Cross-Border E-commerce Payment Encryption Algorithm Model Based on Digital Currency

Zhaogong Lin(✉) and Wenlin Jiang

Shan Dong Management University, Chang Qing, Ji Nan, Shandong, China
linzg222@126.com

Abstract. Based on the analysis of the traditional cross-border e-commerce payment mode, this paper finds that the traditional cross-border e-commerce payment mode is characterized by high cost and long time. Therefore, this paper uses Ripple network and digital currency to optimize the traditional cross-border e-commerce payment mode, and applies the elliptic digital signature encryption algorithm to the digital currency-based cross-border e-commerce payment model, and then further optimizes the cross-border e-commerce payment model based on digital currency, and ensures the security of payment through the elliptic digital encryption algorithm. Finally, the secure and efficient cross-border e-commerce payment encryption algorithm model based on digital currency is proposed.

Keywords: Blockchain · Digital Currency · Cross-border E-commerce · Payment Encryption Algorithm Model · Ripple

1 Introduction

Blockchain technology is a decentralized database based on mathematics and cryptography, supported by the Internet and computer programming, and with a distributed shared ledger as the form of existence. And digital currency is a new currency based on the blockchian technology. Digital currency is a new form of currency produced by Financial science and technology innovation, generally including electronic currency, virtual currency, and legal digital currency. [2] Digital currency based on blockchain technology is different from the current "legal currency", the electronic currency with electronic bookkeeping and the virtual currency provided by network operators and applied to the network virtual space. The current electronic currency refers to the use of electronic method to digitize cash or deposits representing certain wealth, and the direct settlement of creditor's rights and debts through the data trading system, which is the digitization of legal paper money essentially. [10] Mainstream digital currency refers to the service value exchange symbols related to real wealth provided by the network virtual space, which can be roughly divided into three categories: game currency, special currency issued by network service providers (such as Tencent Q currency), and virtual currency used for Internet financial investment (such as bitcoin). [3] With the promotion of blockchain technology application, digital currency payment will become the mainstream, this paper based on digital currency, explore the traditional currency and digital

D. Qiu et al. (Eds.): ICBBEM 2022, AHIS 5, pp. 317–323, 2023.
https://doi.org/10.2991/978-94-6463-030-5_33

currency in cross-border e-commerce payment, and the elliptic curve digital signature encryption algorithm key embedded based on digital currency cross-border e-commerce payment, so as to further guarantee the security of digital currency payment.

2 Journals Reviewed

The British Central Bank, Ail et al.,(2014) made a comparative detailed analysis of bitcoin payment methods and the article believes that the biggest innovation of digital currency is the construction of a globally distributed account system, and people can complete payment activities without needing the support of banks and other intermediaries. [1] Schwartzetal (2014) describe the Ripple's distributed consistency algorithm from the perspective of addressing the Byzantine general problem. [8] A good algorithm needs to be correct, consistent and effective. Correctness refers to a system needs to be able to identify fraudulent transactions. Consistency refers to the distributed system needs to maintain a globally consistent account system. Effectiveness refers to the distributed system can handle transactions efficiently. The ripple distributed consistency algorithm learn from Bitcoin distributed accounts and encryption technology to achieve a balance of consistency and effectiveness by enabling the selective determination of payment nodes. Therefore, this paper adopts ripple distributed consistency algorithm to the Cross-border E-commerce system.

3 Cross-Border E-commerce Payment Model Based on Digital Currency

3.1 Cross-Border E-commerce Payment Model Based on the Traditional Currency

Under the traditional monetary payment model, the seller and the buyer reach the purchase intention through the cross-border e-commerce platform, and the buyer place an order through the platform and pays the currency to the platform through the bank, the platform pays the money to the seller after the agreement through the bank. The goods are sold by the seller through a cross-border e-commerce platform (see Fig. 1). This transaction is completed. Under the condition of payment in traditional currency, capital flows through cross-border e-commerce platforms and banks, passing through many links, and it will take a certain time and cost. And both the buyers and the sellers need to open an account in the bank to meet such transactions, which will produce a certain "Shoe-leather cost". Therefore, such a payment system requires a large cost. [9].

3.2 Cross-Border E-commerce Payment Model Based on Digital Currency

Under the blockchain technology, the buyers and sellers can make cross-border payment and settlement through the ripple. There are mainly includes two core components in the ripple distributed algorithm, ripple connect and ripple network. Among them, the ripple connect is a plug-in module for processing the ripple payment transactions in the banking system. Between the remittance bank and the collection bank, the ripple

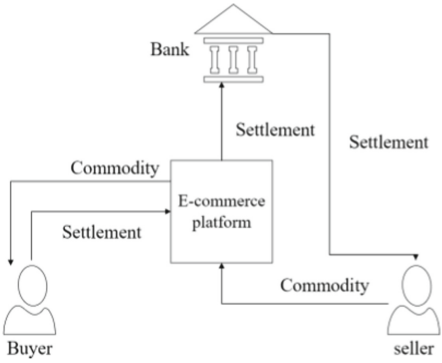

Fig. 1. Centralized payment and settlement system of the traditional currency

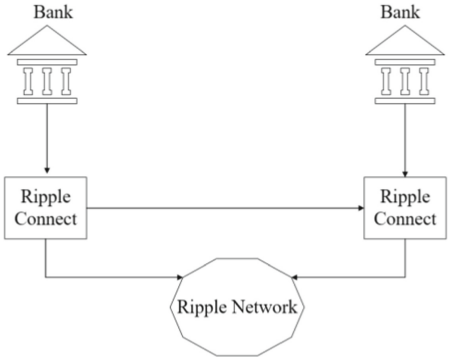

Fig. 2. A decentralized cross-border e-commerce payment model of digital currency

connect has established an information channel for exchanging risk control information, handling fees, exchange rates, and other payment-related information. Before the transaction is initiated, the ripple connect sends the information to the counterparty and needs to check whether the information is correct, and after confirms it can execute the transaction and liquidation funds. With bidirectional messaging in ripple, banks can more efficiently exchange information about the sender, receiver, fees, rates, delivery estimate and payment status to lower their operational cost of processing international payments. With Ripple, banks get the flexibility to validate the transaction before the funds are transferred and confirm delivery of funds, ensuring high STP rates, low returns and negligible investigation and tracking effort.

Although the ripple that based on the district chain technology application has the advantages of decentralization and cost saving, users also need to conduct certain key verification before entering the district chain chain payment, so as to ensure the security of the payment link. Scholars have done many analysis of the encryption algorithm, which mainly has the advanced encryption standard algorithm, elliptic curve encryption algorithm, Diffie-Hellman algorithm. After the comprehensive consideration of the algorithm, because the elliptic curve encryption algorithm has high encryption strength,

short key advantages, so this paper uses the elliptic curve encryption algorithm for cross-border e-business payment encryption.

4 Elliptic Curve Digital Signature Encryption Algorithm

The elliptic curve password system was invented by Neal Koblitz [4] and Victor Miller [6]. Based on the discrete-log-difficult cryptographic algorithm of the finite-domain elliptic curve, it is still the most secure public-key encryption algorithm.

4.1 Main Domain Parameter of ECDSA (Elliptic Curve Digital Signature Algorithm) [7]

The main domain parameters of ECDSA are mainly composed of the following parts: T = (q, FR, a, b, G, n, and h).

(1) Select a domain of q, q = P (prime field), or $q = 2^m$ (Binary field, that is, an exponential domain with the base of 2 and m as the prime); when it is the prime field is GF (P), and p > 3, its equation is $y^2 = x^3 + ax + b$ (where a, b eGF (p) and must meet $4a^3 + 27b^2 (\text{mod } p) \neq 0$ to ensure the non-supersingularity of the ellipse; for the binary field GF (2^m), the equation is $y^2 + xy = x^3 + ax^2 + b$ (where a, b ∈ GF (2^m), and b ≠ 0). The elliptic curve E is defined as the point satisfying the above equation plus the infinity point O constitutes the additive abelian group.

(2) FR domain representation for the elements in F;

(3) Elements a and b in the F represent the coefficients of the elliptic curve equation above;

(4) Elements x and y in F represent one basis point G = (x, y) in E (F) (User A selects an elliptic curve Ep (a, b), and takes the point on the elliptic curve as the basis point G. The basis point meets nG = O, O is the infinite point meeting the elliptic curve equation);

(5) The order of basis point G is n, namely nG = O (namely nG = G + G + + ⋯ + G, The total number of G is n,O represents the infinity point satisfying the above domain equations), n is prime, $n > 4q^{1/2}$And, again, n > 2;

(6) The elliptic curve has the accompanying factor h = E(Fq)/n.

4.2 ECDSA Key Pair

The elliptic curve domain parameters are associated with the key pair-specific set of the elliptic curve digital signature algorithm. After determining the main domain parameter T = (q, TR, a, b, G, n, h) of the elliptic curve, the key pair can be determined. Signature entity A must determine the validity of the primary domain parameter before generating the public key. The public key is a random multiple of the basis point; while the private key is an integer used to generate this multiple. To generate a ECDSA key pair, the algorithm steps requiring member A to normally operate are as follows:

(1) Select a random integer or a pseudo-random integer d_A in the interval [1, n-1] (private key);

(2) Calculate the $Q_A = d_A G$;

(3) The public key of A is Q_A, the private key is d_A.

4.3 The ECDSA Signature Process

The Signing Party A in order to sign the message m, will use the domain parameter T = (q, FR, a, b, G, n, h) and its associated key pair (d_A,Q_A). Do the following operations.

(1) Select a random or pseudo-random integer k, so that k satisfies [l, n-l];

(2) Calculate the kG = (x_1,y_1), And will x_1 Convert to an integer x;

(3) Calculate the r = x_1 mod n, if r = 0,it goes back to step a;

(4) Calculate the k^{-1}mod n;

(5) Calculate the SHA-l (m) message summary value and convert the bit string into an integer e;

(6) Calculate s = $k^{-1}(e + d_A r)$ mod n, if s = 0, then goes back to step a;

(7) Send it to (r, s).

4.4 ECDSA Verification Process

After the verification party B receives A's signature to the message m, to verify that A's signature on the message m is (r, s), you need to obtain the relevant public key Q of A,and the trusted copy of the and domain parameter T = (q, FR, a, b, G, n, h), and to verify T and QA, then B does as follows:

(1) Verify that r and s are integers within the interval [l, n-l];

(2) Calculate the SHA-l (m) message summary value and convert the bit string into an integer e;

(3) Calculate the w = s^{-1}mod n;

(4) Calculate the calculation u_1 = ew mod n and u_2 = rw mod n;

(5) Calculate the X = $u_1G + u_2Q_A$;

(6) Denis rejected if X = O; otherwise the x-axis coordinate of the conversion X is x_1 for integer X_1', and calculate v = x_1' mod n;

(7) B accepts the signature, only if v = r.

On the basis of ECDSA encryption algorithm, the cross-border e-commerce payment supported by digital currency technology can increase the security of payment, improve the income of transactions and save the time of transactions. [5] Therefore, this paper proposes a cross-border e-commerce encryption algorithm model based on digital currency.

5 Cryptographic Algorithm Model of Cross-Border E-commerce Payment Based on Digital Currency

The buyer and the seller enter the ripple network by generating a key through the ECDSA encryption algorithm and pay in a digital currency based on the district payment chain technology. Referring to Fig. 3 for specific procedures. The advantages of security based on ECDSA algorithm and the advantages of non-tamper ability, whole-process traces, traceability, collective maintenance, openness and transparency of district money chain technology ensure the security, timeliness and convenience of cross-border e-commerce payment system. Moreover, digital currencies can avoid currency depreciation fluctuations caused by currency overissuance of monetary authorities.

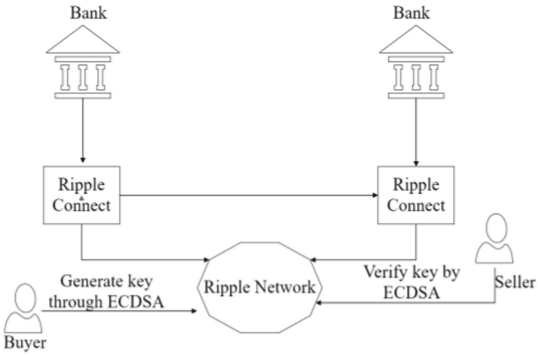

Fig. 3. An encryption algorithm model for cross-border e-commerce payment based on digital currency

6 Conclusions

In this paper, the Ripple network and digital currency based on the regional payment chain technology are used to optimize and improve the traditional cross-border e-commerce payment model, and we use the elliptic digital signature algorithm to encrypt the cross-border e-commerce payment, thus reducing the cost of cross-border payment and improving the efficiency of cross-border e-commerce payment.

References

1. Ali, R., Barrdear, J., Clews, R., & Southgate, J. (2014). Innovations in payment technologies and the emergence of digital currencies. Bank of England Quarterly Bulletin, Q3.
2. Chuen, D. L. K. (Ed.). (2015). Handbook of digital currency: Bitcoin, innovation, financial instruments, and big data. Academic Press, The oxford.
3. Jun, J. F., Lei, K.,(2020). A review of blockchain technology for edge-oriented AI computing. Journal of Applied Sciences (01), 1–21.
4. Koblitz, N. (1987). Elliptic curve cryptosystems. Mathematics of computation, 48(177), 203–209.
5. Li, D. W., Wang, Zh. Y., Zhao, J. G., (2012). Analysis of elliptic curve password system security. Computer Technology and Development (04), 227–230.
6. Miller, V. S. (1985, August). Use of elliptic curves in cryptography. In Conference on the theory and application of cryptographic techniques (pp. 417–426). Springer, Berlin, Heidelberg.
7. Pan, X. J., (2008). A new digital signature scheme based on elliptic curves. Computer System Applications (01), 35–37.
8. Schwartz, D., Youngs, N., & Britto, A. (2014). The ripple protocol consensus algorithm. Ripple Labs Inc White Paper, 5(8), 151.

9. Zhou, L. P., Yu, P. X., (2016). Current status, risks and regulatory countermeasures of cross-border e-commerce payment. Shanghai Finance (05), 73–78.
10. Zhuang, L., Zhao, Ch. G., (2017). Research on the evolution of digital currency under blockchain technology innovation: theory and framework.The Economist (05), 76–83.