2018). EdgeChain: An edge-IoT framework and prototype based on blockchain and smart contracts. IEEE Internet of Things Journal, 6(3), 4719-4732.

[34] Zhang, Z., Tian, J., & Kim, C. (2020). Trusted data sharing platform with on-chain storage and off-chain transmission. Big Data, 6(5).

[35] Liang, X. (2021). Exploring the issues of social media applications in the context of Web 3.0. Audiovisual(2), 139-140.

[36] Liu, W. J. (2021). Personal information protection on social networks. (2015-10), 133-136.

[37] Goya. (2021). The dilemma of online privacy in the age of social media and the way out. Global Premiere.

[38] Liu, Ja. (2022). Protection strategies for personal information of social media users. Mobile Information(11), 3.

[39] EY. (2021). An analysis of the civil law protection of personal information in the age of social media. Times, 000(029), P.1-2.

[40] Huang, D. (2022). A study of personal privacy exposure and protection mechanism in social media from the perspective of privacy paradox. Journal of Jilin Provincial College of Education, 38(11), 4.

[41] Chen, N., & Qiao, X.-F. (2021). Research on the mechanism and innovation of community information dissemination in social media environment. Technology and Innovation.

[42] Wu, C. (2021). Research on the civil law protection of personal information under the social media perspective. Legal expositions (Famous speakers, Classic essays).

[43] Gu, Z. (2022). The dilemma and breakthrough of legal protection of self-disclosed personal information in social media. Young journalists (7), 93-94.

[44] Lee, Y.-C. (2021). A study of parenting social media applications in the context of "use and satisfaction" (Doctoral dissertation, Jilin University).

[45] Cheng, H.-P., Zheng, Y.-F., & Wen, X.-Y. (2021). A study of factors influencing social media users' willingness to set privacy based on rooting theory. Modern Intelligence, 41(10), 130-139, 176.

[46] Yang, X. (2021). A study on the "privacy paradox" of social media: The case of WeChat communication. Journalism and Culture Construction (015), 000.

[47] Tan, C.-M. (2021). Research on privacy protection in archiving management of non-government social media documents. Archival World (6), 4.

[48] Wang, J. (2022). Research on "human flesh search" and privacy protection in the new media era. Journalism culture construction(2), 50-52.

[49] Xiao, X., Cao, Y., & Yufei. (2021). A study on the compliance of personal information protection policy of social applications in China. Intelligence Theory and Practice, 044(003), 91-100.

[50] Wu, G. (2021). Research on user privacy risk and protection in the context of developed social media. Satellite TV and Broadband Multimedia.

[51] Li, H., Yuan, Y.-M., & Zhao, W.-Q. (2020). Blockchain technology development and outlook. Journal of Agricultural Big Data, 2(2), 5-13.

[52] He, Y.-Y. (2020). Blockchain-based Internet of Things Technology Applications. Wireless Connected Technology, 17(7), 21-22.

[53] Yu, Q. (2019). Streaming big data real-time processing technology, platform and application research. Modern Information Technology, 3(1), 86-87.

[54] Benet, J. (2020). IPFS-Content Addressed, Versioned, P2P File System. arXiv 1407.3561.

[55] Wang, S.-F., Shi, J., & Shen, T. Y. (2022). Blockchain+ Technology and Practice. Tsinghua University Press.

[56] Lei, L. N., & Li, Y. (2018). A multi-authorization center access control scheme based on ciphertext policy attribute-based encryption. Computer Application Research, 35(1), 248-252.

APPENDICES

Looking back on the past, this thesis was completed under the guidance and guidance of my lecturer. From topic selection, and conception to the final draft, it was permeated by my lecturer, painstaking efforts, and sweat; My lecturers have profound knowledge and my rigorous learning style has benefited me for life. First of all, I would like to express my special thanks to my lecturer, whose profound knowledge, broad vision, excellent teaching style, modest and rigorous scholarship attitude, academic exploration and realistic spirit, and conscientious and responsible work style have benefited me a lot and deserve my lifelong learning. Under the guidance of my lecturer, I successfully completed the research and writing of my graduation thesis. I want to express my deep respect and gratitude here.

The experience of writing papers will also benefit me throughout my life. I think writing papers is what I really want to do with my heart. This is a real learning and research process. Without careful study and study, it is impossible to have the ability to research, and it is impossible to have its own research, and there will be no gains and breakthroughs. I hope that this experience will continue to inspire me to move forward in my future study and life.

I would like to thank my family, who have always cared about me, provided me with learning opportunities, and cheered me up every moment to promote my continuous growth and progress. At the same time, I would like to thank my roommate and all the friends who care about me and also thank them for accompanying me through many wonderful times. My study life has become wonderful and full. When I encounter difficulties, they care about me and help me. In the process of completing my graduation thesis, many friends have given me selfless help and support. I like to express my heartfelt thanks!

Finally, I would like to pay tribute to all the experts and professors who patiently guided the preliminary examination, review, and defense of the thesis, and sincerely thank you for your valuable comments and suggestions for this article. Because of my limited level, my thesis must have many shortcomings. I sincerely hope that I can have the opportunity to continue to improve it, and I will continue to strive to enrich myself.

CURRICULUM VITAE

Author's Name Miss Yinghong Zhao

Place of Birth Kun Ming, China

Education 2020 - 2023 Master of Science in Digital Innovation and Financial Technology, Chiang Mai University, Chiang Mai, Thailand

Publications Zhao, Y, & Dawod, A. Y. (2023, March). Practical Analyses on the Flipped Classroom Approach to Management Accounting Education. In 2023 IEEE 12th International Conference on Educational and Information Technology (ICEIT) (pp. 256-261). IEEE.