π White Paper

(v1.0 beta)

Contents

Abstract

This article introduces the principles and technical architecture of a brand new blockchain technology **π**.

This article surveys the advantages and disadvantages of the existing blockchains like BitCoin, Litecoin, Ripple and BitShares, then analyses consensus process and usage of these technologies. With combination of the application direction of **π**, we design the blockchain technology of this brand-new concept **π**.

π solves the network efficiency problems through the consensus mechanism of IPoS. The new assets are additionally issued and allocated through the original Pi incentive algorithm to promote the network activity and its healthy and stable development. **π** invented referendum mechanism to decide the subsequent issuance rate. Through this democratic way, every user of **π** has the right to decide the direction of the platform.

π provides rich smart contract interfaces and the users may flexibly create various types of smart contract applications on the blockchain to fulfil their different requirements.

Background

Bitcoin

On November 1, 2008, a person claiming named Satoshi Nakamoto published a thesis titled Bitcoin: A Peer-to-Peer Electronic Cash System on the Internet and proposed how to construct a decentralized electronic transaction system with a point-to-point network.

On January 3, 2009, he achieved the first Bitcoin reference client and dug up the first block in the Bitcoin history. The first 50 Bitcoins were generated in this world.

From then on, Bitcoin became a flourishing ecological system step by step. Although it went through various crises and its market value fluctuates significantly, the thought of Satoshi Nakamoto in the thesis is well known by people all over the world via Bitcoin as a medium. People start to explore the infinite possibility of Bitcoin and blockchain technology behind it in the future.

As an originator of the blockchain technology, Bitcoin has the following characteristics:

1. Record the data in such an open distributed database as blockchain, the data are stored in the blocks, and all blocks have an immutable timestamp, which are connected in a chain manner in chronological order and the data generated cannot be tampered.

2. Ensure the data security as well as participator's privacy in a manner of asymmetric encryption of the cryptology.

3. Issue the new coin in a manner of Proof of Work, which is used as the motive power of network development. Proof of work enhances robustness of the network. The more people involved in the mining, the stronger the network becomes.

4. The transaction parties may safely transact without participation of a centralized mint or authority. This makes Bitcoin a real decentralized currency, which is completely out of control of governments or commercial structures.

5. No risk of double spending.

The PoW mining design greatly enhances people's enthusiasm to participate in Bitcoin and more and more calculation power is invested, which greatly ensure the network reliability.

However, along with expansion of the network scale, Bitcoin mining has undergone several stages of CPU mining, GPU mining, FPGA mining, ASIC mining, large-scale cluster mining. The computational power of the mining from the initial few tens of M Hash per second, developed to the present T Hash per second level. Within just a few years, the computational power has increased millions of times.

With the progress of mining technology and the increase of mining computational power, it is very difficult for the ordinary miners to mine Bitcoin by themselves, this facilitates the miners to work together to form a pool for mining. Such spontaneous behavior is in breach of the design of Satoshi Nakamoto, because once a pool masters more than 50% calculation power, the foundation of the Bitcoin will be fluctuated.

In addition, another side effect brought about by the mining competition is higher and higher operation cost of the network and the maintenance cost apportioned to each Bitcoin is higher and higher, which may result in reduction of low enthusiasm of the Bitcoin to participate in the network, and thus the network scale is reduced.

At present, it will take at least 10min to generate a block for the Bitcoin network, which is too slow for instant spending. In addition, the handling capacity of the Bitcoin network is also limited. At present, it only reaches the handling speed of unit digit transaction per second (TPS), which cannot meet the requirements at the occasion where frequent transactions with a small amount are conducted.

Other Blockchains

The appearance of the Bitcoin also stimulates that of a series of derivative technologies. Based on the basic principles of the Bitcoin, such technologies add their own commercial or technical innovation.

Litecoin

Essentially, Litecoin is built on the same principles of Bitcoin, Litecoin has the following characteristics:

1. Litecoin accelerates the block generation speed, it changes the generation speed from 10 minutes per block to 2.5 minutes per block. Faster block generation speed means faster transaction process speed.

2. The expected total output of the Litecoin is 84 million, which is just 4 times as Bitcoin's 21 million.

3. Litecoin uses crypt as its proof of work algorithm, compared to Bitcoin's Hash algorithm, GPU mining has no advantages beyond CPU mining (This was before ASIC mining machine's invention).

Just as Bitcoin is called the gold of digital currency, Litecoin's goal is to become the silver of the digital currency. It produces faster, its total output is higher, it's more dividable, all these features help it to fulfil this goal.

However, essentially, Litecoin does not change any core idea of Bitcoin. Although it increases total output, accelerates the block generation speed, it's still the same as Bitcoin, the handling efficiency is the same magnitude as Bitcoin, which still cannot meet the highly frequent transaction requirements in the existing commercial society.

Ripple

Ripple's vision is to build the world's first open payment network. It is a distributed P2P clearing network.

Ripple has following characteristics:

1. It supports transfer of multiple currencies, in addition to Ripple's own native currency XRP, it also supports fiat currency (such as dollars, yen, yuan, etc.), a variety of digital currency (Bitcoin, Litecoin, etc.) transfer. It achieves a variety of digital assets transfers through gateway trust.

2. It supports the automatic exchange of trans currency, through the role of market maker, Ripple helps users to pay any type of currency to get any other type of currency, which achieves all currencies circulation over the whole network.

3. Fast transaction confirmation speed, Ripple's transaction confirmation process can be completed within a few seconds. Ripple introduced a "Consensus" mechanism, only special nodes participate the vote process, this helps Ripple to verify and confirm the transaction in very short time.

4. The client does not need to download the blockchain. The ordinary node can drop blocks that has been verified, only to retain the most recent verification of the ledger and a link to the historical ledger, and thus synchronization and download the total ledger are much easier.

5. No mining, Ripple uses consensus mechanism, only the validator nodes are involved in the block generation process. validator nodes have a very strict join mechanism. By ensuring the security of the validator nodes, it can be guaranteed the integrity of the entire network. This reduces the waste of resources generated by the peer-to-peer mining competition

6. The total amount of native currency is limited. Initially, Ripple has issued all 100 billion XRP and is committed to no additional issuance. Users spend a certain amount of XRP on each transaction (the amount is very, very low, less than 1 cent) as a transaction fee. The transaction fee will not be given to anyone, but permanently disappear from the system

In Ripple, everyone can be their own bank. They can issue credits, and become credit channel (for example, A wants to borrow money from B, they do not know each other, but they both know C, then C can be their credit channel, C first borrows money from B, and then lend it to A, this achieves the goal - A borrow money from B).

Ripple is based on acquaintance and trust lines. This design requires a person who wants to transfer or lend money has to have friends on the network, otherwise, he cannot establish a trust line with other users.

This gateway trust model is very similar to the mode of the existing bank and exchange. We can say it's just an expression on P2P network of these institutions. This is in breach of the principles of decentralization and unnecessary trust declared by Bitcoin.

Only a few validator nodes can participate the block generation process helps Ripple accelerate it transaction process speed. But it's validator joining mode is born doubtful. If some of its founder's or later joined validator nodes are malicious, or compromised by a malicious attacker, it's very likely that more than half node's to commit fraud, putting the entire network in dangerous.

Bitshares

Bitshares is an open source distributed trading system that supports virtual currency, fiat currency, precious metals and other valuable assets. The system provides a solution of a decentralized exchange, makes everyone having the ability to become an exchange.

Bitshares' consensus mechanism is DPoS (Delegated Proof-of-Stake). 101 delegates are elected by all shareholders to generate blocks. We can see them as 101 mining pools, they have equal rights. BTS shareholders can vote for other delegates (pools), if these delegates fail to provide stable service or trying to do evil.

Because there is no mining and no blocks generation by multiple nodes, BitShares' processing speed has been greatly improved. Its official statement says it has achieved a processing capacity as VISA and MasterCard's processing capacity sum up.

Bitshares has following characteristics:

Price-Stable Cryptocurrencies and SmartCoins. SmartCoins provides the freedom of cryptocurrency with the stability of the dollar. A SmartCoin is a cryptocurrency whose value is pegged to that of another asset, such as the US Dollar or gold. SmartCoins always have 100% or more of their value backed by the BitShares core currency, BTS, to which they can be converted at any time at an exchange rate set by a trustworthy price feed.

Decentralized Asset Exchange , BitShares provides a high-performance decentralized exchange, with all the features you would expect in a trading platform. It can handle the trading volume of the NASDAQ, while settling orders the second you submit them.

Industrial Performance and Scalability. High performance blockchain technology is necessary for cryptocurrencies and smart contract platforms to provide a viable alternative to existing financial platforms. BitShares is designed from the ground up to process more transactions every second than VISA and MasterCard combined. With Delegated Proof of Stake, the BitShares network can confirm transactions in an average of just 1 second.

Delegated Proof-of-Stake Consensus. Delegated Proof of Stake (DPOS) is the fastest, most efficient, most decentralized, and most flexible consensus model available. DPOS leverages the power of stakeholder approval voting to resolve consensus issues in a fair and democratic way. Deterministic selection of block producers allows transactions to be confirmed in an average of just 1 second.

Referral Rewards Program. BitShares has an advanced referral program built in its software. Financial networks derive their value primarily from their network effect: more people on the same network increases the value of that network for everyone. BitShares capitalizes on this by rewarding those who sign up new users, and does so in a fully transparent and automated way.

Dynamic Account Permissions. Every account can be controlled by any weighted combination of other accounts and private keys. This creates a hierarchical structure that reflects how permissions are organized in real life, and makes multi-user control over funds easier than ever. Multi-user control is the single biggest contributor to security, and, when used properly, it can virtually eliminate the risk of theft due to hacking.

However, Bitshares' concept is very complicated, which slows down people's recognition process for it. The manner of BitShares to issue all BTSs in the beginning makes people doubt the fairness to distribute its original assets.

Introduction to New Blockchain- π

Through introduction above, we see that various blockchain technologies have their respective advantages and disadvantages. By referring to such existing technologies, we want to achieve a safe and efficient blockchain, which is easily expanded and promoted, and named π by us.
π is one of the most famous constants in mathematics. As π, it has unlimited sense of beauty and charm; as a special infinite non-repeating irrational number, it if full of mystery, greatly stimulating the exploration desire of people. The reason that we name our technology with it is to hope that our technology may be perfect and charming like it.

Positioning of π

Positioning of π is to achieve a safe and reliable common blockchain platform with light weight and low cost, which is easily used and expanded and the possible application fields include:

- Decentralized application.
- Digital assets management.
- Smart contract platform.

We issue an original digital asset π as an original driving force of all activities on this platform. To participate in the π network activities in different manners will consume or obtain certain π. The existence of π is to stimulate the user to participate in the construction of the π network and get appropriate income from it. Along with development of π network step by step, all π holders will be benefited continuously.

Consensus Mechanism of π

In the previous article, we studied Bitcoin and Litecoin, which are based on proof of work theory. Their advantage is they are totally decentralized, and their disadvantages are their block generation cycle is too long and their process capability is low. We studied Ripple, whose block generation is based on validator voting consensus. It increases block generation speed and transaction process speed, but these are achieved at the expense of the absolute meaning of decentralize. At last, we studied Bitshares' DPoS (Delegated Proof-of-Stake) mechanism. By electing block generation node, all users are involved in the block generation process. Wiht only a few delegates generate blocks, computation and communication costs are cut down, which helps getting ideal block generation speed and transaction process speed.

Through research on the existing consensus mechanism above, we decide to use a consensus mechanism called IPoS (Improved Proof of Stake) created by us. It's based on PoW (Proof of Work), and we make a lot improvement.

IPoS has following features:

1. Blocks are generated by only a few nodes elected by all users. These nodes usually hold a lot π by their selves, and are widely accepted by the network. They can get more benefits by honest work beyond fraud work. With only a few nodes to generate block, block generation speed and transaction process capability are greatly increased. Block generation speed of π is set as 3 seconds per block, for small amount payment, this can be seen as processed real time.
2. Use construction capital to issue. We'll explain construction capital in detail in the following sections. It's core idea is to encourage uses to hold π, to express their recognition of π, which helps the development of π. Construction capital also gives user income.
3. Through construction capital, we introduce social elements into π, we encourage users to promote π to others, and get more income in promotion process.
4. Increase scalability through smart contract. π executes smart contracts during consensus process, smart contract helps users to build different types of application, to fulfil their requests.

Performance and Expandability

Benefited from the IPoS mechanism, the mining concept in π is completely different from PoW of Bitcoin. The block node mined from π is elected by the algorithm, rather than competition of many nodes.
π generates a block in 3 seconds, this is much faster when compared with Bitcoin's 10 minutes and Litecoin's 2.5 minutes. When compared with Ripple and Bitshares, which produce block in about 10 seconds, it still has advantage.
Therefore, the transaction handling capacity of π is enhanced by several orders of magnitudes compared with that of the Bitcoin. We expect that the handling capacity of π will at least reach the magnitude of VISA and MasterCard in the future or even higher.
As for expandability, π is totally decentralized, every can run their own π node to join the network. By adding new nodes, we can improve the responsiveness of π, so we can say that π has infinite scalability.

Security and Privacy

Like Bitcoin, the whole π system is based on the cryptology system through mathematical theoretical demonstration. Therefore, we have good grounds to believe that π may at least reach the degree of security of Bitcoin.
All transactions on π network are anonymous, so there's no need to worry about leaking personal information.

For the block data, we provide the encryption option to ensure that only transaction parties may know about the specific transaction contents and the nodes on the network only verify the transaction legality, for which it is unnecessary to know about the specific contents, radically meeting the user's requirements for privacy.

Issuance Algorithm

While π is applied wider and wider, the requirements for it will be higher and higher. Moreover, according to the law of economic development, the economic aggregate grows continuously. Therefore, we design a reasonable issuance algorithm to adapt to such economic aggregate and change in application mass.
One reasonable issuance algorithm not only adapts to the economic development law, but also promotes the system promotion and attracts more people to actively use the π network and participate in its construction process.
At the beginning of creation, we will issue 10 million π as initial capital. Then, we will issue more according to certain rules during the process to generate new blocks in the future.

In order to elaborate the specific issuance rules, we first introduce several concepts.

Construction Capital

To hold π stably means to recognize its network. More people holding π stably means that it is recognized more pervasively and the construction capital is a tool designed for the user to recognize the network.

The construction capital means that the user locks π held by him/ her for a certain period (π in the locking period cannot be transacted) to express his/ her recognition and confidence in the network. The system will provide the user with certain issuance rewards. In principle, the more π are locked, the longer the period is, the more income will be earned.

In order to describe the construction capital, the following conditions shall be defined:

- Locked amount V: It is used for describing the user's amount actually locked. Meanwhile, we introduce an effective amount constant V_{min}. Only when the π amount locked by the construction capital V must be greater than the constant V_{min}, it will be regarded to be effective. For the establishment of this constant, more considerations are given to the achievement of the decentralized blockchain. If the user is allowed to establish the construction capital with too small amount, there may be lots of construction capital accounts with small amounts in the system. Although they may get a very little of issuance income during issuance, they consume lots of computing and network resources like the construction capital with normal amount. Therefore, in order for health and efficiency of the Pi network, we introduce this constant V_{min}, which shall meet the conditions when it is expressed with a formula as follows: $\mathbf{V} \geq \boldsymbol{V_{min}}$

- Issuance period T: It is used for setting the income distribution period acceptable to the user. Likewise, for the system efficiency, the user's issuance income is not obtained in each block, but distributed according to the issuance period T designated by the user. Namely, a part of issuance income is distributed every complete period with T blocks. Because the issuance computing per time consumes the system resources, the fixed handling charge F with a small amount will be charged when the issuance income is distributed each time. Theoretically, the longer the issuance period selected by the user, the less the handling charge to be charged finally, which encourages the user to set the longer issuance period to reduce the system resource consumption and handling charge expenditure of the user. We set a minimum issuance period constant T_{min}, which is used for restricting the user to set too short issuance period, with its formula as follows: $\mathbf{T} \geq \boldsymbol{T_{min}}$

- Locking duration L: L is used for marking the locking duration of the construction capital, which is a positive integer greater than or equal to 1 and its value means the locked issuance period quantity. If the block quantity is used for express the locking duration, with the formula as follows: $\boldsymbol{L} * \boldsymbol{T}$

Acceleration Mechanism

The acceleration mechanism is a mechanism to encourage the user to promote the π network to others.

After establishing its construction capital, the account may help other users to accelerate with its construction capital, with the result to accelerate their income output efficiency of the construction capital. Such mechanism forms a flexible social system. The user may develop new users through actively promoting the π network and persuade them to accelerate for him or her to get additional income.

If there are n accounts to accelerate for account A, the construction capital amount of each account is V_i(C = 1,2,3 ... n), the period of the construction capital is T_i (i = 1,2,3 ... n), and the locking duration is L_i (i = 1,2,3 ... n). We use S to represent the acceleration index of account A, with its definition as follows:

$$S = \sum_{i=0}^{n} V_i * T_i * L_i$$

We assume that the construction capital amount of account A is V and the issuance period is T, the acceleration effect is that when the acceleration index S of user A reaches V*T*L, the user will immediately obtain the income of one period and S will deduct V*T*L and L will reduce a period. Namely, the construction capital of A will generate income one period in advance and the unlocking period is also reduced by one period. Acceleration effect has an upper limit, and we specify a maximum acceleration factor – Amax. We assume that the locking duration is L, then we can at most generate income L*Amin issuance periods in advance. One construction capital can only accelerate L*Amin issuance periods even calculated acceleration index is bigger than that.

Issuance Interval

Our issuance algorithm is based on the construction capital. From the moment when the user's construction capital takes effect, the user will get the issuance income every T block(s).
The generation speed of π network block is set to 3s per block the current value of T_{min} is 201,600, i.e. 7 days.

If the value of T set by the user is 201,600, the user may get some issuance income every 7 days.

Issuance Rate and Referendum Mechanism

Issuance Rate

The issuance rate d is used for marking the issuance speed of the system, whose meaning is the yield to be generated by the construction capital for one year.

The system will perform issuance in the initial stage according to the preset issuance rate and the issuance rate is adjusted with 3 months as a period. The initial issuance rate will be reduced step by step according to the pre-set value.

When the issuance rate is reduced to a certain rate (at present, the time point of the first referendum is the 11^{th} period and the income rate for 50 weeks will be reduced to 50%), the system will initiate the referendum mechanism to decide the subsequent issuance rate.

The system performs issuance according to the issuance rates shown in Table below.

Adjustment period of issuance rate	Issuance rate d (%)	Income for 50 weeks (%)

Mar. 1st,2017	104.2857143	100
Jun. 1st,2017	99.07142857	95
Sept. 1st,2017	93.85714286	90
Dec. 1st,2017	88.64285714	85
Mar. 1st,2018	83.42857143	80
Jun. 1st,2018	78.21428571	75
Sept. 1st,2018	73	70
Dec. 1st,2018	67.78571429	65
Mar. 1st,2019	62.57142857	60
Jun. 1st,2019	57.35714286	55
Sept. 1st,2019	52.14285714	50
Dec. 1st,2019	Launch the referendum to determine the issuance rate	
Mar. 1st,2020	Referendum determines the issuance rate	
Jun. 1st,2020	Referendum determines the issuance rate	
Sept. 1st,2020	Referendum determines the issuance rate	
Dec. 1st,2020	Referendum determines the issuance rate	
Mar. 1st,2021	Referendum determines the issuance rate	
…..		

Referendum

On December 1st ,2019, the income rate for 50 weeks will be reduced to 50%, the system will enter a stage of referendum mechanism to determine the subsequent issuance rate. All

Pi holders and construction capital may participate in the vote to determine the subsequent issuance rate.

The referendum system will provide the three options

1. Increase issuance rate to achieve 5% more income rate for 50 weeks.

2. Decrease issuance rate to achieve 5% more income rate for 50 weeks.

3. Maintaining current issuance rate.

The referendum will employ the mechanism of one vote for each π and any account holding π or construction capital may participate in the vote. Accounts can vote from the three options, more π or construction capital they hold, more powerful their vote. The process of voting is entirely fair and transparent.

Referendum will have a voting period. It's usually start a week before next issuance period. For example, December 1st ,2019 will be the first referendum period, the system will launch the referendum on December 25th ,2019. Users can vote and check current vote status during the period.

Referendum ends before the first block of next issuance rate period, options with most votes will become next issuance rate.

Issuance rate referendum has cap and lower limit, the final issuance rate must fulfil the 50 week income rate between 0% and 100%. If 50 week income is 0, there will be no option 2, if 50 week income rate is 100, there will not be no option 1.

Calculation Method

We assume that the construction capital amount of user A is V and the issuance period is T, the income D that A may get during one issuance (may satisfy the period T, or acceleration index reaches the threshold of output in advance) may be calculated with the following formula:

$$D = \frac{\mathrm{V} * \mathrm{T} * \mathrm{d}}{10512000}$$

Where 10,512,000 means the total block quantity during a year, i.e.365 days (one block per 3s).

Node Income

As a distributed network, π network welcomes all people to operate their own node to join it. To operate the π node not only gets better access effects and enhance the soundness of the π network, but also brings about certain income for itself. The system has π which is about equivalent to 15% of the issuance amount increased each day to be distributed to all accounts operating the Pi node.

In the initial network construction period, the service version is changed very frequently and the π network will be operated in a closed manner. The official node will use the node income in this stage for market promotion. When the opportunity is right, the node will be opened for joining and any person may obtain fair income through operating their respective node.

Smart Contract

π provides rich smart contract interfaces and the user may flexibly create various types of smart contract applications on the blockchain. For example:

- The user may create a smart contract for the locked construction capital. When the contraction capital expires, the new contraction capital is established automatically, making the user not suffer the issuance loss due to forgetting the renewal of the construction capital.

- The user may set a smart contract. When receiving the income from issuance increase, it will automatically transfer the income to other designated users, which helps the merchants construct the feedback system to give their own income to the valuable customers, so as to enhance their service attraction to them.

Because π provides rich interfaces, its potential will be infinite only if you have sufficient imagination.

Conclusion

Through analyzing and summarizing the current application situation of the existing blockchain and with combination of its application characteristics, this article proposes a new blockchain platform π.

π uses a brand-new IPoS consensus mechanism, greatly optimizing the energy consumption and efficiency of PoW of Bitcoin and giving consideration to fairness at the same time.

The original π issuance incentive algorithm may distribute the income fairly while ensuring the efficiency, promoting healthy development of the network.

Attached: Discovery Application

Discovery is an application established on π, which achieves some of its functions using the smart contract.

Discovery has concepts of treasure hiding and mining. Treasure hiding corresponds to locking the construction capital, while treasure mining corresponds to getting the income from issuance increase. The yield of treasure mining may be estimated according to the amount of the construction capital. On this basis and with combination of the digital asset spending, develop an application model of Payment.

Meanwhile, using the acceleration mechanism of π and game rules set by Discovery, make the users of Discovery enhance the treasure mining speed of the main account through inviting more users.