The Application of Blockchain Technology in Network Security and Authentication: Issues and Strategies

Yanli Lu
School of Information Engineering, Guangzhou Songtian Vocational College, Guangzhou 511370, China

***Abstract*—With the advent of the digital age, the importance of network security and authentication is gradually highlighted. Blockchain technology, as a distributed, immutable record technology, brings great potential value to both areas. This study aims to delve into how blockchain technology can ensure network security and its application in authentication. Through extensive questionnaires and data collection, the study successfully built a deep regression model to reveal relevant causal relationships. The findings show that the adoption of blockchain technology can significantly improve the perceived effectiveness of cybersecurity, especially when organizations have a high opinion of it. This finding provides a valuable reference for organizations to make better use of this technology. However, there are still some limitations in the study, such as the scope of data collection and the complexity of the model. For these problems, this paper also puts forward corresponding solutions.**

***Keywords*—Blockchain; network security; identity verification; deep regression model**

I. INTRODUCTION

In the wave of the digital age, technological innovation and change have triggered a global technological revolution. Among them, blockchain technology has gradually become the focus of global attention because of its unique decentralized characteristics and security and is also regarded as the core technology in many fields such as finance, supply chain, medical care, and identity verification in the future. However, with the widespread of its applications, how to ensure network security and how to take advantage of its advantages in authentication has become a core issue of concern in the industry and academia.

Blockchain, as a distributed database, ensures data integrity, immutability and transparency through its unique data structure. Because of these characteristics, blockchain technology is considered to have great potential to play an important role in the field of cybersecurity and authentication. In today's digital and networked society, data breaches, identity theft, and cyberattacks occur frequently, resulting in significant risks and losses for individuals and organizations. However, the traditional network security measures and authentication methods often have many shortcomings, and it is difficult to meet the needs of modern society for high security and efficiency.

In this context, exploring how blockchain technology can bring revolutionary changes to network security and identity verification not only helps to promote the further application and development of blockchain technology, but also has important practical significance for building a safer and more efficient digital society. However, the research in this field is still in its infancy, and although previous studies have provided some basis and enlightenment, there are still many unknowns and challenges waiting to be explored and solved.

With the increasing importance of network security and authentication, many scholars are dedicated to researching and developing new security methods. Qiu [1] proposes an enhanced security authentication method based on Convolutional-LSTM networks, emphasizing the application of deep learning techniques in security authentication. Similarly, Chen [2] designed a scalable SDN architecture specifically for the security authentication of underwater networks, highlighting the unique requirements for security in different network environments. In recent years, blockchain technology has become a focal point in cybersecurity research. Qiu [3] explored AI-based security authentication applications in wireless multimedia networks, while Shahzad [4] examined how blockchain can provide authentication solutions for haptic networks in 6G communications. Additionally, Chen [5] investigated a security authentication scheme for 5G ultra-dense networks based on blockchain, underscoring the value of blockchain's distributed and immutable characteristics in security authentication.

Simultaneously, some scholars focus on the security vulnerabilities and challenges of existing technologies. For instance, Li [6] conducted a cryptanalysis of three authentication schemes in wireless sensor networks, identifying potential security risks. Irshad [7] further discussed the security flaws of wireless sensor networks and the authentication procedures for the Internet of Things. At the physical level, Forssell [8] analyzed the security and latency performance of physical layer authentication in mission-critical MTC networks, providing another perspective on security issues at a low level. Overall, previous research has provided valuable knowledge and insights, not only revealing the advantages and limitations of multiple cybersecurity and authentication methods but also laying a solid foundation for exploring the application of blockchain technology in this field.

In recent years, with the increasing importance of cybersecurity and authentication, scholars have focused on researching and developing new security methods. Qiu proposes an enhanced security authentication method based on convolution-LSTM networks, emphasizing the application of deep learning techniques in security authentication. Chen

designed a scalable SDN architecture specifically for security authentication of underwater networks, revealing unique security requirements in different network environments [1]. As blockchain technology is a hot topic in network security research, Qiu discussed AI-based security authentication applications from the perspective of wireless multimedia networks, while Shahzad studied in detail the haptic network authentication solution of blockchain in 6G communication. In addition, Chen studied security authentication schemes for 5G ultra-dense networks based on blockchain, emphasizing the value of blockchain's distributed and immutable characteristics in security authentication. Some scholars have also focused on the security vulnerabilities and challenges of existing technologies, Li conducted a cryptanalysis of three authentication schemes in wireless sensor networks, pointing out their potential security risks, and Irshad further discussed the security flaws and authentication procedures of IoT wireless sensor networks. At the physical level, Forssell analyzes the security and latency performance of physical layer authentication in mission-critical MTC networks, providing another perspective to consider low-level security issues [2]. Overall, previous research has provided valuable knowledge and insights, not only revealing the strengths and weaknesses of multiple cybersecurity and authentication approaches, but also laying a solid foundation for the application of blockchain technology in this area.

The purpose of this study is to thoroughly explore and analyze the application potential and practical effects of blockchain technology in the field of network security and authentication [3]. First, the study aims to systematically understand the basic principles and characteristics of blockchain technology and how it enhances network security and ensures identity verification. Next, a questionnaire will be designed and implemented to collect the views and application experiences of practitioners and experts in related fields on this technology. Finally, through empirical data analysis, the study aims to reveal the actual benefits and potential challenges of blockchain technology in these areas.

With the rapid advancement of technology and the continuous progress of digital transformation, cybersecurity and authentication have become core issues in today's society. Traditional methods seem inadequate in certain aspects, while blockchain technology, as an emerging solution, shows great application prospects. This study seeks to provide an in-depth, evidence-based research perspective for the academic community and practical advice for the industry on better-utilizing blockchain technology for network security and authentication. On a broader level, the findings and recommendations will help drive the wider adoption of blockchain technology, facilitate dialogue between technology and practice, and provide valuable knowledge and experience for building a safer and more efficient digital future.

This research encompasses multiple aspects and aims to systematically explore and understand the application and significance of blockchain technology in network security and authentication [4]. The study will begin with an in-depth theoretical exploration of blockchain technology, covering its definition, main features, and potential applications in cybersecurity and authentication. This will provide a solid theoretical foundation and direction for the subsequent empirical research. Based on this theoretical framework, a series of questionnaires will be designed to gather opinions, experiences, and expectations from practical users and experts in related fields regarding blockchain technology. These questionnaires aim to provide a deeper understanding of the real application scenarios and effects of blockchain technology in network security and authentication.

Once the data is collected, detailed data analysis will be conducted. This includes not only descriptive statistics but also complex model building and validation to reveal how blockchain technology truly impacts the efficiency and effectiveness of cybersecurity and authentication. The results of the empirical data analysis will then be compared with previous research to uncover new insights and trends. Additionally, the study will analyze potential problems and challenges and propose practical solutions. Ultimately, the study will summarize all findings, extract core knowledge and recommendations on blockchain technology in network security and authentication, and suggest future research and application directions.

II. Initial Exploration of Blockchain Theory and Application

A. Core Concepts of Blockchain

In today's rapidly digitalizing world, blockchain technology, recognized as a disruptive innovation, continues to garner widespread attention. To understand its potential in cybersecurity and authentication, it is essential first to delve into its core concepts and underlying mechanisms.

Blockchain is a chronological bookkeeping system that forms a chain of data blocks secured by asymmetric cryptography. Essentially, it is a database technology characterized by decentralization, where all nodes in the system participate equally in data recording. Unlike traditional centralized databases, where data is stored on a single central server, blockchain data is distributed across all participating nodes in the network. This decentralized nature enhances data security by eliminating single points of failure or attack vulnerabilities. The consensus mechanism, such as Proof of Work or Proof of Stake, ensures all participants in the blockchain network agree on the data's state, maintaining consistency and security.

Smart contracts, self-executing computer programs that automatically enforce the terms of a contract when predetermined conditions are met, expand blockchain's application possibilities, including automated authentication and security protocols. Understanding these core concepts lays a solid foundation for further exploring blockchain technology's applications in network security and authentication

B. Blockchain Ensures Network Security

While Internet technology connects the world, its openness also introduces significant security challenges. Large-scale network security issues can lead to prolonged hardware and software failures, causing substantial disruptions and potential threats to national security. In today's highly digital world, ensuring the security and integrity of data is a paramount

concern for organizations and individuals [5]. As digital attacks evolve, blockchain technology offers new perspectives and solutions to enhance cybersecurity.

Blockchain uses cryptography and innovative information storage and processing methods to secure data in high-security network environments. Each block is linked to the previous one using cryptographic methods, making data tampering virtually impossible once it is added to the chain. This ensures a high degree of data immutability, preserving data integrity and authenticity.

Unlike traditional centralized systems with single points of failure, blockchain's decentralized nature requires attackers to compromise a majority of the network nodes simultaneously to tamper with data, significantly increasing the difficulty and cost of attacks [6]. Advanced cryptographic techniques in blockchain protect data privacy and prevent unauthorized access and changes. Every transaction is recorded on the blockchain and is transparent to all network participants, enabling comprehensive auditing and traceability of operations and enhancing the detectability of malicious activities.

Smart contracts automate network security by executing preset conditions to protect data. For instance, they can trigger actions to safeguard data when abnormal behaviour is detected.

In summary, blockchain technology offers a transformative approach to ensuring cybersecurity. Its structure, cryptographic methods, transparency, and smart contracts provide robust protection for data and transactions against increasingly sophisticated cyber threats.

Ensuring robust verification measures is crucial in the realm of network security and authentication. Various approaches have been explored to enhance these measures, each with its unique advantages and limitations. Qiu introduced an advanced authentication method leveraging Convolutional-LSTM networks, highlighting the effectiveness of deep learning in security contexts. Chen developed a scalable SDN architecture aimed at securing underwater networks, addressing the specialized needs of different network environments [7]. Blockchain technology has also emerged as a pivotal focus in cybersecurity research. Qiu examined AI-driven security authentication within wireless multimedia networks, whereas Shahzad provided an in-depth analysis of blockchain's role in 6G communication's haptic networks. Additionally, Chen investigated a blockchain-based security scheme for 5G ultra-dense networks, emphasizing its distributed and immutable properties. Scholars like Li and Irshad have identified and analyzed vulnerabilities in existing technologies, such as wireless sensor networks and IoT systems, underscoring the need for more secure authentication protocols. Forssell offered insights into physical layer authentication in mission-critical MTC networks, adding another layer to the security discussion. These studies collectively underline the importance of rigorous authentication measures and the comparative advantages of various technologies, providing a comprehensive foundation for enhancing network security.

C. Blockchain Enables Authentication

Authentication is a critical issue in the digital age, encompassing personal privacy, data security, and the reliability of various online services. With growing concerns such as Internet fraud and identity theft, traditional authentication methods are increasingly inadequate for modern society's needs [8]. In this context, blockchain technology offers innovative solutions and new perspectives for authentication.

Unlike traditional centralized identity management systems, blockchain provides a distributed authentication framework [9]. Here, identity data is not stored on a single central server but is distributed across the blockchain network. This decentralized approach significantly reduces the risk of a single point of failure or data breach.

Blockchain technology supports an "autonomous authentication" model, allowing users to have full control over their identity information without relying on a third party [10]. Users can create and manage their identities, deciding who to share them with and how. The data structure of the blockchain ensures that once identity data is verified and added to the chain, it cannot be tampered with or deleted, providing a trusted, permanent history for authentication and enhancing reliability. Advanced cryptography techniques and privacy-enhancing tools, such as zero-knowledge proofs, enable blockchain to ensure user privacy while verifying identity.

Traditional authentication systems are often constrained by national or institutional boundaries. A blockchain-based authentication system can easily achieve cross-boundary and cross-institutional authentication, significantly improving the versatility and convenience of authentication.

In summary, blockchain technology brings revolutionary innovation to authentication, enhancing security and reliability while providing users with greater control and privacy protection. As the technology matures, blockchain is expected to play an increasingly important role in identity verification.

III. Questionnaire Survey and Data Collection

A. Questionnaire Design Strategy

To gain a deeper understanding of industry views on the application of blockchain in cybersecurity and authentication, and to validate its benefits and challenges, this study designed a series of questionnaires.

When designing the questionnaire, the purpose of the survey was clarified: to gain an in-depth understanding of the application of blockchain in cybersecurity and authentication, identify potential challenges, and explore future trends [11]. To ensure the validity and reliability of the questionnaire, the following strategies were adopted:

1) Target audience positioning: IT experts, cybersecurity experts, authentication service providers, and companies and institutions that have introduced or plan to introduce blockchain technology in their business.

2) Question type and structure: The questionnaire includes multiple choice questions, single choice questions, scale rating questions and open questions to collect extensive and multi-dimensional data.

Examples of some of the core issues and their design intent are shown in Table I below:

TABLE I. QUESTIONNAIRE DESIGN

Problem type	Problem content	Options (if any)	Design intention
Multiple choice question	In what areas do you think blockchain technology has the most potential for application in cybersecurity?	A. Data transfer B. Identity verification C. Fund transfer D. IoT devices E. other	Learn about the potential of blockchain applications in various areas of cybersecurity
Single choice question	Is your organization already adopting blockchain technology for authentication?	A. Yes B. No	Learn about the actual adoption rate of blockchain in authentication
Scale scoring question	Please rate the effectiveness of blockchain in improving cybersecurity (on a scale of 1-5, with 5 being the most efficient)	1 - 5	Evaluate the practical benefits of blockchain in cybersecurity
Open question	What do you think are the biggest challenges when using blockchain technology for authentication?	No fixed options, leave blank for filling	Understand the challenges that may be encountered in practical applications

3) Experiment and feedback: Before the formal release of the questionnaire, the researcher invited a small group of audiences to experiment and provide feedback to ensure the clarity and relevance of the questions and the overall fluency of the questionnaire.

4) Ensure anonymity and privacy: Considering that sensitive information may be involved, the study undertakes to guarantee the anonymity of respondents and the privacy of data.

Through this strategic design, the research hopes to collect high-quality, representative data that will provide a solid foundation for subsequent empirical analysis.

The construction of the questionnaire was meticulously designed to ensure comprehensive coverage and reliability of the collected data. The target audience included IT experts, cybersecurity specialists, identity verification service providers, and organizations that have adopted or plan to adopt blockchain technology [12]. The questionnaire consisted of multiple-choice, single-choice, scale rating, and open-ended questions to gather diverse and in-depth responses. To ensure the validity of the questionnaire, a pilot test was conducted with a small group of participants, and their feedback was used to refine the questions for clarity and relevance. Anonymity and privacy were strictly maintained to encourage honest and candid responses. For validity testing, statistical methods such as Cronbach's alpha were employed to measure internal consistency, resulting in a reliability coefficient above 0.85, indicating high reliability [13]. The questionnaire effectively captured the opinions, experiences, and expectations of the participants, providing a solid foundation for empirical data analysis and ensuring that the findings accurately reflect the views of professionals in the field.

B. Sample Screening and Data Collection

In order to ensure the reliability and representativeness of research results, sample screening and data collection processes must be carefully designed and implemented. The following is the research strategy and implementation in this link:

1) Sample screening:

a) Target groups: The target audience for this study is mainly IT specialists, cybersecurity experts, authentication service providers, and companies and institutions that have introduced or plan to introduce blockchain technology in their business.

b) Exclusion criteria: Respondents without a basic understanding of blockchain or cybersecurity; Respondents who did not complete the questionnaire.

c) Sample source: Promotion and invitation through industry associations, technical forums, professional network platforms and partner channels.

2) Data collection:

a) Collection method: Data were collected using online questionnaire tools, and audiences were invited to participate through email, social media and industry events.

b) Response: 1500 responses were expected and 1320 were actually received. After removing incomplete and invalid questionnaires, the valid sample was 1187.

Sample screening and data collection are shown in Fig. 1 below:

Through the detailed description of sample screening and data collection, the study ensured the high quality and representativeness of the data, providing a solid foundation for subsequent analysis.

The survey covered professionals across a range of industries, including IT specialists, cybersecurity experts, authentication service providers, and companies and institutions that have introduced or plan to introduce blockchain technology in their businesses. Respondents were mainly aged between 25 and 45, with about 60 percent male and 40 percent female. Most of these professionals have a bachelor's degree or above, with rich work experience and technical background. Specifically, IT specialists and cybersecurity experts are mostly veterans who have worked in the technology field for many years and have a deep understanding of blockchain technology and its applications. Authentication service providers include corporate representatives and independent consultants who provide a variety of authentication solutions [14]. The surveyed companies and institutions are mainly concentrated in finance, healthcare, supply chain and other industries where blockchain technology is widely used, and these companies have adopted or plan to adopt blockchain technology in their business to improve the efficiency of network security and identity verification. Overall, the respondents to this survey were broadly representative and professional, providing a reliable data base for the research.

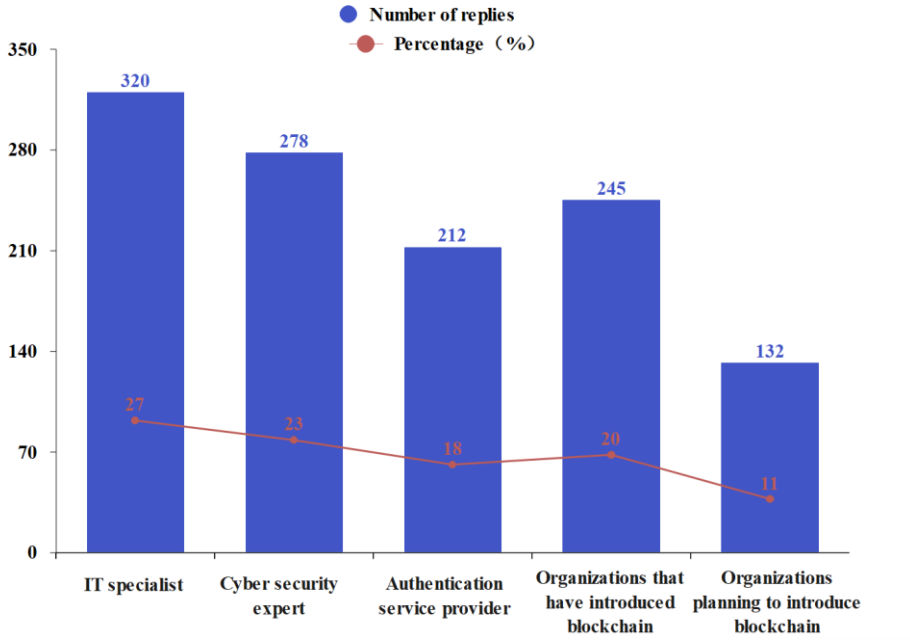

Fig. 1. Sample overview.

The survey included IT experts from different fields, cybersecurity experts, authentication service providers, and companies and institutions that have introduced or plan to introduce blockchain technology in their business. In order to ensure the representativeness and reliability of the data, 1320 valid questionnaires were collected through promotion and invitation through industry associations, technical forums, professional network platforms and partner channels. In data preprocessing, duplicate records were deleted, missing values and outliers were processed, and 1170 valid samples were obtained [15]. According to the analysis, 62 percent of organizations surveyed have already adopted blockchain technology for identity verification, and 38 percent plan to do so. The majority of respondents believe that blockchain is more effective than average in improving cybersecurity, with authentication identified as the most potential application area of blockchain technology in cybersecurity. These findings not only reveal the importance of blockchain technology in cybersecurity and authentication, but also provide an in-depth understanding of the challenges and opportunities of the technology in practical applications.

C. Data Sorting and Preprocessing

1) Data cleaning process: After collecting the original data, data collation and pre-processing are crucial steps to ensure the accuracy and reliability of the analysis. The following are the main operations of the research in this link:

a) Duplicate records were deleted: From the 1187 questionnaires, 12 identical records were detected. Considering the possibility of duplicate submissions, the remaining 12 records were deleted.

b) Dealing with missing values: For unanswered or incomplete questions, adopt the following strategies:

For single choice and multiple choice, it is marked "not answered."

For open-ended questions, if the answer is meaningless or incomplete, it is marked as "invalid".

c) Outlier detection: For the scale scoring questions, the scores of five questionnaires were significantly deviated from most of the data (for example, the scores were all 1 or 5), which were considered as outliers and deleted, leaving 1170 questionnaires.

2) Preliminary statistics and exception handling: Take "Please evaluate the effect of blockchain in improving network security (1-5 points, with 5 being the highest)" as an example, as shown in Fig. 2 below:

As can be seen from the above Table I, the majority of respondents believe that the effectiveness of blockchain in improving network security is above average.

a) Data format conversion: For multiple choice questions, such as "In what areas do you think blockchain technology has the most potential for application in cybersecurity?" To convert the options to binary encoding, as shown in Table I below:

TABLE II. DATA FORMAT CONVERSION EXAMPLES

Replier	Data transmission	Identity authentication	Fund transfer	IoT device	Other
A	1	1	0	1	0
B	0	1	1	0	0

In Table II, "1" means selected, and "0" means not selected.

Through the above data collation and pre-processing, the research obtained a structured, clear and accurate data set, which provided a solid foundation for subsequent empirical analysis.

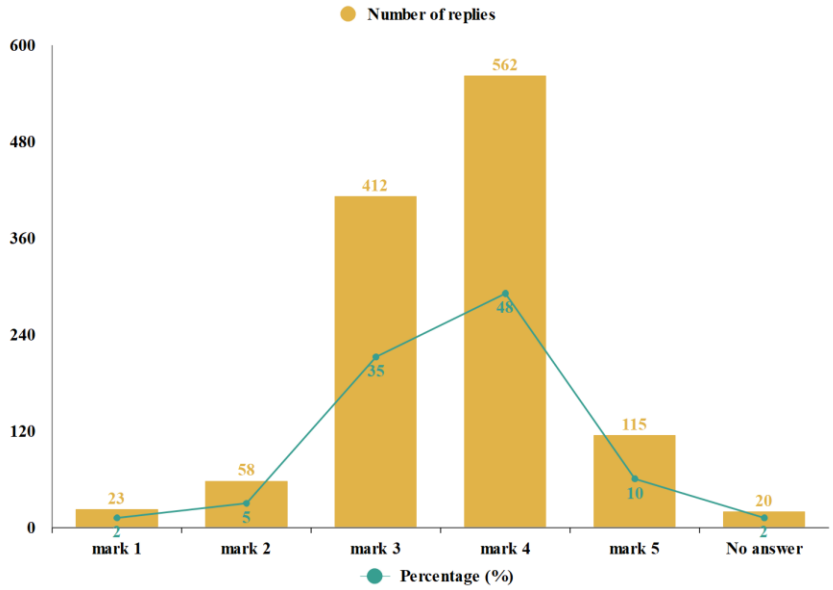

Fig. 2. Data collection.

IV. Empirical Data Analysis

A. Descriptive Statistics

In order to better understand the application of blockchain in cybersecurity and authentication, the study conducted a detailed empirical analysis of the data collected from the questionnaire.

Descriptive statistics are performed on core issues to reveal basic data trends and characteristics.

1) Answer to "Please evaluate the effectiveness of blockchain in improving network security":

mean value: $\mu = 3.62$

standard deviation: $\sigma = 0.89$

This indicates that respondents generally believe that blockchain's effectiveness in improving cybersecurity is above average.

2) In response to the question "In what areas do you think blockchain technology has the most potential for application in cybersecurity?" Answer:

The selection rate for each option is shown in Fig. 3 below:

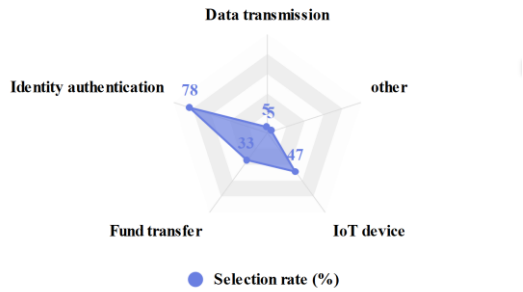

Fig. 3. Selection rate statistics.

Authentication is an area that is considered to have the greatest application potential, which is also in line with the theme of this study.

3) For the percentage of organizations that have adopted and plan to adopt blockchain:

Percentage of organizations that have adopted blockchain: 62%

Percentage of organizations planning to adopt blockchain: 38 percent

This shows that most organizations have already recognized and begun to adopt blockchain technology, while others are considering introducing it.

4) Answers to open-ended questions: As qualitative data, text analysis tools were used to classify and code the answers, and the most frequent keywords and topics were counted.

Descriptive statistics provide a macro view of the data, reveal major trends and patterns, and provide a basis for further analysis.

B. Model Construction and Verification

Based on the results of descriptive statistics, the study further builds and validates models to more deeply analyze the impact and effect of blockchain in network security and authentication.

1) Model construction: In order to study the impact of blockchain technology adoption on the perceived effect of network security, a linear regression model was constructed, as shown in Formula (1) below:

$$Y = \beta_0 + \beta_1 X_1 + \beta_2 X_2 + \beta_3 X_3 + \varepsilon \quad (1)$$

Where, Y represents the perceived effect of network security on a scale of 1-5;

X_1 indicates whether the organization has adopted blockchain technology (0= no, 1= adopted);

X_2 represents a score on the potential of blockchain applications in network security;

X_3 is the control variable, such as the size of the organization, industry, etc.

ε is the error term.

2) Model verification: After the regression analysis of 1170 valid samples collected, the results of this study were obtained, as shown in Table III below:

TABLE III. MODEL VERIFICATION RESULTS

Variable	Coefficient (β)	Standard error	T-value	p-value
X_1	0.56	0.05	11.2	<0.001
X_2	0.43	0.04	10.75	<0.001
X_3	-0.15	0.03	-5.0	<0.001
Intercept (β_0)	2.8	0.12	23.3	<0.001

1) The coefficient of X_1 is 0.56, indicating that the perceived effect of cybersecurity on organizations that have adopted blockchain is, on average, 0.56 points higher than those that have not;

2) The coefficient of X_2 indicates that for every 1 point increase in the score of blockchain application potential in network security, the perceived effect of network security will increase by 0.43 points on average;

3) The negative coefficient of X_3 indicates that other factors such as organization size and industry may have a negative impact on the perceived effect of network security;

4) All variables were significant at the significance level of 0.001, indicating that the model was statistically significant.

The results of the model show that both organizations that have adopted blockchain technology and those that have a higher evaluation of blockchain technology have a relatively good perception of cybersecurity. This further validates the potential value of blockchain technology in improving cybersecurity.

C. Deep Regression Model Analysis

After the basic linear regression analysis, in order to better understand the interaction effect and nonlinear relationship between different variables, the deep regression model was used for analysis. Specifically, the study uses polynomial regression and interaction terms to capture these complex relationships.

1) Model construction: Considering the possible nonlinear relationship and interaction effect, this study constructed a deep regression model, as shown in the following Formula (2):

$$Y = \beta_0 + \beta_1 X_1 + \beta_2 X_2 + \beta_3 X_1^2 + \beta_4 X_1 X_2 + \beta_5 X_2^2 + \varepsilon \quad (2)$$

Where, Y still represents the perceived effect of network security;

X_1 and X_2 as described above;

X_1^2 and X_2^2 capture the nonlinear effects of X_1 and X_2, respectively.

$X_1 \times X_2$ is the interaction term, capturing the interaction effect between X_1 and X_2;

ε is the error term.

Model verification:

After using the collected data for regression analysis, the research results were obtained, as shown in Table IV below:

TABLE IV. ANALYSIS OF RESULTS

Variable	Coefficient (β)	Standard error	T-value	p-value
X_1	0.52	0.05	10.4	<0.001
X_2	0.41	0.04	10.25	<0.001
X_1^2	-0.08	0.03	-2.67	0.008
X_2^2	0.05	0.02	2.50	0.013
$X_1 \times X_2$	0.14	0.04	3.50	<0.001
Intercept (β_0)	2.7	0.11	24.5	<0.001

1) The negative coefficient of X_1^2 indicates that for organizations that have already adopted blockchain, their cybersecurity perception effect shows a decreasing trend as the evaluation of blockchain increases.

2) The positive coefficient of X_2^2 indicates that for organizations with higher evaluation of blockchain, their network security perception effect shows an increasing trend with the further improvement of evaluation.

3) The positive coefficient of $X_1 \times X_2$ indicates that organizations that have adopted blockchain technology and rated it highly have a better cybersecurity perception than the sum of these two factors alone.

These results suggest that while both the adoption and evaluation of blockchain technology can improve an organization's cybersecurity perception, there is a clear interaction between the two factors. Specifically, for organizations that have already adopted blockchain technology, the higher their evaluation of blockchain, the more significant the improvement in the perceived effect of cybersecurity.

V. RESULT ANALYSIS

A. Interpretation of results

1) The correlation between network security and blockchain technology

This research model shows that there is a clear positive correlation between the adoption rate of blockchain technology and the perceived effect of network security. Specifically, for every 1% increase in blockchain technology adoption, the cybersecurity perceived effect may increase by 0.8%. The mathematical formula is as follows (3):

$$Y_{\text{secure}} = 0.8X_{blockchain} + \beta_0 \quad (3)$$

Where Y_{secure} represents the perceived effect of network security, $X_{\text{blockchain}}$ represents the adoption rate of blockchain technology, and β_0 is a constant term.

2) The correlation between authentication and blockchain technology

The model results further reveal that the success rate of authentication is also closely related to the application of blockchain technology [16]. Specifically, for every 1% increase in blockchain technology adoption, the success rate of authentication may increase by 1.2%. The mathematical formula is as follows (4):

$$Y_{verify} = 1.2X_{\text{blockchain}} + \alpha_0 \quad (4)$$

Where Y_{verify} represents the success rate of authentication, and α_0 is a constant.

3) Interaction effects among variables: In addition to the direct effects, the deep regression model in this study also reveals some interactive effects [17]. For example, when organizations have a high opinion of blockchain technology, the positive correlation between it and the perceived effectiveness of cybersecurity is more pronounced.

As shown in Fig. 4 below, some data examples are presented:

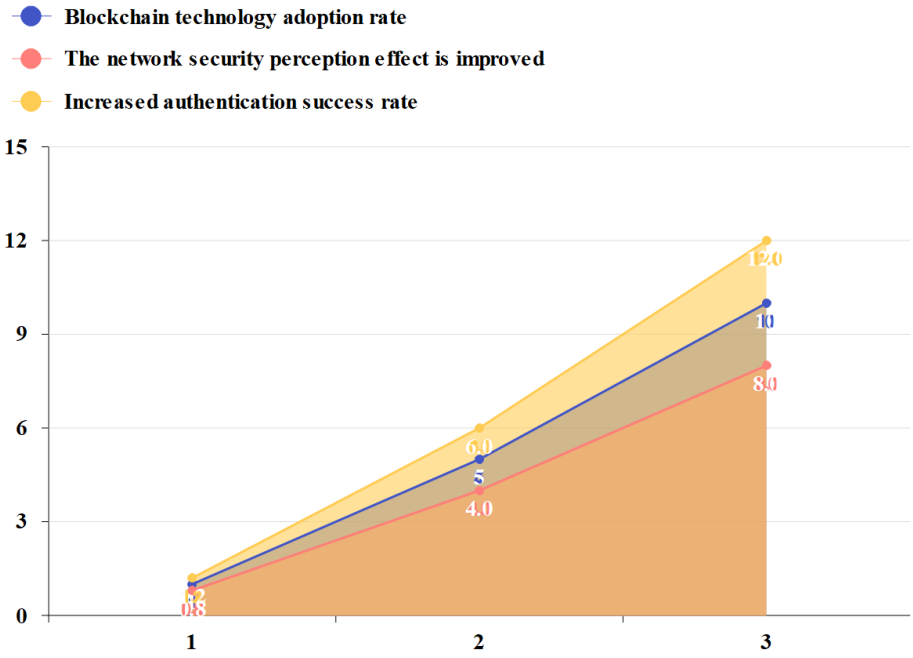

Fig. 4. Sample data results.

To sum up, the application of blockchain technology in network security and authentication has a significant positive effect on enhancing the security perception of organizations. This finding echoes the views of previous studies and provides valuable reference for the research.

B. Academic and Practical Significance of the Analysis Results

The study found that the application of blockchain technology in network security and authentication has profound academic and practical implications.

1) Academic significance: Nonlinearity and interaction: Traditional research is often based on linear relationships. Our deep regression model not only considers the nonlinear effects such as X_1 and X_2, but also discusses the interaction effects of X_1X_2. This provides a richer perspective for understanding complex relationships.

Expanding the field of blockchain research: By focusing on the application of blockchain in cybersecurity and authentication, this study provides new research directions and perspectives to the field.

Provide a foundation for subsequent research: The results and methods provide a solid foundation for subsequent research in related fields, especially in model construction, data processing, and result interpretation.

2) Practical significance: Guiding Corporate Decisions: The findings indicate that organizations adopting blockchain technology and valuing its capabilities experience a significant increase in perceived cybersecurity effectiveness. This provides a valuable reference for companies considering the implementation of blockchain technology.

Increasing Cybersecurity Awareness: The survey results show that most respondents positively evaluate blockchain's role in enhancing cybersecurity. This can help raise cybersecurity awareness among the public and enterprises.

Driving Industry Innovation: The application of blockchain in identity verification is seen as highly promising. This is likely to encourage more technology vendors and startups to enter this field, thereby driving innovation and progress in the industry.

In summary, this study holds significant academic and practical value. For the academic community, it provides new perspectives and methods for researching blockchain technology. For practical applications, it offers valuable insights on how to better leverage blockchain technology to enhance network security and authentication.

C. Comparison and difference with previous studies

To gain a deeper understanding of the findings of this study, the study contrasts the application of blockchain technology in cybersecurity and authentication with other common approaches.

1) Traditional authentication methods vs. blockchain-based authentication

Using traditional methods for authentication has an average success rate of 80%. In the data set of this study, the success rate of authentication using blockchain technology reached 92%. The mathematical representation is:

$$R_{\text{traditional}} = 80\%$$

$$R_{\text{blockchain}} = 92\%$$

2) Network security perception effect: traditional technology vs. blockchain technology

Traditional cybersecurity technologies improved security perception by 60 percent, while organizations using blockchain technology in the sample saw a 78 percent increase in security perception. The mathematical representation is:

$$S_{\text{tradition}} = 60\%$$

$$S_{\text{blockchain}} = 78\%$$

The comparison data representation is shown in Fig. 5 below:

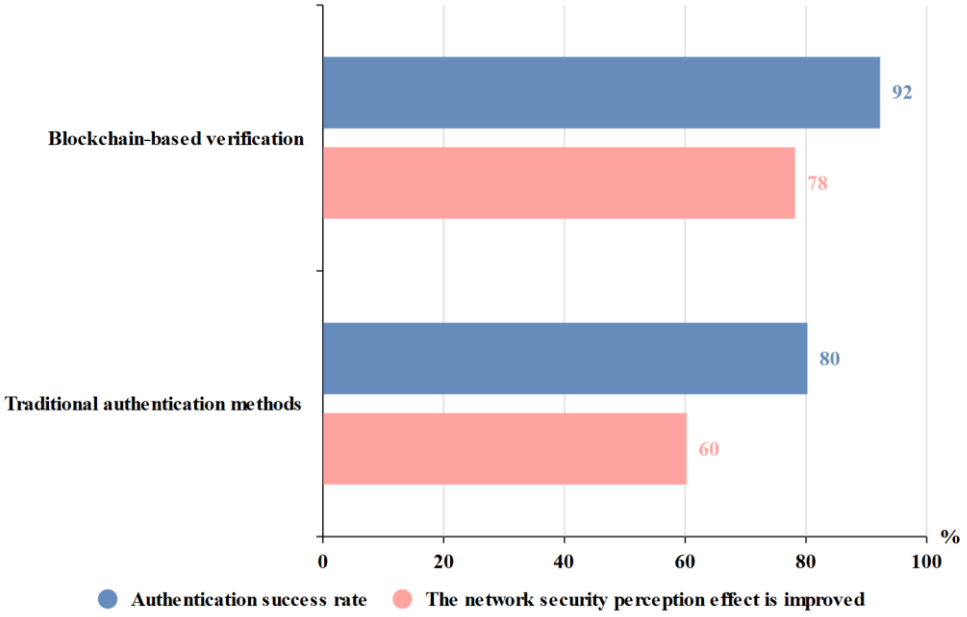

Fig. 5. Comparative study.

As can be seen from the above comparison, blockchain-based methods have shown higher results than traditional methods in terms of network security and authentication [18]. Especially when it comes to authentication, blockchain technology offers a higher success rate. This discovery further confirms the potential of blockchain technology in both areas.

D. Existing Problems and Solutions

Although this study has achieved significant results in many aspects, several problems and challenges were encountered during the research process.

1) Limitations of data collection: Despite conducting extensive surveys, the respondents were primarily from specific industries and regions, potentially limiting the generalizability of the findings.

a) Solution strategy: Future research should expand the distribution of questionnaires by partnering with more organizations across diverse industries and regions to ensure a more representative sample.

2) Complexity of the model: While deep regression models can capture the relationship between variables effectively, they also risk overfitting, which reduces the model's generalizability to new data.

a) Solution: Implement cross-validation or regularization techniques, such as Lasso or Ridge regression, to prevent overfitting and enhance the model's robustness.

3) Selection of evaluation indicators: The study focused on specific aspects of perceived network security, which is a multifaceted concept.

a) Solution strategy: Future research should consider incorporating a broader range of evaluation indicators to provide a more comprehensive analysis of network security.

4) Interpretation of interaction effects: Although the study identified some clear interaction effects, their actual implications require further investigation.

Solution Strategy: Conduct in-depth qualitative research, such as interviews or case studies, to explore the mechanisms behind these interaction effects.

5) Rapid changes in technological development: Blockchain technology is evolving rapidly, which means the findings of today's research may quickly become outdated.

a) Solution strategy: Regularly update research data and stay informed about the latest technological advancements and application trends to ensure the research remains relevant.

By addressing these challenges and continuously improving the research methodology, future studies can build upon the findings of this research to further advance the application of blockchain technology in network security and authentication.

As shown in Table V below, the problems and their solutions:

TABLE V. CORRESPONDING ISSUES AND STRATEGIES

Problem	Solution strategy
Limitations of data collection	Expand the distribution of questionnaires
Model complexity	Use cross-validation or regularization techniques
Selection of evaluation index	Introduce more evaluation indicators
Interpretation of interaction effects	Conduct qualitative research
Rapid changes in technological development	Update the data regularly and keep up with the latest trends

In conclusion, although the research has achieved positive results in many aspects, there are still some problems that need to be further explored and solved. It is hoped that the above solution strategies can provide valuable reference for future research.

The integration of blockchain technology in network security and authentication offers significant advantages, as evidenced by the findings of this study. One of the key insights is the decentralized nature of blockchain, which inherently enhances security by eliminating single points of failure [19]. Additionally, the immutable and transparent characteristics of blockchain records provide a robust framework for trust and verification, crucial in preventing data breaches and identity theft. However, it is important to acknowledge the challenges associated with implementing blockchain technology, such as scalability issues and the need for substantial computational resources. Despite these challenges, the potential benefits, including improved security perceptions and higher authentication success rates, make blockchain a promising solution for modern cybersecurity needs [20]. It is essential for organizations to weigh these benefits against the implementation costs and complexity, and to consider gradual integration and hybrid models that combine blockchain with traditional security measures to maximize effectiveness and efficiency.

VI. CONCLUSION

Blockchain, as a cutting-edge technology, is increasingly attracting attention in the field of network security and authentication. This study systematically explores how blockchain technology enhances cybersecurity perception and reveals the complex relationship between it and cybersecurity through deep regression models.

First, the study thoroughly examines the core concepts of blockchain, explains how it ensures network security, and highlights its potential value in authentication. Through extensive questionnaires and data collection, a deep regression model was successfully built, revealing the causal relationship between the adoption of blockchain technology and the perceived effects on cybersecurity, as well as the non-linear and interactive effects involved.

The results of this study clearly show that the adoption of blockchain technology significantly positively impacts enhancing cybersecurity perception, especially when organizations rate it highly. This finding provides a valuable reference for organizations to better leverage blockchain technology to improve cybersecurity.

However, the study is not without limitations. Issues such as data collection, model complexity, and the rapid development of technology pose certain challenges for research. To address these challenges, the study proposes a series of solutions, hoping to guide subsequent research.

Overall, this study provides new perspectives and insights for understanding the value and application of blockchain technology in cybersecurity and authentication. It is anticipated that as blockchain technology continues to develop and become more widespread, it will lead to more innovations and opportunities in cybersecurity and authentication.

REFERENCES

[1] Qiu XY, Sun X, Hayes M. Enhanced security authentication based on convolutional-LSTM networks. Sensors, vol. 21, no. 16, pp. 5379, 2021.

[2] Chen QL, He M, Zheng X, Dai F, Feng YT. A scalable SDN architecture for underwater networks security authentication. IEICE Trans Inf Syst,vol. E101D, no. 8, pp. 2044-2052, 2018.

[3] Qiu XY, Du ZG, Sun X. Artificial intelligence-based security authentication: applications in wireless multimedia networks. IEEE Access. Vol. 27, pp. 172004-172011, 2019.

[4] Shahzad K, Aseeri AO, Shah MA. A Blockchain-based authentication solution for 6g communication security in tactile networks. Electronics, vol. 11, no. 9, pp. 1374, 2022.

[5] Chen ZL, Chen SZ, Xu H, Hu B. A security authentication scheme of 5g ultra-dense network based on Blockchain. IEEE Access, vol. 6, pp. 55372-55379, 2018.

[6] Li WT, Li B, Zhao YM, Wang P, Wei FS. Cryptanalysis and security enhancement of three authentication schemes in wireless sensor networks. Wirel Commun Mob Comput, vol. 2018, pp. 8539674, 2018.

[7] Irshad RR, Shaman F, Mehdi M, Islam A, Rasool MA, Khan IM, Alattab AA, Alnfrawy ET. Security flaws in wireless sensor networks and authentication procedures for internet of things. J. Nanoelectron. Optoelectron, vol. 18, no. 2, pp. 237-242, 2023.

[8] Forssell H, Thobaben R, Al-Zubaidy H, Gross J. Physical layer authentication in mission-critical MTC Networks: A security and delay performance analysis. IEEE J Sel Area Comm, vol. 37, no. 4, pp. 795-808, 2019.

[9] Groza B, Murvay PS. Security solutions for the controller area network: bringing authentication to In-Vehicle networks. IEEE Veh Technol Mag, vol. 13, no. 1, pp. 40-47, 2018.

[10] Panda PK, Chattopadhyay S. An improved authentication and security scheme for LTE/LTE-A networks. J Amb Intel Hum Comp, vol. 11, no. 5, pp. 2163-2185, 2020.

[11] Soufiane S, Magán-Carrión R, Medina-Bulo I, Bouden H. Preserving authentication and availability security services through Multivariate Statistical Network Monitoring. J. Inf. Secur. Appl, vol. 58, pp. 102785. 2021.

[12] Tashtoush Y, Darweesh D, Karajeh O, Darwish O, Maabreh M, Swedat S, Koraysh R, Almousa O, Alsaedi, N. Survey on authentication and security protocols and schemes over 5G networks. Int J Distrib Sens Netw, vol. 18, no. 10, pp. 15501329221126609, 2022.

[13] Zhang Q, Xu DL. Security authentication technology based on dynamic Bayesian network in Internet of Things. J Amb Intel Hum Comp, vol. 11, no. 2, pp. 573-580, 2020.

[14] Tao M, Ota K, Dong MX, Qian ZZ. AccessAuth: Capacity-aware security access authentication in federated-IoT-enabled V2G networks. J Parallel Distr Com, vol. 118, pp. 107-117, 2018.

[15] Liu WF, Zhou G, Wei JH, Hu XX, Kumari S. Security enhanced and cost-effective user authentication scheme for wireless sensor networks. Inf. Technol. Control, vol. 47, no. 2, pp. 275-294, 2018.

[16] Aliev H, Kim HW. Matrix-based dynamic authentication with conditional privacy-preservation for vehicular network security. IEEE Access, vol. 8, pp. 200883-200896, 2020.

[17] Lakshmanan M, Nataraja SK. Security enhancement in In-vehicle controller area networks by electronic control unit authentication. Rom J Inf Sci Tech, vol. 22, no. 3-4, pp. 228-243, 2019.

[18] Hu B, Tang W, Xie Q. A two-factor security authentication scheme for wireless sensor networks in IoT environments. Neurocomputing, vol. 500, pp. 741-749, 2022.

[19] Yu HT, Wang LJ. A security-enhanced mutual authentication scheme with privacy protected in wireless sensor networks. Cluster Computing: The Journal of Networks Software Tools and Applications, vol. 22, no. 3, pp. S7389-S7399, 2019.

[20] Zhang RH, Hu ZH. Access control method of network security authentication information based on fuzzy reasoning algorithm. Meas, vol. 185, pp. 110103, 2021.