



Baldi Network

open Web3.0 transport network

Let global users enjoy borderless, efficient safety system

Ver. 1.0

Imaging, no country.....

For people who trust the completely dispersed financial system but not
rely on currency issued by government.

Abstract

On January 3, 2009, Bitcoin started to establish a dispersed financial system without currency supported by government. Today the market value of the system exceeds 11.5 dollars. It more likes digital gold reserve, rather than currency used for transaction media and financial account. The exchange rate fluctuation between the cryptocurrency from virtual world and value from physical world makes it harder to establish a healthy blockchain economy. The objective of Baldi protocol is to achieve the mission of Bitcoin, and create a borderless financial infrastructure, so as to realize the development of cryptocurrency economy. It is a completely dispersed and unlimited public chain, while USUS is a stable cryptocurrency on the chain, which provides relatively stable currency reference for value in physical world. USUS uses production costs and miner's arbitrage behaviors in as key feedback on establishing market long-term balance price in PoB system. Such balance price basically fixes the accounting unit in metering system in global electricity price, of which the actual value is more stable than any legal tender. Baldi eliminates the burden of dApp developers, pricing their commodities or services based on the exchange price out of the chain, which is not difficult to be correctly implemented but makes customers confused. The protocol of Baldi aims at laying foundation for stable cryptocurrency reference, paving the way for more complex financial services and correct establishment of tools such as loans, insurance, options, and derivative instruments.

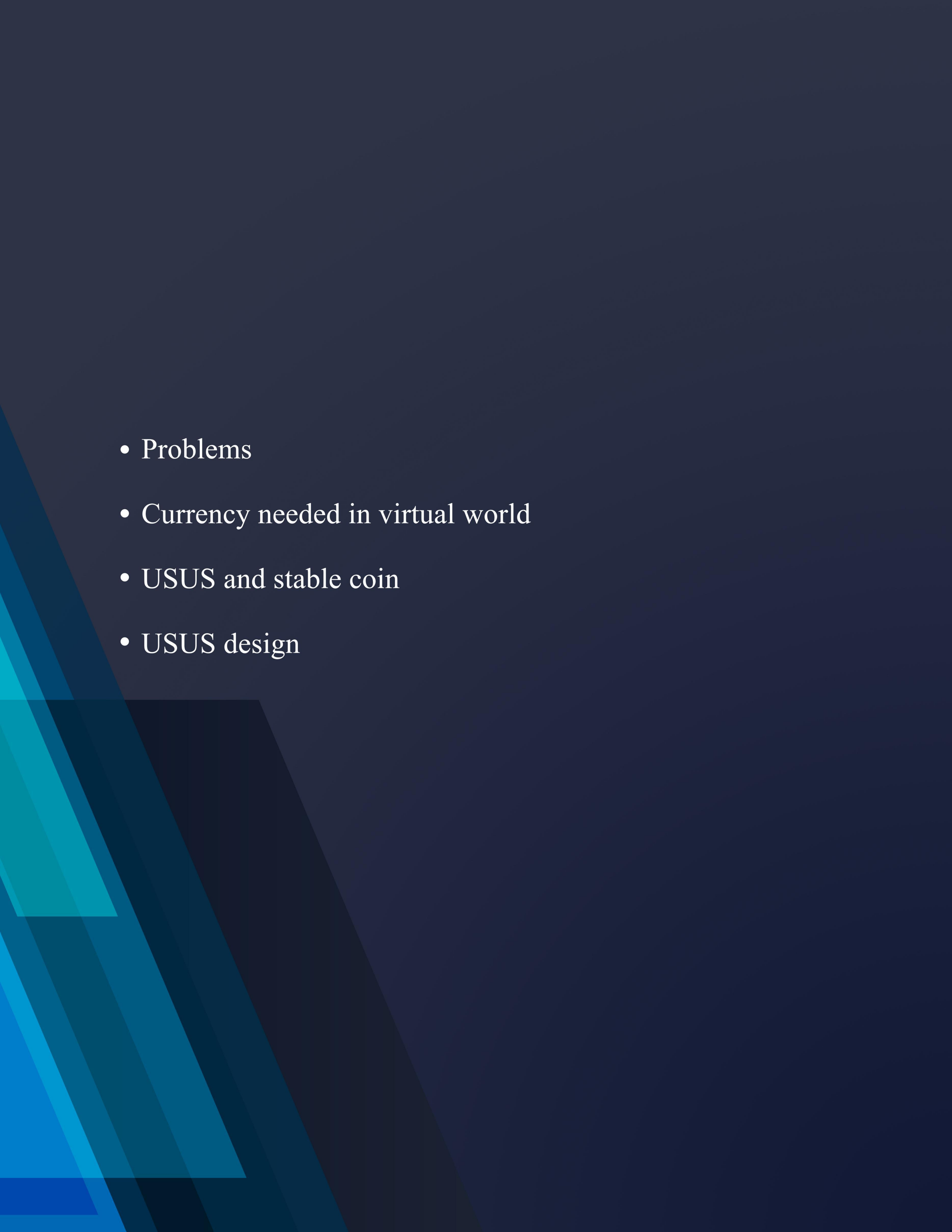
USUS is not related to USD or any other legal tender issued by sovereign state. On the contrary, it is established on the self economy and working certification interaction of it with physical world.

USUS does not compete with Ethereum or other public blockchains, although it is compatible with existing Ethereum dApp and can be used as side chain of most of public chains. Developers can interact with Baldi via Baldi's cross chain adapter and SDK and take Baldi as its reference for dApps local public chain. Each public chain has its own consensus and expansion and implements its own incentive plan, while Baldi focuses on appropriate currency policy, inter-chain communication and value settlement.

Table of contents

1. Problems.....	6
2. Currency needed in virtual world	7
2.1. New socioeconomic structure in virtual world	7
2.2. Functions of currency	7
2.2.1. Account unit	7
2.2.2. Exchange media	8
2.2.3. Store value	8
2.3. Bitcoin is not a currency in virtual world	9
2.4. Decentralization and no trust	9
3. USUS and stable coin	10
3.1. Introduction to USUS.....	10
3.2. Existing stable coin proposals and problems	10
3.3. Impossible trinity and insisting similartiy of basic economic principles.....	11
3.4 Summary.....	12
4. USUS design.....	14
4.1. USUS design priciple	14
4.1.1. Computing power links physical world and virtual world.....	14
4.1.2. Tracking Bitcoin market price using marginal production cost.....	14
4.2. Stable cryptocurrency with long-term equilibrium.....	17
4.3 Government	18
4.4 Proof of Value Consensus for Immediate Termination	19
4.4.1 Proof of Value Consensus Agreement in Guokr.....	19
4.4.2 Comparision of Value Consensus Evidence with PoW and PoS Consensus	22
4.4.3 USUS token.....	23
4.4.4 Governance Token	25
4.5 Monetary Policy	25
4.5.1 Secondary Price and Fluctuations and Block Awards	25
4.5.2 Large volatility and monetary policy intervention	26
4.6 Guidance USUS system.....	28
4.7 Cross chain architecture of Baldi protocol	28
4.8 Launching USUSwill power Ethereum	29

5. Participate in Baldi.....	31
5.1 Verifier.....	31
6. Design overview.....	33
6.1 Consensus.....	33
6.2 Proof pet.....	33
6.3 baldichains and Collators.....	34
6.4 Inter-chain communication.....	35
6.5 Baldi and Ethereum.....	36
6.6 From Baldi to Ethereum.....	36
6.7 From Ethereum to Baldi.....	38
6.8 Baldi and Bitcoin.....	39
7.Conclusions.....	40
8.Risks	40
8.1 Uncertainty of laws and regulations and enforcement actions.....	40
8.2 Inadequate disclosure of information.....	41
8.3 Failure to develop.....	41
8.4 Security hole.....	41
8.5 Other risks.....	41
9. Reference.....	42

- 
- Problems
 - Currency needed in virtual world
 - USUS and stable coin
 - USUS design

1. Problems

After talking with hundreds of developers who are working on ICO project and blockchain products dispersed application (“dApp”), Baldi team found their dApp lacking of the key requirements to success: value dApp established by a stable account unit representative and used by users during the interaction between virtual world of cryptocurrency and physical world of legal tender. Due to the exchange rate fluctuation between cryptocurrency and legal tender, people are unlikely to use the cryptocurrency in transaction other than speculation related activities.

For example, for a landlord who wants to rent a room at 0.1 Ether per night using dApp, which provides similar Airbnb services, the landlord cannot know its value reliably. He obtained 0.1 Ether through calculation by legal tender to judge whether there is any profit through renting the room. The room is worth \$100 per night when full. Travelers may need to pay \$70 to book the room and pay \$140 later. The exchange rate fluctuation puts buyers and sellers at great risk as their costs and incomes are most likely to be priced in legal tender. In addition, please note that this landlord may also compete with other landlords who rent rooms but charge by legal tender. Our landlord will find it more difficult to attract renters, as renters and buyers face the same accounting unit problem that the landlord faces. This problem existing in dApp to connect to physical world can be further confirmed by referring DAPs that have achieved certain commercial success. Some dApp (such as Crypto Kitties) have succeeded by locating cryptocurrency users and restricting user activities in virtual world, without connecting to physical world and exchanging cryptocurrency for or from legal tender.

In order to establish a strong blockchain economy, it needs a public blockchain with local stable cryptocurrency, the blockchain can provide the account units representing the existing value of all dApp in physical world. Converting cryptocurrency into legal tender, vice versa, this is actually an international financial problem on legal tender in physical world economy and cryptocurrency in virtual world.

2. Currency needed in virtual world

2.1. New socioeconomic structure in virtual world

Many of our existing socio-economic structures in physical world are affected by the limitation of working within geographical boundaries, which are being broken with the development of Internet and longer online time of people in virtual world. People in virtual world group themselves into scattered communities according to their common values naturally and believe that the need and acceptance of central governments are weakening. This trend will continue. Blockchain technology is a decentralized economic and governance system elaborately designed, which is suitable for virtual world and can meet the needs of these people with its consensus solution, which provides a contract and settlement system without default risk. The technology forms economic consensus by using the principle of game theory and based on the natural tendency of human beings to take actions for their own interests. New socio-economic structure and financial system in virtual world are being developed. Cryptocurrency and ICO are the initial components of the breakthrough transformation that is going on.

2.2. Functions of currency

In virtual world, existing blockchain economy lacks a cryptocurrency as a real currency. Currency should perform three main functions, namely:

1. Account unit
2. Exchange media
3. Store value

2.2.1. Account unit

As a unit, currency provides a common value measure standard for commodities and services exchanged. Almost all cryptocurrencies have the capability of fixed supply or expanding supply with limited deflation models. This restriction prevents the cryptocurrencies from expanding with the GDP growth of blockchain economy.

For example, Bitcoin is generally compared with gold as they are in limited supply and have same higher perceptive value. However, inspection on golden-based (or silver-based) financial system shows that, when basic economy expands rapidly but the gold cannot expand with it, these systems will crash. Value of Gold and Bitcoin will be improved due to their limited supply, this is exactly why they cannot provide motives for economy.

Deflated money will eventually hinder production and fundamentally damage the economy. For example, supposing you are a baker living in a world of super deflation. You buy food containing money during the day, bake cakes at night, and plan to sell cakes the next day. The next day, you find that the market price of the cake is lower than the cost you pay for the ingredients, your plan for making profits from your labor is hindered. You realize that, you'd better not do anything but stick to your currency. If someone wants to create a stable cryptocurrency to provide power for the entire blockchain economy, including hundreds of blockchains, thousands of cryptocurrencies and millions of dApp products and services, then the currency choosed should not be in limited supply and in deflation.

2.2.2. Exchange media

As a medium of exchange, currency enables buyers and sellers to make wise trading decisions, especially between different products or services; buyers and sellers are not limited to barter trade in goods or services they want. The performance and scalability of most popular cryptocurrency are too limited to serve as an exchange medium for the entire blockchain economy. Popular dApp or major ICO may weaken blockchain, just as Ethernet networks have experienced many times. Related to this, the scalability of the main existing cryptocurrency is further limited by its increased transaction costs. As a cryptocurrency, the market price rises, the activity level increases, and then higher transaction costs are incurred. This phenomenon happened in both Bitcoin and ethernet.

2.2.3. Store value

As a kind of value storage, currency can ensure its set value over time.

The concept of values comes from physical world, which is based on two competing schools of thought among economists. Labor theory holds that the value of commodities depends on the cost of producing commodities, while subjective theory holds that the value of a commodity comes from our belief in the usefulness of a commodity for a specific purpose at a specific point in time. Baldi's team believes that the two theories complement each other and are necessary to understand how people view value: the production cost of labor theory must be considered, especially in the analysis of opportunity cost. At the same time, subjective theory should be used to consider people who use commodities, so as to form opinions on the usefulness of commodities.

In order to create a stable cryptocurrency, the value in virtual world is more subjective than in physical world, because virtual world defines the value according to the perceived utility of individual users. For example, the value of virtual commodities such as Crypto Kitties varies

greatly to different buyers and sellers. There is no standard fixed price. Therefore, in order to have a set value that a large group rather than an individual can agree on, it is necessary to contact physical world to take advantage of the set value. For this reason, most of the existing cryptocurrency stable coins are linked to the dollar of physical world to establish a standard for their value.

2.3. Bitcoin is not a currency in virtual world

Due to various reasons, Bitcoin has cast a huge shadow in the cryptocurrency world, although it generally symbolizes encrypted currency, it cannot fully perform all three functions of currency. It is a valuable storage, but it cannot function well as an account unit and exchange medium.

At the beginning, there was no perceived value of Bitcoin except for the common ideology of paying the consensus cost of transactions in the Bitcoin system. Limitation of the total supply of Bitcoin, and the global instability and long-term central bank easing policies, consolidated its position as a representative of the perceived value and almost indestructible value of gold of Bitcoin. The price of Bitcoin boosted since then.

However, regardless of its inefficient performance, the price of Bitcoin is several orders of magnitude higher than Satoshi Nakamoto imagined, so that the original design is no longer applicable. Bitcoin is designed as a single-lane highway with a fixed amount of transaction throughput. With more and more miners adding more mining hardware to earn Bitcoin, the cost of reaching a consensus has greatly increased. In order to maintain the initial design framework of Bitcoin, the price of Bitcoin must continue to rise sharply or the transaction fee must rise to compensate for the increased production costs experienced by miners. About two years later, when the next Bitcoin mining award is halved, the transaction fee may reach several hundred dollars. This situation will worsen each time the mining incentive is halved again. Bitcoin has never been designed as a stable cryptocurrency. Its price fluctuation, inefficient performance and limited supply prevent it from becoming the currency of the blockchain economy.

2.4. Decentralization and no trust

In addition to the three traditional functions of currency, the stable cryptocurrency, as the economic foundation of the future cryptocurrency, must also be decentralized and untrusted. Although Bitcoin has defects in its operation as a currency, it is good at eliminating the need to trust third parties. It eliminates counterparty risks through decentralized consensus design. For example, in

the real world, people believe the US government has issued US dollars. People must also believe that the U.S. government will not abuse its power, extend credit excessively, and is usually a good steward of U.S. dollar monetary policy. This is not the case. Other governments and their decrees have also encountered problems. Bitcoin introduced the concepts of decentralization and no trust consensus through algorithms and game theory as a substitute for having to trust a third party. The future stable cryptocurrency should also be decentralized and trustworthy to adapt to the spirit of the blockchain community.

3. USUS and stable coin

3.1. Introduction to USUS

USUS is a stable encrypted virtual currency, which plays a role in all three abilities of currency, especially as an account and exchange medium. Baldi creates a stable value reference for cryptocurrency world by linking values from physical world. It is based on the same principles of decentralization, powerlessness and autonomy as Bitcoin and Ethereum, but the money supply is intended to expand automatically or contract with changes in the underlying economy, such as fluctuations in the number of dApp and their use. In the long run, the value of USUS is neither deflation nor inflation. The Baldi team also plans to use a variety of extensions in the USUS protocol, which will allow the main dApp to extend independently without causing transaction congestion on the Baldi chain.

3.2. Existing stable coin proposals and problems

There are already several stable coins in cryptocurrency market or pre-release stage, including Tether, MakerDAO, Basecoin, Fragment and others. None of these stable coins has token economy, except for being used as an account unit for cryptocurrency exchange (i.e., speculation to promote its stable coins). Some of these stable coins need collateral to stabilize their prices, and most of them are centralized. Without a thorough examination of each stable coin, the following sections highlight some of the main features and weaknesses of the existing stable coins.

Stable coins backed by collateral such as MakerDAO may be scattered, but users are required to provide more collateral (e.g. in Ethereum) instead of obtaining it from the value of the received stable coins. Excessive collateral reduces volatility, but users may think twice about why they provide more collateral than they do in stable coins. In addition, these stable coins have the potential fluctuation risk of their subsidiary cryptocurrency, which may lead to a black swan event

in which the user suffers liquidation and loses the stable coins and cryptocurrency that they provide as collateral.

Other stable coins are based on IOU and centralized. Tether is one such example. Users must bear the risks of counterparties and believe that these stable coins are actually supported by legal tender in a 1: 1 manner because the issuing company believes that. If there are trillions of dollars in equity, it is unrealistic to assume the risks of counterparties and believe that the reserves of companies such as Tether Limited (the company that created Tether) are equal to the number of IOU-based stable coins in the market. Moreover, these stable coins usually prevent the free flow of capital (see below).

Another stable group of coins follows the seigniorage stock model. They expand and contract the supply of coins through algorithms, just as the central bank does to legal tender. These stable coins are not collateral, but they are said to retain some value. Basecoin and Fragment are examples that follow this model. These stable coins issue bonds to stabilize and raise prices by removing stable coins from the market. They can buy back bonds freely to reduce prices. Since bond traders have an incentive to wait for prices to fall, these bond issues can easily lower prices. However, as prices fall, the number of stable coins removed decreases in inverse proportion, which has a cascading effect, making it more difficult to remove stable coins from the market for each bond price to fall.

3.3. Impossible trinity and insisting similarity of basic economic principles

To this exchange rate, in which different economies are in the physical world, the transition between stable cryptocurrency and legal tender is an international financial problem between the two economies: virtual world and physical world.

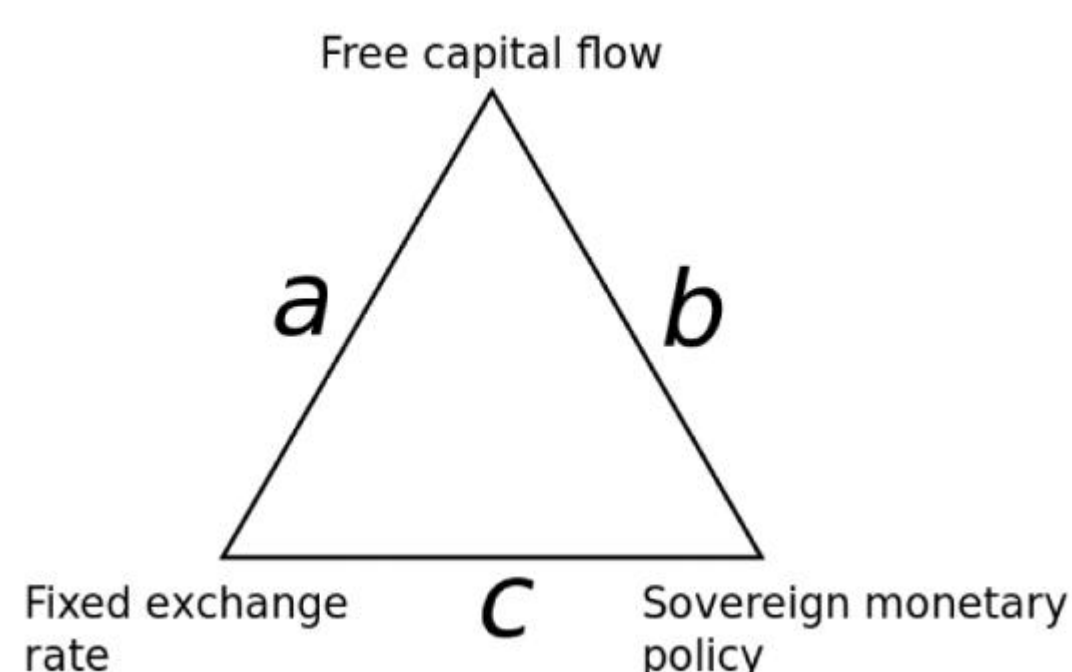
Therefore, Baldi's team believes that in order for a stable cryptocurrency to succeed, it must abide by the Impossible Trinity. In other words, the team does not believe that the basic economic principles can be ignored in creating a stable cryptocurrency mechanism.

Apart from the shortcomings of the existing stable coins and Tether, all the existing stable coins ignore the important theory of international finance, that is, the impossible trinity. The impossible trinity shows that a monetary policy can only achieve two of the following three economic goals at the same time, and it is impossible to achieve these three goals at the same time:

- Free Flow of Capital: Trade and Investment in and Out of Capital
- Fixed exchange rate: where is the currency value another currency that is fixed against the value

- Independent monetary policy: Monetary authorities independently control the supply of relevant currencies.

Existing stable coins are linked to legal bidders such as US dollars. A pegged exchange rate achieves a fixed exchange rate, but these stable coins also claim to provide free flow of funds and maintain an independent monetary policy. These existing stable coins believe that their coins can realize all three economic pillars that cannot be integrated into one at the same time. This is exactly the fundamental mistake that may actually exist in the field of international finance.



Tether is an exception that violates the "impossible trinity" because it explicitly abandons independent monetary policies, claiming that the ratio of Tether to US dollar reserves is 1: 1. It also restricts the free flow of capital. If Tether Limited received US\$ 100 million in the past, the selling of Bitcoin prompted Bitcoin sellers to convert US\$ 200 million worth of Bitcoin into Tether, and the link between Tether and US dollars will break through immediately. This is why Tether Limited restricts the conversion between Tether and US dollars.

For example, shrink or expand the money supply by issuing bonds.

Fig. 1: impossible trinity shows that it is impossible to achieve only one side of the triangle of two of the three possible monetary policy objectives at any given time and to successfully implement all three policies at the same time.

3.4 Summary

To sum up, the Baldi team has examined that how a stable cryptocurrency perform three functions of currency. As part of the value function storage, stable cryptocurrency must transparently connect to physical world. In addition, stable cryptocurrency must be decentralized and untrusted when using Bitcoin protocol. Finally, a stable cryptocurrency should not go against basic economic principles, such as the "impossible trinity", and will not take risks in the cryptocurrency community or interact with physical world.

According to these standards, the USUS team obtained a conclusion that, the existing stable coins

do not meet the specified requirements and USUS protocol is designed to meet all these requirements.

As for the three functions of money, Baldi has an unlimited supply, neither deflation nor inflation. Its relatively stable price design helps it meet the needs of account units, and also stores value functions. Its infrastructure supporting multiple blockchain makes it a medium of high throughput and efficient transaction time. Baldi uses a verified consensus to verify the main chain, which is dispersed among the miners and performs workload proof calculation. Therefore, USUS users can avoid taking risks of counterparties and do not need to trust a third party to operate USUS blockchain. Finally, since Baldi is not linked to a legal bidder, such as the US dollar, it can still provide free flow of funds and run independent monetary policies without violating the impossible trinity.

USUS does not fix the legal bidder of physical world. as mentioned above, the market price of USUS should be linked with physical world. The data generated by our physical world workload proof model is crucial for determining the market price and value of USUS, building community trust and realizing virtual world.

Start building a strong cryptocurrency ecosystem. In the next section, section 4, the analysis of USUS design is explained starting from the design principle behind USUS.

4. USUS design

4.1. USUS design principles

4.1.1. Computing power links physical world and virtual world

Baldi team understands the current blockchain pattern and the need for stable cryptocurrency for interaction between physics and virtual world. Physical world uses legal tender, and virtual world should have a stable cryptocurrency to which thousands of other cryptocurrencies are linked. Physical world exports computing power to virtual world to maintain blockchain's consensus on this stable cryptocurrency. Virtual world in return exports virtual goods and services to physical world. Virtual world must have a healthy internal consumption rate (i.e. its own domestic economy) so that its stable cryptocurrency can resist large fluctuations in export demand (in the bear market or bull market of virtual world, price changes will gradually disappear). Therefore, computing power provides a key link between physics and virtual world, and the miners who make computing power work are businessmen and traders between the two worlds.

4.1.2. Tracking Bitcoin market price using marginal production cost

In workload certification systems such as Bitcoin and Ethereum, computing power is performed through a "mining" process, where the cost of computing power is paid by legal bidder and revenue is collected by cryptocurrency. The process and technical review of Bitcoin mining have been described in depth elsewhere (e.g Kroll et al. 2013; Sapirshtein et al. 2016; Nakamoto 2008) . Mining costs can be divided into fixed costs of semiconductors and variable costs of energy consumption. Semiconductor factors also affect the energy efficiency of mining, in terms of GigaHash/Second/Watt. In terms of revenue, mining is driven by block incentives and other related transaction costs. As a mining pool, each miner is competing to be the first miner to solve the encryption problem for a specific block independently or cooperatively. The first miner to solve the problem received the block award and put the block on the blockchain. The motivation to win rewards when competing with other miners to solve difficult problems makes mining a highly competitive activity.

The competition of mining drives the activity to equilibrium. Based on microeconomics theory, the equilibrium state in this competitive mining scenario should be:

The revenue from combustion production should be equal to the relative proportion of the gas cost of its combustion energy, and should also be equal to the sales price (also known as the competitive price). Competition will drive miners, like self-interested actors, to reach a state of equilibrium and produce competitive prices, otherwise it will be market prices. In the following analysis, historical data will be used to determine whether the average marginal production cost of miners is a strongly correlated representation of market prices.

Electricity cost constitutes a major part of miners' marginal cost. If the global average electricity price is estimated at 0.135 USD per kilowatt-hour, the prices of Bitcoin and Ethereum should be related to their respective electricity consumption rates. Assuming that the energy efficiency of mining equipment is relatively stable, energy consumption can be replaced from the hash rate of blockchain network. Therefore, the network hash rate represents energy consumption, which should be close to the marginal cost and competitive price of mining. The following Bitcoin and Ethereum market price charts show the correlation with their respective network hash rates:



Fig. 2: the graph of Bitcoin and Ethereum prices and network hash rates shows that the network hash rates of bitcoin and Ethereum are related to their respective market prices, supporting the assumption that the energy consumption represented by the network hash rates is approximately close to the marginal cost, and therefore competitive prices.

A rigorous study using Bitcoin network data (Hayes 2016,2017) shows that if the energy costs of mining and daily mining production are first calculated, the marginal cost of Bitcoin production can be estimated. The energy cost of mining can be expressed as:

$$E_{day} = \left(\frac{\rho}{1000}\right) \left(\frac{\$}{kWh}\right) \cdot W_{per} \cdot GH/s \cdot hr_{day}$$

Gas is my daily energy cost, hash power (GH/s) used by pis miners.

\$/kWh is the dollar price per kilowatt hour, Wper GH/s is the energy efficiency of hardware, and hr days are the hours of the day. The following equation calculates the daily Bitcoin production:

BTC/Day is the expected level of Bitcoin production per day, /J is the block reward (currently at 12.5

BTC/block), Tx is the average transaction fee/block, and p is the hash power used by miners.

8 is the difficulty defined in Bitcoin (expressed in GR/block units). Constant sechris is the number of seconds in an hour and hr day is the number of hours in a day. In order to maintain a relatively constant blocking time, 8 must be expanded together with the total hash power in the Bitcoin network.

After calculating the daily energy cost of mines and the amount of Bitcoin mined per day, the competitive price of Bitcoin can be represented as follows:

$$P = \frac{E_{day}}{BTC/Day}$$

P =competitive price

- Eday = daily energy cost for mining
- BTC / Day = daily energy cost for mining

After adjusting the network energy efficiency according to the different efficiency levels of each generation of mining hardware and its deployment date, Hayes 2017 compares the competitive price result of the above formula with the actual market price of Bitcoin, and obtains the following chart:

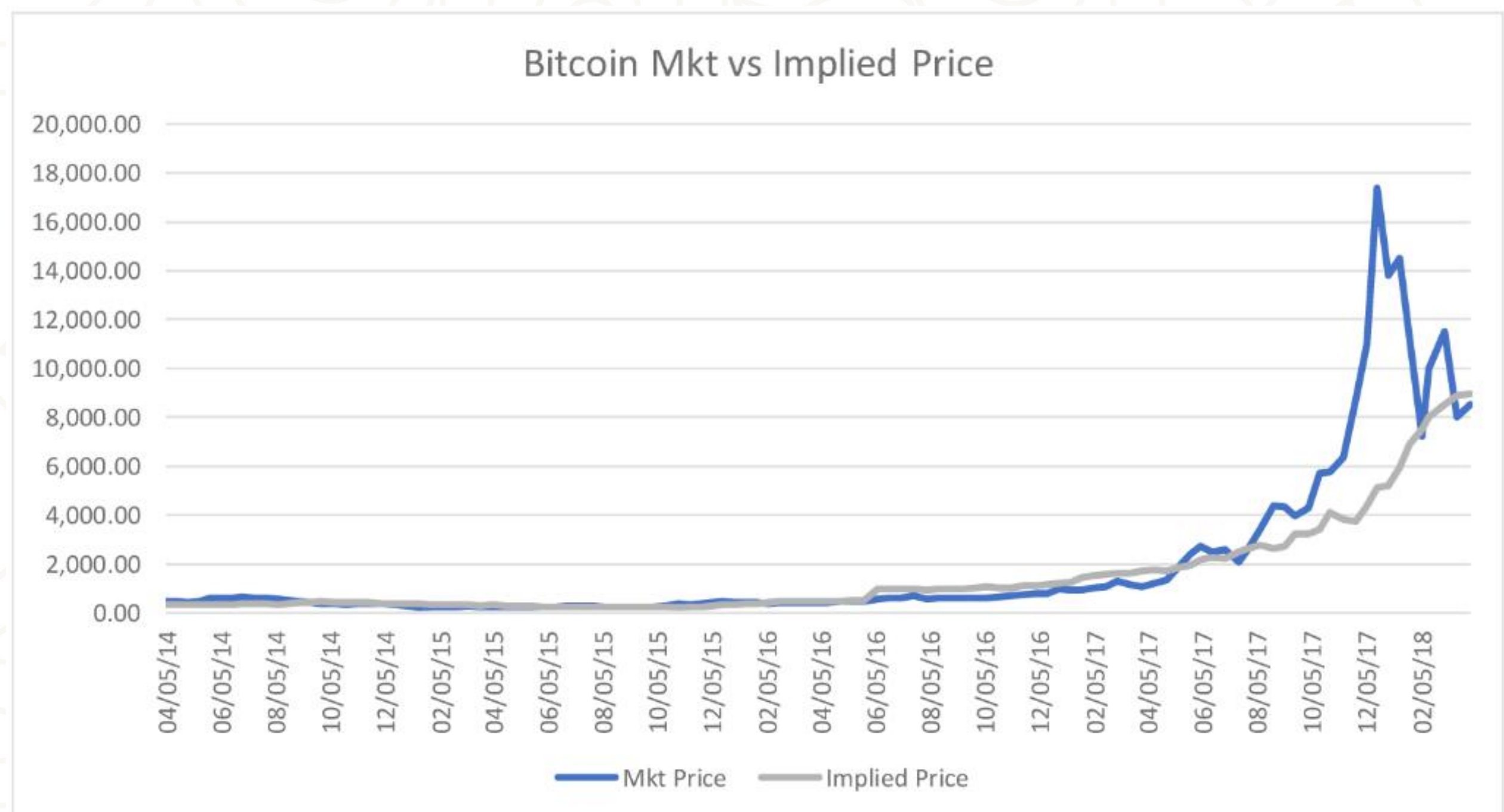


Fig. 3: the implied price of energy consumed by Bitcoin mining (i.e. competitive price) is strongly related to the actual market price of Bitcoin in Hayes research.

Ordinary least squares regression shows that $r = 84.5\%$, which means that nearly 85% of the market price of Bitcoin can be predicted by competitive price formula (itself is seriously affected by the production cost of Bitcoin).

4.2. Stable cryptocurrency with long-term equilibrium

Facts show that the competitive price of Bitcoin can be calculated by calculating the marginal cost of mining, which is closely related to its actual market price. The design of Baldi agreement is similar. As cryptocurrency based on workload proof, except that the marginal cost of mining should be stable, which will tend to stable competitive prices.

With the release of better mining hardware, energy efficiency has been improved, and corresponding adjustments will be made to solve these improvements. In addition, in a relatively long period of time, the marginal cost can be represented by the total hash rate and throughput of the network. If the generation of cryptocurrency is proportional to the hash rate of the network, the competitive price of cryptocurrency should be relatively stable. Miners are profit-driven, so if they watch Baldi's price rise, they will dig up more computing power for Baldi. If Baldi's price falls, their profits will shrink and miners may transfer their computing power to other cryptocurrency. In both cases, the invisible hand of the market will keep the price of rice stable, regardless of whether miners increase or stop adding rice to the market, thus causing prices to fall or increase respectively. Basically, such a plan fixes the production cost of each USUS on the global competitive electricity price. The following figure shows the industrial electricity price in the United States, which is one of the lowest in the world in the past 50 years. Nominal prices (in US cents) have increased nearly five times, while real prices (inflation adjusted according to current US dollar purchasing power) remain basically unchanged. In terms of comparable purchasing power, electricity prices are more stable than any legal bidder in the world in the long run.

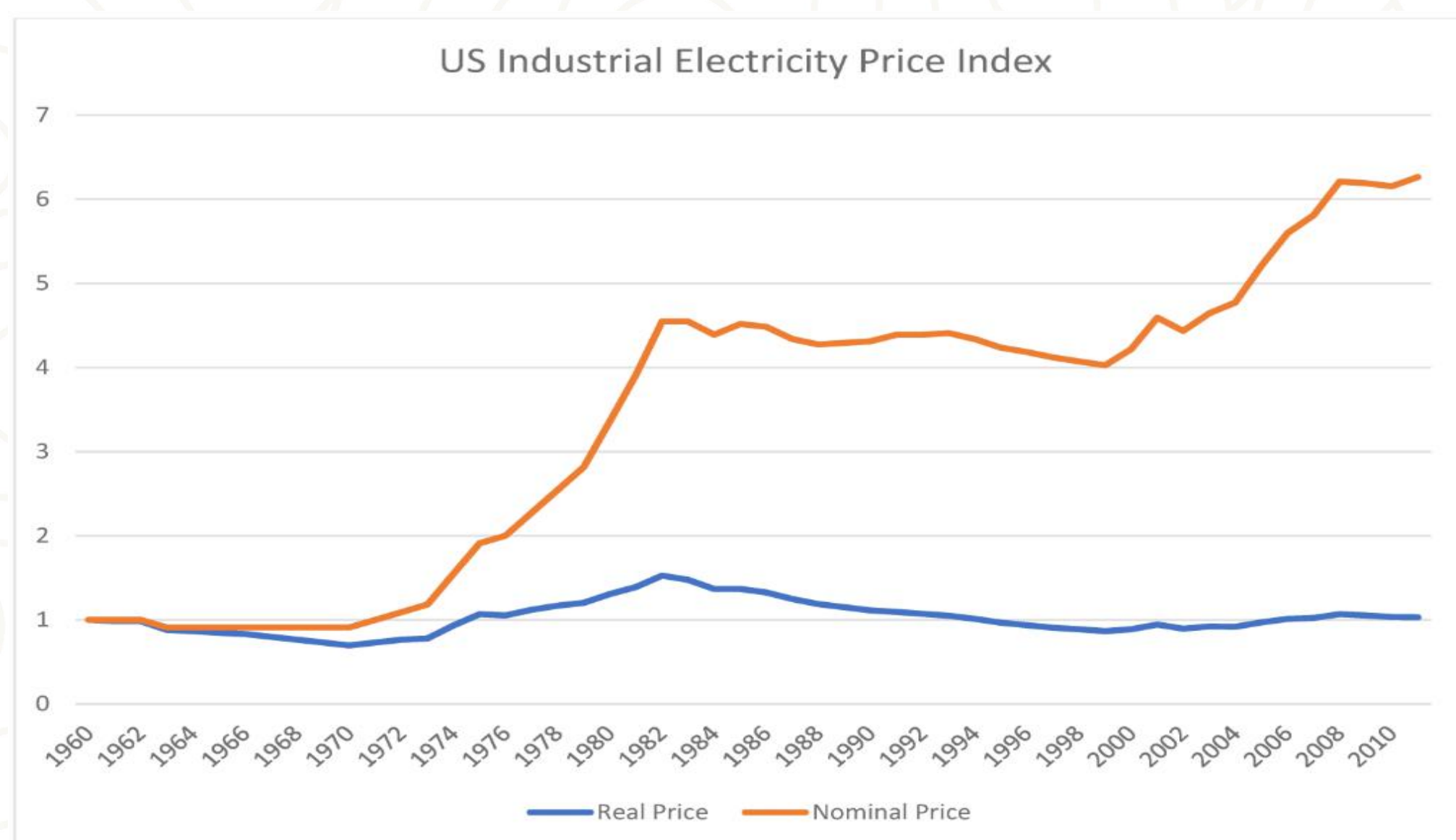


Figure 4: The industrial electricity price in US history is the lowest in the world.

4. 3 Government

The Baldi team believes that it will be the first person to create a real currency with long-term equilibrium value in an encrypted world. However, short-term fluctuations are expected, especially when the USUS economy is still young. Additional monetary policies are needed to absorb this wave. This kind of monetary policy will require constant adjustment and development of agreements. Appropriate governance mechanisms will be a tool to do so, which is crucial to ensure the stability and success of the community. Therefore, Baldi protocol issues BDOS governance token. It is planned that for major changes in monetary policy, the community may need to initiate voting for new functions of production and joining the main chain (and always comply with the current regulatory requirements). Most importantly, the community is part of Baldi's innovative hybrid consensus agreement.

USUS is more environmentally friendly and hundreds of times brighter than the traditional work permit based on blockchain. It also did not suffer from typical problems in evidence of equity blockchain such as "irrelevant", "remote attack" and "weak subjectivity". For the avoidance of doubt, the members of the final community shall not maintain contact with the foundation (or its subsidiaries) in any way, and the assets and funds of the foundation (or its subsidiaries) are still controlled by the relevant board of directors. Judge independently and apply them to achieve the foundation's goals. The right to vote does not grant USUS or BDOS holders the right to vote on the operation and management of the Foundation (or its subsidiaries) or its assets, nor does it constitute any equity

interest in the Foundation (or its subsidiaries).

4. 4 Proof of Value Consensus for Immediate Termination

The proof of value consensus is the proof of the mixed system of work certificate and equity. For cryptocurrency based on work certificate, the network hash rate may be very unstable. The mining pool attempts to play games by causing the network hash rate. Other work proves that cryptocurrency fluctuates significantly. Bitcoin Cash, Fedor and other verification work are based on encryption cryptocurrency. Such attacks sometimes cause the network to wait for hours or days for the next block to be resolved. Recently, Bitcoin gold and Verge have experienced double attacks by hackers and can rent and control over 51% hash values within a few hours. According to the information provided by crypto51, 51% attacks on several cryptocurrency only cost more than 10,000 US dollars per hour, which is more than 1 billion US dollars in market value. USUS systems are particularly vulnerable to attacks if such attacks rely entirely on proof of work as their security mechanism. Therefore, USUS team has introduced mixed PoB combustion proof and Bft Byzantine consensus proof. In the Baldi system, miners are responsible for creating currencies and verifiers, and for maintaining public ledgers and bookkeeping. The work has proved that miners do not directly deal with transactions, but create necessary concepts of randomness and time in the system to improve dispersion and resistance to attacks. This division of labor reflects the material world, where gold or silver miners and bankers maintain the financial system. Their cooperation has made the financial system more stable, safe and expandable. The verifier's bet is a combination of Baldi and USUS. Details of the composition will be explained in the monetary policy section.

4.4.1 Proof of Value Consensus Agreement in Guokr

Baldi's consensus agreement is a variant of the fast Byzantine agreement. The consensus mechanism itself can be paired with any Sybil resistance method (work certificate or equity certificate) to create an open participation model. In Baldi system, the proof of pile was selected for Sybil resistance to provide additional safety layer and check and balance in economic incentive design. It allows users to agree on transaction logs and achieve the following goals:

Consistency. If the agreement confirms transaction a, any future transactions confirmed by the agreement will be displayed in the log that already contains a. This is true even for isolated users who are disconnected from the network (for example, through Eclipse attacks).

Activity. The agreement should be based on the assumption that more than 2/3 of the participants (selected through the securities authorization process) are honest.

And the network is in "strong synchronization" (meaning that most honest users can send and receive messages from other honest users within a known time range). When the network is in a "weak synchronization" state (temporarily overtaken by rivals), it will maintain security until the network returns to synchronization mode.

Consensus agreement is a variant of Byzantine agreement. At a high level, it includes the following steps:

1. Random beacon generation. Decentralized randomness is the core of a truly decentralized blockchain system. Bitcoin implicitly creates randomness through global competitions, involving hash solutions for miners to search puzzles. There is no such plan in the stock ownership certification system, and one must be clearly established. For example, the Dfinity Consensus Protocol (Hanke 2018) utilizes BLS signature scheme, and Algorand (Gilad 2017) relies on verifiable random function (VRF) to generate random numbers for creating committees in subsequent steps.

The miner certification function in USUS is used as a random number generator. They work on a side chain, and the pure proof of work is called the Committee Election Relay (CER). CER periodically splits and merges with the main chain to trigger a committee re-election and ensure the activity of the main chain (the period between each split and merger is called Epoch). Transactions on CER include each miner's block reward (to be confirmed on the main chain) and Merkle root of all transactions on the main chain during the split. There may be multiple CER forks among miners, and only the miner with the longest CER confirmed by the next main chain block can obtain the corresponding block reward. The blocking periods of the main chain and CER are different. Initially, the block period on the main chain is set to 10 seconds, while the CER chain block period is set to 2 minutes. Due to the nature of the proof mining, the blocking period of CER follows exponential distribution. Whenever more than 30 blocks on the CER trigger the Committee to re-elect and synchronize data with the main chain, the CER and the main chain should be merged. The design choice of 30 blocks is mainly to reduce the volatility during the re-election of the Committee and to increase the allocation of block awards.

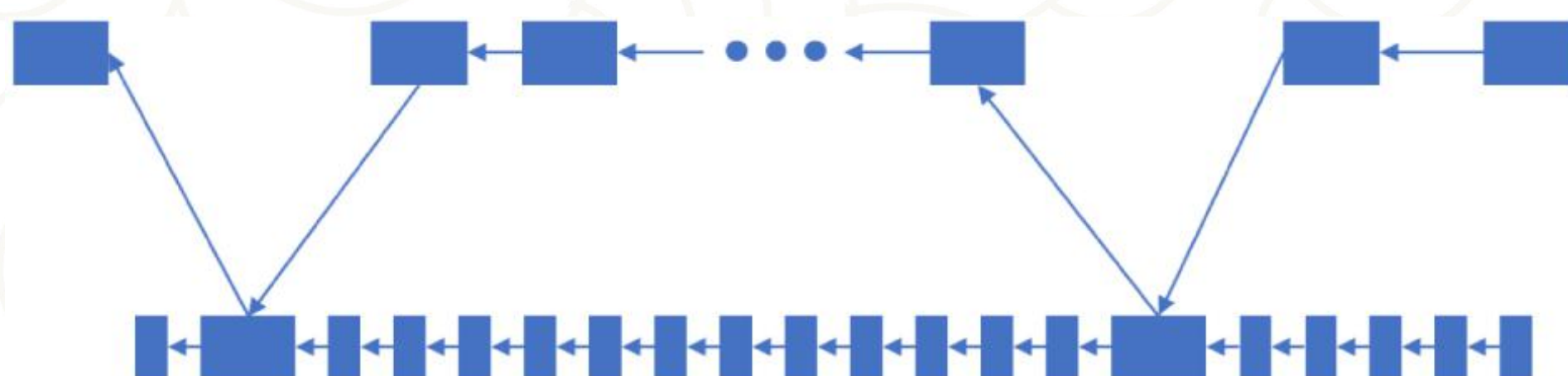


Figure 5: Baldi's equity certificate and work chain cross-reference.

2. Prevent the nominating committee from selecting and ranking. The block proposer committee is selected from the certificates of the equity representative pool. Let individual representatives be marked as 1,2, U.N is the size of the Committee, $N \leq U$. When n is large enough (e.g., a few hundred percent, the probability of more than $2/3$ representing honesty becomes very high. The random beacon P generated from step 1 (based on the longest CER confirmed by the existing committee) can be used to re-elect part or the entire committee from all representatives. In the initial stage, when the USUS network is still relatively small, the committee may become all qualified representatives of stakeholders. At this stage, the main applications will be arranged in the order of block proposals. As the seed of encrypted ranking, the members of the Committee are ranked from 1 to 1. n . the members of the highest ranking Committee will announce the beginning of a new era.

Delegates can be elected to the Committee at the beginning of the epoch.

3. Prevent proposal. Each committee member proposes a new round according to their ranking order. The valid block proposal b in round r should read:

$H(Br) = \text{acknowledge}(Br-1) \text{ confirmed}(Br-1)$ is the last acknowledged block, and the data in Br is valid

Assuming $Br-1$ is confirmed, if the committee member in charge of round R fails to block or obtain block confirmation in BlockTimeOut , the committee member in charge of $r+1$ will start to propose according to confirmation ($Br-1$).

4. Prevent confirmation. Once the committee members receive the blocking proposal. It began to sign proposals and broadcast signatures. It always listens for signed messages from its peers. Once the cumulative signature of Br reaches $> 2/3$ legal quantity, confirm Br confirm signature (Br). Any message of round r and earlier will be rejected once confirmed (Br)

This consistency algorithm does not need the network to keep strong synchronization at all times and will survive sovereign network attacks and partitions. For example, if more than $1/3$ of the committee members are offline due to network partition, block production will stop. However, the work proves that the miners will continue to work on their respective network islands. Once the network connection is restored, the longest working chain certification will trigger a reshuffle of the Committee and a new era. Baldi's team believes that this behavior is safer for ordinary consumers than the random behavior in the traditional Bitcoin work certification system. although

these transactions seem to be moving forward and confirmed based on the network islands around the users, they can be completely erased by the longer chain after the network partitions are merged. Byzantine protocol-style fast consensus scheme can ensure short delay (blocking time less than 5 seconds), high throughput (about 10,000 transactions per second at startup and extending to billions of transactions per second through fragmentation, side chains and multi-layer consensus) and instant termination (it is impossible to split and reverse transactions by proposing a longer blockchain).

4.4.2 Comparison of Value Consensus Evidence with PoW and PoS Consensus

One of the main criticisms of the consensus agreement based on work certification is the waste of energy. It is reported that Bitcoin mining may consume more electricity per year than Ireland. This energy waste is the direct result of Bitcoin incentive design, not the proof of the working concept itself. As mentioned earlier, the miners' profit chasing behavior leads to the total network hash rate of Bitcoin closely following the market price of Bitcoin. Since Bitcoin's total reserve is fixed at 21MBitcoin. The network hash rate of Bitcoin is basically consistent with the total market value of Bitcoin. The higher the market value of Bitcoin, the more energy Bitcoin has to operate and maintain its ledger.

Baldi will be the greenest proof of cryptocurrency's work, because its network hash rate only responds to the demand for additional money in the system, not the price of money. In other words, network energy consumption changes with the increase of market value instead of Baldi's total market value. The Baldi team estimates that with the size and growth rate of the US domestic economy, the annual energy cost of mining USUS will be very similar to the annual budgets of the US mint and engraving and printing bureau.

Proof of work usually provides the following benefits for consensus programs:

1. Sybil's Resilience
2. randomness
3. Time concept
4. No right to access currency

Baldi's mixed consensus uses the 1 bet proof and still relies on the rest of the work proof. Performance and instant termination are wise, and it is proved to be the same as the most advanced interest consensus algorithm. In addition, it will not be affected by the common defects in the ownership certificate system:

1. The rich are getting richer and richer. In the proof of the equity system, only existing coin

holders can participate in mining, and the profits of mining industry are usually proportional to the number of coins they hold, rather than their efforts in the real world. Therefore, change is very difficult. In Baldi system, mining is completely unauthorized. You do not need to hold a coin to start mining on the CER chain and obtain USUS. The certification of equity certifiers will be mainly supported by transaction fees and a small portion of mining incentives (reserves will be explained in later chapters) and occasionally diluted BDOS. In order to obtain more USUS in Baldi system, the best method is to participate in mining.

2. The stakes are nothing. There is no opportunity cost because voting on a specific version of blockchain certification does not require resources. Different from the work certificate, miners must choose which chain to point out their mining rights and exclude other chains. The certificate holder can put coins on each version of the certificate blockchain in order to maximize the return on mining volume. As long as no more than $2/3$ of the verifiers are rivals, Baldi's Byzantine consensus design of immediate termination does not allow bifurcation.

3. 3. Long-range attacks. The initial small number of stakeholders can collude back and "revive" the earlier version of the chain with a brand new transaction history. In USUS protocol, CER chain based on work certificate introduces time symbol in the protocol. Merkle roots of all transactions in each Epoch are recorded in the CER chain. Re-creating the chain requires not only more than $2/3$ of the bet token representatives, but also re-creating the entire CER chain history, which basically takes the same time as creating the original chain. In addition, the new chain will not contain the same amount of rice (or wealth) as the original chain.

4. Weak subjectivity. When a node joins the network for the first time, it must rely on a trusted source to find the hash of the valid chain, which completely destroys the untrusted nature of public blockchain. In Baldi system, the node only looks for the longest CER chain, which contains the information of the active committee.

In short, by combining the benefits of work certification and equity certification, USUS's consensus agreement is green, high performance, but safe and without rights.

4.4.3 USUS token

USUS's native digital password protection utility token is one of the main components of the ecosystem, and is designed to be used alone such as the main token on the network. Basically, USUS contains a series of digital signatures on Baldi blockchain. Baldi's encryption protocol enables the owner of USUS to transfer ownership of USUS to another by digitally signing the hash

of the previous transaction and adding these contents to the end of the digital signature chain. The payee can verify the signature to verify the ownership chain.

USUS is a non-refundable functional utility token that will be used as a unit of exchange between Baldi participants. The purpose of introducing USUS is to provide convenient and safe payment and settlement modes among participants interacting in Baldi ecosystem. USUS does not represent in any way any equity, participation, rights, ownership or interest of foundations, distributors, their affiliates or any other company, enterprise or enterprise, nor does USUS authorize token holders to bear any expenses, dividends, income, profits or return on investment, and does not constitute securities in the United States, Singapore or any relevant jurisdiction. USUS is used on Baldi, and the ownership of USUS does not contain any express or implied rights except the right to use USUS as a means to enable the use and interaction of Baldi.

As discussed herein, verification and validation of additional blocks/information on blockchain will require computing services and resources, so providers of these services/resources will need to pay for the consumption of these resources (i.e., "mining" on the Baldi network) to maintain network integrity and use gas as an economic incentive to encourage the provision of these computing resources. Bdos is an indispensable part of Baldi, because without Bdos, users do not need to spend resources to participate in activities or provide services for the entire ecosystem on Baldi. Users who do not actively participate in USUS or BDOS holders will not receive any incentives.

In particular, you understand and accept USUS:

- (a) any payment obligations of the distributor or any affiliated company;
- (b) does not represent or grant token holders any right in any form to the foundation, distributor (or any affiliated company thereof) or its income or assets, including but not limited to any right to future dividends, income, shares, ownership or equity, shares or guarantees, any voting, distribution, redemption, liquidation, proprietary (including all forms of intellectual property), or other financial or legal rights or equivalent rights, or intellectual property, property rights or any other form of participation or forms related to Baldi, foundation, distributor or its service provider;
- (c) It is not intended to represent any right under a contract for difference or the purpose of any other contract or pretend that the purpose is to obtain profits or avoid losses;
- (d) It is not intended to represent money (including electronic money), securities, commodities,

bonds, debt instruments or any other type of financial instruments or investments;

- (e) It is not a loan provided to the foundation, distributor or any affiliated company of the foundation, distributor or any affiliated company of the distributor, nor is it intended to represent the debts owed by the foundation, distributor or any affiliated company of the distributor, and there is no expected profit; And
- (f) Not to provide token holders with any ownership or other interest in the Foundation, Distributor or any of its affiliates.

If the volume of transactions in the secondary market or exchange does develop, it will be completely independent of the sales operation and operation of the company (or its subsidiaries), USUS. The organization will not create such a secondary market or act as an exchange.

4.4.4 Governance Token

The governance token on Baldi(Bdos) is the main bet token and is qualified as a verifier for maintaining the blockchain ledger. It is also used to collect proposals and votes on major changes in monetary policy. New features or changes to the main chain may require Bdos to initiate voting (and always follow current regulatory requirements).

Bdos cannot assume any payment obligation of any affiliated company, and does not represent any equity, participation, rights, ownership or interest of the company or any other company. The enterprise or enterprise is not used for speculative investment, and (although Bdos may eventually trade on the digital asset exchange), Bdos does not guarantee or represent value or liquidity, nor is it intended to represent currency (including electronic currency)), guarantees, commodities, bonds, Debt instruments or any other type of financial instruments or investments, and Bdos does not intend to constitute securities in Singapore or any relevant jurisdiction, nor will it entitle token holders to any promise, profit or return on investment of dividends, revenues and expenses.

If the secondary market or exchange of Bdos does develop, it will be completely independent of the operation and operation of the company (or its subsidiaries), and any sales of Bdos and Baldi. The company will not create such a secondary market, nor will it act as an exchange for Bdos.

4. 5 Monetary Policy

4.5.1 Secondary Price Fluctuations and Block Awards

Due to the short-term imbalance between supply and demand, the market will experience price fluctuations. When this happens, profit-driven miners will transfer more mining equipment to the network when the USUS market price rises and remove mining equipment when the market price falls. Their behavior will cause the Baldi block reward to change flexibly in response, which will

return the price to its equilibrium or competitive state. Under normal circumstances, the block reward should be the main source of income for miners, and the transaction fee income should be the smallest. During the period of large long-term downward price changes, the collective reward value to miners may be negligible. Transaction costs will be the largest source of revenue for the support network and may increase. Faced with similar conditions in an inflationary environment, Baldi's ecosystem will experience an increase in labor costs.

4.5.2 Large volatility and monetary policy intervention

In the case of a disproportionate and less likely price volatility, further action may be necessary to balance the market and to establish a competitive price. These actions in the form of selling and buying bonds are similar to those of Federal Reserve and Department of The Treasury of the United States in the material world.

Department of The Treasury of the United States holds public auctions on the open market to sell bills, TIP and bonds (all of which will be called "bonds" for simplicity). When the Federal Reserve of the United States buys these bonds, it issues new currencies, thereby increasing the money supply and lowering the market price of the currency (This will lead to inflation). When the public holds and purchases bond with their own currency, the currency is effectively removed from the circulation, which reduces the overall currency supply and increases the market price of the currency (This will lead to deflation). Bonds are essentially a series of regular currency payments supported by collateral from assets or future sources of income. The quality of the collateral directly determines whether people are willing to pay for bonds. U.S. Treasuries are supported by future government tax revenues. The bond mechanism can absorb the impact of the economy and is the basic monetary instrument used by the Federal Reserve and Department of The Treasury of the United States.

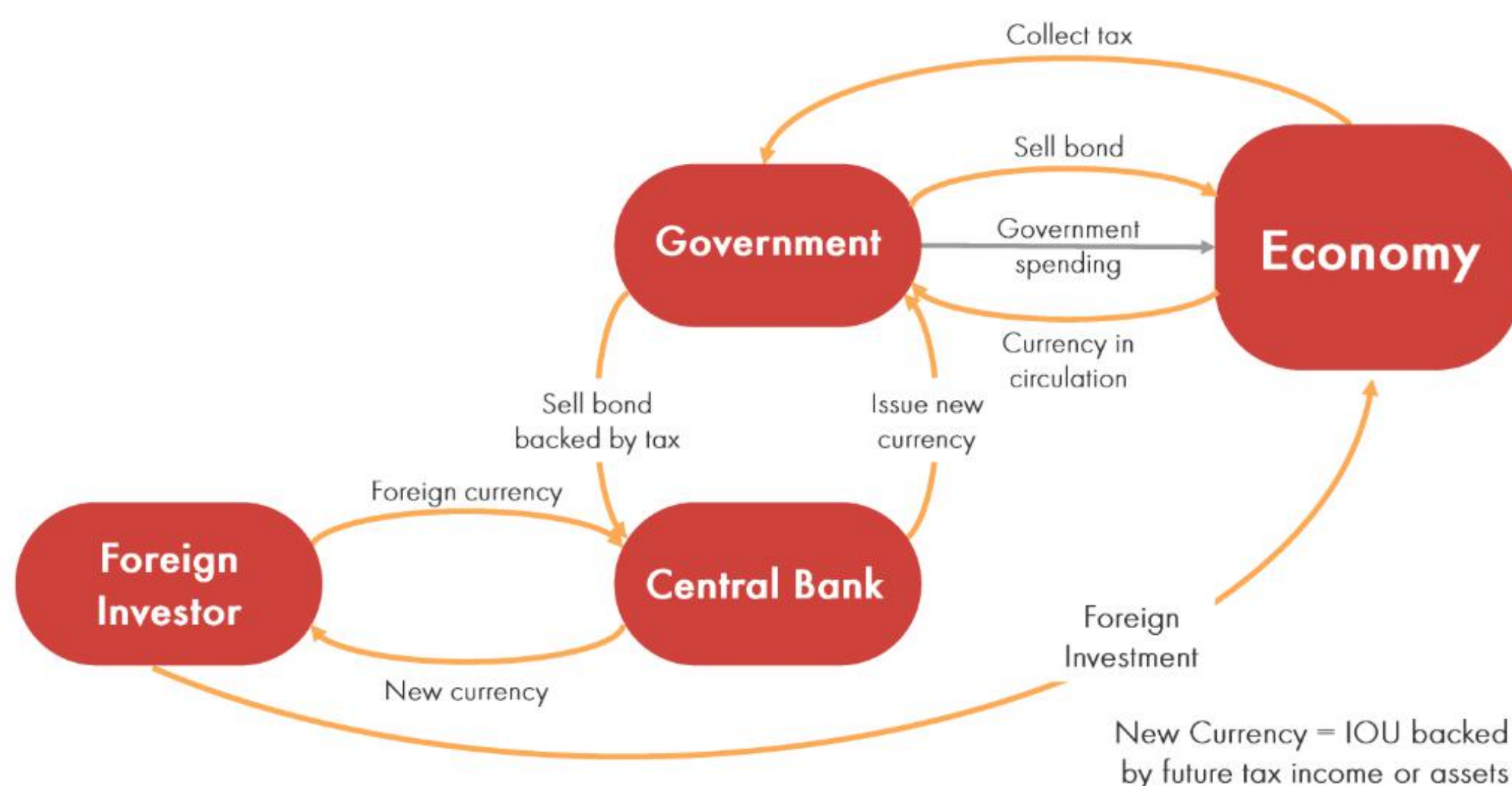


Figure 6: How the U.S. monetary system supports the economy by managing currencies, bonds, taxes and foreign investors.

Baldi protocol lacks a centralized government, but it retains the concept of reserves to absorb any major impact on Baldi price stability ("reserve"). Reserves are a source of future income that can be used to attract currency holders to exchange Baldi liquidity. In Baldi's consensus protocol, a small portion (initially 10 %) of the mining incentive and all transaction costs first entered the reserve and then entered the block verification. Bdos is usually used as tokens to prove the purpose of equity. However, when the system has to reduce USUS cycle, it will begin to allow USUS to also be used as a stake. Part of the block award is used for Baldi stake and the rest is for Bdos stake. By adjusting the ratio of Baldi to governance returns, the system will use market forces removing different amounts of Bdos from circulation. The exact amount of Bdos in the investment process depends entirely on the market.

In Baldi protocol, block verifiers are basically used as commercial banks, while reserves managed through Bdos are used as the Federal Reserve. The Federal Reserve influences the monetary system by adjusting interest rates.

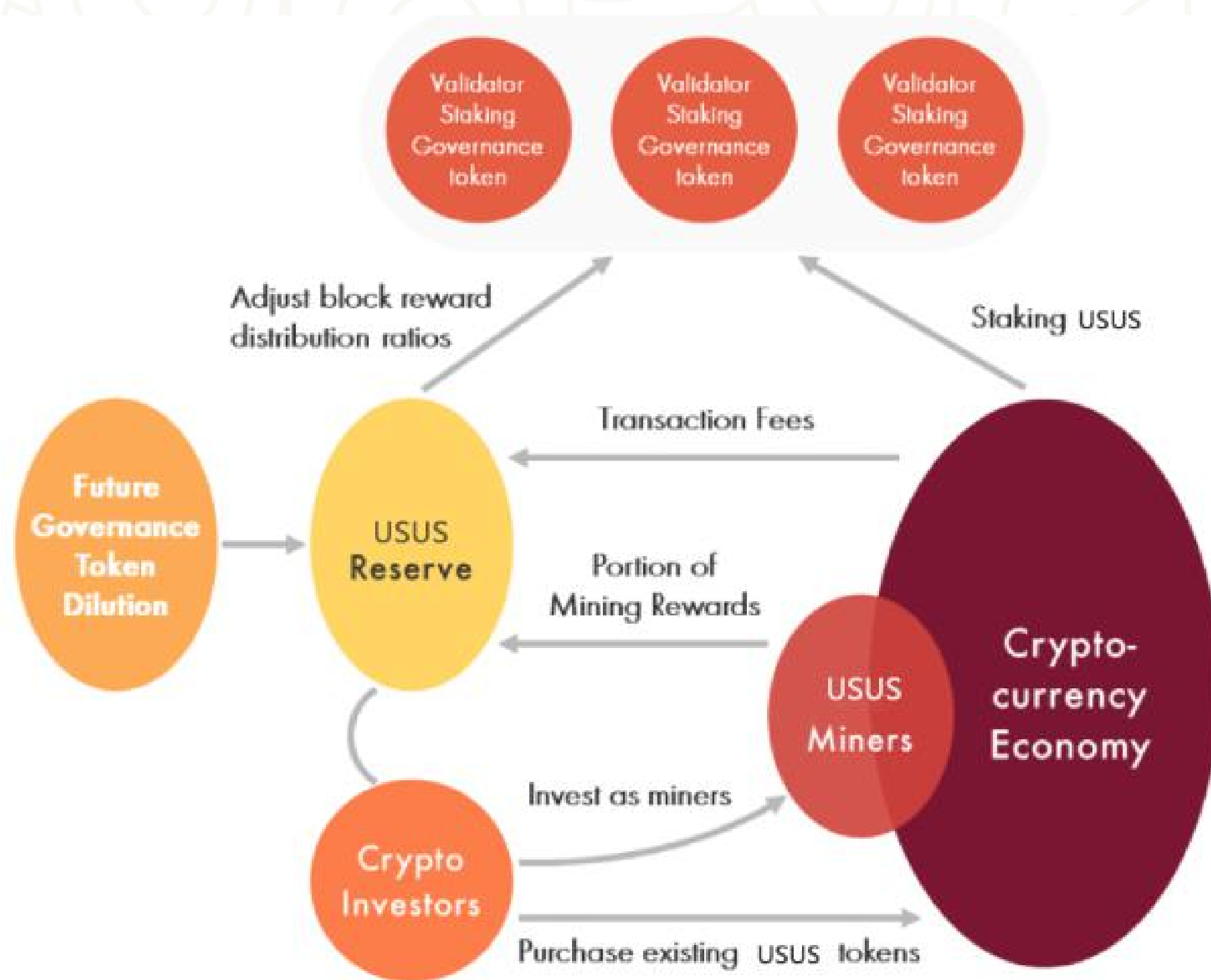


Figure 7: Baldi protocol uses some of the same tools that the US monetary system uses to stabilize its currency.

4. 6 Guidance usus system

USUS is the basic currency and unit of accounts of Baldi financial system. In all transaction costs, the gas for calculation must be measured and paid by USUS. When the network starts up, one of the most important uses of Token is to obtain governance token Bdos to participate in the protection and development of Baldi system. The system will automatically generate a Dutch auction for BDOS token based on a predetermined interval (as an example per day). The only way to participate in an auction is to use Bdos as the bid currency. At the end of the Dutch auction, all the participants in the period will have the same price as USUS. Most Bdos tokens in the auction proceeds will be burnt out, but a will be allocated to verifiers and future growth of Baldi ecosystem. This combustion mechanism will also constantly remove Bdos tokens from the cycle.

4. 7 Cross chain architecture of Baldi Protocol

Baldi is designed as a completely open system with parent blockchain, sidechain and parallel chain structure. The parent blockchain uses proof of work to support Baldi stable virtual currency, monetary policy and transaction settlement records. It also provides a medium for inter-chain communication. The sidechain originates from the parent blockchain, but can join the consensus of the parent blockchain or have its own independent consensus mechanism. Baldi team is actively studying the compatibility of major plans (e.g. segments) in other public chains with Baldi's monetary policy. In addition, high-performance consensus protocols can be implemented on the side, such as delegation certification, direct acyclic diagrams, parallel chains and other functional chains to increase transaction throughput or introduce more complex services, such as storage and software-defined networks.

Although Baldi is a public chain, it is not intended to compete with Ethereum and other public chains. Instead, it provides a stable financial system for these public chains through Baldi's parallel chain infrastructure. Parallel chain is a completely independent blockchain, which communicates with Baldi through inter-chain communication. Baldi team is currently building connectors and SDK for Ethereum, EOS, Bitcoin and other major public chains to facilitate such communication.

For example, dApp developers who build payment services on high-performance sidechains, such as Paypal or Venmo, can issue Baldi-linked payment tokens and provide betting tokens-native tokens for dApp for purposes (except those related to payment). Therefore, a completely different token economy, incentive matrix and development road map can be maintained on the sidechain (and parallel chain). In this example, each dApp payment token is supported by Baldi in the smart contracts, and Baldi

protocol provides the interface and final settlement of dApp payment token when linked to USUS.

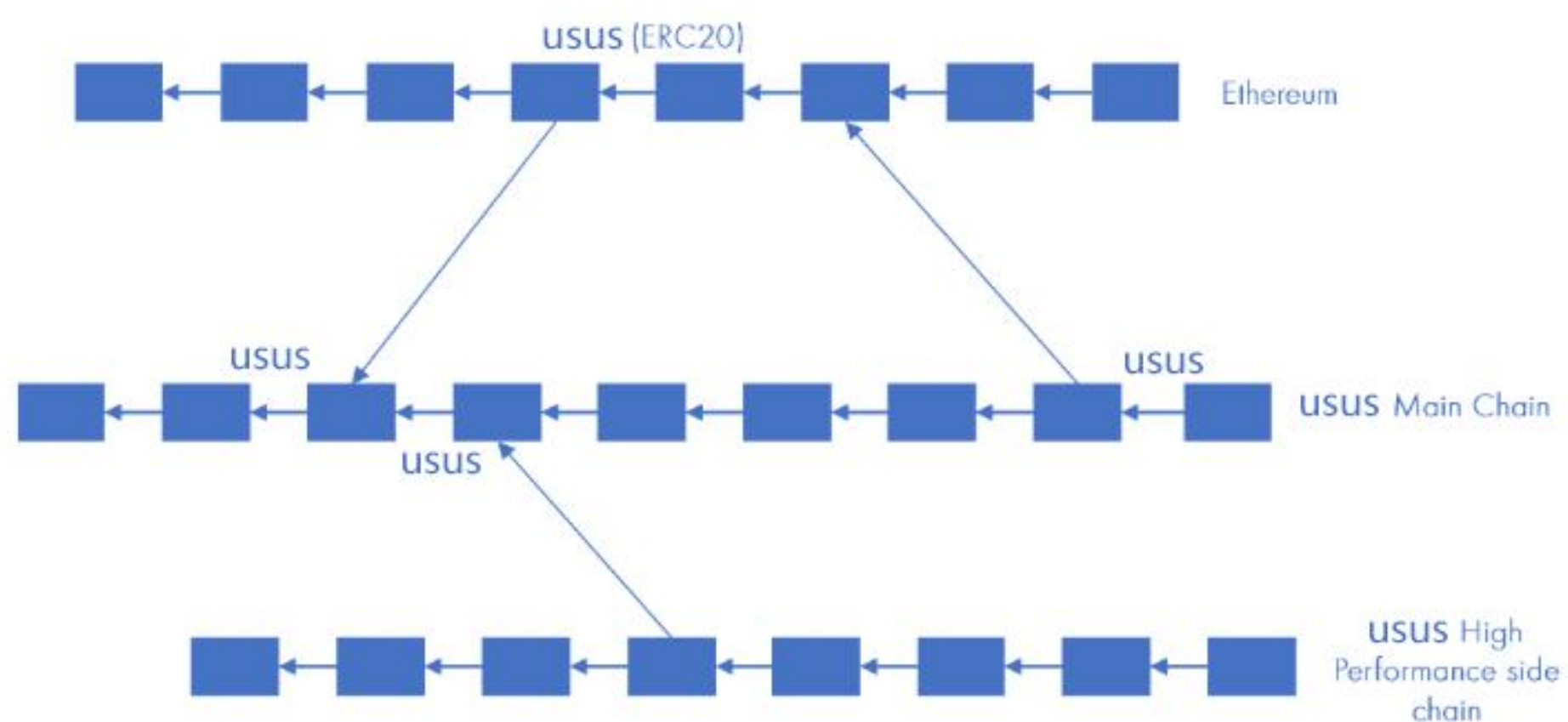



Figure8: Sidechain / parallel chain architecture of Baldi ensures scalability and throughput efficiency, and provides the driving force for the whole cryptocurrency economy.

4. 8 Launching USUS will power Ethereum

Baldi virtual machines ("BVM") are fully compatible with Ethereum virtual machines, and Ethereum developer tools and ecosystems can be easily migrated to Baldi. In addition, adapters will be provided to easily transfer Ethereum and ERC20 tokens between Baldi parent blockchain and Ethereum.

- 
- Participate in Baldi
 - Design overview
 - Conclusions
 - Risks
 - Reference

5 Participate in Baldi

Baldi network maintenance has four basic roles: Collator, combustion nodes, nominator and verifier. In a possible implementation of Baldi, the latter role can actually be divided into two roles: Basic verifier and availability guarantor;

5.1 Verifier

Verifiers are the highest cost and help seal new blocks on Baldi networks. The role of vals depends on the deposit of bonds high enough. Although we allow other bondholders to nominate one or more verifiers to act for them, some parts of the verifier's bond may not necessarily be owned by the certifier itself, but by these nominators.

The verifier must run a relay chain client implementation with high availability and bandwidth. In each block, the nodes must be ready to accept the role of approving a new block on the specified chain. This process involves receiving, verifying, and republishing candidate blocks. The nominations are deterministic, but almost unpredictable in advance. Because the verifier cannot reasonably expect to maintain a fully synchronized database in all chains, it is expected that the verifier will specify the task of designing the proposed new baldichain block to a third party (called the collator).

Once all new baldichain blocks are approved correctly by their specified verifier subgroup, the verifier must approve the relay chain block itself. This involves updating the status of the transaction queue (basically moving the data from the output queue of baldichain to the input queue of another baldichain), processing the transactions of the approved relay chain transaction set and approving the final block, including the final baldichain changes.

According to the rules of consistency algorithm that we select, the verifiers who fail to fulfil their obligations to seek consensus will be punished. For initial, nil failures, this is a reward by withholding the verifier. Repeated failures lead to a reduction in its security protection (through combustion). Adverse acts, such as double signatures or conspiracy to provide ineffective prevention, lead to the loss of the entire bond(which has been partially burned down, but mainly to the wired and honest actors).

In a sense, verifier is similar to the current PoW blockchain mining pool.

Nomination. The nominators are shareholders and are responsible for confirming the surveyor's guarantee. They have no effect other than placing venture capital, thus indicating that they trust specific verifiers (or their assembling) to act responsibly while maintaining the network. Based on the growth of

bonds, they increase or reduce deposits proportionately.

Next, the nominators and partners work together in a sense similar to miners of PoW network.

Trading partner (abbreviated as a partner) is a party who assists the verifier in the production of an effective chain block. They maintain "full nodes" for specific chains; This means that they retain all the necessary information so that they can create new blocks and execute transactions, just as the miners are on the current PoW blockchain. Under normal circumstances, they will collate and execute transactions to create unsealed blocks and provide them with zero knowledge proof to one or more verifiers currently responsible for presenting branch blocks.

The exact nature of the relationship among the collators, nominators and verifiers may change over time. At first, we wanted the collator to work closely with the verifier, because there were only a few (perhaps only one) branch chains with fewer trading volumes. The initial client implementation will include RPC, allowing the baldichain collator node to unconditionally provide a proven baldichain block for the (relay chain) verifier nodes. As the cost of maintaining synchronous versions of all such chains increases, we look forward to seeing additional infrastructure that will help separate responsibilities to independent, economically motivated parties.

In the end, we want to see the tidying pool competing for the most transaction fees. These partners may sign a contract over a period of time to serve a specific verifier in order to obtain a sustained share of the reward proceeds. Or, freelance partners can simply create a market that offers effective baldichain blocks in exchange for a competitive share of the rewards paid immediately. Similarly, the dispersed nominator pool will allow multiple bonded participants to coordinate and share the responsibility of the verifier. This assembling ability ensures open participation, thereby achieving a more decentralized system.

The combustion node is different from the other two active political parties, and is not directly related to the block writing process. Instead, they are independent reward hunters, inspired by large one-off awards. It is because of the existence of combustion nodes that we expect adverse events to occur rarely. And when they do so, it is only because of the bonded party's negligence of secret key security, not through malicious intentions. The name comes from the expected frequency of awards, the minimum requirements for participation, and the final scale of awards.

Combustion nodes are rewarded by certifying timely that at least one bonded party acted illegally. Illegal

acts include signing two blocks, each with the same approved parents, or, in the case of a secondary chain, it helps to approve invalid blocks. In order to prevent excessive reward or compromise and illegal use of the secret key of the session, the basic reward for providing illegal signature messages for a single verifier is minimal. As the provision of more confirmed illegal signatures from other verifiers means real attacks, this reward gradually increases. According to our basic security assertions, the asymptote is set to 66%, and at least $2/3$ of the verifiers show a benevolent attitude.

Burning nodes are somewhat similar to the "completenodes" in today's blockchain system, which require relatively little resources and do not require stable uptime and bandwidth. The burning nodes vary widely because they have to issue a small bond. This binding prevents sybil attacks from wasting verifier's time and computing resources. It can be withdrawn immediately, probably not more than a few dollars. It may get a huge reward for finding a verifier of misconduct.

6 Design overview

The purpose of this section is to provide a brief overview of the entire system. In the following parts, a more comprehensive exploration of the system is given.

6.1 Consensus

Baldi realizes low-level consensus on a set of agreed effective blocks through modern asynchronous BFT (Byzantine Fault Tolerance) algorithm. The algorithm is inspired by simple Tendermint and more complex HoneyBadgerBFT. The latter provides an effective and fault-tolerant consensus for any defective network infrastructure, and gives a set of benign authorities or verifiers.

This is enough for a network of Proof of Burn (POB), but Baldi is assumed to be deployed as a network in a fully open and public situation without the need for any particular organization or trusted authority to maintain it. Therefore, we need a way to identify a set of verifiers and motivate them to be honest. To this end, we use PoS-based selection criteria.

6.2 Proof pet

We assume that the network will have some ways to measure the "benefits" of any particular accounts. To facilitate comparison with pre-existing systems, we will call them measurement unit "Token". Unfortunately, for a variety of reasons, the term is not ideal, especially it is simply an account-related scalar value and has no personality concept.

We imagine using a designated equity certificate (NPoS) program, not often electing verifiers (up to once a day, but perhaps rarely quarterly). Centralization can be achieved through proportional distribution.

Funds come from the expansion of token base (up to 100% per annum, more likely around 10%) and any transaction fees charged. Although the expansion of the monetary base usually leads to inflation, because all token owners have fair opportunities to participate, as long as they are willing to play a role in the consensus mechanism, no token holder needs to reduce the value of his or her holdings over time. A specific proportion of tokens will be the target of the betting process; Effective token base expansion will be adjusted through market-based mechanisms to achieve this goal.

Verifiers are heavily bonded through their bets; After the effective duty ceases (perhaps about three months), the bonds that withdraw from the verifier still exist. This long-term bond liquidation period allows future misconduct to be punished until the chain's periodic checkpoint. The bad behavior leads to a penalty, such as a reduction in the award, or in the event of a deliberate compromise of the integrity of the network, the verifier loses its part or all of its equity to the other verifier, the informant, or the entire stakeholder (through burning). For example, a verifier attempting to approve two branches of a branch (sometimes referred to as a "short-range" attack) may be identified and punished in the latter manner.

Remote "irrelevant" attack 4 is circumvented by a simple "checkpoint" lock, which prevents risk chain reorganization beyond a specific chain depth. In order to ensure that the newly-synchronized client cannot be erroneously linked to the wrong chain, a conventional "hard fork" (up to the same period of the bond liquidation of the verifier) will occur, and the most recent checkpoint block is hard-coded to the client. This has a good effect on further reducing footprints of finite chain length or periodic reset of generating blocks.

6. 3 baldichains and Collators

Each baldichain receives security support similar to that of relay chain: The title of baldichains is sealed in the relay chain to ensure that it cannot be reorganized or "double expended" after confirmation. This is similar to the security provided by Bitcoin sidechain and merge mining. However, Baldi also provides a powerful guarantee for the state transition of Subchains. This is achieved by a set of verifiers randomly split into subsets in an encrypted manner; Each baldichain is a subset, and each block may be a different subset. This arrangement generally means that the blocking time of the chain is at least as long as the blocking time of the relay chain. The specific method of determining the partition is out of scope

The document may be based on a submission disclosure framework similar to RanDAO, or use data from previous block combinations of each chain under password-security hashes.

These verifier subsets need to provide a guaranteed side block candidate (in the case of forfeiture of bonds). Effectiveness revolves around two key points; First, it is essentially valid and all state transitions are faithfully performed, and all referenced external data (that is, transactions) applies to clusion. Second, any external data for their candidates, such as those external transactions, is highly available enough for participants to download and manually execute the block. Validators may provide only one "empty" block that does not contain external "transaction" data, but if you do so, there may be a risk of reducing the reward. They work with a baldichain gossip protocol, collate the transaction with the individual collaborators and provide non-interactive zero knowledge proof that the block constitutes a valid child of their parents (and charges any transaction fees for their troubles).

Baldichain protocol specifies their own spam prevention means: The relay chain has no basic concept of "computing resource metering" or "transaction fee". Nor is it directly enforced through relay chain protocol (although stakeholders are unlikely to select branches that do not provide the right mechanism). This is a clear point to the possibility of a different chain from Ethereum, such as Bitcoin class chain, which has a simpler cost model or some other spam prevention models that have not yet been proposed.

Baldi relay chain itself may exist in accounts and status chains similar to Ethereum, possibly EVM derivatives. Because relay chain nodes will need to do a lot of other processing, transaction throughput will be minimized by a large number of transaction costs, and if our research model is needed, it will reduce the size limit of small blocks.

6. 4 Inter-chain communication

The key final component of Baldi is inter-chain communication. Since there can be some kind of information channel between baldichains, we allow ourselves to consider that Baldi is an extensible multi-chain. In the case of Baldi, communication is as simple as possible: The transaction executed in one chain (as per the logic of such chain) can be distributed to the second chain which may be the relay chain. Like external transaction involving production of blockchain, they are asynchronous and free from intrinsic competence of returning any kind of information to its original point.

To ensure minimum implementation complexity, minimum risk and minimum direct sheath of future chained architecture, the transaction between chains cannot be distinguished from standard external

signature transaction actually. The transaction is of the original segment, provides the ability of identifying the branch and can have the address based on any size. Different from commonly used systems such as Bitcoin and ether, Internet transaction won't give rise to "payment" relating to expenses; Any kind of payment must be managed based on negotiation logics on the source chain and destination chain. The system released by Serenity of Ethereum will be a simple method for managing the cross-chain resource payment, although we think others may stand out at the right moment.

Simple queuing mechanism based on Merkle tree is used to analyze affairs between chains to ensure fidelity. The task of the relay chain vindicator is to move the affair on the output queue of baldichain to input queue of target baldichain. Transmitted affairs are cited on the relay chain which aren't affairs of the relay chain. To prevent baldichain sending junk mails to another baldichain based on the affair. As for the affair to be sent, the target input queue is required to be not too big when previous block is over. In case of the input queue being too big after block processing, it will be deemed to be "saturated" and cannot be routed by affair in the subsequent block until reducing to be under the limit. Such queues are managed on the relay chain and it's allowed to confirm mutual saturation condition by link; As a result, failed attempt about sending the affair to the stalled destination can be simultaneously reported. (Although there is no return path, leading to the failure in auxiliary affairs, it cannot be reported to the original caller and it's a must to implement some other recovery modes.)

6. 5 Baldi and Ethereum

Because of Turing integrity of Ethereum, we predict that Baldi and Ethereum have sufficient opportunities for mutual operation at least within some security ranges easy to be deduced. In short, we imagine the transaction from Baldi can be signed by the verifier and then Ethereum will be inputted which can be explained and formulated by transaction forwarding contract. In the other direction, we predict use of the log based on special format from "breakthrough contract" to facilitate quick verification of specific message which shall be forwarded.

6. 6 Baldi to Ethereum

The verifier formed by a group of stakeholders confirmed by approval voting mechanism after selecting BFT consensus mechanism, we can reach to security agreement with the verifier not changing often based on proper quantity. In one system with 144 verifiers, as per 4s blocking time and finality of 900 blocks (allowing malicious acts such as reporting, punishment and repairing double voting), validity of the block can be reasonably considered and there is no challenge verified based on 97 signatures ($\frac{2}{3} \times 144 + 1$) and subsequent 60min verification period.

Ethereum can preside over one "break-in contract" and maintain 144 signatories that can implement control. Because recovery of Elliptic Curve Digital Signature Algorithm (ECDSA) only needs 3,000 gas under EVM, we may only wish that the verification only happens to super most verifiers (not completely identical) and quantity of gas from Baldi network fails to exceed 300,000 which is only 6% of total gas limit (5.5M), basic cost of Ethereum confirms that the instruction is properly verified. In case of increasing the quantity of verifiers (necessary for processing dozens of chain stores), the cost will be increased inevitably. However, with technology maturity and infrastructure improvement, people widely expect trading bandwidth of Ethereum will increase as time goes on. Based on the fact that the connection doesn't need to involve all verifiers (for example, only verification based on the highest stake can be required to execute such task), the restriction of the mechanism can be well extended.

Supposing that the verifier is alternated every day (every week and even every month can be accepted based on fairly conservative estimate), network cost incurred by maintaining the Ethereum forwarding bridge will be about 540,000 natural gas every day or the price of natural gas now is USD 45/year. sic transaction independently forwarded on the 巴在桥 will cost about USD 0.1; Of course, additional contract calculation will cost more. Running-in authorization cost sharing can be easily realized, substantially lowering the cost of each transaction by buffering and bundle trading; In case 20 transactions is needed before forwarding, the expense incurred by forwarding basic transactions will lower to about USD 0.01.

A funny cheaper alternative

At the moment of signing the contract model, threshold signature will be used to realize multilateral ownership semantics. Although threshold signature scheme of ECDSA is expense in terms of calculation, other schemes such as Schnorr signature are very reasonable. Ethereum plans to introduce element, causing such schemes is used cheaply in the upcoming Metropolis hard fork. In case that such method can be adopted, the cost of natural gas used to forward Baldi transaction to Ethereum network will greatly lower to be nearly zero, exceeding the basic cost of verification of signature and execution of basic transaction.

In the model, verifier nodes of Baldi only involves signing message. To make the affair actually routed to Ethereum network, we suppose that the verifier will also reside on the Ethereum network or it's more likely that small reward will be provided to the first actor forwarding the message to the network (the money reward may be very simple and provided to the transaction initiator).

6. 7 From Ethereum to Baldi

The affair is forwarded to Baldi from Ethereum based on simple log concept. When Ethereum contract hopes to send the transaction to specific branch of Baldi, it only needs to call one special "breakthrough contract". The breakthrough contract will take any payment which may be needed and send the recording instruction to prove its existence by Merkle certification and effective and standardized assertion on the head of corresponding block.

In the latter two cases, validity may be the most direct certification. In principle, the only requirement is each case needing to certify complete synchronization of Baldi nodes (namely designated verifier nodes) operating standard Ethereum nodes. Unfortunately, it's quite a heavy dependence. A more lightweight approach is to use one simple evidence, namely correctly evaluating the head by only providing partial head of trie under Ethereum state necessary for the affair in the block correctly executed and inspecting whether the log (including those in the block receipt) is effective or not. The evidence regarding such "similar SPV" 6 may also need plenty of information; Under normal conditions, they aren't needed: Internal bond system of Baldi allows the third party of bond to submit the header. In case of other third party (such as "combustion nodes) may lose the evidence of reminding the header is invalid by bond risk (especially state root or receipt root is imposter).

In the non-final PoW network like Ethereum, it's impossible to finally certify the normalization. To solve this problem, any type of causality-dependent application is to be "confirmed", or until the dependency transaction is in a specific depth in the chain. On Ethereum, this depth varies from one block to 1,200 blocks from the lowest value transaction with no known network problems, as was the case when the original Frontier released the exchange. On the stable "home" network, this number is 120 blocks for most exchanges, and we might use similar parameters.

As a result, we can imagine that our Baldi-end Ethereum interface has some simple features: It can accept new headers from Ethereum network and verify PoW so that it can accept some evidence that Ethernet issues a specific log, a breakthrough contract with a sufficient depth of header (and forward the corresponding messages within Baldi), and finally accept the evidence that the previously accepted but not yet formulated title (containing invalid receipt).

The data are required for the incentives for forwarding to obtain the Ethereum title data (and SPV certification or validity / normative rebuttal) to the Baldi network.

This may simply be paid (expense fund charged by Ethereum) to anyone who is able to forward the useful block for which the title is valid. The verifier will be required to retain information about the last

few thousand blocks in order to be able to manage the forks either by means of a number of protocols or by a contract maintained on the relay chain.

6. 8 Baldi and Bitcoin

Bitcoin interoperability presents an interesting challenge to Baldi: The so-called "two-way hook" will be a useful infrastructure on both sides of the network. However, due to the limitations of bitcoin, it is very important to securely provide such hooks. Transactions from Bitcoin to Baldi can, in principle, be done through a process similar to that of Ethernet; The "breakthrough address" controlled by Baldi verifier in some way can receive transferred tokens (and the data sent with them). SPV proof can be provided by motivational oracle and, together with confirmation periods, can be used to identify rewards for non-canonical blocks that imply that the transaction has been "double spent". Then, any token held in the detach address will, in principle, be controlled by the same verifier for later decentralization.

The problem, however, is how to safely control deposits from the rotary verifier group. Unlike Ethereum, which can make arbitrary decisions on the basis of the combination of signatures, Bitcoin is substantially more restrictive, and most customers accept up to three parties of multi-signature transactions. Under the current protocol, it is impossible to extend this to 36, or eventually to thousands. One selection is to change Bitcoin protocol to achieve such function. But the so-called "tough issue" in the Bitcoin world is hard to judge by the recent attempts. One possibility is to sign by using threshold value, encrypt schemes to allow single identifiable publickeys to be controlled effectively by several secret "parts", and some or all of them must be used to create a valid signature. Unfortunately, the calculation cost of threshold value signature compatible with Bitcoin's ECDSA is very high in the aspects of creating and polynomial complexity. Other schemes such as Schnorr signature etc. provides much lower costs, but the timeline in which they might be introduced into the Bitcoin protocol is uncertain.

Because the final security of deposit depends on many bound verifiers, the other selection is to reduce the multi- signature key holders to only heavily bound subset of total verifier, and make the threshold value signature feasible (or, the native multi-signature of Bitcoin is possible at worst. In case illegal action of a verifier occurs, this certainly will cause a decrease in the total amount of bonds which will be reduced for compensation. But it is a graceful degradation, it only needs to set the upper limit of capital amount that can be operated safely between two networks), or in fact, if the attack from verifier is successful, the % lost happens.

Thus, we believe that it is not realistic to set a quite safe Bitcoin interoperability "virtual branched-chain".

Even so, this is still a major effort with an uncertain schedule between the two networks, and it might need the mutual cooperation of stakeholders in this network.

7 Conclusions

The Research Institute of Baldi introduces that Baldi is a kind of stable cryptocurrency based on the proof of work, and its value has a fundamental connection with the value concept in the physical world. The proof of work is the fairest way to excavate new cryptocurrency, and is the safest way to protect fully decentralized and free-license public blockchain.

Upon the review of Bitcoin's historical data, it shows that its value can be agented from the marginal production cost. Similary, USUS takes the energy consumption of the physical world as a unit to agent its market price reliably. It provides relatively stable accounts for cryptocurrency economy, and reduces the extremely unstable exchange rate, which the dApp developers have to face so far. The Baldi protocol further absorbs the short-term fluctuations of supply and demand by bond sales and purchasing within the financial limitation set by reserve funds. Although the stable value is the necessary condition for developers, they can freely use other public chains to do so. Development environment, ecological system and other considerations. Baldi provides the chain crosslink communication and value transfer mechanism to help developers anchor their currencies by stable value of Baldi in several public chains. Baldi is a decentralized financial infrastructure, which can not only connect different blockchains in the virtual world, but also connect the physical world. People must enable to use advantages and services of cryptocurrency and the physical world to conduct transactions and establish more prosperous cryptocurrency economy.

8 Risks

You acknowledge and agree that there are many risks associated with Bdos you held and Baldi you participated in. In the worst case, it might cause losses on all or part of assets bought. If you decide to buy Bdos, you have to cleary acknowledge to accept and undertake the following risks:

8. 1 Uncertainty of laws and regulations and enforcement actions

The regulatory conditions of distributed and classified accounting technology remain unknown or are unsolved in many jurisdiction areas. The supervision and control of virtual currency has become the primary target of all major countries in the world. It is impossible to predict how, when or whether the supervision organizations will apply existing laws and regulations or

formulate new laws and regulations for such technology and application (including Bdos/or USUS). Regulatory actions may adversely affect Baldi in a variety of ways. Operate in the area of the jurisdiction to avoid the relevant legal risks as far as possible. For token sales, Baldi Foundation and global distributors must comply with compliance standards.

8. 2 Inadequate disclosure of information

If Baldi still issues development board on this date, mechanisms, algorithms, code, and other technical details and parameters can be constantly and frequently updated and changed. Although this white paper contains the latest information about Baldi, it is not absolutely complete and may be adjusted and updated by Baldi team from time to time. Baldi team does not have the ability and obligation to retain the holder to understand every detail about the development of Baldi program (including development progress and expected milestones), so inadequate disclosure is inevitable and reasonable.

8. 3 Failure to develop

For a variety of reasons, including, but not limited to, the decline in the price of any digital assets, unforeseen technical difficulties, and the following circumstances, it may not be possible to implement or carry out Baldi development as planned.

8. 4 Security hole

Hackers or other malicious organizations or organizations may try to interfere with Baldi in a variety of ways, including, but not limited to, malware attacks, denial of service attack, consensus-based attacks, Sybil attacks, smurfing, and spoofing. In addition, third parties or foundation members, dealers or their subsidiaries may intentionally or unintentionally introduce defects into the core infrastructure, which may have a negative impact on Baldi.

In addition, the future of cryptography and security innovation is highly unpredictable, and the progress or technological progress of cryptography (including, but not limited to, the development of quantum computing) may expose Baldi to unknown risks by invalidating the encryption consensus mechanism. bootstrap protocol.

8. 5 Other risks

Besides that, the above-mentioned potential risks are not exhaustive, there are other risks (especially listed in terms and conditions) in Baldi you hold and use, including risks that the foundation or distributors cannot expect, which might be unexpected change or portfolio of the above risks. You should make a comprehensive due diligence on foundations, distributors, and

their affiliates and hold Baldi's overall framework, mission and vision.

9 Reference

Nakamoto, Satoshi, 2008. Bitcoin: A Peer-to-Peer Electronic Cash System.

Kroll, JA et al, 2013. Bitcoin Mining Economics, or Records of Bitcoin, WEIS Conference
with Opponent Attending Sapirshtein A. et al, 2016. Optimal Selfish Smart Strategy in Bitcoin.
International Conference on Financial Cryptography and Data Security

Algorand: developing Byzantine protocol for cryptocurrency