Galaxy Chain White Paper

Paul Hanks

galaxychain2018@gmail.com

Summary

Since the birth of bitcoin in 2009 years, there has been decentralization, no distribution unit, distributed accounting , encrypted wallet,and digital currency has entered into people's life. The importance of digital currency based on block chain technology and its epoch-making value significance are increasingly found. We recognize the genius idea of Satoshi Nakamoto and the exquisite network technology, but with the continuous mining of bitcoin, we gradually find some defects of this digital currency. We will not discuss the brilliant part of bitcoin. Let's briefly comb out its flaws: 1,the transaction with a long time confirm. When bitcoin wallet is first installed, it will consume a lot of time to download historical transaction data blocks. While bitcoin transactions, in order to confirm the accuracy of data, it will take some time to interact with the P2P network. After the whole network is confirmed, the transaction will be completed. 2,the price fluctuates greatly. As many speculators intervened, the price is greatly fluctuating, like roller coaster.that make bitcoin more suitable for speculation than commercial circulation. 3,the circulation is few.Compare with the 7 billion population in the world, The circulation of 21 million make it’s price is too high, and the ratio of per capita is too small. 4,the vulnerability of the trading platform. Bitcoin networks are robust, but bitcoin trading platforms are fragile. Trading

platform is usually a website, and the website will be attacked by hackers or shut down by the authorities. Based on this situation of bitcoin, we want to work hard to create a new type of alternative currency, which can gather the advantage of many digital currencies and avoid some of the shortcomings of other digital currencies. Because our team are all astronomical enthusiasts, we named it Galaxy Chain, abbreviation GCC. Galaxy Chain, is based on the technology of bitcoin, plus our understanding of the practical currency of the circulation field, the currency conceived by the new method of computing power combination. Here we will make a specific technical interpretation of it.

1 Introduction

It has been thousands years since the human currency went from shell to precious metal to the legal tender and then to the electronic settlement. Nowadays, the electronic payment of Internet business has developed to a stage where almost all financial institutions are required to provide third party trust. Although most transactions can work well enough, they still need to face the inherent shortcomings of trust models. Since financial institutions have inevitably begun to mediate disputes, a totally irrevocable transaction can not be truly realized. Mediation costs increase transaction costs, limit the minimum scale of practical transactions, and cut off the possibility of providing services for daily small transactions. In the broad sense, the system loses the ability to provide irrevocable payment for irrevocable services. Because users have the possibility of revoking payments, they need continuous trust

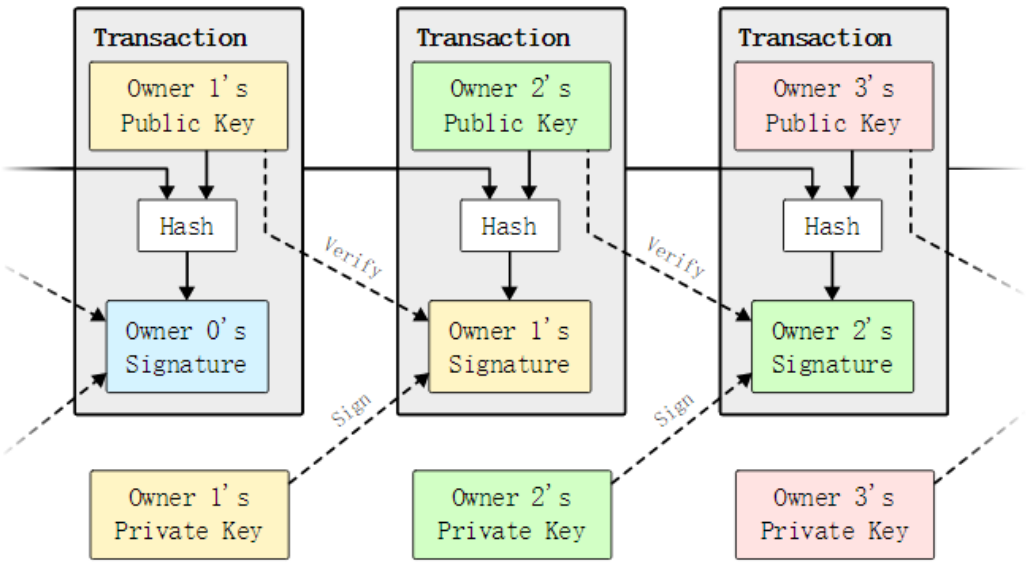
in a certain period of time, which causes businesses to guard against their customers and harass them to get more information that they dont need. Inevitably, fraudulent transactions in a certain proportion are acceptable. Although physical currency can avoid these costs and the uncertainty of payment, there is no business on the premise of not passing through a trusted three party communication channel.

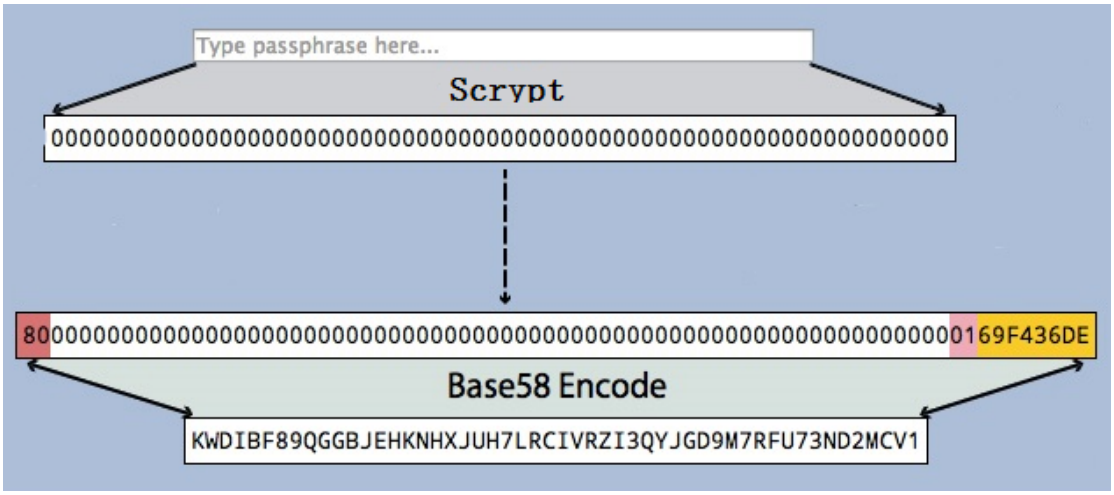
This is why an electronic payment system based on encryption proof is needed instead of the original trust based basic model, allowing either of the two participant to trade directly without the third party based on trust. The calculated invalid transaction will be automatically revoked to protect the seller from the fraud, the conventional conditional contract, which will be mechanized, will be very simple to protect the buyer. Galaxy Chain provides a peer-to-peer based distributed timestamp server to generate a computing proof of time series based transaction orders to solve the double-spending problem. As long as the sum of the CPU computing capacity of the honest node is mor ethan the total number of computing power groups of the joint attack node, the system is safe.

2 Transactions

Galaxy Chain defines an electronic currency as a chain containing a series of digital signatures first. Each currency trader encrypts both the previous transaction information and the next owner's public key with hash, and then digitally signatures, and then adds the information to the end of the electronic currency. The next payee

carries out signature verification through the private key and the public key in the chain to confirm that he is the chain, that is, the owner of the electronic currency.





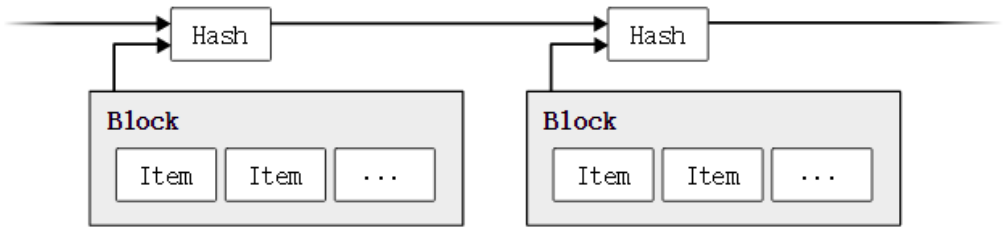
The problem with this process, of course, is that the payee can't verify whether one owner of the coin has double-spent with this coin. The usual solution is to introduce a trustworthy central authority, or a mint to check whether each transaction is double-spending. At the end of each transaction, the coin must be reclaimed by the mint to issue a new one, and only the currency issued directly from the mint will be trusted to not be double-spending. The catastrophe of the solution is that the entire monetary

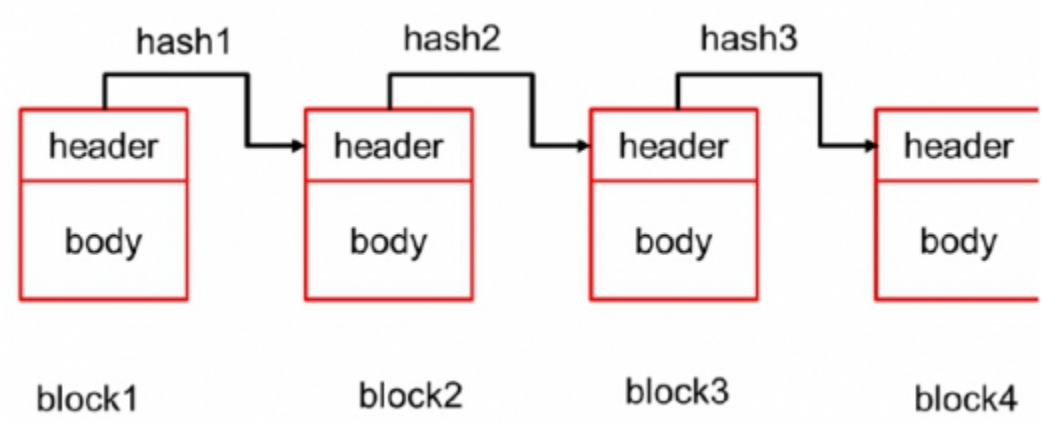
system relies on a company to run the mint, like a bank, every transaction has to pass through them.

We need a way to let the payee know that the last owner of the currency did not sign and authorize in any earlier transaction to cause double spent. Our purpose is to calculate the previous transaction, and we do not need to care about whether the transaction will double spent. The only way is to know all transactions before confirming that the transaction does not exist. Based on the mint model, the mint knows all the transactions and decides which transaction request to arrive at the first time. With no trustworthy three parties doing this, the transaction must be published publicly, and Galaxy Chain requires each participant of a system to agree a single order history that they have accepted. The payee needs to identify each transaction through the main node that they have received the transaction for the first time.

3 Timestamp Server

The Galaxy Chain solution begins with a timestamp server, a timestamp server encrypting a set of data blocks that have been marked by a timestamp, and then publicly publishing the hash, like a news or a previous forum post. Obviously, in order to enter hash, the timestamp must prove that the data must exist at this time. Each timestamp contains the timestamp of the last transaction in its hash, and the timestamp of each transaction has been strengthened to the last one, thus forming a chain.



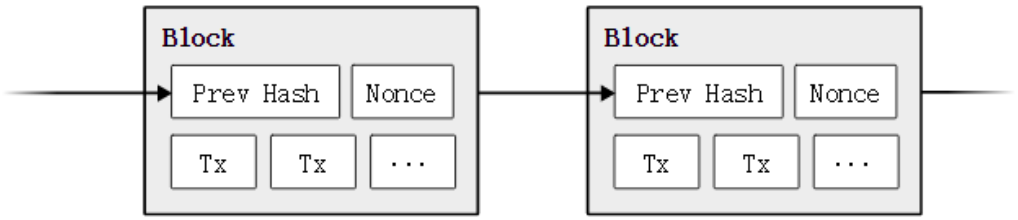


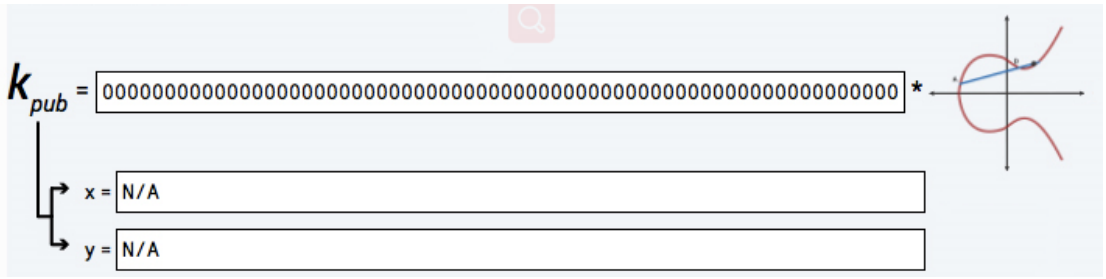
4 Proof of Work

Galaxy Chain will need to use the proof-of-work system to build a distributed timestamp server based on peer-to-peer, very similar to Hash's cash rather than the previous press group and forum mechanism. When data is encrypted by hash, proof-of-work is to check the hash value of a data using the secure hash algorithm scrypt . Hash begins with a certain number of 0 bytes, and the average workload of the check increases exponentially with the number of bytes of 0 bytes, and the check only needs to perform a hash operation.

For the time stamp network feasibility of Galaxy Chain, we add a random number that will not be repeated into the data block and perform a certain amount of work to find it. The hash of this block of data has already contained the 0 bytes that have been required. Once the CPU processing capability has proved that it meets the

required workload and does not redo all jobs. The data block can not be modified. The subsequent data blocks are linked at the end, and the information needed to modify the data block needs to redo the workload of all subsequent data blocks.





This workload system also solves the problem of collective decision making who represents most problems. If the majority is based on a IP one vote mechanism, it will be destroyed by those who can allocate a large number of IP, and the proof-of-work is based on one CPU one vote. Most decisions are represented by the longest chain, and also represent the input of the maximum workload effect. If most CPU is controlled by honest nodes, the honest chain will grow faster than any competing chain. To modify a past block, an attacker will have to redo all the work in the block and all the blocks in the later, and then overtake the work that is more than the honest node. We will then show that the probability of a slow attacker catching up subsequent data blocks increases exponentially with the increase of data blocks.

In order to compensate for the speed of hardware increase and the return of changes in the node's running time, the proof-of-work is determined by a moving average, that is, the average number of data blocks per hour. If they generate too quickly, the difficulty is also increasing.

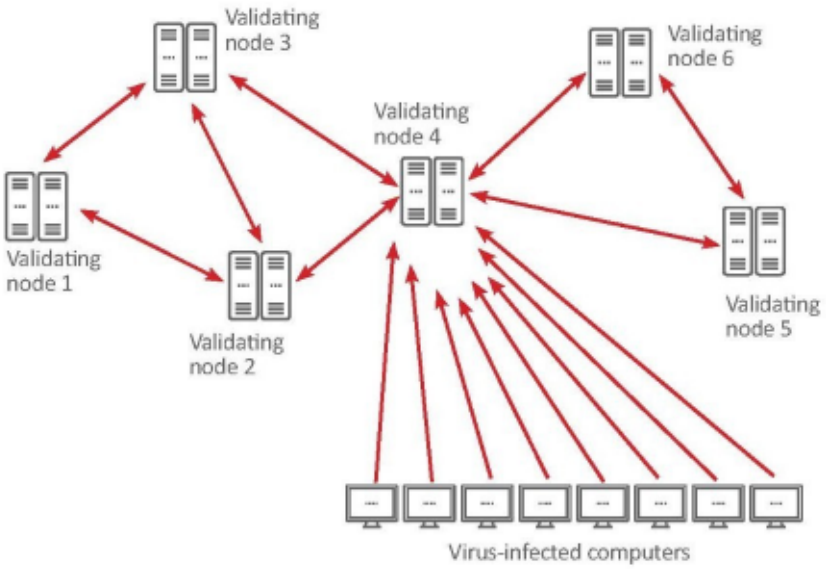


Illustration: a DDoS on all validating nodes

5 Network

The steps to run the Galaxy Chain network are as follows:

1 new transactions are broadcast to all nodes

2 each node collects new transactions into a data block.

3 the difficulty of finding the data block per node.

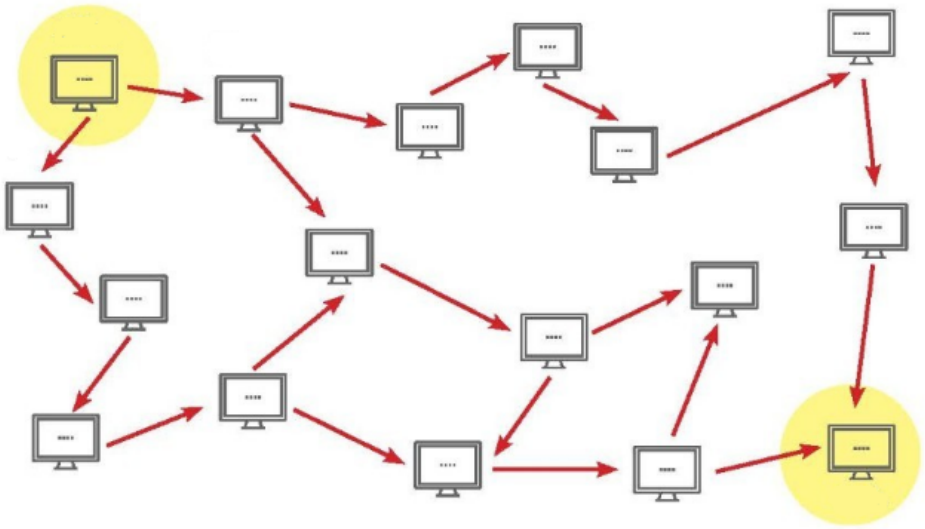
4 when a node proves its workload, it will broadcast the data block to all nodes.

5 a node accepts this data block, only if all transactions in the data block are valid and not paid, the node will accept the data block.

6 By creating the next data block on the data chain, the node takes the hash of the data block of the sending node as the last hash to create a data block, indicating that they accept the data block.

Nodes always assume that the longest data link is correct and will extend over it. If two nodes broadcast different versions of data blocks together, some nodes first receive one or the other. In this case, they will first work on the first received data block, but save another as the next branch to prevent it from getting longer. When the proof-of-work network find that one of the branches becomes longer, the nodes working on the short chain will switch to the longer chain, and their affiliation will be interrupted.

The new transaction broadcast does not need to reach all nodes, they only need to reach as many nodes as possible, and they will be integrated into the data block. Data block broadcasting also tolerates discarding information. If a node does not receive a data block, it will continue to request it until it receives the next data block and believes it is the missing one.



6 Incentive

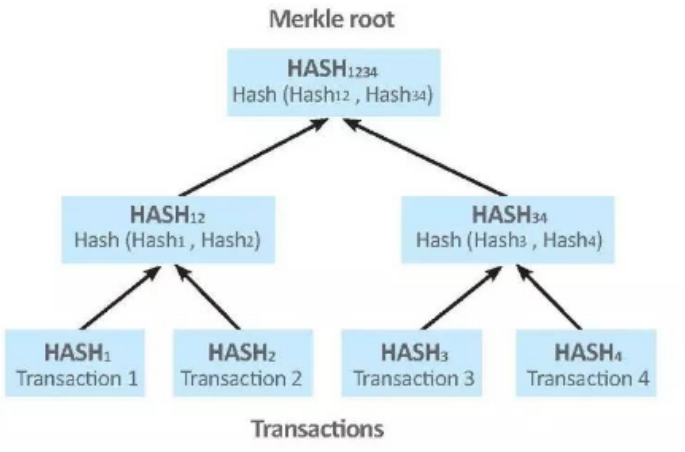
According to the Galaxy Chain rule, the first transaction in a data block is a specific transaction, which creates a new currency, owned by the host of the data block. This adds an incentive to the nodes that support the network, and provides a way to distribute currency distributed throughout the loop, without central authority to affect them. Stable, increasing numbers of new currencies and gold diggers spend resources to add gold to the same as the golden circle system, increasing by the compound interest model.

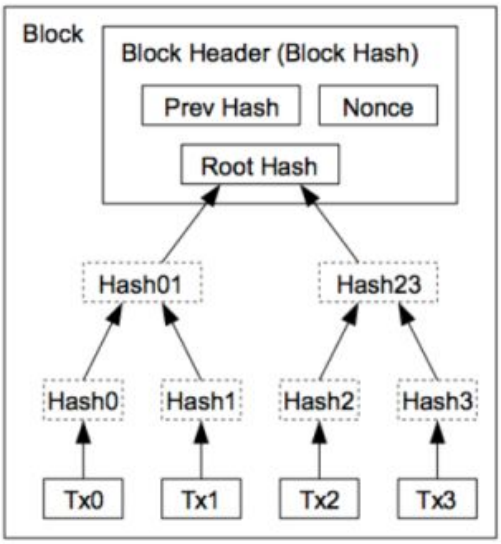
Incentives can also help the nodes to be honest. If a greedy attacker has the ability to assemble a lot of processors over honest nodes, he either chooses to cheat others from his own business or use it to generate new money. He should find that it is more profitable to comply with the rules, which will help him make new money with others,

more than the effectiveness of his impairment of the system and the health of his own wealth.

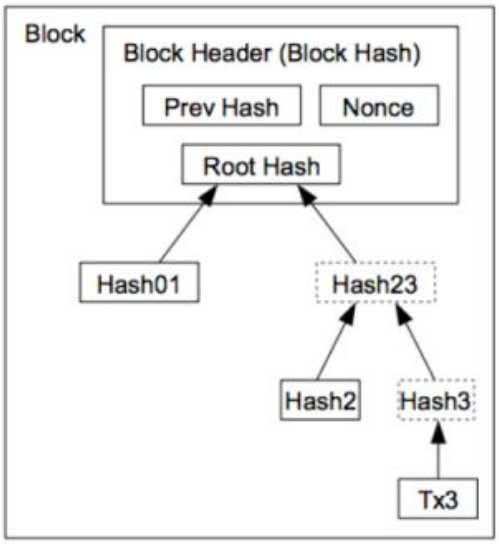
7 Reclaim disk space

The last transaction in a currency has been covered with enough data blocks, and the data before the payment transaction can no longer be used to save disk space. To promote it without interrupting the hash of data blocks. The transaction is hashed into the Merkel tree, so that only the root of the data block hash needs to be included, and the old block of data can be compressed into the next branch of the tree and removed. The internal hash does not need to be stored.





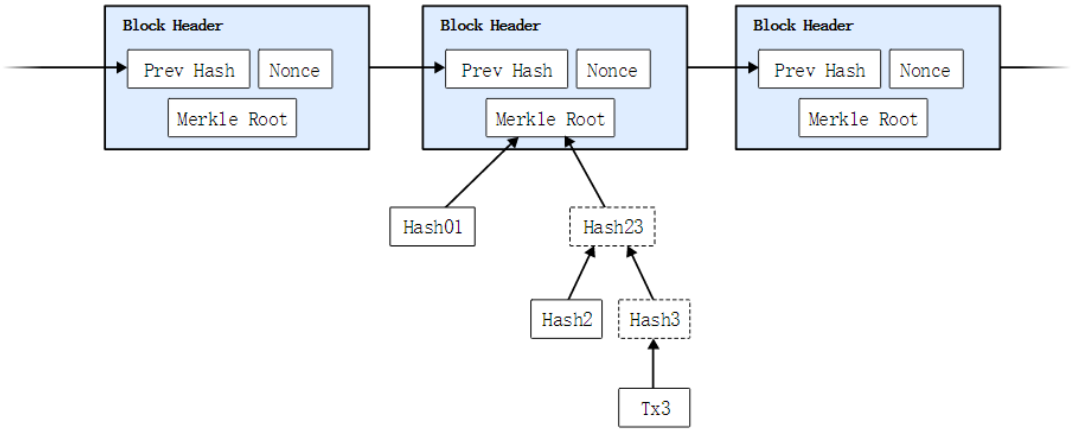
Transactions Hashed in a Merkle Tree

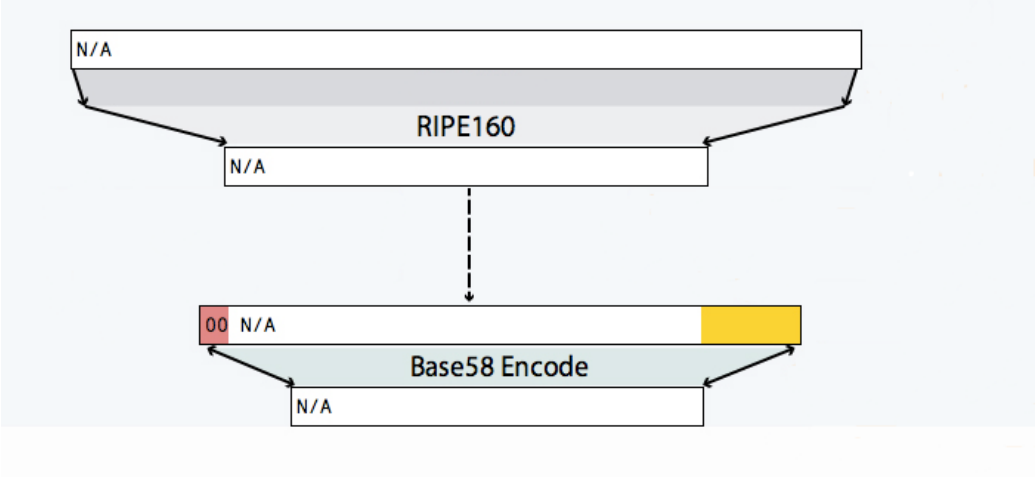


After Pruning Tx0-2 from the Block

8 Simplified Payment Verification

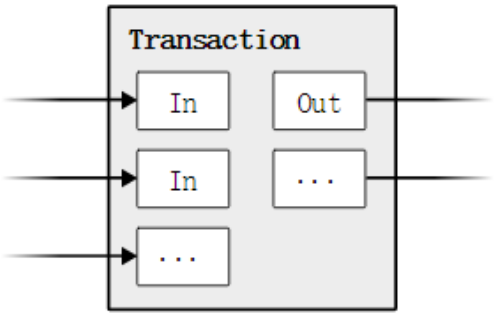
Galaxy Chain does not need to run a complete network node and can authenticate payment, a user only needs to save the copy of the data block head of the longest data chain of the workload network, and he can wait in the line on the network node until he believes that he has got the longest chain, and the block contains all transactions has been connected by the Merkel branch.He can't check his own transaction, but by connecting to a location in the chain, he can see that the network node has accepted the data, and the subsequent added data blocks have also proved that the network node has accepted it.





9 Merge and Split Data

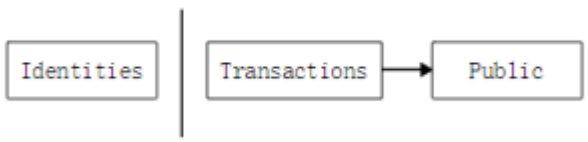
Although it can control the transaction of a single currency, it is a stupid way to deal with each cent separately. Transactions involving multiple inputs and outputs ,we should allow value to be split and combined. Usually it is either a single input from the last larger transaction, or a combination of multiple inputs into smaller numbers, with up to two output, one responsible for payment, one responsible for Changing, and if so, return to the sender.

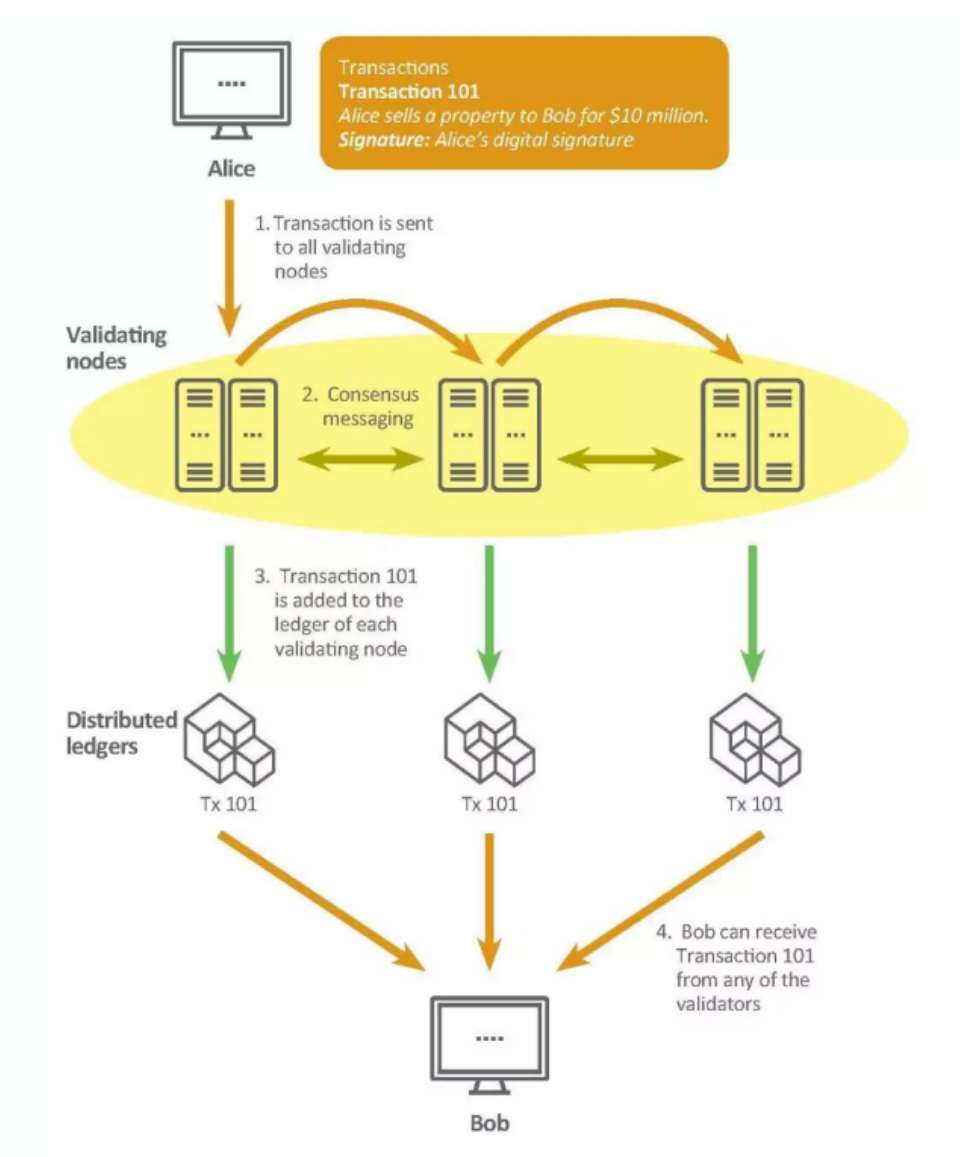


What needs to be noted here is the output end. A transaction comes from several transactions, and at the same time, these transactions come from more transactions. This is not a problem. There is no need to extract a complete historical copy of a transaction here.

10 Privacy

Traditional banking mode is to give partners limited access rights, and at the same time, through a trusted third party to call, to view a certain level of privacy. In addition to this method, maintaining privacy also involves breaking through some parts of the information flow, through anonymous public keys, to disclose all the transactions . The public can see the numbers that someone sends to other people, but there is no information about the sender, which is like the level of information release on the stock exchange. The public records the time and size of a single transaction, but it does not know who is dealing.





As an additional firewall, every new transaction of the same owner can connect a pair of new pairing keys. Some connections will inevitably contain inputs from multiple transactions, which must expose the other inputs of the same owner in the past. The risk is that if the owner's key is exposed, the connection will expose other transactions that belong to the same owner.

11 Calculations

We assume a scenario that an attacker tries to generate a faster chain instead of an honest chain. Even if it is done more thoroughly, it disposes the system to change freely, for example, creating a value in the air or taking away the money that never belongs to him, the node will not accept an invalid payment transaction, and the honest node will never accept the chain that contains them. An attacker can only do his best to change his own business so as to get the money back from his recent payment.

The game between the honest chain and the attack chain is characterized by a random walk of two distributions. The successful event is that the honest node is extended by a block of data, its lead increases one point, and the failed event is the attacker's chain extending a block of data, and the gap is reduced by one point.

The likelihood of an attacker catching up from a given deficit is similar to that of a gambler's bankruptcy. Suppose that a gambler starts with a deficit and has unlimited credit, at the same time, unlimited attempts to gamble make the profit and loss balance. We can calculate his chance of break even, that is an attacker catching up with the chain of honesty. As shown below.

p = The possibility of an honest node finding the next block of data

q = The possibility of an attacker finding the next block of data

qz =The possibility of attackers trying to catch up from Z data blocks

$$q_z = \begin{cases} 1 & if\, p \leq q \\ (q/p)^z & if\, p > q \end{cases}$$

We assume p>q, the possibility of an exponential decline as the attacker overtakes the block of data, and with the probability that he does it, if he is not lucky to catch up in the early days, the more his chances become slim.

We now consider how long it will take to confirm that the sender can not change the transaction. We assume that the sender is an attacker. He wants the receiver to believe that he has paid the money to him, and later he pays the money to himself again. When it occurs, the receiver will receive a warning, but the sender wants it to happen later.

The receiver generates a new pairing key before signing and sends the public key to the sender quickly. This prevents the sender from preparing a data block chain before and starting to work until he is lucky to run to the front and then execute the transaction at this time. Once the transaction has been issued, the dishonest sender has begun to work secretly in a chain that contains parallel versions of his transaction.

The receiver waits until the transaction has been added to a data block and the Z data block has been linked to it. He does not know the exact numbers of the data blocks that the attacker has made, but assuming that honest data blocks are generated by the expected average of each block, the expectation of the attacker's possible progress will be presented as the Poisson distribution.

$$\lambda = z\frac{q}{p}$$

In order to get the probability that an attacker can catch up, we use the Poisson distribution density by multiplying the number of progress that he may catch up with the probable probability at this point:

$$\sum_{k=0}^{\infty} \frac{\lambda^k e^{-\lambda}}{k!} \cdot \begin{cases} (q/p)^{(z-k)} & if\, k \le z \\ 1 & if\, k > z \end{cases}$$

Rearrange and avoid the tail summation of infinite loops.

$$1 - \sum_{k=0}^{z} \frac{\lambda^k e^{-\lambda}}{k!} \left(1 - (q/p)^{(z-k)}\right)$$

The conversion to C code is shown as follows

```
#include
double AttackerSuccessProbability(double q, int z)
{
        double p = 1.0 - q;
        double lambda = z * (q / p);
        double sum = 1.0;
        int i, k;
        for (k = 0; k <= z; k++)
        {
                double poisson = exp(-lambda);
                for (i = 1; i <= k; i++)
                        poisson *= lambda / i;
                sum -= poisson * (1 - pow(q / p, z - k));
        }
        return sum;
}
```

Running some result values for comparison, we can see that with the increase of z value, the probability decreases exponentially.

```
q=0.1                   q=0.3
z=0    P=1.0000000      z=0    P=1.0000000
z=1    P=0.2045873      z=5    P=0.1773523
z=2    P=0.0509779      z=10   P=0.0416605
z=3    P=0.0131722      z=15   P=0.0101008
z=4    P=0.0034552      z=20   P=0.0024804
z=5    P=0.0009137      z=25   P=0.0006132
z=6    P=0.0002428      z=30   P=0.0001522
z=7    P=0.0000647      z=35   P=0.0000379
z=8    P=0.0000173      z=40   P=0.0000095
```

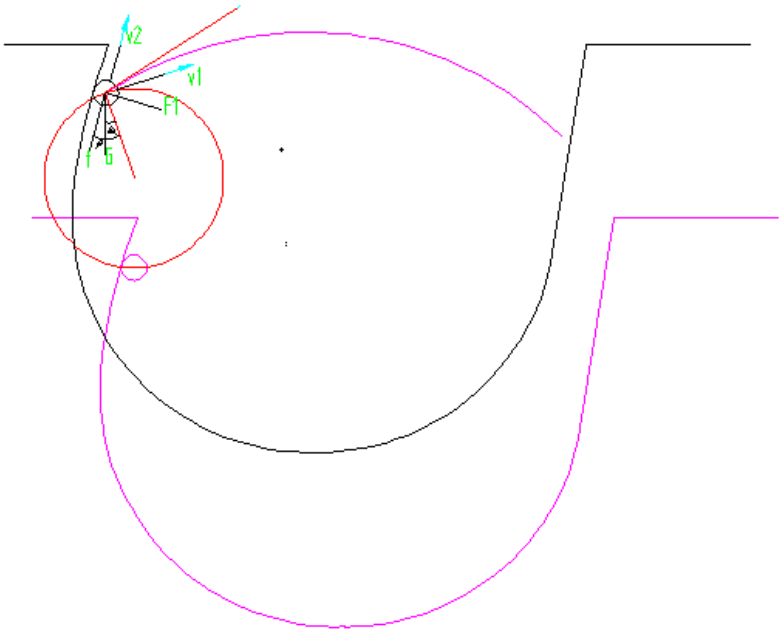
Solving the value of P less than 0.1%

```
P < 0.001
q=0.10   z=5
q=0.15   z=8
q=0.20   z=11
q=0.25   z=15
q=0.30   z=24
q=0.35   z=41
```

12 Generate

The total amount of digital money in Galaxy Chain gradually increases according to the rate set by source code, and the rate of increase gradually slows down. Bitcoin deals with one block in 10 minutes. Litecoin deals with one block in 2.5 minutes, and GCC takes 1 minutes to process one block. The final total of bitcoins is 21 million, and the final total of GCC is 280 million. The speed of bitcoin increased at 50 coins per 10 minutes: when the total amount reached 105,000,000 (50% of 21 million) and the reward was reduced to 25; when the total amount reached 157,500,000 (52,500,000 of the new output, that is 50% of 10.5 million), the reward was again reduced to 12.5; and so on. GCC increases the speed of 50 per 1 minutes: when the total amount reaches 140 million (50% of 280 million) and the reward is reduced to

25; when the total amount reaches 210 million (70 million of the new output, that is 50% of 140 million), the reward is again reduced to 12.5; and so on.



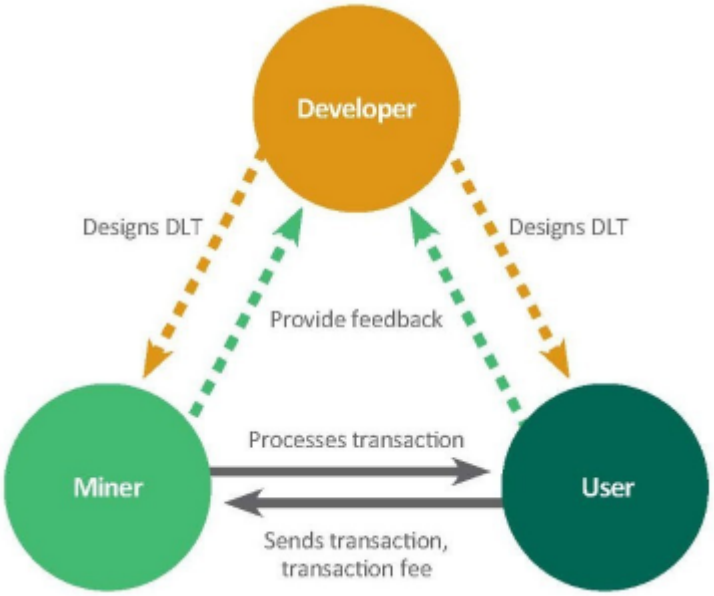
13 Issue

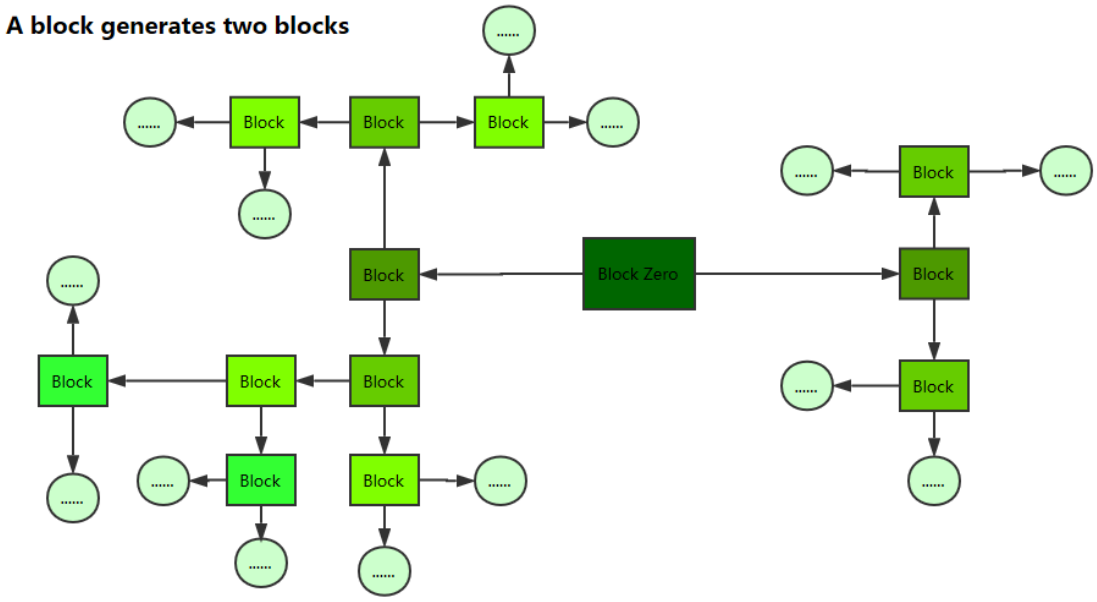
The emergence of bitcoin provided detailed technical ideas for latecome currencies, which is groundbreaking, originator level. Satoshi Nakamoto's original intention was to conceive a virtual currency that was decentration, without intermediation, distributed accounting, and encrypted wallet address, making people's transactions more fair, without looking at the face of banks and government, which was undoubtedly a hall level achievement in the history of human currency.but in the conditions at that time ,the circulation attribute of currency was not taken into consideration and realized through corresponding technical method. Obviously, the total amount of 21 million is far less than 7 billion of the population's demand for currency. Of course, at the historical stage of 2009, it is hard to predict that the

world's total GDP will reach an astonishing 70 trillion over the next few years.A constant distribution of 21 million bitcoin is not enough to correspond to the total population of 7 billion and the world's annual output of more than 70 trillion, and the rules in the source code are too slow. In the past few years, the total amount of money has just reach half, and more and more slow. Because of the small amount and the difficulty of digging coins, bitcoin was accepted only a few years later. Because its quantity is too small, it can only be used as an investment currency, difficult to become a commercial currency.So we have conceived a kind of currency that can quickly be recognized by people and the total amount of circulation can match the world wealth value and is more conducive to commercial circulation. Considering that the world's annual output value will be expected to exceed 100 trillion in the next few years, the total amount of 280 million constant circulation can not only retain the appreciating space in the previous section, but also match the world's future total wealth, so the circulation property of its currency will be reflected.We calculate the power by generating each block. According to the code rules,Each block can only generate two blocks . The difficulty is corresponding to the increasing speed. The increase of currency value and the increase of the amount of currency correspond to the circulation speed and the total amount of circulation. The first 140 million coins will be generated by the compound interest model generated by the blocks, and the remaining amount of money will be generated by node links in two blocks. This way is as difficult as bitcoin to be absolutely fair, because the rule of generation doomed the early participants to a huge profit, and of course they might

pay more energy in the field of circulation. This is undoubtedly the fastest way to get approval and circulation.In the code rules, the total amount of constant circulation is 280 million. According to the calculation method of the previous section, we used a certain amount of time to the international labor day in 2018 to mine a amount about 32 million. 3 million of them will be the development award of our three person team, and 7 million will be the reward for early circulation. The remaining 22 million will be used as initial coin offering, and revenue will be compensated for our R & D costs ,and only accept the payment of bitcoin at the corresponding price on the day of the issue. According to the circulation of early mainstream currencies, we chose seven countries as the ICO area. respectively: 5 million in United States, and the price is 0.15USD, 20 persons will be the early Fundraiser. 2 million in British , and the price is 0.1GBP, 10 persons will be the early fundraisers.1 million in Germany, and the price is 0.1EUR, 5 persons will be the early fundraiser. 2 million in Australia, and the price is 0.2AUD, 10 persons will be the early fundraiser. 1 million in Singapore, and the price is 0.2SGD, 5 persons will be the early fundraiser. 1 million in Malaysia , and the price is 0.6MYR, 5 persons will be the early fundraiser. China has the largest population and a wide range of commercial circulation. In view of this, 10 million in China (including Hongkong and Taiwan) ,and the price is 1CNY, 50 persons will be the early fundraisers. When the total amount of currencyis not up to 180 million, the issuing areas will freely trade in the regional trading centers. When the total amount of the currency reaches 180 million, the value of all the issued currencies will be settled at the US dollar exchange rate and will be freely traded in the same

international trading center. The ICO day will be on the International Labour Day 2018. We will send an email to the early fundraiser in the issuing area three days before the issue.





14 Peroration

On the basis of bitcoin technology,based on the generation of the block of the mainstream currencies such as the ether and litecoin, we have proposed an electronic trading system Galaxy Chain, which does not need third party .We start with the commonly used monetary framework including digital signature. Although it provides powerful control, it is not complete in preventing double spend. To solve this problem, we propose a peer-to-peer network that relies on the workload proof, and uses it to record a common transaction history. If the honest node controls the main processing capacity, the effort of the attacker to modify the record will be unrealistic. This network is simple and robust. All nodes on the network need only a little bit of coordination. They do not need to be authenticated, and the information does not need to be routed to any special place. It only needs to disseminated int best way.It is only necessary to accept the data chain generated by the workload network when they leave. Computing nodes can join and leave the network at any time. They vote with processor power by extending new data on a block of data to show approval for the validity of a block of data, and refusing to extend the block to reject invalid data blocks on a block of data. Any required rules and rewards have been integrated into this consistent mechanism and enforced. Compared with the previous mainstream currency, the technical level of the initial installation of the wallet, the download of historical transactions data is faster, the higher encryption parameters of the wallet address,no tedious multiple audits are needed in the transaction,the whole network confirmation time is quicker, it becomes impossible to tamper the data, even if the world's hackers form a strong team, its CPU computing power can not be higher than

the sum of the world computer CPU computing power based on this technology. At the application level, the special currency rules and the enforcement of the calculation bonus will make the recognition and circulation faster.