International Journal of Sciences

Research Article Volume 7 – June 2018 (06)

The Design of Self-purchasing System for Train Tickets Based on Block Chain Identity Authentication Technology

Kun Yang[1,2]✎, Chen Yang[1,2], Feng Yang[1,2]

[1]State Key Laboratory of Geohazard Prevention and Geoenvironment Protection, Chengdu University of Technology, Chengdu 610059, China
[2]College of Nuclear Technology and Automation Engineering, Chengdu University of Technology, Chengdu 610059, China

Abstract: As a frontier technology, block chain has great prospects in the fields of internet of things and finance field. In the process of bitcoin transaction, the legality authentication of identity information is realized through block chain technology and cryptography knowledge. Based on this, block chain identity authentication and distributed storage technology are applied to a train ticket purchasing system in this paper. The system mainly consists of four modules: communication terminal, ticketing digital encryption database, block chain identity authentication center and self-service ticket collecting machine. The communication terminal receives ticket and purchaser identity encryption information, it also subscribes to tickets on the Internet through a timestamp server. The ticket digital encryption database encrypts the identity and ticket information and sends it to the communication terminal. The block chain identity authentication center completes the legality verification of the ticket collector identities through the key matching and decryption algorithm. Self-service ticket collection machine finishes printing tickets. The system uses block chain and secret key matching to achieve the identity authentication of the ticket collector. The collector can also take out the ticket without identity card, which provides great convenience for passengers who have lost their ID cards or temporarily can not show their identity cards.

Keywords: Block Chain, Distributed Storage, Identity Authentication Technology, Ticket Collection System

1. **Introduction**

At present, tourists are used to booking tickets on the Internet through mobile terminals, after completion of payment [1], the mobile phone will receive information of successful booking. And then take out your ticket on the ticketing window or the self pick up machine [2]. Nowadays, the general operation of the self-help ticket is to put the ID card in the identification area of the self-help ticket machine, but in this way tickets can only be printed after identity information and ticketing information are authenticated [3-5]. So the identity card is an indispensable document to complete the ticket collection [6]. This brings great trouble to the passengers who temporarily lose their ID cards and those who can't print tickets without their ID card. This situation will delay passengers' travel and cause certain property losses.

Therefore, we study distributed storage and identity authentication of block chain applied to this problem of train ticketing system [7-10]. The ticket purchaser can complete the self-service ticket collection without ID card, which is convenient for people to travel, especially for passengers who can not produce ID cards temporarily, it has important practical significance.

2. Related Works

2.1 Basic Ideas and Research Methods

According to the characteristics of block chain identity authentication technology, Block chain enables us to be more secure and more control over identity information [11]. It is necessary to encrypt the identity information and ticket information of ticket purchasers. In particular, the main idea of this method is used the hash encryption as the encryption method of this work.

After encrypting the identity of the ticket buyer, a secret key representing its identity will be allocated，the secret key is exclusive, can be divided as public key and private key [12]. Then the ticket information is encrypted with the public key of the ticket holder and after which the hash summary of ticketing information will be obtained. The ticket collector decrypts the encrypted ticketing information by providing his own private key, and once the decryption is successful, it is authenticated. At last self-service ticket collection

Published at: http://www.ijsciences.com/pub/issue/2018-06/
DOI: 10.18483/ijSci.1700; Online ISSN: 2305-3925; Print ISSN: 2410-4477

✎ Kun Yang (Correspondence)
✉ y2321567752 @ sina.com
☎ +

machines will print tickets for them and complete the whole process of self-service ticket purchase.

2.2 Identity Authentication Technology

Identity authentication based on block chain is implemented through distributed encryption [13]. First, using the encryption algorithm to digitally encrypt the actual identity information, after which a string of binary digits is obtained, and it is used as the address value of the identity. Replacing the identity information with the encrypted address value can effectively isolate user identity information, in this way illegal users can not get users' privacy data through any information mining technology [14-15]. When the validation of its identity is done, the only step that's left is to provide the private key of the identity to match the public key, and matching success is the completion of identity authentication.

3. Design Formulation

3.1 System Structure Design

The train ticket collection system of block chain identity authentication technology mainly includes four modules: communication terminal, ticket digital encryption database, block chain identity authentication center and self-service ticket collection machine. After the identity authentication of the ticket collector is realized by these four modules, the self-service ticket collection will be completed. Specifically, the structure of train self service ticketing system of block chain identity authentication technology is shown in Figure 1.

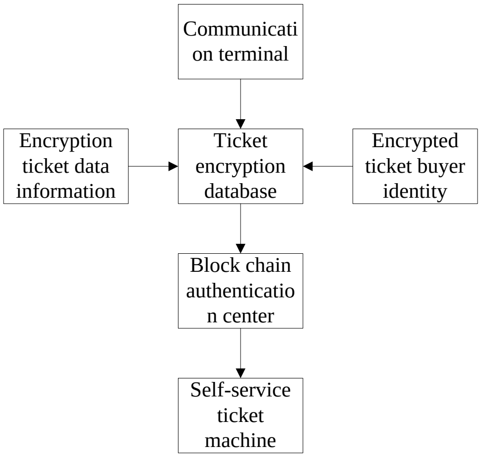
Communication terminal
Encryption ticket data information
Ticket encryption database
Encrypted ticket buyer identity
Block chain authentication center
Self-service ticket machine

Fig. 1 Structure of self-purchasing system for train tickets based on block chain identity authentication

The communication terminal is the connection module of the ticket buyer and the ticketing system. It is to realize the docking and interworking between the ticketing network and the self service ticketing system. Generally, smart phones and computers are selected as communication terminals. The ticket purchaser completes the reservation of the ticket through the communication terminal. In the self service ticketing system based on block chain, the identity authentication center and communication terminal must realize real-time communication. After the booking is completed, the ticket and the identity encryption information are sent to the block chain identity authentication center.

The ticketing digital encryption database is mainly used to encrypt ticket purchaser identity information and ticketing information. The identity and ticket information transmitted from the communication terminal are hashed twice by a dual SHA256 hash function. It is converted to a binary digit of 256 bits to store uniformly. The encoded data information is fed back to the communication terminal for ticket purchasers to view and use. The code corresponding to the encrypted information is encoded and transmitted to the block chain identity authentication center module.

Block chain identity data authentication center is the central link of the self-service ticketing system. Its function is to realize the identity authentication of the ticket purchasers. When the ticket holder enters the identity of the ticket collector, the authentication center decrypts it. And compare it with the corresponding code sent by the ticketing encrypted database. This is also the verification of ticket (including order number) and identity information of ticket purchasers. The two encrypted information is verified by the block chain identity authentication center before completing the identity authentication of the ticket purchasers.

The self fetching ticket machine is the external execution module of the self-service ticketing system. Once the identity of the ticket purchaser is authenticated by the block chain identity authentication center, the self-service ticket collection machine prints out the purchased ticket. It realizes that the purchaser can complete the self service ticket collection without providing his own identity card.

3.2 Information Encryption

After the ticket purchase is completed, the ticketing digital encryption database will encrypt its identity and ticket information. According to this, the specific solution is: the asymmetric encryption algorithm (ECC) is used to encrypt the identity of the ticket buyer, after which the address value will be generated, with public key and private key on behalf of its identity; the digital encryption center uses the public key of the ticket holder to encrypt the ticket, thus forming ticket information with the digital signature of the ticket buyer, then the encrypted information will be sent to the block chain identity authentication center, and the ticket collector provides his own private key for identity authentication and completes the self-service ticket collection. The specific encryption process is shown in Figure 2.

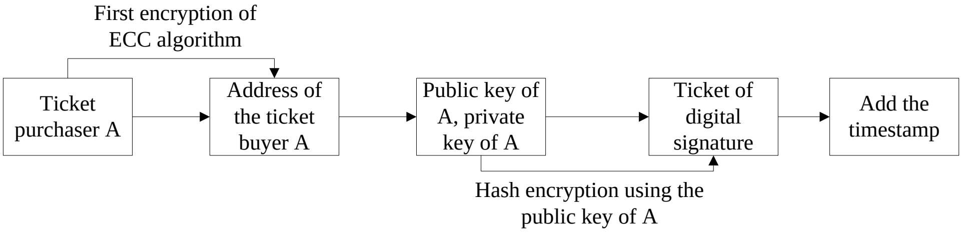
First encryption of ECC algorithm
Ticket purchaser A
Address of the ticket buyer A
Public key of A, private key of A
Ticket of digital signature
Add the timestamp
Hash encryption using the public key of A

Figure.2 The encryption process of ticket purchase

Elliptic hyperbolic encryption algorithm is used for encrypting the identity of the ticket buyers. The address value obtained by encryption represents the identity of each ticket purchaser, and the identity of the ticket buyer is protected by hiding the true identity information. Since the ticket cannot be completed without the address value of the ticket holder, the ticket information is hashed by the public key of the ticket holder. By doing this, the ticket collector are only able to pass the authentication after providing the matching private key for decryption. When the ticket information is encrypted, the time stamp is added to prevent illegal operations as tampering the ticket information without its owner’s permission.

3.3 Self-service Ticket Collection Process

The train self-service ticket system of block chain identity authentication can realize the ticket purchase and collection under the situation that ticket buyers are not able to provide identity documents for the completeness of the self-service. Cryptography is used to encrypt identity and ticket information. The secret key of the ticket buyer is used for decrypting encrypted information. The identity authentication of the block chain identity authentication center is completed and the ticket collection is realized. The train ticket self-purchase process of the system is shown in Figure3.

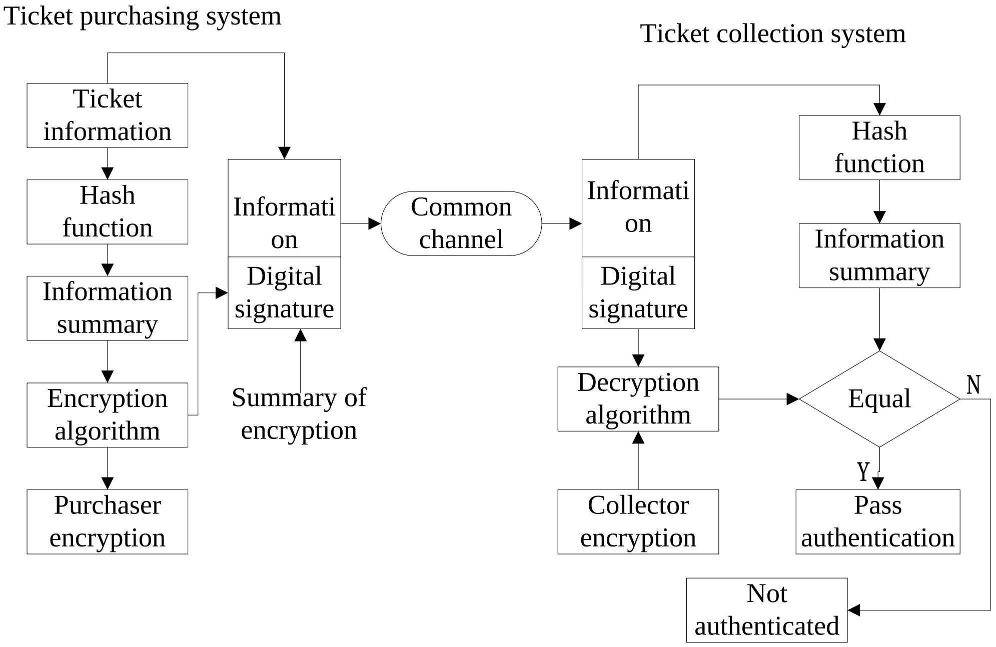

Figure.3 Train ticket self-purchase process of the system

The ticketing system uses the elliptic curve encryption algorithm (ECC) to encrypt the identity of the ticket buyer. The ticket information is encrypted with the purchaser’s public key through a hash encryption algorithm, it will acquire a summary of the ticket information digitally signed by the ticket purchaser. The ticketing information with the digital signature will be sent to the ticketing system through the public channel. Now that the ticket collector can get the summary by providing his own private key to decrypt the encrypted ticket information, the identity authentication process transfers to a comparision of the summary and the digest of ticket information encrypted by hashing algorithm. If the ticket information obtained by the two declassified methods is consistent, the ticket collector is authenticated by the block chain identity authentication center, otherwise, they can not be authenticated by the block chain identity authentication center.

4. Conclusion

This paper designs a self-purchasing system for train tickets based on block chain identity authentication. It realizes the ticket reservation of the communication terminal through the peer to peer network and the timestamp server, and the block chain digital signature technology is used to encrypt the ticket purchasers and ticketing information and send these encrypted information to the communication terminal. The ticket holder provides its own private key to decrypt the ticket information, and authenticates by the identity legitimacy in the block chain identity authentication, thus completing the self-help pick up without the need to provide the identity card. The block chain identity authentication center authenticates the identity of the ticket collector, if it is authenticated, the ticket can be taken out. By applying the method proposed in this paper, for purchasers who currently don't have the identity cards or are not able to use them at this moment, the self-service ticket can still be completed. Through the block chain identity authentication technology, the train self-service ticket acquisition system can solve the problem that the ticket holder can not take out the ticket and delay the user's travel because of the inability to provide the ticket, it provides an ideal solution for more convenient and concise purchase of train tickets and is of great significance to practical application.

Reference

1. Hyun-Woo K and Young-Sik J. Secure Authentication-Management human-centric Scheme for trusting personal resource information on mobile cloud computing with blockchain. Human-centric Computing and Information Sciences 2018.
2. Zhou Z, Lixin L I, Zuohui L I. Efficient cross-domain authentication scheme based on blockchain technology[J]. Journal of Computer Applications, 2018.
3. Khan M A, Salah K. IoT security: Review, blockchain solutions, and open challenges[J]. Future Generation Computer Systems, 2017.
4. Lee J H. BIDaaS: Blockchain Based ID As a Service[J]. IEEE Access, 2018, 6(99):2274-2278.
5. Myojo S. Method to Estimate Passenger Flow Using Stored Ticket Gate Data[J]. Quarterly Report of Rtri, 2006, 47(4):178-181.
6. Lin Q, Yan H, Huang Z, et al. An ID-based linearly homomorphic signature scheme and its application in blockchain[J]. IEEE Access, 2018, PP(99):1-1.
7. SeungJin, H. A Secure Decentralized Storage Scheme of Private Information in Blockchain Environments. Journal of The Korea Society of Computer and Information 2018,23(1):111-116.
8. Wyglinski A M, Irvine J, Chapman J. The Future of Vehicular Security and Privacy [From the Guest Editors][J]. IEEE Vehicular Technology Magazine, 2018, 13(1):26-27.
9. Yin W, Wen Q, Li W, et al. An Anti-Quantum Transaction Authentication Approach in Blockchain[J]. IEEE Access, 2018, 6(99):5393-5401.
10. Dorri A, Steger M, Kanhere S S, et al. BlockChain: A Distributed Solution to Automotive Security and Privacy[J]. IEEE Communications Magazine, 2017, 55(12):119-125.
11. Yan Z, Gan G, Riad K. BC-PDS: Protecting Privacy and Self-Sovereignty through BlockChains for OpenPDS[C]// Service-Oriented System Engineering. IEEE, 2017.
12. Günlü O, Kittichokechai K, Schaefer R F, et al. Controllable Identifier Measurements for Private Authentication with Secret Keys[J]. IEEE Transactions on Information Forensics & Security, 2018, PP(99):1-1.
13. Ou R, Zhang Y, Zhang M, et al. After-the-Fact Leakage-Resilient Identity-Based Authenticated Key Exchange[J]. IEEE Systems Journal, 2017, PP(99):1-10.
14. Jiguang Li. The Processing Monitoring Framework and the Random Authorization Using Blockchain [J]. Information Security Research, 2017, 3(8):752-757.
15. Jiang P, Guo F, Liang K, et al. Searchain: Blockchain-based private keyword search in decentralized storage[J]. Future Generation Computer Systems, 2017.