北京郵電大學

Queen Mary University of London

Undergraduate Project Report
2018/19

Vcoin:A Blockchain Algorithm for Cryptocurrency

Name:	Wang Jieping
School:	International School
Class:	2015215120
QM Student No.:	151007028
BUPT Student No.:	2015213429
Programme:	Internet of Things Engineering

Date: 06-05-2019

Table of Contents

Abstract

A peer to peer electronic cash system will allow us to execute transactions and manage assets without the financial third party. Thus far, some famous cryptocurrency such as Bitcoin and Ethereum have designed feasible architecture to solve the problems. I try to propose a simple algorithm to build up a new electronic cash system which is called as Vcoin. Vcoin has the basic functions for the cryptocurrency and open-source for all users or developers. In fact, Vcoin is similar to Bitcoin because it stems from the Bitcoin .Vcoin will record all valid transaction with the timestamp and organize them into an ongoing chain. At the same time, the system will use the Pow(proof-of-work) algorithm to ensure the safety and consistency of Vcoin which will consume a great deal of CPU power to perform the hash computation to find the solutions. Once a node solves the hash function, it can get the power of adding blocks to blockchain. Moreover, Vcoin will hash all transaction and their blocks, so it will be impossible for attackers to tamper with the transaction data unless he modifies the whole blockchain. Simply speaking, CPU power is the key point for Vcoin system, the Vcoin system will keep the longest chain safe as long as a majority of CPU power are not malicious because a majority of CPU power can generate the longest chain. As for the network, Vcoin will runs on the P2P network and all nodes can leave or join the network at any time. All the transactions will be broadcasted over the P2P network. Certainly, Vcoin system will reach a consensus and maintain a global blockchain ledger over the network.

Key Words: Blockchain, Algorithm, P2P, Cryptocurrency

摘要

一种点对点的电子现金系统可以允许我们不通过第三方金融组织去执行交易并管理资产。目前为止，一些著名的加密货币像是比特币和以太坊就已经设计可行的架构去解决这些问题。我尝试提出了一种简易的算法来构建一种被称为 Vcoin 的新型电子现金系统，Vcoin 具有加密货币的一些基本功能并且对于所有使用者和开发者均是开源的。事实上，Vcoin 与比特币十分相似因为它的构想正是源于比特币。Vcoin 将会记录所有合法交易及其时间戳并将它们组织成为一个不断延长的链条。与此同时，系统将会使用 POW（工作量证明）去确保系统的一致性和安全性。这种机制会消耗大量的 CPU 算力来寻求哈希计算的解。一旦一个节点解决了哈希计算问题，它将会获得往链中添加新区块的权力。Vcoin 将会对所有的交易和区块进行哈希，所以对于攻击者而言篡改交易变得不再可能除非他可以修改整个区块链。简单来说，在 Vcoin 系统中 CPU 算力就是关键点，其将会保持最长链的安全只要大部分的 CPU 算力不是恶意的，因为大部分的 CPU 算力足可以产生新的最长链。至于网络，Vcoin 将会运行在 P2P 网络之上，所有的节点都可以随时加入或离开，所有的交易都会在网络中广播。当然，Vcoin 系统也将会在网络上达成共识并维护一个全局的区块链分类账。

关键词：区块链，算法，P2P，加密货币

Chapter 1: Introduction

Commerce on the Internet has come to rely almost exclusively on financial institution serving as trusted third parties to process electronic payments. But it is still a trust based model. Nowadays, the whole world is experiencing this kind of trustful crisis dejectedly. There is no doubt that we need a brand new model for transaction and economic system. That is why I want to develop algorithms for cryptocurrency.

In my project, I plan to design an architecture and algorithm for my cryptocurrency Vcoin. Then I will develop software based on this algorithm which will implement some basic functions of my design. As far as I'm concerned, it will contain 4 parts:

(1) A decentralized P2P network

(2) A public transaction ledger (block and blockchain)

(3) A set of rules for independent transaction validation and currency issuance (consensus rules)

(4) A mechanism for reaching global decentralized consensus on the valid blockchain(proof-of-work)

So I try to illustrate Vcoin architecture to make you understand the system easier. According to Figure1.1, you can see how I transform four parts into three layers to implement.

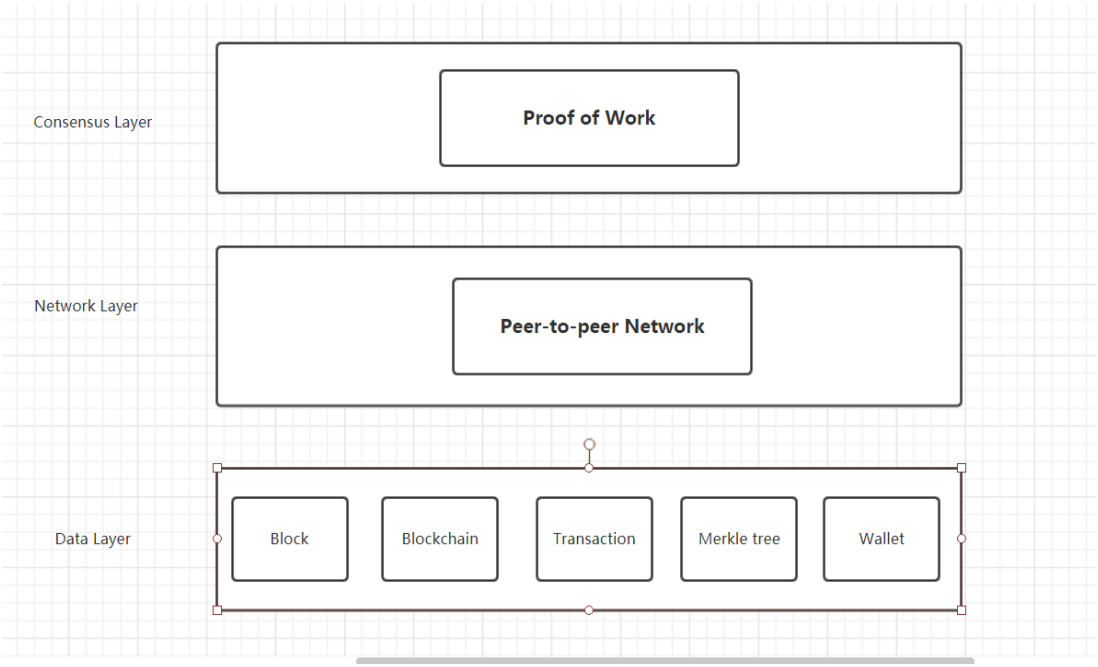

Figure1.1 Architecture of Vcoin

At first, about the P2P network in network layer, that is the most important part in my cryptocurrency. Because we don't have enough computers to simulate the P2P network, I choose to design a hybrid P2P network and implement some basic function in my software. My design of P2P network is hybrid model which consists of many centralized subnets and only one main network. That is because of the different roles of nodes. Some special nodes which are known as SPV node will connect to a full node to constitute a subnet which seems like a centralized network. SPV node will not maintain the whole blockchain because it just needs a small part of blockchain to verify its own related transactions which will be downloaded from full node. The full node, though, will maintain the whole of blockchain. In main network, there will be some full nodes and miner nodes which is similar to a pure peer-to-peer network. Full node will connect to each other and miner node will use CPU power to fight for the power of adding block to blockchain (it can get Vcoins in return). By the way, the network will also involve some issues like node discovery and block synchronization. However, in my software, I will implement it in a simple way. In reality, because the software will run on my computer, I will use port number and node ID to replace the IP address and implement a centralized model. All nodes will connect to a central node and download the longest chain from it. Certainly we can execute some transactions and start current node to finish the data synchronization to create a global blockchain ledger. You have to know that I just design the P2P architecture but I don't implement one.

Secondly, a public transaction ledger in data layer which means the blockchain is the basis of Vcoin system. I refer to the real Bitcoin system and simplify it to build up my own blockchain. The block will have some basic attributes such as timestamp and hash. However, to simplify the data structure of block, I will not pay attention to the block header and block body which are components of Bitcoin. Every blockchain will have a genesis block. Other blocks are added into the blockchain later by miner nodes. A blockchain will record all the transaction lists and it can't be modified once has been added to the chain. Some other useful mechanism will keep the blockchain consistent and safe which are known as merkle tree and so on.

Finally, consensus algorithms in consensus later and POW mechanism are related so we can talk about them together. I try to develop a POW algorithm to create Vcoin and reach a consensus. From my perspective, we shouldn't allow any nodes to add blocks into the blockchain because it may be malicious nodes which attackers can use a computer to create a lot of malicious nodes to attack the Vcoin system. However, this kind of attack which is called as Sybil attack can be solved by POW algorithm because even there are many nodes. There is

still one CPU and memory space. POW needs a difficult hash computation so only the real users can perform it. In my software, all transaction need to be proved by POW, the transaction can be valid only if the miner nodes find the solutions to hash computation successfully. Moreover, to reach a consensus, Vcoin system will broadcast all the transaction over the network and maintain a longest valid chain. All the valid transaction which haven't been added to blockchain will be put into a memory pool and wait for processing. Then the miner nodes get the accounting power and choose some transactions to create a block and add it into blockchain. Then the miner node will acquire some Vcoin which is known as block reward or Coinbase transaction. Unfortunately, that is the only way to create new Vcoin(it is also a great excitation mechanism).

So far, Vcoin has achieved all the basic conditions and functions for the cryptocurrency in business. The inspiration and general frame result from Bitcoin. However, it is still a nice try for me to create a new electronic cash system. You may think Vcoin system is obscure and I will introduce all the implementation and design in my report. In Chapter2, you can understand some basic concepts of technologies which are applied in my algorithm. In Chapter3, you can figure out my algorithm and design in details. And then in Chapter4, all the test results and screenshots will be illustrated. At the same time, you can compare Vcoin to some existing cryptocurrencies. In Chapter5, I will summarize my project and put forward my own perspective and reflection. Moreover, I will do some risk assessment and environment assessment later.

Generally speaking, Vcoin is a promising cryptocurrency implementation. It is combination of multiple technologies. However, its core idea is revolutionary. As a developer, you can download the source code and try to redesign and fork it. I believe that this kind of mechanism which represents cooperation, decentralization and freedom will be popular increasingly in the future.

Chapter 2: Background

As we all know, in essence, Vcoin and other cryptocurrency try to use the technologies to replace the third party to revolute the economic system. Obviously, our Vcoin system is related to many cryptocurrency basis and mathematic theory, now I will introduce them in my Background chapter

2.1: Basic Concept of Asymmetric Encryption

As the core technology in my design, there is no doubt that the concept of asymmetric encryption should be discussed. It is a basic concept of cryptography and adopted by many cryptocurrencies including Vcoin. Now I will introduce the asymmetric encryption to you.

In conventional encryption, we just use one secret key. But in asymmetric encryption, we will use a pair of secret key whose name are public key and private key. As the following picture, we can use the other's public key to encrypt the plaintext and only the nominated receiver can decrypt the ciphertext because it keeps the private key. Certainly, before the communication, All the participants can exchange their public keys for the encrypted communications.

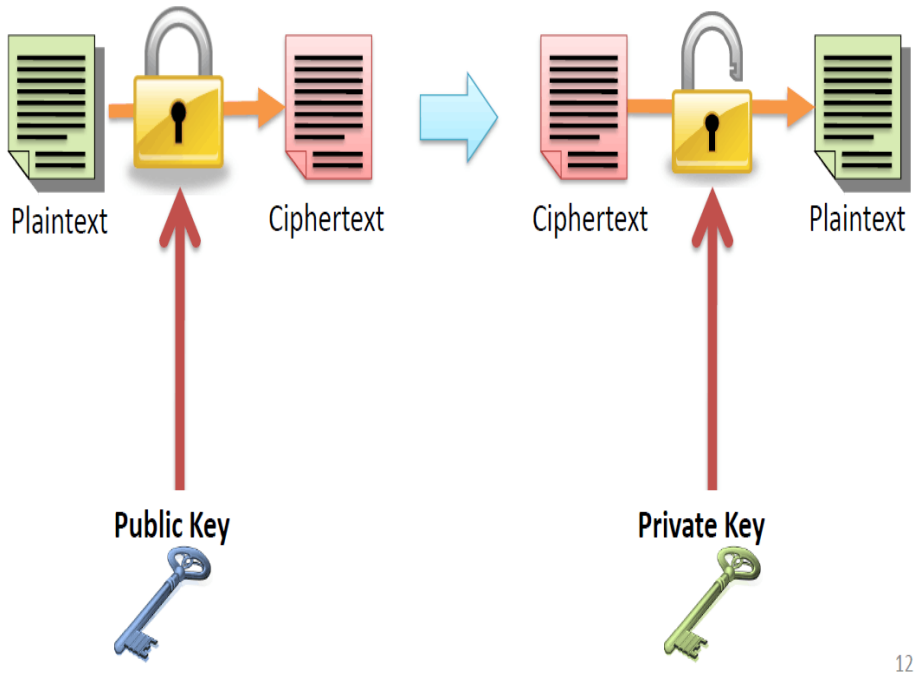

Figure2.1 Asymmetric Encryption

Actually, digital signature and ESDSA is related to the asymmetric encryption and we will introduce these technologies later.

2.2: Elliptic Curve Cryptography

An elliptic curve is the set of points that satisfy a specific mathematical equation. The equation for an elliptic curve looks something like this: $y^2 = x^3 + ax + b$.

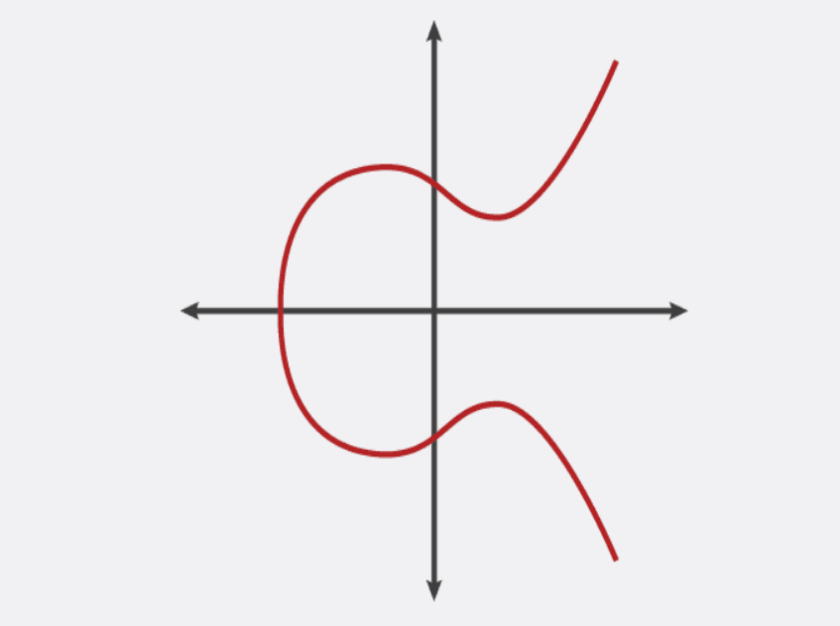

Figure2.2 Elliptic Curve

And the elliptic curve has some useful features. For examples, one of these is horizontal symmetry. Any point on the curve can be reflected over the x-axis and remain the same curve. A more interesting property is that any non-vertical line will intersect the curve in at most three places. Now we can image a condition. We take two points A and B on the curve and draw a line through them. Then we will find the other intersect point C' and the point C which is symmetric to the X-axis. Now we can name this kind of operation as "dot". That's to say, A dot B is equal to C. Moreover, we define a double calculation for the "dot". If we choose a tangent line which intersects with curve on point G. We can find the -2G and the symmetric point 2G.

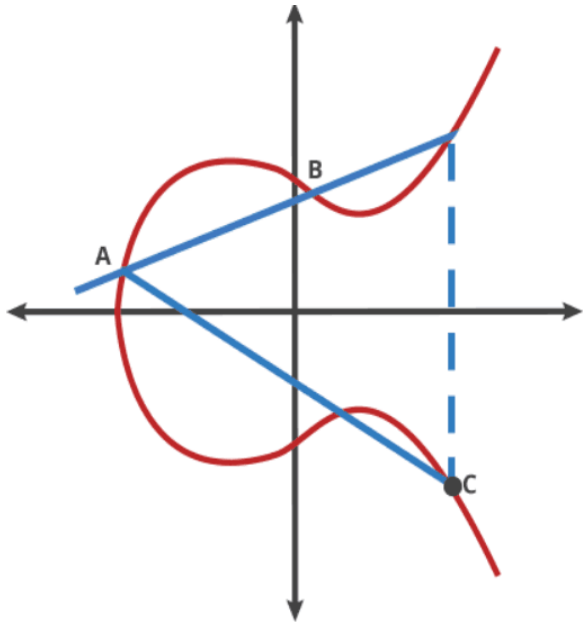

Figure2.3 “dot” operation on Elliptic Curve

Certainly, if we just use only one point to “dot”, we can do it many times and get many intermediate results. For instance, according to Figure2.4, we regard G as the initial point and do the “dot” operation many times to get 2G, 4G, 8G. That is the basic mathematic knowledge about ECC. It is impossible for us to find the times we do the “dot” and the initial point depending only on the final point Q(which is equal to NG). So we will regard Q as public key and N is our private key.

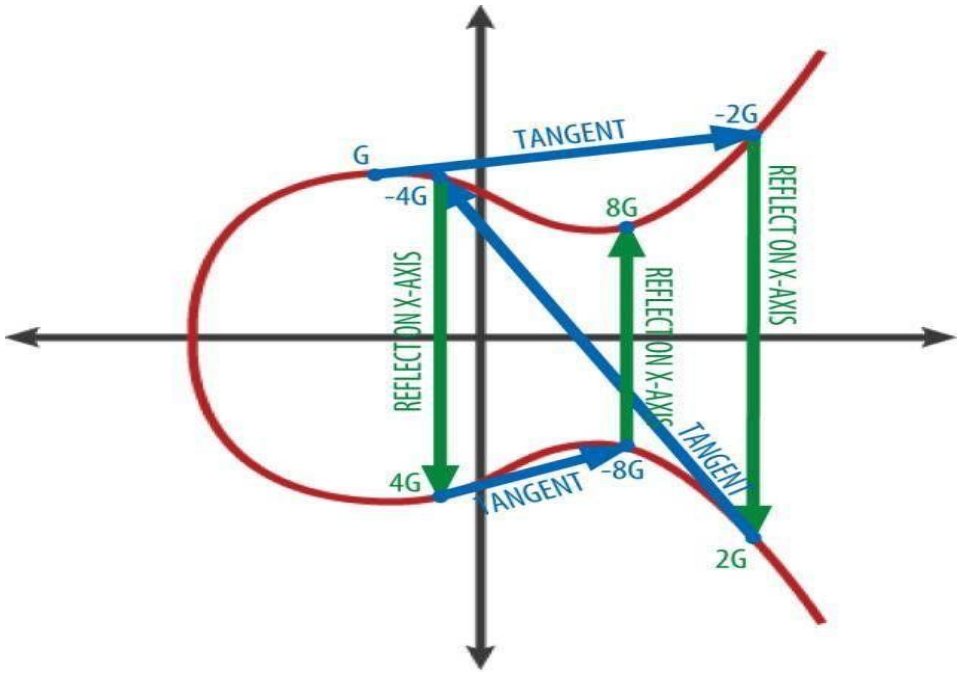

Figure2.4 How to get 2G, 4G and so on

2.3: ECDSA

ECDSA represent the combination of ECC(elliptic curve cryptography) and DSA(digital signature algorithm). Simply speaking, it is the implementation of DSA based on the elliptic curve. Because we have introduced the elliptic curve cryptocurrency, we will pay more attention to the digital signature algorithms (DSA).

Firstly, we should figure out what is the digital signature and its application in our cryptocurrency system. As a matter of fact, digital signature is a technology which results from asymmetric encryption. When we want to create a digital signature, we have to know our private key and the data you want to signature. Then the digital signature is created and the receiver will try to verify the signature. The verification needs the data and the public key of senders. Following picture is the signature and verification.

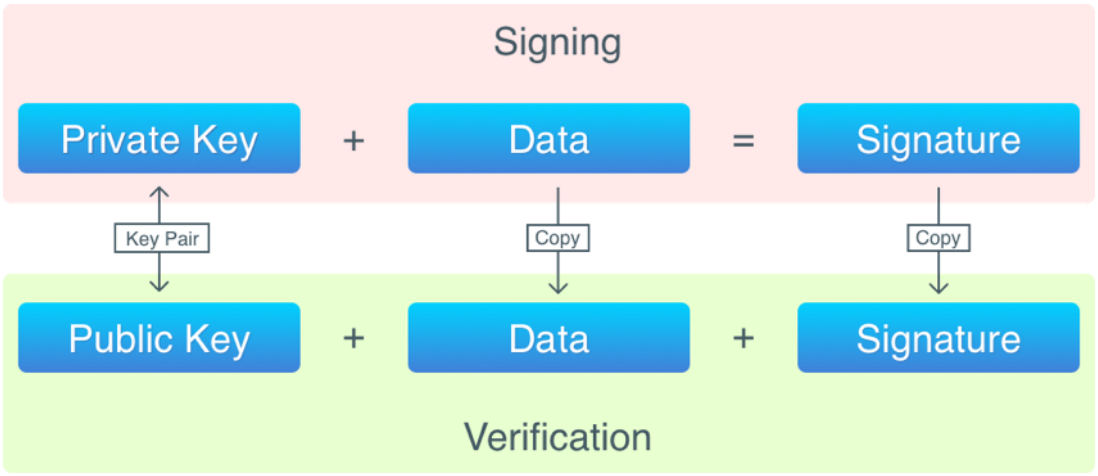

Figure2.5 Signing and Verification

As for the ECDSA, the basic principle is similar to the DSA. Now let me introduce the process of ECDSA.

Signature process:

(1)Select an elliptic curve Ep(a,b) and a base point G

(2)Choose the private key k, then use the base point G to create the public key K=kG

(3)Generate a random interger r, then calculate the point R=rG

(4)Regard the original data and the coordinate values of point R as parameters. Then calculate its SHA1 value. In other words, Hash=SHA1(original data, x, y)

(5)Calculate s=r-Hash*k(mod n)

(6)r and s will be the parameters of signature. That is to say, signature=(r,s)

Verification process:

(1)Receiver will receive the message M and signature (r,s)

(2)Calculate: sG+H(m)P=(x1,y1), r1=x1 mod p

(3)Verify the equation: r1=r mod p

(4)If the equation is true, we accept the signature successfully.

2.4: Base58 Encode

Base58 encode is a useful algorithm which convert binary data to visual string. The alphabet is“123456789ABCDEFGHJKLMNPQRSTUVWXYZabcdefghijkmnopqrstuvwxyz”. It is obvious that Base58 encode delete some letters and number (O, I, l and 0) to avoid confusion. The input of Base58 is a stream of [0,256) values and the output is a stream of [0,58). Then, refer to the alphabet for each value to get a visual string. Actually, the conversion process is a hexadecimal value converted to a 58 decimal value. In Vcoin system, Base58 will generate the Vcoin address.

2.5: BoltDB Database

As a ledger, it is impossible for us to store the data in the memory so we need a database. In Vcoin, BoltDB will be chosen and I will introduce why we use it and its basic principle.

BoltDB is a key-value database which means there are no lines, rows or tables comparing to the MySQL database(actually, it is a NoSQL database). It will support complete ACID transaction (atomicity, consistency, isolation, durability).The similar key-value pair will be stored in the same bucket. To get a value, we need to know its bucket and the key.

Chapter 3: Design and Implementation

3.1 The Architecture of Vcoin

To illuminate the Vcoin system, firstly, I will introduce the architecture of the Vcoin and then illustrate the main parts of it.

As shown in Figure3.1, I try to divide this system into three main layers.

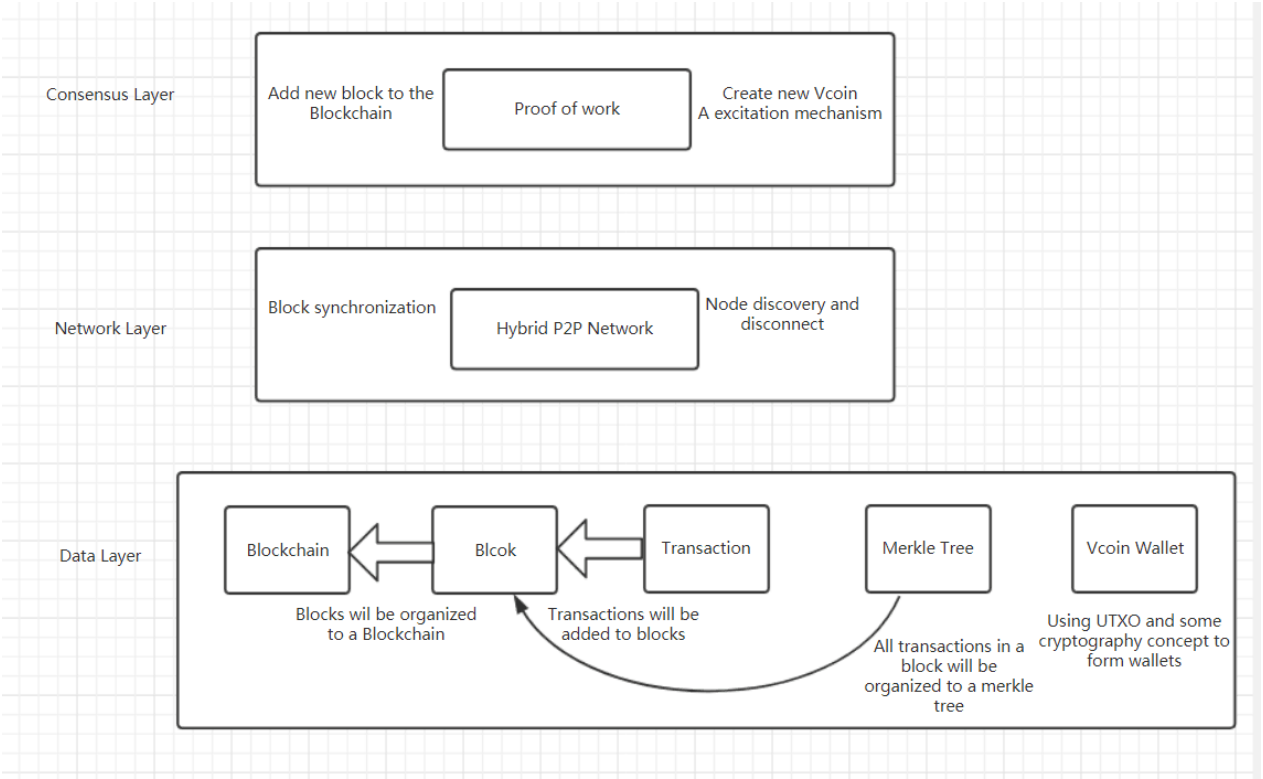

Figure3.1 Architecture of Vcoin(in details)

In this system, there are three layers which are known as data layer, network layer and consensus layer. Data layer will store the data and necessary data structure. Some valid transactions will be added to the block and organized into a mekle tree. All the block will be organized into a blokchain which known as a global ledger and no one can tamper with it expect attacker can modify all the blocks from the genesis block. Moreover, the wallet file will consist of all wallets on the node. A secret key pair will make up of a wallet where we use the asymmetric encryption. Network layer will be designed to a hybrid p2p network which consist some full node subnets (centralized) and a decentralized main network. The network will handle the node discovery and disconnection. At the same time, data synchronization and transaction broadcast will be accomplished in network. As for the consensus layer, we will adopt the proof-of-work algorithm to reach a consensus. In the process of consensus, the

blockchain will be longer and the new Vcoin will be created. Figure3.2 is directory of my software which I try to implement.

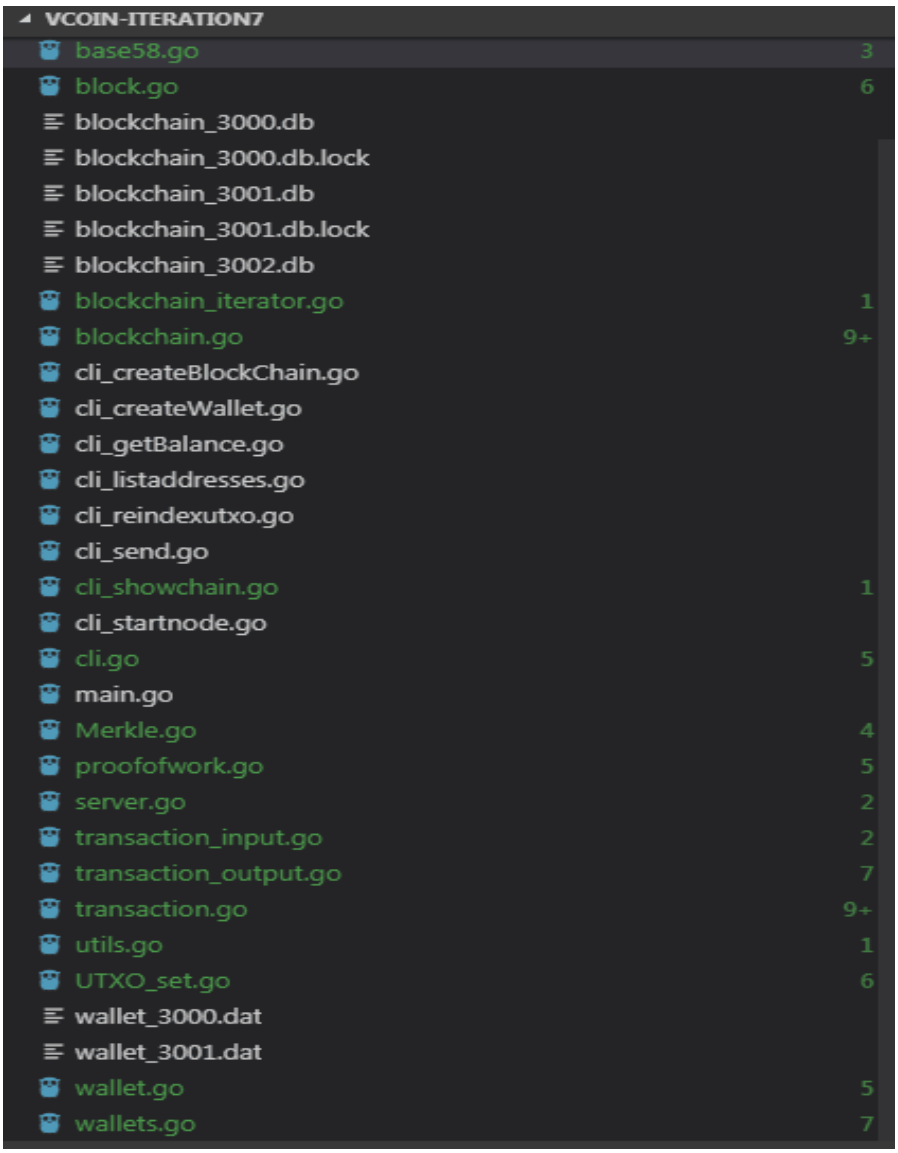

Figure3.2 Directory of Software

3.2 Block and Blockchain

As a distributed ledger, data structure of blockchain is one of the most important architecture. Some transaction will be organized into the block and all the valid block will be organized into a global blockchain. That is my data structure of block

```
type Block struct {
    Timestamp int64              //时间线，1970.1.1到现在有多少时间
    Transactions  []*Transaction //交易的集合
    PrevBlockHash []byte         //上一个块的哈希
    Hash          []byte         //当前区块的哈希
    Nonce         int            //工作量证明
    Height        int            //高度
}
```

Figure3.3 Data structure of Block

It will contain some useful attributes in the block:

(1)Timestamp: it represent the time when the block is created

(2)Transaction: it is the information about transaction which store in blocks

(3)PrevBlockhash: it is the hash value of the previous block

(4)Hash: it is the hash value of the block

(5)Nonce: it is a random value to find the solutions of the hash computation

(6)Height: length of the blockchain to verify whether it is the valid longest chain

In fact, blockchain is the real ledger which will store the data and it seems like a linklist which use hash pointers. All the valid block will be organize into a long chain and it is a global ledger that can record the whole historical transactions and states. In my Vcoin system, I will use the BoltDB database to store the blockchain rather than the LevelDB despite the real Bitcoin choose to use it. BoltDB is a typical K-V database.

About the function of every attributes, I will talk about it in details later(corresponding part)

3.3 Consensus Algorithms

The consensus algorithm is the core part of Vcoin system. In reality, it can not only reach a consensus in distributed system but also can be used to generate the new Vcoin which reserves the mintage. In my Vcoin system, I plan to choose a simple consensus algorithm based on the POW(proof of work). Its principle is a bit like the labor system in daily life. Every node can work hard to perform the hash computation and try to find the target solutions which will be fair and difficult enough. The first node which solves the puzzle will acquire the power of adding block to blockchain. Certainly, to encourage the miner, they will get a lot of Vcoin that is the only way to create new Vcoin(we will call it Coinbase Transaction).Now we can talk about the POW in details

To understand the POW, we should understand what is hash and hash value. Hash means the process to get the hash value of data. The different data will have very different hash value even there is only one letter difference. At the same time ,hash has the property of puzzle

friendly, collision resistance. It means that it will be impossible to get the original data from the output. In general, hash can be used to check consistency of data. In fact, some famous cryptocurrencies including bitcoin and ethereum choose the hash to guarantee the consistency of blocks which make it impossible to tamper with the block unless we modify the whole blockchain and their hash value.

In my opinion, Nakamoto Satoshi is a genius in that he uses the POW and it has a great influence on the cryptocurrency. The POW algorithms stem from the HashCash algorithm which is used to prevent email spam at first. HashCash algorithm is easy to prove but hard to solve, that is property of hash. We need to use a kind of difficult computation to prove that it is a real node that tries to maintain the blockchain in case the attackers create many malicious nodes which is known as Sybil attack. The logic of POW is not sophisticated. That is the simple pseudocode:

```
    Get(data)                                  //get the transaction data
    GetHash(data)                              //use the SHA256 algorithm to get hash
    Set Targets(target)                        //set a target bits for hash computation
    Int Nonce(nonce likes a counter)           //Nonce is random value, and it will be
                                               //adjust to meet targets
    For(Nonce==0;HashValue<targets;Nonce++){
      Hashvalue==GetHash(data+nonce)
      If(Hashvalue<targets){
            Return Pow true
      }
}                                              //adjust the Nonce until the targets is met
```

For example, I set the targets=16

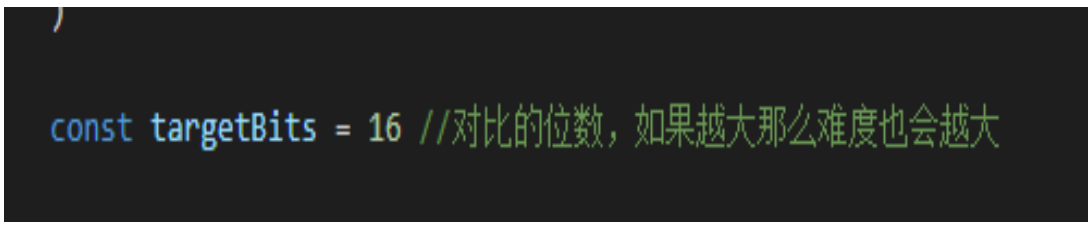

Figure3.4 Target bits

And then try to create a blokchain using the command line

Figure3.5 Create a Blockchain

The software will change the value of nonce and try to find a solution to meet with the target. In this kind of condition, you can see that the first four hex numbers are 0000.That is to say, the first 16 bits are 000000000000000 which satisfy the targets.

What's more, there is another significant thing which is called as block reward. Unfortunately, it is the only way to create new Vcoin and this kind of mechanism results from the Bitcoin and some other cryptocurrencies. It sounds like a sad story because seems like a difficult task to create more new Vcoins. But that is where Vcoin(and other cryptocurrencies) is revolutionary. No one can control the speed of creating the Vcoin and a new economic system will appear. Now we return to the technology topics under discussion. Block reward means any nodes which acquire the accounting rights can choose some transactions to organize them into a block and add block to the blokchain, then the node will be rewarded and get a lot of Vcoin. In fact, the block reward is equal to a Coinbase transaction when we try to implement it. Significantly, Coinbase transactions don't have the TXInput and we will talk about it when we introduce the transaction mechanisms.

3.4 Vcoin Wallet and Its Address

Compared to the other digital currency, there is a concept which we shouldn't ignore. That is the wallet .As a user, apparently, you want to know your asset at all times. In my Vcoin system, I design a wallet and accounts based on some cryptocurrency knowledges. I will introduce some basic theory of them but not prove them, after all they are not the key points of our Vcoin.

In our Vcoin, the identification is a pair of secret keys which is the concept of asymmetric encryption. Every user will keep a public key and a private key. In essence, Vcoin wallet is a pair of secret keys. When we use the command line to create a wallet address, the secret key will be created at the same time. Remember, anyone who own your secret keys can seize your property. Unfortunately, private keys and public keys are just random sequence of bytes, thus they can't be read by human. So we should use an algorithm which is called Base58 to convert public keys into a readable

format. About the Base58 algorithm, it is used to convert the data formats (it is similar to Base64).Following is the procedure to generate the address

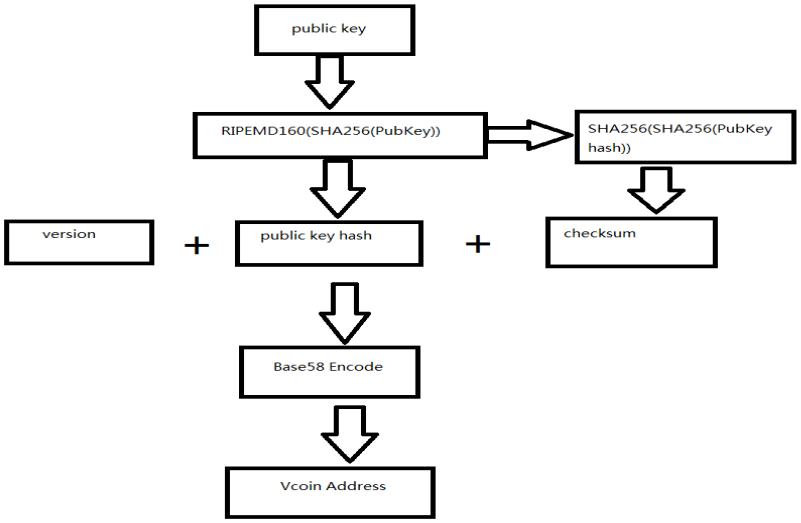

Figure3.6 Generate Vcoin address

Now we know how to convert the public key format. But we are supposed to pay more attention to the procedure of creating the public/private keys. That is a mathematical question. Actually, we use the ECC algorithms to create private key. ECC is Ellipse Curve Cryptography. Actually, it is a difficult mathematic theory to generate a big random number and the private/public key. The advantage of ECC is that ECC can ensure the private key is unique. About the details and proof of ECC, you can refer to my background chapter.

That is an example of Vcoin address: 1CmrUZyQVPTXdkeFyXfm9CSDKebbVcrrwD

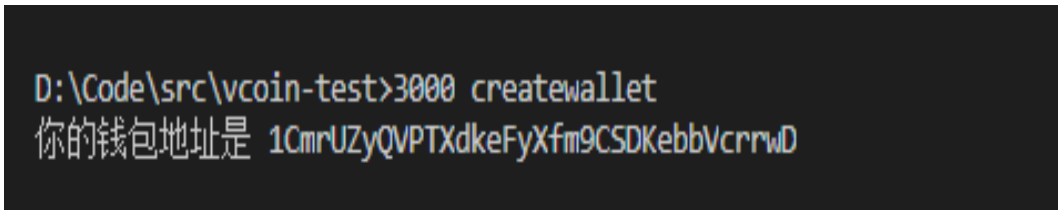

Figure3.7 An example of Vcoin Address

3.5 Transaction

As a cryptocurrency system, we must ensure the circulation of Vcoin. Certainly, it needs the transaction mechanism. From my perspective, Vcoin will use the very different concepts of transactions. Because Vcoin will be open-source, we don't want to store more sensitive information. So there will not be accounts, balance, customers or something else. We just store the transaction information and use it to build the whole Vcoin system. Then again, from the Vcoin perspective, there are no accounts or balances, it just can understand the transaction

list. As for the accounts and balance that we see on the screen, they are the results which we deal with.

When we talk about the transactions mechanism of Vcoin in details, we'd better to know some problems about traditional digital currency. That is the double spending which means the attackers can use the digital cash twice or more because the digital currency is just a file that we can copy many times. To solve this problem without third party, Bitcoin come up with a great idea which we will adopt in our Vcoin. According to the idea, In the Vcoin sytem, there will no real accounts and balance. All the accounts and balance are the results based on the UTXO(unspent transaction output). It may be an obscure word for us,. Now I will introduce my Vcoin transaction part for you.

From the beginning, we should know that a transaction in Vcoin system is just a well-defined structure. There are important parameters, input and output

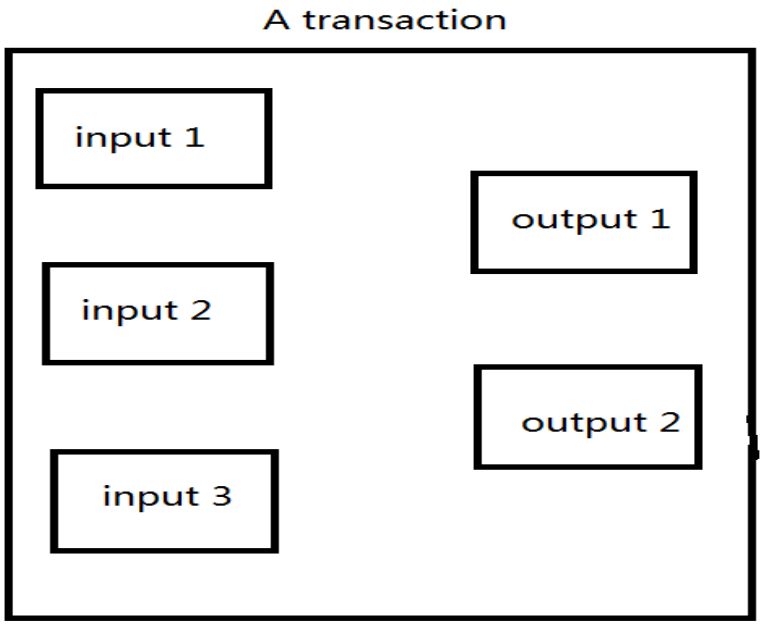

Figure3.8 Transaction Structure

In transactions, inputs represent the accounts which pay the Vcoin. Certainly, outputs represent the accounts which receive the money. More importantly, all inputs should be relevant to the former outputs besides one kind of special transaction which is called as Coinbase transaction (we will discuss it later). The benefit of this kind of design is that the system will know all sources of money and it will prevent from double-spending because it is impossible for attacker to modify the historical data.

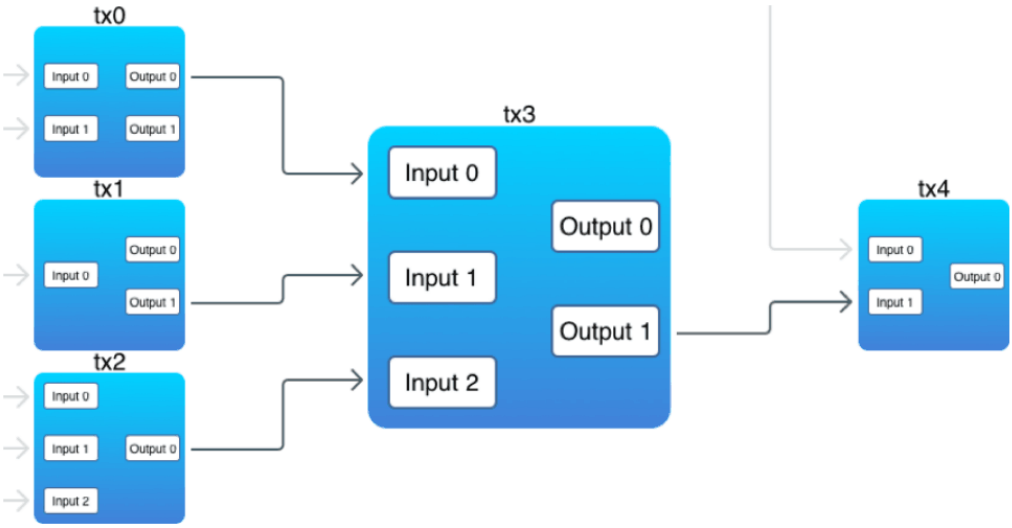

Figure3.9 Transaction inputs and outputs

There is a common condition we need to pay attention to. When an output is smaller than the input, we need to use another output to represent the paying party which is similar to give change. As mentioned before, there is not only one kind of transaction in Vcoin system. Coinbase transaction and normal transaction are different. Coinbase transaction has a null input which will not be relevant to any transaction output t because it is the block reward. That is the biggest difference between Coinbase transaction and normal transaction.

Now we start to understand the basic concepts of Vcoin transaction. But we don't know how to use inputs and outputs to find the balance of accounts. Actually, it is an easy work for us. In theory, we can use all the unspent transaction outputs which are known as UTXO to define the balance. You may have noticed that not all outputs are related to inputs because some outputs haven't been "spent". If we can add the outputs which an account doesn't spend together, we can get the balance of that account. For example, according to the figure above, there are four unspent transaction outputs in UTXO set: (1) tx0, output1; (2) tx1, output0; (3) tx3, output0; (4) tx4, output0. In the whole Vcoin system, traversing the UTXO set is the way to query balance.

3.6 Merkle Tree

After the transactions, we must put forward a specialized data structure which is known as merkle tree and we will use it to index transactions. But why we need a merkle tree? As I have mentioned before, there is a peculiar SPV node which means simplified payment verification. That is to say, nodes don't need to get the whole of blockchain to verify one transaction. As a

SPV node, we are still concerned about the paying party and recipient party. So if we can propose a plan that just need a small part of blockchain to verify a transaction, we can save time and memory. Therefore, merkle tree is adopted.

Merkle tree is similar to a binary tree but I will use the hash pointers. According to the Figure3.10, all the leaf nodes (from a to g) are transactions and the other nodes are just some nodes store hash value. By hash transaction a and transaction b, we can calculate the H(ab) and regard it as the father node of a and b. As the same reason, a complete merkle tree can be built until the root has been created. In Figure3.11, we know that we will use the SHA256 algorithm to handle the transactions. If the transactions are odd, we need to copy the last transaction and keep the number even to build a merkle tree.(only in tree, not in block)

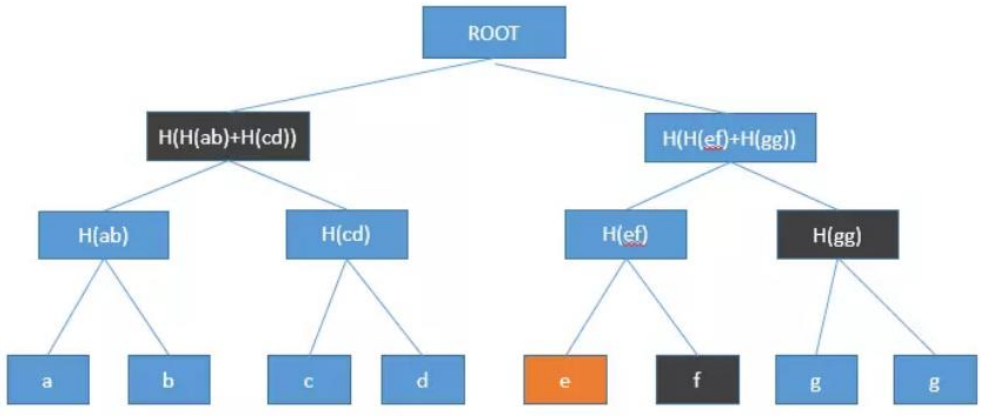

Figure3.10 Merkle Tree(1)

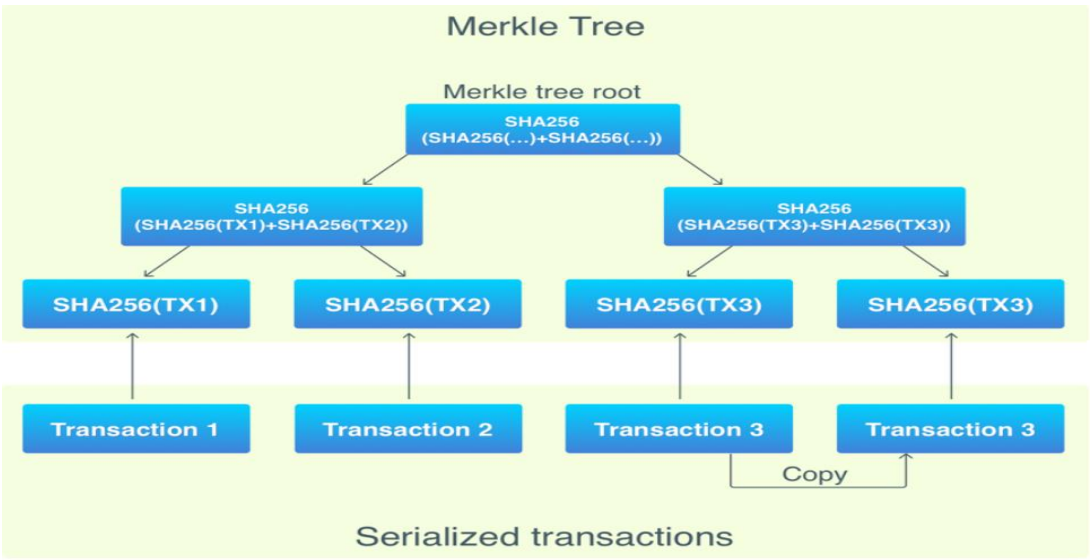

Figure3.11 Merkle Tree(2)

Once the merkle tree has been created, we can try to verify the transaction without the whole blockchain which will base on merkle path. Merkle path is a very simple concept. We assume that we have stored all the hash value in merkle tree. Then we want to verify the transaction “e” in Figure3.10. Now we will try to get the black nodes in tree which are transaction “f”, H(gg) and H(H(ab)+H(cd)). After that, we should find the path from transaction “e” to the root and try to verify the root hash value. In Figure3.12, that is the merkle path.

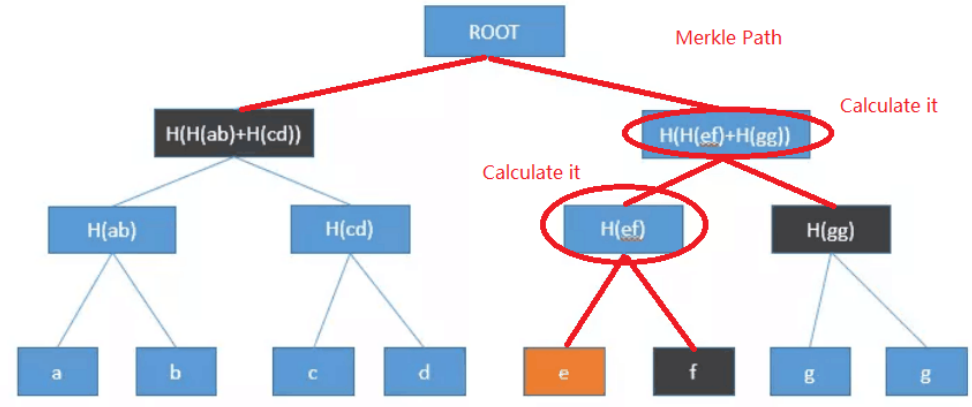

Figure3.12 Merkle Path

3.7 P2P Network

For the cryptocurrency, a peer-to-peer network is essential. I try to design a P2P network model for my Vcoin cryptocurrency system. As we all know, P2P means all the nodes are peers in the network. The nodes need to communicate with each other and cooperate with each other. The most difficult task for peer-to-peer network is how to handle the changes of node state and data synchronization without a third party

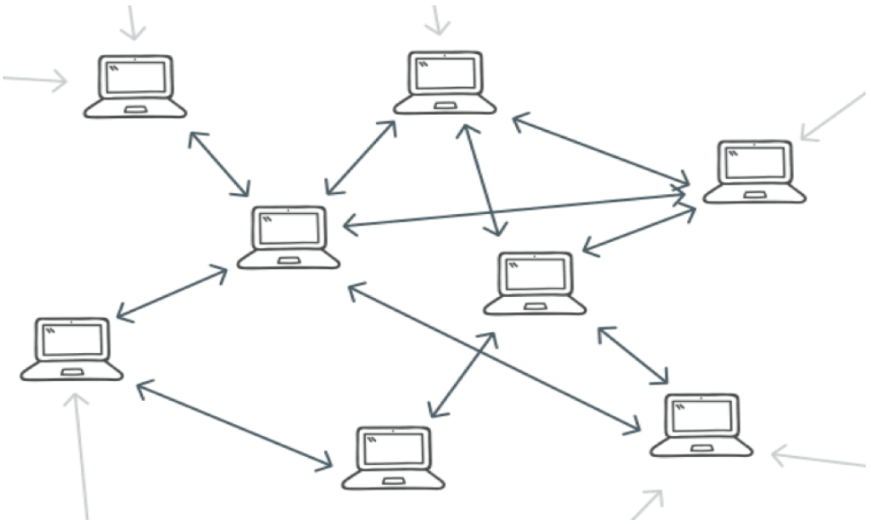

Figure3.13 Traditional P2P Network

Now I will illustrate the topology of my p2p network. In this architecture, it is a flat topology so there are no layers. In this picture, we can know that there are 3 main kinds of nodes in the p2p network which will perform the different roles in Vcoin system. There are (1)Full node, (2)SPV node and (3)Miner node. Full node means that the node will maintain the whole of blockchain and have the ability to verify the transaction which can prevent from being attacked by double spending. SPV node is special node which is known as simplified payment verification. As a normal user, we don’t need to care about the global ledger. We just want to know something related to our accounts. So SPV will not maintain the whole of blockchain and it will download the necessary information from the full node such as hash values of merkle roots to verify the validation of transactions. Moreover, there are some nodes to use their CPU power for the block reward which we call miner nodes. They just try to solve the hash puzzle and fight for the power of adding blocks to blockchain. Miner node would better to maintain the global ledger. Certainly, a full node can become a miner and we can regard a miner node as a special full node. In fact, because of the different roles in network, I don’t think that a pure peer-to-peer network is a good idea for my design. So I try to put forward a hybrid P2P network in the Figure3.14.

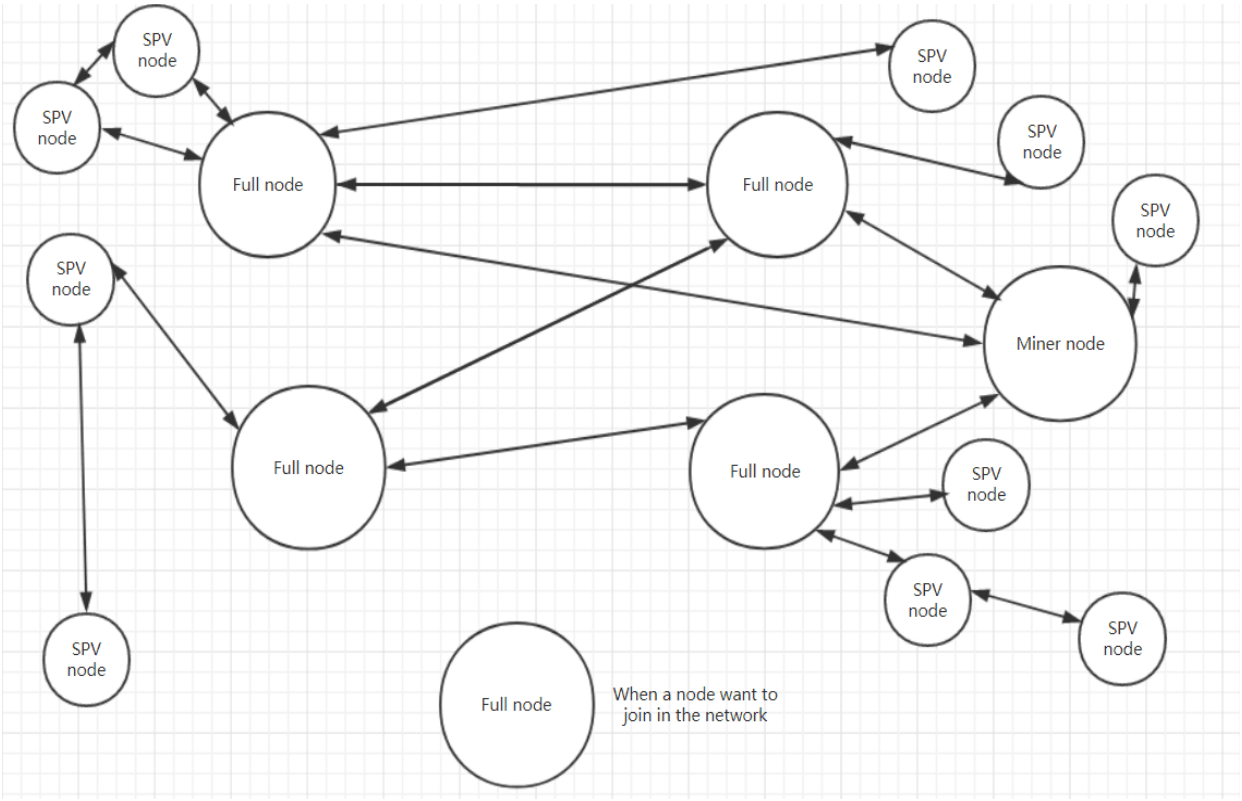

Figure3.14 Vcoin P2P Network Topology

Besides the roles of nodes, we can find that the specialized design for this architecture. The full node seems like a “super node” which is connected to many SPV nodes because they will download a part of blockchain data from “super node”. Moreover, miner nodes don’t need to waste bandwidth to handle the network communications but it surely has this kind of ability. All the super nodes will be organized to a decentralized P2P network. However, for the SPV node which belongs to a super node, they will be more centralized. This kind of design is a hybrid P2P network that is flexible and easy to implement.

In this hybrid P2P network, we can pay attention to the centralized subnet and decentralized main network. The centralized subnet consists of many SPV nodes and a “super node”. The only “super node” will maintain the list of SPV nodes which seems like a server. All the SPV nodes which belong to the ‘super node” will forward the transaction data to the “super node” and the super node will create a transaction pools to save all transactions that haven’t been added to blockchain. At the same time, if a SPV node needs one of the block information to verify the transaction, it will download what it needs from the full node. That is why a “super node” must be a full node. In Figure3.15, you can see the centralized architecture of “super node” subnet. It is also important to note that a SPV node can connect to full node directly and it is also able to connect to full node through other nodes which depends on the network

state. In fact, we just need a path from SPV node to full node to download the data.

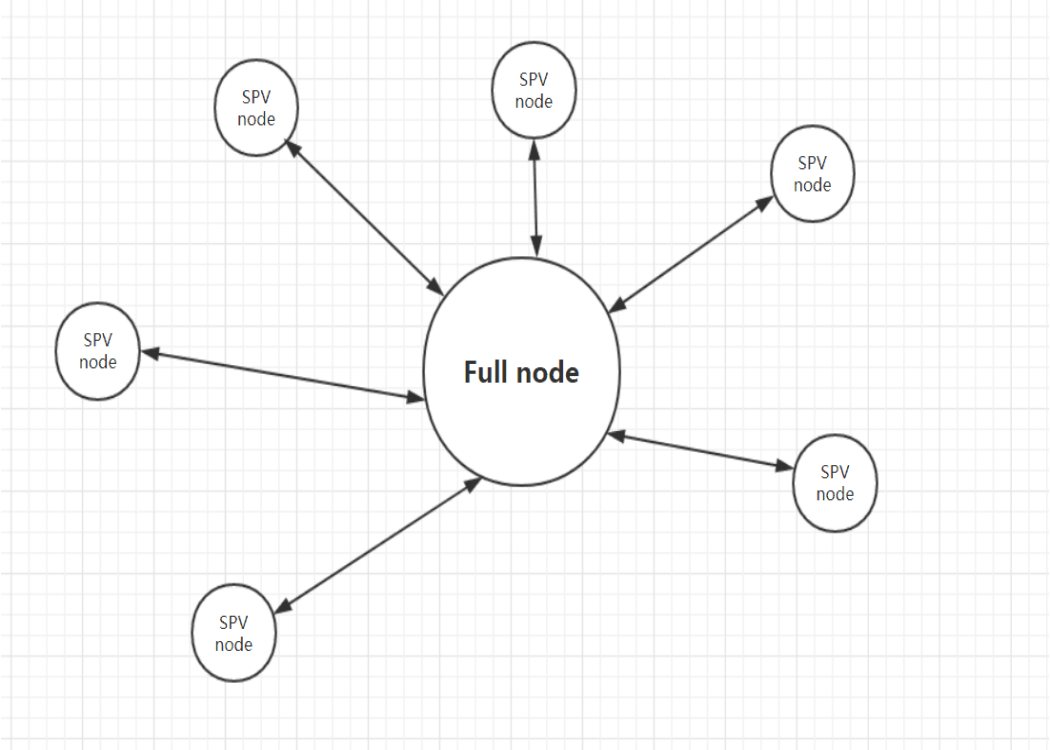

Figure3.15 “Super node” Subnet

However, decentralized main network is very different from the “super node” subnet. From perspective of full nodes and miner nodes, this is more like a pure P2P network. After all, the network is unstructured and decentralized enough. All full nodes will maintain the blockchain and have the global perspective of UTXO and so on. Full node has functions such as wallets, miner, router and storage of blockchain. Generally speaking, full node must be more powerful than SPV node because it has to handle the transactions which result from all SPV nodes. However, every node has different memory and bandwidth. So I propose an idea. SPV node should test the capability of processing information and choose the suitable “super node” when this SPV node joins in a full node subnet. By this way, the full node in main network will achieve load balancing. For example, I want to create a full node on my laptop and an internet company create a full node on large computer system. It is possible that just one or two SPV node will connect to my full node on laptop and thousands of SPV nodes will choose the large computer system because the computer power of my laptop is far below the counterpart of large computer system. In Figure3.16, you can see the main network architecture clearly.

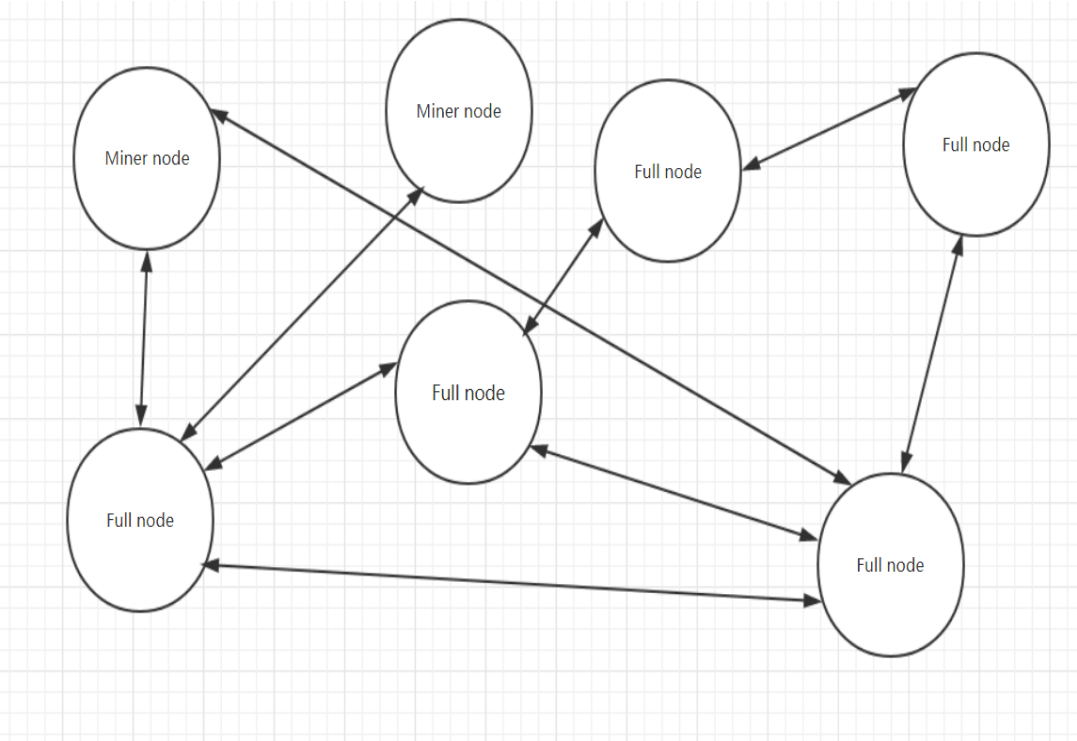

Figure3.16 Decentralized Main Network

As a peer-to-peer network, a node can join in the network at any times and that is the first step to understand the p2p network. Because it is a hybrid P2P network, we will figure the process out from two networks. As a fresh new node in main network, you have to join in the network and get information about other nodes in network. The way is using the DNS seed. DNS will be hardcode in source code which will provide new nodes with IP address of some stable Vcoin node. It is worthwhile to note that DNS seed is not the real node in network. It is just a DNS server that knows the addresses of nodes. Actually, if we use the real nodes as seed nodes, the seed nodes will run the risk of being attacked which results in a terrible fact that new nodes are unable to join in the p2p network. When new node find IP addresses of other nodes, it can try to send messages which contains their own IP address to other nodes so that other nodes are able to know their existence. The later process is similar to passing balls. The neighbour will, in turn, forward the message to their neighbours, ensuring that the newly connected node become well known and better connected. During the process, the basic connection has been build and that is the node discovery in my Vcoin network. Certainly, it is different when we talk about the node discovery in subnet. After previous processes, a SPV node finds enough full nodes in main network. It will choose the node which has low load and latency then try to connect it. Finally the new SPV node just needs to maintain the connection between its own and “super node” which represents the new SPV node has been discovered by full node.

After the node discovery, we should pay attention to another key point in p2p network which is data synchronization and communication. There is no doubt that node communication is the first problem we need to solve. In my Vcoin system, I think nodes will use the message to implement the communication. In addition, we will use the TCP protocol to build connection. There are many kinds of messages in my Vcoin system. For examples, version messages, inv messages, data message and so on. I will analyse messages in details.

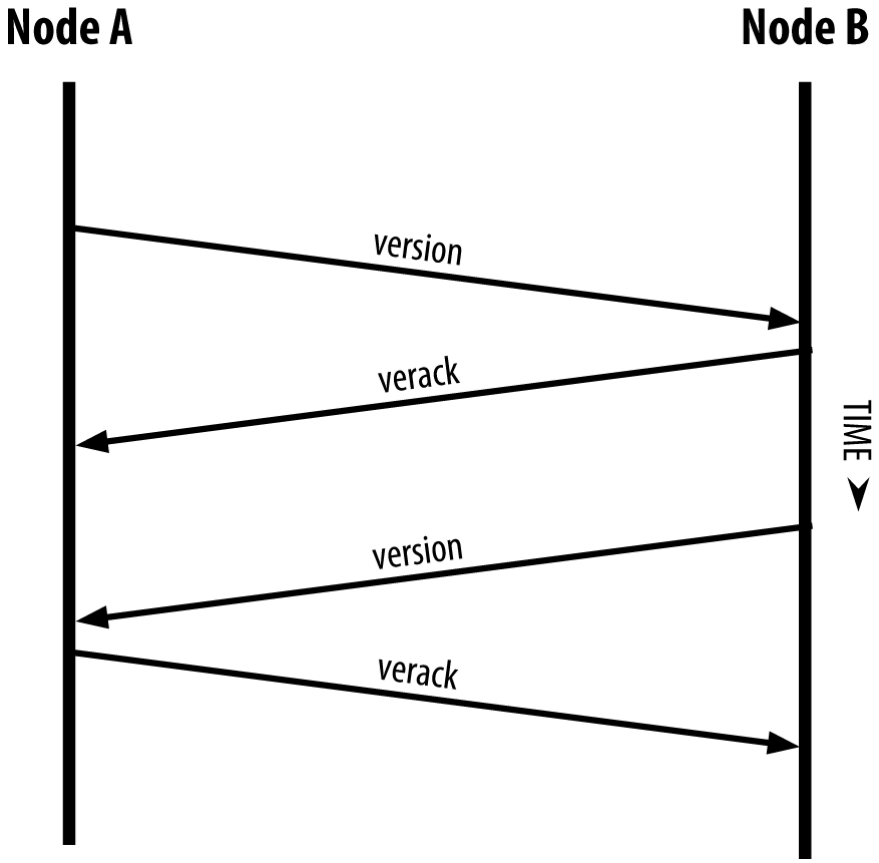

Figure3.17 Version message

According to the Figure3.17, version message is the first message we will handle when we first join in the network. If a new node tries to join in the network, it will send version message to the known node. The message will be responsible for telling peers version of blockchain and some basic information such as the length of blockchain. Version message can be used to find a longest chain in network. If a node receives the version message, it will check BestHeight filed which means the length of blockchain. Once the node finds the longer blockchain, it will send the getblock command which is used to receive blocks from longer blockchain.You can see the attributes in my software in Figure3.18.

```
54  type verzion struct {
55      Version    int
56      BestHeight int
57      AddrFrom   string
58  }
59
```

Figure3.18 Version message in my software

Furthermore, there is an absolutely necessary message in my design. As I have mentioned before, after a fresh new node find known node, it will query nodes which the known node knows. So we need a getaddress message to complete the process. In Figure3.19, we should find that the new Node A will tell the known Node B its IP address by the addr message. And Node A will query other node by message getaddr. Then Node B will tell Node A IP address which belong to other known nodes. However, in my software, I will use the port number and NodeID to simulate the IP address, so there are no this kind of process or these messages.

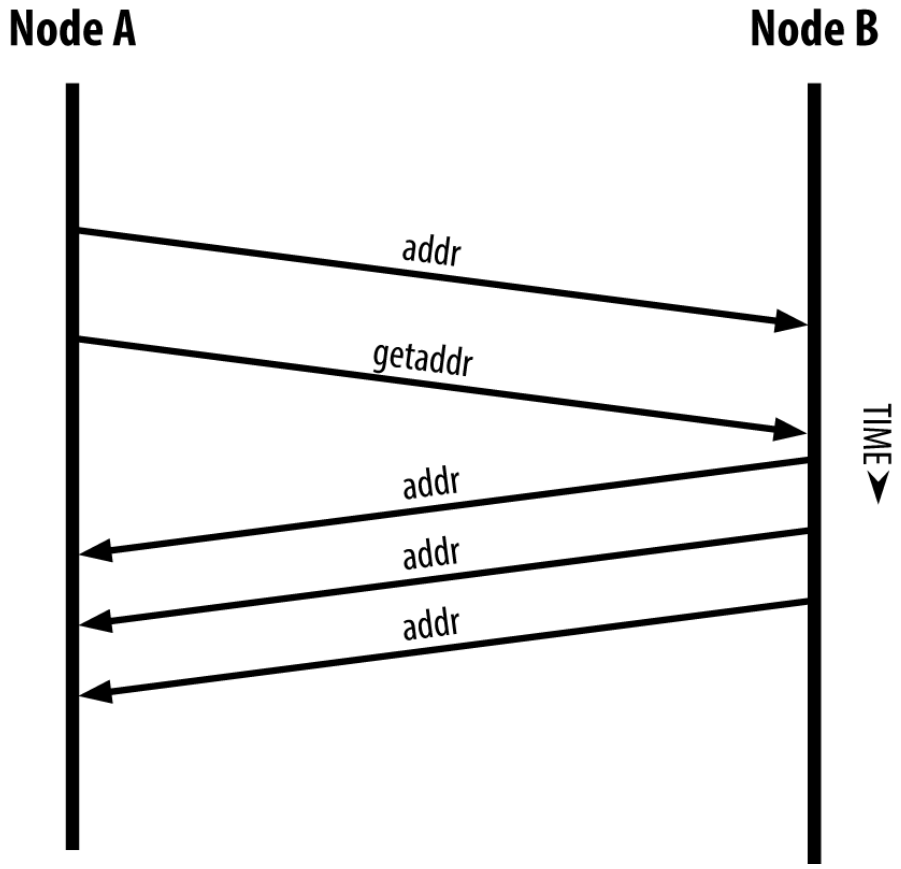

Figure3.19 IP address discovery and transmission

In addition, inv message is also important in Figure3.20. We assume that Node A is new node and Node B is older node which represent that Node B has the longer blockchain. When a new node finishes the node discovery and connection (we assume that it is a full node), it will start to get missing blocks and try to build a complete blockchain. At first they just know the

genesis block and it will check the BestHeight to ensure that it does lack some blocks by version message. Then they will exchange the getblock message which contains hash value of top blocks on their local blockchain. One of the peers will be able to identify the received hash as belonging to a block that is not at the top, but rather belongs to an older block, thus deducing that its own local blockchain is longer than the counterpart of peers. After that, Node B will send the inv message to show all blocks it has. Then Node A will send getdata message to request that Node B send blocks to it.

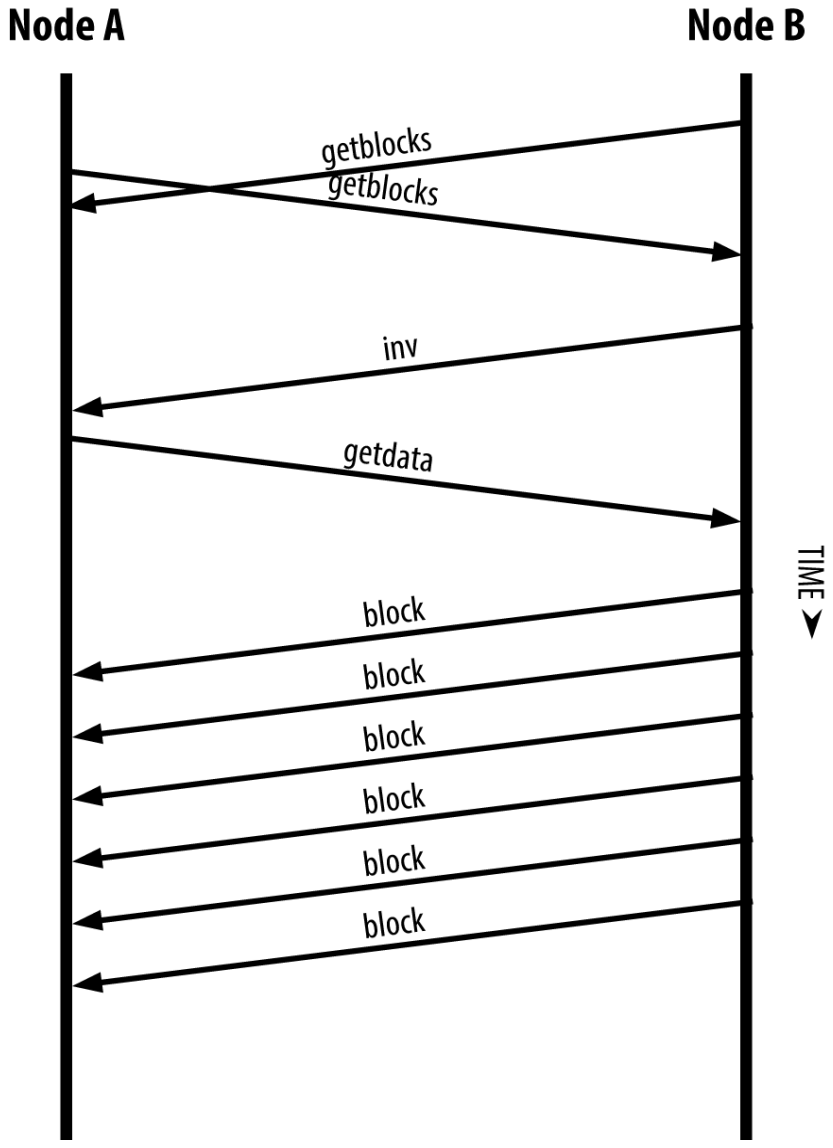

Figure3.20 Block Synchronization

In Figure3.21, you can know the inv message in my software.

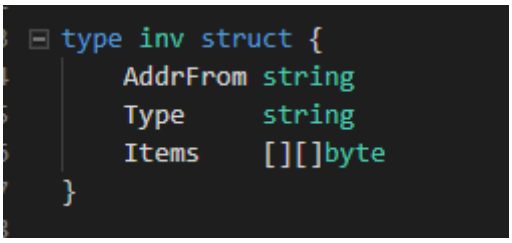

Figure3.21 Inv message

Until now, the node finish many processed in network and it want to disconnect from network. In fact, the node can cut off connection without informing any nodes. If there is no traffic on a connection, its peer nodes will send messages to maintain the connection. And if a node doesn't communicate with other nodes more than 90 minutes, it will be assumed that the node has been disconnected and a new peer node will be sought. Thus, the network can adjust its topology dynamically without any central control.

That is all my design of P2P network. In my software, I achieve some main functions in a special situation such as data synchronization. All other wallet nodes will connect to a well-known central node without node discovery and exchange the version message to identify longest valid chain. Once a wallet node needs to download the chain, it will receive inventory message from central node and send getblock message. Then the wallet node is going to receive all the blocks and add them to their own local blockchain. Finally, the blcokchain in network will be consistent. All above are my design and implementation and I will show my test results later in Chapter 4.

Chapter 4: Results and Discussion

4.1 Running the Vcoin and test it.

Now I will briefly show some test data and screenshots to make you understand my Vcoin system easier. Moreover, there are three kinds of nodes, so I plan to create three CMD to simulate it.

CMD1 is central node(like “super node” in network and will perform the mining process)

CMD2 is wallet node

CMD3 is another wallet node (in reality, there are all full node)

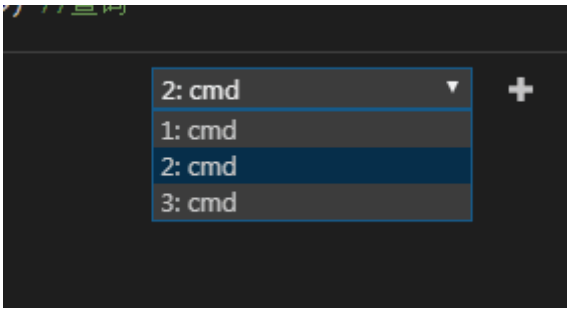

Figure4.1 Three kinds of Nodes

Step1: Creating a central node and use it to create a new blockchain

We name the central node as “1” which means the node id=1

```
欢迎使用我的区块链加密货币 Vcoin
Welcome to my Vcoin system


使用方法如下
listaddresses                    显示所有账户
createwallet                     创建钱包
getbalance -address              你输入的地址 根据地址查询金额
createblockchain -address        你输入的地址 根据地址创建区块链
send -from From(转出的地址) -to TO（转入的地址） -amount Amount（输入金额） 转账 -mine
showchain                        显示区块链
reindexutxo                      重建索引
startnode -miner ADDR            开启一个节点

D:\Code\src\vcoin-test>1 createwallet
你的钱包地址是 17UYUGFqw3xSnrsvkyMbYgwgNiP88EMzk1

D:\Code\src\vcoin-test>1 createblockchain -address 17UYUGFqw3xSnrsvkyMbYgwgNiP88EMzk1
00009c5a1f351ddf31c8a001164de7f1b323347bb2892d3185227498734ebb7e


创建成功
```

Figure4.2 Create Wallet and Blockchain on Node1

Then we can find that a wallet file and a database file which store the blockchain

Figure4.3 Wallet File

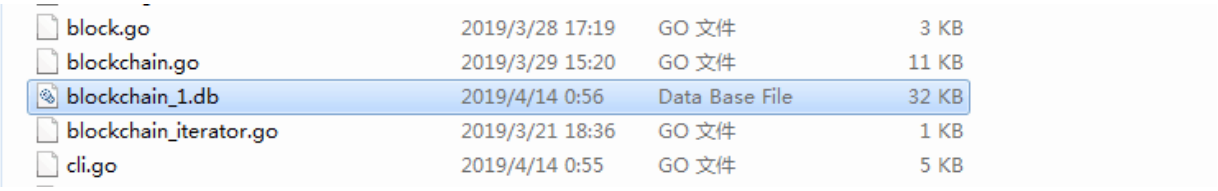

Figure4.4 Blockchain Database File

Step2: Creating some wallet address

We name the wallet node as “2” which means the node id=2

And we try to create two new Vcoin wallets.

```
D:\Code\src\vcoin-test>2.exe


欢迎使用我的区块链加密货币 Vcoin
Welcome to my Vcoin system


使用方法如下
listaddresses                    显示所有账户
createwallet                     创建钱包
getbalance -address              你输入的地址 根据地址查询金额
createblockchain -address        你输入的地址 根据地址创建区块链
send -from From(转出的地址) -to TO（转入的地址） -amount Amount（输入金额） 转账 -mine
showchain                        显示区块链
reindexutxo                      重建索引
startnode -miner ADDR            开启一个节点

D:\Code\src\vcoin-test>2 createwallet
你的钱包地址是 1CnxXNXH49NJWTQu82Sbb4z4BSH2mXcGYH

D:\Code\src\vcoin-test>2 createwallet
你的钱包地址是 1PMGKoLa3C6VETMHCVGXUw8gG6vwuZEYWz
```

Figure4.5 Create Wallets on Node2

Then we will copy the database file three times and rename them

2.exe	2019/4/14 0:55	应用程序	4,353 KB
3.exe	2019/4/14 0:55	应用程序	4,353 KB
base58.go	2019/3/16 15:16	GO 文件	2 KB
block.go	2019/3/28 17:19	GO 文件	3 KB
blockchain.go	2019/3/29 15:20	GO 文件	11 KB
blockchain_1.db	2019/4/14 0:56	Data Base File	32 KB
blockchain_2.db	2019/4/14 0:56	Data Base File	32 KB
blockchain_3.db	2019/4/14 0:56	Data Base File	32 KB
blockchain_iterator.go	2019/3/21 18:36	GO 文件	1 KB
cli.go	2019/4/14 0:55	GO 文件	5 KB
cli_createBlockChain.go	2019/3/28 22:17	GO 文件	1 KB
cli_createWallet.go	2019/3/28 22:18	GO 文件	1 KB
cli_getBalance.go	2019/3/28 22:19	GO 文件	1 KB

Figure4.6 Copy Three Database File for Nodes

Step3: Execute some transaction on central node

Now we can get balance of central node (because we create the genesis block and blockchain and get the block reward)

```
欢迎使用我的区块链加密货币 Vcoin
Welcome to my Vcoin system


使用方法如下
listaddresses                    显示所有账户
createwallet                     创建钱包
getbalance -address              你输入的地址 根据地址查询金额
createblockchain -address        你输入的地址 根据地址创建区块链
send -from From(转出的地址) -to TO（转入的地址） -amount Amount（输入金额）  转账 -mine
showchain                        显示区块链
reindexutxo                      重建索引
startnode -miner ADDR            开启一个节点

D:\Code\src\vcoin-test>1 getbalance -address 17UYUGFqw3xSnrsvkyMbYgwgNiP88EMzk1
查询金额如下17UYUGFqw3xSnrsvkyMbYgwgNiP88EMzk1 : 1000
```

Figure4.7 Balance of Central Node1

Then we try to execute some transactions on central node

```
D:\Code\src\vcoin-test>1 send -from 17UYUGFqw3xSnrsvkyMbYgwgNiP88EMzk1 -to 1CnxXNXH49NJWTQu82Sbb4z4BSH2mXcGYH -amou
nt 50 -mine
00005e9d8c4f0de3b525b5d5835580a060bd96d6279c89ba27b3a50449b9af14


交易成功

D:\Code\src\vcoin-test>1 send -from 17UYUGFqw3xSnrsvkyMbYgwgNiP88EMzk1 -to 1PMGKoLa3C6VETMHCVGXUw8gG6vwuZEYWz -amou
nt 100 -mine
0000a57759311c8ece5e90a5fd167a603f796b47faa63061ca26845ab377bc22


交易成功
```

Figure4.8 Execute Transaction

There are two transactions which is executed on central node 1

(1)Transaction1:Transfer 50 Vcoin from 17UYUGFqw3xSnrsvkyMbYgwgNiP88EMzk1 to 1CnxXNXH49NJWTQu82Sbb4z4BSH2mXcGYH(one of the wallet node)

(2)Transaction2:Transfer 100 Vcoin from 17UYUGFqw3xSnrsvkyMbYgwgNiP88EMzk1 to 1PMGKoLa3C6VETMHCVGXUw8gG6vwuZEYWz

Then we can check accounts on central node

```
D:\Code\src\vcoin-test>1 getbalance -address 1CnxXNXH49NJWTQu82Sbb4z4BSH2mXcGYH
查询金额如下1CnxXNXH49NJWTQu82Sbb4z4BSH2mXcGYH : 50

D:\Code\src\vcoin-test>1 getbalance -address 1PMGKoLa3C6VETMHCVGXUw8gG6vwuZEYWz
查询金额如下1PMGKoLa3C6VETMHCVGXUw8gG6vwuZEYWz : 100
```

Figure4.9 Balance of other Wallets on Node1

However, that is just the transaction on central node, we need to synchronize the transaction. As you can see, there are no transactions on wallet node(and the file size of database is different because there are no synchronizations)

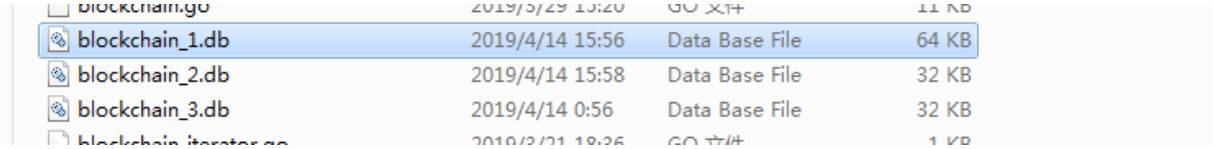

Figure4.10 File size of Three Database

```
D:\Code\src\vcoin-test>2 getbalance -address 1CnxXNXH49NJWTQu82Sbb4z4BSH2mXcGYH
查询金额如下1CnxXNXH49NJWTQu82Sbb4z4BSH2mXcGYH : 0

D:\Code\src\vcoin-test>2 getbalance -address 1PMGKoLa3C6VETMHCVGXUw8gG6vwuZEYWz
查询金额如下1PMGKoLa3C6VETMHCVGXUw8gG6vwuZEYWz : 0
```

Figure4.11 Balance of other Wallets on Node2

Step4: Start wallet node to synchronize the transaction information

We start the node1 and node2, they will connect with each other and synchronize the blocks

That is central node1 in Figure4.12

Figure4.12 Start Nodes

That is wallet node2 in Figure4.13

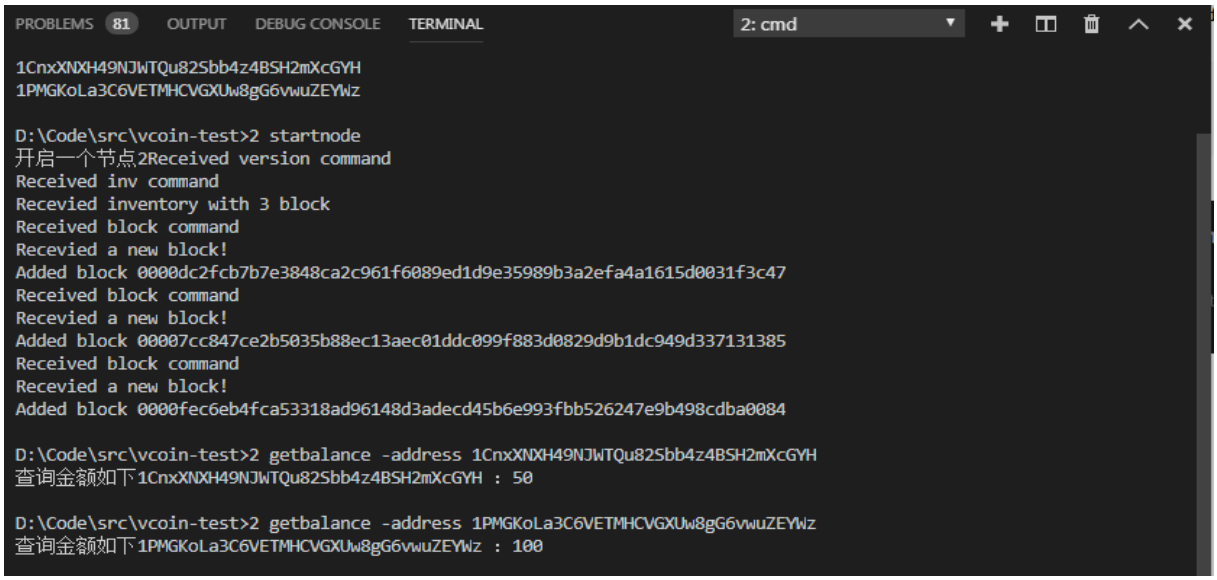

Figure4.13 Balance of other Wallets on Node2 Now

Now we can find that the transaction and balance information on wallet node which means that synchronization has been completed, the file size of database also shows the fact.

Figure4.14 File size of Two node’s Database

Step5: Start the other wallet node and synchronize the blockchain

According to the Figure 4.15 and Figure 4.16, you can see the same synchronization has been finished on Node3

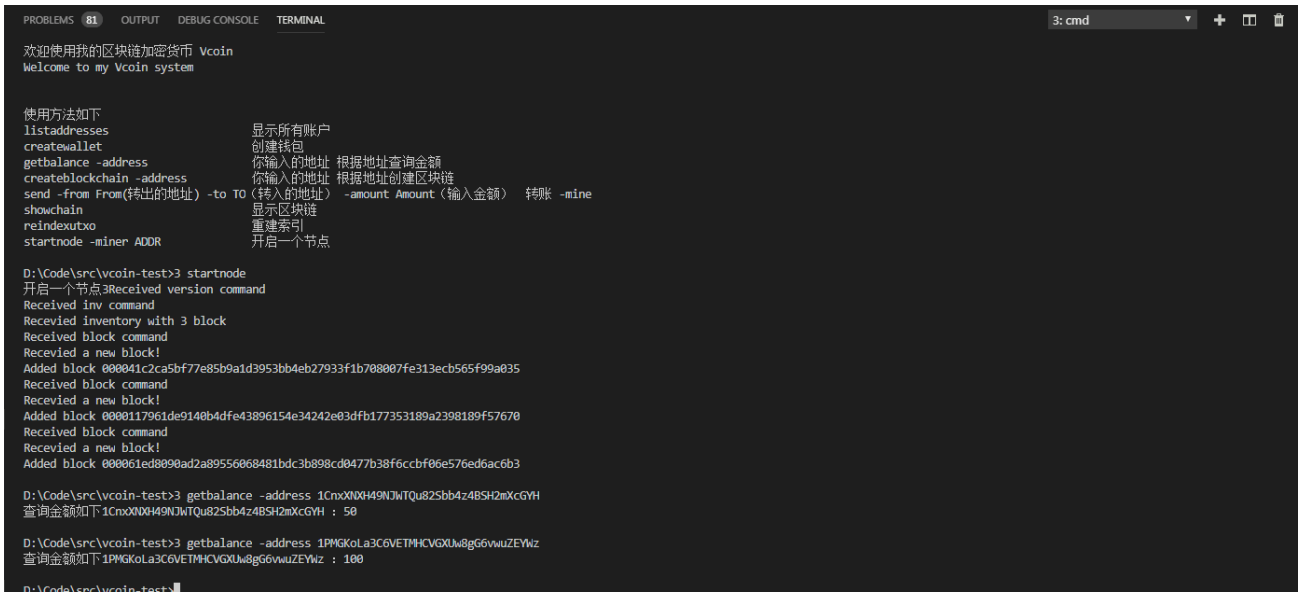

Figure4.15 Block Synchronization on Node3

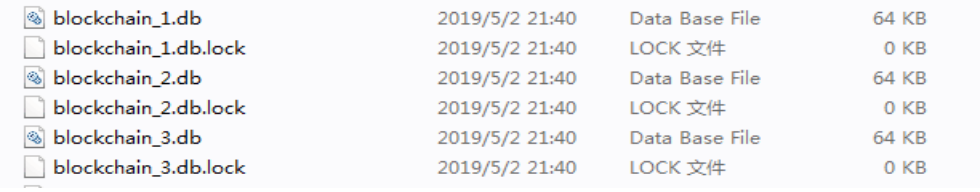

Figure 4.16 File sizes of Three Database now

4.2 Comparing to the existing cryptocurrency

When the Vcoin is compared to other cryptocurrencies, I have to say that Vcoin is not mature enough. But I will choose Bitcoin and Ethereum to compare with Vcoin.

Firstly, Vcoin will choose the BoltDB database to store the blockchain. However, Ethereum and Bitcoin adopt LevelDB database. Certainly, they are all key-value databases and can be used to store massive data. But we have to admit this significant difference

Secondly, in Vcoin system, there are no concepts of accounts. The system tries to maintain the UTXO and uses it to calculate the balance which is similar to the Bitcoin. But when it compared to the Ethereum, it is a very different model. Ethreum is based on the accounts which mean there are real accounts in Ethereum system.

Thirdly, the difficuly of mining in Vcoin is not high. (Certainly we can adjust it). By the way, the block reward is a constant which is similar to Ethereum. But in Bitcoin system, the block reward will decrease progressively.

Fourthly, consensus algorithms are different. Vcoin and Bitcoin will use the proof-of-work

although the details in Pow can be not same. Ethereum will adopt the combination of proof-of-work and proof-of-stake and become the pure proof-of-stake eventually.

And then, Vcoin will not support the smart contract which means the application is not very wide, and therefore we can fork the Vcoin to improve it. In reality, Bitcoin and Ethereum are all support the smart contract and that is the main direction in the future. However, Ethereum is turing complete and able to perform any algorithms in the system so that the advanced smart contract can be deployed. That is why Ethereum is more potential than Bitcoin.

Finally, and the most important part, is network. Vcoin will adopt the hybrid p2p network and some nodes in network seem like more powerful and important. But in Bitcoin network, it is a pure decentralized network. However, in Ethereum, it adopts a series of algorithms and data structured to build the structured P2P network. For example, an improved Kademlia algorithm will base on DHT(distributed hash table) which is widely used in distributed storage. Kad algorithm will calculate a specialized distance between nodes which use the exclusive or. And it will create a data structure which is known as K-bucket to store the node information. The Kad algorithm will improve the efficiency of node discovery and routing.

Above all, Vcoin can be regarded as a combination of Bitcoin and Ethereum. You can see the differences between Vcoin and other cryptocurrencies in Figure4.16

Cryptocurrency / Difference	Vcoin	Bitcoin	Ethereum
Database	BoltDB	LevelDB	LevelDB
Account model	Based on UTXO	Based on UTXO	Account state
Difficulty and block reward	1000 Vcoin and will not decrease	12.5 Bitcoin and will decrease progressively(every 210,000 blocks)	2 ETH and will not decrease(if no forks)
Network	Hybrid p2p network	Pure p2p network	Structured p2p network(Kad)
Smart Contract	No smart contract	simple smart contract	Turing complete and advanced smart contract
Consensus Algorithm	POW	POW	POW+POS

Figure4.16 Vcoin and Other Cryptocurrencies

Chapter 5: Conclusion and Further Work

Above all, I try to design and implement an open-source cryptocurrency which is known as Vcoin. Vcoin has well-defined three layers architecture. Data layer is responsible for storing blocks, blockchain and so on. Network layer will be a peer-to-peer network which can implement the function of data synchronization and communication. Then consensus layer is able to reach a consensus and keep the Vcoin system consistent. Frankly speaking, the core technologies result from Bitcoin but it is a brand new electronic cash system. In my Vcoin system, anyone can download the source code and try to be a user or a miner. Users can execute the financial transactions. At the same time, miners can pay their CPU power to maintain the blockchain and process the valid transactions. Certainly, they will acquire new Vcoins in return.

As for the implementation of software, I choose a special situation to implement. I can use the command line to create a blockchain and some wallets. Then I can execute some transactions on one of nodes. After that, there is no doubt that we can let other nodes to connect to the node where the transaction has been executed to synchronize blocks. Finally all nodes will maintain the same blockchain. Certainly, we can use the API to get balance of all wallets, print the details of blockchain and so on. It can’t be all the functions but will be the inevitable situation in Vcoin system.

It is a pity that my ability and experience are limited. At the same time, I don’t have enough time to update all the functions of Vcoin. I must admit that the implementation of Vcoin is far from perfect comparing to the existing cryptocurrencies. In reality, I have some preliminary plans about how to improve the Vcoin. In my opinion, if I have more time to learn some knowledge about distributed system. I can implement a real peer-to-peer network and let my Vcoin runs well in the network. And then, I can solve the problems of mining. In my previous design, I want to separate the miner nodes and the wallet nodes. But I can’t debug some problems. If someone can discuss it with me, I believe I can solve it with my own effort. To speak honestly, if I have another chance to do the project again, I will pay more attention to the source code of Bitcoin or Ethereum although I have compiled them many times. It is better to communicate with specialists and programmers. Unfortunately, I don’t have that kind of opportunities. From my perspective, source code is the soul of a project and I can implement a better system based on the understanding of source code.

In general, the mechanism looks likes the Bitcoin and Ethereum. Frankly speaking, it surely

can be regarded as the simple version of Bitcoin. But, as an open-source project, it can be developed and forked many times. I believe that it can get better in the future no matter who will redesign or redevelop it.

References

Andreas, A. (2014). *Mastering Bitcoin. In Unlocking Digital Cryptocurrencies.* O'Reilly Media. pp.2-192.

Narayanan, A. , Bonneau, J. , Felten, E. , Miller, A. , and Goldfeder, S. . (2016). *Bitcoin and Cryptocurrency Technologies: A Comprehensive Introduction*. Princeton University Press. pp.1-169.

Stallings, W. , Brown, L. , Howard, M. , & Bauer, M. . (2008). *Computer security: principles and practice*. William Stallings Books on Computer & Data Communications Technology(Dec). pp.30-49.

Nakamoto, S. (2008). *Bitcoin: A peer-to-peer electronic cash system.*

Buterin, V. (2014). *A next-generation smart contract and decentralized application platform*. white paper.

肖辉远, 肖培森, and 葛利军. (2017). *基于 ecc 的数字签名方案在网络可信身份认证中的设计与实现. 警察技术*(4), 83-86.

程冠菘. (2018). *区块链 p2p 网络协议的演进过程. 信息与电脑(理论版), 416*(22), 10-11.

Ivan Kuznetsov,(2017). *Building Blockchain in Go.* [online]Available from: http://jeiwan.cc/ [Accessed 22 Dec 2018]

Nick Sullivan,(2013). *A(relatively easy to understand)primer on elliptic curve cryptography.* [online]Available from: http://arstechnica.com/security/2013/10/a-relatively-easy-to-understand-primer-on-elliptic-curve-cryptography [Accessed 10 April 2019]

Damon Lin,(2018). *椭圆曲线算法，secp256k1 如何生成公钥和私钥.* [online]Available from: http://www.zhihu.com/question/22399196 [Accessed 11 April 2019]

Kalafinalan,(2017). *Ecc 椭圆曲线详解（有具体事例）.* [online]Available from: http://www.cnblogs.com/Kalafinaian/p/7392505.html [Accessed 12 April 2019]

Jacky_jin1,(2018). *ECDSA 数字签名算法.* [online]Available from: http://blog.csdn.net/m0_37458552/article/details/80250258 [Accessed 15 April 2019]

齐杠开,(2018). *Key-Value 数据库实现 part1：什么是 Key-Value 数据库，为什么要实现它*. [online]Available from: http://www.cnblogs.com/fangqi96/p/9121627.html [Accessed 17 April 2019]

Irita,(2017). *Boltdb 源码分析-MVCC/持久化-3*. [online]Available from: http://studygolang.com/articles/9939 [Accessed 20 April 2019]

Jupiterwangq,(2018). *比特币源码分析——p2p 网络初始化*. [online]Available from: http://blog.csdn.net/ztemt_sw2/article/details/80291705 [Accessed 21 April 2019]

renqHIT,(2018). *比特币源码阅读笔记网络篇*. [online]Available from: http://blog.csdn.net/renq_654321/article/details/79588567 [Accessed 23 April 2019]

Homeabic,(2018). *区块链中的双花攻击*. [online]Available from: http://www.cnblogs.com/w-i-n-d/p/9111149.html [Accessed 24 April 2019]

GavinXujiacan(2018). *[我的区块链之路]-理解传统 Kademlia 和以太坊 Kademlia 网络*. [online]Available from: http://blog.csdn.net/qq_25870633/article/details/81939101 [Accessed 29 April 2019]

Ajax(2018). 通过 BoltDB 对区块链区块进行持久化存储. [online]Available from: http://www.imooc.com/article/263623 [Accessed 1 May 2019]

Acknowledgement

First of all, I would like to express my sincere gratitude to my supervisor for his instructive advice and useful suggestions. I can’t finish my final project without his helps.

Secondly, high tribute shall be paid to my senior whose name is Han Runchao. He majors in Blockchain and gives me some advices. For example, the book *Master Bitcoin* is recommended by him.

Thirdly, special thanks should go to Martin Holst Swende who is a complete stranger to me. When I fail to compile the source code of Ethereum, he gives me some advices on Github.

Fourthly, I would like to extend my gratitude to two programmers whose name are Yin Cheng and Ivan Kuznetsov. Their blogs and Mooc make me understand how to use the Golang to build my own simple cryptocurrency.

Last my thanks would go to the BUPT and QM, they provide me with the chance to finish my final project. That is the first chance for me to finish a difficult and cutting-edge project by myself. It will be a great honour for me to graduate from these two universities.

Appendix

北京邮电大学 本科毕业设计（论文）任务书

Project Specification Form

Part 1 – Supervisor

论文题目 Project Title	VCoin: A Blockchain Algorithm for Cryptocurrency		
题目分类 Scope	Software Development	Implementation	Software
主要内容 Project description	A blockchain consists of blocks of information linked together using the linked list data structure. Blockchains used cryptography to provide data integrity and confidentiality to the blocks of data it generates. Blockchain algorithms are used to generate or create virtual currencies also known as cryptocurrencies. Cryptocurrencies such as Bitcoin and Lightcoin are very popular media of business transactions over the cloud powered by the internet. Blockchain and cryptocurrency used decentralised distributed ledger for transactions within a peer-to-peer (P2P) architecture. This project aims to develop a blockchain algorithm for cryptocurrency known as VirtualCoin (VCoin) which will have a ledger and digital wallet interface and can perform hypothetical business transactions over the internet. The project will consider the risks and limitations involved in implementing blockchain algorithms for use as virtual currency.		
关键词 Keywords	virtual currency, cryptocurrency, blockchain, algorithms		
主要任务 Main tasks	**1** Do a literature review and risk analysis of blockchain and cryptocurrency algorithms and implementation applications		
	2 Design a implementation P2P architecture for bloackcain and cryptocurremcy		
	3 Develop the algorithm for the VCoin bloackchain cryptocurrency		
	4 Implement the software which consists of ledger interface and VCoin cryptocurrency transation with reports as contained in your thesis		
主要成果 Measurable outcomes	**1** Peer-to-peer architectural design for blockchain and VCoin cryptocurrency		
	2 The blockchain algorithm developed for VCoin cryptocurrency implementation		
	3 The working software for the VCoin cryptocurrency with web-based ledger interface and hypothetical transactions		

北京邮电大学 本科毕业设计（论文）任务书

Project Specification Form

Part 2 - Student

学院 **School**	International School	专业 **Programme**	**Internet of Things Engineering**		
姓 **Family name**	Wang	名 **First Name**	jieping		
BUPT 学号 **BUPT number**	2015213429	**QM 学号** **QM number**	151007028	班级 **Class**	2015215120
论文题目 **Project Title**	VCoin: A Blockchain algorithm for Cryptocurrency				

1

论文概述 **Project outline** **Write about 500-800 words** **Please refer to Project Student Handbook section 3.2**	To begin with, I will try to know the mechanism which the realistic currency use and figure out why the VCoin can emerge. It will involve some basic economic problems and the origin of blockchain(and its creator satoshi nakamoto).And then, try to do the risk assessment is a necessary task. At this stage, we can find out the difference between distributed database and decentralized blockchain concept. About the risk, we should analyse the inherent property of the blockchain and the potential risk. Trying to understand how the PBFT(or POS,POW and so on) to prevent the malicious tampering. For myself, in this assessment, I can harvest lesson of the existing consensus algorithms. In the second place, I plan to analyse the VCoin, especially its algorithms and p2p architecture by learning some famous papers and searching some useful material. I will pay more attention to the Bitcoin(or ethereum). From my perspective, using a existing model to analyse the problems is a better way. At this stage, I am supposed to learn some cryptology and its information in that I can perceive that how the VCoin can work and what is the possibility. As far as I am concerned, there are several kinds of algorithms about the cryptocurrency. Such as Hash algorithm. And in the consensus algorithms, it can be POW, POS ,DPOS , PBFT. Frankly speaking, they have different performance. That is why we do this research and try to optimize them(maybe it is a big challenge for us).To implement one or several them will help me to broaden my horizon Thirdly, I want to try to design a p2p architecture. Because of my limited scholarly level, I choose to make effort to achieve some kings of existing model and make a lot of modification. About the programing language, I think it can be java, python or C++. What is more, it is involve some computer network knowledge. As a senior, we should learn how to apply our knowledge to work out some realistic problem and try to build up a basic model of P2P by myself. Certainly, it is a cutting edge research, I have to try my best to do it. Fourthly, I will begin to work out the Web front-end which will be ocular to us. In my opinion, JavaScript is the best way to achieve the web visualization. I commend that the final version can work based on the web and we can create account , transfer account and so on. It should be a process that we can manipulate. Finally, I will try to make the integration and combine front-end and back-end. At the final stage , the whole project will be a software which have some function and interface. It will have its own web-based ledger and VCoin.
道德规范 **Ethics**	Please confirm that you have discussed ethical issues with your Supervisor using the ethics checklist on QMPlus. Yes

	Summary of ethical issues: (put N/A if not applicable) In my project, it will not involve many private information, But I will promise that I can do it by myself and keep away from plagiarism. Certainly, it will inevitable to refer to some material and paper. About the references, I will note it in my thesis.
中期目标 **Mid-term target.** **It must be tangible outcomes, E.g. software, hardware or simulation.** **It will be assessed at the mid-term oral.**	In my Mid-term oral exam, I want to achieve some specific function in my project. From my perspective, it will be suitable to finish the P2P architecture and do the comprehensive risk assessment to my system. 1. Be familiar about the origin of blockchain 2. Have some basic knowledge about the cryptology 3. Know the p2p architecture and distributed database 4. Learn the basic architecture of the blockchain(hash function,data structure and so on) 5. Implementation of the p2p architecture 6. Perceive the risk of all the consensus algorithms and have my own perspective about how to optimize them(some my own idea, maybe it is not correct)

Work Plan (Gantt Chart)

Fill in the sub-tasks and insert a letter X in the cells to show the extent of each task

	Nov	Dec	Jan	Feb	Mar	Apr	May
Task 1 break down							
Economic problems about the currency	X						
The origin of blockchain	X						
Some famous algorithms and their implementation	X	X					
To assess the risk and performance of the algorithms	X	X	X				
Task 2 break down							
P2P application in blockchain	X	X	X				
Understand some existing model of P2P and their machanism	X	X	X				
Try to optimize some p2p model and implement it	X	X	X				
Task 3 break down							
Learn how to use python(or c++, java and so on)	X	X	X	X			
Try to run other's program and comprehend the code	X	X	X	X			
Try to modify the algorithm and make it more effective	X	X	X	X	X		
Task 4 break down							
Learn how to use the javascript(web programming)	X	X	X	X	X		
Integration of the software	X	X	X	X	X	X	
Finish the web-based fragment	X	X	X	X	X		

北京邮电大学 本科毕业设计（论文）初期进度报告

Project Early-term Progress Report

学院 **School**	International School	专业 **Programme**	**Internet of Things Engineering**		
姓 **Family name**	Wang	名 **First Name**	Jieping		
BUPT 学号 BUPT number	2015213429	**QM 学号 QM number**	151007028	班级 **Class**	2015215120
论文题目 **Project Title**	VCoin: A Blockchain algorithm for Cryptocurrency				

已完成工作 **Finished work:**

During my early-term study and research, I have some deep understanding about the VCoin and blockchain. According to my specification, I manage to learn some background of the cryptocurrency, especially bitcoin and their economic meaning. On the other hand, I have obtain some authentic details about the famous blockchain algorithm for the cryptography.

1. The background of Cryptocurrency

   The cryptocurrency is a trading medium that uses cryptography to ensure transaction security and control the creation of trading units. A cryptocurrency is a type of digital currency (or virtual currency). Bitcoin became the first decentralized cryptocurrency in 2009, after which the term cryptocurrency refers to this type of design. Since then several similar cryptocurrencies have been created, often referred to as altcoins. The cryptocurrency is based on a decentralized consensus mechanism, as opposed to a banking financial system that relies on a centralized regulatory system. As for the earliest birth and the most famous currency, the concept of Bitcoin was invented by the Japanese Nakamoto (a pseudonym). In 2008, a person named Zhong Bencong first proposed Bitcoin in a paper entitled "Bitcoin: A Peer-to-Peer Electronic Cash System." He combined several previous digital currency inventions, such as B-money and HashCash, to create a fully decentralized electronic cash system that does not rely on central authority for currency protection or settlement verification.

   The key innovation is the use of distributed computing systems (called "workload proof" algorithms) to perform a "network selection" every 10 minutes, enabling the use of decentralized networks to synchronize transaction records. This elegantly solves the double payment problem (that is, a single currency unit can be used twice. Previously, the double payment problem was a weakness of the digital currency and was handled by a central clearing house to clear all transactions).Bitcoin was originally a network virtual currency that could buy real-life items. It is characterized by decentralization, anonymity, can only be used in the digital world, does not belong to any country and financial institutions, and is not restricted by geography. It can be exchanged anywhere in the world, and it is therefore used as a money laundering tool by some lawless elements. .

2. Bitcoin and its economic influence

   Nowadays, countries and national alliances all have their own legal currency. The legal currency is responsible for production investment and management by the central bank machine, which leads to many man-made financial problems. For example, over-currency will lead to inflation and thus seriously affect the rights and interests of ordinary citizens. The control of the currency by the state means that the rights and interests of citizens are not fully guaranteed. And Nakamoto's bitcoin is the dream of some technical geeks. Bitcoin uses the p2p network architecture to directly remove the third party of the state machine, avoiding the central bank's arbitrary manipulation of the currency. Moreover, it uses distributed ledgers,

consensus algorithms and other mechanisms to ensure the privacy and non-tampering of currency transactions. And compared to the natural currency of gold, Bitcoin is more convenient to store and trade and can be split indefinitely. Of course, the wave of digital cryptocurrencies will inevitably lead to earth-shaking changes in the financial systems of countries around the world. No one can know what the future will look like. However, Bitcoin can at least avoid Venezuela, Zimbabwe's super-currency tragedy for the people. In my opinion, Bitcoin is not only a technology integration innovation, but also a new attempt in the field of finance and life.

3. Core algorithm related to blockchain
   Blockchain Core Algorithm 1: The Byzantine Byzantine story is probably the case: the Byzantine Empire has enormous wealth, and the surrounding 10 neighbors have been long-lived, but the Byzantine walls are towering, impregnable, and no single neighbor can successfully invade. . Any single neighbor's invasion will fail, and it may also be invaded by the other nine neighbors. The Byzantine empire's defense ability is so strong that at least half of the ten neighbors must attack at the same time, and it is possible to break. However, if one or several of the neighbors themselves agree to attack together, but the actual process of betrayal, then the intruder may be annihilated. So every party is careful and does not dare to trust neighboring countries easily. This is the question of General Byzantine. In this distributed network: each general has a message book that is synchronized with other generals in real time. Each general's signature in the ledger is verifiable. If there are any inconsistencies, you can know which generals are inconsistent. Despite the inconsistency of the news, as long as more than half agree to the offensive, the minority obeys the majority and the consensus is reached. Thus, in a distributed system, despite the bad guys, the bad guys can do anything (not subject to protocol restrictions), such as not responding, sending error messages, sending different decisions to different nodes, joining different bad nodes, doing bad things, etc. Wait. However, as long as most people are good people, it is entirely possible to achieve consensus centrally.

   Blockchain Core Algorithm 2: Asymmetric Encryption Technology In the above-mentioned Byzantine agreement, if several of the 10 generals simultaneously initiate messages, it will inevitably cause system confusion, resulting in various attack time scenarios, and actions are difficult to be consistent. Anyone can launch an offensive message, but who will issue it? In fact, this can be done by adding a cost, that is, only one node can propagate information for a period of time. When a node sends a unified attack message, each node receives the initiator's message and must sign and seal to confirm their identity. In the present view, asymmetric encryption technology can completely solve this signature problem. Asymmetric encryption algorithms use two different keys for encryption and decryption. These two keys are the "public key" and "private key" we often hear. The public key and the private key generally appear in pairs. If the message is encrypted with a public key, the private key corresponding to the public key needs to be decrypted. Similarly, if the message is encrypted with a private key, the public key corresponding to the private key is required to be decrypted.

   Blockchain Core Algorithm 3: Fault Tolerance Problem We assume that in this network, messages may be lost, corrupted, delayed, and repeatedly sent, and the order of acceptance is inconsistent with the order of transmission. In addition, the behavior of the node can be arbitrary: it can join, exit the network at any time, can discard messages, forge messages, stop work, etc., and various human or non-human failures may occur. Our algorithm provides fault tolerance for a consensus system consisting of consensus nodes. This fault tolerance also includes security and availability, and is applicable to any network environment.

   Blockchain Core Algorithm 4: Paxos Algorithm (Consistency Algorithm) The problem solved by the Paxos algorithm is how a distributed system agrees on a certain value (resolution). A typical scenario is that in a distributed database system, if the initial state of each node is the same and each node performs the same sequence of operations, then they can finally get a consistent state. To ensure that each node executes the same sequence of commands, a

"consistency algorithm" is required on each instruction to ensure that the instructions seen by each node are consistent. A common consistency algorithm can be applied in many scenarios and is an important issue in distributed computing. There are two models of node communication: shared memory and messaging. The Paxos algorithm is a consistency algorithm based on the message passing model.

Blockchain Core Algorithm 5: Consensus Mechanism The blockchain consensus algorithm is mainly proof of workload and proof of equity. In terms of bitcoin, in fact, from a technical point of view, PoW can be regarded as a reusable hashcash. The proof of the generated workload is a random process in terms of probability. When mining new confidential currencies and generating blocks, all participants must agree, and the miner must obtain proof of PoW work for all the data in the block. At the same time, the miners have to observe the difficulty of adjusting the work from time to time, because the network requirements are to generate an average block every 10 minutes.

Blockchain core algorithm 6: Distributed storage Distributed storage is a data storage technology that uses the disk space on each machine through the network, and these scattered storage resources constitute a virtual storage device, and the data is stored in a distributed manner. Every corner of the network. Therefore, distributed storage technology does not store complete data on every computer. Instead, it cuts the data and stores it on different computers. It's like storing 100 eggs, not in the same basket, but in separate places, adding up to a total of 100.

Actually, to begin with, I met many difficult problems which makes me feel obscure to the blockchain and bitcoin. But the Peking university MOOC is a great way for me to understand the principle of blockchain and its application. Many ideas from the Teacher Xiaozhen is provoking and smart. That is a best tool for me to start my own research.

Reference：**1.** Bitcoin: A Peer-to-Peer Electronic Cash System Satoshi Natamoto

2. Blockchain core algorithm analysis Roger Wattenhofer

3. Blockchain technology and application **Xiaozhen Peking university** **https://study.163.com/course/introduction/1006145002.htm**

4. Bitcoin and Cryptocurrency Technologies Arvind Narayanan .....

是否符合进度？**On schedule as per GANTT chart?**

Yes

下一步 **Next steps:**

According to my specification, I have a plan that we can assess the risk and performance of the algorithms ，try to understand some existing model of P2P and their machanism （then manage to implement them，maybe we can have some optimised idea）.Certainly， we should find a way to use the bitcoin trading system to feel it closely.

From my perspective， In the next stage，I will understand more core knowledge about the blockchain and bitcoin. That is a interesting and challenging experience for me

北京邮电大学 本科毕业设计（论文）中期进度报告

Project Mid-term Progress Report

学院 **School**	International School	专业 **Programme**	**Internet of Things Engineering**		
姓 **Family name**	Wang	名 **First Name**	Jieping		
BUPT 学号 BUPT number	2015213429	**QM 学号 QM number**	151007028	班级 **Class**	2015215120
论文题目 **Project Title**	VCoin: A Blockchain algorithm for Cryptocurrency				

是否完成任务书中所定的中期目标？**Targets met (as set in the Specification)?**

Yes

已完成工作 Finished work:

At this stage, I tried to understand more about the core algorithms and cryptographic basic knowledge of blockchain and cryptocurrency, and learned about the blockchain peer-to-peer network according to specification. Finally, I manage to evaluate the p2p system performance and some optimized ideas.

1.Some important data structure and mechanisms in blockchain

In order to understand the blockchain technology, we can choose Bitcoin as an example. In fact, almost all cryptocurrencies use some of the same cryptography basics knowledge and data structures. I think this is because these algorithms and data structures can make blockchain technology work well. From my perspective, The most important concepts are hash function, merkle tree, asymmetric encryption and consensus algorithms.

At first, hash function is the key part of the cryptocurrency including bitcoin. In reality, Blockchain is a linklist which using the hash pointer. Hash pointe will save a unique value which is calculated by the former block. If the former block is tampered with, all the hash value will be different.

Secondly, Merkle tree is an important data structure for blockchain.it is similar to the binary tree which using the hash pointer. According to the hash value, we can figure out whether the block is valid.

Thirdly, asymmetric encryption is also of importance because of its application in blockchain p2p network. The public key and private key make the node can join in the network and quit free.

Finally, and may be the most important. It is the consensus algorithms. In Bitcoin system, all nodes must agree on which transactions are broadcast and the order in which these transactions happen. This will result in a single global ledger for the system. However, According to the Fischer-Lynch-Paterson Impossibility, we may think that it is impossible for all nodes to keep consensus in asynchronous system. But Luckily, it is applied in bitcoin system well in that we introduce the incentive and proof of work.(Pow).I will explain in detail my understanding of consensus mechanisms(such as POW,POS,DPOS).

.

2.The peer-to-peer network in blockchain

The Bitcoin work at the application layer whose bottom layer is a peer-to-peer overlay network. Bitcoin net is very simple in which all nodes are fully equal (no super node).it is not a central system, if you want to join in it, you will seek one seed node at least. And then you try to communicate with these seed nodes. Certainly, these nodes will tell you other nodes that they know. In addition, the communication will use TCP protocol in order to penetrate the firewall. Moreover, if a node wants to leave the system, it doesn’t need to inform other nodes.

In fact, they will delete you if don't receive your message for a long time (3 hours). To join in the P2P network, all nodes will maintain the blockchain. When we start a transaction, we want to inform all the nodes by flooding(or gossip protocol). And then other nodes will verify the validation of this transaction. If some transactions are valid, nodes will put them into a pool of transactions (if it has already existed, it will not be added in the pool again).

What we still need to know is that the nodes in the Bitcoin network mainly have four functions, wallet, mining, blockchain database, network routing. Each node will have routing functions, but other functions may not be available. Different types of nodes may only contain some functions. Generally, only the bitcoin core node will contain all four functions. According to whether the node itself stores the complete blockchain information, the p2p node can be divided into SPV and Full nodes.

3. The evaluation of P2P system.

For a P2P system, the performance and features is of great significance. In Bitcoin blockchain system, it is robust and simple but not efficient. The selection of neighbour is random where we will not take the physical topology into consideration. That is to say, a node in London may choose the node in Beijing as the neighbour. It will be simple and improve the robustness. But obviously, the efficiency is a potential problem. Some near neighbour's communication still requires a relatively large overhead.

4.Some advises on Bitcoin(Blockchain) P2P network optimization

Frankly speaking, blockchain P2P network has some great advantages. But I realize that there will be some inevitable problems. That is the network overhead and scalability. With more and more nodes join in the network. The latency and need of computing ability will increase. What's more, the cryptographic algorithms are not safe enough. I think we are supposed to use hard fork or soft fork to improve the performances.

尚需完成的任务 **Work to do:**

1. learn some new high-level language
2. Try to compile and run some little blockchain application
3. Analyse some blockchain algorithms and try to optimize it

存在问题 **Problems:**

1.It is too theoretical and lack of implementation so that it is hard to understand some concepts.

2. Bitcoin is just an typical example for us to analyse the problems. There are different cryptocurrency which is significant to us.

3. I find that it is not difficult to point the disadvantages of Bitcoin or other cryptocurrency but it will be hard to make some optimizations.

拟采取的办法 **Solutions:**

1. Read more materials and Mooc 2. Using the Github, download and run some little blockchain application 3. To understand some knowledge about ETH,LTC and so on
论文结构 **Structure of the final report:** **Abstract**(brief article content) **Chapter1:**Intruduction to the purpose and work **Chapter2:**Background **Chapter3:**The theory and related knowledge **Chapter4:**Result and Discussion **Chapter5:**Conclusion and Further work **Reference**(reference materials and people who help me) **Appendix**(code and screenshots, include some previous submitted files)

Risk Assessment

Every system has its own risk and we can take measures to assess the risk of our Vcoin.

L represents the likelihood level and C represents the consequence level. The result R will represent the assessment of risk. And R=L.C

(1) User perspective risk

As a user, you may input the wrong address. Unfortunately, the transaction can't be rolled back because of the feature of Vcoin. However, the same problem also exists in the other cryptocurrency and I don't think it is fatal problem. I evaluate the likelihood is 2 and the consequence is 3. So the rating of the risk is 6

In reality, if we lost our wallet file which means we will lost the secret key of our accounts. It is a very serious problem for the users. Nevertheless, if we protect our computer from being attacked by some malicious software or virus, the wallet file can be safe enough. I evaluate the likelihood is 1 and consequence is 4. So the final rating of risk is 4.

(2) System perspective risk

From the Vcoin system perspective, there are some risk problems. For example, if an attacker or an organization masters the CPU power which is more than 51% in Vcoin system. It can deliver 51% double spending attack. It means that attacker or organization can roll back the transaction when they try to build their longest valid chain. It will destroy the Vcoin economic system. Luckily, it is not an easy thing and only can happened at initial phase which means the value of Vcoin is not very high. I evaluate the likelihood is 1 and consequence is 4. Then the rating is 4.

In addition, some cryptocurrency algorithms may run risk of being attacked. We shouldn't forget how the MD5 algorithm cracks. In reality, with the development of computer, some hash algorithms such as SHA-1 and SHA-256 will not be safe anymore. I evaluate the likelihood is 1 and consequence is 5. Then the risk rating is 5.

Finally, we should consider the distributed denial of service which is also a famous attack in real Bitcoin system. In my P2P central subnet, attacker can start the DDOS but I use the load balancing to defend it. So I think the likelihood is 2 and consequence is 2. Then risk rating is 4

Environmental Impact Assessment

For the environmental impact assessment, I will consider it based on these four main parts

(1) Cost of manufacture

As we all know, digital cash has almost no production cost because we will not use the rea l materials to create the money. All we need to use the Vcoin are just computers. Compared to the conventional currency, it is a better way.

(2) Waste disposal and recycling

Because we don't use the real materials to manufacture the money, we don't need to talk a bout the problems of disposal and recycling. Frankly speaking, it is a great advantage of V coin and other cryptocurrencies.

(3) Energy use in service

In my design of Vcoin, we will use the POW algorithm so it needs a lot of electricity to complete the hash calculations. In my opinion, it is an inevitable problem unless we choose another consensus algorithm such as POS.

(4) Saving in energy

As I have mentioned before, POW algorithm will cost a lot of energy. For example, Bitcoin which use the POW has been prohibited by Chinses government because of the wasting electricity problem. Nevertheless, compared to the conventional currency and mints, it is still a great idea to choose the cryptocurrency.