

WEB3 DIGITAL IDENTITY AUTHENTICATION
FRAMEWORK

LIU XIAOYU

UNIVERSITI KEBANGSAAN MALAYSIA

WEB3 DIGITAL IDENTITY AUTHENTICATION FRAMEWORK

LIU XIAOYU

PROJECT SUBMITTED IN PARTIAL FULFILMENT FOR THE DEGREE OF
MASTER OF CYBER SECURITY

FACULTY OF INFORMATION SCIENCE AND TECHNOLOGY
UNIVERSITI KEBANGSAAN MALAYSIA
BANGI

2025

WEB3 DIGITAL IDENTITY AUTHENTICATION FRAMEWORK

LIU XIAOYU

PROJEK YANG DIKEMUKAKAN UNTUK MEMENUHI SEBAHAGIAN
DARIPADA SYARAT UNTUK MEMPEROLEH IJAZAH SARJANA
KESELAMATAN SIBER

FAKULTI TEKNOLOGI SAINS DAN MAKLUMAT
UNIVERSITI KEBANGSAAN MALAYSIA
BANGI

2025

DECLARATION

I hereby declare that the work in this thesis is my own except for quotations and summaries which have been duly acknowledged.

I have not used any AI tools or technologies to prepare this report.

24 January 2025

LIU XIAOYU
P131657

ACKNOWLEDGEMENT

Praise to Allah the Almighty, who provided me with the strength and wisdom to complete this research.

I am truly grateful for the guidance and expertise provided by my esteemed supervisor, Associate Professor Dr. Khairul Akram Zainol Ariffin. His insight and direction were invaluable throughout this journey.

I extend my appreciation to the Faculty of Information Science and Technology at Universiti Kebangsaan Malaysia, where this research was conducted. The resources and support from the faculty were crucial to my work.

I am also thankful for the financial support received from various sponsors, which made this research possible. Their contributions have not only supported my academic pursuits but have also significantly enhanced the quality of my work.

Lastly, I wish to express my general gratitude to everyone who supported me during this endeavor, especially Zhang Haiying and Liu Ruoxun. Your encouragement and belief in my capabilities have been a source of motivation throughout this journey.

ABSTRAK

Dengan perkembangan teknologi Internet, orang ramai semakin bergantung kepada identiti digital untuk menjalankan aktiviti dalam talian. Walaupun rangka kerja pengesahan identiti digital terpusat tradisional menyediakan perkhidmatan yang mudah, pengurusan terpusat dan kaedah penyimpanan datanya terdedah kepada tidak sah. Serangan. Ia mula-mula menggunakan kaedah pembelajaran tinjauan literatur sistemik (slr) dan meneroka pengenalan pusat (JPS), kelayakan boleh disahkan (VC), kontrak pintar, protokol kebolehooperasian, mekanisme kawalan pengguna, ciri keselamatan, privasi dipertingkatkan dan komponen pemantauan dan analisis lanjutan.. Selepas bahawa, data tinjauan dikumpul dan dianalisis selepas menggunakan pakej Statistik untuk sains sosial. Akhirnya, rangka kerja pengesahan identiti digital web3 yang baharu telah dibangunkan. Rangka kerja menggunakan komponen pemantauan dan analisis lanjutan untuk memantau dalam masa nyata. Analisis teori dan menunjukkan bahawa rangka kerja meningkatkan fleksibiliti dan kecekapan sistem pengurusan identiti, menjadikannya sumbangan utama kepada bidang pengesahan identiti digital Web3.

ABSTRACT

With the development of Internet technology, people increasingly rely on digital identity to carry out online activities. Although the traditional centralized digital identity authentication framework provides convenient services, its centralized management and data storage methods are vulnerable to illegitimacy. Attacks. It first uses Systemic literature review(slr) learning methods and explores central identification (DID), verifiable credentials (VC), smart contracts, interoperability protocols, user control mechanisms, security features, enhanced privacy, and advanced monitoring and analysis components.. After that, the survey data was collected and analyzed after using Statistical package for the social sciences. Finally, a new one was developed web3 digital identity authentication framework. The framework's uses advanced monitoring and analysis components to monitor in real time. Theoretical analysis and show that the framework enhances the flexibility and efficiency of the identity management system, making it a key contribution to the field of Web3 digital identity authentication.

LIBRARY FTS

TABLE OF CONTENTS

		Page
DECLARATION		iii
ACKNOWLEDGEMENT		iv
ABSTRAK		v
ABSTRACT		vi
TABLE OF CONTENTS		vii
LIST OF TABLES		x
LIST OF ILLUSTRATIONS		xi
LIST OF ABBREVIATIONS		xii
CHAPTER I	INTRODUCTION	
1.1	Research Background	1
1.2	Problem Statement	2
1.3	Research question	3
1.4	Research objective	3
1.5	Research scope	4
1.6	Report lay out	4
1.7	Conclusion	5
CHAPTER II	LITERATURE REVIEW	
2.1	Introduction	6
2.2	Discussion	7
	2.2.1 The development trend of Web3 Digital identity authentication	7
	2.2.2 The challenges and limitations of current digital identity authentication applications.	12
	2.2.3 The essential components of Web3 digital identity authentication	22
2.3	Conceptual framework	26
2.4	Conclusion	28
CHAPTER III	METHODOLOGY	
3.1	Introduction	30

3.2	Research design	31
3.3	Systemic literature review(slr) methodology	31
	3.3.1 Research question(RQ)	32
	3.3.2 Search process	33
	3.3.3 Selection of literature	34
	3.3.4 Literature quality assessment	35
	3.3.5 The result of the SLR	38
3.4	Questionnaire validation	40
3.5	Pilot testing	40
3.6	Data collection	41
3.7	Data analysis	42
3.8	Conclusion	43
CHAPTER IV	RESULTS AND DISCUSSION	
4.1	Introduction	45
4.2	Survey results	46
	4.2.1 Gender identity	46
	4.2.2 Age groups	47
	4.2.3 Professional roles	47
	4.2.4 Experience with WEB3	48
	4.2.5 Education level	49
4.3	Results of the validity and reliability test	49
	4.3.1 Cronbach' s alpha	49
4.4	Descriptive statistics:key metrics for WEB3 components	52
	4.4.1 Decentralized identifiers(DIDS) table	52
	4.4.2 Verifiable credentials(VCS)	53
	4.4.3 Smart contracts table	54
	4.4.4 User control table	55
	4.4.5 Security mechanisms table	56
	4.4.6 Privacy enhancements table	57
	4.4.7 Interoperability protocols	58
4.5	Interpretation of descriptive statistics general overview	58
4.6	Discussion	59
	4.6.1 Decentralized identifiers(DIDS)	60
	4.6.2 Verifiable credentials (VCS)	60
	4.6.3 Smart contracts	60
	4.6.4 User control	61
	4.6.5 Security mechanisms	62
	4.6.6 Privacy enhancements	62
	4.6.7 Interoperability protocols	63
	4.6.8 Advanced monitoring and analysis component	63

4.7	Conclusion	64
CHAPTER V WEB3 FRAMEWORK CONSTRUCTION		
5.1	Introduction	66
5.2	Web3 digital identity authentication framework	66
5.2.1	Decentralized identifiers (DIDS)	66
5.2.2	Verifiable credentials(vcs)	67
5.2.3	Smart contracts	67
5.2.4	User control	68
5.2.5	Security mechanisms	69
5.2.6	Privacy enhancement	69
5.2.7	Interoperability protocols	70
5.2.8	Advanced monitoring and analysis component	70
5.3	Conclusion	72
CHAPTER VI CONCLUSIONS AND FUTURE DIRECTIONS		
6.1	Introduction	75
6.2	Summary of the results	75
6.3	Limitations	75
6.4	Future research directions	76
6.5	Significance of the study	77
REFERENCES		79
APPENDICES		
Appendix A	Questionnaire	84

LIST OF TABLES

Table No.		Page
Table 2.1	Comparative Analysis of Web 1, Web 2, and Web 3	11
Table 2.2	Summary of Challenges and Constraints	21
Table 2.3	Framework Comparison	24
Table 3.1	Summary of database search result	34
Table 3.2	Methodology for achieving output results	39
Table 3.3	Cronbach alpha obtained in pilot study	41
Table 4.1	Reliability analysis	50
Table 4.2	Descriptive Statistics of Decentralized Identifiers Table	52
Table 4.3	Descriptive Statistics of Verifiable Credentials (VCs) Table	53
Table 4.4	Descriptive Statistics of Smart Contracts Table	54
Table 4.5	Descriptive Statistics of User control	55
Table 4.6	Descriptive Statistics of Security Mechanisms Table	56
Table 4.7	Descriptive Statistics of Privacy Enhancements Table	57
Table 4.8	Descriptive Statistics of Interoperability Protocols Table	58
Table 4.9	Interpretation of Descriptive Statistics General Overview	59

LIST OF ILLUSTRATIONS

Figure No.		Page
Figure 2.1	The basic process of the development of the Internet	8
Figure 2.2	Conceptual framework diagram	27
Figure 3.1	The process Search	37
Figure 3.2	Flowchart of methodology process	44
Figure 4.1	Demographic Distribution of Respondents by Gender	46
Figure 4.2	Age Distribution of Respondents	47
Figure 4.3	Professional Role Breakdown of Survey Respondents	47
Figure 4.4	Experience Level of Respondents with Web3 Technologies	48
Figure 4.5	Educational Background of Survey Respondents	49
Figure 5.1	Web3 digital authentication framework	72

LIST OF ABBREVIATIONS

AMAC	Advanced monitoring and analysis component
AI	Artificial Intelligence
DIDS	Decentralized identifiers
PETs	Privacy Enhancing Technologies
SLR	Systemic literature review
UKM	Universiti Kebangsaan Malaysia
VCS	Verifiable credentials

LIBRARY FETSM

CHAPTER I

INTRODUCTION

1.1 RESEARCH BACKGROUND

With the development of Internet technology and the digitization of information, people are increasingly relying on digital identities for online activities, such as online banking, social media, etc., and the security of digital identity authentication systems is becoming increasingly prominent. Although the traditional centralized digital identity authentication framework provides convenient services, its centralized management and data storage methods are extremely vulnerable to attacks by criminals.

With the emergence of web3 digital identity authentication technology, the way digital identity authentication is managed is undergoing a revolutionary change. Web3 digital identity authentication technology refers to a decentralized framework (Schmidt & Wagner 2021). Unlike traditional centralized systems, the new digital identity authentication framework fundamentally changes the way digital space is created, managed and used. This decentralized shift avoids the damage that is prone to occur in the web2 centralized model.

The shift in the way web3 digital identity management is represented by Web3 digital identity authentication systems that use decentralized identifiers (DIDs) and blockchain technology. But even if these systems have innovative solutions, they may still have security vulnerabilities. For example, the decentralized structure of blockchain may make it more difficult to respond quickly to illegal access, etc. (Sullivan 2022). And while using DID, because it enhances the user's autonomy over personal data, it also puts a heavy burden on users to securely manage their digital identities. In some cases, users lose access to their encryption keys, making it impossible to authenticate

their digital identities, resulting in an irrecoverable situation. This situation highlights the user-related risks inherent in web3 digital identity authentication systems (Li et al. 2021).

Nowadays, cyber attacks are becoming increasingly sophisticated. In 2022, smart contract vulnerabilities were used to exploit popular decentralized applications (dApps) for digital identity management. (Hughes et al. 2022) The complexity of Web3 systems may expose them to different attack vectors not found in more traditional digital identity frameworks, resulting in unauthorized access and data leakage (Hughes et al. 2022). There are still many areas and components in the field of web3 digital identity authentication that need to be explored, so the goal of this article is to explore the components of the web3 digital authentication identity framework and build a more secure web3 digital identity authentication framework.

1.2 PROBLEM STATEMENT

First, There is a great deal of controversy in the existing literature regarding the important components that make up the web3 digital identity system. This fuzzy understanding of the clarity of key components has greatly slowed down the technological progress and efficient application of the web3 digital identity field (Peters 2021). As the digital landscape evolves, a deeper understanding of the components that make up web3 digital identity is critical. These components are the basis for enhanced security and user autonomy, but their roles and interactions remain under explored.

The current literature on Web3 digital identity also does not satisfactorily discuss the performance or contribution of its components with respect to security and general operation. Poor understanding of how all components interrelate translates to serious vulnerabilities in addition to inefficient use of resources in line . Moreover, most of them talk of results derived through operation without proposing integration with a conceptual framework for solutions to systemic challenges at the moment. This fragmented research approach prevents the development of a more secure, efficient, powerful web3 digital identity system.

Finally, the existing web3 digital identity framework still has security risks that must be urgently addressed to improve the overall security and reliability of the system (Johnson 2021). Although blockchain has the potential to revolutionize identity management by decentralizing the control and storage of personal data, there are still some key areas that need improvement, especially in data privacy, key management, and mitigation of man-in-the-middle attacks (Singh 2022). Therefore, developing a new and more secure authentication framework is important to address these risks. And a more secure web3 digital authentication identity framework lays a solid foundation for the future development of web3 digital authentication.

This paper aims to address existing problems by comprehensively exploring the key components of digital authentication within the Web3 framework. In addition, this paper will also focus on developing a more secure and powerful web3 digital authentication framework, and propose a new web3 digital authentication identity framework through data collection and careful analysis. Through the new Web3 digital authentication model, this study hopes to help improve and optimize digital identity solutions and promote their integration into mainstream applications and services.

1.3 RESEARCH QUESTION

Based on the problem statement, there are several research questions that have been identified, namely:

1. What is the development trend of Web3 Digital identity authentication?
2. What are the challenges and limitations of current digital identity authentication applications?
3. What are the essential components of Web3 digital identity authentication?

1.4 RESEARCH OBJECTIVE

1. Explore the essential components in web3 digital identity authentication.
2. Investigate the criticality of web3 components.
3. Design a more new web3 digital identity authentication framework.

1.5 RESEARCH SCOPE

This study will explore and analyse in detail the key technical components that make up the Web3 digital identity authentication framework. After fully investigating the components that make up web3 digital authentication, the study will evaluate the functionality, security, and effectiveness of these components in improving user privacy and control through a questionnaire. After that, the criticality of these Web3 technical components will be investigated, including their role in the system, the main challenges they face, and how to solve existing digital identity authentication problems. This project will study the design and development of a more secure and efficient Web3 digital identity authentication framework. The framework will integrate all the essential components into one.

To ensure the wide applicability and depth of the research results, the survey subjects of this study will focus on IT professionals and network security experts who have work experience in the field of digital identity management or have a deep understanding and practical experience in Web3 technology. Through such a research scope setting, this study aims to provide empirical basis and theoretical insights for building a more secure and effective Web3 digital identity authentication model, thereby promoting the development of digital identity authentication technology and improving the security and privacy protection level of digital interactions.

1.6 REPORT LAY OUT

This paper aims to comprehensively explore the application prospects of Web3 digital identity authentication and build a more secure authentication framework. The paper is divided into six chapters, each of which discusses the central theme in detail.

Chapter 1 introduces the background, problem statement, research questions, research objectives and research scope of the study. In addition, this section also outlines the structure and main content of the entire paper, providing readers with a clear research blueprint. Chapter 2 explores the development trends, challenges and key technical elements of Web3 digital identity authentication through a systematic literature review. This chapter aims to provide theoretical and literature support for the

research questions. Chapter 3 details the research design, data collection methods and analysis strategies. The study adopts a combination of quantitative surveys and qualitative interviews to ensure a comprehensive understanding of the key issues of Web3 digital identity authentication from multiple dimensions. Chapter 4 presents the results of the survey and interviews and conducts an in-depth analysis of the data. Through the fusion of quantitative data and qualitative insights, the main trends and problems in the current Web3 digital identity authentication practice are revealed. Chapter 5 proposes a new Web3 digital identity authentication framework based on the analysis results of Chapter 4. The construction of the framework takes into account the feasibility and security of the technology, and explains the various components within the framework in detail. Chapter 6 summarizes the main findings of the entire study and discusses its theoretical and practical significance. In addition, this chapter also explores the future research directions and potential improvement paths of Web3 digital identity authentication.

1.7 CONCLUSION

This chapter first introduces the research background and existing problem statements to lay the foundation for in-depth research on the web3 digital authentication framework. Then, the research questions and research objectives are proposed, which provide a clear research direction for this paper. Finally, the scope of the research is described. The research questions raised in this chapter aim to explore the development trends, limitations and key elements of Web3 digital identity authentication technology, which will be addressed throughout the report.

CHAPTER II

LITERATURE REVIEW

2.1 INTRODUCTION

The following chapter will carry out a systematic review of related literature in an attempt to answer the fundamental research questions on the development and effectiveness of the authentication system of Web3 digital identities. Navigation through transitions in the digital identity systems faces substantial challenges that relate to privacy concerns, susceptibility to data breaches, and intricacies regarding user control over personal data (Kanwar et al. 2022). This review will critically look at how the advent of Web3 technologies is reshaping the landscape of digital identity, focusing on the promise and pitfalls associated with these emerging paradigms.

It introduces digital identity authentication development trends; from traditional centralized models that give way to new approaches characteristically decentralized, security-oriented, and user-autonomous (Smith et al. 2021). The idea remains that this historical understanding allows a deeper understanding of motives toward the shift into technologies known as Web3.

In turn, following the development trends, this chapter will outline the challenges and limitations faced specifically by Web3 digital identity systems. This will be done with a focus on ongoing privacy issues, technical and operational obstacles to preventing data breaches, and the tricky dynamics in ensuring users are in control in a decentralized environment as pointed out by Brown (2021). The following analysis shows the challenges that must be overcome for the full deployment of Web3 technologies to improve digital identity authentication.

The chapter also intends to detail the main components that make up a Web3 digital identity system. Among such, it will consider: decentralized identifiers enabling users to have self-sovereign identities that are independent from any kind of central registry, verifiable credentials through which it becomes possible to certify digital attributes by keeping personal data locked in, and smart contracts-ensuring adherence to the terms of the rules of the game for maintaining digital identity (Chen et al. 2020).

The chapter concludes with the synthesis of all the insights from the literature review in providing answers to the research questions set at the beginning of this study. This will also provide a preliminary background for subsequent chapters in regard to going into the practical implementation of Web3 digital identity systems and the challenges therein.

2.2 DISCUSSION

2.2.1 The development trend of Web3 Digital identity authentication

As the Internet itself has developed, the digital identity authentication landscape has also undergone a major transformation. From the static, centralized system of web1 to the dynamic, user-centric network of Web2, and now the revolutionary decentralized framework of Web3. This development reflects not only technological progress but also a paradigm shift, that is, improving user autonomy, privacy, and security in digital authentication.

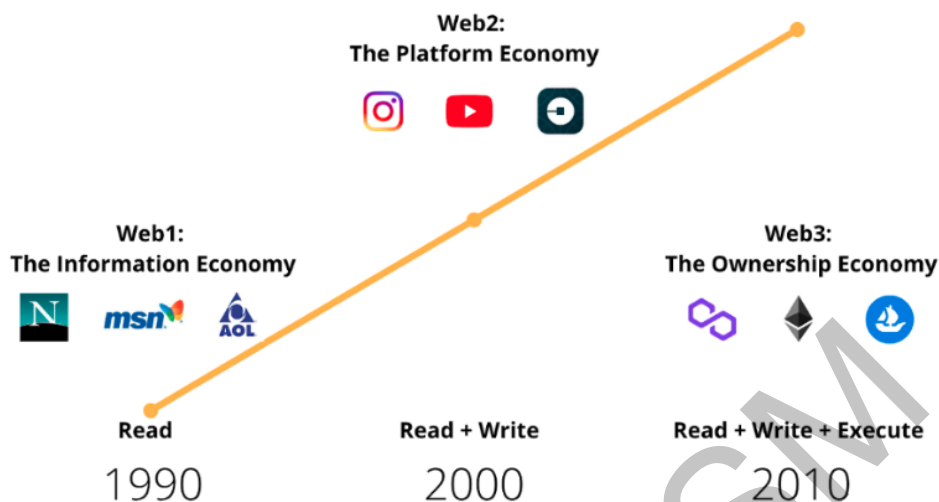


Figure 2.1 The basic process of the development of the Internet

Web1 is the first version of the Internet. It marks the birth of the Internet, with most participants being content consumers and creators being mainly developers. The websites they produced mainly contained text or visual content. Figure 2.1 shows that Web1 existed between about 1990 and 2000. Its main feature is that websites provide static content rather than dynamic Hypertext Markup Language (HTML) content. Data and content come from static file systems rather than databases, and there is limited interactivity on web pages (Smith 2022). Digital identity authentication in this era is very simple and completely dependent on central servers. Users mainly interact with the Internet through browsers to view web pages that rarely change.

Web1 versions of digital identity authentication are still in their infancy, involving simple username and password systems that provide minimal security and almost no data encryption. Control of personal data is mainly in the hands of website administrators, posing significant risks in terms of data privacy and security vulnerabilities (Nita& Mihailescu 2024).

With the advancement of technology, as shown in Figure 2.1, web2 emerged around 2000 and was first proposed by Dale Dougherty. Web2 allows each user to change from an observer to a participant. The Internet has become an interactive platform for people at both ends to obtain information, and the so-called social network has emerged.

In this era of interactive networks, users can share their information with the rest of the world. Users can submit videos for everyone on the network to view, participate in, and comment on. As shown in Table 2.1 (Lee 2020), the degree of user usage has also been qualitatively improved. Data transmission, which involves the transfer of data such as videos, comments, and other user-generated content across the network, plays a critical role in facilitating these interactions (Smith 2021). Business activities have become easier due to the improvement of the ability to share ideas, enhanced communication technology, and the reduction of travel and operating costs (Ziqiang Zu 2023). The efficiency and reliability of data transmission not only accelerate the speed of information sharing but also enhance team collaboration and market responsiveness. The advent of Web2 has dramatically transformed the marketing landscape by significantly decreasing the duration needed to execute marketing campaigns and by broadening the potential reach of these activities. This technological evolution enables more rapid dissemination of marketing content, allowing businesses to react swiftly to market changes and consumer feedback. Furthermore, Web2 has facilitated a vast expansion in the audience that can be reached, making it possible for marketing strategies to have a global impact, transcending traditional geographical and demographic boundaries (Jones & Taylor 2018). It makes it easier for companies to spread their products. The most important thing is to get customer feedback through online business. Today, many well-known online business platforms and social platforms are attributed to web2. For example, YouTube, Facebook, Instagram, Twitter and other social platforms.

The idea of a digital identity in the era of Web2 is predominantly managed through centralized services. This, while ensuring a smooth and seamless experience for users, has several demerits, with the most serious concerns related to privacy, security, and ownership of data. Centralized systems often create single points of failure,

thus turning themselves into lucrative targets of cyber-attacks that quite frequently result in large-scale data breaches. Moreover, these systems typically give users limited control over their personal data, raising issues about data privacy and misuse. As a result, there is an increasing demand for models that ensure greater user control and legal frameworks that protect personal information (Smith & Johnson 2021). As Web2 matured, user data stored in large centralized databases became a prime target for leakage and abuse. This was the time when the federated identity model came into being, which tried to make life easy for the user by enabling single sign-on across different platforms. The model has failed largely in assuaging the deeper concerns about privacy and data sovereignty despite its well-voiced advantages. While the federated model allows for ease of access and interconnectivity between different systems, it also rests on centralized data management; thus, it failed to enable users to have control over their own data. Data privacy refers to a condition of control that individuals have over their personal information. Data sovereignty, on the other hand, is about data being subjected to the laws and governance structures of the nation in which it is collected. In this period, these concepts became very important because public awareness and regulatory discussions made it obvious how easily vulnerabilities could be used to mislead personal information for various misuses (Zheng et al. 2018).

The concept of Web3 was initially proposed by Tim Berners-Lee. He envisioned an internet where data is connected in a meaningful way, enabling machines to understand human-like requests and process data in a contextually aware manner. As shown in Figure 2.1, Berners-Lee et al. further outlined this concept in scientific articles and speeches around 2000. The main aspects of web3 are mainly Financial Transactions, Privacy and Security, Transfer Speed, Technology, Ownership and Control, as shown in Table 2.1(Lee, 2020).

Web3 introduces a radically different approach to digital identity, characterized by decentralization and user empowerment. Unlike Web2, where identities are tied to services and controlled by central authorities, Web3 empowers users with self-sovereign identities (SSIs). These identities are managed by individuals themselves using blockchain and decentralized technologies, allowing for greater control over personal data and interactions (Buterin, 2014; Wang et al., 2022).

The advent of Web3 and its impact on digital identity Web3 represents a paradigm shift toward a more decentralized internet, leveraging technologies such as blockchain and peer-to-peer networks (Bashir 2020). In this context, digital identity is evolving toward self-sovereignty, where individuals have greater control and ownership over their digital identities, independent of central authorities (Hacioglu 2020). Technologies like blockchain enable the creation of secure, verifiable digital identities, enhancing privacy and reducing the risk of identity theft (Doğan 2023). Concepts such as decentralized identifiers (DIDs) and verifiable credentials are becoming the new standard for self-managed, interoperable digital identities (Omar, A.S 2020). Web3 also brings the potential for interoperable digital identities across different platforms and services without sacrificing user privacy or security (Alzahrani 2020). Digital identities, however, still face many challenges in Web3.

Table 2.1 Comparative Analysis of Web1, Web2, and Web3

Category	Web1	Web2	Web3
Interaction	Static content	Dynamic, interactive content	Decentralized, interactive, real-time exchanges
User Role	Information consumer	Information participants; content creators	Information control by users; decentralized participation
Data Management	Centralized on servers	Centralized, with dynamic content delivery	Decentralized data across a distributed network
Technology	Basic HTML, static webpages	Rich Internet applications, AJAX	Blockchain, AI, machine learning
Management Model	Managed by website administrators	User-generated content, community management	Autonomous, user-controlled through smart contracts
Usability	Simple, limited user interaction	Enhanced usability, user-centric design	Advanced, with emphasis on security and user empowerment

2.2.2 The challenges and limitations of current digital identity authentication applications.

Digital identity, which came with the development in the Web3 era, besides the groundbreaking benefits, also brought a lot of challenges along the way, according to Bashir I. (2020), including those linked to user privacy and the security of the identity systems. These challenges stem from the inherent complexity in the management and understanding of digital identities within a decentralized framework—a prospect intimidating for users and making usability more complex. Furthermore, this has also become a great hindrance to regulatory compliance as the lack of clear regulatory oversight in decentralized systems results in abuses and difficulties with legal liability.

Besides the aforementioned above challenges, there are specific institutional barriers in Web3 to deploying the digital identity system in the Web3 era. These are such issues as the absence of a common framework, which would provide interoperability across different systems, and the reluctance of existing institutions to accept new models based on decentralization. This might hamper the use and successful performance of the systems of digital identity in various spheres. As Bashir (2020) underlines, it is overcoming these challenges and institutional barriers that is an indispensable step toward the full realization of the potential of digital identity in the Web3 era.

The first challenge is user privacy. In an age where identity information is so important, concerns about user privacy have become paramount. As digital interactions and transactions become increasingly integral to everyday life, protecting personally identifiable information has become a basic necessity, not just a luxury. User privacy issues in digital identity systems are complex and greatly influenced by the architecture of the deployed system. In traditional systems, the centralization of user data creates inherent vulnerabilities. These centralized repositories are attractive targets for malicious actors because a single breach can expose sensitive data of millions of users (Doe 2022). Such breaches can lead to severe consequences, including identity theft, financial losses, and even irreversible harm to an individual's physical and mental health. Furthermore, the impact of a compromised digital identity is not limited to

personal losses but can also affect social trust and the overall integrity of the digital ecosystem (Smith & Anderson 2021).

While blockchain provides a secure foundation by making data changes easy to detect, it does not encrypt the data itself. This is where encryption comes into play. Encryption converts readable data into a secure format that can only be restored to its original format by an authorized party using a cryptographic key. In a blockchain-based DID, each piece of user data can be encrypted before being stored on the blockchain. This ensures that even if the data is accessed, it remains confidential and protected from unauthorized viewing.

However, the security and privacy benefits of combining blockchain with encryption also bring new challenges, especially in the management of encryption keys. Users must manage their keys securely, as losing access to a key means losing access to the encrypted data it protects. This creates usability challenges that need to be addressed to ensure that users can manage their keys without compromising security (Johnson 2021).

To ensure that decentralized systems truly protect user privacy, they must implement strong encryption and strict access controls. Encryption algorithms need to be constantly updated to protect against evolving cryptographic attacks (Lee 2019).

Similarly, access controls must be sophisticated enough to allow complex permissions and sharing settings that enable users to share different parts of their digital identity in different situations without exposing other unrelated personal information.

Users are responsible for their key management, and losing access to a cryptographic key can mean losing access to one's digital identity. This not only poses significant usability issues but also raises concerns about user capacity to manage keys securely without compromising the integrity and accessibility of their own data (Johnson 2021). This is a severe challenge for web3 digital identity authentication.

The second challenge is the security of identity systems. The security of identity systems is critical because these systems store and manage vast amounts of personal information in sectors as diverse as banking, healthcare, and government services. Given their criticality, digital identity systems are attractive targets for cybercriminals, requiring constant innovation in security strategies to protect sensitive data from increasingly sophisticated threats (Smith et al. 2021).

Digital identity systems face a range of cyberattacks, each designed to exploit specific vulnerabilities:

1. **Phishing attacks:** These occur when cybercriminals impersonate legitimate entities through electronic communications in order to trick users into revealing sensitive information. Such attacks are becoming increasingly sophisticated and often bypass traditional security measures (Johnson 2021).
2. **Malware attacks:** Malware is used to disrupt operations, steal sensitive data, or gain unauthorized access to computer systems. The variety and sophistication of malware, including ransomware and spyware, poses a significant challenge to identity security systems (Brown & Green 2022).
3. **Man-in-the-middle (MitM) attacks:** These attacks involve an attacker intercepting communications between two parties to steal or manipulate data. The increasing use of insecure IoT devices in identity systems has expanded the scope of such vulnerabilities (White & Black 2023).
4. **SQL injection:** These attacks inject malicious SQL code into a database through a web form or query parameter, allowing an attacker to gain unauthorized access and manipulate sensitive information stored in the database (Tan & Lee 2020).
5. **Distributed denial of service (DDoS) attacks:** These attacks use traffic to overwhelm a system, network, or service to exploit capacity constraints, severely disrupting service availability and functionality (Jones et al. 2020).

This could be quite critical in having an effective combat of such vulnerabilities through multi-layer security that comes in advanced techniques of encryption, strict access control, and continuous monitoring of the security systems. Advanced detection with the use of AI and machine learning in discovering the threats and their elimination before it happens to affect the system will be helpful (Anderson & Thomson, 2022). It has thus placed promising avenues for improving the security of digital identities. By decentralizing storage and management, blockchain allows for a reduction in some of the risks associated with centralized data breaches and improves resilience against attacks (Buterin, 2014; Wang et al. 2022).

Security in digital identity systems is but one paramount concern that requires continuous attention and innovation. Since the cyber threat landscape keeps pace with developments in technology, from sophisticated attacks to deepfakes and AI-driven phishing, strategies and technologies to protect them must equally evolve. To date, the integration of biometric authentication, the use of machine learning algorithms in detecting anomalies, and blockchain-based authentications are but some of the latest endeavors toward strengthening the robustness of digital identity systems.

Biometric technologies, such as face and fingerprint recognition, offer a layer of security difficult to duplicate or forge, thus providing full-scale user authentication. However, the wider these technologies spread, the more they become targets of correspondingly sophisticated attacks. For instance, studies have demonstrated that face recognition systems can be deceived by advanced image processing methods (Smith & Johnson 2021). There are constant innovations necessary regarding improving both biometric sensor technology and sophisticated algorithms to detect the difference between forged or original data.

The application of machine learning in security systems enables continuous learning from new data, thereby enhancing the ability to detect anomalous patterns that may indicate a security breach. For example, machine learning models can analyze access logs and user behavior to identify potentially malicious activities that deviate from normal patterns (Lee 2022). This proactive approach to security helps mitigate threats before they can cause significant damage.

It will always remain a steep challenge because, aside from bringing into view and taking advantage of new technologies, securing them requires making sure different components all work seamlessly as a part of one system-the system of digital identity. It requires a holistic approach where, apart from the technical solution, even the legal and regulatory frameworks must guarantee that the use of these technologies will be ethical. As these systems become integral to industries such as banking, healthcare, and government services, maintaining confidence in digital identities is indispensable. Therefore, there has to be a firm commitment to the continuous development of security, acceptance of new threats, and innovations that will enhance the integrity of digital systems.

The third daunting challenge facing digital identity systems is regulatory compliance. The international regulatory landscape governing data protection and privacy is highly fragmented and constantly changing. Complying with these different regulations is critical for businesses to operate legally in different jurisdictions and maintain user trust.

European Union - General Data Protection Regulation: The GDPR is one of the most rigid laws in the world on the subject of privacy and security. It demands an extremely high degree of protection of personal data and endows individuals with a wide range of rights, such as access to data, the right to be forgotten, and data portability. The academic literature suggests that, with its wide approach, the GDPR has totally changed the way businesses deal and process information about individuals, requiring that it be treated lawfully, used transparently, and erased when no longer necessary. (Smith & Wagner 2019) .

United States - California Consumer Protection Act, CCPA: The CCPA bares some spirit from GDPR in that it focuses on granting consumers certain rights to their personal information. It applies to any business operating in California: the right to know, access, and opt-out of the sale of personal data. As scholars note, this focus of the CCPA on consumer rights reflects the increasing awareness toward the strengthening of data protection in the United States but with a focus on commercial use of personal data (Brown et al. 2020).

APAC - Singapore's PDPA: The PDPA of Singapore provides a GDPR-like framework for personal data protection but has particular foci on consent and organizational practices. Unlike the GDPR, data portability is not required under the PDPA. These illustrate regional differences in priorities for data protection. Research has shown that the PDPA increases consumer trust through emphasis on consent and security measures but does not afford as many individual rights as does the GDPR (Lee & Tan 2018). These different regulatory frameworks illustrate different approaches to data protection. The GDPR is known for its stringency and broad scope, emphasizing individual rights and imposing harsh penalties for noncompliance. In contrast, the CCPA focuses more on consumer rights related to commercial data sales, while Singapore's PDPA emphasizes organizational responsibility and consent without the scope of individual rights provided by the EU (Nguyen & Tran 2021).

Companies operating internationally must navigate this complex regulatory landscape, adapting their practices to comply with the legal requirements of each jurisdiction. This involves not only implementing strong security measures, but also continually monitoring and adapting these measures to remain compliant with evolving laws (Jensen & Wright 2022).

Most critical for crossing borders are international digital identity solutions. Their creation and management might sometimes be very challenging due to various or even contrasting regulatory frameworks. Companies need to be good at navigating this so that serious trouble can be avoided from that which may bring in fines very largely or damage the brand.

The European Commission (2016) highlights that the sanctions for non-compliance with the GDPR are up to 4% of worldwide annual sales or €20 million, whichever is greater. In turn, this has brought financial risk for non-compliance to the fore.

Furthermore, compliance is more than mere adherence to the law. It also involves keeping pace with any new regulatory developments and making the changes necessary. When new issues regarding privacy arise or technological advances, such as

the rise of blockchain technology and its consequences for data security and anonymity, regulations often change to accommodate them. The constant problem for companies is how to stay abreast of these developments, understand them, and quickly make the necessary modifications (Smith 2022).

Digital identity systems have to overcome the highly complex array of regulatory challenges in different jurisdictions, each with its legal framework that must be adhered to. This regulatory environment places great marks on how technology is implemented and functions within these systems. However, it is not just the external regulations that create challenges but also internal technical limitations to growth.

First, the limitation of technology is in regard to digital identity authentication. While there have been considerable technological milestones that promise better security and efficiency in systems dealing with digital identities, these improvements are only very relative because of some intrinsic limits.

Biometric technologies include voice identification, iris recognition, facial recognition, and fingerprint scanning; because these offer a high degree of security and unique identification, they are increasingly included in digital identity systems. These methods have certain weaknesses, however. Unlike passwords or PINs, biometric features are essentially immutable; once compromised, biometric data poses a singular problem. The person's biometric identification may be irreparably compromised if this data is leaked or stolen (Jain et al. 2016).

Additionally, inaccuracies may also affect the reliability of biometric systems since it can be compromised with variations in environmental conditions such as aging and physical state changes that may affect some of the biometric patterns. For example, very minor injuries to fingers prevent recognition techniques of fingerprinting; for face recognition systems, weak light and changes to facial hair disrupt the systems (Kumar & Zhang 2017). The more sophisticated ones include spoofing, a method where fake biometric characteristics are presented, like a fake fingerprint or even a mask. These challenges call for further advancement in sensor technology and robust algorithms to keep the integrity and security of biometric systems intact.

The potential of blockchain technology for offering a transparent and decentralized structure in digital identity management is often discussed. Especially, with features of transparency, immutability, and with no intermediaries, it serves in the creation of a digital identity that is safe and valid. In spite of all these, several disadvantages of blockchain remain-considering energy consumption and scalability in particular. Given that blockchain is decentralized, with the rise of the number of transactions, gigantic delays and increased costs can arise because each transaction should be verified by several nodes within the network. This scalability problem seriously restricts the wide applicability of blockchain technology in digital identification systems where fast and efficient processing is in demand (Zheng et al. 2018).

Though the advance of biometric and blockchain technologies seriously influenced digital identification systems, the limitation of those technologies drew the attentions of others to the difficulties of the usage of those technologies (Smith 2020). These challenges need to be weighed in a balanced manner regarding technological, practical, ethical, and environmental considerations of digital identity systems. Much more research and development is needed to surmount these challenges and fully exploit the potential of these technologies for better management of digital identity. Second, Institutional barriers while deploying or implementing the Digital Identity system. The majority of times, these have to do with large institutional barriers that come in the way of successful implementation of these digital identity systems, which vary greatly from region to region and impact how accessible these technologies are. Such differences in technological infrastructure, especially in developing countries that lack advanced digital frameworks, have a crucial role in this, according to Smith (2020). This impacts the degree to which modern digital identity systems can be absorbed and function effectively.

Strong technology infrastructures that facilitate the easy integration and functioning of complex digital identity systems are generally beneficial to developed countries. On the other hand, less developed technological frameworks in developing countries inhibit the efficiency and reliability of the systems. The requirements for real-time processing and verification by digital identification systems can be greatly

compromised by inferior telecommunications and high-speed internet connectivity, which reduces the utility value of the systems (Smith 2020).

The other important component that determines the rate and level of adoption and effectiveness of the digital identification technologies is the level of digital literacy within the population. According to Johnson (2021), a higher level of digital literacy corresponds to simpler adoptions and more efficient use of the technologies. For instance, if the level of digital literacy is low, it will be difficult even to use digital identity systems with some sort of reluctance. If the government wants to let citizens navigate the digital environment safely and efficiently, the entity has to pay adequate attention to improving the level of digital literacy.

Successful implementation of the digital identity systems depends on two things: one, if the government has all the resources, financial and logistical, necessary for their successful use; and two, constructing the appropriate legislative and regulatory frameworks that the systems need to work properly. According to Williams (2019), local political will or government resource deficits might impede proper development and implementation of digital identity systems in some regions. All this is further complicated by a lack of clear regulatory frameworks, which can put legal ambiguities into operation and discourage participation and investment by both the public and private sectors.

Furthermore, the practice of legal compliance in foreign operations depends on whether the national legislation is compliant with the set global data protection standards, such as the GDPR. As Bennett (2022) talks about misalignments, he mentions that these can lead to legal problems and prevent huge multinational corporations from integrating their systems in the non-compliant locations, further alienating those locations from the technological advancements.

Overcoming institutional barriers to the deployment of digital identity systems requires collaboration between governments, international organizations, and local stakeholders. This should be channeled into the improvement of technological infrastructure, digital literacy, and harmonization of legal frameworks. This will not

only ensure that the benefits of technology are equitably distributed but also guarantee inclusive growth and participation in the global digital economy.

This may also be an indication that there is something rather challenging to implement fully in the digital identity system. As shown in Table 2.2. These are matters that must be solved when devising a fair, inclusive, and effective global digital identity management system. The institutional barriers can be surmounted with improvements in education, infrastructure, and regulatory frameworks, but technological limitations regarding blockchain and biometrics are yet to be innovated continuously. In order to meet these challenges, Johnson et al. (2021) mention that continuous adaptation and innovation are crucial.

Table 2.2 Summary of Challenges and Constraints

Challenge/Constraint	Description	Key Implications
Regulatory Compliance	Varying data protection and privacy laws across regions require strict compliance.	Legal barriers, need for adaptation to diverse laws.
Technological Limitations	Biometric inaccuracies and blockchain scalability issues limit effectiveness.	Need for advanced sensor technology and improved scalability.
Security Threats	Phishing, malware, MitM, SQL injections, and DDoS attacks.	Continuous innovation in security strategies required.
Institutional Barriers	Differences in technological infrastructure and digital literacy across regions.	Challenges in adoption and operation in less developed areas.
Privacy Concerns	Centralized systems pose risks of massive data breaches. Decentralization can help.	Management of encryption keys and secure data handling.

2.2.3 The essential components of Web3 digital identity authentication

The research question given tries to respond to what the architecture of essential components of web3 digital identity looks and works, analyzing the essential components common to the models referenced in the literature.

Based on the literature reviewed, it is concluded that the key components of Web3 digital identity authentication include Decentralized Identifiers (DIDs), Verifiable Credentials (VCs), Smart Contracts, Interoperability Protocols, User Control, Security Mechanisms, and Privacy Enhancements.

Decentralized Identifiers (DIDs) are critical for establishing user-controlled digital identities, eliminating reliance on central authorities and reducing risks associated with centralized data control (Spataru 2020). DIDs enhance privacy and enable users to control the disclosure of their identity information, crucial for maintaining user autonomy in digital interactions (Hardjono et al. 2019). However, the implementation of DIDs faces challenges related to interoperability and user education, which must be addressed to achieve broader adoption (Reed et al. 2021).

VC has the potential to offer a decentralized method for improving trust and making the verification of identity easier. It provides a chance for subjects to prove something about their identity without necessarily leaking any of the underlying personal data, increasing the level of privacy and security (Sullivan 2020). These are digitally signed by some trusted issuers and can be verified anywhere in the network without some central verifying authority, enhancing user autonomy and reducing fraud risks (Mühle et al. 2018).

Smart contracts automate interactions and agreements directly on the blockchain and can be used to clearly provide a tamperproof mechanism for managing digital identities (Christidis & Devetsikiotis 2016). They form an integral part of automatic verification processes in identity applications and reduce the possibility of human error, hence improving the speed of transactions (Zhang et al. 2017). Despite their advantages,

smart contracts are prone to various vulnerabilities due to coding bugs, and therefore require strict testing and auditing processes concerning security (Atzei et al. 2017).

Interoperability protocols are the keys to ensuring that Web3 identities can be interoperable among the different blockchain platforms seamlessly, which guarantees a consistent user experience (Kuperberg 2019). These protocols provide a fix for the fragmentation of the blockchain ecosystem so that there can be the recognition of digital identity on various systems and applications (Wang et al. 2020). Still, substantial technical challenges lie in the development of interoperability protocols that require continuous research and standardization efforts toward their resolution (Belchior et al. 2020).

User control over personal data is a fundamental aspect of Web3 identity systems, empowering individuals to manage their digital footprints (Graglia et al. 2018). This empowerment supports compliance with global privacy regulations and builds trust in digital services (Mühle et al. 2018). Nonetheless, increased control demands that users possess or acquire a certain level of digital literacy to manage their identities effectively (Birch 2020).

Security mechanisms within Web3 frameworks ensure the integrity and confidentiality of digital identities, safeguarding them against unauthorized access and cyber threats (Dai et al. 2019). Advanced encryption techniques and consensus algorithms are employed to enhance security, but they must continually evolve to counter new and emerging security threats (Al Omar et al. 2019).

Privacy-enhancing technologies, such as zero-knowledge proofs, are employed in the Web3 frameworks to allow users to prove identity claims without necessarily revealing the underlying personal information supporting those claims (Sasson et al. 2014). While these provide strong privacy protections, they do introduce complexity and performance overheads that must be carefully managed (Goldreich 2017).

Table 2.3 Framework Comparison

Framework Authors / Components	(DIDs)	(VCs)	Smart Contracts	Interoperability Protocols	User Control	Security Mechanisms	Privacy Enhancements	Economic Opportunities	Reputation Systems	Privacy Enhancement Technologies	Regulatory Considerations	User Education
Petcu et al.(2019)	✓		✓	✓	✓	✓			✓			
Bambacht & Pouwelse(2020)	✓	✓	✓	✓	✓		✓	✓			✓	
Yiwei Lai(2021)	✓	✓	✓		✓	✓	✓					✓
Spatru, A.(2020)	✓		✓		✓	✓	✓	✓		✓		
Lee, C.(2020)	✓	✓			✓		✓					✓
Tan, L.(2020)	✓		✓	✓		✓				✓		

... to be continued

... continuation

Lee, C.(2020)	✓	✓		✓		✓		✓
Tan, L.(2020)	✓		✓	✓		✓		✓
Lim, E.(2021)		✓	✓		✓		✓	✓
Choi, H.(2020)	✓	✓		✓	✓	✓		✓
Tsang, S.(2017)	✓		✓	✓		✓		✓
Christidis, K.(2016)	✓	✓	✓		✓		✓	

LIBRARY FETSM

In Table 2.3, analysis of different Web3 digital identity frameworks is presented, strikingly, all of the first seven are shared by all: DIDs, VCs, smart contracts, interoperability protocols, user control, security mechanisms, and privacy enhancements; each of the reviewed leading examples incorporates these in an effort to guarantee functionality, security, and user autonomy of a digital identity system in a Web3 context.

The Economic Opportunities components are less considered. This neglect shows that the importance of integrating digital identity with wider economic activities and social trust system is underestimated, and this kind of integration is to improve the applicability and credibility of digital identity the key (Dai et al. 2019).

In addition, inconsistencies in regulatory considerations may lead to compliance challenges when deploying these systems in different jurisdictions, which may hinder the technology's global scale application and acceptance. At the same time, most frameworks do not consider user education as a core. In part, this may cause difficulties for users to adopt, because the effective use of Web3 technology requires users to have a certain understanding and adaptation to these technologies.

2.3 CONCEPTUAL FRAMEWORK

In the course of a literature review about improvements in Web3 digital-identity authentication systems, some are into designing the conceptual framework, taking as main core for construction decentralized identifier-DIDs, verifiable credential-VCs, and smart contract along with a User Centric security mechanism (Spataru 2020).

By integrating these key components, this model is targeted to solve core issues of the existing system, such as privacy and security, and user control, and further push digital identity management in a more secure, transparent, and user-led direction.

Traditional authentication methods for digital identity, especially those under centralized management, provide a certain degree of security, while their centralized storage characteristics bring a great deal of vulnerability to users' personal information

in the face of hacker attacks. Besides, the system usually lacks sufficient transparency and the users have little control over their own data. This is in response to these problems through this conceptual framework that makes a proposal for a blockchain technology-based decentralized solution so that more security and user's full autonomy can be given. Figure 2.2 shows the core of the important conceptual framework.

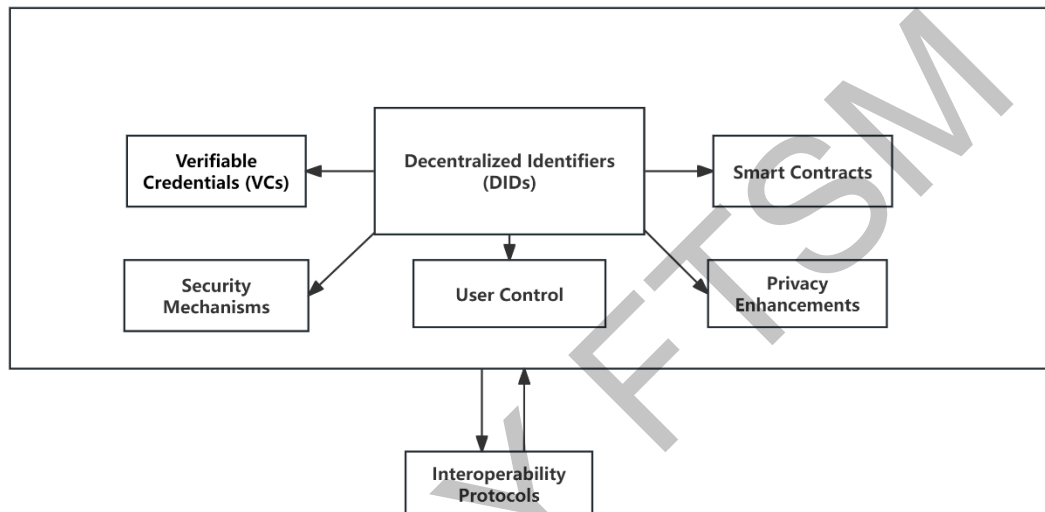


Figure 2.2 Conceptual framework diagram

It places the DIDS at the center, which reflects the core in identity authentication. DID is the unique and continuous identifier for users across a wide range of Web3 services and the point from which all else emanates. Positioning the centralized identifier in the middle captures its central role in the centralization of consistency and security of user identities.

On one side of the centralized identifier are verifiable credentials, and on the other side, smart contracts, showing that they are major technologies interacting directly with the centralized identifier. The VCs are used in the proof of the attributes or identity of users, while the smart contracts automate the verification process of such proofs. This is to show that the VCs and smart contracts have to do directly with the implementation of the centralized identifier authentication.

The user control module is put under the central identifier DIDS and has a direct linkage, highlighting the control that users have to exercise over their identities. This hierarchy of structure is an illustration that DIDS, or centralized identifiers, support the control to be exerted by the users themselves over their identity information, clearly pointing toward user sovereignty-that users are the true owners of their personal identity data.

Correspondingly, according to VCs and smart contracts respectively, it illustrates the lower-left corner for the security mechanism component and the lower-right corner for privacy enhancement in Figure 2.2. Obviously, that means only good supporting securities of both can provide good authentication systems, enable identity authentication with security guaranteed and ensure a complete data protection for the user during operation.

Finally, the interoperability protocol component is located at the bottom of the entire layout, supporting all the above elements. This shows that interoperability is the foundation for the entire identity authentication system to work across different networks and services, and is the bridge connecting all components.

This conceptual framework diagram effectively shows the relationship and interaction between the components, as well as the role and importance of each component in the identity authentication process.

2.4 CONCLUSION

This chapter cites many existing literatures, studies the evolution of digital identity authentication through SLR, explores the challenges and limitations of current digital identity authentication, and finally explores the key elements of web3 digital identity authentication. Research Question 1 focuses on the transition from web1 to web3. It emphasizes the progress of web3 digital identity authentication technology from centralized to decentralized digital identity authentication systems. Research Question 2 explores the challenges and limitations of digital identity authentication systems from the aspects of user privacy, risk security, regulatory environment, and technology. Research Question 3 explores the key elements of Web3 digital identity authentication,

such as decentralized identifiers (DIDs), verifiable credentials, and smart contracts, emphasizing their role in enhancing user privacy, security, and control over personal data.

Through this SLR, Several gaps in the literature have been identified. Mühle(2018) pointed out in his research that although Web3 technology provides enhanced user control and decentralization features, in practice how to effectively protect users' sensitive information and prevent unauthorized data access is still a problem. The problem is not fully resolved. Although Web3 technology promises greater user control and decentralized features, in practice how to effectively protect users' sensitive information and prevent unauthorized data access remains an under-addressed issue. Besides, existing research seldom pays attention to how these measures for the protection of privacy can be implemented without sacrificing user experience. More in-depth research is needed in this respect to ensure that digital identity systems are secure yet easy to use.

CHAPTER III

METHODOLOGY

3.1 INTRODUCTION

Chapter 3 will detail the concrete research methods to be applied in investigating Web3 digital identity. The research methodology includes a systematic literature review, questionnaire, statistics analysis, and reliability test. These methods were chosen for comprehensive understanding of the existing literature and to collect empirical data related to the research questions outlined in Chapter 1 and to develop a new framework for web3 digital identity.

The SLR has been done to identify, analyze, and synthesize existing research on Web3 digital identity. Selection of research papers should be made from several databases to avoid selection bias and broadly cover the topic. Following the guidelines of Kitchenham and Charters (2007), screening of the papers in the databases was performed to select the content suitable for study. It seeks to provide a clear and reproducible framework for searching and analyzing the literature. Specific steps include defining inclusion and exclusion criteria, searching relevant databases, selecting studies based on predefined criteria, and synthesizing research results.

The questionnaire was used to retrieve primary data to supplement the insights from the SLR. Such a questionnaire targets professionals or experts in the Web3 technology field. Practical challenges and key components are key areas that the questionnaire on Web3 digital identity is built on. The guidelines offered by Artino Jr. et al. (2014) outline considerations that should be placed in developing survey items to conform with the research objectives since a survey is only useful as its items.

Lastly, the statistics analysis and reliability test were performed on the data collected from the questionnaire. The results have laid the foundation for the development of a new web3 digital identity authentication framework in Chapter 4.

3.2 RESEARCH DESIGN

This study will comprehensively analyze the development trends, challenges, limitations, and essential components of Web3 digital identity authentication. This research design aims to propose a new digital identity authentication framework and explore how decentralized identity authentication technology can better protect users' personal privacy and security.

The method for collecting essential components and framework information will be in the form of an online questionnaire survey, with the goal of collecting data from IT professionals and cybersecurity experts to assess their views and acceptance of current web3 digital identity authentication technology. The questionnaire will include questions such as participants' views on existing digital identity authentication systems and their assessment of the importance of each component. The data will be analyzed using SPSS software to determine the components of the web3 digital authentication identity framework to be constructed. All collected data will be integrated and analyzed to fully understand the application of Web3 digital identity in cybersecurity.

Through this research design, this study hopes to comprehensively evaluate the application prospects of Web3 digital identity authentication components and propose a new web3 digital authentication identity framework and provide empirical foundations and theoretical insights for the field of cybersecurity.

3.3 SYSTEMIC LITERATURE REVIEW(SLR) METHODOLOGY

The purpose of this review is to identify, evaluate, and discuss all available literature to answer relevant research questions about the key components of digital identity for web3. The academic sources were collected and evaluated based on the methodology of Kitchenham (2004) and Rojas et al. (2016).

Kitchenham's(2004) method is widely respected in the software engineering community, especially for conducting systematic literature reviews (SLRs). The method involves several steps: defining the research question, identifying related work, selecting and evaluating studies based on predefined inclusion and exclusion criteria, and synthesizing the collected data. By adopting this approach, the report ensures that all relevant literature is fully and objectively covered, minimizing bias and maximizing the breadth of the review.

Additionally, Rojas et al.' s(2004) methodology enhanced the quality of the research evaluation, which is critical to understanding the strength of existing evidence. The methodology provided guidance for evaluating the reliability, validity, and relevance of research findings, helping me critically analyze the impact and applicability of the reviewed research in the context of Web3 digital identity.

Combining these two methodologies, the literature review reported here systematically collected and rigorously evaluated existing academic research, supporting a deeper understanding of Web3 digital identity. This approach not only strengthened the foundation of my research, but also ensured that the conclusions drawn were based on rigorously reviewed evidence, providing a solid foundation for further research.

3.3.1 Research question(RQ)

This report designs a series of research questions (RQs) to comprehensively explore and discuss the application prospects of Web3 digital identity authentication and the basic model of digital identity in network security. In addition, this study also explore the development trend from Web1 to Web3. The goal of the study is to review the existing Web3 digital identity authentication models to overcome current technical challenges. Through this literature review, the shortcomings of the existing framework will be identified and new ramework be proposed. Chapter 2 of this report addresses the following research questions:

1. RQ1:What is the development trend of Web3 Digital identity authentication?
2. RQ2: What are the challenges and limitations of current digital identity authentication applications?
3. RQ3: What are the key elements of Web3 digital identity authentication?

3.3.2 Search process

The literature search process is to create a combination of search strings to help search for literature. This article starts with the following steps:

1. Determine the professional terms and keywords used to solve each problem. It is very important to use the correct professional terms to avoid deviations in the research direction of the search literature. Keywords can make the searched literature more in line with the direction of your own research.
2. List the keywords of existing literature. Searching previous literature helps to list the most commonly used keywords. However, not all literature is conducive to the research of the problem. Therefore, filter out keywords that are irrelevant to the topic and have a low degree of relevance, and select the keywords that best answer the research question.
3. Find synonymous keyword replacement words. The search for synonyms needs to be done based on a thesaurus, which is a set of databases used to provide standardized synonyms.
4. Using the Boolean 'AND' to link the major keywords.
5. Use the Boolean 'OR' in the search string to include synonyms.

The following are the main keywords related to the research questions:

1. Web3 digital identity authentication model OR web3 digital identity authentication framework

2. Web3 digital identity authentication development trend OR web3 digital identity authentication development history
3. Web3 digital identity authentication limitations OR web3 digital identity authentication challenges

Literature search was done using the following search string:

(Web3 digital identity authentication model OR web3 digital identity authentication framework) AND (Web3 digital identity authentication development trend OR web3 digital identity authentication development history)AND(Web3 digital identity authentication limitations OR web3 digital identity authentication challenges)

According to Kitchenham (2004), in order to avoid bias in the review process, multiple different databases should be selected during the search process to ensure the reliability of the literature. In the process of searching for academic literature, a total of three online databases were used for memorial review and review. The selected databases are Scopus and Web of science. The results of the search using the search string are summarized in Table 3.1 below.

Table 3.1 Summary of database search result

Digital Library	Year	Number of results
Scopus	2014-2024	416
Google Scholar	2014-2024	6930
Web of science	2014-2024	172

3.3.3 Selection of literature

The results compiled in the above search table include all questions related to the research question. The following inclusion and exclusion criteria should be used to narrow down the scope of literature related to this review paper

Scholarly publications considered for review must match the specified search keywords, ensuring relevance to the subject matter. They should be published within the last ten years, from 2014 to 2024, to guarantee that the discussions are current and relevant. Additionally, these publications must discuss issues pertinent to the research topic, offering valuable insights and perspectives.

Publications not written in English are excluded to maintain comprehension and coherence in analysis. Unpublished articles from websites, magazines, classroom lectures, advertisements, and similar sources will not be considered. Publications that receive very poor (0-2) or poor (2-3) evaluation scores based on the literature quality assessment are also excluded to ensure the integrity and credibility of the review process.

In order to maintain higher relevance to the current problem, this review only selected literature published within 10 years from 2014 to 2024. In addition, the collected literature is mainly related to the comparison of web3 digital identity authentication framework with challenges and limitations.

3.3.4 Literature quality assessment

Kitchenham (2004) explained the methods and importance of evaluating the quality of review articles, including:

1. More detailed inclusion and exclusion guidelines need to be included.
2. To examine whether differences in quality could explain differences in study results.
3. As a way of measuring the value of individual studies when evaluating results.
4. Guide the analysis of results and assess the strength of inferences between the literature.
5. Helps to make suggestions for future research.

Kitchenham (2004) proposed using a checklist to evaluate the quality of literature in the review. The check shown in Table 3.2 below is composed of seven general questions for evaluating the quality of literature using scores. Use the following scoring table: Yes=1, Probably=0.5, No=0, and comprehensively score the quality of the literature using seven questions.

1. Is the article cited by other scholars who study web3 digital identity authentication?
2. Is the research objective clearly stated? For example, there are clear research questions that meet web3 digital identity authentication.
3. Is the research objective fully described? For example, the framework and key components of web3 digital identity authentication.
4. Is the data collection sufficient? For example, sufficient questionnaire results or interviews, etc.
5. Are potential confounding factors adequately controlled during analysis? For example, policy and legal environment, technical infrastructure, user behavior diversity, etc.
6. Are the survey results credible? For example, the method of collecting data or the design of the questionnaire, etc.
7. Are the methods of discussion and explanation of analysis well presented?

All the literature was evaluated using the above evaluation criteria to select the best quality literature. Literature with very poor scores (0-1) or poor (2-3) will be excluded and not used because it is considered to be poor quality literature and cannot solve the relevant problems in the study. The results of the literature search and review are in the second chapter of this study.

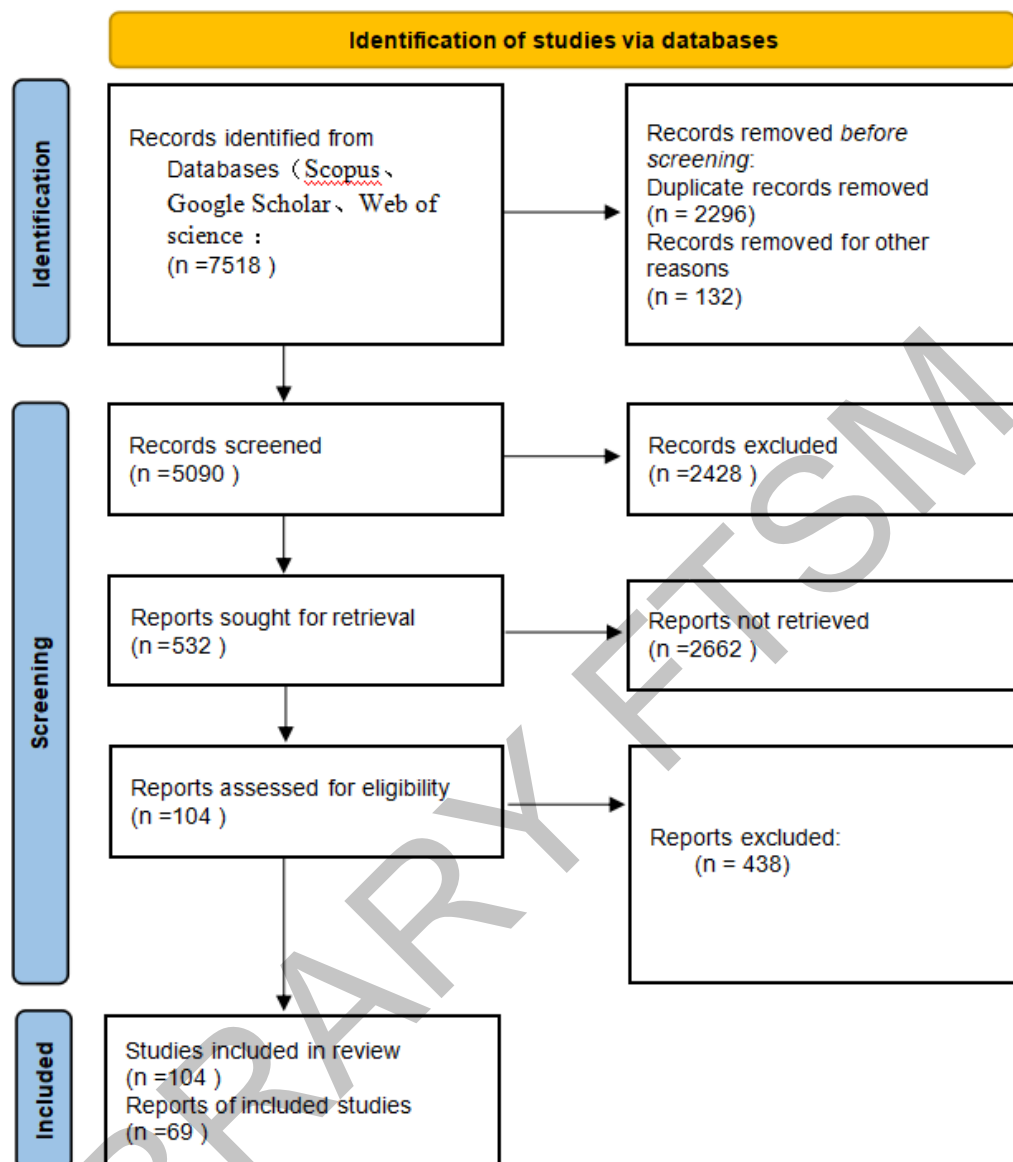


Figure 3.1 The process Search

According to Kitchenham (2004), I identified 7518 records from Scopus, Google Scholar, and Web of Science databases. Before screening, a total of 2428 records were removed due to duplication and other reasons, leaving 5090 records for further screening. During the screening process, 2428 records were excluded. Afterwards, a detailed search was attempted on the remaining 2662 records, and 532 were successfully retrieved. These successfully retrieved reports were then assessed for eligibility, of which 428 were excluded for low article rating and ultimately 104 studies

were included in the review, including 69 detailed reports. This process, as shown in Figure 3.3.2, shows how a large number of initial records can be screened and evaluated to identify studies that meet specific research criteria.

3.3.5 The result of the SLR

The results of the literature review informed the structure of the questionnaire and focused on the identified key components of web3 digital identity authentication based on the results obtained from the literature. Namely, Decentralized Identifiers (DIDs), Verifiable Credentials (VC), Smart Contracts, Interoperability Protocols, User Control, Security Mechanisms, and Privacy Enhancements. These key components serve as the basic survey part of the questionnaire and provide a comprehensive framework for evaluating web3 digital identity authentication in a research context. Table 3.2 shows the relevance of the problem statement, research objectives, methods, and predicted results.

Table 3.2 Methodology for achieving output results

Aspect	Problem Statement	Objective	Methodology	Output
1	There is currently a lack of clear and systematic understanding of which components are the key factors that make up the Web3 digital identity authentication system. This has led to difficulties in achieving optimal design and implementation in practical applications, and has also hindered the further development and adoption of the technology.	Explore the essential components in web3 digital identity authentication.	Explore the essential components of web3 digital identity authentication through the SLR process.	Identify essential areas to include in the questionnaire.
2	Existing research on web3 components often fails to fully evaluate the role of each component in ensuring the security and reliability of digital identities. This lack of data-driven understanding may lead to security vulnerabilities and inefficient resource allocation.	Investigate the criticality of web3 components	Investigate the criticality of web3 components and collect data through questionnaires.	Use the questionnaire to assess the importance of web3 digital identity components.
3	The current Web3 digital identity authentication model has security risks. In order to improve the overall security and reliability of the system, it is urgent to develop a new and more secure authentication framework.	Build a more secure web3 digital identity authentication framework.	Analyze the data.	Identify component importance and propose a more secure web3 digital identity framework.

3.4 QUESTIONNAIRE VALIDATION

Through SLR, I learned about the key components of web3 digital identity authentication. Next, we used Google Form to compile a questionnaire that included the seven key components of web3 digital authentication, namely decentralized identifiers (DID), verifiable credentials (VC), smart contracts, interoperability protocols, user controls, security mechanisms and privacy enhancements, and components broken down by each key component. The focus was on determining its criticality. The specific questionnaire questions are in Appendix A.

The design of the questionnaire, from its visual layout to the wording of the questions, will have a significant impact on the data collected (Tsang et al. 2017). After the initial drafting of the questionnaire items, I consulted experts from Shandong Luying Information Technology Co., Ltd. to review the accuracy of the items, as well as the structural and grammatical correctness of the items (Aithal & Aithal 2020). The questionnaire was then sent to a panel of experts for pilot testing to assess whether the questionnaire items effectively captured the criticality of the web3 digital identity components. The questionnaire will be distributed to the employees of Shandong Luying Information Technology Co., Ltd. via email for data collection.

The final stage of questionnaire development includes conducting reliability and validity tests (Tsang et al. 2017). Data analysis will be conducted using software such as spss. Chapter 4 will describe the detailed analysis of each component composition.

3.5 PILOT TESTING

A pilot test will be conducted before the questionnaire is widely distributed. The pilot test will invite 30 experts from Shandong Luying Information Technology Co., Ltd. Practitioners from the field of Web3 technology to evaluate the validity and comprehensibility of the questionnaire. The questionnaire design focuses on evaluating the seven essential components of Web3 digital identity authentication: decentralized identifiers (DIDs), verifiable credentials (VCs), smart contracts, interoperability protocols, user controls, security mechanisms and privacy enhancements, as well as the small components that constitute the seven essential components. The Cronbach alpha

value of the pilot study is greater than 0.7, indicating that the questionnaire is valid and comprehensible. The results are shown in Table 3.4.

Table 3.3 Cronbach alpha obtained in pilot study

Component	Cronbach's Alpha	Number of Items	Component
Interoperability Protocols	0.959	4	Interoperability Protocols
Decentralized Identifiers (DIDs)	0.943	6	Decentralized Identifiers (DIDs)
User Control	0.917	4	User Control
Smart Contracts	0.910	4	Smart Contracts
Security Mechanisms	0.901	4	Security Mechanisms
Privacy Enhancements	0.903	4	Privacy Enhancements
Verifiable Credentials (VCs)	0.905	4	Verifiable Credentials (VCs)

3.6 DATA COLLECTION

The purpose of data collection is to evaluate the importance of the seven key components of Web3 digital identity authentication and the small components that make up the seven key components to the overall security architecture. The data collection process is precise and systematic to ensure the reliability and validity of the research results. The questionnaire was published online using the Google Forms platform. First, respondents were asked to provide basic demographic information, including gender, age, education, and job level. The questionnaire then asked a series of questions for each key component to assess its importance and validity. Finally, there will be open questions for respondents to answer. The questionnaire design was optimized based on the results of the above-mentioned guided testing to ensure that each question has high reliability and validity (Aithal & Aithal 2020).

The target sample group is technical experts and developers from Shandong Luying Information Technology Co., Ltd. working in the Web3 field. It is expected that about 100 valid questionnaires will be collected. The survey distribution cycle is 3

weeks, and all participants are employees of formal units of the enterprise to ensure the reliability of the data.

The specific questions in the questionnaire revolved around the importance of the seven key components and the subcomponents that make up the seven key components to the overall security architecture, using a 5-point Likert scale ranging from 1 (strongly disagree) to 5 (strongly agree).

Based on the methodology of Parsons et al. (2017), the questionnaire asked about the seven related components and provided a brief description of each question. If all responses throughout the questionnaire followed a consistent response pattern, such as all responses strongly agree or all responses strongly disagree, it indicates a lack of concern among the respondents. Therefore, it is reasonable to exclude the responses of such participants from the final analysis.

3.7 DATA ANALYSIS

During the data analysis phase, I conducted various tests to ensure the rigor of the analysis. These included data cleaning, descriptive statistics analysis, and reliability tests (Cronbach's Alpha). The details of each test are described below.

Data cleaning is a critical step in the data analysis process, especially when dealing with questionnaire data. Ensuring data quality is essential to obtaining reliable and accurate research results. In addition to handling missing values, another important data cleaning task is to identify and exclude invalid questionnaire answers. These invalid responses may be due to participants filling in answers randomly without carefully considering each question. I will exclude participants who choose the same answer option on all questions, such as choosing "strongly agree" or "strongly disagree" on all questions. This pattern may indicate that participants did not read the questions carefully and answered randomly or mechanically.

Reliability tests were conducted after data cleaning, and according to (Chan & Idris 2017), Cronbach Alpha values above 0.7 are considered reliable.

The collected data were processed using statistical tools such as SPSS and Microsoft Excel. This involved calculating basic statistics like mean score, median, mode, and standard deviation for each key component. These statistics provide an overall understanding of the dataset, including the general acceptance and consistency of participant responses to each component. The results of the descriptive statistics analysis can be displayed graphically, using bar graphs and box plots to depict the distribution of the data. The analysis process will exclude options with a score of 3, as these responses do not accurately reflect the importance of the component.

3.8 CONCLUSION

Figure 3.2 shows the methodology of this study starts with using SLR research literature to identify the key components of Web3 digital authentication, followed by expert validation. After establishing a questionnaire, the criticality of the seven components was investigated, followed by data collection and final data analysis. This comprehensive research approach provides in-depth insights and key data support for the development of the Web3 digital identity authentication framework, ensuring that the information needs of the development process are fully met, laying the foundation for the proposal of the web3 digital identity authentication framework in Chapter 5.

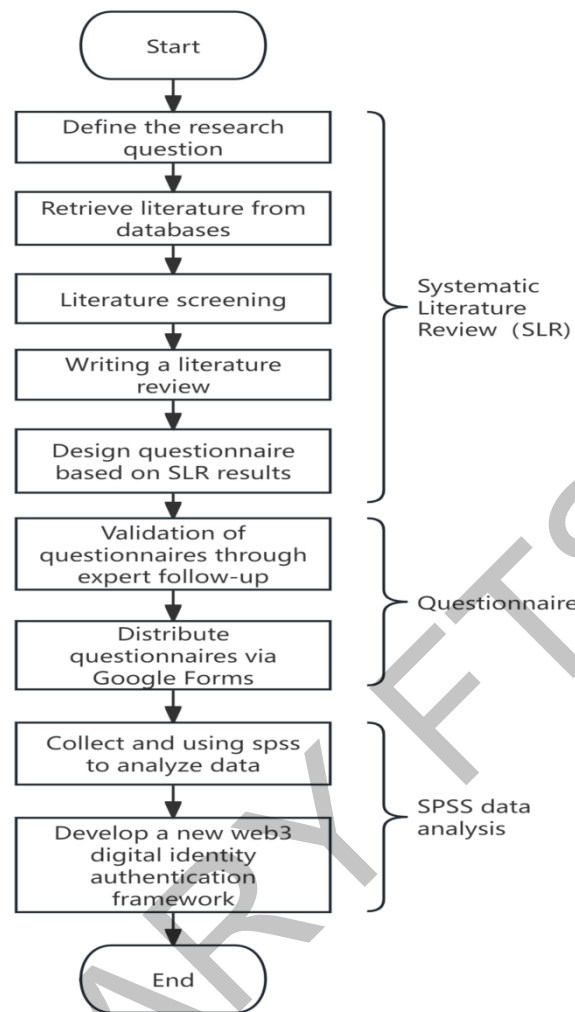


Figure 3.2 Flowchart of methodology process

CHAPTER IV

RESULTS AND DISCUSSION

4.1 INTRODUCTION

Chapter 4 presents the analysis and interpretation of the survey results conducted to assess the Web3 digital identity authentication framework. This chapter will discuss the assessment of the critical components of the framework, which includes DIDs, VCs, Smart Contracts, User Control, Security Mechanisms, Privacy Enhancements, and Interoperability Protocols. Besides these seven key elements, the chapter also elaborates on the addition of the newly developed Advanced Monitoring and Analysis Component, AMAC, which applies artificial intelligence and machine learning for the immediate detection of threats and the monitoring of systems.

The chapter has been divided into several sections, each detailing different aspects of the survey and the insights obtained. Section 4.2 presents the demographic outcome of the respondents, which puts the analysis into context by showing the breakdown of the participants' gender, age, professional roles, and experience with Web3 technologies. The demographic distribution is important to understand while interpreting the survey responses because it helps us assess how relevant and expert the participants are in relation to the Web3 domain.

Results from the validity and reliability tests are presented in Section 4.3. This discusses the Cronbach's Alpha scores for the various components, thus providing insight into how reliable this survey instrument is consistently. In such cases, the reliability analysis shall ensure that the data ensuing from the survey is reliable, as the responses accurately reflect perceptions of the participants on the components making up Web3 digital identity.

Section 4.4 describes the descriptive statistic analysis-mean, median, mode, and standard deviation-of each component that makes up Web3 digital identity. The analysis generally presents an agreement on the ranking of the importance of various components as identified by respondents in order to pinpoint areas that may require further development or enhancement. This section provides further graphical representations for insight into the distribution of responses.

These results are discussed in-depth and their criticality in setting a basis for the next chapter on the proposed Web3 digital identity framework within Section 4.5.

Through the in-depth analysis carried out, an understanding of data will be provided about those elements of primary importance to compose the Web3 digital identity systems and thus permit ways for further developments within the same field.

4.2 SURVEY RESULTS

This section will introduce the personal information of the respondents, including gender, age, education, experience, etc. It lays the foundation for the analysis of specific component data later.

4.2.1 Gender identity

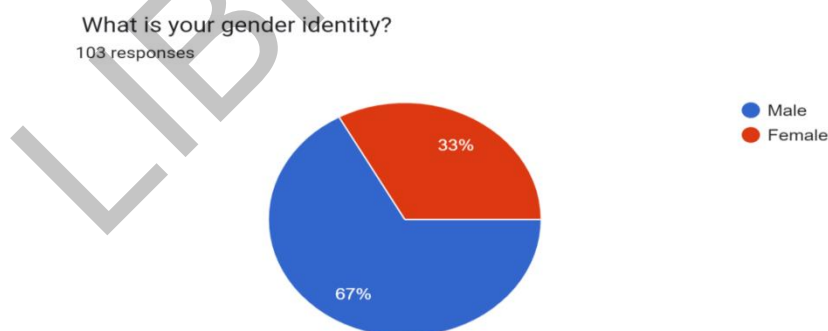


Figure 4.1 Demographic Distribution of Respondents by Gender

The survey results show that males are the majority of the respondents, accounting for 68% of the respondents, while females account for a smaller proportion of 23%.

4.2.2 Age groups

What is your age category?

103 responses

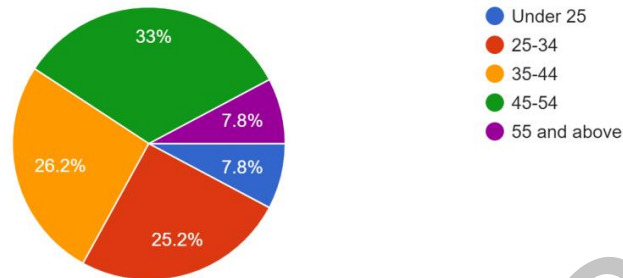


Figure 4.2 Age Distribution of Respondents

The survey results showed that 7% of the respondents were under 25 years old, 26% were 25-34 years old, 27% were 35-44 years old, 34% were 45-54 years old, and the last 6% were 55 years old and above.

4.2.3 Professional roles

What is your Professional Background?

103 responses

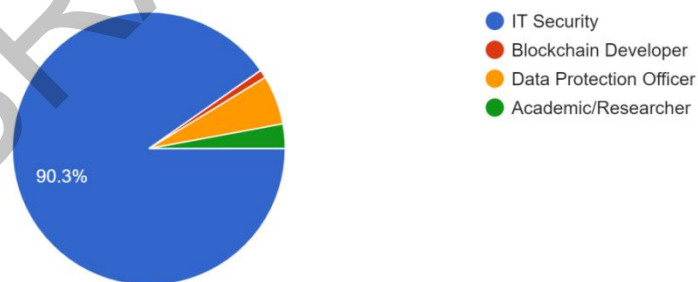


Figure 4.3 Professional Role Breakdown of Survey Respondents

The majority of respondents (91%) were IT security professionals, with blockchain developers making up 2% of participants, data protection officers making up 4% of respondents, and academics and researchers making up 3% of the sample.

4.2.4 Experience with WEB3

What is your level of experience with Web3 technologies?

103 responses

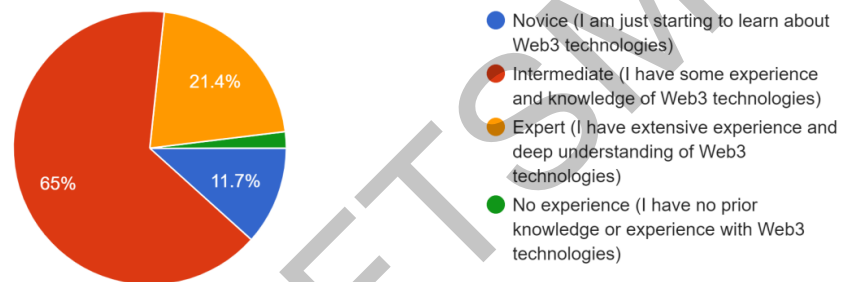


Figure 4.4 Experience Level of Respondents with Web3 Technologies

The respondents' experience level with Web3 technologies is divided into four groups: novice, intermediate, expert, and inexperienced. Figure 4.1 shows the distribution of respondents according to their self-reported experience level with Web3 technologies. The largest group is intermediate, accounting for 65% of the respondents, while novices account for 12%, experts account for 21.4%, and experienced respondents account for 2%.

4.2.5 Education level

What is the highest level of education you have completed?
103 responses

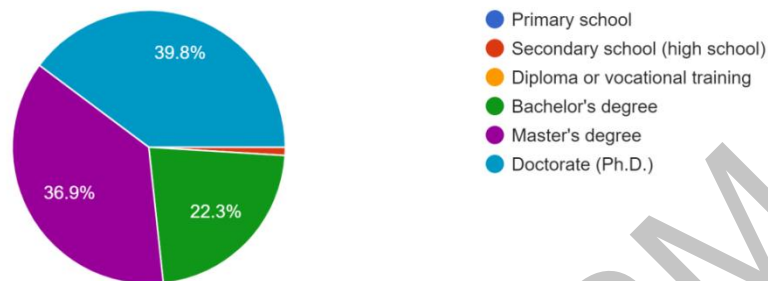


Figure 4.5 Educational Background of Survey Respondents

21% of the respondents had a bachelor's degree, 36% had a master's degree, 41% had a doctorate (PhD), and 2% had secondary education. Most of the respondents have a doctorate degree.

4.3 RESULTS OF THE VALIDITY AND RELIABILITY TEST

To conduct the reliability test, Cronbach's Alpha is used to measure the internal consistency of the survey instrument. This involves grouping related survey items, such as those assessing the various components of the Web3 digital identity framework, and calculating the Cronbach's Alpha coefficient using statistical software like SPSS. A value of 0.7 or higher indicates acceptable reliability, meaning that the items within each component consistently measure the same underlying construct. If necessary, items with low reliability can be removed or adjusted to improve the overall consistency of the instrument. The results of this test ensure that the survey produces valid and reliable data for assessing the Web3 framework.

4.3.1 Cronbach's alpha

In conducting Cronbach's Alpha, the first thing to do is to group those items of the survey which are designed to measure the same underlying construct. Hence, components of the Web3 digital identity framework, such as DIDs, Smart Contracts,

and User Control. These items should be entered into a statistical software package like SPSS, where the Cronbach's Alpha coefficient is calculated. The software correlates the items on their tendency to consistently reflect the same construct. The Cronbach's Alpha ranges from 0 to 1, and generally, above 0.7 indicates acceptable internal consistency. If it is less than 0.7, the items are not reliably measuring the same construct, and some changes might be necessary: rewording or removing problem items. This process makes sure that the survey instrument is reliable and captures only what it is intended to capture in the Web3 digital identity framework.

Table 4.1 Reliability analysis

Component	Cronbach's Alpha	Number of Items
Interoperability Protocols	0.968	4
Decentralized Identifiers (DIDs)	0.946	6
User Control	0.921	4
Smart Contracts	0.914	4
Security Mechanisms	0.904	4
Privacy Enhancements	0.901	4
Verifiable Credentials (VCs)	0.901	4

The reliability analysis results, evaluated using Cronbach's Alpha, indicate strong internal consistency across all components of the Web3 Digital Identity Authentication Framework. This confirms that the survey instrument reliably captured participants' perceptions of the significance of each component.

Interoperability Protocols achieved the highest Cronbach's Alpha score of 0.968, showcasing exceptional reliability. This suggests a high level of agreement among respondents regarding the importance of interoperability metrics such as data format standards, protocol bridges, standardized APIs, and cross-chain communication. These findings underline the critical role of seamless interaction between various blockchain platforms in ensuring the success of Web3 identity systems.

Decentralized Identifiers (DIDs) ranked second, with a reliability score of 0.946 across six items, including DID Controllers, DID Methods, and Authentication Protocols. This strong reliability score affirms the essential role of DIDs in supporting user ownership and control over their digital identities. The high consistency also highlights the importance of standardization and integration within DID components to enhance their effectiveness.

User Control and Smart Contracts followed with Cronbach's Alpha scores of 0.921 and 0.914, respectively. The consistency in User Control responses reflects the strong emphasis placed on data privacy, consent management, and robust access controls, aligning with the Web3 paradigm of empowering users with control over their identity data. Similarly, Smart Contracts exhibited high reliability, reinforcing their importance in enabling secure, efficient, and interoperable identity verification processes.

Other components, including Security Mechanisms (0.904), Privacy Enhancements (0.901), and Verifiable Credentials (VCs) (0.901), also demonstrated excellent reliability. These scores highlight the significance of encryption technologies, zero-knowledge proofs, authentication protocols, and public keys in ensuring the security and privacy of Web3 systems. The inclusion of revocation mechanisms and issuer information within VCs was noted as areas requiring further refinement.

Overall, the high Cronbach's Alpha scores across all components validate the dependability of the survey instrument. These findings provide a solid foundation for analyzing the survey data, identifying gaps, and developing recommendations to enhance the Web3 Digital Identity Authentication Framework.

The dependability of the survey instrument is confirmed by the high Cronbach's Alpha scores for each component. They attest to the survey items' consistent measurement of their corresponding components, offering a strong basis for analyzing respondents' responses and guiding the creation of a strong Web3 digital identification framework. This guarantees that the survey results may be utilized with confidence to determine Web3 system goals, evaluate gaps, and suggest enhancements.

4.4 DESCRIPTIVE STATISTICS:KEY METRICS FOR WEB3 COMPONENTS

4.4.1 Decentralized identifiers(DIDS) table

Table 4.2 Descriptive Statistics of Decentralized Identifiers Table

Subcomponent	Mean	Median	Mode	Std. Deviation
Inclusion of DID Documents	4.82	5.00	5	0.458
Inclusion of DID Methods	4.80	5.00	5	0.471
Role of DID Controllers	4.82	5.00	5	0.460
Use of Verifiable Data Registries	4.13	4.00	4	0.497
Specification of Service Endpoints	4.07	4.00	4	0.443
Implementation of Authentication Protocols	4.10	4.00	4	0.465

The analysis of DIDs therefore highlights a number of interesting insights into the perceived importance of its subcomponents for developing Web3. In support, the inclusion of DID Documents was rated highly, with an average of 4.82 and low standard deviation of 0.458, which suggests a strong level of consensus among respondents as to their critical role in underpinning transparency and structural integrity of the framework. In the same light, the DID Methods scored a mean of 4.80 with a slightly higher SD (0.471), indicating foundational value but with somewhat more variability in agreement.

The importance of DID Controllers was very high, with an average of 4.82 ± 0.460 , reflecting their key contribution to decentralized governance and identity management. Conversely, Verifiable Data Registries are important but of a lower mean, 4.13, with higher standard deviation, 0.497, indicating that there is room for improvement or further clarification on their relevance in the ecosystem.

In this respect, both the Specification of Service Endpoints, mean = 4.07; SD = 0.443, and Implementation of Authentication Protocols, mean = 4.10, SD = 0.465, reached a moderate level of criticality but with lower levels of consensus than other

subcomponents. While these are foundational tenets to Web3 security, they tend to be seen as secondary in immediacy or urgency compared to core elements, such as DID Controllers and Documents. Overall, the results underlined the need to focus on universally valued components while considering variability in the perception of less central aspects in order to have a cohesive and robust DID framework for Web3.

4.4.2 Verifiable credentials(VCS)

Table 4.3 Descriptive Statistics of Verifiable Credentials (VCs) Table

Subcomponent	Mean	Median	Mode	Std. Deviation
Inclusion of VCs	4.76	5.00	5	0.551
Integration of Public Keys	4.78	5.00	5	0.541
Authentication Methods	4.78	5.00	5	0.541
Inclusion of Issuer Information	4.01	4.00	4	0.551
Revocation Mechanisms	4.00	4.00	4	0.542

The analysis of Verifiable Credentials (VCs) provides valuable insights into their significance for enhancing secure digital identity verification in Web3 mechanisms. The integration of public keys and the use of diverse authentication methods both received exceptionally high ratings, with identical means of 4.83, medians of 5.00, and low standard deviations (0.451). These results indicate strong consensus among respondents regarding the critical role these components play in ensuring security and user verification in decentralized systems.

In contrast, the inclusion of issuer information was rated with a mean of 4.11 and a standard deviation of 0.474, reflecting a lower level of agreement about its importance for transparency and trust. This suggests that while it is recognized as relevant, its role might require further clarification or enhancement to meet stakeholder expectations.

Similarly, the robustness of revocation mechanisms, essential for managing the lifecycle and validity of credentials, showed a slightly lower mean of 4.10 and a standard deviation of 0.465. This indicates that while respondents recognize their importance, there is less consensus compared to other aspects of VCs.

Overall, the findings emphasize that public keys and diverse authentication methods are universally valued for securing Web3 applications, while components like issuer information and revocation mechanisms could benefit from focused improvements to strengthen their role in fostering trust and reliability in decentralized identity verification framework.

4.4.3 Smart contracts table

Table 4.4 Descriptive Statistics of Smart Contracts Table

Subcomponent	Mean	Median	Mode	Std. Deviation
Importance of Smart Contracts	4.78	5.00	5	0.541
Execution Efficiency	4.13	4.00	4	0.489
Security Features	4.82	5.00	5	0.458
Interoperability with Blockchains	4.09	4.00	4	0.461
Upgradeability and Maintenance	4.09	4.00	4	0.527

The questions in the survey regarding Smart Contracts were pointed to gauge users' perceptions about the importance and roles of different elements, including performance, security, and interoperability within Web3 environments. The importance of Smart Contracts in automating the procedures of identification and transaction security in Web3 has been assessed. The survey also focused on the issue of centrality related to efficiency in implementation and the security features of Smart Contracts and their compatibility with other chains, considering seamless integrations across diverse chains. Additionally, the flexibility to update and maintain Smart Contracts was emphasized, reflecting concerns about future-proofing and ensuring compliance with evolving requirements. These questions aimed to understand both the prospects of

Smart Contracts in enhancing the efficiency and capacity of Web3 networks and the potential challenges, especially regarding performance optimization, security concerns, and adaptability to future changes.

4.4.4 User control table

Table 4.5 Descriptive Statistics of User control

Subcomponent	Mean	Median	Mode	Std. Deviation
Governance and Operation	4.76	5.00	5	0.548
Identity Ownership	4.77	5.00	5	0.546
Data Privacy and Consent	4.77	5.00	5	0.546
Access Control Mechanisms	4.75	5.00	5	0.555
Auditability	4.01	4.00	4	0.586

The table for user control components within Web3 systems displays a high level of agreement on the importance of governance, identity ownership, data privacy, and access control, with all these subcomponents achieving means close to 5.00 and medians and modes at 5, indicating strong consensus and prioritization among respondents. Specifically, "Governance and Operation," "Identity Ownership," and "Data Privacy and Consent" each scored 4.77 for mean, suggesting these aspects are viewed as nearly indispensable in managing and safeguarding user data within Web3 technologies. The relatively high standard deviations (around 0.546 for most) indicate a slight variability in opinions, yet still within a range suggesting overall strong agreement.

"Auditability," however, is perceived somewhat differently, with a mean of 4.01, a median of 4.00, and a mode of 4, alongside the highest standard deviation of 0.586. This lower scoring and higher variance might point to uncertainties or inconsistencies in how audit processes are implemented or understood in Web3 frameworks. It suggests that while considered important, auditability may not be as well integrated or emphasized as other aspects of user control, signaling a potential area for further focus

and standardization to ensure robust, transparent auditing mechanisms in Web3 environments.

4.4.5 Security mechanisms table

Table 4.6 Descriptive Statistics of Security Mechanisms Table

Subcomponent	Mean	Median	Mode	Std. Deviation
Advanced Encryption Technologies	4.83	5.00	5	0.453
Robust Authentication Protocols	4.81	5.00	5	0.467
Intrusion Detection Systems	4.08	4.00	4	0.516
Decentralized Security Models	4.08	4.00	4	0.519

The descriptive statistics for the security mechanisms in Web3 systems illustrate a clear prioritization of encryption and authentication as central to maintaining security. "Advanced Encryption Technologies" and "Robust Authentication Protocols" are highly valued, with means of 4.83 and 4.81 respectively, and both holding median and mode values of 5. This highlights a consensus on their critical importance for securing Web3 environments. The standard deviations are relatively low (0.453 and 0.467), indicating a strong agreement among the respondents.

Conversely, "Intrusion Detection Systems" and "Decentralized Security Models" both have lower mean values of 4.08, with median and mode at 4, accompanied by higher standard deviations (around 0.516 and 0.519). These statistics suggest that while these components are recognized as important, there is slightly less consensus on their effectiveness or implementation compared to encryption and authentication technologies. This could indicate areas where further development or clarification might be needed to align perceptions and enhance security practices within the rapidly evolving Web3 framework.

4.4.6 Privacy enhancements table

Table 4.7 Descriptive Statistics of Privacy Enhancements Table

Subcomponent	Mean	Median	Mode	Std. Deviation
Data Anonymization Techniques	4.11	4.00	4	0.472
Consent Mechanisms	4.15	4.00	4	0.435
Zero-Knowledge Proofs (ZKP)	4.79	5.00	5	0.480
End-to-End Encryption	4.80	5.00	5	0.471

The descriptive statistics in this section show the valuation of different privacy enhancements that can be used in the systems of Web3. The emphasis on "Zero-Knowledge Proofs" and "EndtoEnd Encryption" comes highest, with means at 4.79 and 4.80 and a median and mode for both questions of 5, showing strong consensus around the vital role these technologies could play in enhancing privacy within a Web3 framework. This could show that there is still significant interest in protecting user data and transactions from unauthorized access or exposure.

In contrast, the average scores of "Data Anonymization Techniques" and "Consent Mechanisms" are 4.11 and 4.15, with medians and modes of 4, and considering also that standard deviations were still in the middle range-too for data anonymization at 0.472 and for consent mechanisms at 0.435, these represent satisfaction and/or agreement that has not been as high or widespread in the current effectiveness or way these components are done today, while generally recognized for their active roles in enhancing privacy. These lower ratings may be indicative of areas that require more focus or development for better alignment with the high-value technologies such as ZKP and end-to-end encryption so that the approach to privacy within the landscape of Web3 is holistic.

4.4.7 Interoperability protocols

Table 4.8 Descriptive Statistics of Interoperability Protocols Table

Subcomponent	Mean	Median	Mode	Std. Deviation
Cross-Chain Communication	4.10	4.00	4	0.586
Standardized APIs	4.11	4.00	4	0.474
Protocol Bridges	4.05	4.00	4	0.424
Data Format Standards	4.05	4.00	4	0.424

The descriptive statistics for interoperability protocols in Web3 systems reveal a somewhat moderated valuation across the subcomponents, reflecting challenges or diverse opinions on their effectiveness. "Standardized APIs" have the highest mean score of 4.11, closely followed by "Cross-Chain Communication" at 4.10, both with a median and mode of 4. This indicates recognition of their importance, but with room for improvement, as suggested by the relatively high standard deviations, especially 0.586 for Cross-Chain Communication. These figures imply variability in respondent opinions, possibly due to different experiences with the practical implementation of these technologies.

"Protocol Bridges" and "Data Format Standards" both score slightly lower, with means of 4.05 and the same median and mode of 4, accompanied by the lowest standard deviations (0.424). These lower scores and tighter spread of responses might suggest a consensus on their current limitations or the need for enhanced development and standardization to fully enable seamless interoperability across different blockchain platforms. The overall modest ratings across these subcomponents highlight critical areas where further innovation, clarity, and consensus are needed to improve interoperability within the Web3 ecosystem.

4.5 INTERPRETATION OF DESCRIPTIVE STATISTICS GENERAL OVERVIEW

According to the survey's findings, there is broad agreement among participants about the crucial significance of some Web3 digital identity system components, especially

those related to security mechanisms, privacy enhancements, verifiable credentials, and decentralized identifiers (DIDs). The mean, median, mode, and standard deviation statistics show patterns in respondents' opinions and the degree of agreement with these elements.

Table 4.9 Interpretation of Descriptive Statistics General Overview

Mean	Median	Mode	Standard deviation
<p>The majority of the components have consistently high mean scores, with all subcomponents falling between 4.00 and 4.78. This suggests that most respondents think these elements are crucial to the advancement of Web3 technologies. For instance, DIDs and Smart Contracts often received scores close to the top (mean of 4.78), indicating their crucial function in Web3 identity authentication.</p>	<p>Almost every component had a mode of 5, which was in line with the median. This indicates that the majority of respondents concurred that the components—particularly those pertaining to Smart Contracts, DIDs, and Security Mechanisms—were important. Revocation Mechanisms and Service Endpoints had lower values of 4 than other features, indicating that fewer respondents gave these features the greatest priority.</p>	<p>Almost every component had a mode of 5, which was in line with the median. This indicates that the majority of respondents concurred that the components—particularly those pertaining to Smart Contracts, DIDs, and Security Mechanisms—were important. Revocation Mechanisms and Service Endpoints had lower values of 4 than other features, indicating that fewer respondents gave these features the greatest priority.</p>	<p>Response variability was moderate to low, as indicated by the standard deviation values, which varied from 0.510 to 0.625. This indicates that, with only minor deviations, the majority of participants shared similar opinions regarding the significance of these elements. Higher standard deviations for elements like Protocol Bridges and Cross-Chain Communication suggest that respondents' perspectives on the importance of these interoperability aspects were more varied.</p>

4.6 DISCUSSION

This section corresponds to the results of the survey responses in relation to the seven key factors of Web3 digital identity systems: DIDs, VCs, smart contracts, user control, mechanisms of security, enhancement of privacy, and interoperability protocols. The importance of each component was analyzed using the mean, median, mode, and standard deviation of the participants' perceptions of the survey data. Specific subcategories under each of the above categories included DID controllers, public keys,

methods of authentication, and a variety of other related items. This subcategory incorporates end-users' views regarding which elements are considered important.

4.6.1 Decentralized identifiers(DIDS)

Survey responses placed a premium on the importance of DIDs to create in Web3 digital identity solutions the ability for users to manage their identity independent of any central authority, a needed advantage in Web3 environments. They also pointed out that DID Controllers are important in managing identity and, at the same time, avail access control, while methods of DIDs are important in ensuring interoperability across systems. Furthermore, it was realized that authentic authentication protocols are quite important in developing trusted and secure identities within Web3; thus, the comprehensive need for strong mechanisms in the management of identity within the decentralized digital space.

4.6.2 Verifiable credentials (VCS)

Public keys form the foundation of secure digital identity verification in most Web3 applications and a key factor in trusting relationships that come with cryptographic security. In sum, most of the respondents pointed out that the assurance of reliable and secure interaction within Web3 is afforded by public keys. Moreover, there are multiple methods of authentication, including multi-factor authentication, which nowadays has become considered indispensable by a large part of people while seeking enhanced security. The more layers of security these represent are relevant in improving identity verification processes, and thereby, it's not only making identities secure but also resilient against multiple forms of cyber threats and vulnerabilities. This robust authentication would, in turn, allow for a secure infrastructure on which to build the applications of Web3, where again, much trust and security will have to be granted.

4.6.3 Smart contracts

The survey results also show that a small number of users are somewhat dissatisfied with the efficiency of smart contracts in Web3 applications; there is a need for a more streamlined execution process that is not only faster but also more reliable due to

minimal reliance on the involvement of a large number of people. This efficiency is key to improving the performance and user satisfaction of decentralized applications. In this respect, from a security point of view, it was underlined that strong safeguards should be embedded in smart contracts; therefore, participants called for secure coding practices, regular audits, and the implementation of strong cryptographic measures to protect against vulnerabilities and preserve the integrity of transactions.

Besides interoperability between various blockchain platforms was also underlined as a core aspect of smart contract functionality. They indicated that, for smart contracts to be effective, pervasive, and have more significant impacts, they need to be interoperable across a number of blockchain systems. Interoperability will be fundamental in building a coherent and working ecosystem that enables different applications and services in the Web3 space, allowing for greater interconnectedness and access to blockchain..

4.6.4 User control

Answers to this survey underline how critical this sense of identity ownership is in Web3; thus, the principle it holds-irremovable and critical toward further improvement of sovereignty and privacy among its users-presents an underpinning precisely on decentralizing questions of identity. Thus, such models enable decentralized personal-centered governance in an important kind of what digital communications will be all about. Furthermore, data privacy and consent management received a great deal of support from participants, who would like systems to give users the ability to actively manage and consent to the use of their data, engendering greater trust and better adherence to regulations regarding the protection of privacy.

Besides that, strong access control mechanisms and auditability also came through strongly in the survey responses. They said that clear permission settings, those that are easy to maintain, decide who has permission to see what data in order not to release sensitive information. In terms of security, they had said it is important to have transparency and accountability when the action of any user needs to be traced further for any necessary action in order to prevent misuse. These cumulatively help in building

a more secure, user-centric framework in Web3 technologies wherein the ownership of digital identity and associated data remains within the full control of the users.

4.6.5 Security mechanisms

As would be confirmed by the survey responses, encryption is among the core parts of security in Web3, adding that high levels of encryption are actually needed to protect the identity data in peer-to-peer cases. This goes a long way in keeping the information free from those who should not have access within decentralized networks. They also ranked secure user authentication protocols very high, showing this approach is of great importance in user identity confirmation and providing access to only authenticated users as a means of protecting sensitive and personal data within the Web3 environments.

Besides, the requirement of intrusion detection systems in real-time was put forward, and such systems were pointed out as necessary for timely intrusion detection in Web3 infrastructures. These systems are vital to maintaining security vigilance at all times and responding to any potential threats in a timely manner. Finally, there was a general belief that decentralized security models were superior to centralized alternatives, offering higher levels of security by virtue of their inherent complexity and resistance to compromise. In summary, this represents a strong trend in leveraging security architectures that apply the intrinsic strengths of decentralization toward better overall security postures in Web3 systems.

4.6.6 Privacy enhancements

The survey results on privacy enhancements technologies show that respondents, especially blockchain developers, attach great importance to them. The survey results reveal the core position of privacy enhancement in the development of Web3. By implementing advanced privacy protection technologies, Web3 platforms can better integrate into existing systems and structures, thereby improving their scalability and practicality. In addition, the development of standardized privacy protection APIs will be a necessary step to ensure that Web3 technology can achieve efficient and secure privacy protection in different applications and services.

4.6.7 Interoperability protocols

The responses to the survey underlined interoperability as crucial in Web3 systems, which will require cross-chain communication, standardized APIs, protocol bridges, and data format standards. Cross-chain communication was singled out as especially vital for seamless operations across a variety of blockchain networks, and the willingness to support interactions between different blockchain infrastructures in order to further enhance system functionality and user experience was strongly expressed. Discussions also brought to the limelight the need for standardized APIs, which, on one hand, do support integration across diverse systems, but on the other hand, there are concerns that greater standardization is necessary to ensure compatibility and functionality across diverse platforms.

Secondly, participants unanimously agreed on the very need for protocol bridges and standard data formats. It also contains such elements that would provide the power of efficient data transfer across Web3 applications, with the ability for information to flow seamlessly and reliably among a variety of blockchain systems. This is important because it reduces friction to interoperability, allowing deeper functionality of the decentralized web for a well-rounded and strong Web3 ecosystem. These components are combined to deliver the underlying support for making a collaborative ecosystem in which different blockchain technologies interface with each other seamlessly, fostering further development and adoption of the Web3 technologies..

4.6.8 Advanced monitoring and analysis component

In the questionnaire, 8 respondents mentioned that the Advanced Monitoring and Analysis Component is very important for the web3 digital identity authentication framework. The "Advanced Monitoring and Analysis Component" (AMAC) is a critical enhancement for Web3 infrastructures, designed to bolster the operational capabilities of blockchain technologies through comprehensive monitoring and detailed analytics. This sophisticated tool facilitates real-time monitoring to swiftly detect and respond to anomalies or threats, ensuring that any potential disruptions are addressed promptly to maintain network integrity. AMAC incorporates advanced data analysis techniques, including predictive analytics and machine learning, to process large datasets generated