Security Architecture and Services for The Bitcoin System

HUAN MENG

ROYAL INSTITUTE
OF TECHNOLOGY

Master's Degree Project
Stockholm, Sweden April 2014

TRITA-ICT-EX 2014:32

Table of Contents:

Chapter 1:Overview of the Bitcoin System 4

1.1 Functions and Features 4

1.2 omponents of the System and Roles 5

1.3 Examples of Payment Transactions 7

1.4 Current Security Features and Analysis 11

1.5 Conclusions: Problems and Attacks 13

Chapter 2:Current Standards, Initiatives and Deployments 15

2.1 Bitcoin System Standards 15
- 2.1.1 Block and Blockchain 15
- 2.1.2 Timestamp Server 18
- 2.1.3 Proof of Work 18
- 2.1.4 Incentive 19
- 2.1.5 Merkle Tree 19
- 2.1.6 Bitcoin Address (Account) 20

2.2 Current Status of the Bitcoin Network Pool 22

2.3 Bitcoin Community and Other Supporting Organizations 22

2.4 Open–Source Resources 23
- 2.4.1 Wallets for Consumers 23
- 2.4.2 Various Servers 24
- 2.4.3 Various Tools 25

Chapter 3:Roles, Components and Protocols 27

3.1 Bitcoin Network 27

3.2 Miners 27
- 3.2.1Mining: Components, Process, and Protocol Messages 27
- 3.2.2Verification of Transactions 33

3.3 Users / Individuals 35

3.4 Merchants – Over-The-Counter and Web 35

3.5 Exchanges 36

3.6 Service Providers 37

Chapter 4:Demonstration 38

4.1 Description of the Overall Demonstration System 38

4.2 Downloaded and Installed Components 39

4.3 Examples of Transactions and Demonstration 39

Chapter 5:Conclusions and Future Work 43

5.1 Further Research and Design Activities 43

5.2 Future Implementation and Deployment Activities 43

5.3 New Standards 43

References 45

Executive Summary:

Bitcoin is a digital currency which is based on P2P network and open source software. It is a virtual currency without any control by any centralized organization. New Bitcoins are issued by lots of specified algorithms. The whole Bitcoin network utilizes the distributed database to verify and record all the transactions through the nodes in the P2P network in which the double spending is prevented. No person or organization is able to control Bitcoin based on a decentralized P2P network and algorithm. The cryptographic functions of Bitcoin are designed to allow only the real Bitcoin owner to pay and transfer, and ensure the anonymity and marketability.

The purpose of this thesis is to analyze the security architecture and services for the Bitcoin system and describe of all the features and infrastructures of the whole Bitcoin network. A whole establishment demo including wallet client, mining server with GUI and mining client is implemented. Further improvement will be suggested and recommended for the system.

Chapter 1: Overview of the Bitcoin System

1.1 Functions and Features

Bitcoin is the world's first decentralized digital currency system. It combines together P2P network and cryptographic knowledge to make a totally new digital payment system without the trusted third party. The system uses distributed time stamp to bind all the transactions through transaction blocks. People make transactions using public-key cryptography – public key known by everyone and personal private key. Anyone in the Bitcoin P2P network can verify those transactions. As for these functions, the double-spending is avoided in the whole system. People all over the world can use this system without any limitation. Nowadays anything in daily traditional business can be reflected into this system.

People can download Bitcoin wallet software to generate Bitcoin account (address) and receive money. Once you know your friend's account, you can simply send Bitcoin to your friend. Since Bitcoin uses public key cryptography, you can sign your transaction with your private key. In the meantime, your public key will be known by everyone.

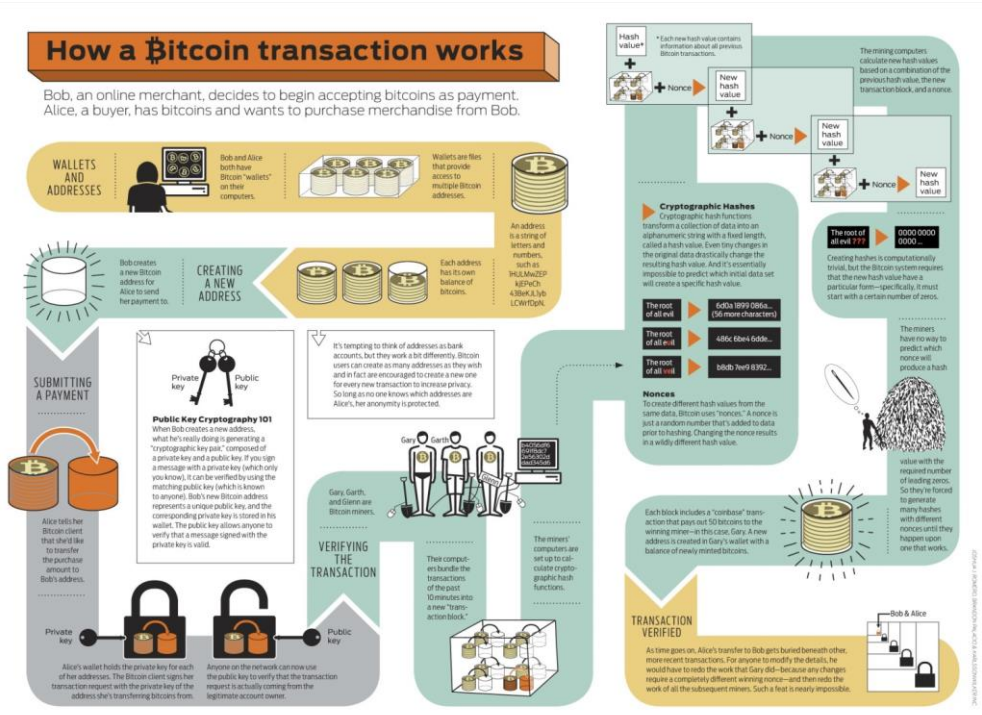


Figure 1: Bitcoin Transaction Process [1]

Features and Advantages of Bitcoin:

1. Anonymity: Bitcoin improves users' anonymity by using a hash value of public key as user address/account, but it's not absolute anonymous, since the transactions and behaviors of users can be analyzed.
2. Open source: Since Bitcoin is an open source system, merchants, consumers, investors and service providers can build up
3. Powerful: Based on P2P, single person or organization can't close and affect it.
4. International: No any limitation among countries and people.
5. Competitive: Nobody can forge more than 51% of the whole Bitcoin network since it is strong enough now.
6. Cheap transaction: Low transaction fee, no limit for the transaction amount and transaction itself.

1.2 Components of the System and Roles

Bitcoin network is formed by millions of people who run the Bitcoin program on the Internet. In the Bitcoin network there is no server, central node and administrator, and all nodes of Bitcoin are equal.

At the beginning, the user runs Bitcoin, he will be connected to a specific IRC (Internet Relay Chat) Server（irc.lfnet.org）, then join the "#bitcoin" chat channel and declare your IP address. When Bitcoin software checks the users in the channel, he can get the IP address of other nodes. Then Bitcoin will connect a certain number of nodes. If IRC server is down, the Bitcoin software will call some internal IP address and try to connect them. After connection is established, it will connect to more nodes through the connected node. So the IRC and nodes are intermediaries which form a Bitcoin P2P network in this case. [2]

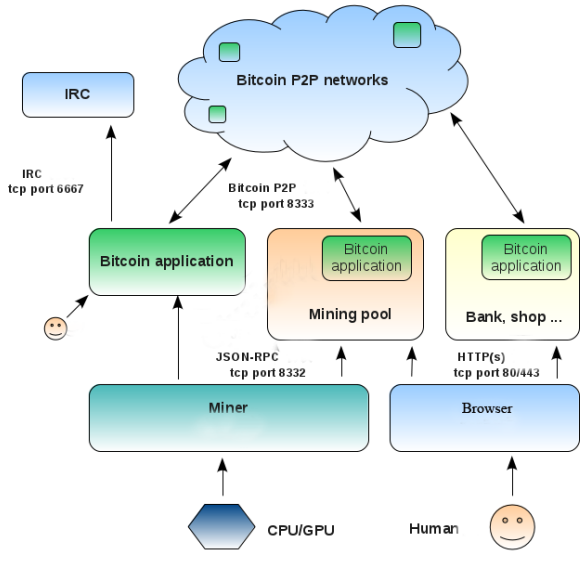


Figure 2: Bitcoin Network [2]

There are several components and roles in the Bitcoin network:

1. Wallet: They are kinds of Bitcoin software which support different system and devices to provide basic function of Bitcoin transaction. A wallet can generate account (Bitcoin address) which can be used for receiving Bitcoins and sending Bitcoins to others
2. Client/User: A client/user is supposed to be the person who is involved in the Bitcoin network and use Bitcoin for transferring money, exchange and business.
3. Miner: A miner is a very important role in Bitcoin system. They will check all the transaction and produce new block. In such a way, new Bitcoins are generated as a reward to people who first build a new block.
4. Mining Pool: Since the mining is a massive computer calculation process, miners get together using mining pool to mine Bitcoin. This is an efficient way to get new Bitcoin nowadays. Because the difficulty is rather large so that single mining (calculation) seems impossible to get new Bitcoin.
5. Exchanges: Bitcoin is just digital currency. Its value depends on the market. People can use dollars, Euros and Chinese Yuan etc. to buy and sell Bitcoin in an exchange platform.
6. Business Operators (Online shops, Banks and so on): Business operators for Bitcoin develop very fast when Bitcoin has a certain value. Online shops, banks, foundation based on Bitcoin transaction are built for diverse Bitcoin operation.

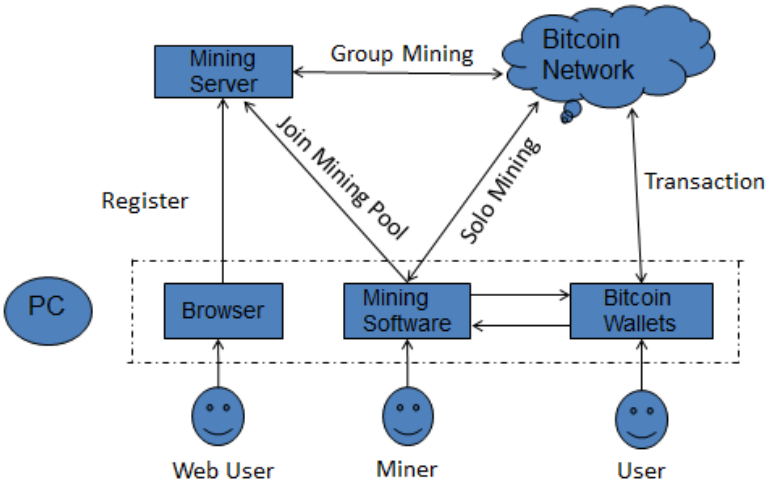


Figure 3: Bitcoin Network Architecture

All Bitcoin mining pools, exchange centers, shops, banks internally run the Bitcoin program and follow the same communication protocol. The difference is that they have different user interfaces for their logical business operation. All the transaction must follow the Bitcoin system regulation to ensure that the transaction is unique and valid in the Bitcoin network.

1.3 Examples of Payment Transactions

In general view, Bitcoin transaction (Tx) from one person to another can be simply described as a previous transaction (Output) with a certain number of Bitcoin transfer money from its address to one or several addresses, which becomes the inputs of the next transactions. We call the first input as Coinbase which generates from the mining reward. In Bitcoin transaction, several inputs can be one output, and one input can be several outputs. [3]

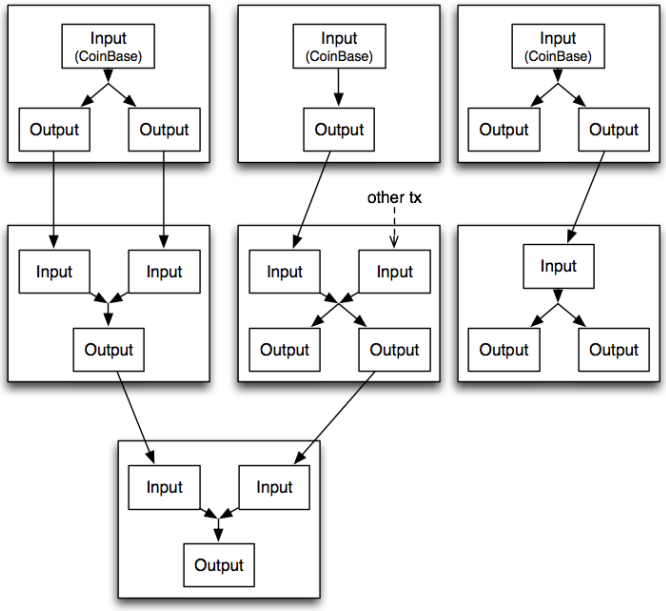


Figure 4: Bitcoin Transaction Outputs and Inputs [3]

See the diagram below and take transaction from B to C for example. The transaction from B to C includes the hash and signed value of previous transactions and the public key (address) of C by using the private key of B, and the public key of B.

The transaction and the public key of B will be broadcasted to the Bitcoin network. Everyone can verify this transaction. People can use public key of B to check the signature inside the transaction if the transaction is really from B or not. C has his private key, so he is the only one that can match the public key of C (address) inside the transaction.

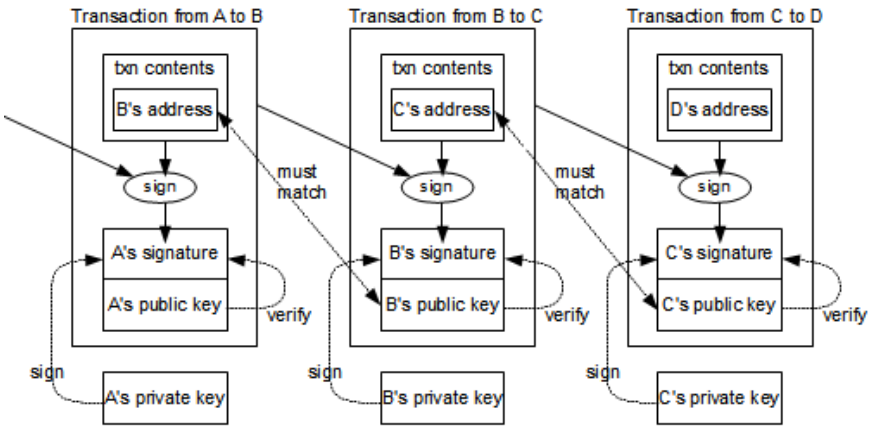


Figure 5: Bitcoin Transaction [4]

The transaction process can be explained as the message below:

Tx(B to C)= {PrevTx, BTC, PubC, SigB&Hash(PubC, PreTx, BTC)}

Bitcoin Payment Transaction Message Structure

Field Size	Description	Data type	Comments
4	magic	uint32_t	Magic value indicating message origin network, and used to seek to next message when stream state is unknown
12	command	char[12]	ASCII string identifying the packet content, NULL padded (non-NULL padding results in packet rejected)
4	length	uint32_t	Length of payload in number of bytes
4	checksum	uint32_t	First 4 bytes of sha256(sha256(payload))
?	payload	uchar[]	The actual data

Table 1: Bitcoin Payment Transaction Message Structure [5]

Here is a previous block example for two transactions. 50 Bitcoin is generated in one of them and transferred to the address 16ro3Jptwo4….:

Hash: 000000000043a8c0fd1d6f726790caa2a406010d19efd2780db27bdbbd93baf6
Previous block: 00000000001937917bd2caba204bb1aa530ec1de9d0f6736e5d85d96da9c8bba
Next block: 00000000000036312a44ab7711afa46f475913fbd9727cf508ed4af3bc933d16
Time: 2010-09-16 05:03:47
Difficulty: 712.884864
Transactions: 2
textbfMerkle root: 8fb300e3fdb6f30a4c67233b997f99fdd518b968b9a3fd65857bfe78b2600719
Nonce: 1462756097

Input/Previous Output	Source & Amount	Recipient & Amount
N/A	Generation: 50 + 0 total fees	Generation: 50 + 0 total fees
f5d8ee39a430...:0	1JBSCVF6VM6QjFZyTnbpLjoCJ...: 50	16ro3Jptwo4asSevZnsRX6vf..: 50

Figure 6: Block Example [6]

General format of a Bitcoin transaction (inside a block) is:

Field	Description	Size
Version no	currently 1	4 bytes
In-counter	positive integer VI = VarInt	1 - 9 bytes
list of inputs	the first input of the first transaction is also called "coinbase" (its content was ignored in earlier versions)	<in-counter>-many inputs
Out-counter	positive integer VI = VarInt	1 - 9 bytes
list of outputs	the outputs of the first transaction spend the mined bitcoins for the block	<out-counter>-many outputs
lock_time	if non-zero and sequence numbers are < 0xFFFFFFFF: block height or timestamp when transaction is final	4 bytes

Table 2: Format of a Bitcoin Transaction [5]

General format (inside a block) of each output of a transaction - TxOut

Field	Description	Size
value	non negative integer giving the number of Satoshis(BTC/10^8) to be transfered	8 bytes
Txout-script length	non negative integer	1 - 9 bytes VI = VarInt
Txout-script / scriptPubKey	Script	<out-script length>-many bytes

Table 3: Format of TxOut [5]

Here is a finished/confirmed Bitcoin receiving transaction with receiving account 189iWaUVkcyXQgrXa9Sfz8QpvY4Xbr7gomm, which has received 14 confirmations in the Bitcoin network.

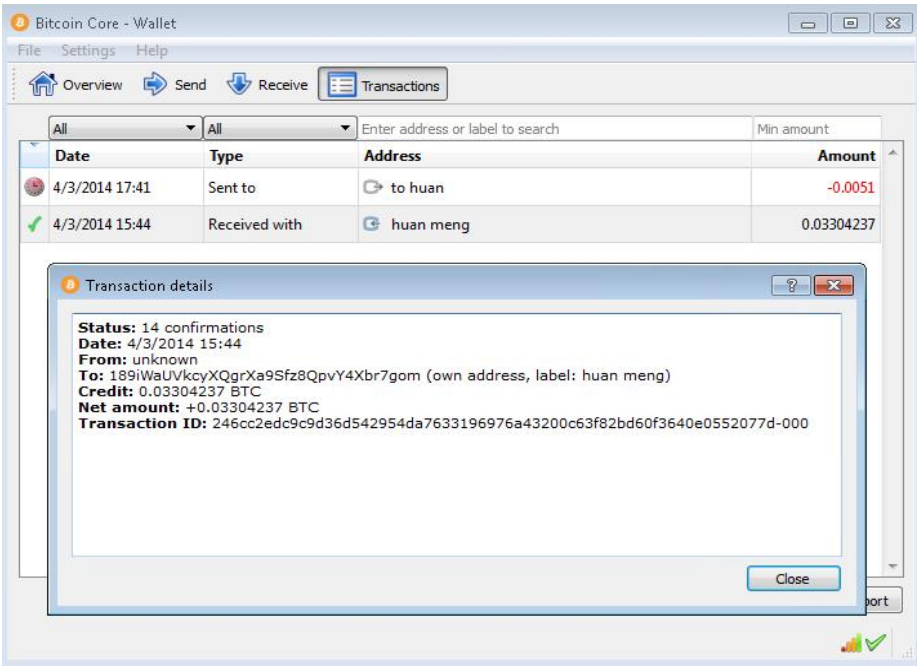


Figure 7: Confirmed Transaction Example

This is a processing Bitcoin payout transaction to the sending account 1Jb5LtYQpbuyejjPJVsqTzu28M94UodmFL with transaction fee 0.0001 BTC. It shows that 8 nodes have seen this transaction in the Bitcoin network and it has only 1 confirmation. After 6 confirmations, this transaction will be confirmed by the Bitcoin network.

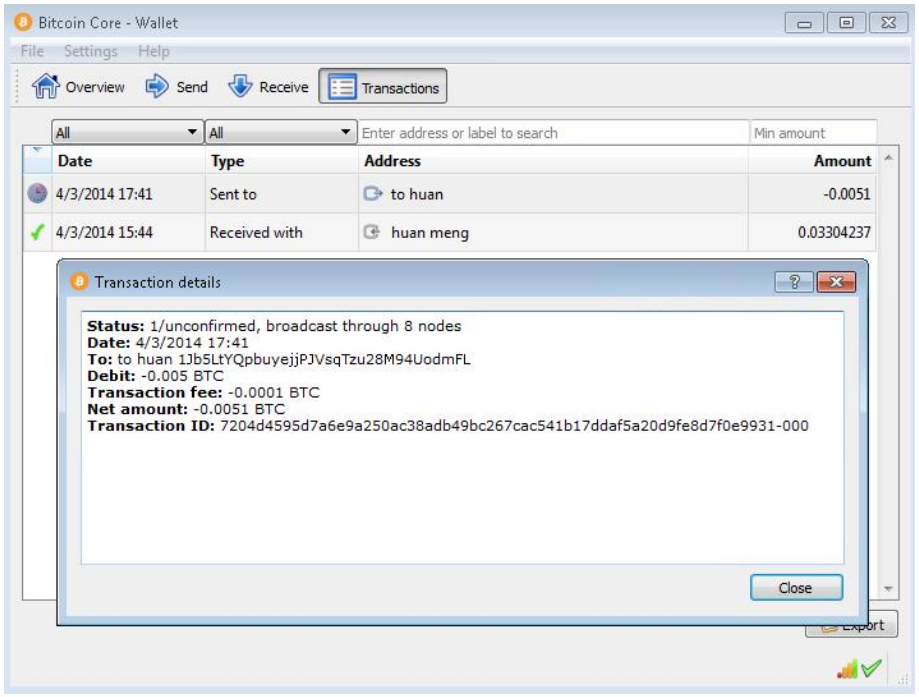


Figure 8: Unconfirmed Transaction Example

Since each transaction and account is transparent to the Bitcoin network, we can get the information through the address and transaction ID. This diagram shows the information

about account 189iWaUVkcyXQgrXa9Sfz8QpvY4Xbr7gom and related transaction history. (Data from blockchain.info)

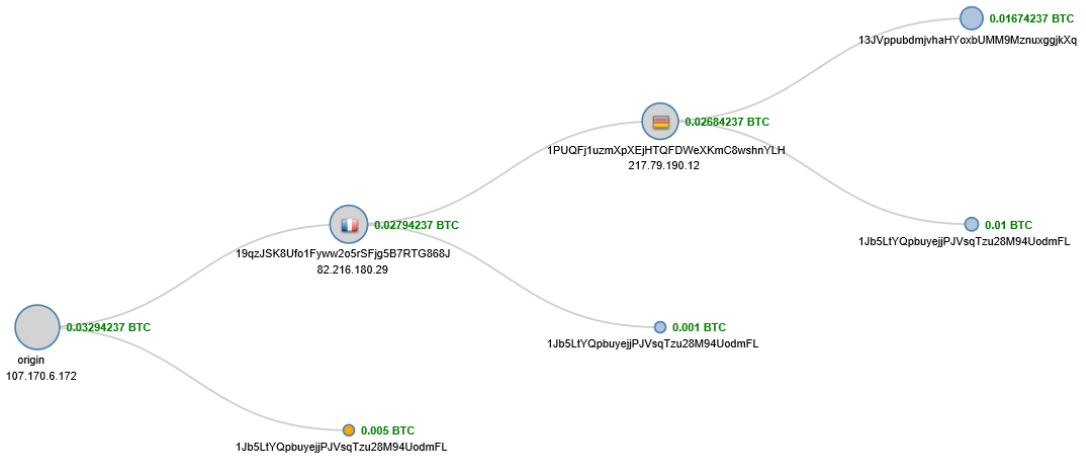


Figure 9: Account History [7]

1.4 Current Security Features and Analysis

Bitcoin system stores all previous transactions with time stamps (block chain), which means each previous transaction in the entire system can be checked and found. New transaction has to be broadcasted and verified by people in the Bitcoin network and then added to the previous transaction. In this case, Bitcoin is not completely safe or reliable theoretically. [8]

The vulnerability all people know (The 51% Attack)

Since the new transaction should be verified and added into new block, someone of course can forge a transaction and double spend. But the problem is that he must have the ability to let people in the network trust this transaction and accept it. So he must have enough network processing power to add his fraudulent transaction faster than other people add the real transaction and continue to make several next transactions. That means he must have more than 50% of the complete Bitcoin network processing power to achieve this goal. This is an impossible task today. Everyone is watching the new transaction and no one can control such big processing power. Nowadays, Bitcoin system is strong enough to resist attacks since nobody or no organization can forge the whole block chain or have more than half of the whole processing power. [9]

Bitcoin Wallet

Bitcoin wallet is very important to a Bitcoin user because normally it stores your bitcoin and private key. Once someone hacks user's wallet and acquires private keys, he will lose all his Bitcoins too. So how to store and protect the private key is a vital issue for

Bitcoin users. Now people have several ways to protect and store the private key by using cold storage. [10]

1. Use Offline Brain wallet and save the phrase in your mind
2. Use Offline Paper wallet and print the private key on paper
3. Use Offline Armory wallet software
4. Make your own ECDSA Private key without third party

Future hardware wallet: An isolated environment for offline transaction signing. This device use USB cable to connect to the computer. There are only two buttons with “agree” and “deny” the transaction. That's why the entire process of setup and operation runs safely.

Figure 10: Hardware Wallet

Online Websites and Wallets

The Bitcoin normally can be exchanged to other currency through online exchanges. In the meantime, they provide online wallets for convenience. That is the normal service that any Bitcoin online shops, banks or other service websites will provide in relation to Bitcoin. Those websites may be easier to attack for hackers. Once the website is down, the user information and Bitcoins will be lost.

DOS

Denial of Service (DoS) or DDoS attacks may affect the Bitcoin network to the network so busy that normal transaction can’t be handled. Bitcoin system has some protections against DoS attacks nowadays, but this may still be a problem when facing this kind of attacks.

Sybil

The attacker may control some network nodes. Victim is likely to connect only to those controlled nodes. Then he will be connected to attacker’s network rather than the real network. In this case, attacker can intercept victim’s transaction and execute a double-spending attack. [9]

Pseudo-anonymity

Bitcoin improves user anonymity by using a random number as a Bitcoin address (public key). All transaction use public keys as the address. There is no any identity binding to specific user. The user can generate lots of public key and use different key for different transaction, which will be very helpful to anonymity. But in fact, 40% of the real owners can be traced according to the research from Germany and Switzerland. There is some liking to analyze and trace the user behavior, since all the transactions are transparent and it is easy to check links between them. There is a risk that if a user's behaviors or one of his transactions is revealed, then all the rest information can be revealed.

1.5 Conclusions: Problems and Attacks

The Bitcoin infrastructure uses complicated cryptographic functions and theories to make sure that all transactions are safe and can't be double-spending. The security issue is considered to be the most important problem. Although the infrastructure seems to be safe now, there are also some risks need to be paid attention.

The 51% Attack

As we talked above, this attack must be related to a ridiculous cost on a supercomputer or some new technology to obtain high hash calculation ability. It seems impossible and not wise to spend resources that are much more worthy than attacks. Global Bitcoin computing power now is 256 times faster than top 500 supercomputers. [11]

"Block Withholding" Attack

The Bitcoin transaction should be actually finished when it is in a block. So an attacker may intentionally hold a conflicting transaction and doesn't announce it to the Bitcoin network. In the "Block Withholding" attack, the attacker will try to find the block which has the transaction which the attacker sends to himself or other business, and then hold the block without broadcasting. In the meantime, he will send the Bitcoin to someone else and broadcast the "holding" block. The Bitcoin system then will first find the "holding" block and reject the other because of the forbidden of double spending. In this case, the attacker has to be very precise in time issue and has the ability to beat other nodes in the Bitcoin network. [9]

Brute Force Attack

Bitcoin uses elliptic curve digital algorithm and hash functions. It's impossible to acquire user's private key from his public key. It's even ridiculous to guess it or reduce it. There are also a lot of ways to protect your Bitcoin private key as mentioned above.

Non-Bitcoin / Infrastructure Attacks

Bitcoin infrastructure is completely safe. User just needs to wait for the confirmation after making transaction. But when it is related to web service and online companies, it's another issue. Deal with reputable companies and service providers. But they are still not totally safe. MtGox which is the biggest online exchange has bankrupt because of attacks. [9]

Social Attacks

Just be careful about the investment and advertisement or any other sales or fraud. It's quite common in the whole society. Never be tempted by any so called profit and beautiful things. [9]

Chapter 2: Current Standards, Initiatives and Deployments

2.1 Bitcoin System Standards

The most important Bitcoin standards and mechanisms are reviewed briefly here. The aspect of the system is analyzed through each of them.

2.1.1 Block and Blockchain

Block is a very important concept in Bitcoin system, since it contains hundreds of transactions and other information of the Bitcoin system. All the transactions from the beginning are recorded in the network, which is managed by the Bitcoin system (now it's about 13G). Each block is added to the previous block. Then all the blocks become a huge chain, we call it Blockchain which includes all transaction information from the beginning. In the meantime, the generating of new block is related to the creation of new Bitcoin according to the system.

The first block is called Genesis Block in which all of the variables needed to recreate the block are defined exactly. The first 50 Bitcoins (BTC) were released when this program first ran.

This code should be intended as evidence that the block was created on or after January 3rd, 2009. A comment as the first time stamp "The Times 03/Jan/2009 Chancellor on brink of second bailout for banks" was written in the code which can never be changed. The first 50BTC block reward went to address 1A1zP1eP5QGefi2DMPTfTL5SLmv7DivfNa, which can't be spent due to a quirk. Now this address remains like a founding address for people to thanks to the creator of Bitcoin. [12]

```
// Genesis Block:
// GetHash()      = 0x000000000019d6689c085ae165831e934ff763ae46a2a6c172b3f1b60a8ce26f
// hashMerkleRoot = 0x4a5e1e4baab89f3a32518a88c31bc87f618f76673e2cc77ab2127b7afdeda33b
// txNew.vin[0].scriptSig     = 486604799 4 0x736B6E616220726F662074756F6C69616220646E6F6
// txNew.vout[0].nValue       = 5000000000
// txNew.vout[0].scriptPubKey = 0x5F1DF16B2B704C8A578D0BBAF74D385CDE12C11EE50455F3C438EF4
// block.nVersion = 1
// block.nTime    = 1231006505
// block.nBits    = 0x1d00ffff
// block.nNonce   = 2083236893
// CBlock(hash=000000000019d6, ver=1, hashPrevBlock=00000000000000, hashMerkleRoot=4a5e1e
//   CTransaction(hash=4a5e1e, ver=1, vin.size=1, vout.size=1, nLockTime=0)
//     CTxIn(COutPoint(000000, -1), coinbase 04ffff001d0104455468652054696d65732030332f4a
//     CTxOut(nValue=50.00000000, scriptPubKey=0x5F1DF16B2B704C8A578D0B)
//   vMerkleTree: 4a5e1e

// Genesis block
const char* pszTimestamp = "The Times 03/Jan/2009 Chancellor on brink of second bailout f
CTransaction txNew;
txNew.vin.resize(1);
txNew.vout.resize(1);
txNew.vin[0].scriptSig = CScript() << 486604799 << CBigNum(4) << vector<unsigned char>((c
txNew.vout[0].nValue = 50 * COIN;
CBigNum bnPubKey;
bnPubKey.SetHex("0x5F1DF16B2B704C8A578D0BBAF74D385CDE12C11EE50455F3C438EF4C3FBCF649B6DE61
txNew.vout[0].scriptPubKey = CScript() << bnPubKey << OP_CHECKSIG;
CBlock block;
block.vtx.push_back(txNew);
block.hashPrevBlock = 0;
block.hashMerkleRoot = block.BuildMerkleTree();
block.nVersion = 1;
block.nTime    = 1231006505;
block.nBits    = 0x1d00ffff;
block.nNonce   = 2083236893;
```

Figure 11: Genesis Block [12]

Blockchain keeps being added by one block every 10 minutes without maximum number. New Bitcoin is generated when new block is added as a value of 50 BTC. But this number is halved every 210,000 blocks which means every 4 years in the system. The block structure includes Magic No, Blocksize, Blockheader, Transaction counter and Transactions. See the table below:

Field	Description	Size
Magic no	value always 0xD9B4BEF9	4 bytes
Blocksize	number of bytes following up to end of block	4 bytes
Blockheader	consists of 6 items	80 bytes
Transaction counter	positive integer VI = VarInt	1 - 9 bytes
Transactions	the (non empty) list of transactions	<Transaction counter>-many transactions

Table 4: Block Structure [5]

The system constantly hashes the block header when generating new block. The block is also occasionally updated as you are working on it. The procedure is the following:

1. Nodes listen to all the transactions in the Bitcoin network. Enter the memory pool (Tx Mem Pool) through verified transaction and update the Merkle Hash of transaction data
2. Update time stamp

3. Hash calculation to find the nonce
4. Redo the calculation until find the proper nonce for the reasonable hash
5. Package block: Put block header, then transaction data
6. Broadcast to the network
7. After new block is verified by other nodes, it is added to the blockchain.
   Main chain length + 1

A block header contains these fields:

Field	Purpose	Updated when...	Size (Bytes)
Version	Block version number	You upgrade the software and it specifies a new version	4
hashPrevBlock	256-bit hash of the previous block header	A new block comes in	32
hashMerkleRoot	256-bit hash based on all of the transactions in the block	A transaction is accepted	32
Time	Current timestamp as seconds since 1970-01-01T00:00 UTC	Every few seconds	4
Bits	Current target in compact format	The difficulty is adjusted	4
Nonce	32-bit number (starts at 0)	A hash is tried (increments)	4

Table 5: Block Header Structure [5]

Here is the code to show the hash calculation in Block 125552 as an example. The system first packages data and then applies double SHA256.

```php
$header_hex = "01000000" . // version
              // previous block hash
              "81cd02ab7e569e8bcd9317e2fe99f2de44d49ab2b8851ba4a308000000000000"
              // merkle root hash of transactions in this block
              "e320b6c2fffc8d750423db8b1eb942ae710e951ed797f7affc8892b0f1fc122b"
              // Time
              "c7f5d74d" .
              // Bits (Difficulty)
              "f2b9441a" .
              // Nonce
              "42a14695";
$header_bin = pack("H*", $header_hex);  // hex to bin
$h = hash('sha256', hash('sha256', $header_bin, true), true);  // double sha256

echo bin2hex($h), "\n";
// output: 1dbd981fe6985776b644b173a4d0385ddc1aa2a829688d1e0000000000000000
echo bin2hex(strrev($h)), "\n";
// output: 00000000000000001e8d6829a8a21adc5d38d0a473b144b6765798e61f98bd1d
```

Figure 12: Hash Function Source Code [13]

2.1.2 Timestamp Server

The Bitcoin system indeed relies on a powerful and non-manipulated Timestamp system. The timestamp ensures that the blocks must exist at the time, definitely, in order to get the blocks into the chain. Each timestamp includes the hash value of the previous timestamp, one by one to form the blockchain. In this case, each timestamp reinforces the ones before it. [3]

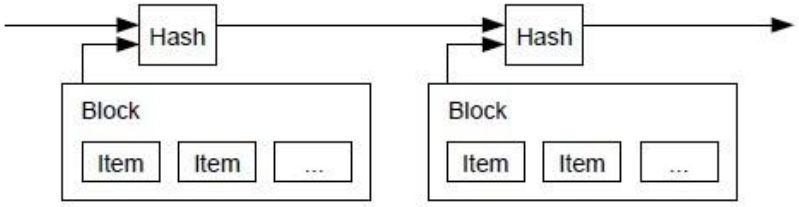


Figure 13: Timestamp Server [3]

2.1.3 Proof of Work

The Bitcoin system adopts proof-of-work by using a nonce in the blockheader. The block hash is started by N zero bits. The N is decided by the difficulty. So people have to calculate to find the nonce for the reasonable hash. The calculation ability depends on the CPU/GPU. After this process, the block is added to the chain and can't be changed. The final result is decided by the longest chain, which involves the biggest effort of proof-of-work. [3]

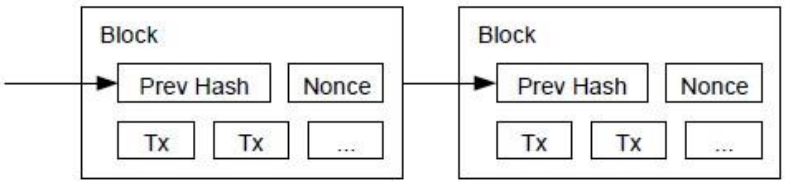
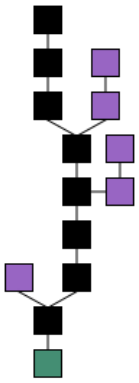


Figure 14: Proof of Work [3]



The longest chain must be chosen by system mechanism when branches exist. Branches will be abandoned when main chain is decided, which means the calculation work for those branches is in vain. [3]

Choosing the best chain:

1. Choose the longest branch from the branches with different length
2. Choose the most difficult branch from the branches with the same length
3. Choose the latest branch from the branches with the same length and difficulty
4. Follow the acceptance from the network if all terms are the same in the blockchain. Wait block length + 1 and start selecting the chain again.

2.1.4 Incentive

Bitcoin system has its own convention to generate new coins to those people who make contribution to the Bitcoin network. In the system convention, the first input is from the first transaction in a block with new coins which come from the reward of the first creator of the new block. This process becomes an incentive for users to support the Bitcoin network and provides new coins to the Bitcoin system. It's a very smart convention without any other third or central party compared with the traditional currency. This process seems like a gold miner's work. So we call the process mining, and the people who participate in the work miners. In this case, the mining work is a large amount of calculation which is related to CPU and GPU time and electricity expended. [3]

In the beginning, the reward is 50BTC for per new block, and then becomes 25 after 4 years due to system convention. So we can deduce that the maximum number of Bitcoin is 21,000,000. After that, the incentive can be turned to transaction fees. If the transaction output is less than its input, the difference will be added to the reward of the new block which includes the transaction. After the 21,000,000 Bitcoin is mined, the incentive can be totally transferred to transaction fees.

2.1.5 Merkle Tree

A block includes many transactions of which hashes are stored like a tree and finally stored in the root hash. The Bitcoin system will discard some part of the previous transactions information in order to save disk space. This process will not break the block's hash. All the transactions information is still hashed in a Merkle Tree. A block header would be about 80 bytes after compressing process. New block is added every 10 minutes, 80 bytes * 6 * 24 * 365 = 4.2MB per year.

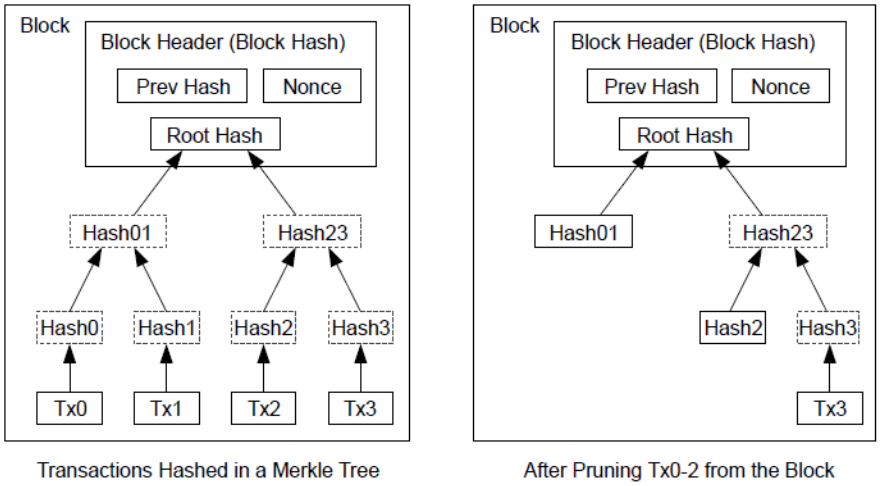


Figure 15: Merkle Tree [3]

Blockheader of 80 bytes fields inside is the following:

Field	Size (Bytes)
Version	4
hashPrevBlock	32
hashMerkleRoot	32
Time	4
Bits	4
Nonce	4

Table 6: Blockheader Structure [14]

2.1.6 Bitcoin Address (Account)

Bitcoin account is formed by random numbers and letters, we call it address. It's indeed a hash value of a public key generated by a public key algorithm. Private key is a personal key for the account owner while the account itself is the binding public key which can be broadcasted to the Bitcoin network as a receiver's account. No one can deduce the private key from the Bitcoin address. The key pair is generated randomly using ECDSA -- Elliptic Curve Digital Signature Algorithm. The Bitcoin address is calculated using SHA-256.

The process of generating an address from a private key is shown in the following and described after the figure:

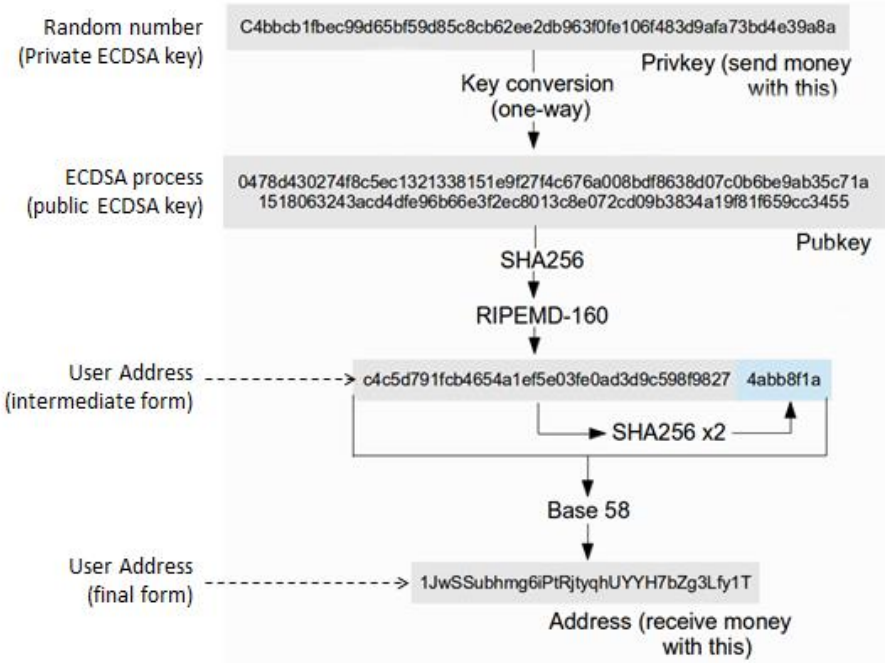


Figure 16: Process of Generating Address [15]

Step 1: Generate ECDSA Private Key:
Example:
18E14A7B6A307F426A94F8114701E7C8E774E7F9A47E2C2035DB29A206321725

Step 2: Using ECDSA Private Key, calculate ECDSA Public Key:
Example: 0450863AD64A87AE8A2FE8….82BA6

Step 3: Create Hash of the public key using SHA-256 algorithm:
Example:
600FFE422B4E00731A59557A5CCA46CC183944191006324A447BDB2D98D4B408

Step 4: Apply RIPEMD-160 algorithm to the value created in Step 3:
Example:
010966776006953D5567439E5E39F86A0D273BEE

Step 5: Suffix Bitcoin version number to the value created in Step 4:
Example:
00010966776006953D5567439E5E39F86A0D273BEE

Step 6: Apply SHA-256 to the result of Step 5:
Example:
445C7A8007A93D8733188288BB320A8FE2DEBD2AE1B47F0F50BC10BAE845C094

Step 7: Apply SHA-256 to the result of Step 6:
Example:
D61967F63C7DD183914A4AE452C9F6AD5D462CE3D277798075B107615C1A8A30

Step 8: Extract the first four bytes of the result of Step 7:
Example:
D61967F6

Step 9: Append the value from Step 8 to the value from Step 5:
Example:
00010966776006953D5567439E5E39F86A0D273BEED61967F6

Step 10: Encode in Base58 the value from Step 9:
Example:
16UwLL9Risc3QfPqBUvKofHmBQ7wMtjvM (This is user’s Bitcoin Address)

The Wallet (online or local) verifies the address using the following process:

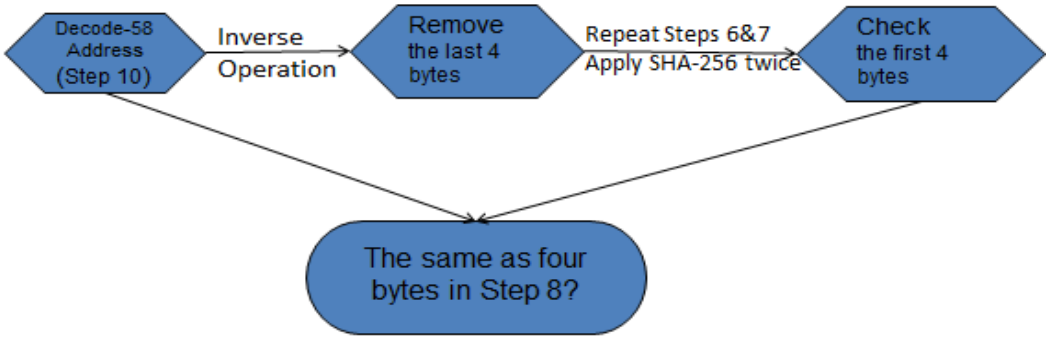


Figure 17: Verification of Address

2.2 Current Status of the Bitcoin Network Pool

There is no central Bitcoin server in the Bitcoin network. All users (nodes) use the same Bitcoin protocol and form a P2P Bitcoin network. Bitcoin users make transaction between online or local wallets, and broadcast the transaction to the network. The transactions are combined into a block. Then miners calculate the Nonce of the new block in order to get the reward for their work. All the merchants and exchanges using the Bitcoin protocol inside their web portal are established to develop the Bitcoin related business.

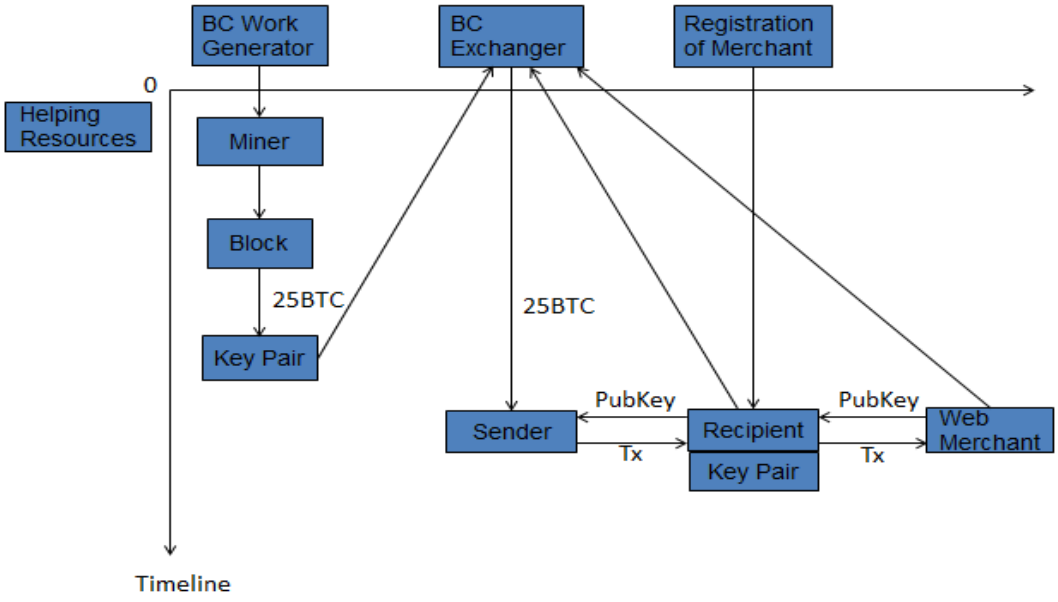


Figure 18: Bitcoin Function Architecture

2.3 Bitcoin Community and Other Supporting Organizations

Bitcoin was first known by people through a paper published by Satoshi Nakamoto. After the system was set up, Bitcoin Foundation (https://bitcoinfoundation.org) and Community (https://bitcoin.org/en/community) were set up to support further improvements and network operations where we can find important information about

Bitcoin and its official client (https://bitcoin.org). The chairman of the Bitcoin Foundation is Peter Vessenes. The aim for the Foundation is to support the core development team led by Gavin Andresen, hold conference and enhance the digital security of the Bitcoin network, like an opt-in certification for Bitcoin business.

Companies or individuals can be a member of Bitcoin Foundation by support to them. There are different rights for the different membership levels. Donate Bitcoin is a more transparent and worthy way to charity, since all the transactions are broadcasted to the network. So people will know what exactly they do for those donations.

Figure 19: Bitcoin Charities [16]

2.4 Open–Source Resources

Bitcoin is an open-source project, the official wallet and some related resources can be found and downloaded from Github, Gitorious and luke.dashjr.org, such as wallets, web application, mining software, servers and so on.

2.4.1 Wallets for Consumers

Component Name: [Bitcoin-Qt]
Download URL location: [https://bitcoin.org/en/download]
Component Function: [Official Bitcoin wallet UI using C++, which supports Linux/MacOSX/Windows. The whole block chain must be downloaded]

Component Name: [MultiBit]
Download URL location: [https://multibit.org/]

Component Function: [Light Bitcoin wallet in Java for Linux/MacOSX/Windows, which synchronizes fast and does not download the complete block chain]

Component Name: [Electrum]
Download URL location: [https://electrum.org/]
Component Function: [Light wallet for Linux/MacOSX/Windows/Android in python, which doesn't need to download the block chain]

Component Name: [Armory]
Download URL location: [https://bitcoinarmory.com/]
Component Function: [Bitcoin wallet for Linux/MacOSX/Windows in Python, which needs to download block chian]

Component Name: [Bitcoin-js-remote]
Download URL location: [http://tcatm.github.io/bitcoin-js-remote/]
Component Function: [A Bitcoin UI in JavaScript with QR code]

Component Name: [Bitcoin WebUI]
Download URL location: [https://github.com/TheSeven/Bitcoin-WebUI]
Component Function: [JavaScript Bitcoin user interface]

Component Name: [Bitcoin webskin]
Download URL location: [https://github.com/zamgo/bitcoin-webskin]
Component Function: [PHP Bitcoin user interface]

2.4.2 Various Servers

Component Name: [btcguild]
Download URL location: [https://www.btcguild.com/]
Component Function: [Mining pool sever with web registration]

Component Name: [ghash.io]
Download URL location: [https://ghash.io/]
Component Function: [mining pool server with web registration]

Component Name: [Slush's pool]
Download URL location: [https://mining.bitcoin.cz/]
Component Function: [mining pool server with web registration]

Component Name: [Deepbit]
Download URL location: [https://deepbit.net/]
Component Function: [mining pool server with web registration]

Component Name: [p2pool]
Download URL location: [http://p2pool.org/]
Component Function: [Python Bitcoin mining server using Bitcoin address without registration]

Component Name: [stratum-mining]
Download URL location: [https://github.com/slush0/stratum-mining]
Component Function: [Bitcoin mining pool server open source code with stratum protocol for Slush pool]

Component Name: [50BTC]
Download URL location: [https://50btc.com/]
Component Function: [Mining pools sever with web registration]

2.4.3 Various Tools

Component Name: [BFGMiner]
Download URL location: [http://bfgminer.org/]
Component Function: [Mining software in C]

Component Name: [MultiMiner]
Download URL location: [http:// http://www.multiminerapp.com/]
Component Function: [Mining software in C# with BFGminer engine]

Component Name: [CGminer]
Download URL location: [http://ck.kolivas.org/apps/cgminer/]
Component Function: [Mining software in C]

Component Name: [GUIMiner]
Download URL location: [http://guiminer.org/]
Component Function: [CPU/GPU mining software in Python]

Component Name: [50miner]
Download URL location: [http://50miner.org/]
Component Function: [GUI mining software which supports Poclbm, Phoenix, Diablo Miner, Cgminer]

Component Name: [MultiBitMerchant]
Download URL location: [https://github.com/gary-rowe/MultiBitMerchant]
Component Function: [Source code for Bitcoin ecommerce platform in Java]

Component Name: [MultiBitExchange]
Download URL location: [https://github.com/zscott/MultiBitExchange]
Component Function: [Source code to build Bitcoin exchange platform in Java]

Component Name: [ghash.io]
Download URL location: [https://ghash.io/]
Component Function: [mining pool server with web registration]

Component Name: [P2PoolExtendedFrontEnd]
Download URL location: [https://github.com/hardcpp/P2PoolExtendedFrontEnd]
Component Function: [P2Pool front end source code which shows the status of the mining pool]

Component Name: [P2Pool]
Download URL location: [https://github.com/forrestv/p2pool]
Component Function: [The source code of the P2Pool server in python]

Component Name: [bitcoinjs-gui]
Download URL location: [https://github.com/bitcoinjs/bitcoinjs-gui]
Component Function: [The source code of a web browser Bitcoin client in JavaScript]

Chapter 3: Roles, Components and Protocols

3.1 Bitcoin Network

There is no central administration for Bitcoin system, since it's a P2P network. However, the whole network can be described as three groups of components: (1) Online and local wallets, (2) miners and mining pool, (3) service servers (exchange, bank, shops, merchant and so on). The function of wallets is just for transaction no matter it is online or local software. Services are related to how to use, store, buy, sell, pay and exchange Bitcoin. They are normally different web user interface which integrate the Bitcoin core protocol. Miners and mining pools are the most import part of Bitcoin system, because the whole Bitcoin relies on the process. Bitcoin system can't work without miners and mining. The mining pool is the way to let people get together and make the mining process more efficient. It's impossible for a single person to mine Bitcoin without a strong computing power now.

3.2 Miners

Miners have two groups of functions: mining and transactions verification. Their work is to verify transactions and add new blocks in order to get Bitcoin reward. It is an incentive way to keep the Bitcoin system running as we mentioned in the previous chapter. At the beginning, it was easy to be a solo miner with normal computer by using CPU/GPU computing for hash. But now, the difficulty is too high to mine the Bitcoin only by single person with normal computer. A lot of specific hardware and a group of GPUs are developed to do the mining work.

3.2.1 Mining: Components, Process, and Protocol Messages

Bitcoin mining server uses **getblocktemplate** as the mining protocol which is developed to replace the old getwork mining protocol. It gives the block creation to the miner rather than the authority, which improves the blocks decentralization. [17]

Communication between a miner and mining server in the mining process is the following:

1) The miner who would like to join the mining pool requests a block template by vreating and sending to the mining server the following messages:

{"id": 0, "method": "getblocktemplate", "params": [{"capabilities": ["coinbasetxn", "workid", "coinbase/append"]}]}

2) Mining server will reply with the following messages that are needed to start mining procedure:


```
{
 "error": null,
 "result": {
   "coinbasetxn": {
     "data": "0100000001000000000000000000000000000000000000000000000000000000000000000000
0000000000ffffffff1302955d0f00456c6967697573005047dc66085fffffffff02fff1052a01
0000001976a9144ebeb1cd26d6227635828d60d3e0ed7d0da248fb88ac0100000000000001976
a9147c866aee1fa2f3b3d5effad576df3dbf1f07475588ac00000000"
   },
   "previousblockhash": "000000004d424dec1c660a68456b8271d09628a80cc62583e5904f5894a2483c",
   "transactions": [],
   "expires": 120,
   "target": "00000000ffffffffffffffffffffffffffffffffffffffffffffffffffffffff",
   "longpollid": "some gibberish",
   "height": 23957,
   "version": 2,
   "curtime": 1346886758,
   "mutable": ["coinbase/append"],
   "bits": "ffff001d"
 },
 "id": 0
}
```


Figure 20: Mining Server Reply Message [17]

Now it is almost impossible to mine Bitcoins by a single person due to the high difficulty. Normally, miners use mining pools to make mining more efficient. To be a miner, normally you need mining software which can be downloaded and choose the mining pool you prefer. Take GUIminer below as an example. You can choose different mining pool servers in the list and then register yourself on its website. After registration, check your workers and make settings for your worker. Then log in with your worker information to start mining. Note that registration account is different from the worker account.

This is an example for worker information. Visit Slush pool's web page and register as a user. Then create workers in order to mine.

Registration of a miner at the Slush Pool:

Workers

Average hashrate in last 10 rounds: 0 Mhash/s

Register new worker

Login	Password	Found blocks	Current shares	Score	Last share at	Mhash/s*	Actions
mhuan169.worker1	xBK5uSBh	0	0	0	-	0	Edit | Delete

* The calculation is based on the number of shares so far, which may not be accurate for slow workers.

Figure 21: Registration of a miner at the Slush Pool

Normally you can input any Bitcoin address for receiving rewards like Slush pool. Those kinds of websites integrate the transaction and wallet function inside. Your reward will

be recorded in your account and will be transferred to your address when reaching a certain amount. In Slush pool, you can input your offline Bitcoin address to get your reward in Bitcoins. Your reward can only be sent when it reaches a certain amount which you set.

Panel for account setting in Slush Pool:

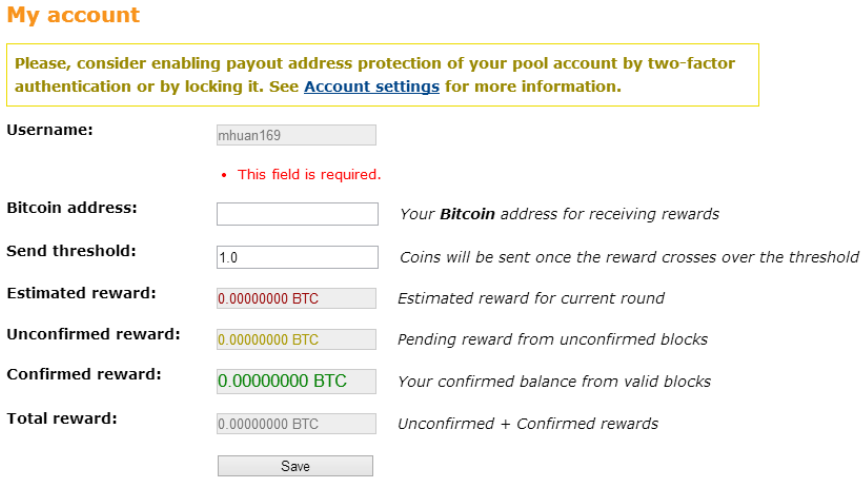


Figure 22: Panel for account setting in Slush Pool

There are other popular mining pool operators, like BTC Guild, Ghash.io, F2Pool and Eligius:

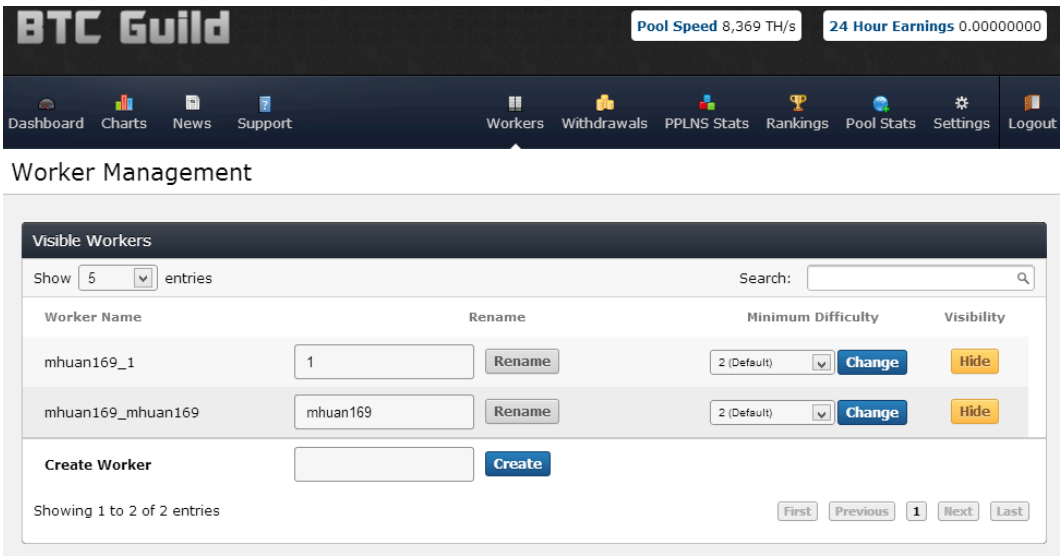


Figure 23: Registration of a miner of BTC Guild

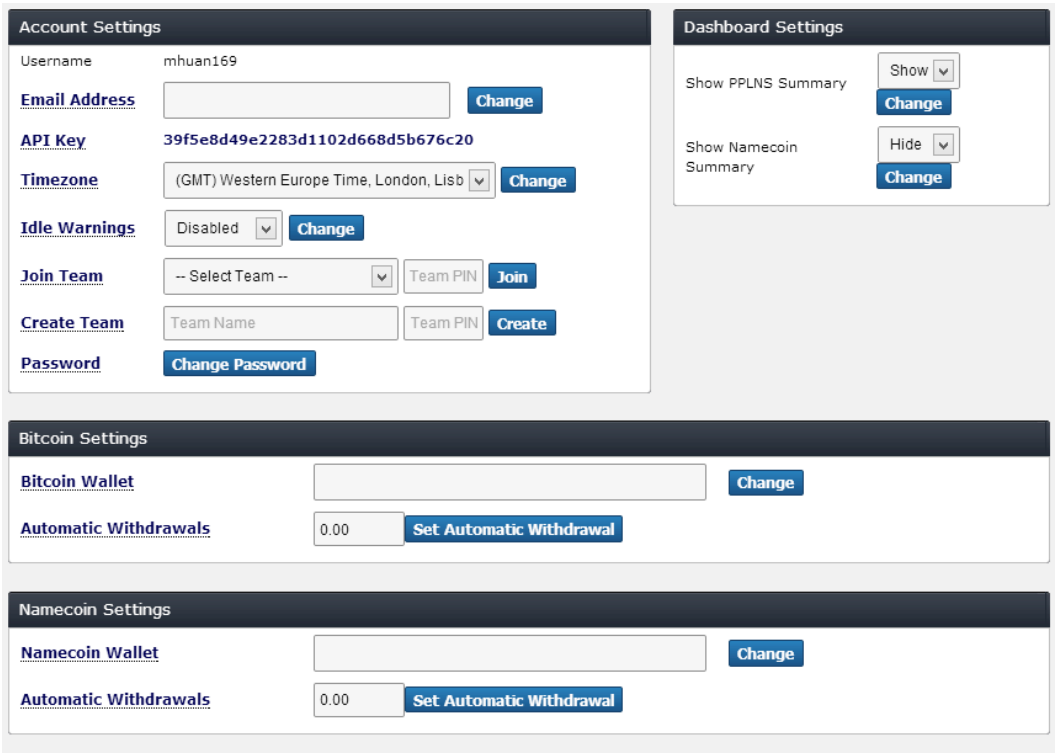


Figure 24: Panel for account setting in BTC Guild

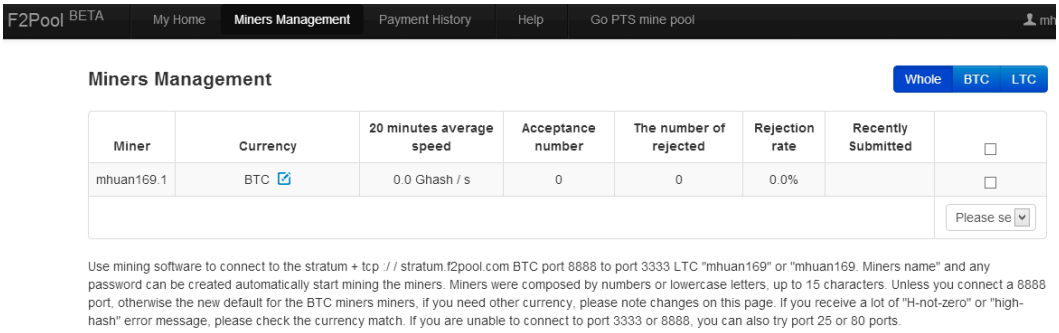


Figure 25: Registration of a miner of F2Pool

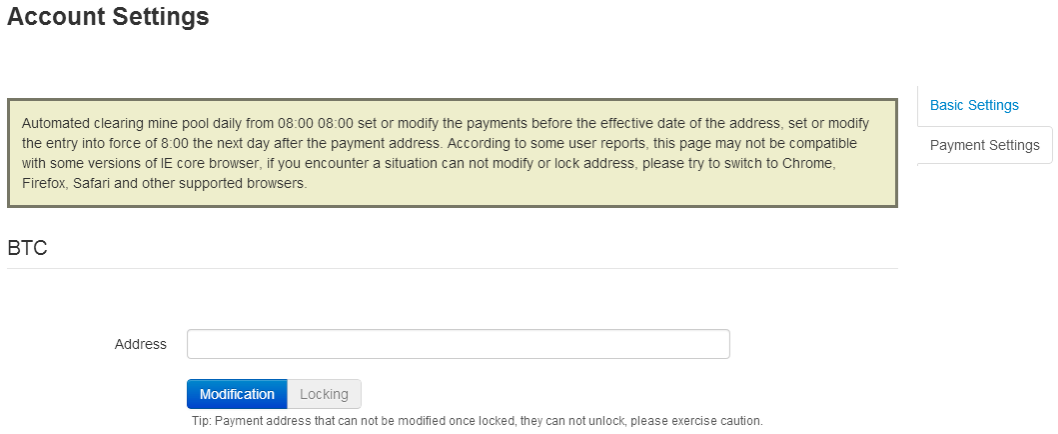


Figure 26: Panel for account setting in F2Pool

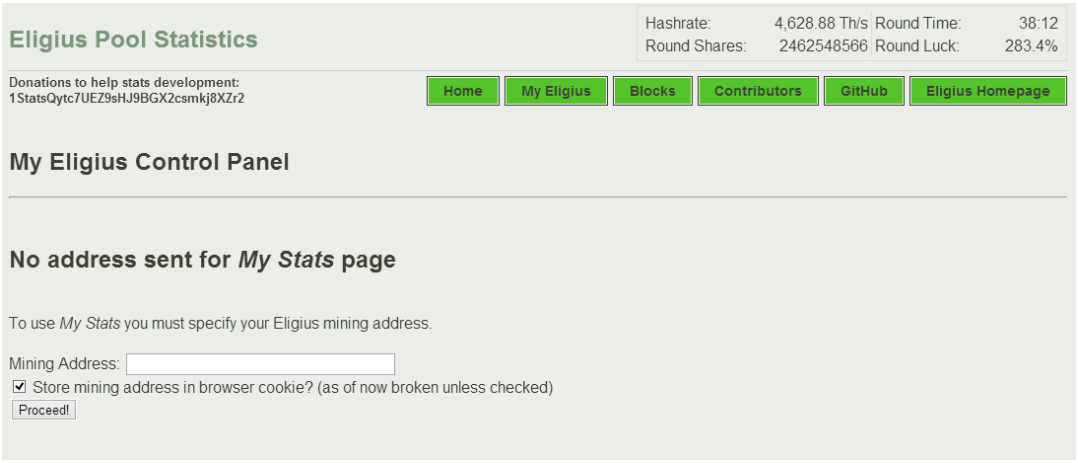


Figure 27: Eligius Pool Control Panel

The mining operation of Ghash.io is different from others. They have their own hardware to handle all mining work in their pool. In order to be a user, you need to buy some computing power based on the real time market on their website and then mine Bitcoin with the bought computing power. The worker will be automatically generated when you have bought computing power.

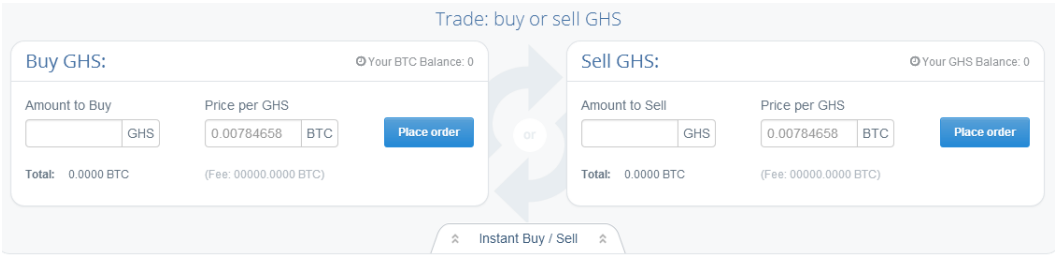


Figure 28: Computing Power Trade of Ghash.io

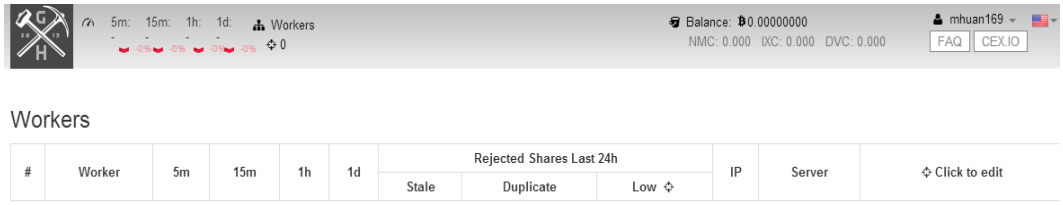


Figure 29: Miner Panel of Ghash.io

The aim of mining software is to connect the local device to the mining pool server and use your GPU/CPU to mine Bitcoin. GPU is proved to have much stronger computing ability for hash than CPU, more and more mining software just abandon CPU mining and turn to GPU approach. Some of them have GUI, but some of them just have command line. If you would like to try single mining, you have to download all the blockchain in your local computer and use official Bitcoin wallet Bitcoin-Qt as a communication server. Then initialize the process with one of the mining software.

Panel to choose a mining pool and to input worker information using GUIMiner

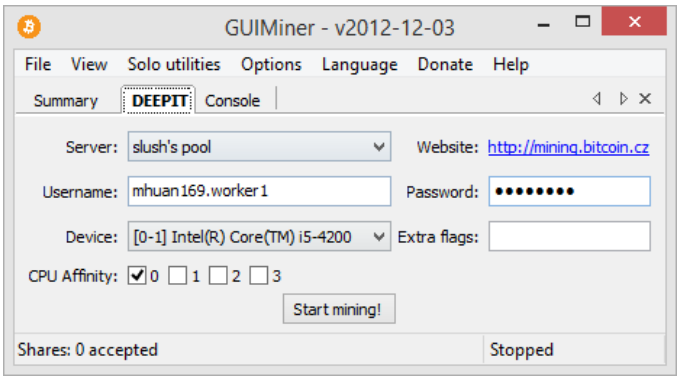


Figure 30: GUIMiner Interface 1

Different mining pools have their websites for registration on the right side. Some mining software has no GUI like "cgminer" and "bfgminer". Normally miners just need to input the mining pool address and port in order to connect to the server with their username and password. The general principle of mining is to join the Bitcoin P2P network and compute the hash with others.

The panel for selecting Mining Pool with Mining Client is the following:

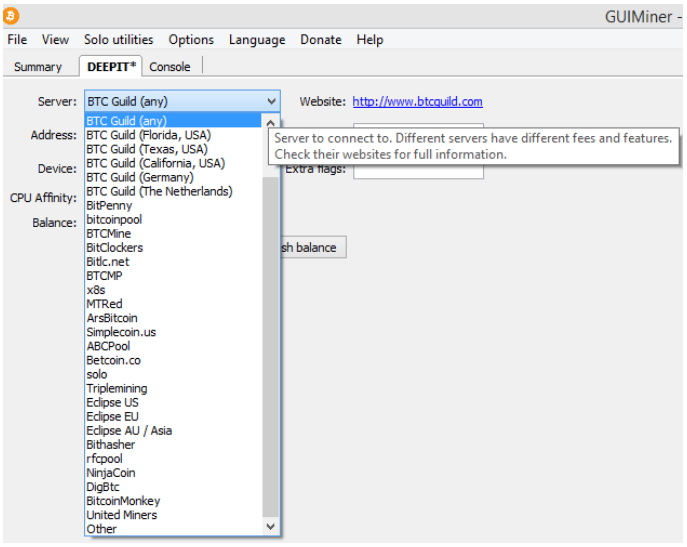


Figure 31: GUIMiner Interface 2

Different mining pools use different kinds of share policies for its miners. The most common share policies used for current mining pools are PPS and PPLNS. But there are also other policies like Scores, Slush, DGM and so on, which may be more or less extended from PPS and PPLNS. The world's biggest mining pool BTC Guild uses PPS and PPLNS for its miners. Its total mining capability is 5609 TH/s in February. [18]

PPS (Pay Per Share) Policy

This method is a stable way to share the rewarded Bitcoin. The miners get a guaranteed rate for each of their valid shares. The risk is low compared to PPLNS. But the profit is quite low with a high handling fee in this policy. [19]

PPS example in BTC Guild (per share):
(1 / Network Difficulty * 25) - Pool Fee (7.5%)

PPLNS (Pay Per Last N Shares) Policy

The policy is based on the last N shares to pay the miners. The submitted shares are put into a "group" with certain number of shares. When a "group" is formed, it will be considered an "open group". The group will continue working until the later 10 "open group" are formed. While a "group" is open, all "open groups" will get payment from any block the pool finds (10% of the block per "group"). Then you can continuously receive payment if you stopped mining. So it depends on if you are lucky or not. [19]

PPLNS example in BTC Guild (Per "group"):
((Block Value + Transaction Fees) / 10) - Pool Fee (3%)

Different reward policies are captured at these references. [20] [21]

The chart below is the computing speed pie chart for mining pools in April which is real - time update based on the information of latest 2016 blocks. There will be a risk to make the 51% Attack if one mining pool has more than 50% computing availability of the whole Bitcoin network.

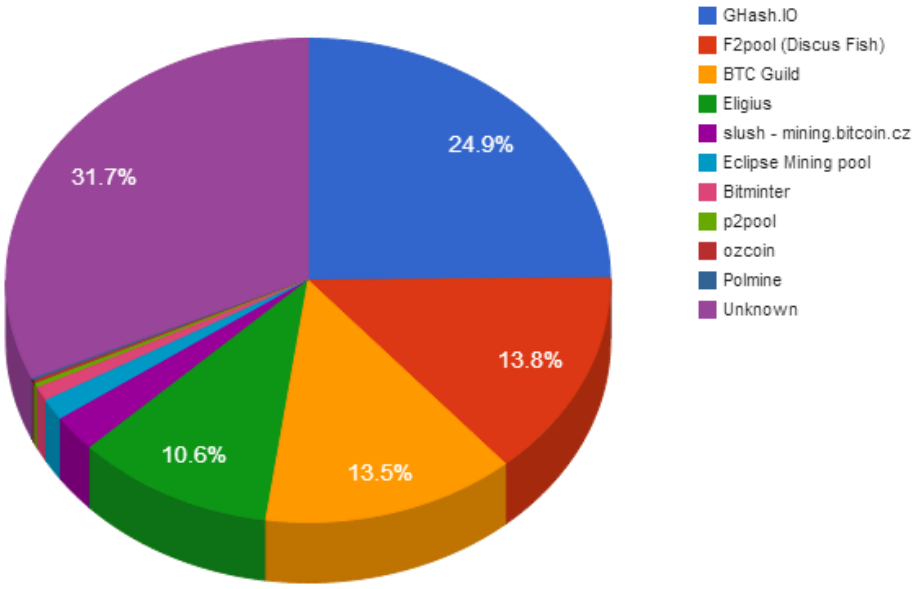


Figure 32: Computing Availability of Whole Bitcoin Network [22]

3.2.2 Verification of Transactions

Miners use Bitcoin core module to synchronize with all the blocks in the Bitcoin network, and get blocktemplate to know what they need to calculate and verify. Each node in P2P

network collects new transactions and packages them into new block. Miners will work to find the nonce of new block and then broadcast to the network. Others will check the hash and accept it when all the transactions inside are valid.

The steps to validate transactions within a new block are the following:

1) Bitcoin new transactions will be seen by all nodes in the Bitcoin network.
2) New transactions are packaged into a block.
3) Miners work on finding a nonce for the block.
4) When a nonce is found, the block will be broadcasted to the Bitcoin network.
5) The block will be accepted only if all the transactions inside are valid.
6) After the acceptance, the previous block will be used as block hash for creating the next block in the chain.

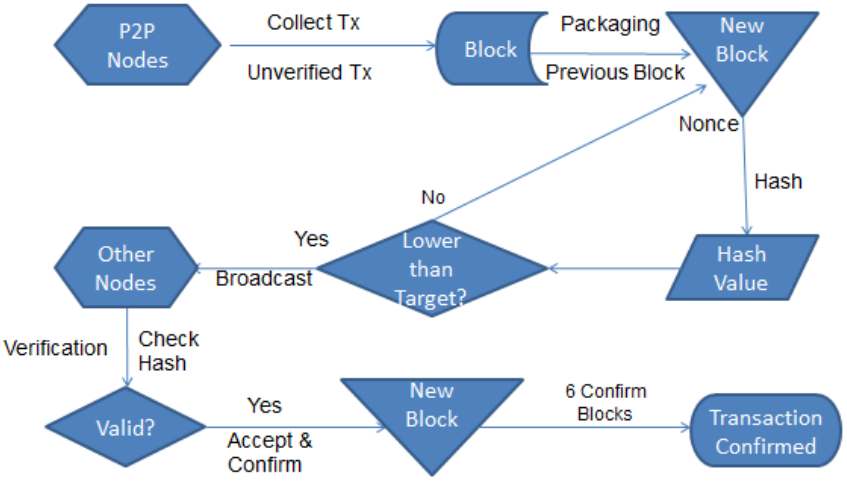


Figure 33: Verification and New Block Creation

Miners calculate the cryptographic hash functions using the formula:

SHA256(SHA256(version + prev_hash + merkle_root + ntime + nbits + x)) < TARGET (256 bit number)

What miners are doing is to find out the X; X= nonce(0~2^32).

TARGET depends on the generating time of new block. The Bitcoin network tries to produce one block every 10 minutes. But the real time of producing new block varies, since there are more and more users join the whole bitcoin network and more and more new transactions are made. So the network will retarget after 2016 blocks which is about two weeks. The smaller the value of the target, the more difficult it is to generate a block.

3.3 Users / Individuals

To be a Bitcoin user is not a complicated issue, but to be a secure and professional Bitcoin user is another issue. Each user needs a Wallet which can generate the Bitcoin address (account). The official Bitcoin-qt, MultiBit, Armory and Electrum are the main wallets people choose. For computer, the official Bitcoin-qt is a basic wallet which needs to download the whole blockchain (20G). The other three are light wallets which just need simple synchronization with the wallet server. There are also online wallets people can choose which will be easier for online exchanges. However, there is a risk to be hacked when storing your Bitcoin in online wallets. The encryption of the wallet normally should be manually done. Cold storage methods mentioned in 1.4 are strongly recommended to store the bitcoin address, since there is no absolutely safe when connected to Internet. By using a Bitcoin wallet, the user can easily transfer Bitcoin to any other address and receive Bitcoin through different receiving addresses created by the wallet. Bitcoin can be obtained by mining or bought through online exchanges. Now there are also ATMs in several countries which support selling and buying Bitcoins. What's more, you can just make a deal with your cash with any Bitcoin owners and ask them to directly transfer Bitcoin to your address. The signature can be used to identify that the account is truly owned by the person or not.

3.4 Merchants – Over-The-Counter and Web

There are a lot of ways to run business which support Bitcoin transaction. A merchant who has already run his business with good reputation can directly open the Bitcoin service if they want. They can just use a Bitcoin account to receive payments and synchronize the Bitcoin price with some exchanges for his goods. They can use an offline address as payment address to improve the security. Since the real Bitcoin price depends on different platforms and always fluctuate, merchant can put goods for auction for a period of time, and make a deal with the highest bid.

There are two most common way to support Bitcoin for business. Use API, like Bitpay and Coinbase for the payment method in merchant's online store to send invoice to buyer, or accept intermediate called Escrow services to support Bitcoin payment. The intermediate will charge merchant for each transaction and make sure the trading will be secure with anonymous buyers and sellers. If the buyer does not release the escrow payment to the seller then after 30 days the funds are donated to the I2P project.
https://en.bitcoin.it/wiki/Bitcoin_Escrow_Service

The picture below is an invoice created by Bitpay for an online shop. You can use app in mobile to scan QR code or transfer the money to the address. The validity time for the invoice is 15 min.

Figure 34: Bitpay Invoice

3.5 Exchanges

Exchanges are important in Bitcoin network. They deal with buying and selling between Bitcoin and normal currencies. They could be ATMs, market exchanges or fixed rate exchanges.

Bitcoiniacs put the first ATM for Bitcoin in realty in Canada. Now there is another one in Singapore. ATM only supports the local currency. The maximum amount of exchange is limited. The ATM in Canada is based on the exchange service from VirtEx.

Market exchanges are based on the match of buy and sell orders. So the exchange rate will fluctuate based on the market situation. The world's largest exchange MtGox was hacked so that the exchange rate of its Bitcoin fell to less than 100 USD compared with 600 USD in other exchanges at that time. Now the main market exchanges are Bitstamp, BTC-E, CAMP BX, Coinbase and so on. To be a verified user of those exchanges needs extremely requirement of copy of identity and proof of address like Bank statement, official home address certificate, tax return or bill and permanent Drivers' License. Users who would like to sell Bitcoin have to transfer Bitcoin from other wallets to the market exchanges. Users who would like to buy Bitcoin should normally input their bank account information as basis and then pay money to the account in the exchanges. The market exchanges don't support credit cards. When users have balance in Bitcoin or normal currency, they can buy or sell Bitcoin through the market exchanges. It's risky that the exchanges may be hacked and lost its Bitcoin.

The fixed rate exchanges use a fixed exchange rate according to the Bitcoin exchange market. The whole process will be much easier than the Market exchanges. Take btcx.se for example, the fixed exchange rate is specified. Like the exchange rate in bank, the selling price is higher the buying price. Users just need to transfer the money to the

operator's bank account with the order number. Then the transaction will be processed later. The Bitcoin exchange has a high risk sometimes. So finding a trusted exchange is most important and also trying not to deposit any money on the internet will be much appreciated.

3.6 Service Providers

There are many providers of services that assist consumers and merchants with various Bitcoin functions, other than exchanges. Like transaction counters, Bitcoin banks, payment brokerage servers and other convenient services.

Coinbase (https://www.coinbase.com) is browser based online wallet with cold storage technology. A user must bind the bank information and get verified to start buy and sell Bitcoin. There is strict verification process to open an account. Coinbase also provide Bitcoin support payment. A merchant can create an embedded payment button on his website which is linked to his Coinbase account. The buyer can choose to pay with Bitcoin through this service.

Blockchain (https://www.blockchain.info) is an online wallet with encryption and also support wallet app for Android and iOS with QR code. The feature of Blockchain is that it provides various Bitcoin charts and currency statistics, different APIs for developers to acquire data from Blockchain.info.

Snapcard (https://www.joinsnapcard.com) is a convenient Bitcoin payment cart which supports Amazon, Ebay and so on. It uses the snapCard bookmark to user's browser and supports with most online stores. Instead of using merchant site's shopping cart, the user can check out with snapCard's shopping cart using the snapCard bookmark. Ordered items will synchronize in the snapCard account, and the order will be invoiced within 20 minutes. Once the user has made payment to the invoice, Snapcard will place the order with related merchant and update the tracking/shipping information in the account.

Bitcoinera (https://bitcoinera.net/) is a kind of online bank which pays user 6% monthly interest for deposit. In the meantime, there are also different investments provided by the operator

Chapter 4: Demonstration

4.1 Description of the Overall Demonstration System

The system is a whole set of Bitcoin functions which includes Bitcoin wallet, mining server with web interface to show real-time data and mining software. The mining server is based on P2Pool technology.

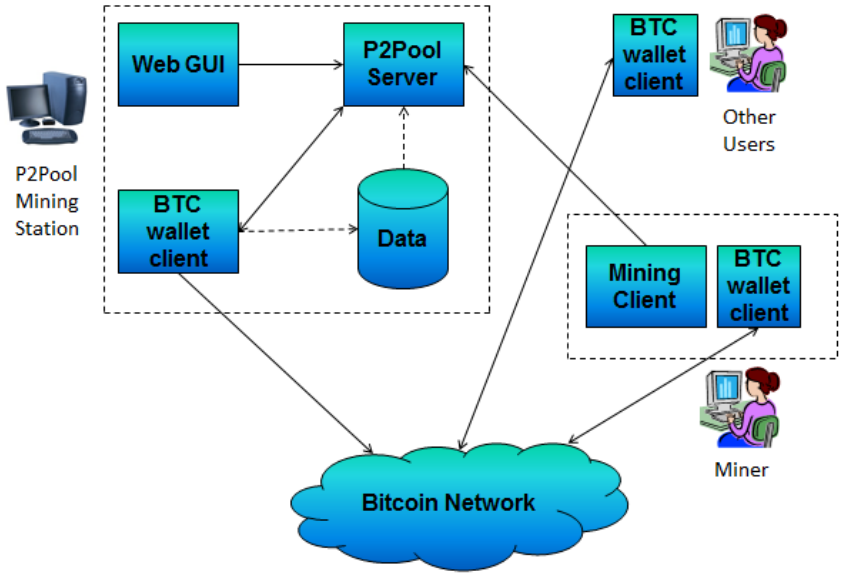


Figure 35: Architecture of Demo System

P2Pool is a decentralized Bitcoin mining pool that works by creating a peer-to-peer network of miner nodes. P2Pool mining nodes work on a chain of shares similar to Bitcoin's blockchain. When a block is found, the reward is divided among the most recent shares in this share-blockchain. So the P2Pool network is something like P2P Bitcoin network, there is no central server. How Bitcoin network is created is like how P2Pool is created. So the demo P2Pool server is under P2Pool network and share the reward with other P2Pool server. The miner use Bitcoin address as the username to connect to the server in order to get reward. All rewards from P2Pool server will be transferred automatically to miner's Bitcoin address, the server Bitcoin address won't get any reward if the operation fee is set to zero. The administration of the people who join my server will be another issue. However, all the mining information will be recorded and shown on the web interface. So it's possible to develop services and become administrator based on the local mining pool. The aim of P2Pool is to use decentralization against attacks and improve security, the same like Bitcoin network. Other centralized pools like Deepbit and BTCguild were attacked before. They are also controlled by the people who run them in the dark. There will be a risk if one of them

has more than 50% computing power. But for P2Pool, there won't be DOS attack, cheating or 51% attack. So using decentralized mining pool is the perfect match to decentralized Bitcoin network. P2Pool is much complicated for common miners, compared with other centralized pools by just registering and connecting. That's why it's not so popular among mining pools. [23]

4.2 Downloaded and Installed Components

There are the components used in section 2.4 for the demo system, including P2Pool server, web front end for P2Pool server, wallet client Bitcoin-qt, and two different mining clients: CGminer and Multiminer.

Component Name: [P2Pool]
Download URL location: [https://github.com/forrestv/p2pool]
Component Function: [The source code of the P2Pool server in python]

Component Name: [P2Pool web front end]
Download URL location: [https://github.com/hardcpp/P2PoolExtendedFrontEnd]
Component Function: [Extended front end web interface for p2pool]

Component Name: [Bitcoin-Qt]
Download URL location: [https://bitcoin.org/en/download]
Component Function: [Official Bitcoin wallet UI using C++, which supports Linux/MacOSX/Windows. The whole block chain must be downloaded]

Component Name: [CGminer]
Download URL location: [http://ck.kolivas.org/apps/cgminer/]
Component Function: [Mining software in C]

Component Name: [MultiMiner]
Download URL location: [http:// http://www.multiminerapp.com/]
Component Function: [Mining software in C# with BFGminer engine]

4.3 Examples of Transactions and Demonstration

This is a processing Bitcoin payout transaction to the sending account 1Jb5LtYQpbuyejjPJVsqTzu28M94UodmFL with transaction fee 0.0001 BTC. It shows 8 nodes have seen this transaction in the Bitcoin network and only 1 confirmation. After 6 confirmations, this transaction will be confirmed by the Bitcoin network.

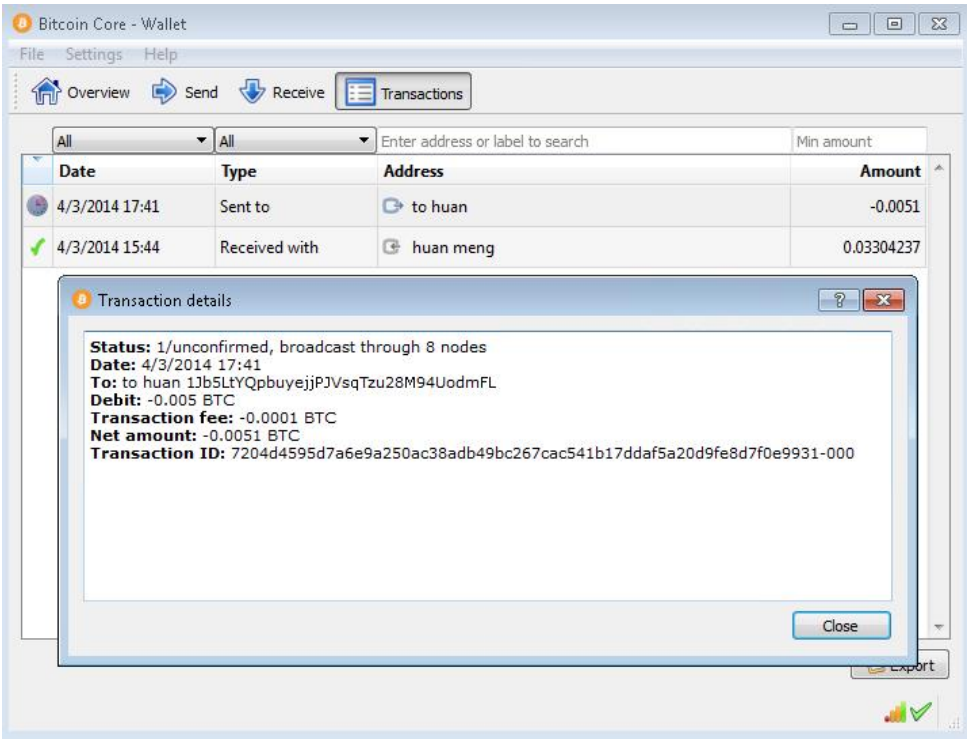


Figure 36: Transaction Information

This is the initialization of the P2Pool server. The Server needs to synchronize with the P2Pool shares, which takes several minutes. The server has a Bitcoin address 1Gx93ix…. which is used as for group mining. Therefore all rewards will be transferred to the server address if all miners input server address as the mining username. Otherwise, the reward will split automatically to the miners who use their own Bitcoin address as the mining username. In this case, the server can't get anything if there is no operation fee charged.

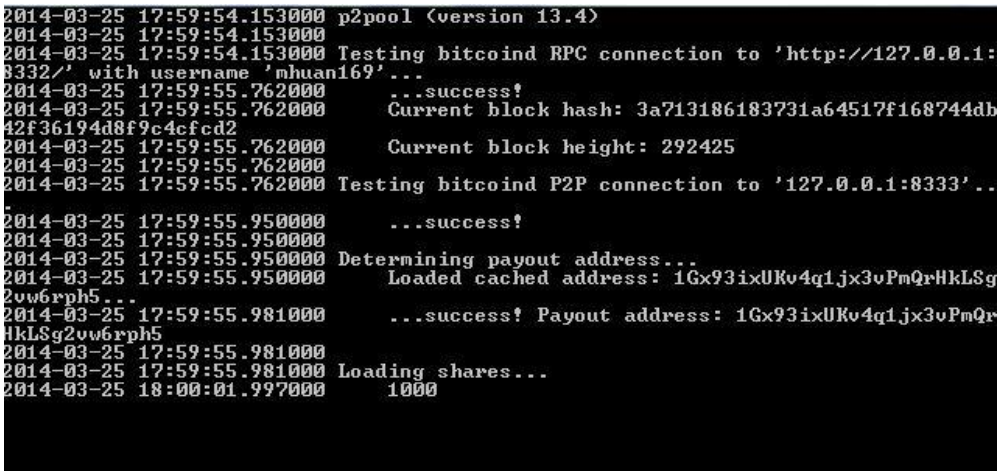


Figure 37: P2Pool Server Loading Share

The miner can use a mining client to mine BTC at the server. All the information can be seen on the mining client, especially the computing speed of hashes. The speed will

synchronize with the server and can be checked on the web GUI of the P2Pool server in the diagram.

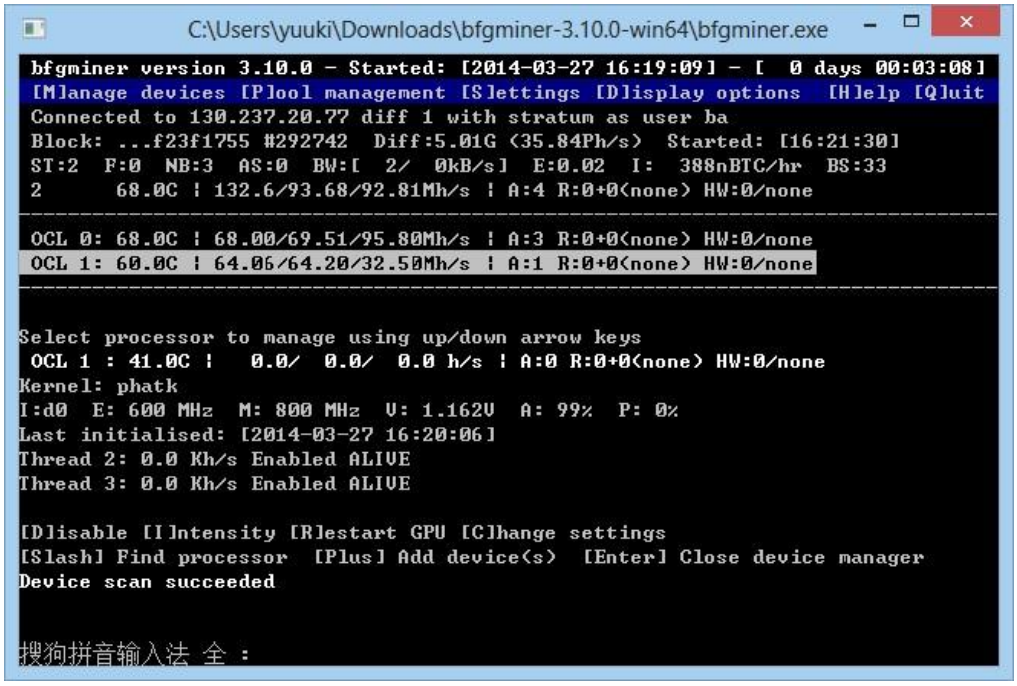


Figure 38: BFGminer

Multiminer is a miner with GUI based on bfgminer engine.

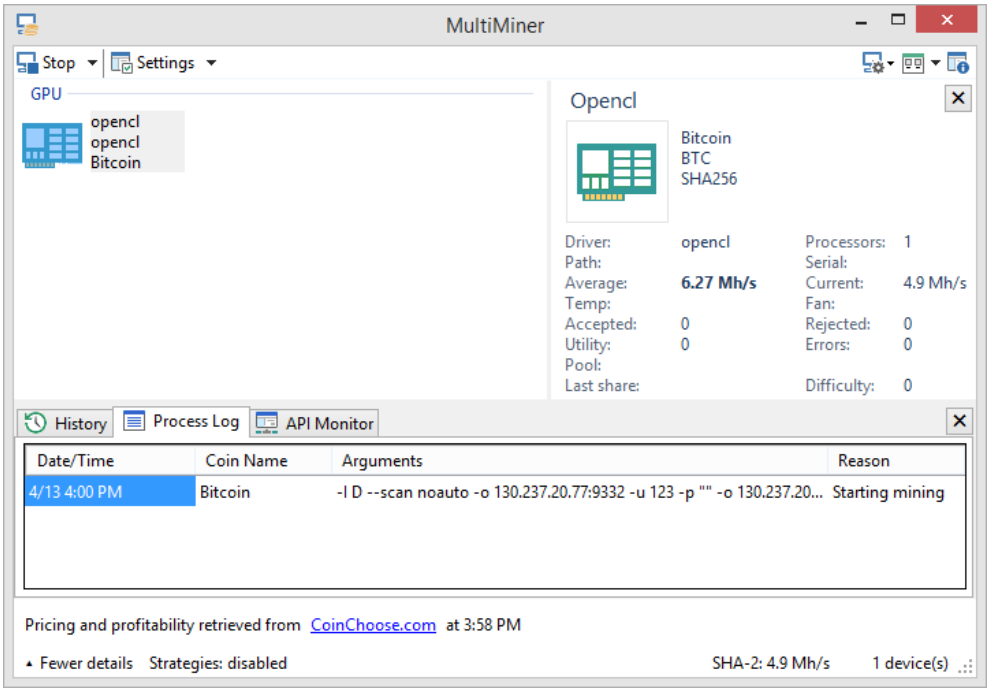


Figure 39: Multiminer

The P2Pool server displays local hash speed and the estimated time to have a share. The hash speed of the whole distributed P2Pool network can also be seen here together with the estimated time to find a block.

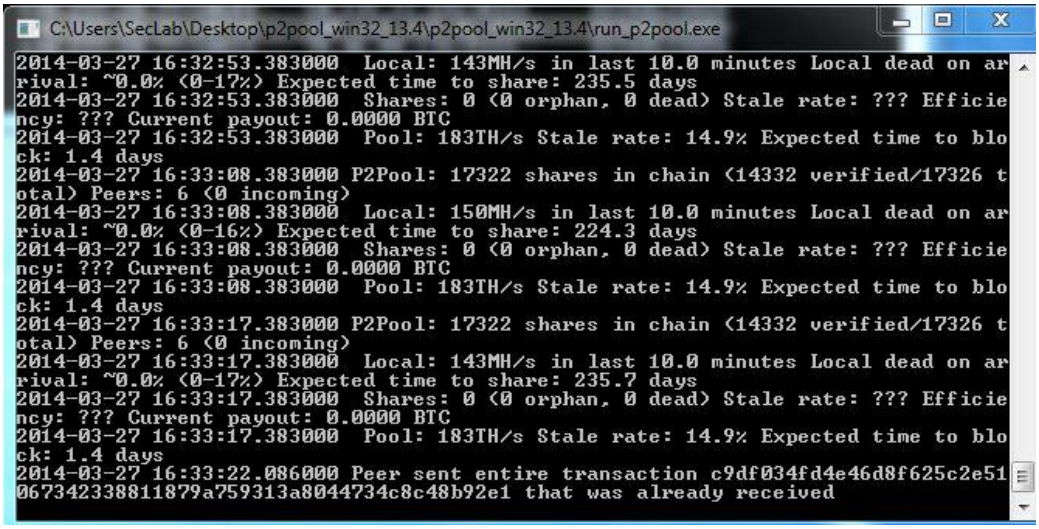
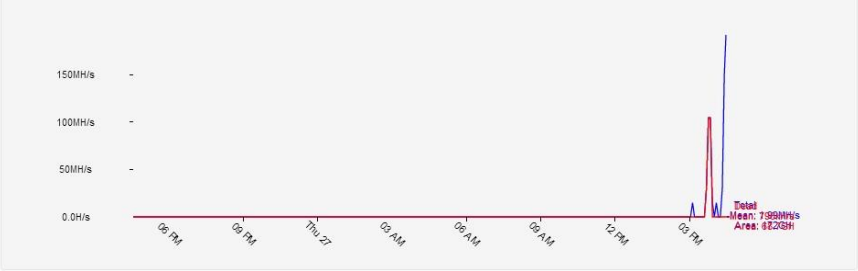


Figure 40: P2Pool Server Running Status

The web GUI for P2Pool is a display of the real-time P2Pool server and network situation, including local rate, pool rate, miners, time issue, traffic rate and so on. It's is possible to develop administration and management of the P2Pool server.



Local rate	150MH/s (0.0% DOA)	Expected time to share	5400 hours (324000 minutes)
Shares	0 total (0 orphaned, 0 dead) Efficiency: ???	Payout if a block were found NOW	0 BTC
Pool rate	183TH/s (15% DOA+orphan)	Share difficulty	680000
Node uptime	0.077 (1.848 hours)	Peers	6 out, 0 in
Current block value	25.10231634 BTC	Expected time to block	32.6 hours

Figure 41: P2Pool Server GUI

Chapter 5: Conclusions and Future Work

5.1 Further Research and Design Activities

The demo system is a whole set of Bitcoin functions with Bitcoin wallet, P2Pool mining server with web interface to show real-time data and mining software. Mining server is based on P2Pool technology. The whole set can be installed as a P2Pool mining station in any single computer as a server, and others who need only mining software and any kind of Bitcoin wallet can connect to this server to form a mining group and get paid. There are several issues that should be taken into consideration for further research.

1. Bitcoin wallet: The Bitcoin-qt wallet supports Bitcoin transaction and can be used to provide the address in order to get paid from mining. The wallet has only an option for user to encrypt the wallet with simple password, which is far from enough in security aspect. In the meantime, all transactions will be broadcasted to the network. Even though the account/address is formed by random characters, the transaction and the node information can be traced and analyzed by anyone in some ways.
2. The P2Pool server is based on a distributed P2Pool network. It is somehow intelligent to distribute the reward to miners in PPLNS. When the P2Pool server starts running, it will first get the share in P2Pool network from other nodes and keep communicating with the nearest nodes. The administration and security of P2Pool server should be taken into consideration in order to be an operator of the P2Pool server. [25]

5.2 Future Implementation and Deployment Activities

For a digital currency system, the most important issue is the security of the property and the reliability of transactions. Some new security extensions could be added to the demo system and improve the whole security of the system. The backup and recovery of the wallet data which contain private key for each address should be designed and organized in Bitcoin-qt. A better solution of concealing the user information including the transaction history and account in random characters should be improved and implemented. In the meantime, making the whole system user-friendly should also be considered.

5.3 New Standards

The offline wallet: The offline wallet is a kind of wallet which supports creation of transactions on an offline computer, and to broadcast the transactions from another computer with the wallet which has no private keys. If the wallet which broadcasts the

transaction is hacked, the user won't lose anything since there are no private keys in the wallet and that computer. The important information is always offline. [24]

References

[1] How Bitcoin Works – A Flowchart. http://www.sikharchives.com/?p=18828

[2] Bitcoin-depth analysis of the principles and techniques to achieve.
http://ivarptr.blogspot.se/2011/05/bitcoin_31.html

[3] Satoshi Nakamoto, “Bitcoin: A Peer-to-Peer Electronic Cash System”. 2009.
Available at https://bitcoin.org/bitcoin.pdf

[4] Bitcoins the hard way: Using the raw Bitcoin protocol
http://www.righto.com/2014/02/bitcoins-hard-way-using-raw-bitcoin.html

[5] Bitcoin – Wikipedia, Available from https://en.bitcoin.it/wiki

[6] Fergal Reid, Martin Harrigan, “An Analysis of Anonymity in the Bitcoin System”. 2011.
Available at http://arxiv.org/pdf/1107.4524v2.pdf

[7] https://blockchain.info/sv/tree/54323084

[8] Simon Barber, Xavier Boyen, Elaine Shi, Ersin Uzun. “Bitter to Better—How to Make Bitcoin a Better Currency”. 2012
Available at http://crypto.stanford.edu/~xb/fc12/bitcoin.pdf

[9] Bitcoin Attacks in Plain English. 2012.
http://codinginmysleep.com/bitcoin-attacks-in-plain-english/

[10]Elli Androulaki, Ghassan Karame, Marc Roeschlin, Tobias Scherer and Srdjan Capkun. “Evaluating User Privacy in Bitcoin”. 2013
Available at http://fc13.ifca.ai/proc/1-3.pdf

[11]http://www.forbes.com/sites/reuvencohen/2013/11/28/global-bitcoin-computing-power-now-256-times-faster-than-top-500-supercomputers-combined/

[12] Genesis Blcok. https://en.bitcoin.it/wiki/Genesis_block

[13] Bitcoin transactions, Bitcoin Labs - 618.io. http://618.io/

[14] https://en.bitcoin.it/wiki/Blocks

[15] http://8btc.com/article-386-1.htm

[16] https://bitcoin.org/en/community

[17] Getblocktemplate. https://en.bitcoin.it/wiki/Getblocktemplate

[18] Meni Rosenfeld. “Analysis of Bitcoin Pooled Mining Reward Systems”. 2011. Available at https://bitcoil.co.il/pool_analysis.pdf

[19] https://www.btcguild.com/index.php?page=support&section=howamirewarded

[20] https://en.bitcoin.it/wiki/Comparison_of_mining_pools

[21] https://en.bitcoin.it/wiki/Pooled_mining

[22] http://blockorigin.pfoe.be/chart.php

[23] https://en.bitcoin.it/wiki/P2Pool

[24] https://en.bitcoin.it/wiki/How_to_set_up_a_secure_offline_savings_wallet

[25] Jerry Brito, Andrea Castillo. “Bitcoin: A Primer for Policymakers”. 2013. Available at http://mercatus.org/sites/default/files/Brito_BitcoinPrimer.pdf