Research on Elliptic Curve Cryptography in Blockchain of Efficiency and Security

Xiangqi Ruan[a]
Software Engineering in Maynooth College, Fuzhou University, Fuzhou, China

Keywords: Elliptic Curve Cryptography; Blockchain; Bitcoin.

Abstract: This study explores the application and future potential of Elliptic Curve Cryptography (ECC) in blockchain technology, with a particular focus on Bitcoin. As a key cryptographic algorithm in blockchain, ECC is valued for its high efficiency and small key size, significantly reducing computational and storage demands while maintaining robust security. The research delves into the mathematical foundations of ECC and compares it with other cryptographic algorithms, such as Rivest-Shamir-Adleman (RSA). The role of ECC in blockchain systems is thoroughly examined, highlighting its principles and applications in securing cryptocurrencies like Bitcoin. Through performance analysis, ECC is shown to excel in terms of speed, resource efficiency, and security. The results demonstrate that ECC not only conserves bandwidth and computational resources but also provides strong protection against attacks. Despite its complexity and limited current adoption, this study emphasizes the security advantages of ECC, offering a strong case for its broader application in blockchain systems. The findings provide valuable insights for future cryptographic research, supporting the role of ECC in enhancing blockchain security.

1 INTRODUCTION

Blockchain, a distributed ledger technology, was first widely known and used in the field of digital cryptocurrencies. Due to its decentralization, lack of reliance on trust mechanisms, and high security, the technology is increasingly favored and applied by several fields, including finance, supply chain management, and the Internet of Things (Gamage et.al, 2020). At the same time, blockchain security is also directly related to its credibility and application prospects. Blockchain uses more complex asymmetric encryption algorithms for higher security and confidentiality. Blockchain has a pair of secret keys, i.e., public and private keys, which are used to encrypt and decrypt each other to prevent information from being tampered with and forged. Rivest-Shamir-Adleman (RSA) and elliptic Curve Cryptography Algorithm (ECC) are commonly used algorithms. ECC is one of the most robust and efficient encryption technologies in blockchain due to its ability to use more minor keys than traditional algorithms while maintaining high security. It has a faster response time, can reduce computation and storage requirements without sacrificing security, and is used as the encryption algorithm for the virtual currency Bitcoin. Consequently, advancing the advancement and use of blockchain technology requires a thorough examination of the security and ECC implementation in blockchain.

Neal Koblitz and Victor S. Miller's 1985 proposal to combine elliptic curves with encryption established ECC as the cornerstone (Koblitz, 1987). Cryptographers have validated that Shorter keys can be used with the same level of security because of ECC's practicality and attack resistance.

This lowers the requirement for computational resources while also increasing efficiency. The United States' National Institute of Standards and Technology (NIST) released the first ECC standard, FIPS 186-2, in 1998, which marked the beginning of the practical application. ECC was incorporated into many cryptographic protocols and standards, such as Secure Sockets Layer/Transport Layer Security (SSL/TLS), IPsec, and wireless communication standards. In 2009, Satoshi Nakamoto, the creator of Bitcoin, chose ECC as a core part of the Bitcoin encryption mechanism. Bitcoin uses Secp256k1

[a] https://orcid.org/0009-0009-1222-6385

Ruan and X.
Research on Elliptic Curve Cryptography in Blockchain of Efficiency and Security.
DOI: 10.5220/0013524200004619
In *Proceedings of the 2nd International Conference on Data Analysis and Machine Learning (DAML 2024)*, pages 369-373
ISBN: 978-989-758-754-2

elliptic curves, a real-world example of a large-scale application of ECC, primarily for generating addresses, digital signatures, and exchanging keys. ECC is a viable solution for applications like Bitcoin that demand great data storage and transmission efficiency, as seen by its implementation in cryptocurrency (Joppe et.al, 2014). The main objective of this study is to comprehensively explore the development history of ECC, its core technology, and its application prospects. This paper first reviews the history of ECC's development. The next part of this paper is arranged as follows: Section II introduces ECC and other related concepts. Section III Compare and analyze the advantages and disadvantages of ECC in practical applications. Finally, Section IV concludes.

2 METHODOLOGY

This study offers a comprehensive examination of the development, core technologies, and prospects of ECC. It begins with an overview of the historical trajectory of ECC, detailing its fundamental concepts, the mathematical principles underlying its operation, and the theoretical foundation for ensuring information security. The study delves into technical components, exploring related fields such as cryptography, Bitcoin, blockchain, and the core algorithms that enable its functionality. These sections provide thorough explanations of how ECC works, including its implementation methods. The paper also demonstrates practical applications, such as digital signatures, key exchanges, and data encryption, using real-world examples to analyze its performance and security in actual use cases. Additionally, an evaluation of performance across various practical scenarios highlights its strengths, limitations, and the challenges it faces in implementation. Solutions to these challenges are discussed in detail. The paper concludes with a summary of the findings and presents recommendations for future research directions, offering a well-rounded, multi-faceted insight into the current state and future potential of ECC. The structure of the study is illustrated in Figure 1.

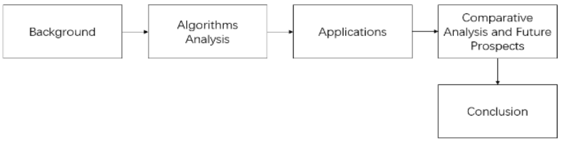

Figure 1: The pipeline of the study (Picture credit: Original).

2.1 ECC and Cryptographic Algorithms

Depending on whether the keys are the same, cryptographic systems can be classified as symmetric or asymmetric (Kumar et.al, 2020). When an encryption technique uses symmetric encryption, only one key is needed for the sender and the recipient to encrypt and decode the data. When using a symmetric encryption algorithm, the data sender encrypts the original data, or plaintext, using the encryption key and runs it through a specific encryption algorithm to create a complicated encrypted ciphertext. Its defining features are small computation, quick encryption, outstanding operability, and efficiency; nonetheless, it necessitates prior key sharing, which is easily compromised.

Also referred to as a dual-key or public-key cryptosystem is asymmetric encryption. There is a difference between its encryption and decryption keys; the former is the public key and may be used by anybody, while the latter is the private key and can only be obtained by the decryptor. Decrypting the communication without the private key is impossible, even if the public key is compromised. The strength of an asymmetric encryption algorithm determines its security; a complicated algorithm can safeguard information security more effectively than a symmetric method by enhancing both encryption and decryption speed and efficiency (Chandra et.al, 2014).

The asymmetric encryption method known as ECC is based on the algebraic structure of elliptic curves over a finite field and the complexity of the Elliptic Curve Discrete Logarithm Problem (ECDLP). Key exchange, signatures, and encryption are the three primary operations of an asymmetric cryptosystem that ECC implements. In an ECC system, key generation begins with selecting and setting an appropriate elliptic curve and associated parameters. Subsequently, a fixed-point G (the generating element) is selected as the base point, whose order (i.e., the smallest positive integer n such that n times the point G is equal to the point at infinity) should be a large prime number. The user later picks a random number k less than n as the private key. The public key Q is then obtained by multiplying the private key k with the base point G, i.e., $Q = kG$. During encryption using ECC, if the plaintext is M, the sender chooses a random number r and computes two points: $r = rG$ and $S = rP + M$, where P stands for the receiver's public key and the ‘+’ denotes the addition on an elliptic curve. The generated ciphertext is the point pair (R, S). After receiving the ciphertext, the receiver uses his private key k to compute $T = kR$ and obtains the original plaintext M by $S - T$. In this way, the receiver can decrypt the message encrypted by the public key using his private key (Jao, 2010).

2.2 Bitcoin and Blockchain

The blockchain application scenario that has been the most successful to date is Bitcoin. Peer-to-peer (P2P) networks, used by Bitcoin nodes for communication, enable direct payment between the two parties to a transaction. By eliminating third-party intermediaries like commercial banks, the traditional payment paradigm is eliminated, resulting in a completely new monetary system. Bitcoin employs a probability-based distributed consensus protocol to enable nodes to reach a consensus. Irreversible cryptographic hashing on the user's public key generates the receiving address, also known as the Bitcoin address.

Users can create multiple public keys linked to one or more wallets, allowing them to have many addresses in the Bitcoin system. Spending the bitcoins that an owner has requires the usage of their private keys; these are digitally signed transactions (Conti et.al, 2018). In the Bitcoin network, resource-rich nodes called ‘miners’ process and validate transactions using the SHA256 algorithm to ensure their integrity and correctness. When the "root" is located, the miner continues to compute until it does. The subsequent block is then added to the blockchain overall, containing the transaction tree and hash value from the preceding block packed into its header. The block is processed and then posted on the network for mining rewards (Conti et.al, 2018) (Yang and Ming, 2014).

Blockchain is a distributed ledger system that allows data decentralization and security by storing data across multiple nodes. Every node has a copy of the entire ledger, thus even in the event of a node failure, the others can continue to operate. Furthermore, data cannot be modified once stored on the blockchain, making it unchangeable and traceable. Blockchain technology was initially applied to cryptocurrencies such as Bitcoin, but its continuous development has been widely used in finance, IoT, and other fields. Blockchain‘s emergence solves two significant problems of digital currencies: the problem of double payments and the problem of Byzantine generals. Blockchain uses Proof of Work (PoW) and Proof of Stake (PoS) or other consensus mechanisms, coupled with cryptography, to turn an untrustworthy network into a trustworthy one. All participants can agree on something without trusting a single node. The blockchain infrastructure is shown in Figure 2, where the dotted lines indicate the differences between Ether and Bitcoin.

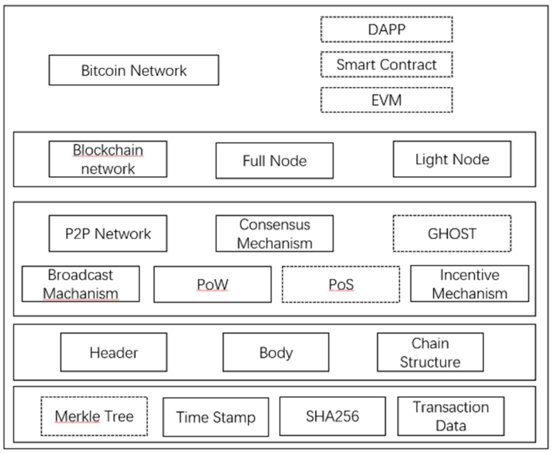

Figure 2: Blockchain Infrastructure (Shen et.al, 2016)

3 RESULT AND DISCUSSION

Asymmetric encryption techniques safeguard information by encrypting it at the transmitting end and decrypting it at the receiving end. They include RSA, Digital Signature Algorithm (DSA), ECC, Diffie-Hellman, ElGamal, and XTR algorithms. The first of these, RSA, can be used for digital signatures and encryption. It is used in various applications, including e-commerce transactions, software licensing, and secure communication protocols (e.g., SSL/TLS). The core security foundation of the RSA algorithm relies on the prime factorization of large integers. When a sufficiently long key (e.g., 2048 bits or longer) is used, it is virtually impossible for existing computing power to break RSA encryption in real time, thus ensuring information security. With advances and improvements in extensive integer decomposition methods, increased computer speeds, and the development of computer networks, RSA keys need to be constantly improved to secure data. Nevertheless, the pace of encryption and decryption is significantly slowed down with an increase in key length. Therefore, a new algorithm is needed to replace RSA.

ECC is a discrete logarithmic problem in the group of points on an elliptic curve over a finite field ECDLP. The most essential advantages of ECC are the following advantages. First, ECC provides more flexibility and uses a smaller key size for the same level of security (ChavhanAssist, 2020) (Amara and Siad, 2011) (Xiao et.al, 2021). As the security level rises, the key lengths of existing encryption techniques increase exponentially, while ECC key lengths only increase linearly. For instance, a 3,072-bit RSA key is needed for 128-bit secure encryption, whereas just a 256-bit ECC key is needed. Second, exponentiation and prime numbers are not needed for ECC. Since ECC is based on elliptic curve theory, it does not require the generation of large prime numbers or exponential operations for its algorithmic implementation, which primarily consists of adding and multiplying points defined on elliptic curves. In contrast, the RSA algorithm depends on these mathematical operations (Yang and Ming, 2014).

In this way, ECC bypasses the complex process of dealing with mathematical problems, thus simplifying the computational process of encryption and decryption. Finally, ECC provides significant bandwidth savings. ECC's encryption function is particularly efficient when processing short messages and can significantly reduce the required bandwidth. This is particularly valuable in application scenarios where network communication is frequent (Ghosh et.al, 2020). However, ECC has some drawbacks; ECC is based on complex mathematical principles involving the addition and multiplication of elliptic curve points over a finite field. This complexity makes it more challenging to implement ECC correctly and securely than it is to implement RSA based on the multiplication of large integers. Incorrect implementations can lead to serious security vulnerabilities, such as side-channel attacks or incorrect random number generation, among other problems. RSA has a long history of application and a relatively easy-to-understand mathematical foundation; therefore, it is more accepted and trusted than ECC. At the same time, although ECC provides a higher secure unit key length than RSA, it is still theoretically under threat from future quantum computing.

4 CONCLUSIONS

This study explored the role of ECC in cryptography and blockchain technology, focusing on its development, core technologies, and prospects, particularly in blockchain systems such as Bitcoin. Through a detailed analysis of blockchain security mechanisms, the study examined applications in digital signatures, key exchanges, and data encryption within blockchain environments. The smaller key sizes and improved efficiency make it a strong alternative to traditional algorithms like RSA. The research evaluated mathematical foundations and their practical implementation in blockchain use cases, comparing their performance to other cryptographic methods. The findings indicate that ECC delivers superior security and efficiency compared to RSA and other schemes, particularly due to its lower computational overhead. Nevertheless, the study also recognized several obstacles linked to ECC, such as implementation difficulties and possible weaknesses in quantum computing. Future research will focus on enhancing resilience to quantum computing threats. This will involve improving security measures and exploring alternative cryptographic techniques to address its limitations. Additionally, ECC's integration into broader applications, such as the Internet of Things (IoT), and its further development within blockchain technologies will be key areas of exploration.

REFERENCES

Amara, M., & Siad, A. 2011. Elliptic Curve Cryptography and its applications. In International Workshop on Systems, Signal Processing and their Applications, 247-250.

Chandra, S., Paira, S., Alam, S.S., et al. 2014. A comparative survey of symmetric and asymmetric key cryptography. International conference on electronics, communication and computational engineering, 83-93.

ChavhanAssist, S.J., 2020. On study of some asymmetric key cryptography algorithms. International Journal of Advance Research and Innovative Ideas in Education, 6(2), 671-676.

Conti, M., et al. 2018. A Survey on Security and Privacy Issues of Bitcoin. IEEE Communications Surveys and Tutorials, 20(4), 3416-3452.

Gamage, H.T.M., et al. 2020. A Survey on Blockchain Technology Concepts, Applications, and Issues. SN Computer Science, 1(2), 114.

Ghosh, A., et al. 2020. Security of Cryptocurrencies in blockchain technology: State-of-art, challenges, and future prospects. Journal of Network and Computer Applications, 163.

Jao, D., 2010. Elliptic curve cryptography. Handbook of information and communication security, 35-57.

Joppe, W., Bos, et al. 2014. Elliptic Curve Cryptography in Practice. Lecture Notes in Computer Science, 8437, 157-175.

Koblitz, N., 1987. Elliptic curve cryptosystems. Mathematics of Computation, 48 (1987), 203-209.

Kumar, S., et al. 2020. A survey on Symmetric and Asymmetric Key based Image Encryption. IEEE International Conference on Data Engineering, 1-5.

Shen, X., et al. 2016. Survey of block chain. Journal of Network and Information Security, 2(11), 11-20.

Xiao, S., et al. 2021. New digital signature algorithm based on ECC and its application in bitcoin and IoT. High Perform, 10(1), 20-31.

Yang, X.C., and Ming, Z., 2014. Bitcoin: Operational Principles, Typical Features, and Future Outlook. Chinese Review of Financial Studies, 38-53.