****

**Year**

**2019**

**BitSilver**

****

**BitSilver**

**白皮书**

**构建面向未来的全球白银价值交易中心**

**重塑世界经济格局**

**Contents**

[Preface 4](#_Toc2795)

[Foreword 1](#_Toc24705)

[Project Introduction 4](#_Toc9738)

[Project Philosophy 6](#_Toc31620)

[Design Philosophy 8](#_Toc24075)

[Chapter I. Pain-points of Global Silver Market and Birth of BitSilver 10](#_Toc19974)

[1.1 A Brief History of Silver 10](#_Toc13845)

[1.2 Modern Silver Market 12](#_Toc6616)

[1.2.1 Investment-grade Physical Silver 12](#_Toc3824)

[1.2.2 Challenges in Today’s Silver Market 13](#_Toc12784)

[1.3 Blockchain Will Subvert the Traditional Financial Industry 15](#_Toc22469)

[1.4 BitSilver Was Born at the Right Moment 17](#_Toc14524)

[Chapter II. Project Introduction of BitSilver 19](#_Toc24993)

[2.1 What is BitSilver？ 19](#_Toc31234)

[2.2 Usage of BitSilver 21](#_Toc21601)

[2.3 Vision of BitSilver 22](#_Toc1200)

[Chapter III. Technology Innovation System of BitSilver 24](#_Toc30641)

[3.1 Top Technical Architecture of BitSilver 24](#_Toc3152)

[3.1.1 Data Layer of BitSilver 24](#_Toc22848)

[3.1.2 Network Layer of BitSilver 25](#_Toc5883)

[3.1.3 Consensus Layer of BitSilver 25](#_Toc24921)

[3.1.4 Incentive Layer of BitSilver 26](#_Toc25599)

[3.1.5 Contract Layer of BitSilver 26](#_Toc12672)

[3.1.6 Application Layer of BitSilver 27](#_Toc6290)

[3.2 Underlying Technology of BitSilver 29](#_Toc17610)

[3.2.1 Transaction 29](#_Toc27468)

[3.2.2 Time Stamp Server 30](#_Toc18427)

[3.2.3 PoW (Proof-of-Work) 30](#_Toc3131)

[3.2.4 Network 31](#_Toc4032)

[3.2.5 Incentives 32](#_Toc14031)

[3.2.6 Recycle of Hard-disc Space 32](#_Toc1399)

[3.2.7 Simplified Payment Verification 33](#_Toc1010)

[3.2.8 Combining and Splitting Value 35](#_Toc26459)

[3.2.9 Privacy 35](#_Toc1537)

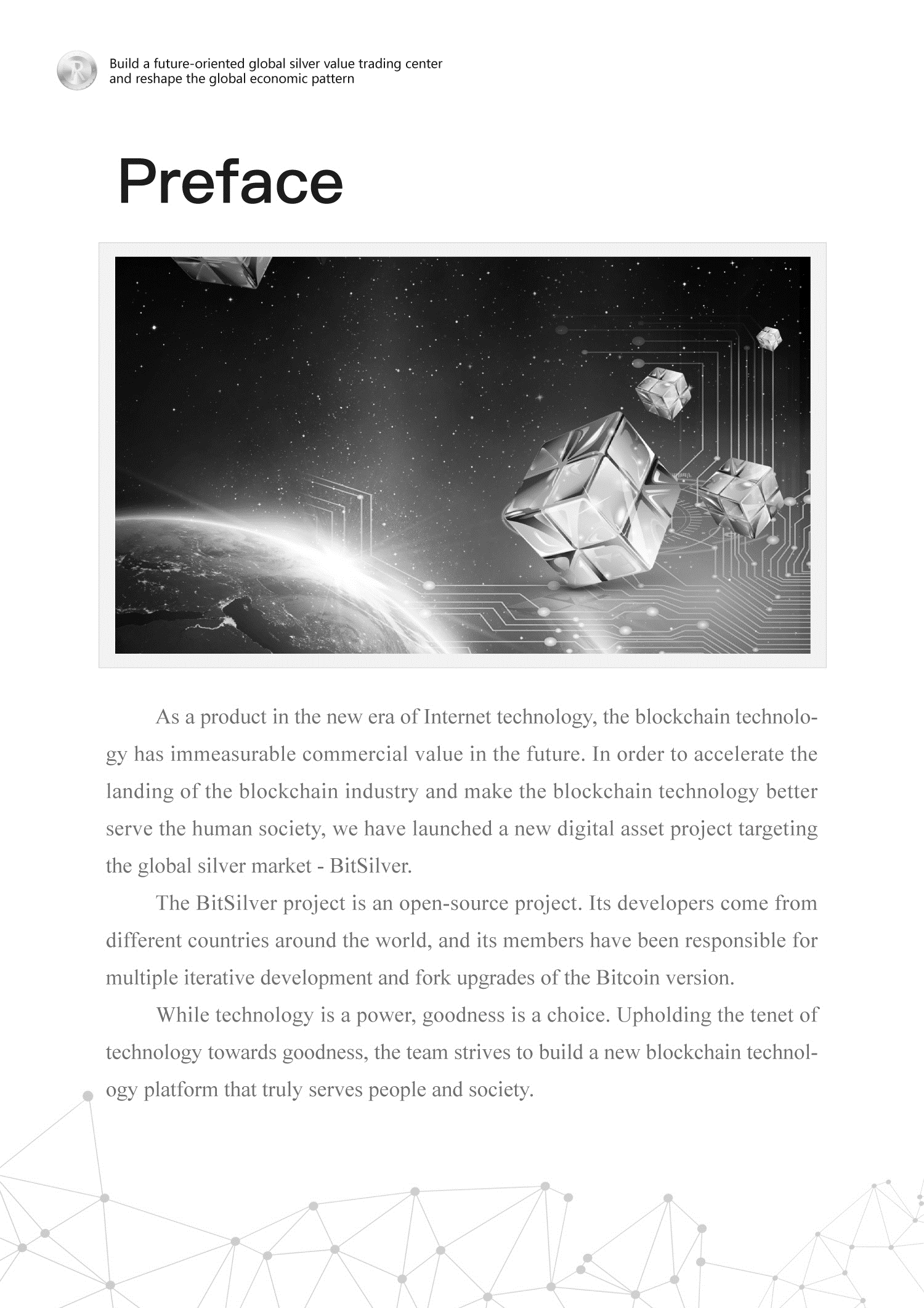
[3.2.10 Calculation 36](#_Toc24349)

[Chapter IV. Economic Model of BitSilver 40](#_Toc17804)

[4.1 Introduction to BitSilver 40](#_Toc18987)

[4.2 Property of BitSilver 41](#_Toc11517)

[4.3 Decentralized Self-governed Community 42](#_Toc10541)

序

Foreword

Today, human wealth is supervised and controlled by third-party organizations. People cannot truly be free, and can’t avoid the situation that assets are frozen at any time. Silver has historically played an important role in the global financial system. Due to its scarce quantity, stable chemical properties, strong plasticity and attractive appearance, silver is recognized as very valuable. Silver has been used to store value for thousands of years and it is still very popular now. More than $50 billion worth of silver is traded daily through exchange-traded fund derivatives and physical markets. However, silver has high storage costs, division difficulty, mobility inconvenience, and transaction or utilization difficulty. Currently, there are no investment-grade physical silver products that can be easily owned and traded

We hope that everyone can be free and move towards a better life. In this white paper, we designed a decentralized distributed ledger system for the global silver market regulation, so that ordinary people may easily own and trade investment-grade physical silver products. This project is named BitSilver. This paper will discuss how to create a decentralized consensus ecological network based on the silver market from the perspectives of design and basic information

By utilizing the technical characteristics of blockchain, BitSilver ecology has built the first truly fair and decentralized ecological network for human beings, so that human assets will not be supervised and controlled by third parties. As long as the users own BitSilver, they can access all the life services in the BitSilver ecosystem.

We have created the most convenient way for people, so that they can obtain, own, trade or lend the investment-grade physical silver that is stored in the treasury in an affordable way, without worrying about the cost, inconvenience and security of their physical storage. In addition, the BitSilver ecosystem will increase the liquidity and popularity of silver across the world.



Project Introduction

To cope with the basic contradiction that it is difficult to own and trade investment-grade physical silver products in the current silver market, BitSilver has launched an innovative solution - BitSilver, thereby addressing pain points in the market. With the design principle of decentralized anonymity, BitSilver has created a “privacy Internet” built on distributed nodes for serving the society and enterprises. Through a specific gateway, the BitSilver system benchmarks global silver reserves in fixed proportions and moves them digitally to the silver network, so that people can participate in the silver market investment and personal assets management in a more convenient, quicker, safer and stabler way. Also, BitSilver solves the fundamental problems of the silver market and realizes the complete ecology of silver spot chain transaction and silver asset management.

BitSilver is an independent public blockchain developed based on the underlying technology of Bitcoin, and all transactions are operated in accordance with the smart contract on the blockchain. Thanks to the smart contract, the system operates strictly as per procedures, thereby eliminating human errors. Moreover, BitSilver supports round-the-clock transaction, which facilitates settlement of various assets. Compared with the traditional silver, which is only settled during bank business hours, BitSilver’s on-chain participation is more convenient and fast.

BitSilver public blockchain is a point-to-point transmission currency system based on elliptic curve cryptography (ECC for short, an asymmetric cryptography implemented based on elliptic curve mathematical theory). For the management of private keys, we have also adopted the Bitcoin asymmetric encryption technology and the original silver consensus mechanism, so as to promote the technological evolution, ecological evolution and service evolution of digital asset transaction platforms.

Project Philosophy

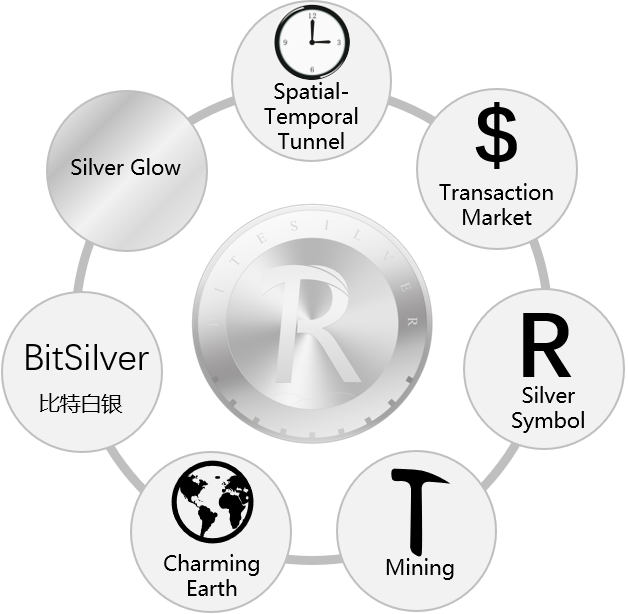
The civilization has always been closely related to the scientific and technological development. From the industrial revolution to the information age, scientific and technological development has promoted social progress and increased productivity; from the industrial revolution to the global Internet age, technological change has influenced the direction of future social progress. In an age when the Internet connects information and resources around the world, we have never been closer and know each other better. Human beings are going through a higher level of consensus civilization development process, which is the progress of human society civilization. Only by establishing a higher level of consensus can human beings better collaborate to create higher values, completely eliminate contradictions and conflicts in social development to push the distribution of wealth to a more equitable and just path, and enable the world to become a community to pursue the new stage of human civilization.

This centralized world is full of problems. No matter how we improve our social and economic systems, we cannot solve these problems fundamentally. As the Asimov elevator effect points out, before key technologies are invented, our imagination is limited to the existing technology.

In this case, the advent of blockchain opens a window of hope. Blockchain technology has broken the human perception of traditional concepts, such as privacy, wealth and even freedom. For a centralized financial system and organization, this is also an unprecedented challenge. All of these will be given a new meaning in the ideal world realized by blockchain technology, where human beings will find their true selves.

The future society will be an entirety linked by blockchain. As a certain product of blockchain technology, BitSilver adopts the decentralized design principle, reaching the consensus of wealth, comment, innovation, network, ideology and even soul progress. By relying on the wisdom of all people, the whole human society will get the freedom.

Design Philosophy



In the BitSilver LOGO, the inner circle represents the transaction market, the outer circle represents the charming Earth, the gimmick symbol represents mining, and the outer circle scale represents the spatial-temporal tunnel. Besides, the logo is combined with the grayish silver luster and the letter R, a silver symbol. BitSilver is a journey of time and space of the soul, which awakens human’s subconsciousness, makes people concentrate on it and realizes the freedom and eternity of life. It represents a silver-based order that opens up an infinitely possible future and leads global practitioners into a higher-level form of collaboration.





**全球白银市场痛点与BitSilver的产生**

**第一章**

Chapter I. Pain-points of Global Silver Market and Birth of BitSilver

1.1 A Brief History of Silver

Like gold, silver is the oldest currency in the world. It was once the main currency in many countries. Silver is synonymous with “money” in over 50 international languages. In the monetary history, silver has played the role of a standard currency earlier than gold. The earliest metal coins came from the kingdom of Lydia in Asia Minor. The metal of money is “white gold”. This “white gold” is not pure gold as imagined, but a natural gold-silver alloy.

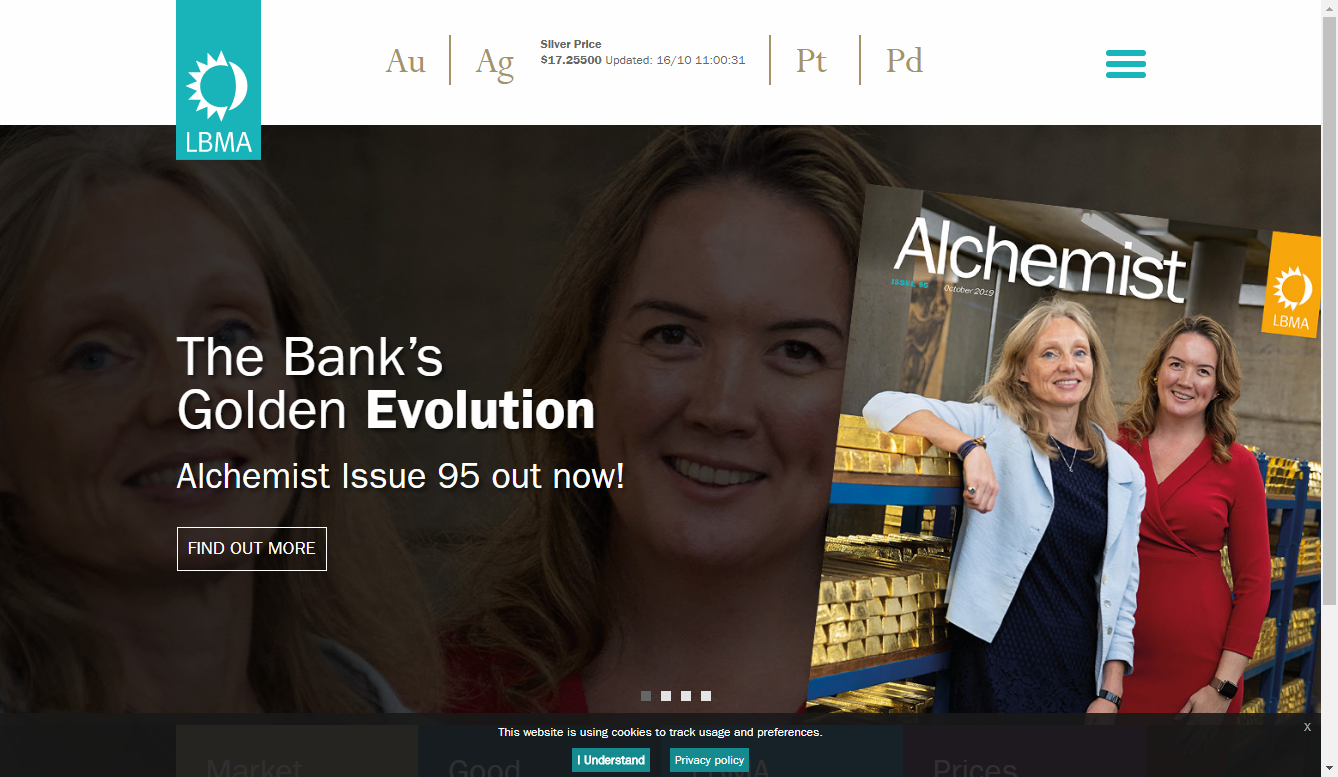
As early as 4,000 years ago, due to the rich silver mines in their colonies such as Macedonia and Thrace, ancient Greeks minted a large quantity of silver coins. As commercial trade activities rose, Greek silver coins began to substantially circulate to the surrounding Mediterranean areas and became an important link for trade activities. Later, the ancient Roman empire collapsed, but some changes brought about by it continued, and the history of silver as currency was preserved.

Throughout the 19th century, from the European medieval period to the Renaissance, the Age of Discovery and the Industrial Revolution, it can be said that white silver was synonymous with money in the western world: money was silver coins and silver coins are money.

Despite the changing times, the demand and value of silver has remained the same. Currently, investment-only silver is worth more than $2 trillion. However, the core challenge still exists: Silver is a heavy unwieldy asset that cannot be moved or accessed on a large scale.

1.2 Modern Silver Market

1.2.1 Investment-grade Physical Silver



LBMA (London Bullion Market Association) was established in 1987. Its main responsibilities are to improve the efficiency of the London silver market, expand the impact of the London silver market, attract investment for London, and promote all participants (including silver producers, refiners and buyers) to carry out business activities. In addition, it cooperates with the relevant British regulatory authorities (such as the British Monetary Authority and the Customs and Excise Department), and maintains the stable and orderly development of the London silver market.

LBMA has set standards for silver bars and for refineries that produce them for the London market. The most reliable silver bars that meet the highest quality standards and are produced by authorized refineries are called “London Standard Silver Bars for Delivery (London Silver)”. LBMA ensures that refineries producing London Standard Silver Bars for Delivery comply with quality standards and due diligence practices.

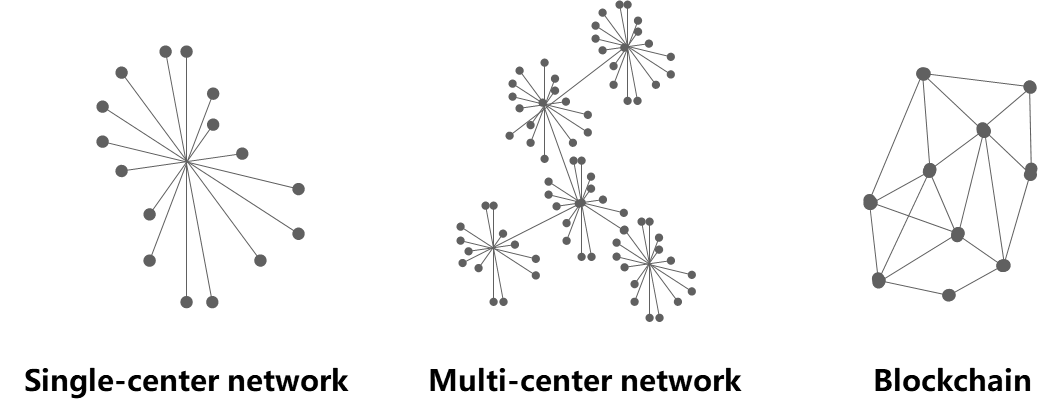
There are two purchase forms of London Standard Silver Bars for Delivery: registered and unregistered. Customers who purchase registered silver will have the right to own specific silver bars that are placed in gold inventory or deposited by the customer. Customers who purchase registered silver will be entitled to certain silver bars that are kept in the vault or at the customer’s discretion. Customers who purchase unregistered silver are not entitled to particular silver bars, but own a portion of the value of a certain amount of silver.

1.2.2 Challenges in Today’s Silver Market

At present, most of the processes for the purchase, sales, transfer, confirmation and settlement of silver assets between the parties are still mainly completed manually, which is not only lacking in transparency but also outdated. Manual processing is prone to errors and it may severely affect market liquidity. The market is largely constrained by a small number of qualified investors, making most of the value of silver unavailable or available to the public.

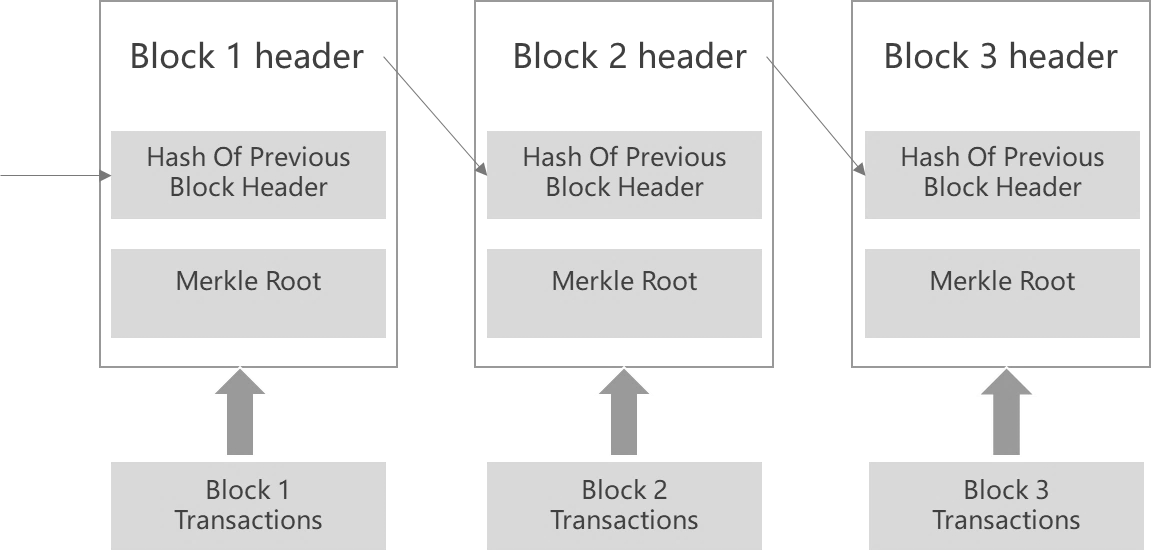
In addition, the size and weight of physical silver becomes a fundamental challenge for the market. Physical silver bars are confronted with difficult transportation and high storage cost, so investors will find silver to be an investment asset to be invested in. Both institutional and retail investors in silver bars face these challenges. Although the existing investment methods have overcome some inherent challenges of physical objects, each market or instrument has its own unique constraints.

1.3 Blockchain Will Subvert the Traditional Financial Industry



In 2008, Satoshi Nakamoto published a paper titled *Bitcoin: A Peer to Peer Electronic Cash System* in which the concept of blockchain was proposed for the first time, established the technical base for encrypted transmission of transaction information, and structured the Bitcoin network. From then on, digital currency has become the most important application of the blockchain technology, and has gained rapid development.

Solving the problems of valued transmission and decentralization, blockchain is praised as the most subversive technological innovation since the Internet was invented, and even the next generation of “value Internet”. Currently, more and more enterprises, after perceiving the powerful energy contained in the blockchain, are actively arranging the industrial layout, thus enabling blockchain to find commercial application in more and more industries and fields.



Value interaction is based on the establishment of mutual trust. The revolutionary character of blockchain technology lies in its realization of a new trust mode. With the design innovation on the aspect of technology, the trust relationship between man and man in the value interaction process can be converted to the trust between man and technology. Some links can even be executed by program automatically, thus enabling the financial activities to be realized at a lower cost.

The peer-to-peer value transmission of blockchain has subverted people’s understanding of Internet. The blockchain application has been extended to all fields in the economic society, among which it most accords with the financial field (payment, transaction, settlement, trade finance, digital currency, stock right, private placement, bond, financial derivative instrument, crowd-funding, credit and loan, risk control and credit investigation). In the future, blockchain will be applied in all aspects of society.

1.4 BitSilver Was Born at the Right Moment

At present, there have been several attempts to digitize silver based on blockchain and non-blockchain, yet no significant market size has been reached. Many digital silver is anchored in silver of unknown origin (not London Standard Silver Bars for Delivery) or even not necessarily backed by physical silver. Another major problem is how to determine the storage cost. Some stipulate that any exchange or wallet that holds user coins must pay a certain amount of custodial fees on a regular basis. Others force the currency to depreciate for payment. However, neither is optimal.

BitSilver was born at the right moment. It hopes to use a public blockchain to help global investors to make confirmation of the digital assets, so that the transaction ledgers are more open and credible. At the same time, it hopes to expand the liquidity of the partners and the depth of the transaction. Besides, it refunds the returns to individual investors from market-makers who take advantage of the spread between exchanges, provides the most humanized high-end services for global members, completely breaks the old ecology of the industry, and forms a new situation.





**BitSilver项目介绍**

**第二章**

Chapter II. Project Introduction of BitSilver

2.1 What is BitSilver？

The core value of blockchain is that it solves the trust issue by technical means and reaches a decentralized consensus. From the perspective of long-term human development, the birth of blockchain technology is not only an embodiment of human freedom consciousness, but also a general trend to promote the development of civilization through science and technology.

BitSilver is an independent public blockchain developed based on the underlying technology of Bitcoin, and all transactions are operated in accordance with the smart contract on the blockchain. Thanks to the smart contract, the system operates strictly as per procedures, thereby eliminating human errors. Moreover, BitSilver supports round-the-clock transaction, which facilitates settlement of various assets. Compared with the traditional silver, which is only settled during bank business hours, BitSilver’s can be circulated at any time and any place.

The public blockchain of BitSilver is a pint-to-point transmission currency system based on the SHA256 algorithm. It applies the Bitcoin-based asymmetric encryption technique and original sliver consensus mechanism to promote the technical, ecological and service development of the digital asset trading platform itself.

As a real-time, open and transparent transaction community in the world, BitSilver does not use a traditionally centralized corporate structure, without a CEO or board of directors. The transaction system of BitSilver can realize the financial-grade speediness and stability, making all transactions efficient and guaranteed.

2.2 Usage of BitSilver

BitSilver account holders may exchange BitSilver for USD or unregistered silver in the unregistered silver account, and vice versa.

For investors and active traders (whether retail or institutional) and market participants inside and outside the crypto asset ecosystem, BitSilver is a hugely attractive asset.

Bitcoin enthusiasts are also often attracted to silver because it shares many qualities with Bitcoin. Both are decentralized “external” assets, not held accountable by any other person or agency, nor bound to any particular government. Besides, both are rare in number and universally recognized across national borders. It is estimated that many Bitcoin holders and traders may be interested in holding and trading silver, and BitSilver will be a new asset that is easy to understand within a well-known ecosystem. BitSilver plans to go live on crypto asset exchanges around the world and will trade for the first time directly with Bitcoin and other crypto assets.

BitSilver is an attractive investment option for many people around the world who are interested in owning physical silver. It can achieve high quality silver registration and it is very convenient to obtain and use.

2.3 Vision of BitSilver

After BitSilver completely accords with sliver, it will build the ecological public blockchain of food, amusement, travel, shopping, medical treatment, finance, insurance, health, energy and so on required by human beings in the public blockchain ecology, so as to meet people’s all demands for life yearned for by them.

BitSilver is committed to providing global users with value flows and user experiences, building the most transparent, shared and democratic ecological transactions for users, solving the liquidity problem of digital assets and silvers, optimizing the allocation of social financial capital, improving the efficiency of asset allocation, and solving the financing needs of projects with industrial advantages. Meanwhile, it will provide a safe, fair and open transaction platform for global digital technology fans.





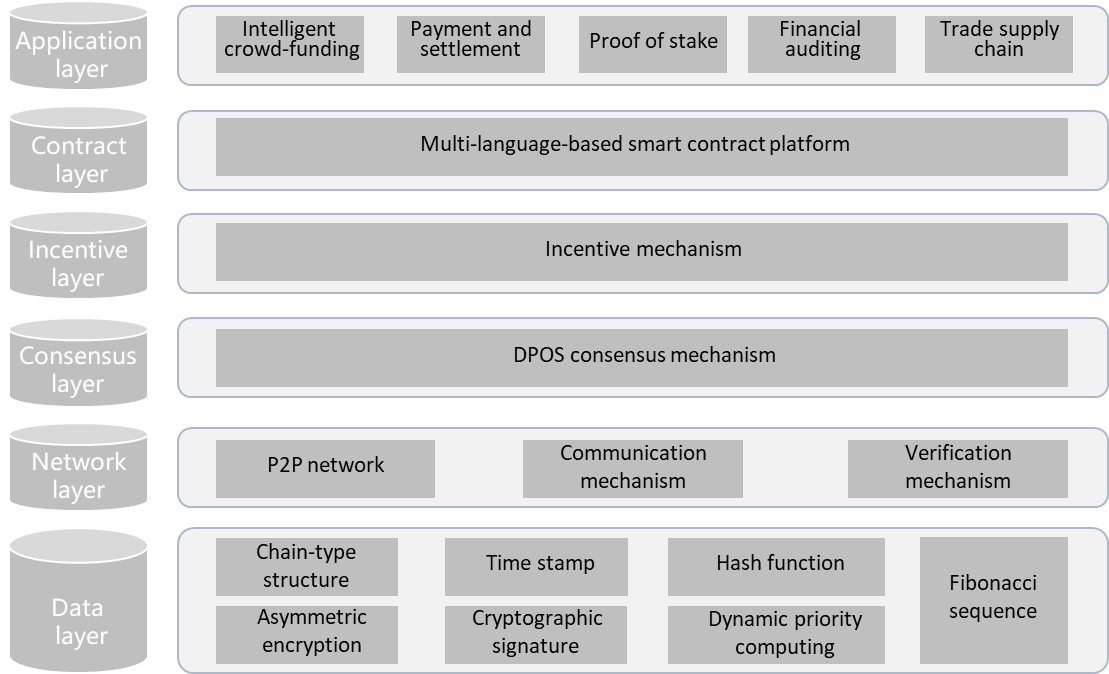
**BitSilver的技术创新体系**

**第三章**

Chapter III. Technology Innovation System of BitSilver

3.1 Top Technical Architecture of BitSilver

The top technical architecture of BitSilver consists of the data layer, network layer, consensus layer, incentive layer, contract layer and application layer, in a bottom-up order. Each layer can provide services for certain applications, meet the specific needs of different applications, and help users to quickly and safely realize the business application scenarios of all kinds.



3.1.1 Data Layer of BitSilver

Besides the standard chain-type structure of blockchain, Merkle tree, hash function, asymmetric encryption and time stamp, BitSilver also introduces other technologies to the data layer, such as dynamic priority computing, Fibonacci sequence, cryptographic signature and so on. The traditional blockchain-based data structure fails to take the expansibility into full consideration when it was designed, thus causing it unable to hold mass data. What’s worse, its structure was not flexible enough, thus making the on-chain data structure which is based on the current blockchain technology applicable to the circulation of digital currency only.

3.1.2 Network Layer of BitSilver

To improve the network’s carrying capacity and transaction processing speed, the network layer adopts the P2P networking mode. The P2P protocol supports the data transmission and signaling exchange between nodes of the blockchain network, and serves as an important communication guarantee for distributing data and reaching the consensus mechanism. In the system design, BitSilver can use protocols flexibly as the application scenarios require, and support a variety of P2P protocols. To achieve a high communication security, it flexibly supports the safe communication protocols such as HTTPS, TLS and so on.

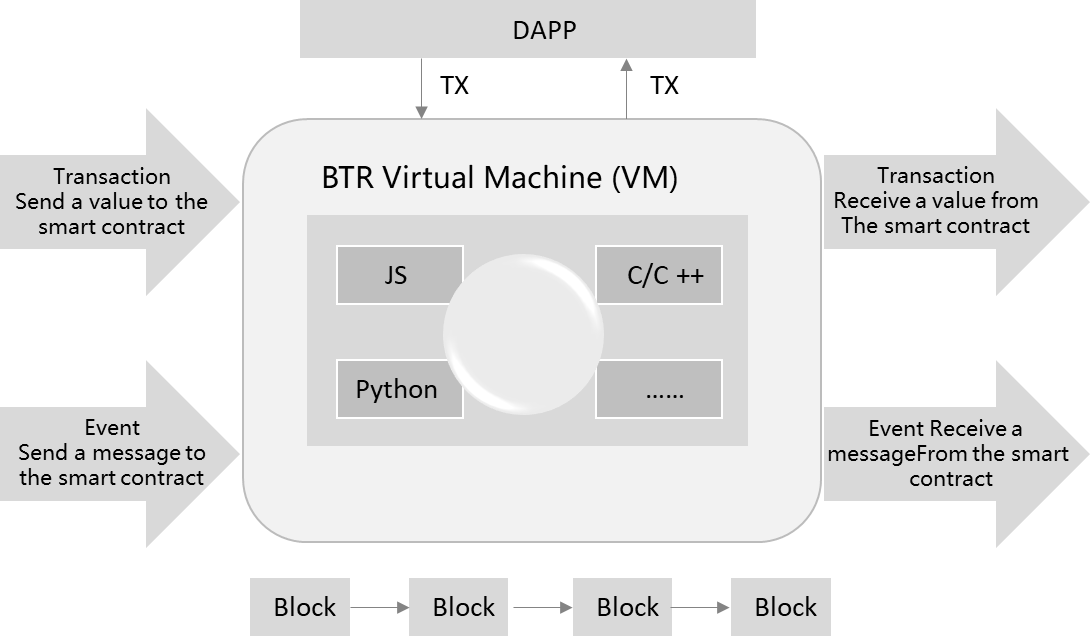
3.1.3 Consensus Layer of BitSilver

The consensus mechanism of BitSilver is based on DPOS, and also uses the client election system. In the later part of the algorithm, an optimized PBFT algorithm variant is used, which enables the loyal nodes to reach consensus at the message complexity of O(n^2) and at the time complexity of O(1), when t<n/3, and will not make them diverge. t represents the number of Byzantine nodes (the nodes which may have any act, such as network delay, downtime, malicious attack and so on), while n represents the number of all nodes.

3.1.4 Incentive Layer of BitSilver

Transaction is the basic operation on BitSilver, which results in the change of equity. BitSilver will be consumed in any transaction. Besides the return on assets, BitSilver also uses the bookkeeping contribution reward to give an incentive to the bookkeeping nodes. The bookkeeping contribution reward will become an equity basis for another bookkeeping. With the improvement of BitSilver technology and ecology, the value of BitSilver will keep increasing.

3.1.5 Contract Layer of BitSilver



BitSilver has designed a special BitSilverVM for itself to improve the computing performance, reduce the cost of contract development and optimize the memory allocation model. In the future, BitSilver will, based on VM, support a greater diversity of programming languages, and create a friendly development environment. Developers can use the high-level languages they like to program.

3.1.6 Application Layer of BitSilver

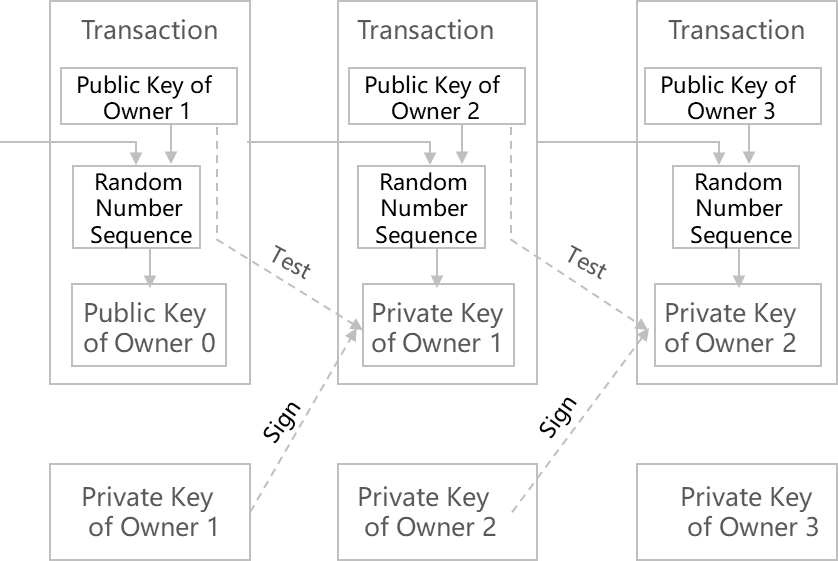
The DAPP ecology for end-users involves multiple tourism-related applications, such as BitSilver wallet, resource distribution, community and so on. The application layer of BitSilver will provide the service providers in the ecology with with the open data interface system. For different applications, BitSilver will provide special and general interfaces for the application layer to call directly.

BitSilver will establish the access system for relevant service providers, and build up the core application ecology. When the resource and energy ecology becomes sound, BitSilver will open the access conditions on the application layer of the public blockchain, and make BitSilver as the fuel for the access.

3.2 Underlying Technology of BitSilver

3.2.1 Transaction

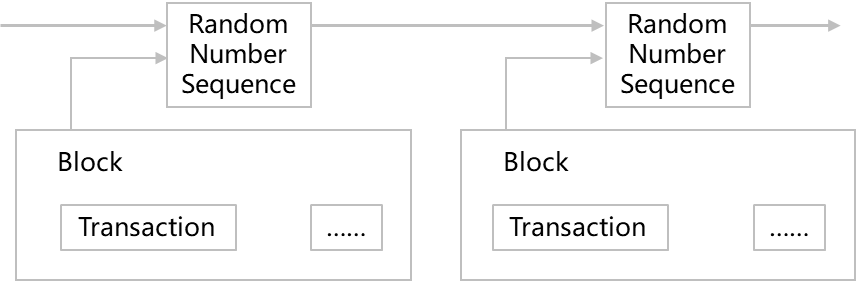
An electronic coin is defined as such a string of digital signatures: each owner signs a random hashed digital signature on the previous transaction and the public key of the next owner, and attaches this signature to the end of this electronic coin, so the electronic coin will be sent to the next owner. By verifying the signature, the payee can verify the owner of the chain.



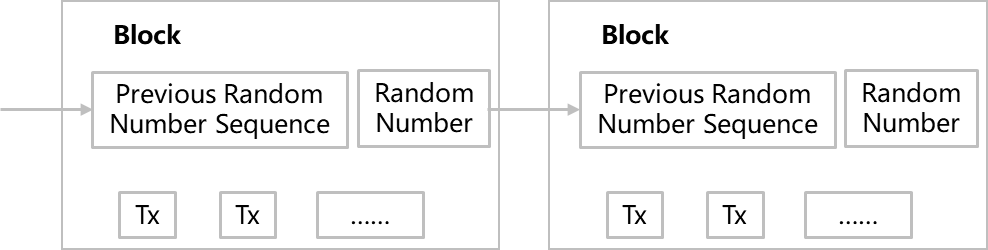
The problem of this process is that it will be difficult for payee to verify whether a previous owner has made double payment on the electronic token. The usual solution is to verify each transaction for the prevention of double payment by introducing a trusted third-party authority or a mechanism similar to the mint. At the end of each transaction, this electronic token will be collected by the mint, and a new electronic tokenmint will be issued by mint; only electronic tokens issued directly by the mint will bevalid, so the double payments can be prevented. However, the problem with this solution is that the fate of the entire currency system completely depends on the company that runs the mint, because every transaction must be verified by the mint, which is like a bank.

3.2.2 Time Stamp Server

This solution first proposes a “time stamp server”. The time stamp server adds a time stamp by randomly hashing a set of data in the form of a block, and broadcasts the random hash, just like posting on the news or the Usenet. Obviously, the time stamp can verify that certain data must exist at a certain time, because the corresponding random hash can only be obtained if it exists at that time. Each time stamp shall incorporate the previous time stamp into its random hash, and each subsequent time stamp reinforces the previous time stamp, thereby forming a chain.



3.2.3 PoW (Proof-of-Work)

In order to build a decentralized set of time stamp servers on a point-to-point basis, it is inadequate to work just like a newspaper or Usenet. We also need a hashcash similar to that proposed by Adam Back. In the random hashing, the PoW mechanism introduces the scanning of a specific value. For example, under the condition of SHA256, the random hash starts with one or more zeros. Then, as the number of zeros rises, the amount of work required to find this solution will increase exponentially, and testing the results requires only one random hashing.

3.2.4 Network

The steps to run the network are as follows:

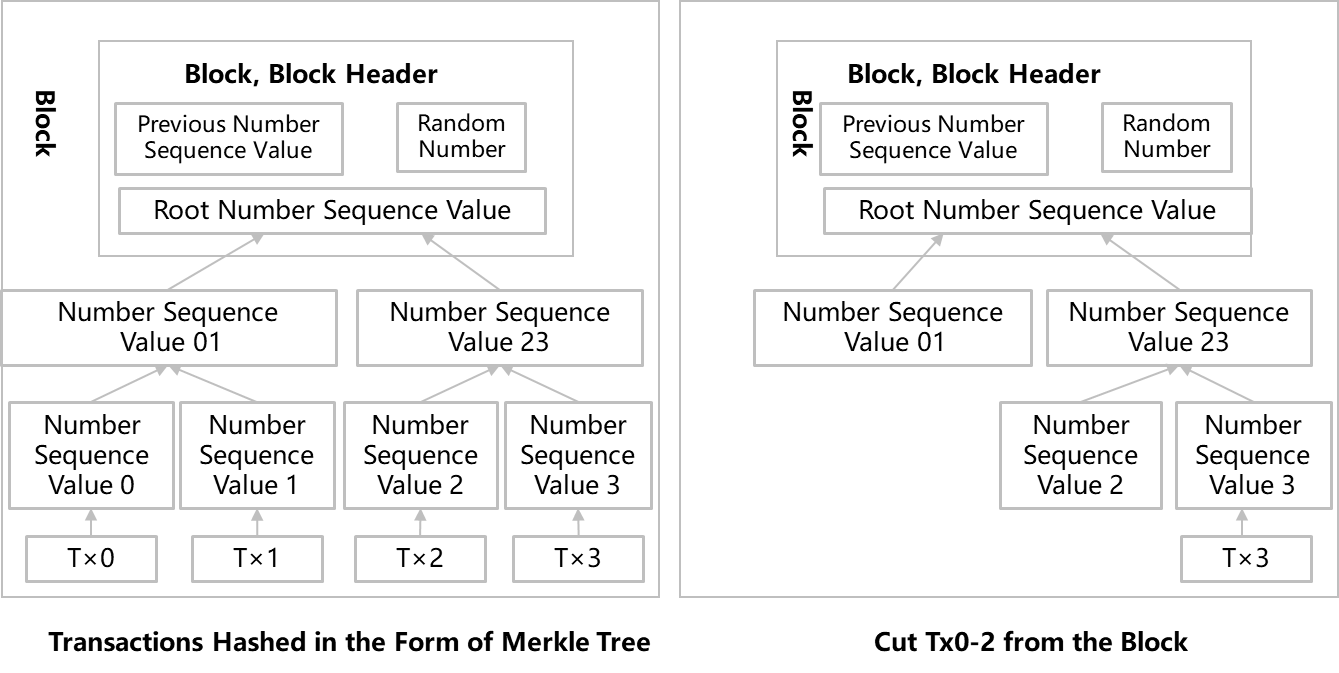
1. New transactions are broadcast to the entire network;
2. Each node incorporates the received transaction information into a block;
3. Each node tries to find a PoW with sufficient difficulty in its own block;
4. When a node finds a PoW, it broadcasts to the entire network;
5. Other nodes recognize the validity of the block if and only if all transactions contained in the block are valid and have not previously existed;
6. Other nodes indicate that they accept the block by following the end of the block and making a new block to extend the chain, and the random hash of the accepted block is deemed as the random hash that is faster than the new block.

3.2.5 Incentives

We agree as follows: the first transaction of each block is treated in a special manner, and the transaction generates a new electronic token owned by the creator of the block. In this way, the incentives for nodes to support the network have increased, thereby providing a way to distribute electronic token into circulation without central authorities issuing currency. This method of continuously adding a certain amount of new money to the monetary system is very similar to mining gold by consuming resources and injecting it into circulation.

3.2.6 Recycle of Hard-disc Space

If the most recent transaction has been incorporated into enough blocks, the data before the transaction can be discarded to recycle the hard disk space. In order to simultaneously ensure that the random hash of the block is not damaged, the transaction information is constructed as a Merkle tree when it is randomly hashed, so that only the root is incorporated in the random hash of the block. By stubbing the branch of the tree, the old block can be compressed. Besides, the internal random hash does not need to be saved.

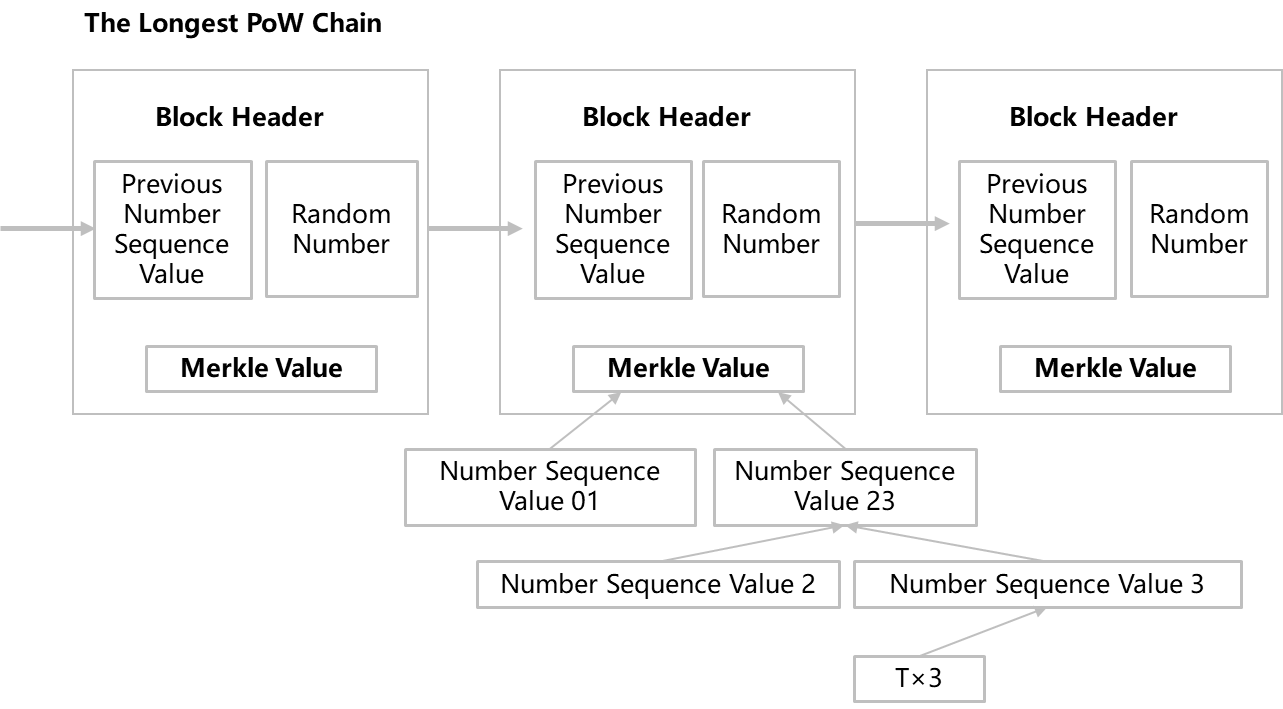


The size of the block header without transaction information is only 80 bytes. If the block generation rate is set to one per minute,the annual data bits generated are 42MB (80 bytes \* 60 \* 24 \* 365 = 42MB).

In 2019, the memory capacity of PC systems is usually 4GB. According to Moore’s Law, all the block headers can be easily stored in memory.

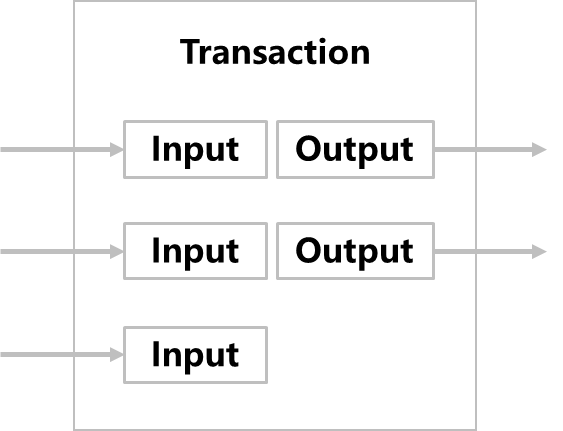
3.2.7 Simplified Payment Verification

It is possible to verify payments without running full network nodes. A user needs to retain the data of the longest PoW block header, so that it can keep asking the network until it is convinced that it has the longest data chain, and must pass the branch of merkle, lead to it and be incorporated into that transaction of the block after being time-stamped.



In this case, as long as the honest nodes control the network, the inspection mechanism is reliable. However, when the entire network is attacked with a dominant computing power, it will become more vulnerable, because network nodes can confirm the transactionvalidity by themselves. As long as the attacker can continue to keep the advantage of computing power, the simplified mechanism will be deceived by the attacker’s fabricated transactions.

One possible strategy is to issue the alert as soon as they find an invalid block, and users who receive the alerts will immediately start downloading the full information about the block or transaction being warned, thereby determining the informationinconsistency. For business organizations where large amounts of receipts and payments occur on a daily basis, they may still want to run their own complete nodes to maintain greater independent completeness and fast validation.

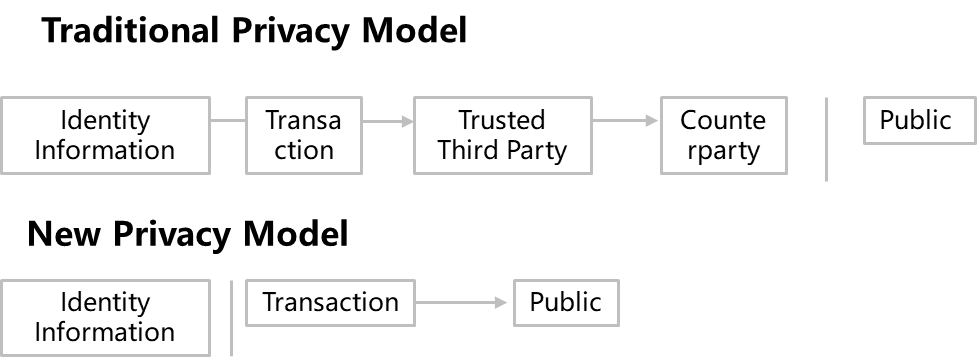


3.2.8 Combining and Splitting Value

Although electronic tokens can be processed individually, it would be clumsy to initiate a transaction for each electronic token separately. For the convenience of combining and splitting value, transactions are designed to incorporate multiple inputs and outputs.

Generally speaking, it is a single input consisting of a previous transaction with a larger value, or a parallel input consisting of several previous transactions with a lower value. However, there are two outputs at most: one for payment and the other for change. It should be noted that when a transaction depends on previous transactions, these transactions depend on multiple transactions. Nevertheless, this is not a problem, because this working mechanism does not require checking the history of all previous transactions.

3.2.9 Privacy

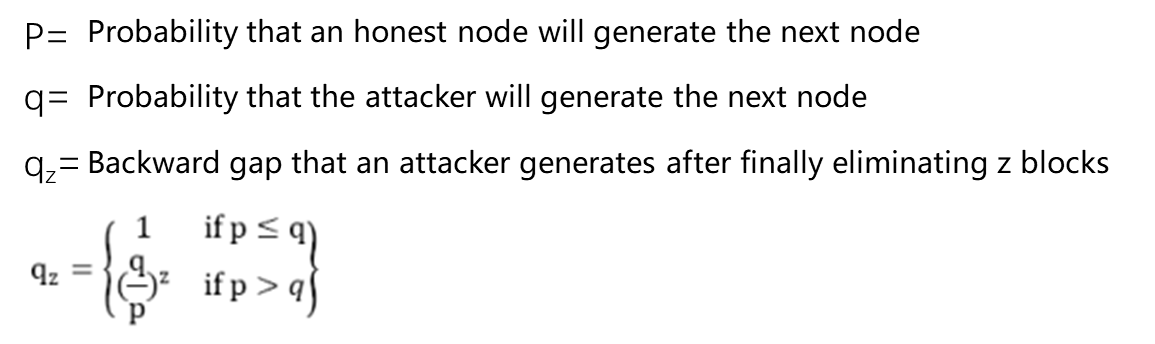


The traditional mint model provides a certain degree of privacy protection for transaction participants, because it attempts to obtain transaction information from trusted third parties are strictly restricted. If the transaction information is broadcast to the whole network, it means that the method fails. However, privacy can still be protected: keeping the public key anonymous. The only information available to the public is that one person has given a certain amount of money to another person, but it is difficult to associate the transaction with a specific person. In other words, it is difficult for the public to be sure who these people are. This is similar to the information released by the stock exchange. The timing and volume of stock transactions are recorded and available for inquiry, yet the identities of the parties are not disclosed.

3.2.10 Calculation

The contest between the honest chain and the attacker chain can be described by a random walk of the binary tree. A success event is defined as an honest chain that extends a block, giving it a lead of +1; a failed event is that the attacker’s chain is extended by a block, making the gap of -1.

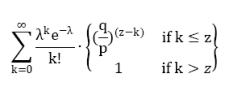
The probability that an attacker succeeds in filling a given deficit can be approximated as the bankruptcy of a gambler. Assuming that a gambler has unlimited overdraft credits and starts to gamble a potentially infinite number of gambles, in an attempt to fill the deficit. Then, the probability that he will fill the deficit can be calculated, i.e., the attacker will catch up with the honest chain, as follows:



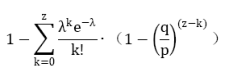
The payee generates a new pair of key combinations, and then reserves a short time to send the public key to the payer. Afterwards, the payee will wait for the transaction to appear in the first block, and then wait for z blocks are linked afterwards. At this point, he still doesn’t know exactly how many blocks the attackers have made. However, assuming that an honest block will consume the average expected time to generate a block, the potential progress of an attacker is a Poisson distribution, and the expected value of the distribution is:



In order to calculate the probability that the attacker will catch up, we multiply the probability density of the Poisson distribution of the number of blocks that the attacker will make progress by the probability that the attacker can still catch up with that number.



Convert to the following form for avoidance of summing infinite series:





**BitSilver经济模型**

**第四章**

Chapter IV. Economic Model of BitSilver

4.1 Introduction to BitSilver

BitSilver is the built-in and protogenetic encrypted digital token of BitSilver network, which can be used in transaction, settlement and smart contract performance on the chain. BitSilver can conveniently represent and measure the digitized economic activities in BitSilver network. Its value is based on the following two points. Firstly, a certain amount of BitSilver will be consumed as the fuel by the applications on the BitSilver chain. Secondly, BitSilver holders can participate in the governance of XKB blockchain communities.

As the key link to maintain the operation of BitSilver ecosystem, BitSilver guarantees the successful establishment of the ecosphere closed-cycle, and functions to circulate value, buy services, get returns and encourage interaction. It can be applied in many scenarios within BitSilver and under the BitSilver Ecosystem, and will be applied in all ecological chain projects on the BitSilver platform in the future.

BitSilver is a proof of equity for the BitSilver transaction platform itself. It will positively inspire community members such as platforms, miners and users and help BitSilver to achieve ecological health.

4.2 Property of BitSilver

|  |  |
| --- | --- |
| Full name of token | BitSilver |
| Total quantity | 1050000000 |
| Pre-mining | 80000000 |
| Pre-mining Use | Ecological construction |
| Mining Method | POW |
| Mining Algorithm | SHA256 |
| Block Interval Time | 60s |
| Block Size | ≤1MB |
| Initial Single Block Output | 1BitSilver |
| Reduction Cycle | 1000000000 Block |
| Date of Issuance | 2020/04 |
| Incentive Mechanism | POW |
| Arrival Time | 6 Block |
| Initial Conversion Ratio | 1BTC=6326BitSilver |

4.3 Decentralized Self-governed Community

As a product inthe new era of Internet technology, the blockchain technology has immeasurable commercial value in the future. In order to accelerate the landing of the blockchain industry and make the blockchain technology better serve the human society, we have launched a new digital asset project targeting the global silver market - BitSilver.

The BitSilver project is an open-source project. Its developers come from different countries around the world, and its members have been responsible for multiple iterative development and fork upgrades of the Bitcoin version.

While technology is a power, goodness is a choice. Upholding the tenet of technology towards goodness, the team strives to build a new blockchain technology platform that truly serves people and society.

