# Interflow chain white paper

**Editor: INC community in the Asia Pacific Region**

# Catalog



# Introduction

An ideal free market financial system, realize information scheduling, Internet businesses, integral Tongdui, should allow the parties involved in the premise of minimizing the risk and cost, storage, trading and transfer of value. Based on the first open source protocol put forward by bitcoin for the first time, we

have improved and expanded, and redefined a new protocol called Interflow chain to achieve an ideal free market financial system. In the interworking chain network, we have created a new financial product called polymorphic digital assets. It can track the value of gold, silver, dollar, or other currencies, and let the holder gain dividends while avoiding all the risk of the counterparty. The interworking chain has expanded bitcoin technology, and has provided many traditional monetary functions in a new point to point multi-function network, as well as check accounts, savings accounts and securities broking tools that can make bitcoins and other common financial assets jointly used.
Exchange chain as a universal encryption assets, either as a means or high value trading system, the key elements of successful exchange chain is widely used, therefore, to have sufficient exchange chain attraction for each individual income, to compensate the use of exchange chain to bring the technology, society, risk supervision and politically.


# The characteristics of the ideal free market financial system

We first discuss the nature of an ideal free market financial system. Starting from the motive of establishing it to the principle of need. Our aim is to develop a foundation that can be used for mutual links and competitors.

## The motivation to build IFMFS

We need a digital free financial system that allows any kind of assets to be traded without the need for middlemen or centralised asset issuers 2. In fact, we want to retain their functions as far as possible, as far as possible, as far as possible to reduce the problem of the central node, as well as the regulatory and credit needs. We should strive to make the market go beyond the restrictions of geographical and sovereign manipulation, and integrate traditional exchanges and financial services institutions without considering the specific legal and regulatory issues.

## The principles of the ideal free market financial system

Through careful consideration and co audit, we select the following principles to define the characteristics of a IFMFS to determine the basic objectives of the interoperability chain network.

## Centralization principle

All parties involved in IFMFS enjoy equal status and do not need any privileges. No one can claim resources owned and used by any group of people who have not yet been over 50% at any time.

## The principle of trust

None of the parties involved in the IFMFS need to trust each other. No party can default and should not take the contractual obligation as a precondition.

## Principle of responsibility

No one needs to engage in illegal activities or highly regulated in IFMFS, or take over with friends or family of legal risk and currency exchange directly encrypted currency.

## Principle of ease of use

A IFMFS should be easy to use so that anyone who has the ability to use e - mail can master and succeed in making a profit in the system.

## Extensible principle

A IFMFS must be able to extend to any level of processing power without damaging other principles of the system or introducing other centralization

participants.

## The principle of diversity of assets and transactions

A IFMFS should support the common investment tools, including Maikongmaikong, call and put options. It should support the transaction of any tangible assets.

## Principle of aggregation

In IFMFS, a single purchase should be able to match the list of the minimum transaction units. A user trying to do a big deal only needs to initiate a deal.

## Atomicity principle

In IFMFS, no exchange or transaction is partial, incomplete, or ineffective.

## Intermediary principle

The transaction of the assets of the IFMFS system and the balance of the assets within the system should not depend on the trust of any of the parties including the buyer, the buyer or the intermediary agent. The intermediary system should not be easily attacked by the buyer or seller and intermediary agent.

## The principle of overall pricing

IFMFS shall not use any price information that is not offered by the user from the system.

## Zero sum principle

A IFMFS must neither create nor destroy the value, and the profit of any party must be based on the loss of the other party. No party has debt to the system.

## Principle of entirety attraction

A IFMFS should offer attractive benefits, beyond the risks associated with them, to promote each individual participation, sharing and promotion, as with any regulatory risk control, these gains should be possible market depth of the largest, most liquid,

the most widespread public support, and the maximum demand.

Privacy principle

A IFMFS can provide at least the privacy protection of all participating users with the same level of bitcoin. Ideally, it can be completely anonymous.

Hermes principle

A IFMFS should be as fast as possible to handle deposits, transactions and withdrawals for users. Transactions within the system should be confirmed at the fastest speed.

Security principle

A IFMFS must have the same or better security level as bitcoin.

Open source principle

For an ordinary developer, all IFMFS related hardware and software must be open, censorable, and regenerated.

The principle of passive order execution

The order can be executed without the interactive participation of the user or their computer.

# Interoperability chain

A interworking chain is a polymorphic digital asset, which means that it can evolve into a variety of Bit Assets forms. Bit assets operate in a way similar to bitcoin, but some optimizations and new rules enable interworking chains to support their value. Besides all the characteristics of exchange chain have bitcoin, also provides some new characteristics that hold exchange chain or chain exchange derived from assets of more than 24 hours after the bit can get bonus, a part of the bonuses from mining incentives and transaction costs, will be awarded to each block, and with an increase in network burden distribution.

## Definition

Bonus (Dividend) - mining reward and transaction costs of a part, according to the number of exchange have accounted for the existing chain exchange chain proportion distribution.

(Bit Asset) bits of assets -- a mortgage, supported by the communication chain to 1.5 to 2 times or more high margin, with all the alternative exchange chain, divisibility and transferability of assets and can obtain bonus assets, all collateral and pay dividends from generation to exchange chain form.

Margin - as a supporting asset that is worth more than the current market value of a bit asset.

Bit USD - a kind of assets supported by interworking chains, which are highly related to the value of the dollar through the self imposed market feedback mechanism.

Bit X (Bit X) -- a universal way of naming bits assets, is based on self forcing market feedback mechanism and related assets to achieve value relevance (such as bit Bit (Bit Gold), bit Apple stock (Bit APPL), etc.

Block chain (block chain) - a globally synchronous, block - structured, orderly transaction account.

The output of Guadan (output) - defined under certain conditions will be used the transaction ledger balance.

The transaction (Transaction) - a group of no matching output Guadan and another group of new no matching output Guadan matching to meet the output matching conditions and other rules under the condition of block chain.

# Block chain Market

Transaction algorithms and rules

The purpose of a block chain is to establish a consensus on the order of events and the current state of the global transaction account. The interoperability chain requires this global account to establish the order of transfer, sale and market transactions. Every 5 minutes all contained in a block in the sale of Guadan will match. As with bitcoin, each transaction is a set of output, sale Guadan under certain conditions. The main difference is the conditions that allow the formation of a transaction. (for interoperability chain) these conditions include:
1, M private key signed by N;
2, the sale of Guadan is filled in the specified transaction rate;
3. The deposit is in place;
4, repurchase the bit assets to use the remaining margin;
5, the subscription or put option is exercised at the appropriate price;
6. Intermediary transactions are released;
7, the intermediary transaction is controversial;
8, the dispute of intermediary transaction is solved;
9, cross chain trading confirmation.

The block chain market is a channel for price information to enter the block chain. It is very important to ensure that the price information is accurate and not subject to human manipulation based on market power. These price information will be used to make mandatory margin supplement.

Users can freely trade, record transactions will be recorded in the block chain, but based on the agreement between individuals, the transaction for automatic price discovery is meaningless, because the network can not identify whether the same person is trading with two accounts. A successful transaction must be agreed to by both sides, the same, not successful sale of Guadan is certainly because everyone thinks the bid is too low or the price is too high. Those who do not want to carry out "off the chain" negotiations can put their purchase orders into the block chain. When the miner has finished all the transaction data that has been accepted, he will match all the compatible purchase orders in the order of the

highest buying price and the lowest selling price. Once all the matched transactions are completed, the block chain will leave the list of unfulfilled purchase orders. These orders indicate that the consensus price of the market is between the purchase price and the selling price. At this time, we will check the margin requirements of all the empty positions according to the buying price. All the short positions that are short of security will be forced to liquidate at the current selling price, and the short positions with the largest margin will be levelled first.

The miners, sale of assets in the chain can block until 24 hours after the bifurcation of the window period of posting, for as coin base transactions, all generated by the miners did not have signed a deal will not be transferred to other chain in the reorganization, when you are in a deal after 24 hours is still not in the block chain the market posted assets, you can block the new middle chain market to buy / sell for subsequent execution of miners.

Cancel a pending open 24 hours to comply with the principles, because after a block chain reorganization if you cancel the order and before, may cause other miners to execute your order.


Create a bit of dollar

The bit dollar is a bit asset derived from an interworking chain, which must be

created for an effective purchase and after a transaction with the equivalent value of the transaction amount. If the purchase price is accepted, the collateral and the purchase price are locked up by the network until the dollar is repurchased. The block chain will transfer the dividend of the collateral to all the holders of the bit of the dollar. Bits and dollars are completely substitutable, and all the dividends generated by interworking chains supporting bits and dollars are aggregated to determine the holders of the bit dollars.

The interworking chain used to support the bit dollar may be used in two ways:
1, the purchase money in the bit dollar transaction is honoured.
2, when the value of the interworking chain that supports the bit dollar is less than 150% of the value of the dollar, the miners will use it to launch a forced flat.

When a coal miner initiates the forced liquidation when creating blocks, it uses the interworking chain used to support as a support to buy the bit dollar and pay it. After payment, the bits and dollars do not exist. The remaining collateral will be sent to the address of the empty end (not retained by the miner).

When the miners were forced to initiate forced liquidation, the network will charge 5% of the transaction costs in order to encourage market participants to actively manage their deposit, if the market changes too fast leads to insufficient margin, if the demand for the dollar relative to the bit supply, than the market price of the dollar will feature a short time to parity.

$p$ = probability an honest node finds the next block
$q$ = probability the attacker finds the next block
$q_z$ = probability the attacker will ever catch up from z blocks behind

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

## Advanced transactions and contracts

By the communication chain and automatic forced liquidation consisting of infrastructure, means a similar call and put options such as contracts can be created and traded, these contracts selling and advertising can be away from the chain, once the transaction

intention reached by relatively simple script execution rules Guadan in the chain.

Exchange chain bonus

Half of all mining incentives and transaction costs will be in accordance with the total number of holdings exchange chain chain proportion allocated to existing exchange holders, the total will exchange chain growth rate according to a decreasing growth by 50 per minute, until 12 years later reduced to zero, which means that the red start will be very high finally, an approach is proportional to the number and transaction cost.

The 12 year exchange chain selection issue, rather than bitcoin 128 years, because a currency's legitimate function does not require inflation, but in 12 years, to block the chain space (to meet to the center and extension principle is restricted) competition will drive the transaction cost / trading volume to make a miner profitable, and meet the market requirements of the level of security level.

The Internet has other means to generate cost - motivated miners: idle taxes, flat charges, and 'red dust'. Bitcoin suffered disproportionately and reward pricing mining security level required for the trouble.

Based on mining reward and ignore all fees, effective interest rate on a monthly basis on the right shows a red. You will notice that early miners gained a lot of benefits through mining and holding. This will create market demand that promotes the net present value of the early interoperability chain far higher than the later interoperability chain and will continue to push up the price until the price is stable. Please note that those who hold a bit of dollar will gain more than 2 times the rate of return, and thus have an opportunity to have an annual interest rate of more than 20% in the first 10 years of the new block chain.

As the bonus of the dollar dollar is so high, it will be trading at a much higher premium than the actual dollar. This is the risk premium will be short and / on the basis of perceived market redemption relative demand $bit annual effective yield means, but from the investment point of view, if the dollar exchange chain

prices doubled, the price of $bit will be doubled, which means that as the premium may fluctuate, but there will be no exchange rate risk.

The bonus structure is zero and the reward to the miners is through the "inflation" from the exchange of all the chain holders, holders the same bonus from this bonus, an analogy is one of every 10 minutes by 1 to 1.0000001 of the proportion of the stock split. The result is, this bonus does not pass the new "purchasing power" to the holders, because half of the bonus holders exchange chain only through the "inflation" reward of mining.

The results from the inflation (or redistribution) low 50% dividend exchange chain holders feel lead to inflation than bitcoin holders feel, the initial dividend mainly from inflation, and the final dividend is no inflation return completely from the transaction cost.

There are a few other reasons why the bonus has to be:
1, they created the opportunity cost of holding short positions (encourage cover);
2, they create incentives for holding rather than selling (increasing the value of possession);
3, they subsidize the risk of multiple heads.
4, they turn the interworking chain into an asset with cash flow, making it possible to compare prices and cash.
5, they make bit dollars, and bit gold can attract anyone seeking a return on the exchange rate risk, making it likely to be popular.


A small number point position / segmentation comparison of interworking chain and bitcoin

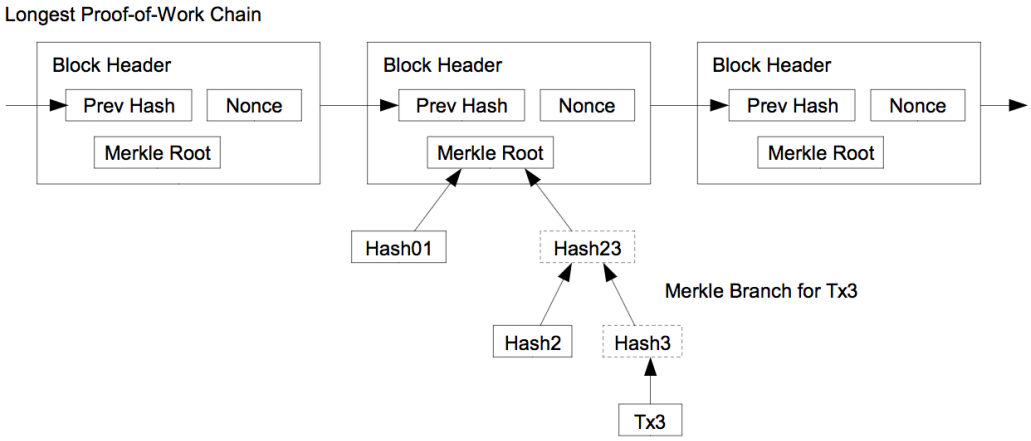
1 bitcoins are traditionally defined as 100 million Cong, and we start to see some things priced at 0.0001BTC or less. With the appreciation of bitcoins, the decimal point has been added to more and more 0 prefixes. This makes it difficult for users to understand and compare prices, and to make a very small price tag in need of a large number of numbers. In addition, people are not familiar with the use of milli, micro or nano units and other units, and used to use thousands, millions, millions of units. These large units seem to be more easy to talk about, round, perceive and compare.

In this paper, when we talk about the 1 interworking chain, it seems that the proportion of 1 interworking chains in all interconnected supply chains is similar to that of 1 bitcoins in all bitcoin supply. The fact is that the mining reward is the 5 million interlinked chain, and the 0.001 interworking chains are not more divided than the one. Users will begin to use millions of interworking chains to bid for items, and as time goes on, it will fall to thousands or even hundreds of interworking chains. With the mobile decimal point used in the interconnected chain network, the effective supply of the interworking chain will exceed 15 trillion. If the 0.001 interworking chain is equivalent to 0.01 dollars, it can

support the total cash flow of more than 150 trillion dollars. The US money supply (M2) is about 10 trillion US dollars, which means that when the 1 interworking links are equivalent to 10 US dollars, the interworking chain can support about 15 times the current economies of the world scale.

Extend

Block chain has a basic rate limiting, makes the transaction can be confirmed based on the proof of work and network delay and confirmation of block chain performance to a certain extent after the needs of high-end computer, hard disk and network, finally began to make network centric. In order to meet the requirements of the exchange to the center of the chain block chain will be limited without the total amount of transactions Guadan, and limit each chain support up to 32 kinds of assets.




Each of these block chains is called Interflow chain Exchange (BSEx). The overall block chain is called the Interflow chain Free Market System (BSFMS). BSFMS has been designed as an independent competition / free cooperation market entity and has continuously established new BSEx compatible with interoperability chain. It will benefit from meeting market demand. Four such BSEx forms the illustrated BSFMS. Each BSEx can have up to 32 encrypted currencies - plus local and global interworking currency. Each BSEx has its own block chain to support the encrypted currency and name it in the local interconnected chain currency (represented by red, green and blue interworking links). These local interworking chains can trade locally with the global interworking chain (yellow) which constitutes currency BSEx.


Interflow chain Interflow exchange (Interflow chain Currency Exchange, BSCurEx) and three potential BSEX chains, unlike bitcoin, interoperability chain can expand the scope and support multiple independent and parallel blocks. Since each block chain can trade bit asset derivatives bundled on other block chains, it is easy to move the value between blocks. Some users can join two block chains for arbitrage. The result of a parallel block chain is that the interconnected chain can be extended to any capacity without the need for a block chain outside the 1-2 block chains that have a transaction requirement for a common computer. System native support of the new "combined mining technology can effectively ensure that miners and mining block chain, and does not allow the operator to take over idle proof of the actual needs of the workload, one-time mining hundreds of block chain, which led to the burden of the network.

Some big players who want to move billions of dollars in one time can combine all the block chains in large data centers, and the arbitrage between chains and chains. These players do not cause system centralization, because they are not necessary. On the contrary, these large players only make certain separate chains more stable.

# Fair combined mining

Combined mining is the key aspect of the extensibility of many different block

chains. Unfortunately, combined mining requires Merkle tree (Merkle Hash Tree), which is commonly used to keep all nodes updated synchronously in distributed computing as workload proof, which requires more space for more than one year in the block. If we need to build a system like an interworking chain that will eventually have more than 1000 chains and have a series of bits and sets of assets on each chain, merging mining is very important. However, you don't want to artificially limit the depth of Merkle tree, nor allow the merged miners to ignore the potential value of each chain, and to expose everyone's chain to their Merkle tree to harm others to get a free lunch.

The interconnected chain adopts a new way to support merger mining, and through the appropriate profit incentive to minimize the workload of Merkel, to prove branching rather than limiting its size. If there are two interconnected chain chains (red and blue), and each chain has different asset subset, there are three choices for the miners who combine mining, digging red chain, digging blue chain or merging mining. If he chooses to merge mining, so the red and blue network will have more work that accept the cost, while the miners pay will be doubled, so the new method can use the Merkle branch depth to get proof of work, so the reward will be discounted to the miners to balance and flow of dividend, bonus formula of miners block-reward / 2^ (merkel-branch-depth). The final result is that if the chain of red and blue interoperability has the same market value and difficulty, then the profit of the combined mining is the same as that of the individual. Both red and blue benefit from the increased hash ability, while miners won't get any extra value unless he wants new variable chains to increase value over time.

If the red and blue chains have different values and difficulties, the miners must carefully choose the chains they want to mine based on their growth expectations for the relative distribution of the two chains to Hashi capacity. This can not impose unprofitable merger mining to a large network or to create a "master / slave" chain set of circumstances, to make good and useful with possible mining.

Atomic cross chain transaction

The problem of atomization cross chain trading is that when (at least) two traders, Alice and Bob have their own encrypted currencies, such as bitcoin and Wright currency, and want to exchange without having to trust the third party (central exchange).

A non atomic trivial solution is that Alice sends her bitcoin to Bob, then let Bob Antony Wright currency to Alice - but Bob received in bitcoin after the choice

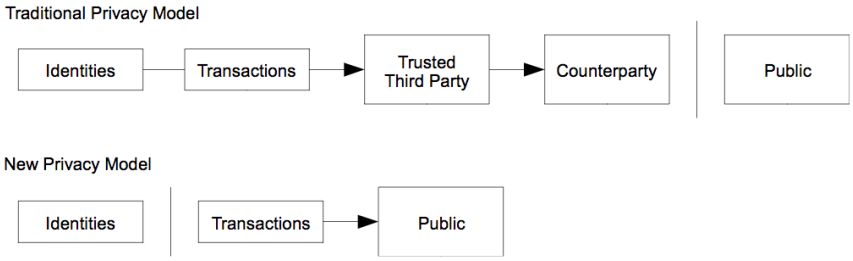
of default, the loss of Alice send bitcoin.

The algorithm of atomization cross chain transactions has been described in bitcoin wiki. The interworking chain will support this algorithm, which will enable users to trade Bit BTC and real bitcoins without intermediary agents or trusts. The whole process can be automatically executed by software.

This feature can be used to trade between two parallel chain chains and increase the scalability of the network.

Rotation block chain

Another aspect of exchange chain block chain, is not all, Guadan output cannot exist for more than 1 years. More than 1 years, the output will not be confiscated pending bonuses, and will be in the block chain to move forward and impose a 5% transaction fee. The balance is lower than the average transaction fees will be all confiscated. This will enable the network to recover from the loss of key value and to eliminate the ever-increasing cost (and no gain if the key is lost if) permanent storage transactions and data demand guadan.




Because the block sprocket turns, it is possible to define the maximum disk capacity required to handle the block chain. In the future, the maximum capacity can be adjusted upwards, but it is suggested that the network set the limit based on the average capacity of the RAM in the new computer. This will ensure that all data sets can be easily placed in RAM, so that all nodes can handle all transactions efficiently, which is very important when extra work is needed to perform market maker functions.


# Mediator of generalized physical delivery

Intermediaries become very important when dealing with untrusted "anonymous" individuals with possible default. The traditional approach is to use mediator agents (such as Pay PAL) that can withdraw transactions and resolve disputes. Unfortunately, the traditional intermediary agent must be the third party that is trusted in each transaction. If the agency is not anonymous, they may be liable for dealing with certain transactions. If they are anonymous, how can they be trusted?

For the reasons of law, it is very important for any party, including intermediary agents, to be obliged to comply with any legally binding contract. Such a contract may trigger the risk of the counterparty and touch many laws and regulations associated with intermediary and arbitration services. On the contrary, the assumption of intermediary operation of interconnected chain is that at any time, no party has any legal obligation to take any specific actions, and all traders will act honestly and morally under the drive of market power.
The interworking chain solves this problem by using the mediator function built in the block chain. Any user can be anonymous intermediary agent in block chain and registration parameters, including: definition of intermediary exchange need to schedule, fees, good margin, required evidence in the

dispute when the need to communicate with the anonymous Bit Message address, and other related processes recommended the relevant intermediary agent. Some parameters are mandatory by block chain (such as handling fees, good faith margin and timetable). All others are not mandatory, depending on the wishes of all parties. Fortunately, in terms of integrity, profit driven is proven to be more effective than the law or court decisions.

If everything goes smoothly, the intermediary agent will not intervene. However, if there is any dispute in the transaction, any party can initiate a new transaction in the block chain to "freeze the fund" until the intermediary agency makes a decision. Intermediary agents have the power to divide funds only on both sides of the transaction. Intermediary agents are also bound to other agents. Therefore, if any party is willing to pay, it can repeatedly argue about the ruling made by the intermediary agency until the same ruling is awarded three times in a row.

If an intermediary agent has an unresolved dispute, then any new transaction involving the agent can not enter the network. This will solve all disputes honestly and efficiently by motivating intermediaries financially.

All parties will benefit from honesty, because dishonesty will suffer losses, and conspiracy will not succeed because there is a complaint process and the two parties can choose intermediary agents together. Intermediary agents will charge fees from each transaction according to their services, so they will not risk losing their reputation and margin to help one side and deceive the other party.

Although this intermediary agency system provides relatively fast and safe wire transfers or transfers within banks, it has limited functions in preventing payment / rotation. In view of this, it is recommended that all payments be made through wire transfer or ACH (Automatic Clearing House), so that these payments will be allowed to expire before the agency is released to the intermediary.

# Centralization

### De centralization hash function

The bitcoin's workload has proved that the use of double SHA256 algorithms has led to the production of a dedicated ASIC chip that specializes in this function. This specialized degree of specialization has become a small part of

mining high risk control in the bitcoin community. This centralization has become a network burden, because the miner may be manipulated or closed as an exchange. The mineral pool is another form of centralization of the centralized calculation force. Taking out a pool is likely to destroy the hash computing power of the entire network, which may delay the transaction for several days until the difficulty is adjusted.

The first step to maintain the degree of de centralization of workload certification is to design a hash function that can best run on the CPU universal device, which simply can't benefit from specialized GPU or even more specialized ASIC. There are several key points in the design of this algorithm.

First, it must be based on the most efficient use of the most widely used transistors by consumers. The use of RAM and caching is very dense, and the high - optimized ASIC is also widely distributed. Historically, RAM and CPU increased the speed of computing power basically. Therefore, the use of RAM will make specialized ASIC chips and even GPU chips unable to optimize through parallel mode. This naturally makes all the performance serial. Another feature of using RAM is that when CPU lacks data for most of the time, the speed of the system bus is much more important than the ability of the CPU. If we optimize the processing speed of CPU, it is impossible to solve the bottleneck of CPU's lack of data, so even improving computing power by 10 times will not improve data passing ability.

Second, it must be based on continuous data processing without branch prediction. This only prevents most of the parallel data or prefetching optimization operations, because the architecture of the GPU is far worse than the CPU. GPU is also constrained by the memory bus, and its performance will decline significantly if the local cache is not kept small enough for each GPU core. These features can allow CPU capabilities to be dispersed and prevent some specially designed attacks with huge advantage hardware.

The proposed workload shows that the use of SHA256 provides seeds for 8 bit fast random number generators, which are widely distributed in 128MB RAM. In the process of filling RAM, the pseudorandom branch prevents transmission and causes some extra CityHashCRC128 operations to be mixed into pseudo random to fill the entire 128MB address space. When all 128MB is filled, hash is calculated by CityHashCRC128 and the result is obtained by using the SHA1 of CityHashCRC32.

The operation of these recommendations is to make full use of the advantages

of the following CPU relative to GPU to ensure that CPU is the ideal ASIC.
1, GPU can execute only 1 instructions per 4 clock cycles in a single thread case.
2, the working frequency of CPU is about 3 to 4 times that of GPU.
3, using City Hash superscalar CPU similar to the Intel Core i7 can execute multiple instructions in each period;
4, CityHashCRC128 accelerates CRC32 instructions by hardware, which requires processors to support SSE4.2 instruction set. SSE4.2 is not present in GPU at present.
5. In the case of branch error prediction, the performance of GPU is very bad.
According to factors 1, 2, and 3, the processing speed of CPU in a single thread mode is about 32 to 64 times that of GPU. Due to the increase of CRC32 speed by 4 times, the total CPU processing speed will be 128 to 256 times of GPU speed in single thread mode. Finally, the branch error prediction will exacerbate the disadvantage of GPU. Overall, we expect a GPU requires about 2048 complete multi processor (not stream processors) processing capacity and about 256GB to RAM in this particular problem and a 4GHz Intel core is i7. We set the number to be more than 64, so that the low enough memory will be able to cope with the top end of the GPU.

Because workload certification consumes more CPU power than signature verification. An auxiliary cost of one second workload will be executed and verified by a separate SHA256 operation before the block workload is verified and verified by the node. This will prevent denial of service attacks on the network.

The last guarantee to centralization is that it is possible to upgrade the hash algorithm through the network to maintain its ability to optimize the CPU. Once it is obvious that the commercialized hardware can have strong advantages in mining, before the advantage is realized, the network can upgrade the hash algorithm. The small threat in this area and the Declaration on the intention of executing this plan when blocking the block chain will prevent players from making significant investments in special purpose hardware and make them ineffective in any unfair competition when such investments are devalued.

## A built-in de centralization pool (P2Pool)

The technology adopted by P2Pool will build a distributed pool without central servers, which enables most users to mine quickly and conveniently even under increasing difficulty. This will not be required by the interoperability chain agreement, but there will be network support.


# Security

51% denial of service attack

Because all the nodes are motivated by a dividend such as the dividend, they will actively reject the new blocks that do not contain 80% known correct transactions. All nodes have financial incentives to verify the block chain and refuse to work with those users who create new blocks that cause them to lose dividends. All miners are encouraged to reject blocks that contain lots of "unprecedented" transactions and fees, which means that someone is cheating to cheat fees or manipulate the Internet. Because most users are "profitable" for mining, they will actively cooperate to prevent this manipulation attempt. So, to carry out a 51% DOS attack requires the attacker to buy a huge cost of the whole network, and their opponent's earnings will improve the mining, 51% double pay attacks become more expensive.

Encrypted communication

Communication between all nodes is encrypted for two reasons: it can prevent packet filtering and make it harder to determine the source of new transactions.

# Interoperability chain Economics

The interoperability chain tries to make all participants active to ensure that even the mortgage requirements in extremely volatile markets can be met. In order to illustrate how forces interact with the block chain rules of the interworking chain in the market, we consider several market scenarios.

A rapid decline in the value of interoperability

If the exchange chain relative to the value of bits of gold fell quickly, then the system must face all short "Bikong", forcing them in action before the explosion. If they fall to their red line, they will pay 5% of the fees or worse, and lose all the collateral. The result is a bit Bikong gold will rise rapidly over the market price of gold, the more short faced explosion. This will create opportunities for new empty heads to enter the market through full mortgage short selling. These new bears will profit in the end of the price drop in bikong. Therefore, all the participants in the market will actively monitor prices and their collateral, thereby reducing the volatility of the market.

Rapid appreciation of interoperability

If the price of interworking chains is rising faster than gold, then bit gold holders will see that the relative interworking chain of bit gold is overestimated. Understand that other market participants will try to relative price of gold based on the bit to buy or sell gold exchange chain market will be a large number of bits of selling gold, gold exchange chain bit until prices fell to the gold exchange chain price.

The fall in the gold price of bits means that the empty head will exceed the amount of mortgages and lead to unnecessary opportunity costs. This will drive them to make a profit.

The price of gold and bit gold

If there is a consensus that bit gold is the derivative of 1 ounce gold bonds under the current red interest rate, all market participants will make profits. However, the market will not "trust" bit gold at the beginning. The result is all market participants initially Guadan price will be scattered. When the market depth increases, the price range will shrink until a consensus price is formed, which will be close to the price of 1 ounce gold bonds under the current red interest rate.

The trading parties are going to decide whether to make a decision or to make a short decision on the price of the bit gold they judge. The only rational investment method is to assume that it will follow the price of physical gold. Why is there any reason to think that it will deviate from the price of physical gold in a specific direction? The only reason for the price deviation is that the supply and demand changes of bit gold make the value of physical gold higher or discounted, so the promotion or discount will be basically fixed and not affected by exchange rate risk between exchange chain and physical gold.

There is a clear difference between the ETF gold and the real gold price. Because most individuals can't deal directly with ETF gold, but they can trade gold coins. Bits of gold can be defined as an ounce of gold eagle (United States Mint standard 1 ounces of gold spot price). This and the ETF price manipulation has a slight decoupling, but also for the premium plus gold eagle. What would happen if nobody bid for bit assets?

We must first understand is that the value of the assets is always bit and support its bonus is proportional to the value, therefore, will have the opportunity cost of short positions, also will have the bull does not depend on the exchange value chain revenue streams, which is higher than the market level of red interest rates will attract buyers bit new assets, too that is to say, there is always a bit of assets liquidity and the relative interest rate based on red, so as long as people exchange chain will be bidding, bidding bit assets.

So, early users who first buy bit gold will face a limited risk (if any). If the annual red interest rate of the interworking chain is 10%, then when the transaction becomes a bit gold, the user will gain twice the income, even if they are the only buyers. When the need to "release" of this transaction, the price will be decided in a much-needed liquidity to a party, if eager to let people pay to stop short but the opportunity cost, they will be forced to buy at higher prices. If multiple heads need to convert bits gold into other assets, they will choose to sell it at a low price. In any case, there are not only two players in any bit asset market that only focus on getting higher returns.

## The market effect of bonus

The rate of dividend payment is usually between 1.5 and 2.5, as the bit and interworking chains pay dividends at a certain interest rate, because the mortgage ratio of bit assets is usually 1.5-2.5. When pricing, we must calculate the net present value of the revenue streams on both sides, which is proportional to the bit US dollar

and the interconnected chain, so that the price of bit dollars relative to the interlink chain will be almost 100% related to the exchange rate between the US dollar and the non dividend exchange chain. In the end, the premium or discount of the dollar dollar relative to the dollar will be determined by the "loaned opportunity cost" and the "risk premium" of multiple demands. The return of all other bit - dollar holders will come from the overall appreciation of the interoperability network that they belong to.

What would happen if the market crash led to a lack of margin?

In this case, the empty account will be liquidated at the market price, and in the short term the value of the multiple positions will fall below the market parity. Only the collapse of the most serious interconnected chain value triggers such an event, because it is unlikely that the appreciation of all other asset types relative to the value stable interchanges within 60 minutes. When the market price is lower than the parity, market participants have two choices, hold until the market is stable, the market adjustment period or in the flesh, because all market participants know the price will be $bit recovery because of market forces, any flesh disk appears when there will be a lot of buyers entry positions so as to provide support for the price.

Only when the whole system crashes, will the interworking chain become worthless and everyone will be damaged, which is a very low probability event unless the block chain algorithm or encryption mechanism is destroyed. Early users will have a higher rate of return because of the small amount of money, which is a compensation for them to take a huge risk. Later users will be more confident in the algorithm and their returns will be lower.

How to price the dollar dollar

So far, we have shown how the bit dollar is highly correlated with the US dollar. However, we haven't yet provided a reasonable way to really establish the price. Now let's take a look at the investment proposal that has a bit of a bit of a bit. You will receive an anonymous, safe, service assets, it has all the characteristics of bitcoin, but no currency risk any exchange chain / $20% annual rate of return, because you must have it and other investment $3% per annum, such as the comparison of bank deposits. After

calculating the net present value, you can make sure that only about $1.14 should be sold on the basis of the yield of 1 bits only based on the yield.

This value should be adjusted according to the premium and risk discount brought by the characteristics of the encrypted currency, and the price of bit dollars will fluctuate between 1.10 and 1.20 dollars. This price range will decrease with the perceived risk, and the profit will continue to clear and shrink.

So far, we have discussed only the buyer's pricing formula, but before anyone can own the bit dollar, someone must create it first, which means that someone must give up 10% of the annual revenue and establish a short position. The minimum cost of the dollar will be 10% lower than the interconnected chain, so that only if it sells on the price of 1.14 dollars, can it get enough cost to cover the cost (10%). This will lead to an increase in the supply of bit dollars until the price is stable at around $1.14. If he expects the interoperability chain to rise more than 10%, he will be able to attract more buyers by selling short at a price of $1.14, thus effectively expanding the empty position.

The ability to buy bit dollars at the price of 1.14 yuan means that the actual annual rate of return has increased to over 20%, and we must pay a premium of more than 1.14 dollars for the bit dollar, which means that the actual annual revenue has decreased to 20%. Finally, the market will be based on the balance of the dollar to the net risk / rate of interest rates required to establish the correct premium for the bit dollar supported by the interworking chain.

Hint: the prices in the above examples are based on the 3% discount rate contained in the assumed net present value, and can only represent a way to assess the fair market price. The final price will be decided by much more than the factors mentioned in the market. The key point to understand is that bit dollar is an asset that allows interoperability to hedge against the fluctuation of interworking / dollar exchange rate and should not be expected to have an accurate 1:1 rate with the US dollar.

The significance of enabling a local exchange to trade bit dollars
Local Bitcoins (a bitcoin exchange website) the user is facing the challenge of, any one of the specified city spreads than the global

market spreads much, result in a small local market transaction cost is much greater, and did not make accurate transaction possible globalization center market, price discovery will become more difficult, and this further expand the spread.

Due to the fact that the bit dollar is traded in a globalized way of centralization and keeps similar to the price of US dollar interest bearing bonds, the spread difference between bit US dollar and US dollar will be much smaller than that on Local Bitcoins. The effect of this decreasing price difference is that it may compete with intermediary fees and time delay of remote exchanges, so larger local exchanges will appear.

It also means that your friends and family may be willing to lend you US dollars to get bit dollars, because they don't have to worry about exchange rate risk and get real rewards from them. Once they start to make a profit, I'm afraid they won't stop.

# Case

### Local deposit

Grandma wants to get 10% of her dollar in return, but she won't use a computer. So her grandson decided to help her, and he took the dollar from her grandmother to buy Bit USD. He posted on the classified advertising website that he sought to buy some Bit USD. Someone responded to him saying that he could exchange Bit USD with his paper money. After the deal was completed, Sun Tzu could print out his private key and give her grandma and let her under the mattress.

### Local presentation

A year later Grandma decided to take her dollar back, so she contacted her grandson and gave him his private key. So Sun Tzu searched the classified ads for people who need to buy Bit USD. After their meeting and the success of the deal, the Sun Tzu handed the dollar to her grandmother.

### Intermediary long distance deposit

George lived in a remote place, his nearest hold people in addition to $bit hours away, fortunately, he has a family living in a big city, so he called his brother offered to pay $10 to help him to buy $1000 worth of extra than $from local. After his brother agreed, George hit 1010 dollars, and after buying 1000 bits of dollars, his brother sent the dollar to George (through the interlinked chain).

Short selling

Sam is a trader who specializes in encrypting money. He has been paying close attention to the market, and he finds that the dollar dollar is overvalued relative to the interoperability chain. So it decided to sell bit dollars to "empty". In this way he must give up the bonus. If he is right, the price of bit dollars will decrease compared with the interworking chain, so he can buy back the bit dollar at a lower price, and the profit will exceed his bonus. If he is wrong, the price of the dollar will rise and the network is forced to lose. So if you want to make short profits, you'd better expect the price to drop more than the dividend you give up, or you can sell the bit dollar at a premium.

Leveraged speculator

Alex, an early enter of a BTS, had dug 100 BTS and believed that they would add 3 times in a few months. He can hold it simply, but he wants to appreciate by leveraging. So Alex sold out bit dollars. If he is right, then he will get more bonus than a simple possession of BTS from the sale of the air. In this way, Alex created a bit of dollar in the early days of the exchange chain, which has rapidly appreciated and paid high dividends to avoid risk.

Currency hedge trader

Alice is a currency trader in the dollar / euro market. Alice has dug some interoperability chains and uses them to buy the Bit EUR and short bit dollars because she expects the euro to appreciate relative to the dollar. When she keeps such a position, she has no risk of net exposure to the price change of interchanges, because any loss of empty positions will be compensated in long positions. Exchange chain bubble speculation

David thinks that the price of the interconnected chain has already

bubble, so he buys the bit dollar to expect appreciation relative to the exchange chain, and also hopes to get a high bonus in the process.

merchant services

Fernando is operating an online store, hoping to receive payment by encrypting money. Unfortunately, all of his suppliers are using the dollar. Fernando chose to use the bit dollar to mark the price. The result is that his clients get a stable price. Fernando avoids the transaction fees generated by Mt. Gox and other exchanges, and Fernando can get dividends when he waits for settlement.

Bitcoin speculator

Lu Keyou some bits, it wants to use interworking chains to buy some Bit BTC. First, he had to find some Bit BTC, so he found Charles with some Bit BTC and wanted to change to a real BTC. So, Luke and Charles used cross - chain trading to exchange Bit BTC and BTC, not much to worry about 'exchange rate', and they should be 1:1.

The function of cross - chain trading will be built in the interworking chain client, and Luke and Charles only need to specify their respective addresses and exchange rates. The client will support the broadcast bid to "real time" and negotiate with the opponent, and all transactions will be "expired" within 20 minutes. Because BTC is a very small market for Bit BTC, it should have fast liquidity and enable all nodes to be activated and interactive without worrying about the market being too thin. Even 2 people online can work properly.

Gold bank of 100% reserve

In the payment of dividends can create an interesting bit of gold products, it will establish a decentralized, peer-to-peer, "100% Gold Reserve Bank", if someone want to deposit in the bank, advertising that want to use 1 gold coins to buy a 1 bit of gold. And someone who wants to extract gold from the bank will respond to the advertisement. Assuming that the funds for the depositors and the withdrawals are 1:1, there should be almost no premium or transaction fees.

If the depositor is more than the withdrawer, then the depositor will have to pay a small "ATM" fee for the deposit. If the situation is the opposite, the ATM will have to pay the "ATM" fee. The "ATM" fee will be a supply and demand regulator for the depositors and the withdrawals. When the deposit cost is made, the depositor will hold it until it falls. High deposit costs will stimulate empty money to sell more bits of gold to get real gold to gain profit from the handling fee. When the cost of the withdrawal rises, it will attract those who understand it as a deposit.

# The legal classification of the bit assets derived from interworking chains and interworking chains

Before providing our opinions on the law, we must remind readers that we are not lawyers, and the following statements do not constitute professional legal advice. Before taking any action according to the opinions expressed below, please consult the legal profession according to your situation.

Throughout the full text, we refer to buying many, selling short, margin, buying put option and other traditional financial terms and tools, but these are used to explain the analogy of new bit asset performance. We believe that in addition to the most commonly used term "assets", these tools do not conform to the legal definition of financial assets, tools, bonds or any other written terms. Before we try to classify these new bit assets, let's review the current definition.

Financial assets are intangible assets derived from the requirements of the contract.

A financial instrument is defined as "a contract to form a financial asset of an entity and form another entity's financial liabilities or equity instruments." According to International Accounting Standards No. 32 and 39.

A contract is a voluntary agreement of two or more than two parties, and each party has the intention to create one or more legal obligations between them. A contract is a promise of legal force to ensure that something happens or does not happen.

The elements of a contract include:
1. the agreement between the proposal and the reception and the opinion.
2. The intention bound by the law.
3. The factors to be considered.
In addition, the parties to a contract must have the ability to perform the contract. The purpose must be lawful, and the form must also be lawful. The purpose must be to establish a legal relationship, and all parties must agree.
According to EU law, you have to consider the MIFID (financial tool market directive). The instruction set of a regulated market is defined as a market operator operations and / or management of multilateral system, which the multiple third party transactions through financial instruments together in the system according to the non discretionary rules - with a financial tool to produce a contract commitment in its trading rules and under way and / or system. These third parties are authorized and operate according to law three.
The common point behind all existing financial assets and liabilities (including cash) is the contractual obligation. If there is no contractual liability made by the other side, the bit assets derived from the interworking chain are not financial instruments. So let's see if we can find out from the interworking chain the features that meet all, or most of the contract requirements.

1) enter and sell trade to block chain
Buy or sell Guadan is issued by a single anonymous transactions encrypted signature of a party. There are no other parties' signatures and legal obligations. Buy or sell Guadan has no legal status, nor create legal relations. These are your personal network anonymous and do not have the ability to submit anonymous trading pending the contract. In theory, including the buying Guadan Guadan to block the payment, and can be regarded as miners signature and acceptance. However, when the transaction is included in the block, the two sides of the anonymity still have no clear obligation or legal relationship. Further, it is not true that a miner simply includes a deal in a block that does not really lead to the execution of the transaction. It must be accepted by all the other nodes in the network. Even so, there is no legal relationship and obligation between the two parties. Even, the outcome of the accepted transaction is only an anonymous update of the global shared database, which is equivalent to free speech.

2) short selling is entered into the block chain
This kind of transaction has the characteristics of all buy / sell transactions, and the only difference is the type of bit assets entered in the transaction and the nature of the output. It is still signed by a single anonymous dealer and will never be signed by other traders. There is no legal obligation created here or

legal relationship between two parties or parties.

3) miners' additional and flat deposit
No one have a contractual obligation to add the deposit or liquidated, however, when the network most agreed, no one has the ability to stop their positions by squaring a result, none of the margin obligations, there is no mandatory legal consequences do not need to take additional time. In fact, no market entity can impose an additional margin, so no one needs to be responsible for the failure.

4) contracts between developers and users
The interworking chain is a protocol that can be used to deliver information among any number of individuals. Developers publish software open source code, but do not guarantee or promise any special performance. Software users choose to use the software version and join the network, so it can fully control how to respond to the information they get from the network. Users can even be free to modify their software as they want, so the performance and decision of the software is a user, not an extension of the will of the developer.

Finally, developers of interworking chain create a financial system to manage centralization database. Any input of database is not under the control of developers.

5) exchange regulation
A centralization bitcoin / Wright currency exchange operated by a market operator can be supervised, because the accepted encrypted currency deposits are converted to cash commitments on a specific server based on account balances.
There is no market operator in the interworking chain, nor any party at any point, converting the bit assets into financial instruments for the purpose of connecting more than third parties. The reason is that there is no Party B, Party B or the contract between the parties.

6) distributed intermediation and arbitration system
In order to promote the exchange of traditional assets and financial instruments, the interoperability chain provides a distributed, informal, unbundled intermediary and arbitration system. Every undisputed intermediary transaction has two parties, and there will be three parties when the dispute arises. The two parties have a binding agreement, including arbitration clauses, which are allowed to be set in advance, but the third party on the basis of anonymity decides them in a completely non binding (legal

sense) manner. There is a private informal agreement between the two parties that other network members know about. Intermediary agents can not receive the funds or send the funds to the third party outside the two party.

Intermediary agents will comply with any laws, regulations, and arbitration licenses, if the user wants their adjudication to be legally enforceable. Fortunately, intermediary agents and users clearly have no legal obligation to perform specific actions, and therefore have no intention to create a legal relationship. By declaring at any time, no party has any legal obligation to comply with any special clause at any time, it will eliminate the will to establish legal relationship. As a result, all parties are going to move away from the court decision in an informal and totally voluntary way. It's like meeting someone in a bar and failing to get there.

Social and market pressure will lead to an honest and moral decision by all parties in the absence of legal obligations.

The only remaining legal issues is a bit in assets and tangible goods or traditional financial assets (such as cash) whether transactions between individuals will be rational regulatory system or court classified as money transfer, Fin CIN has issued guidelines in bits of assets trading financial assets are not considered in the money or money transfer service business, as long as there are only two transactions, no contract, and no party is represented in the third party transactions, there is no transfer of money. It is like claiming that someone who exchanges cash with gold in a non commercial way in a classified ad is the same as a currency transfer.

Since we are not a lawyer, all the views described above do not constitute legal advice. So when you are ready to take any action that may have legal consequences, seek professional legal advice.

# Alternative system

Many attempts have been made to de centrate exchanges with other assets, such as US dollars, gold or silver, and the exchange chain is introduced as an alternative to these attempts. We will list the more mature solutions in the existing attempts and discuss the differences between them and the interworking chains from the beginning of the standard formulation.

Ripple

Ripple is a point - to - point network that uses a custom currency (XRP) to facilitate transmission and transaction or exchange money in any unit. Ripple is not a network without trust, but a way of allowing friends or family to transfer credit through a network. Each individual must publish a credit path that extends credit to everyone they know, which leads to a risk of breach of contract. In our view, this is not a socialized feasible arrangement, which means that most people eventually use the Ripple gateway. And Ripple's gateway is like a bank that accepts deposits by exchanging credit on the Ripple network. The gateway may encounter legal and regulatory problems encountered by money transfer providers or any deposit taking company. The final result is that Ripple is not centralization, nor does it provide limited liability for all parties.

In addition, Ripple does not support short selling, and options are therefore not diversified. With the dependency on the centralization gateway of Mt. Gox and Bit stamp, currency transactions are not aggregated, atomic or passive.

Finally, Ripple doesn't protect privacy, because everyone must associate their Ripple identity with their real world identity, so as to establish credit paths with friends, family members and gateways. Ripple is not open source at the moment, although it promises to open source later.

Finally, the commercial value of Ripple is not enough to attract people or business organizations outside the encrypted currency movement to start a gateway. Therefore, it is difficult to be popular.

Local Bitcoins

Local Bitcoins is an over-the-counter exchange with a built-in intermediary service. Although transactions occur between individuals, the web site is not centralization, and intermediary services depend on personal credit.

In addition, transactions are not rapid, atomized, privacy, aggregated, and unsafe. The price is not correct because there is no buying and selling system and all transactions are finally referenced to the price of the centralization exchange.

It is not diversified, because there is no short selling, options, etc. Web sites may also face huge responsibilities because of intermediary services.

Colored Coins

A colored coin is a method of turning it into an encrypted, anonymous bond by marking the bitcoin in the block chain. In essence, the system is based on the trust of the issuer and is responsible for the enormous legal responsibility, and the unregistered bonds produced are unreplaceable among the issuers. This system is still not short option and lack of diversity, there is no solution to the center of the pending list and execution of the passive guadan. Finally, because there is no price suggestion, it will be difficult to be popular, and it is difficult to increase the liquidity in the market. The transaction of the colored currency is not passive, and the non centralization of the exchange can not be gathered.

Open Transactions

OpenTransactions is a joint trading server system that allows users to handle, broker, and trade secret bonds encrypt by third parties. The system is essentially based on trust for issuers, and needs to audit transaction servers. Moreover, because different issuers of dollar bonds can not replace each other, they will lead to wide spread of price in narrow market. The creation of a "basket of issuers" will be dispersed, but it does not eliminate the risk of default, and is equal to the use of high credit issuers to subsidize low credit issuers. The system does not provide attractive features to promote popularity, and the recommended system for coordinating prices among multiple servers also violates the principle of price correctness.