IC card-based bitcoin payment design and implement

Weihong Wang[1, a] and Peng Li[1, b]

[1]College of Computer Science and Technology,

Zhejiang University of Technology, Hangzhou 310023,China

[a]wwh@zjut.edu.cn, [b]alvalp@live.com

Keywords: Bitcoin payment; IC card; Transaction selection

Abstract. Bitcoin is a virtual currency based on the P2P network. Because of decentralization, anonymity, stability and other advantages, Bitcoin develops rapidly. In order to cope with increasingly wide application fields of bitcoin, this research designs bitcoin's payment based on the IC card, which improves its safety and convenience. According to Bitcoin's unique utilization, we've designed and achieved the documental structure of Bitcoin IC card and mutual authentication between PSAM card and IC card. With the combination of IC card private key and user's private key leading to account's private key, it will be safer to private key. Besides using merge-avoidance algorithm when trading improves the security of the account.

Introduction

Bitcoin was first mentioned in a research paper published on 31 October 2008 under the name Satoshi Nakamoto[1] and issued ever 50 bitcoins[2] in January 2009.The history of its transactions is shared using a peer-to-peer network and is agreed upon using a proof-of-work system [3、4]. Bitcoin is an electronic money-based cryptography and P2P network communication, through a complex algorithm to achieve output and distribution of Bitcoin. Bitcoin system utilizes signature mechanism and timestamp server to authenticate each transaction to ensure that money cannot be forged and double payments. Due to the neutral, anonymous [5], high security and other features to make Bitcoin expanded rapidly in a short period of 3, 4 years, and stand out in a number of e-money. Bitcoin is a viable digital currency with a market capitalization valued at more than $100 million [6] and between $2 and $5 million USD in transactions a day.

Bank of China issued the first credit card in 1985. Until 2010, the national issuance volume has been over 2.42 billion. IC card with its high security, portability and other virture has become a most widely used payment tool in the financial sector. Compared to the disadvantages of magnetic stripe cards with little storage, easy to be forged and copied and bad security, IC card has much more advanced function, better security and more reasonable cost. Therefore, using IC card as the payment of Bitcoin can become more convenient and secure. With the popularity of IC card, everyone can use IC card more easily. Moreover, when it comes to the way of Bitcoin IC card payment, it remains the same as the financial IC card; users will not have the problem in using it. With the wide acception of IC card, it can accelerate the promotion and popularization of Bitcoin as a means of payment. Last but not the least, the terminals of IC card has been mature gradually. The CoinJar which is the biggest bitcoin company of Australia develops the swipe card. It is IC card which can exchange between each and bitcoins.

Payments comparisom

Based on that whether the user has the private key, bitcoin wallets can be divided into off-chain wallet and on-chain wallet. Off-chain Wallet is a pure center wallet; the user does not have the private key of his bitcoin account. However, Off-chain wallet has its own advantages, such as high efficiency, real-time arrival. The private key of the off-chain wallet is managed by the company, so users do not need to worry about the security. But the wallet company is also likely to suffer attacks from hackers.

Currently, the main payment of the bitcoin is on-chain wallet. Because the user of on-chain wallet can have his bitcoin account private key, he has sufficient autonomy and transparency of his account. According to the using situation, it can be divided into local wallet and cold wallet.

At present, local wallet and on-line wallet are particularly popular. Local wallet, such as BTC-Core purse and bither wallet can be installed on your computer or mobile phone. Local wallet is a full-service bitcoin wallet, containing all the functions needed for bitcoin transportation. It's really easy to use, but the device is connecting to the Internet all the time, leading the computers or cell phones easily getting virus. Therefore, hackers can steal your wallet files through network.

Cold wallet is pretty safe in spite of high cost and poor usability. Like traditional Armory, cold wallet requires a non-networked computer installed Armory program. When you want to use the bitcoins, you have to use a media to exchange dates between the off-line and on-line computer. But the media can also be with the risk of got virus.

Document structure

Bitcoin IC card is mainly used to store bitcoin account information and IC card information. Its data is divided into the following categories: IC card authentication data, IC card identification data, user account data, card count data, and user data as show in Fig.1.

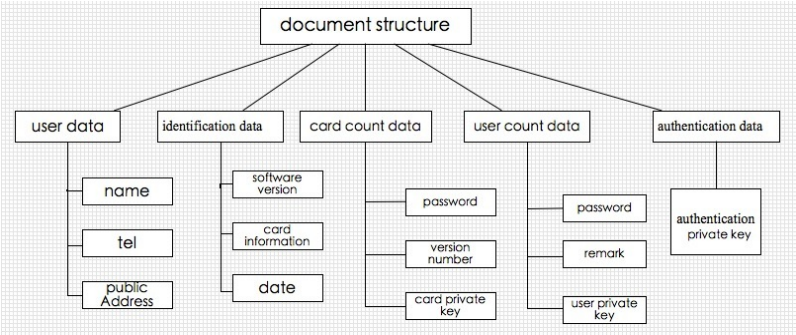

Fig.1 the document structure of the card

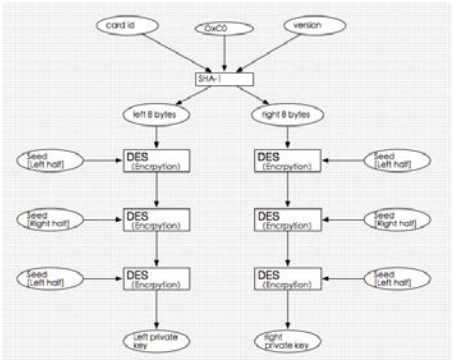

Fig.2 Disperse Algorithem

Validation

There is a CPU chip in the IC card, so IC card has the function of powerful processing capabilities, advanced encryption and decryption functions and protected file system. IC card has high security, but the terminal has comparatively lower security. In order to improve the safety of the terminal, you need to bind the security module in the payment module. In addition, you have to ensure that ont only sensitive data willnot be leaked, but also other terminals cannot be forged. PSAM is chip that can check the authentication between the terminal and the IC card, so it can establish a secure channel between them. Use the serial number as the parameter of the dispersion algorithm in the PSAM card, the secure module can calculator the authentication private key for authentication. The private key of the card is dispersion from the 16-byte master card private key according to the card serial number and other parameters as show in Fig.2.

Before the terminal read or write the IC card files, it must through mutual authentication between the IC card and the PSAM card. If the IC card is unreliable or the terminal is untrustworthy .IC card and terminals cannot carry out subsequent operations.The authentication process of the IC card, terminal, PSAM card is as follows:

- Terminal sends an order to get a random number generated by the card.
- The terminal sends a command to the PSAM card to encrypt the random number.
- Terminal device sends external authentication command with the result to the user card. After the card gets the result, it is determined whether authentication is successful. If successful, the transaction can be carried out subsequent operations.

Address conversion

Bitcoin IC card has two private keys: IC card private key and user private key. IC card private key is randomly generated by the system, but the value cannot be modified after it is generated. The private key can be backed up to the provider's server. User private key can be randomly generated or the value that the user want to. The user can back up the private key in his local computer. The bitcoin address of the IC card is depending on the IC card private key and user private key. Even if anyone of the private keys is theft will not cause account theft. The conversion relationship of the public address、IC card private key, user private key and private key is show in Fig.3 and Fig.4.

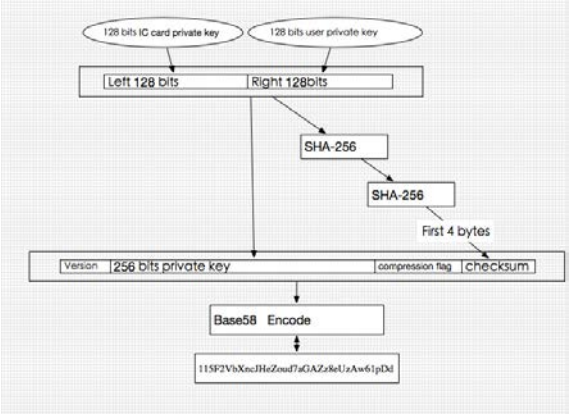

Fig3. Bitcoin private address conversion

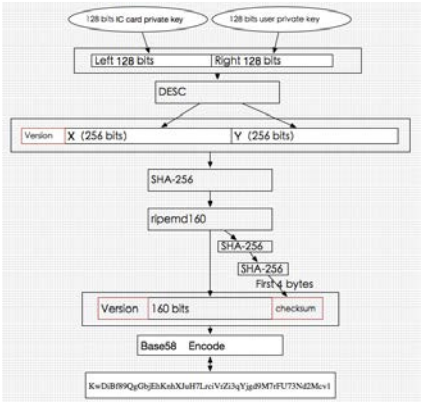

Fig4. Bitcoin public address Conversion

Transaction Selection

When the receiver spends bitcoins they should decide which transaction will be chosen as the input of the spent transaction. There are a few different algorithms, which lead to different results.

- Last in first out

Bitcoin can be spent as soon as they are received, even before they are confirmed. However, this would increase the risk of the recipient of the deal. Because the transaction has not been confirmed, these bitcoins have more likelihood of double spent. LIFO should not be used when the primary transaction recipient's reputation might be at stake, such as when paying employees.

- First in first out

The earliest bitcoin are the most readable, so if someone wants to double spend those bitcoins they should modified more blocks.

Another advantage is the older bitcoin can ben payment without transaction fee. The transaction fee is so low, so this advantage is not a significant advantage. The only practical use of FIFO is by receives who spend all or most of their income within a few blocks.

- Merge Avoidance

Each of those spenders will see the other spender's payment, if the receiver spents satoshis from two different spenders in the same transaction. This is called a merge, and the more a receiver merges outputs, the easier it is for an outside to track how many satoshis the receiver has earned, spent, and saved. Merge avoidance is trying to avoid spending unrelated outputs in the same transaction. A bitcoin IC card represents a bitcoin account, so we use merge avoidance to keep the transaction data secret from other people.

Implementation

After getting the bitcoin address from the bitcoin IC card, system will check the available balance of the account and the corresponding transactions. When using this bitcoins, users should enter the receiver's address and the amount of the transaction as shown in Fig.5. Entering the password of the IC card through the POS machine is to get the permission to read private key in the IC card. Using

account private key, which converses form IC private key and user private key signature the transaction. We can find the detail of the transaction on the Internet as Fig.6.

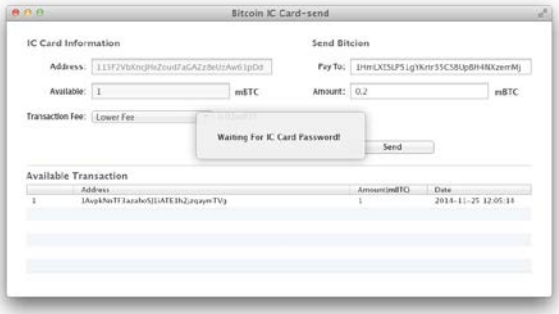

Fig.5 sends satoshis

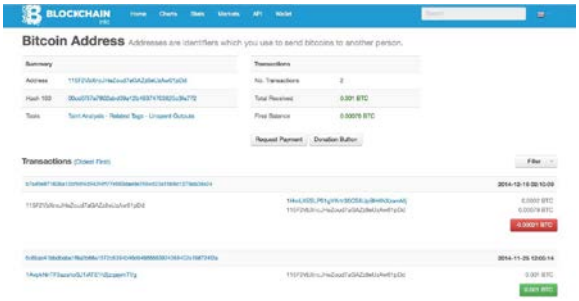

Fig.6 details of the transaction on blockchain.info

Conclusions

Bitcoin uses P2P network technology and cryptography to achieve and maintain the safety and reliability of the system. The issuance and transaction authentication mechanisms of Bitcoin allow Bitcoin currency system no longer to depend on a particular government agency, thus preventing the regular economic crisis. Bitcoin IC card uses IC card as means of payment, not only strengthing the security of payment but also making it more convienent. Through existing POS machines, card readers and other terminal devices, Bitcoin will become more widespread and popular.

Acknowledgements

This paper issupported by the National Natural Science Foundation of China (61340058), the Natural Science Foundation of Zhejiang Province (LZ14F020001) and theState Key Laboratory of Software Development Environment Open Fund(SKLSDE-2012KF-05).

References

[1] Nakamoto S (2008) Bitcoin: a peer-to-peer electronic cash system, http://bitcoin.org/bitcoin.pdf, Retrieved 12 Nov 2011.

[2] Bitcoincharts.Various bitcoin charts and cur- rency statistics [OE].http://bitcoincharts.com/bitcoin/, 2013,(08).

[3] Back A (2002) Hashcash – a denial of service counter-measure. http://www.hashcash.org/ papers/hashcash.pdf, Retrieved 12 Nov 2011.

[4] Dwork C, Naor M (1992) Pricing via processing or combatting junk mail. In: Proceedings of the 12th Annual International Cryptology Conference on Advances in Cryptology (CRYPTO'92), Santa Barbara. Springer, pp 139–147.

[5] Fergal Reid and Martin Harrigan, An Analysis of Anonymity in the Bitcoin System, Privacy, Security, Risk and Trust (PASSAT) and 2011 IEEE Third Inernational Conference on Social Computing (SocialCom), 2011 IEEE Third International Conference on Year: 2011, Page(s): 1318 - 1326.

[6] D. Ron and A. Shamir, "Quantitative Analysis of the Full Bitcoin Transaction Graph," Cryptology ePrint Archive, Report 2012/584, 2012, http://eprint.iacr.org/.