International Journal on Semantic Web and Information Systems
Volume 19 • Issue 1

Fabric Blockchain Design Based on Improved SM2 Algorithm

Jinhua Fu, Zhengzhou University of Light Industry, China*
Wenhui Zhou, Zhengzhou University of Light Industry, China
Suzhi Zhang, Zhengzhou University of Light Industry, China

ABSTRACT

As one of the most widely used federated chains, hyperledger fabric uses many cryptographic algorithms to ensure the security of information on the chain, but the ECDSA cryptographic algorithm used in the fabric system has backdoor security risks. In this paper, the authors adopt SM2 algorithm to replace the corresponding ECDSA algorithm for blockchain design based on fabric platform. Firstly, they optimize the part of SM2 signature algorithm process with inverse operation and effectively reduce the time complexity by reducing the inverse operation in the whole process, and the experimental results show that the improved SM2 algorithm improves the signature and verification efficiency by about 5.7%. Secondly, by adding SM2 algorithm template and interface to the BCCSP module of fabric platform to realize the shift value of SM2 algorithm and compare the performance with the native fabric system, the network startup time is reduced by about 29%. The experimental results show the effectiveness of the improved SM2 algorithm, and also the performance of the optimized fabric system is improved.

KEYWORDS

Blockchain, Cryptography, Digital Signature, Hyperledger Fabric, SM2

INTRODUCTION

Blockchain, a new type of distributed database (You, 2022) in essence, integrates a series of emerging information technologies including consensus mechanism, encryption algorithm, network communication, distributed architecture, and smart contract. All these technologies also contribute to the characteristics of blockchain, such as decentralization, openness, transparency, traceability and non-tampering. Its emergence has brought new solutions to the trust problems, privacy problems and data differences (George, 2022) in the process of multi-party cooperation. It is a huge boost to the establishment and strengthening of the integrity system of the whole Internet, and even to the strengthening of the integrity system in the real world. Blockchain can realize reliable trust transmission at low cost; therefore, it can definitely serve as the cornerstone of trust in the Internet of value and trust of the next generation.

DOI: 10.4018/IJSWIS.322403 *Corresponding Author

At present, blockchain technology has penetrated into the development of all walks of life, and it has made continuous innovations and breakthroughs. Meanwhile, the problems of Internet and information security caused by its development should be taken into consideration (Avkurova et al., 2022). Individuals, enterprises, and countries cannot ignore network and information security, especially in the current international environment that is becoming increasingly complicated, challenging, and uncertain.

In blockchain technology, a large number of cryptographic algorithms are used (Guo & Yu, 2022; Jose & Prakash, 2014), such as the Hash algorithm (Kuznetsov et al., 2021), digital signature technology, symmetric encryption algorithm, and the asymmetric encryption algorithm. Different types of encryption algorithms are all crucial in different modules, and they jointly ensure the security of data in blockchain. However, many cryptographic algorithms used worldwide now have been cracked and attacked frequently, for there are backdoor security risks and a large number of uncontrollable factors. Therefore, research on how to solve the security risks of cryptographic algorithms in blockchain application has become critical to determine whether blockchain technology can be widely used in all walks of life or not.

To keep encryption and decryption algorithms independent and controllable, China's State Cryptography Administration has released a series of more efficient and secure commercial cryptographic algorithms since 2010, such as SM2, SM3, SM4, SM9, and so on. After 2020, a range of national standards related to cryptography were promulgated, such as the Cryptography Law of the People's Republic of China, which effectively standardized and promoted the application of national commercial cryptographic algorithms in every field.

The alliance chain (Li et al., 2021) has different forms and structures from public chains, such as BTC and ETH, and it achieves a balanced state between decentralization and centralization, both of which make the alliance chain the main form of blockchain that attracts wide attention from people. Hyperledger Fabric (Androulaki et al., 2018) is one of the most popular alliance chains at present, and its security mechanism is particularly important. The encryption and decryption algorithms involved in it are all international algorithms, such as Elliptic Curve Digital Signature Algorithm (ECDSA), AES, SHA-256, and so on (Cao et al., 2022).

Among some special application scenarios, the transaction rate may be limited owing to the high computational complexity of the SM2 algorithm. Song et al. (2019) designed an improved proxy signature scheme based on the existing SM2 proxy signature scheme. By improving the generation of authorization information, the scheme can still satisfy identifiability and nonrepudiation without the need of certificate generation by trusted parties, and at the same time, it can prevent malicious proxy signers from forging authorization information and proxy signatures. The improved scheme improves the verification efficiency by about 26% over the existing SM2 proxy signature scheme. Li et al. (2022) proposed a reconfigurable optimization method of the prime domain SM2 algorithm for the problems of low software efficiency, low resource use of hardware implementation, and poor scalability of the SM2 algorithm. The analysis of experimental results shows that the optimized SM2 makes full use of the field-programmable gate array (FPGA) resources, shortens the dot product cycle, and improves the computational performance and scalability by up to 352.48 times more computations per second than the CPU (Intel i5-8300).

In this paper, we describe how to use the SM2 algorithm (Wang & Zhang, 2016) to improve the original security mechanism of Fabric. At the same time, in special application scenes, the transaction rate may be limited to some extent owing to the high computational complexity of SM2 algorithm. Therefore, in this paper, based on the description of the principle of the SM2 algorithm, we explain how we optimized the algorithm (Xue et al., 2022) and designed and improved the blockchain of SM2 algorithm based on Fabric platform, thus increasing the efficiency of blockchain to some extent.

SM2 ALGORITHM OPTIMIZATION

SM2 Signature Algorithm

The design of the SM2 algorithm is derived from the elliptic curve cryptography algorithm (ECC), a public key cryptography algorithm designed by the National Cryptography Administration. The

core part of the SM2 cryptographic algorithm includes the SM2-1 digital signature algorithm, the SM2-2 key exchange protocol, and the SM2-3 public key encryption algorithm. In the SM2-1 digital signature algorithm process, if we assume that the data information to be signed is M, the signature user A needs to perform the following steps to obtain the signature of M (r, s):

A1: Let $\bar{M} = Z_A \,||\, M$, where Z_A is a hash value obtained by hashing together with SM2 elliptic curve parameters and user identity information.

A2: Calculate $e = H_v\left(\bar{M}\right)$ and convert e data type into integer.

A3: Randomly generate a scalar $k \in \left[1, n-1\right]$ and calculate the elliptic curve point $\left(x_1, y_1\right) = \left[k\right]G$, convert x_1 to integer.

A4: Calculate $r = \left(e + x_1\right) \bmod n$, if $r = 0$ or $r + k = n$ and then return to step A3.

A5: Calculate $s = \left(\left(1 + d_A\right)^{-1} \cdot \left(k - r \cdot d_A\right)\right) \bmod n$, if $s = 0$ and then return to step A3.

A6: Verify the signature of the output message M: $\left(r, s\right)$.

To verify the received information M' and the signature $\left(r', s'\right)$ from the signer, perform the following validation steps:

B1: Verify whether $r' \in \left[1, n-1\right]$ and $s' \in \left[1, n-1\right]$ are verified; if not, the verification failed.

B2: Set $\overline{M'} = Z_A \,||\, M'$.

B3: Calculate $e' = H_v\left(\overline{M'}\right)$ and convert the data type of e' into integer.

B4: Calculate $t = \left(r' + s'\right) \bmod n$; if $t = 0$, then the verification is not passed, where the data types of r' and s' are converted into integers.

B5: Calculate the elliptic curve points $\left(x_1^{'}, y_1^{'}\right) = \left[s'\right]G + \left[t\right]P_A$ and $R = \left(e' + x_1^{'}\right) \bmod n$ to verify whether $R = r'$ is validated. If it is validated, the signature is accepted; otherwise, the signature is refused, and the data type of $x_1^{'}$ is converted into an integer.

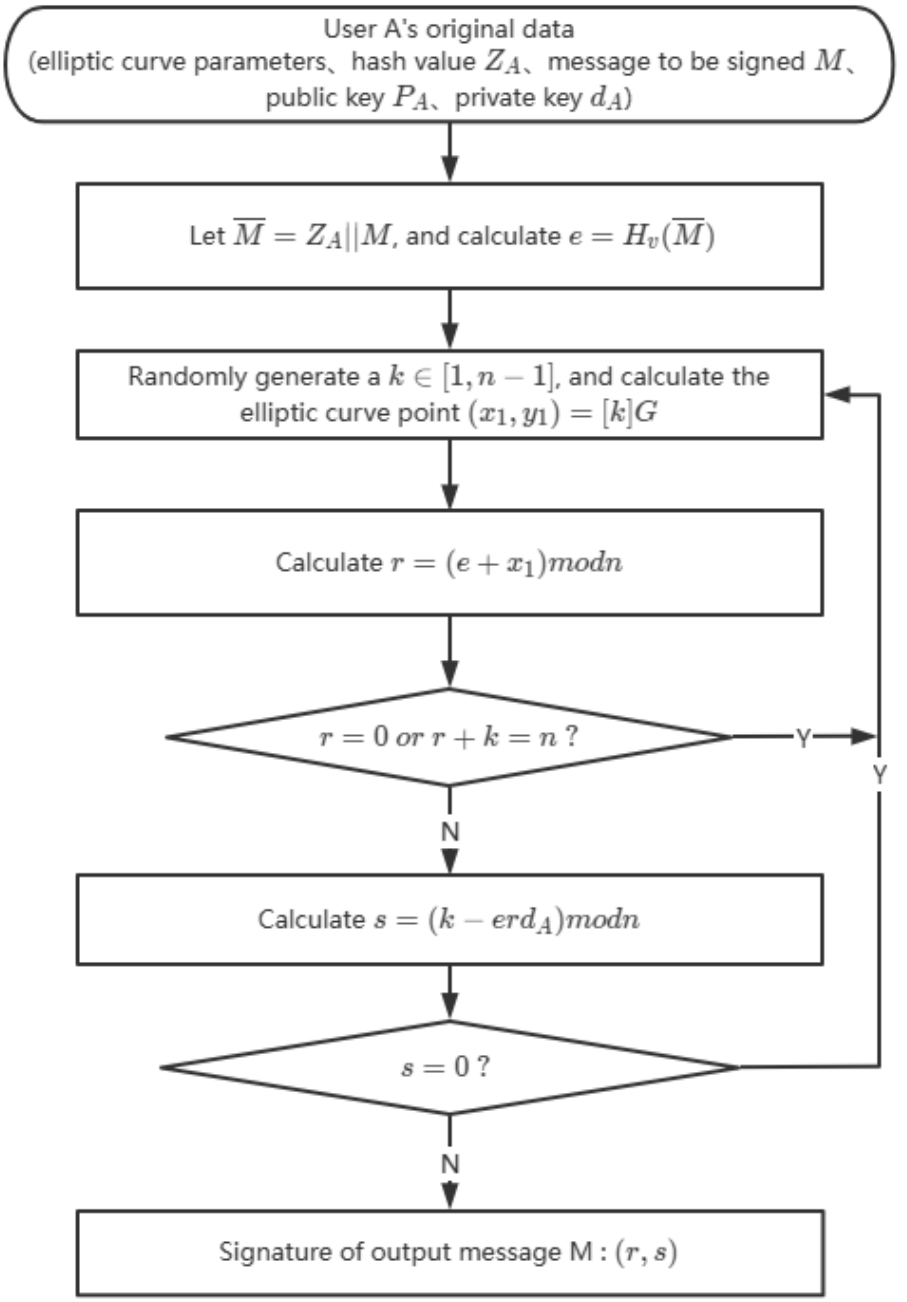
Improved SM2 Algorithm

The traditional SM2 signature scheme involves more time-consuming modular inversion operation, which makes the signature process more complex, thus increasing the time to complete the signature process. Therefore, the improved scheme is mainly aimed at optimizing the inversion operation in the SM2 signature algorithm process, reducing the inversion operation in the whole process to effectively reduce the time complexity.

The optimization scheme for the SM2 signature algorithm is composed of two parts. First, in the digital signature generation stage, the A5 step of the original SM2 signature algorithm is improved. The step improved is A5: Calculate $s = \left(k - erd_A\right) \bmod n$, and if $s = 0$, it returns to step A3; its steps are consistent with the original SM2 signature algorithm and do not change. The signature process is shown in Figure 1.

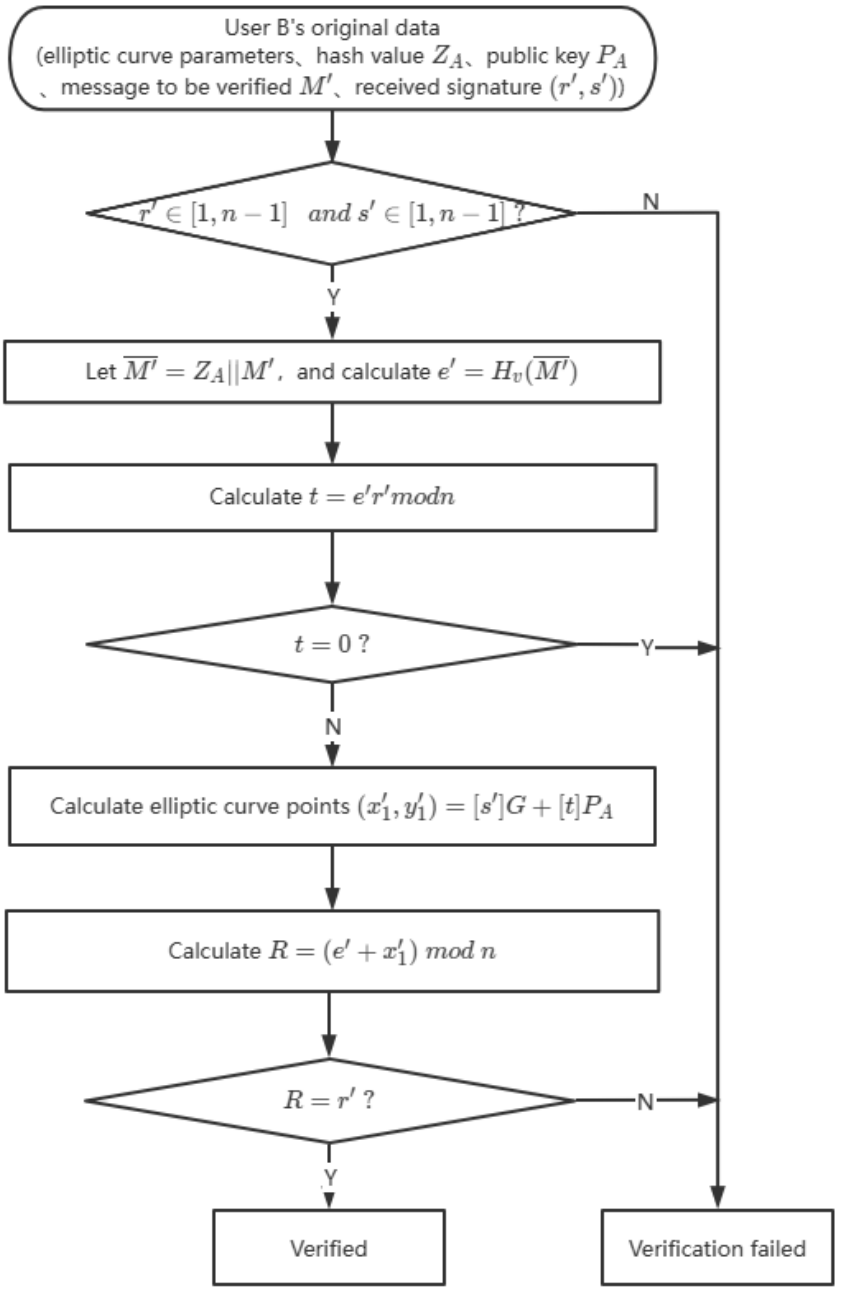
Second, in the digital signature verification stage, the B4 step of the original SM2 signature algorithm is improved. The step improved is B4: Calculate $t = e'r^{'} \bmod n$, and if $t = 0$, the verification fails, where the data types of r' and s' are converted into integers. The improved SM2 signature verification flow chart is shown in Figure 2.

Figure 1.
Improved SM2 signature process



The improved algorithm in this paper is slightly improved on the SM2 algorithm, so the signature is also realized by the discrete logarithm problem (Ezziri & Khadir, 2021) of elliptic curve. The correctness of the scheme depends on whether the signature verifier can successfully verify the information to be verified after the signature message is signed by the signer. The principle of the improved scheme is shown in Equation 1:

Figure 2.
Improved SM2 signature verification process



$$\left(x_1^{'}, y_1^{'}\right)$$
$$= \left[s'\right]G + \left[t\right]P_A$$
$$= \left[s'\right]G + \left[e'r^{'}\right]P_A$$

$$= \left[k - e'r'd_A\right]G + \left[e'r'\right]P_A$$
$$= \left[k - e'r'd_A\right]G + \left[e'r'\right]\left[d_A\right]G$$
$$= \left[k\right]G$$

$$= \left(x_1, y_1\right) \tag{1}$$

Finally, $R = \left(e' + x_1'\right) \bmod n$, $r = \left(e + x_1\right) \bmod n$, e' and e are equal, x_1' is equal to x_1, so in general, the signature verification is successful.

IMPROVED SM2 ALGORITHM DESIGN BASED ON FABRIC

Hyperledger Fabric provides signature verification, encryption, and decryption functions through its encryption component BCCSP (Blockchain Cryptographic Service Provide). With this encryption component, a variety of cryptographic algorithm packages can be implemented in the form of plug-ins without any changes to the core code to adapt to different specification standards and implementation forms.

The core point for Fabric's domestic cryptographic algorithms is to replace the ECDSA elliptic curve signature algorithm with the national security SM2 algorithm, where the ECDSA algorithm is implemented by the golang underlying source code crypto package. The main idea is to extend the design of BCCSP, the cryptographic module of Fabric, to add support for the SM2 algorithm in the basis of the existing one, and to develop external interface functions according to the same function writing standard so that the naming patterns, interface functions, and calling methods can be unified.

The first step is to refer to the file structure of the source code of the crypto/ecdsa algorithm in the golang language and determine that the source code of the SM2 algorithm has the files sm2sign.go and sm2curve.go. The sm2sign.go file defines the data structures that need to be used in the context and implements the external interface, and the sm2curve.go file implements some mathematical operations that need to be used in the principle of the SM2 algorithm, such as block operations and transformation functions.

In the second step, according to the principle of the SM2 algorithm, the public key is a point on the elliptic curve, and the private key is a large number. According to this principle, a pair of secret key structures can be defined and stored in the sm2sign.go file, where the public key is PublicKey, which implements the PublicKey interface in crypto/crypto.go, and the private key is PrivateKey, which implements the PrivateKey interface in crypto/crypto.go and the Signer interface.

In the third step, the SM2 algorithm standard is followed to implement the two most critical functions—signature and verification. The main operation is to use the math/big package and crypto/elliptic package in golang to implement large number operation in the field of a prime number (additive operation, subtraction operation, modulo arithmetic) and some elliptic curve operations (number multiplication operation, point multiplication). The related basic operations are shown in Tables 1 and 2.

After completing the replacement of the SM2 algorithm in the underlying crypto package, we replaced the Crypto package introduced in the BCCSP-related files with a redesigned Crypto package, and the national cryptographic transformation of the blockchain was completed by waiting for the second successful compilation (Q et al., 2021).

Figure 3.
SM2 public and private key data structure

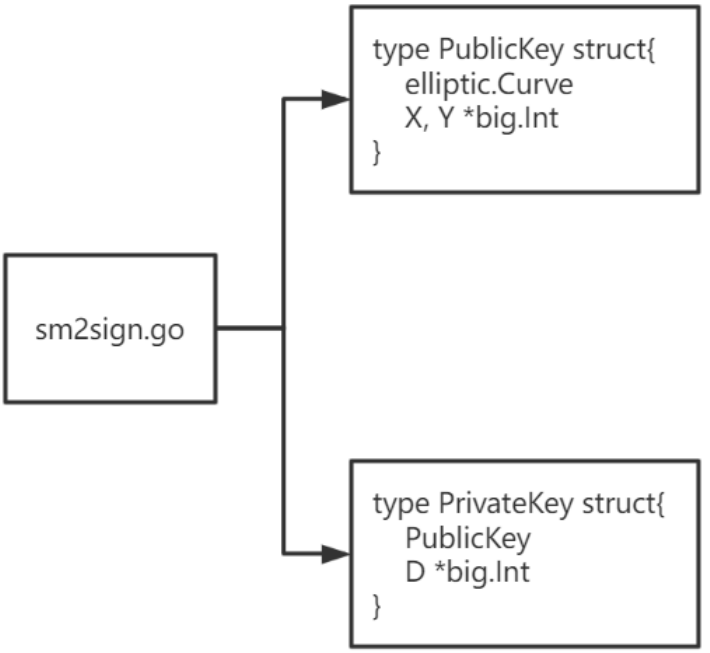


Figure 4.
Structure of SM2 public-private key pair

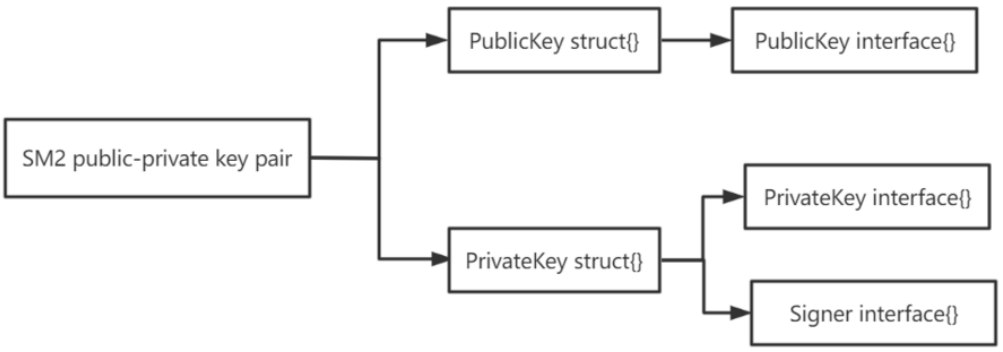


Table 1.
Calculation of large numbers in the field of prime numbers

Basic Operation Function	Function Name
Additive operation	func(z *Int) Add(x, y *Int) *Int
Subtraction operation	func(z *Int) Sub(x, y *Int) *Int
Modulo arithmetic	func(z *Int) Mod(x, y *Int) *Int

Table 2.
Calculation of elliptic curve

Basic Operation Function	Function Name
Multiplication operation	func(z *Int) Mul(x, y *Int) *Int
Point multiplication	func(curve *CurveParams) BaseMul(k []byte)(*big.Int, *big.Int)

THE IMPROVED SM2 ALGORITHM TEST

The Performance Test of Improved SM2 Algorithm

In the test environment, the host configuration was Win10 x86_64, Intel Core i5-10400, and the virtual machine configuration was Ubuntu 21.04. Two cores were available for the CPU, and the memory was 8 GB.

To analyze the performance of optimized SM2 algorithm, we implemented the SM2 algorithm by Go language. To keep the signature information, the signer's unique identification, and key pair unchanged, the number of signatures and verification processes were set to 100 times, and the original SM2 signature algorithm and improved algorithm were tested for five times. The total time was recorded for the comparative analysis. The test results are shown in Table 3 and Figure 5.

Experimental results showed that the improved signature algorithm has a lower time complexity. The SM2 algorithm uses the elliptic point, modular inversion, hash, and point multiplication operations. Starting from the angle of removing or reducing modular inversion and point multiplication operations that have higher time complexities, we optimized the improved algorithm proposed in this paper to further shorten the signature time and improve the calculation efficiency of algorithm.

Performance Test of Improved SM2 Algorithm Based on Alliance Chain

In the virtual environment, we deployed the original blockchain system and the blockchain system based on the optimized SM2 algorithm in the development environment, respectively. In the case of ensuring that the construction of the alliance chain network was consistent in the chain code, the average time-consuming of the five-time start-up of the alliance chain test network was calculated in the two environments. The test results are shown in Table 4, which shows that the start-up rate of the Hyperledge Fabric SM2 blockchain system is higher than that of the original system.

Next, we created channels in the Fabric network in the two environments and added nodes to the channels. Then, we installed the same chain code and initialized it. For the "chain code installation

Table 3.
The comparative analysis of operation time consumption between original SM2 algorithm and improved SM2 algorithm

Testing	Original SM2/ms	Improved SM2/ms	Increase Proportion $\eta\%$
1	1,729	1,664	3.7
2	1,809	1,672	7.5
3	1,787	1,709	4.3
4	1,744	1,639	6.0
5	1,768	1,652	6.5
The average value	1,767.4	1,667.2	5.7

Figure 5.
Comparative analysis of algorithm running time

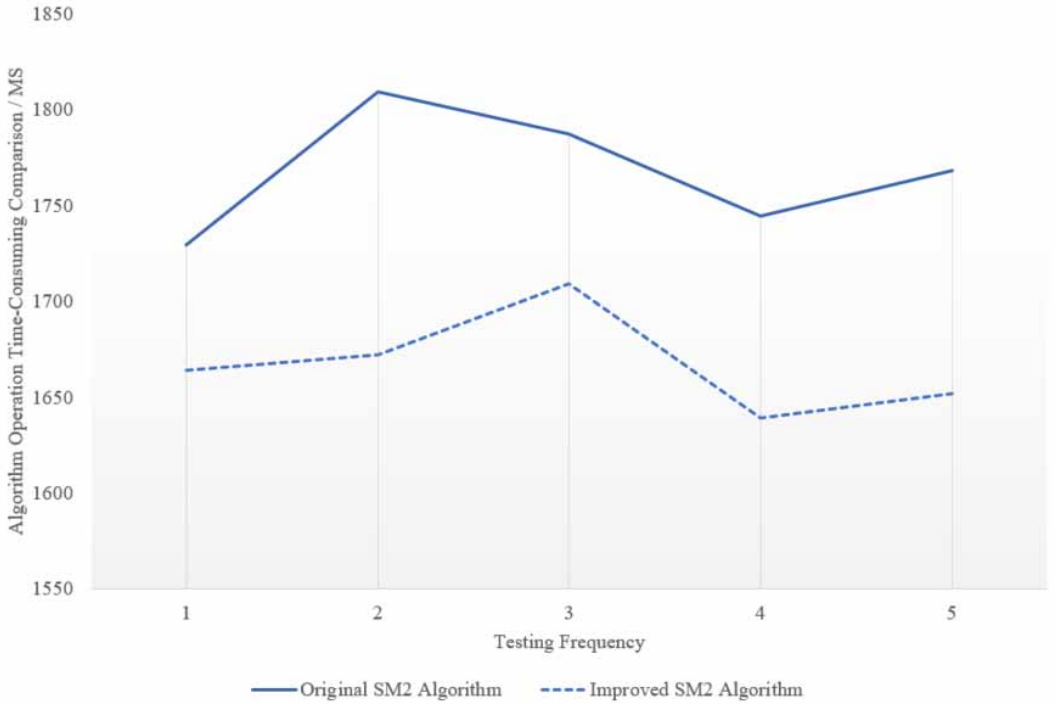


Table 4.
Comparison of start-up time of alliance chain network

Test Number	ECDSA Algorithm	Improvement of SM2 Algorithm
1	3,583 ms	2,587 ms
2	3268 ms	2,281 ms
3	3, 358 ms	2,239 ms
4	3,487 ms	2,290 ms
5	3,130 ms	2,486 ms
Average value	3,365 ms	2,376 ms

and initialization," the core functions of the Fabric blockchain system were tested. Five tests were carried out for each of the two systems. We noticed that the performance of the SM2 Edition Fabric blockchain system was significantly better than that of the original system. The experimental results are shown in Table 5.

A more intuitive look at the experimental results can be found in Figures 6 and 7, which show that the performance of the optimized blockchain system improved by comparison with the original system, as can be seen from the signature algorithms used in the underlying layers of both systems. The signature algorithm used in the original system was the ECDSA algorithm, and its performance was similar to that of the SM2 algorithm, for the reason that both of them have the same theoretical basis, relying on the calculation of the elliptic curve discrete logarithm problem, and the code was

Table 5.
Comparison of chain code initialization rate of alliance chain network

Test Number	ECDSA Algorithm	Improvement of SM2 Algorithm
1	59.760 s	59.741 s
2	62.500 s	61.523 s
3	64.298 s	59.218 s
4	62.988 s	60.500 s
5	58.150 s	58.604 s
Average value	61.539 s	59.9172 s

implemented based on the large number operations and some elliptic curve operations functions in the golang language. However, relatively speaking, the optimized SM2 algorithm outperformed the ECDSA algorithm (Sun, Cai, Zhou, Zhao, & Yang, 2013), which verified the superiority of the blockchain system based on the optimized SM2 algorithm.

CONCLUSION

With the increasing maturity of blockchain technology, its application in various industries is becoming more and more promising (Chauhan & Patel, 2022), but network and information security, as an important red line for all technologies to be implemented, should be ensured. To address the potential

Figure 6.
Comparative analysis of start-up time of alliance chain network

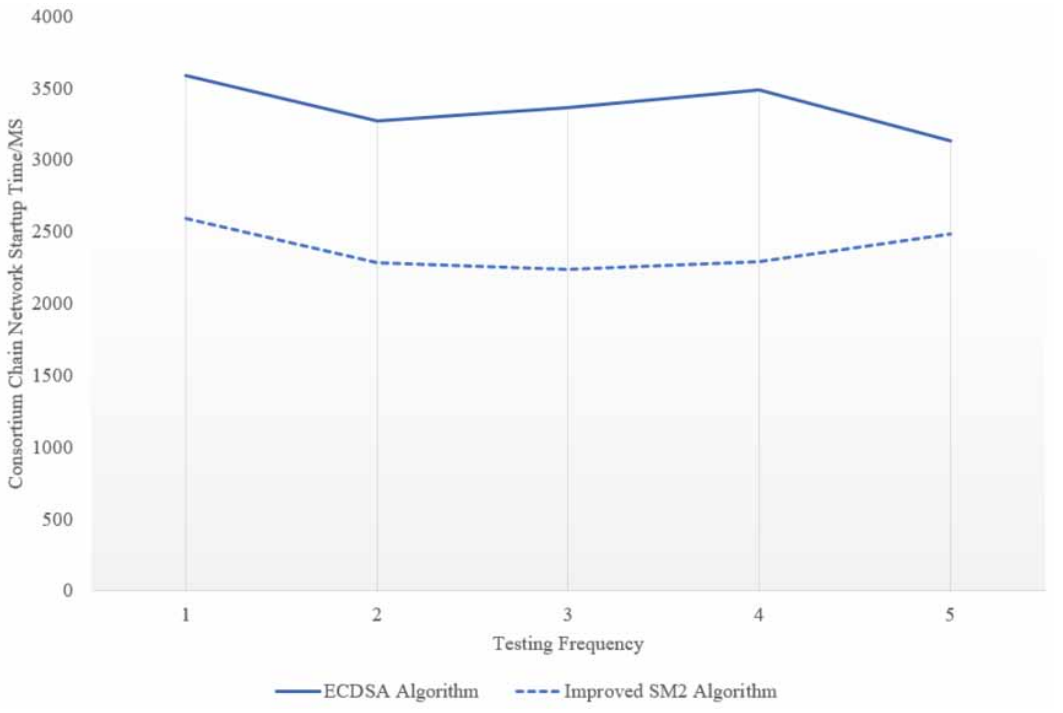
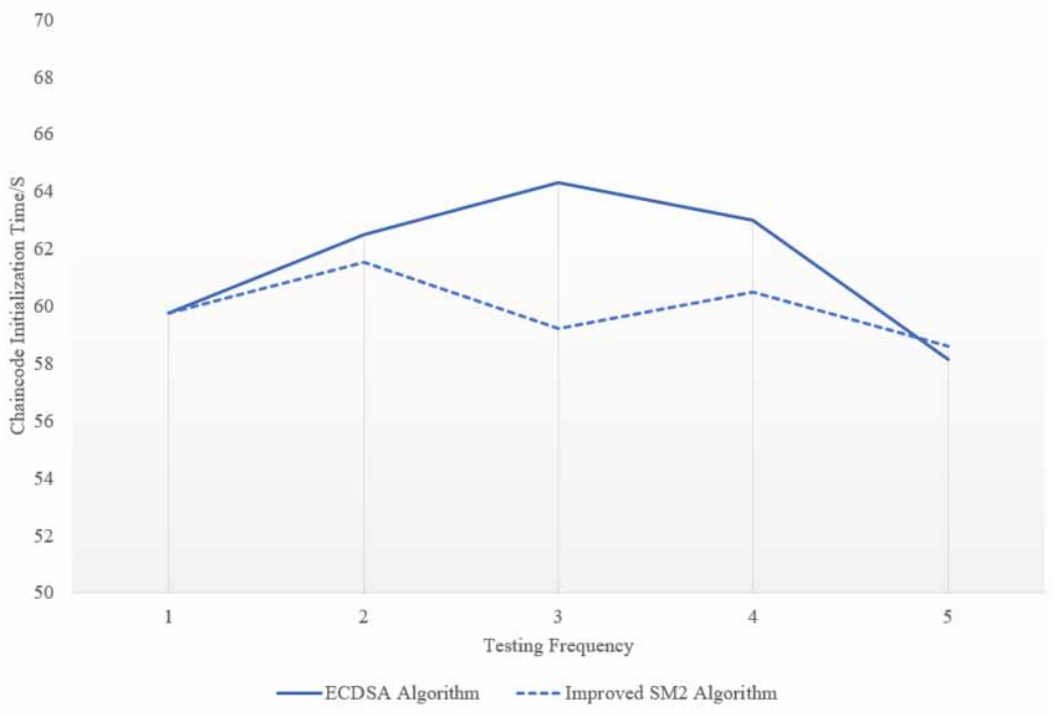


Figure 7.
Comparative analysis of chain code initialization rate in alliance chain network



security risks of the cryptographic algorithms used in blockchain technology, we improved the SM2 algorithm and reduced the time complexity of the SM2 algorithm, while ensuring that the security of the algorithm itself was not affected. We also improved the signature and verification efficiency by about 5.7%, compared with the original SM2 algorithm. At the same time, the Hyperledger Fabric platform was embedded with the SM2 algorithm, and it successfully passed the network start-up test. The system performance was tested, and the network start-up time was reduced by about 29%. The experimental results proved the feasibility of the optimization scheme, and provided a theoretical basis for the rapid promotion of blockchain technology in practical applications.

ACKNOWLEDGMENT

This research work is supported by the Innovative Research Groups of the National Natural Science Foundation of China (Grant No.61521003), Intergovernmental Special Programme of National Key Research and Development Programme (2016YFE0100300, 2016YFE0100600), National Scientific Fund Programme for Young Scholar (61672470), and Science and Technology Project of Henan Province (182102210617, 202102210351).

REFERENCES

Androulaki, E., Barger, A., Bortnikov, V., Cachin, C., Christidis, K., De Caro, A., Enyeart, D., Ferris, C., Laventman, G., & Manevich, Y. (2018). Hyperledger fabric: A distributed operating system for permissioned blockchains. In *EuroSys '18: Proceedings of the Thirteenth EuroSys Conference*. Association for Computing Machinery. doi:10.1145/3190508.3190538

Avkurova, Z., Gnatyuk, S., Abduraimova, B., Fedushko, S., Syerov, Y., & Trach, O. (2022). Models for early web-attacks detection and intruders identification based on fuzzy logic. *Procedia Computer Science*, *198*, 694–699. doi:10.1016/j.procs.2021.12.308

Bai, X., Qin, B., Guo, R., & Zheng, D. (2022). Two-party collaborative blind signature based on SM2. Chinese. *Journal of Network and Information Security*, *8*(6), 39–51.

Bin, L., Qinglei, Z., Xiaojie, C., & Feng, F. (2022). Reconfigurable optimization method for prime domain SM2 algorithm. *Journal of Communication*, *43*(3), 30–41. doi:10.11959/j.issn.1000-436x.2022043

Cao, Q., Ruan, S., Chen, X., Lan, X., Zhang, H., & Jin, H. (2021). Embedding of national cryptopgraphic algorithm in Hyperledger fabric. *Chinese Journal of Network and Information Security*, *7*(1), 65–75. doi:10.11959/j.issn.2096-109x.2021007

Cao, W., Shi, H., Chen, H., Chen, J., Fan, L., & Wu, W. (2022). Lattice-based fault attacks on deterministic signature schemes of ECDSA and EdDSA. In S. D. Galbraith (Ed.), Lecture Notes in Computer Science: Vol. 13161. *Topics in Cryptology—CT-RSA 2022. CT-RSA 2022*. Springer. doi:10.1007/978-3-030-95312-6_8

Chauhan, B. K., & Patel, D. B. (2022). A systematic review of blockchain technology to find current scalability issues and solutions. In D. Gupta, A. Khanna, V. Kansal, G. Fortino, & A. E. Hassanien (Eds.), *Proceedings of Second Doctoral Symposium on Computational Intelligence (DoSCI 2021). Advances in Intelligent Systems and Computing* (vol. 1374). Springer. doi:10.1007/978-981-16-3346-1_2

Ezziri, S., & Khadir, O. (2021). A zero-knowledge identification scheme based on the discrete logarithm problem and elliptic curves. In F. Saeed, T. Al-Hadhrami, F. Mohammed, & E. Mohammed (Eds.), *Advances on Smart and Soft Computing. Advances in Intelligent Systems and Computing* (Vol. 1188). Springer. doi:10.1007/978-981-15-6048-4_3

George, J. T. (2022). *Blockchain technology and distributed system future scope and B-coin project. In Introducing blockchain applications: Understand and develop blockchain applications through distributed systems*. Apress. doi:10.1007/978-1-4842-7480-4

Guo, H., & Yu, X. (2022). A survey on blockchain technology and its security. *Blockchain: Research and Applications*, *3*(2), 100067. doi:10.1016/j.bcra.2022.100067

Jose, J., & Prakash, E. G. D. (2014). CBC and interleaved CBC implementations of PACTS cryptographic algorithm. *International Journal of Computer Network and Information Security*, *6*(4), 63–71. doi:10.5815/ijcnis.2014.04.08

Kuznetsov, A., Oleshko, I., Tymchenko, V., Lisitsky, K., Rodinko, M., & Kolhatin, A. (2021). Performance analysis of cryptographic hash functions suitable for use in blockchain. *International Journal of Computer Network & Information Security*, *13*(2), 1–15. Advance online publication. doi:10.5815/ijcnis.2021.02.01

Li, J., Wu, S., Yang, Y., Duan, F., Lu, H., & Lu, Y. (2021). Controlled sharing mechanism of data based on the consortium blockchain. *Security and Communication Networks*, *2021*, 1–10. doi:10.1155/2021/5523489

Song, J.-W., Zhang, D., Meng, W.-T., Gao, F., & Liu, X.-D. (2019). An improved SM2-based proxy signature scheme. *Journal of Zhengzhou University*, *51*(2), 9–16.

Sun, R., Cai, C., Zhou, Z., Zhao, Y., & Yang, J. (2013). The comparison between digital signature based on SM2 and ECDSA. *Technology and Implementation of Internet Security*, 2.

Wang, Z., & Zhang, Z. (2016). Overview on public key cryptographic algorithm SM2 based on elliptic curves. *Journal of Information Security Research*, *2*(11), 972–982.

You, J. (2022). *Blockchain framework for artificial intelligence computation*. 10.48550/arXiv.2202.11264

Jinhua Fu was born in Weifang, Shandong Province, China. He is an associate professor at the Zhengzhou University of Light Industry. He received his Ph.D. degree in computer science in 2020 from the University of Information Engineering, China. His research interests include blockchain and big data analysis.

Wenhui Zhou is a postgraduate student at Zhengzhou University of Light Industry. Zhou's research focus is on blockchain.

Zhang Suzhi is professor and director of the School of Software at Zhengzhou University of Light Industry. He graduated from Beijing Light Industry College in 1987 with a bachelor's degree in computer application, Southeast University in 1995 with a master's degree in computer application technology, and Huazhong University of Science and Technology in 2003 with a doctorate degree in computer software and theory. He is a member of the Chinese Computer Society, a director of the Henan Computer Society, a young and middle-aged key teacher in Henan Province, and a leader of the key disciplines of computer science and technology in Henan Province.