ISBN: 978-981-14-2136-5

Design of Electronic Wallet Based on Block Chain

Chih-Cheng Chen*,Guang-Song Yang

School of Information Engineering, Jimei University
No.185 Yinjiang Rd., Jimei District, Xiamen,361021, Fujian, China
Xiamen 361021, Fujian, China
Center Phone:0952-6182599 and Fax Numbers:0952-6180996 and E-mail:201761000018@jmu.edu.cn, gsyang@jmu.edu.cn

Abstract

With the rising value of Bitcoin and some digital currencies, this brand-new technology has entered the people's daily lives and received widespread attention. With the popularity of technology and the increasing population of users, the transaction issues is getting significant. At present, the centralized transaction methods, such as Alipay, WeChat payment and bank cards, are widely accepted by the general public. However, the drawbacks and trust brought by centralized products are also people's concerns. In view of the fact that society is now paying more and more attention to the issues of trust, this article will develop a smart contract based on block chain technology to solve the transaction problem on the decentralized Ethereum platform.

Key words: Block chains，intelligent contracts，transactions

Introduction

At the core of the block chain is a decentralized public accounting. This public account can be reviewed by people on the website, and no other independent users or agencies can change its content. The participants in the block chain system will work together to ensure the maintenance of the book: it will only be modified according to rigid rules and consensus, hidden by a very magical design.

For example, the residents in the apartment have to be charged the management fee. Suppose one resident did hand in the management fee to the residential guard, but the guard denied it. Didn't the residential guard take the blame for the indiscriminate charges? Based on the block chain technology, we set every resident as a node to make every payment correct.

People must be very familiar with Bitcoin. It is often regarded as a very advanced concept in the financial and monetary fields because it is the first digital currency in the world. It does not have intrinsic values, nor does it have a strong background to support it. It also does not have powerful publishers and controllers.

Satoshi Nakamoto created Bitcoin and it became the world's first digital currency[1]. As its lowest technology and basic framework, the core is a decentralized database. Using cryptography makes the block chain produce data blocks. Each block can contain detailed records of transactions. There will be 6 people verifying the transaction to avoid counterfeiting and thus to produce the next block.

As a relatively new concept, the block chain has several unique features[2]:

1. Decentralized: because of the use of decentralized layout, computing and memory, there is no centralized hardware or management unit. And arbitrary nodes are equal in rights and obligations. The data blocks in the system are protected by nodes with maintenance functions. With this decentralized feature applied to the block chain, Bitcoin also has decentralized features.

2. Openness: The entire system is accessible to anyone and open to the public, except encrypting private information on both sides.

3. Permissionless: The block chain network is that guarding against bad actors is not required and no access control is needed.

4. Unchanged information: if a party wants to modify the data for a certain purpose after the information is added to the block chain, it must modify more than half of the information in the block chain at the same time. The workload is so huge that it is almost impossible to complete.

5. Anonymity: Anonymous transactions may bring insecurity in everyday transactions.In blockchain transactions, there is no need to worry about the problem.Because the interaction of each node has its corresponding algorithm, there is no need to trust, and the essential reason is that this is a very reliable process.

Classification of block chains

The block chain is divided into three types according to the user's right to the system. Divide into main and side chains[3].

1. Public blockchains

A public block chain has no access limitations. Anyone with an Internet connection can send transactions to it and become a validator. Such networks often offer economic incentives for those who secure them and make use of a Proof of Stake or Proof of Work algorithm.

Public chains are also commonly referred to as non-licensing chains, and can be viewed or examined by all. There is no central organization, nor a core processor, but the mechanism specific to the block chain is used to ensure irreversibility.

2. Private blockchains

A private blockchain is permissioned. One cannot join it unless invited by the network administrators. Participant and validator access is restricted.This type of blockchains can be viewed as a middle-ground for companies that are interested in the blockchain technology but are not comfortable with a level of control offered by public networks.

Typically, they seek to incorporate blockchain into their accounting and record-keeping procedures without sacrificing autonomy and running the risk of exposing sensitive data to the public internet.

3. Consortium blockchains

doi: 10.35745/icice2018v2.010

A consortium blockchain is semi-decentralized and permissioned. Instead of a single organization controlling it, a number of companies might each operate a node on such a network. The administrators of a consortium chain put limits on users' reading rights as they see fit and only allow a limited set of trusted nodes to execute a consensus protocol.

Operation of block chains

Main workflow [4].:
1. Assume the transmitted nodes, add new information, and transmit it to the network.
2. Assume the receiving node, check the receiving information. If the message is correct, then the resources are stored in the block.
3. A consensus algorithm for block chains is executed by all receiving nodes in the environment.
4. When the consensus algorithm is completed, the block is stored in the block chain, and any node in the system determines the block and expands the block chain from the back.

Smart contracts

Blockchain-based smart contracts are proposed contracts that could be partially or fully executed or enforced without human interaction [5]. One of the main objectives of a smart contract is automated escrow.

An IMF staff discussion reported that smart contracts based on blockchain technology might reduce moral hazards and optimize the use of contracts in general. But "no viable smart contract systems have yet emerged." Due to the lack of widespread use their legal status is unclear

System scheme

The main processes and functions of our proposed scheme are shown in Fig. 1. The introduction of the roles in the system is described as follows:

User (U): The user is processing data-mining in this block chain. After data-mining is done, the coin will be made. With verification in the thid party, the system will save the coin value in the bank . The user then can use the digital currency to make purchases in the e-commerce websites.

Block Chain System (BCS): The system where enterprises issue virtual coins, manage coins and transactions. The system can encrypt, and give signatures to make an e-

Store (S): The place where customers make purchases.

Mobile (M) The device that customer take to the stores to make purchases.

Platform (P) :

Bank (B): The place where user deposit and withdraw the digital currency.

Our Schema

Notations: The following is the notations that will be used in our scheme.

SK_X : the X 's private key

PK_X : the X 's public key

$Cert_X$: the X 's certificate issued by BCS server

ID_X : the X 's identity

$S_X(m)$: use X's private key to sign a message m

$V_X(m)$: use X's public key to verify a message m

$h(\,)$: the one way hash function

Sig_X : the Xo signature

R: Random Number

t1, t2, t3: the time stamps are generated by User

M: the order message, where

$$M = (ID_U,\ ID_S,\ ID_B, M_{order}, Invoice)$$

A?=B: determines whether A is equal to B

The electronic wallet proposed scheme of the enhanced transaction safety that we categorize into 4 phases: public phase , registration phase, prescription phase, transaction phase, and payment phase. The transmitted messages are protected by secure channel (such as secure socket layer, SSL) in Blockchain network.

A. Public phase

The user can mine on the website, as long as they can connect to the Internet, and have a computer device such as a central processing unit CPU, a graphics processor GPU, or a special application integrated circuit ASIC called a "mine machine." In order to obtain the bitcoin that the system rewards every ten minutes, and finds a mathematical problem that makes the book section difficult to be maliciously modified but easy to verify. This process is as difficult as mining minerals, so it is called "mining," mining with mining machine People are called "miners." Mining also includes packing and verifying thousands of transactions into sections, proving that the transferee has enough bitcoin to prevent the occurrence of one-currency overpayment and earning a bitcoin fee[6].

B. registration phase

User Ui has to register his information and record his password from the BCS server. Then the BCS will execute the following steps. The flow chart of the registration phase is shown in Fig. 1.

Step 2 : The User, mobile phone and Store should register with the BCS server.

Step 2 : First, the User (U), Store (S), Bank (B) and mobile phone (M) should provide his/her identity to register with the HIS server to be a legal party. Only pass the identity authentication, the corresponding party only can obtain the certificate CertU, CertS and CertB from BCS server respectively.

C. Verify phase

After User Ui can buy something in the store. Then the BCS will execute the following steps. The flow chart of the verify phase is shown in Fig. 2.

Step 1: The User adopts the private key to give the signature to the client's order. The User then gives the identity code, signature value and M order information to the Store.

Step 2: The Store uses the user's public key to verify the correction of the order. If the order information is correct, the M order will be made and the Store will give the signature to the shop.

Step 3: If the shop gets the M odrer from the user, it will verify the invoice.

Step 4: The BCS server will made msg then send to Mobile and made Order report.

Step 5: The BCS server will computer Msg and M order. The Mobile adopts the private key to give the signature to the client's order.

Step 6: The BCS server will store msg and M order.The user uses the user's public key to verify the correction of the order. If the order information is correct, the M order and invoice will give the signature to the shop.

D. Payment *phase.*

The shop can buy something in the store. Then the BCS will execute the following steps. The flow chart of the verify phase is shown in Fig. 3.

Step 1: The shop adopts the private key to give the signature to the client's order. The shop then gives the identity code, signature value and order information to the bank.

Step 2: The bank uses the shop's public key to verify the correction of the order. If the order information is correct, the invoice will be made and the bank will give the signature to the shop.

Step 3: If the bank gets the invoice from the shop, it will verify the invoice. The result will be transmitted to the user's cell phone.

Conclusion

We have developed the blockchain technology in this paper, and a variety of applications in different fields can be designed based on the blockchain. For example, in the financial industry, we can use blockchain's characteristics of the decentralization to create an encrypted electronic money system without a third-party. This system prevents the transaction from going through a third-party. People can save some transaction costs, such as application fees or transaction fees. But this system doesn't have a third-party to control data. It may result in a lack of security in each wallet in the blockchain. Therefore, we will use the public key certificate and signatures technology to improve security and use software and hardware as a dual authentication to keep the wallet from being stolen.

References

[1] Satoshi Nakamoto, *Bitcoin: A peer-to-peer electronic cash system*, pp. 28, 2008.

[2] A. Shanti Bruyn, *Blockchain an introduction*,August 26, 2017 .

[3] Xiwei Xu,et al., *A Taxonomy of Blockchain-Based Systems for Architecture Design:ICSA'17: IEEE International Conference on Software Architecture. Apr, 2017* .

[4] Michael Crosby,et al., "*Blockchain technical*," Sutardja Center for Entrepreneurship & Technology Technical Report.2015

[5] McKinsey&Company. Blockchain Technology in the Insurance Sector. In Proceedings of the Quarterly Meeting of the Federal Advisory Committee on Insurance (FACI); McKinsey & Company: New York, NY, USA, 2017.

[6] Web Available online: https://en.wikipedia.org/wiki/Blockchain

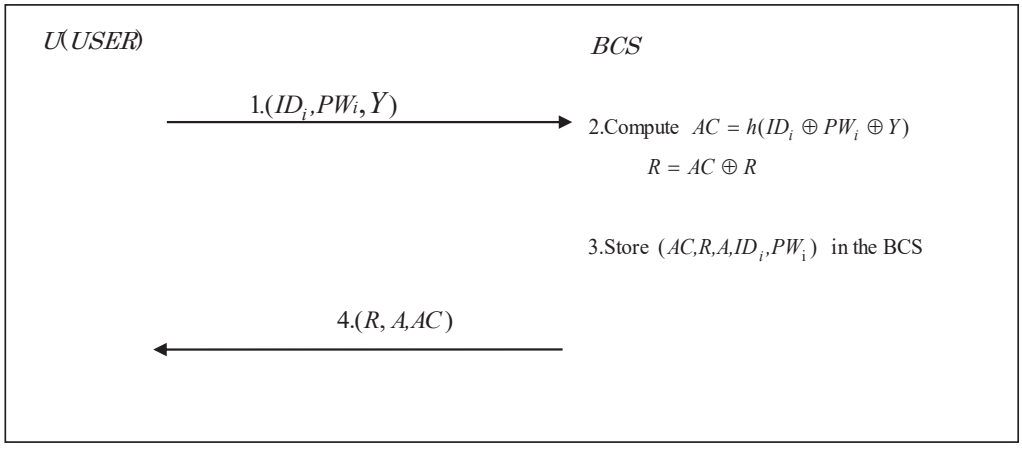

Fig. 1 The flow chart of the registration phase phase.

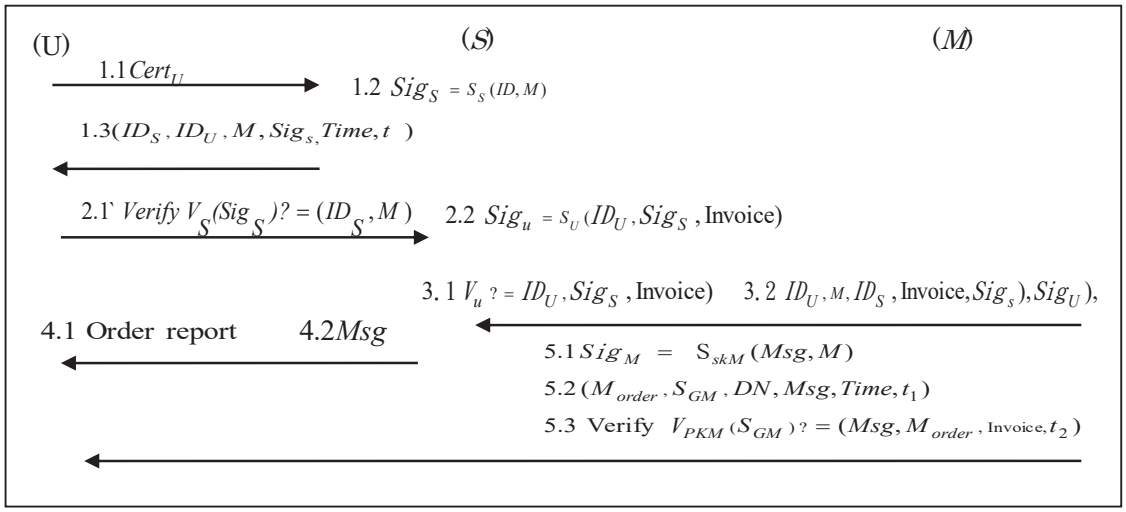

Fig. 2 The overview of the Verify phase phase phase.

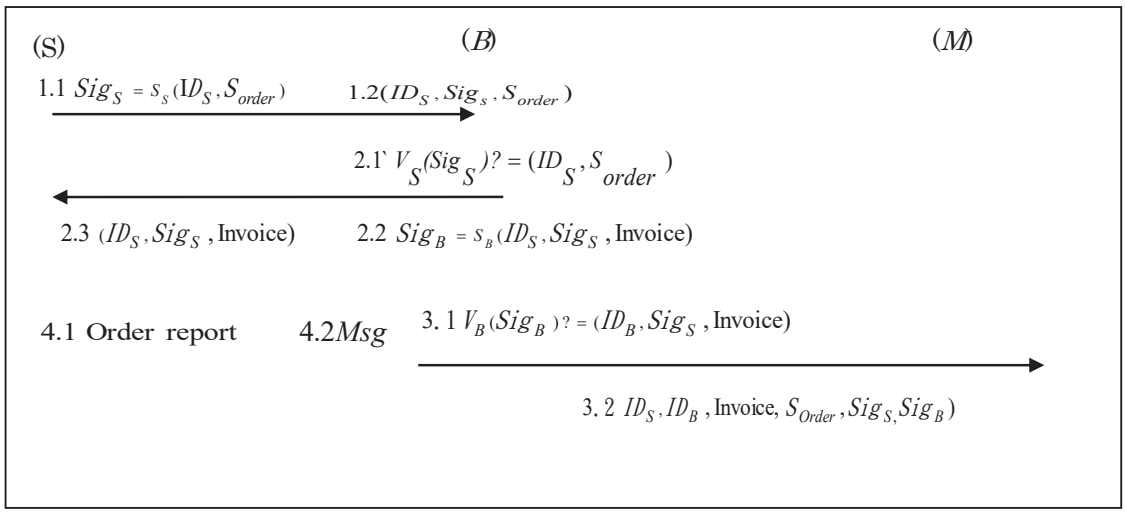

Fig. 3 The overview of the payment phase