Decentralized Encrypted Communication: An Investigation of the Current Landscape and Future Prospect

Hexing Shao
College of Electronic and Information Engineering, Tongji University, Shanghai 201800, China

Keywords: Blockchain Technology, Encrypted Communication, Decentralization, End-to-End Encryption (E2EE), Decentralized Data Storage

Abstract: Blockchain and encrypted communication technology have emerged and have also been greatly developed, and have also greatly affected individuals' lives. Therefore, this article discusses in depth the decentralized encrypted communication program based on Blockchain technology and its related core technologies. This paper first analyzes the workflow of the decentralized encrypted communication programs, and then discusses the key technologies involved in the whole process, such as Blockchain technology, End-to-End encryption (E2EE), and decentralized data storage technology. This paper reviews the development history of these technologies and discusses their relationship with decentralized encrypted communication programs. This paper comprehensively evaluates the development status and challenges of these core technologies, and predicts the future development trend of decentralized encrypted communication programs based on the available information. The results show that the decentralized encrypted communication program effectively combines Blockchain technology, E2EE and decentralized data storage technology, and is a completely new communication method, which is profoundly affecting and changing traditional digital communication methods. It provides users with a more secure and efficient communication platform. At the same time, this emerging communication method also faces challenges such as poor scalability, low efficiency of Blockchain technology, and the threat posed by quantum computing, which is currently advancing at a rapid pace. The paper also emphasizes the importance of focusing on post-quantum cryptography (PQC) to bolster the security and reliability of these programs in an ever-evolving technological landscape.

1 INTRODUCTION

Since the beginning of the 21st century, with the rapid development of Internet technology, the level of Blockchain technology and encrypted communication technology has been greatly improved and widely used and has had an important impact on lives (Sarıtekin et al, 2018, Vilhelmson et al, 2017, Firth et al, 2019). At the same time, the combination of Blockchain technology and encrypted communication technology - decentralized encrypted communication programs based on Blockchain technology have also been developed and widely used (Sarıtekin et al, 2018).

In contrast to traditional communication programs or web pages that rely on centralized servers, decentralized applications (DAPPs) have the characteristic of running on decentralized Peer-to-Peer (P2P) networks (Ellebrink, 2022). Due to their unique mode of operation, they have the characteristics of not being controlled by a single authority, implementing decentralized storage schemes, and having strong resistance to failures (Ellebrink, 2022). The decentralized encrypted communication programs built on this basis also have the characteristics of strong anonymity, high security, and anti-censorship (Sarıtekin et al, 2018, Yu et al, 2016). This technology is considered to be a revolution of traditional digital communication technology, which is expected to affect the current communication methods of human society profoundly (Firth et al, 2019), and has the potential to change the development trend of the entire digital communication industry (Firth et al, 2019).

This study tries to start with the workflow of the decentralized encrypted communication programs and analyze the characteristics of each link in the process of program operation (Sarıtekin et al, 2018).

Shao, H.
Decentralized Encrypted Communication: An Investigation of the Current Landscape and Future Prospect.
DOI: 10.5220/0012821000004547

In *Proceedings of the 1st International Conference on Data Science and Engineering (ICDSE 2024)*, pages 275-280
ISBN: 978-989-758-690-3

In addition, the research will further analyze the key technologies in the working process, and discuss the development process of these technologies in conjunction with the decentralized encrypted communication program (Sarıtekin et al, 2018). Through comprehensive analysis of its current development status and the challenges it faces, it is expected to predict future development trends. To discuss these problems is of great significance for the popularization and further development of decentralized encrypted communication programs (Sarıtekin et al, 2018).

2 METHOD

2.1 Overview of Decentralized Encrypted Communication Programs

The most important characteristics of decentralized encrypted communication programs are decentralized mode of operation and high security (Sarıtekin et al, 2018).

The first step for every user of the program must be to create an account. After that, the program will verify the identity information with a decentralized authentication system with high confidence. If the authentication passes, the Public Key Infrastructure (PKI) function is used to generate a pair of keys for the user: a public key and a private key (Khalifa et al, 2004). This pair of keys plays a very important role in the encryption workflow: the sender first uses the receiver's public key to encrypt the information to be sent, and converts the information into ciphertext, while the receiver uses the private key to decrypt the ciphertext after receiving the ciphertext. It is worth mentioning that this type of encryption is the foundation of communication security because it ensures that only the trusted recipient can read the information correctly, which is the basic principle of encrypted communication (Khalifa et al, 2004).

After the encryption process is complete, the program will enter the ciphertext transmission process. In this process, the decentralized encrypted communication program will use end-to-end encryption (E2EE) technology to transmit ciphertext through a decentralized network such as Blockchain or Ethereum. This unique transmission method makes the entire transmission process more secure and reliable, while also reducing the risk of third parties intercepting or tampering with the information. After receiving the encrypted message, the receiver can get the original message by decrypting the ciphertext using the receiver's private key (Sarıtekin et al, 2018, Khalifa et al, 2004, Ermoshina et al, 2016).

In terms of information storage strategy, the decentralized encrypted communication program does not use the traditional local storage strategy but instead stores information and other data in a decentralized network through Blockchain data storage technology (Hao et al, 2017), which improves the security and stability of information while also improving the traceability and reliability of data.

2.2 Key Technologies

2.2.1 Blockchain Technology

The history of the recognized Blockchain can be traced back to the origin of Bitcoin. The concept of Bitcoin was proposed by Satoshi Nakamoto in 2009 (Nakamoto, 2008), the concept laid the foundation of modern Blockchain technology, opened and ushered in the era of digital currency and decentralized technology, and created a whole new field of technology and finance. The core features of Blockchain technology are distributed ledger, cryptographic security, consensus mechanism, and smart contracts. The Blockchain also verifies the transaction data carried out on the network while recording it and links these data to the blocks of the data chain through a specific algorithm, thus ensuring the immutability of the data. Encryption algorithms such as the SHA256 hash function are used to ensure data integrity and security. The introduction of consensus mechanisms, such as Proof-of-Work (PoW) or Proof-of-Stake (PoS), ensures the consistency of data between the various decentralized nodes on the network (Nakamoto, 2008, Wang et al, 2019).

As an important part of Blockchain, smart contracts realize the automatic execution of contract terms, improve the operating efficiency of Blockchain, and greatly expand the application field of Blockchain. In the Blockchain 1.0 era, it mainly focused on virtual currency transactions of Bitcoin, and then in the Blockchain 2.0 era, the smart contract technology was introduced by Ethereum, expanding the application scenario of Blockchain to finance, law, and other fields, while today's Blockchain 3.0 era is more inclined to the construction of decentralized groups. For example, decentralized autonomous organizations (DAOs) are expected to become a new type of effective

organization for dealing with uncertain, diverse, and complex environments. It can be seen that the development of Blockchain shows a trend of diversification, practicality, and popularization (Hao et al, 2017, Buterin, 2014, Wang et al, 2019).

Based on the analysis of the above technologies, the article points out that there is a close technical correlation between decentralized encrypted communication programs and Blockchain Based on Blockchain, these encrypted communication programs have a safe and reliable operating platform, ensuring the traceability and immutability of information data in the communication process (Nakamoto, 2008).

In the entire process, the decentralized encrypted communication program will also use Blockchain technology to verify the user's identity and exchange relevant information. This not only improves the efficiency of communication, but also reduces the dependence on the central server due to its decentralized structural characteristics, further reduces the potential risk of failure, and improves the stability of the entire communication network. In addition, the immutable nature of the Blockchain itself also means that the relevant information data can't be tampered with by anyone once it is recorded(Nakamoto, 2008), which provides a strong guarantee for the authenticity and traceability of digital communications. In general, the decentralized encrypted communication programs based on Blockchain technology can provide users with a more secure and efficient new communication platform, and with further development, its application range and application scope and potential are continuing to expand (Sarıtekin et al, 2018).

In general, Blockchain technology is not only the cornerstone of virtual digital currencies but also a key factor in building secure and efficient decentralized cryptographic communication programs (Nakamoto, 2008).

2.2.2 End-to-End Encryption Technology

E2EE technology plays a particularly prominent role in ensuring the communication security of decentralized encrypted communication programs. Its core principle is to ensure that only the communication parties, that is, the sender and receiver of information, can process and obtain effective information in the process of communication, and the security of information will not be affected by the unreliability of the middle node of the network. In E2EE's workflow, messages are encrypted on the sender's device and then decrypted on the receiver's device. This mechanism ensures that even if a message is intercepted during transmission by a third party, including an Internet Service Provider (ISP), communication program platform, or other entity monitoring the communication, those third parties cannot read the original message content (Ermoshina et al, 2016).

In 1991, Phil Zimmerman et al proposed Pretty Good Privacy (PGP) (Garfinkel, 1995), which is recognized as the first program on the Internet that allows users to communicate over long distances without being monitored. Since then, E2EE technology has played a vital role in email communication, becoming the common standard used for email encryption. In 2004, the advent of the Off-the-Record Messaging (OTR) protocol further improved the privacy and security of instant messaging systems (Di Raimondo et al, 2005). In contrast, PGP is mainly concerned with the encryption of email messages, and OTR is more concerned with the privacy and security of instant communications. More recently, in 2013, Open Whisper Systems developed Signal (S1SxMq, 2024), a non-federated protocol that provides E2EE for group communications, which is widely used in modern communications applications.

Taken together, E2EE technology has made significant progress and plays an important role in protecting the privacy and security of email communications and instant digital communications. In decentralized encrypted communication programs, these technologies further reinforce their critical role in protecting communication data security and user privacy.

But with the rapid development of quantum computing technology, E2EE faces new challenges now. Traditional encryption methods, such as the RSA algorithm, will be vulnerable to quantum computing attacks in the future. According to relevant predictions, quantum computers are expected to crack the RSA algorithm by 2030 or earlier. Because of this situation, the global information security community is accelerating the research and application promotion of Post-Quantum Cryptography (PQC) to cope with the great challenges to traditional encryption methods in the post-quantum era (Bernstein & Lange, 2017). These outreach efforts are essential to maintaining the stability and security of decentralized encrypted communication programs and to protect against

possible new threats arising from further technological developments in the future.

2.2.3 Decentralized Data Storage Technology

Decentralized data storage technology is a revolutionary data storage method developed based on Blockchain technology, which subverts the traditional centralized storage and data processing system. Its core features include decentralization, redundant storage, collective maintenance, and tamper-proof, making it possible to implement decentralized applications. Bitcoin and Blockchain technology, as the earliest practitioners of decentralized data processing, have profoundly affected the pattern of traditional centralized storage.

In terms of a decentralized storage model, Hao Kun et al proposed a decentralized distributed metadata storage model (DMB). The model first ensures the integrity of metadata by storing it in blocks and further redundantly on the Blockchain. The DMB model solves the security and efficiency problems of traditional centralized metadata storage (Ermoshina et al, 2016).

As of June 2023, the total storage capacity of decentralized storage has exceeded 22,000 PB, but the overall network utilization is only about 20% (PANews, 2024). This shows that there is even greater potential for growth in the future. In the existing decentralized storage market, Filecoin controls approximately more than 80% of the storage capacity, which allows it to dominate the overall market. At the same time, it also introduced projects such as Filecoin Plus and FVM to motivate developers to participate and promote the healthy development of the entire decentralized storage ecosystem (PANews, 2024).

The development of these decentralized storage technologies has a profound impact on decentralized encrypted communication programs, providing them with secure, decentralized, and efficient storage solutions, and greatly promoting the development and promotion of decentralized technology.

3 DISCUSSION

3.1 Current Application Progress

The development and application of decentralized encrypted communication programs mark a critical advance in the field of digital communications and information security. The organic integration of Blockchain technology, E2EE, and decentralized data storage technology has completely changed the traditional sense of digital communication mode. The immutable ledger technology of Blockchain, combined with the security provided by public key infrastructure, heralds a new era of trust and security in digital interactions. E2EE, on the other hand, ensures that only the designated recipient can decrypt and understand the information, thus achieving the purpose of privacy and confidentiality protection in the contemporary Internet digital environment (Firth et al, 2019, Ermoshina et al, 2016).

The development of Blockchain technology from the very beginning of virtual currency transactions (such as Bitcoin) to the realization of complex smart contract functions and the formation of DAOs highlights the diversity of its functions and great development potential (Wang et al, 2019). In the development of decentralized encrypted communication programs, the application of Blockchain provides a stable basic framework for the secure exchange of information with tamper-proof characteristics.

In addition, the rapid development of platforms like Filecoin demonstrates the potential of decentralized data storage technology to create more secure, efficient, and scalable storage solutions (PANews, 2024). The application of these technologies in the decentralized encrypted communication programs can not only enhance the security of data but also improve the processing speed and transmission efficiency of data.

3.2 Limitations and Challenges

Overall, although decentralized encryption programs have made great progress and wide application, there are still some problems and challenges. One of the most important problems is the contradiction between the shortcomings of Blockchain technology in terms of scalability and operational efficiency and the contemporary requirements for high scalability and high operational efficiency. Due to the limitations of its nature, its working speed is relatively slow, and the Blockchain needs to consume a lot of energy during the working process, so these reasons cause objective difficulties for the further promotion of the program (Yuan & Wang, 2016). In addition, the integration of Blockchain technology and E2EE technology into the communication program requires a high level of expertise, which will likely hinder the further

adoption of decentralized encrypted communication programs in the general user population.

Another major challenge is the emergence and rapid development of quantum computing. Compared with traditional cracking methods, quantum computers are hoped to crack traditional encryption schemes more effectively, such as RSA and ECC algorithms, which will pose a serious threat to the existing encryption communication security standards. Because of this imminent technological threat, current researchers must accelerate the research and application of PQC to effectively cope with possible future cryptography breakthroughs (Bernstein & Lange, 2017).

In addition, due to the decentralized nature of these platforms themselves, it is possible to trigger undesirable events such as abuse of anonymity by users or illegal activities through virtual name communication. Therefore, there is an urgent need to address the issue of privacy, security, and the balance between laws and regulations in the current field.

3.3 Future Prospects

It is found that the development prospect of decentralized encrypted communication programs is very broad. Based on further development and improvement of Blockchain technology, especially breakthroughs in terms of scalability and efficiency, there is hope to break through the current limitations and gain a larger scale of popularity. At the same time, the introduction of Ethereum 2.0 technology will enable the entire system to transition from the traditional PoW model to the PoS model, thus further transforming it into an environmentally friendly Blockchain solution (Yuan & Wang, 2016, Anwar et al, 2020).

Further developments in PQC are expected to provide strong defenses for decentralized encrypted communication programs against quantum computing threats (Bernstein & Lange, 2017). The development and application of decentralized storage technology indicates that it has great potential to build a decentralized data ecosystem, which will provide the development foundation for next-generation Internet applications such as decentralized finance (DeFi) and Web 3.0 (Zetzsche et al, 2020).

Overall, although the current decentralized encrypted communication programs have made breakthroughs, they still face huge challenges. Further refining the complex balance between privacy, security, and efficiency will be the focus of future development (Yuan & Wang, 2016). In the future, the further development of Blockchain technology, E2EE technology, and decentralized storage technology will provide power for the development of a more secure, efficient, and privacy-conscious digital communication environment.

4 CONCLUSION

This study delves into the technical details, application scenarios, and future development prospects of decentralized encrypted communication programs, and discusses the role of E2EE technology, decentralized data storage technology, and Blockchain technology in improving the security and privacy of decentralized encrypted communication programs. The results show that the above key technologies play an important role in ensuring the security of decentralized encrypted communication programs, especially thanks to the use of E2EE and decentralized storage technology, secure and efficient data storage solutions have been established.

However, the study does have some limitations. It lacks a detailed discussion of how to solve the scalability and efficiency problems of Blockchain technology, does not in-depth analysis of the challenges caused by quantum computing to current encryption methods, and does not in-depth analysis of the practical application and impact of PQC in the field of contemporary cryptography and future development potential. Future research should complement and improve these parts in time to further discuss solutions to the scalability, efficiency, and sustainable development problems of Blockchain technology.

REFERENCES

R. A. Sarıtekin, et al. Blockchain based secure communication application proposal: Cryptouch. 2018 6th International Symposium on Digital Forensic and Security (ISDFS). IEEE (2018)

B. Vilhelmson, E. Thulin, E. Elldér. Where does time spent on the Internet come from? Tracing the influence of information and communications technology use on daily activities. Information, Communication & Society, 20.2 250-263 (2017)

J. Firth, et al. The “online brain”: how the Internet may be changing our cognition." World Psychiatry, 18.2 119-129 (2019)

G. Ellebrink. An Open and Nonproprietary Decentralized Messaging Protocol: Operating Entirely on the Internet Computer Blockchain. (2022)
H. Yu, E. Lee, S.-B. Lee. SymBiosis: Anti-censorship and anonymous Web-browsing ecosystem. IEEE Access, 4 3547-3556 (2016)
O. O. Khalifa, et al. Communications cryptography. 2004 RF and Microwave Conference. IEEE (2004)
K. Ermoshina, F. Musiani, H. Halpin. End-to-end encrypted messaging protocols: An overview. Internet Science: Third International Conference, INSCI 2016, Florence, Italy, September 12-14, 2016, Proceedings 3. Springer International Publishing, (2016)
K. Hao, et al. Decentralized distributed storage model. (in Chinese), Computer Engineering and Applications, 53.24 1-7 (2017)
S. Nakamoto. Bitcoin: A peer-to-peer electronic cash system. Decentralized Business Review, (2008)
V. Buterin. A next-generation smart contract and decentralized application platform. White Paper, 3.37 2-1 (2014).
S. Wang, et al. Decentralized autonomous organizations: Concept, model, and applications. IEEE Transactions on Computational Social Systems, 6.5 870-878 (2019).
S. Garfinkel. PGP: Pretty Good Privacy. O'Reilly Media, Inc., (1995)
M. Di Raimondo, R. Gennaro, H. Krawczyk. Secure off-the-record messaging. Proceedings of the 2005 ACM Workshop on Privacy in the Electronic Society (2005)
S1SxMq, ZhiHu user. Signal: Secure chat software. January 16, 2023. Retrieved on January 15 Retrieved from: https://zhuanlan.zhihu.com/p/344792749#Signal%E7%9A%84%E5%8E%86%E5%8F%B2 (2024)
To the top bar. Fujitsu's research estimates that quantum computers could crack RSA by 2030. January 28, Retrieved on January 15, 2024. Retrieved from: https://www.thepaper.cn/newsDetail_forward_21697128 (2023)
D. J. Bernstein, T. Lange. Post-quantum cryptography. Nature, 549.7671 188-194 (2017)
PANews. The Data Revolution: The full picture of decentralized storage. August 4, 2023. Retrieved on https://new.qq.com/rain/a/20230804A04CA000 (2024)
Y. Yuan, F. Wang. The current status and prospects of Blockchain technology. (in Chinese), Acta Automatica Sinica, 42.4 481-494 (2016)
S. Anwar, et al. Generation Analysis of Blockchain Technology: Bitcoin and Ethereum. International Journal of Information Engineering & Electronic Business, 12.4 (2020)
D. A. Zetzsche, D. W. Arner, R. P. Buckley. Decentralized finance (defi). Journal of Financial Regulation, 6 172-203 (2020)