WCG Blockchain White Paper

WORLD CRYPTO GOLD

华克金

Preface

Gold has always been regarded as the highest form of wealth throughout different civilizations, time, race, religions and political communities. It has been in recorded history for over 5,000 years, and will continue to be the most recognized form of wealth or all economic activities in the future, as gold is still considered to have the highest level of liquidity among all existing assets.

From the perspectives of the international market, gold is catching up with long-term bull markets, thus establishing a strong confidence level for institutions and individual investors. Quoting a Chinese Proverb, “To achieve possession of gold, one must first possess gold in the market." In other words, to build a good, diversified gold market, we must let the people understand the significance of gold, and turn it into an important investment tool by financial means.

With the rapid development of the Internet, gold trading is on a brink of a new revolution of wealth. With the advent of the blockchain technology, you will now be able to “swipe your gold” like what you would do with a credit card.

The WCG Global has announced significant progress in the gold trading test based on blockchain technology, and will launch a blockchain-based gold trading product called, "WCG". This will definitely bring trust and value appreciation to the gold spot market.

In the traditional gold market, asset ownership is often opaque. With blockchain technology however, it can provide a "higher level of traceability and auditing" characteristics. It also provides a record of ownership that cannot be tampered, and thus enabling gold ownership to become more transparent, which then provides the trading market with higher liquidity for traders and investors.

The use of a blockchain distributed ledger means that the gold exchange ownership can now be divided into many smaller portions, all of which transactions can therefore be recorded on a distributed ledger.

Traditional gold pricing mechanisms have been to known to have serious problems, a few of which include the issue of transparency, inefficiency and highly susceptible to manipulation. These have brought about a huge obstacle to the development of modern gold trading.

Physical gold preservation and the carrying of it is inconvenient, where the risk is also difficult to justify. However, the long awaited "golden age" of gold possession is now possible with the availability of blockchain technology, which will subvert the traditional gold market.

The gold trading platform based on the blockchain technology is a huge milestone in the gold trading market. Investors will have more trust on "digital gold" as gold pricing system problems would have been eliminated as the authenticity of the assets can be identified, thus expanding the gold market and increasing trading volume.

Not long ago, the Islamic countries financial market issued a new regulation, allowing the Islamic financial market to use digital gold as an investment. This has again boosted the blockchain-based gold platform by opening up a potentially huge market.

Today, WCG investors will no longer rely solely on "paper gold" and "gold reserve bank", but are also able to own gold through the supply of blockchain-based gold products as a solid backing.

Strong market demand and the expansion of options will further improve and increase its liquidity. The process of this virtuous circle has enhanced the function of gold as collateral and trading means. The higher the validity, the greater the value.

Blockchain technology has opened up a new era of digital money. If all gold deals are eventually traded through a blockchain platform, investors can sell in cash or electronic form. The distributed ledger mechanism will enable settlement and the establishment of an asset ownership in an effective timely manner. This will significantly simplify the actual amount of gold savings. As central banks such as People’s Bank of China (PBOC) and Bank of England has become increasingly interested in blockchain technologies and digital money, eventually more and more people will come to explore cryptocurrencies.

Table of Contents

1. 0 WCG：Peer-to-Peer Smart Economic Ecosystem

1.1 Abstract

Bitcoin has proven that a peer-to-peer electronic cash system can indeed work and fulfill payments processing without requiring trust or a central mint. However, for an entire electronic economy to be based on a fully decentralised, peer-to-peer solution, it must be able to meet the following:

1. To process transactions securely, quickly and efficiently, at the rate of thousands per minutes or more; provide incentives for people to participate in securing the network; scale globally with a minimal resource footprint;
2. To offer a range of basic transaction types that launch cryptocurrencies past the core feature of a payment system alone;
3. To provide an agile architecture that facilitates the addition of new core features, and allows for the creation and deployment of advanced applications; and
4. To run on a broad range of devices, including mobile ones.

WCG satisfies all these requirements. It eliminates the massive computing power and competition in Proof of Work (POW). WCG is a 100% Proof of Stake (POS) cryptocurrency.

1.2 Introduction

WCG’s most fundamental innovation is Transparent Forging, which is the core of WCG transformation and innovation that is able to handle an extremely high per second rate of trading volume. Transparent Forging allows the entire network to predict which node will forge the next block so that it can transfer transactions directly and ensure immediate confirmation in the transaction, which eliminates the network speed problem. The way to make money directly through Bitcoin is to predict its future price. WCG has an innovative mechanism to allow the transaction fees to be recycled, that is, all of the transaction fees included in that block of the forging account be rewarded. For the time being, there are only three ways to generate transaction fees: arbitrary messages, WCG transfers and aliases. However as WCG adds more features, each of the WCG accounts that are forged will continue to increase. As WCG has a practical mechanism to get more new features through its voting system, it is hoped that the community would agree to add more promising new features, to correspond to the increase of transaction fees and WCG's real interest rate.

By combining all these features with a scalable framework, WCG has become the foundation of a well-established and mature peer-to-peer economy. From micro-trading, return on investment, open IPO, instantaneous transactions, and with all the things WCG can achieve.

2.0 The Problems of Bitcoin and WCG Solutions

2.1 Blockchain Size

The Bitcoin blockchain is the complete sequential collection of generated data blocks containing the electronic ledger book for all Bitcoin transactions occurring since its launch in January 2009. Four years later in January 2013, the size of the Bitcoin blockchain stood at 4 gigabytes (GB) – about the amount of data required to store a two hour movie on a DVD disk. A year later in January 2014, Bitcoin's blockchain has expanded 300% to 13 gigabytes (GB). The Bitcoin blockchain is undergoing exponential growth and modifications to the original Bitcoin protocol that is required to deal with it.

2.2 Transactions per Day

In late 2013, the number of transactions being processed on the Bitcoin network was peaking at 70,000 transactions per day, which is about 0.8 transactions per second (tps). The current Bitcoin standard block size of one megabyte, generated every ten minutes (on average) by the "full node" clients, limits the maximum capacity of the current Bitcoin network to about 7 tps. Comparing this with the VISA network's capacity to handle 10,000 tps, you will see that Bitcoin cannot compete with VISA as it exists today.

Increasing public use of the Bitcoin system will cause Bitcoin to soon hit its transaction-per-day limit and halt further growth. To forestall this, Bitcoin software developers are working on the creation of "lite node" that employ simplified payment verification (SPV). To handle greater throughput in the same 10-minute-average time, SPV lite node will not perform a full security check on the larger blocks they process. They will instead examine multiple hashed blockchains from competing miners and assume that the blockchain version generated by the majority of miners is correct. According to Mike Hearn, "Instead of verifying the entire contents, SPV just trusts that the majority of miners are honest. As long as the majority is honest, SPV works. However, the full node does give you better security. If you’re running an online shop for example, it makes sense to run a full node.”

2.3 Transaction Confirmation Time

Transaction confirmation times for Bitcoin ranged from 5 to 10 minutes for most of the time in 2013. Since the announcement in September 2017, that banks in China are not allowed to accept Bitcoin, the average Bitcoin transaction time significantly increased from 8 to 13 minutes, transaction hours are filled with uncertainties all the time. China's bank estimated that, there are approximately 650,000 volume of Bitcoin being transacted in one day and the confirmation time can take up to 20 minutes per transaction. As the confirmation time of Bitcoin transaction requires a lot of verification, it is highly time consuming.

2.4 Centralisation Concerns

The increasing difficulty and combined network hashrate for Bitcoin has created a high barrier to the entry for newcomers, and diminished returns for existing mining rigs. The block reward incentive employed by Bitcoin has driven the creation of large, single-owner installations of dedicated mining hardware, as well as the reliance on a small set of large mining pools. This has resulted in a "centralisation" effect, where large amounts of mining power are concentrated in the control of a decreasing number of people. Not only does this create the kind of power structure that Bitcoin was designed to circumvent, but it also presents the real possibility that a single mining operation or pool could amass 51% of the network’s total mining power and execute a 51% attack. Attacks requiring as little as 25% of total network hashing power also exist. In early January, 2014, GHash.io began voluntarily decreasing its own mining power because it was approaching the 51% level. After a few days, the pool’s mining power was reduced to 34% of the total network power, but the rate immediately began to increase again. In the third week of January, the two largest pools of Bitcoin had reached 60% of the total network power.

2.5 Proof of Work's Resource Costs

Transactions' confirmation for existing Bitcoin, and the creation of new Bitcoin into circulation, requires enormous background computing power that must operate continuously. This computing power is provided by so-called "mining rigs" operated by "miners". Bitcoin miners compete among themselves to add the next transaction block to the overall Bitcoin blockchain.

This is done by "hashing" - bundling all Bitcoin transactions occurring over the past ten minutes and trying to encrypt them into a block of data that also coincidentally has a certain number of consecutive zeros in it. Most trial blocks generated by a miner's hashing effort do not have this target number of zeros, so they make a slight change and try again. A billion attempts to find this "winning" block is called a gigahash, with a mining rig being rated by how many gigahashes it can perform in a second, denoted by GH/sec. The first miner who produced the block would receive 25 Bitcoins as reward, with the current price of $25,000 as of 2016. These will be repeated every 10 minutes for miners in order to win the competition. In early 2014, Bitcoin's mining reward was up to $3.5 million per day.

With so many rewards, miners have started a fierce competition in order to increase the probability of winning. At the beginning, Bitcoins were mined using the central processing unit (CPU) of a typical desktop computer. Then the specialised graphics processing unit (GPU) chips in high-end video cards were used to increase speeds. Field programmable gate array (FPGA) chips were used, followed by mining rigs specialised application specific integrated circuits (ASIC) chips. ASIC is the top technology for Bitcoin miners, the competition continues with various generations of ASIC chips now coming into mining services. The current generation of ASIC chip is the so-called 28nm units, based on the size of their microscopic transistors in nanometers. These are due to be replaced by 20nm ASIC units by mid-2014. An example of mining rig would be the "Monarch" 28nm ASIC card from Butterfly Labs, which is to provide 600GH/sec, with electricity consumption of 350 watts, priced at $2100 each. Hashblaster newly launch chip contains of three 20nm ASIC chip, which provide calculated power of 3300 GH/sec, energy consumption of 1800 watts.

The mining rig infrastructure currently in place to support ongoing Bitcoin operations is astounding. Bitcoin ASICs are not smart at all - they are only able to calculate the Bitcoin block and nothing more, but they can perform calculation at the speed of a supercomputer.

In November 2013, Forbes magazine published an article, "Global Bitcoin Computing Power Now 256 Times Faster than Top 500 Supercomputers, Combined!" written by Reuven Cohen. In mid-January 2014, blockchain.info showed in statistics that of ongoing support of Bitcoin operations required a continuous hash rate of around 18 million GH/sec. Within a day of 86,400 seconds, this means that miners in order to find a $3.5 million reward in the block, there will be about 1.5 trillion of block trying to be generated and rejected and it means that there are about 99.99999999% of the Bitcoin’s computing power has not used in the treatment of cancer in DNA models or E.T radio research instead, the computations are totally wasted.

The power and cost involved in this wasteful background mining support of Bitcoin is enormous. If all Bitcoin mining rigs had "Monarch" levels of capability as described above - which they will not until they are upgraded - they would represent a pool of 30,000 machines costing over $63 million and consuming over 10 megawatts of continuous power while running up an electricity bill of over $3.5 million per day. The real numbers are significantly higher for the current, less-efficient mining rig pool of machines actually supporting Bitcoin today. And these numbers are currently headed upward in an exponential growth curve as Bitcoin marches from its current one transaction per second to its current maximum of seven transactions per second.

2.6 Proof of Work’s Resource Costs Pertaining to Coinholders

In addition to massive electrical costs, there is a hidden fee for simply holding Bitcoins. For each block found, the entity that generates the block receives a stipend. At the time of writing, this stipend is 25 BTC, producing 10% inflation in the total Bitcoin supply this year alone. For each USD$1,000 worth of Bitcoin someone owns, that person is paying USD$100 per Bitcoin this year to "pay" miners for keeping the network secure.

3.0 WCG Solutions

3.1 Cryptographic Foundations

Key exchange in WCG is based on the Curve25519 algorithm, which generates a shared secret key using a fast, efficient, high-security elliptic-curve Diffie-Hellman function. The algorithm was first demonstrated by Daniel J. Bernstein in 2006.

Message signing in WCG is implemented using the Elliptic-Curve Korean Certificate based Digital Signature Algorithm (EC-KCDSA), specified as part of IEEE P1363a by the KCDSA Task Force team in 1998. Both algorithms were chosen for their balance of speed and security for a key size of only 256KB.

3.2 Encryption Algorithm

When Alice sends an encrypted plaintext to Bob, she:

1. Calculates a shared secret:

- shared_secret = Curve25519 (Alice_private_key, Bob_public_key)

2. Calculates N seeds:

- seedn = SHA256 (seedn-1), where seed0 = SHA256(shared_secret)

3. Calculates N keys:

- keyn = SHA256 (Inv(seedn)), where Inv(X) is the inversion of all bits of X

4. Encrypts the plaintext:

- ciphertext[n] = plaintext[n] XOR keyn

Upon receipt Bob decrypts the ciphertext:

1. Calculates a shared secret:

- shared_secret = Curve25519(Bob_private_key, Alice_public_key)

2. Calculates N seeds (this is identical to Alice’s step):

- seedn = SHA256(seedn-1), where seed0 = SHA256(shared_secret)

3. Calculates N keys (this is identical to Alice’s step):

- keyn = SHA256(Inv(seedn)), where Inv(X) is the inversion of all bits of X

4. Decrypts the ciphertext:

• plaintext[n] = ciphertext[n] XOR keyn

Note: If someone guesses part of the plaintext, he can decode some part of subsequent messages between Alice and Bob if they use the same key pairs. As a result, it is advised to generate a new pair of private/public keys for each communication.

3.3 Blockchains

As in other cryptocurrencies, the ledger of WCG transactions is built and stored in a linked series of blocks, known as a blockchain. This ledger provides a permanent record of transactions that have taken place, and also establishes the order in which transactions have occurred. A copy of the blockchain is kept on every node in the WCG network, and every account that is unlocked on a node has the ability to generate blocks, as long as at least one incoming transaction to the account has been confirmed 1,440 times. Any account that meets these criteria is referred to as an active account.

In WCG, each block contains up to 255 transactions, all prefaced by a 192-byte header that contains identifying parameters. Each transaction in a block is represented by a maximum of 128 bytes, and the maximum block size is 256KB. All blocks contain the following parameters:

- A block version
- A block timestamp, expressed in seconds since the genesis block
- The ID and hash of the previous block
- The number of transactions stored in the block
- The total amount of WCG transaction volumes in the block
- The total amount of transaction fees in the block
- The payload length of the block
- The hash value of the block payload
- The account's public key generated by the block
- The block's generation signature
- A signature for the entire block

Each block on the chain has a "Generation signature" parameter. Activate the account with its own private key to sign "Generation signature" on the original block. This produces a 64-byte signature, followed by SHA256 hash column for the signature. The hash generated by the first eight bytes gives a number as a "hit". The "hit" is compared with the current target value (which is a 64 bit number). If the calculated "hit" value is lower than the "target value", then the next block can be generated.

Thus, the "Proof of stake" algorithm is generated because the "target value" is proportional to the balance it confirms for each activation account. An account holding 1,000 coins has a target value of 50 times the target value of a 200-dollar account. Thus, the number of blocks produced by holders of 1,000 coins is more than 50 times (from a long-term perspective) of those who hold 20 coins.

The "target" value is not fixed. With the passage of the time of the previous block, it is growing every second. If there is no account in the first second of the "hit" and the value is lower than the "target" value, then the next second target value will turn. The "target" value will continue to double until the "hit" value of an active account has a lower value. There is also a "base target" value set to the target value at intervals of 60 seconds. It is for this reason the average time for a block will be generated within 60 seconds. Even if there are only a few active accounts on the network, one of them will eventually produce a block because the "target" value will become quite large. By comparing the "hit" value of your account to the current "target" value, you can estimate how long you "hit" value will be successful.

When an activation account wins the right to generate a block, any available and unacknowledged transactions can be placed in the block and the block is filled with all the required parameters. Then the block will be propagated to the network as an alternative to the blockchain.

The load value, "hit" in each block, the generated account, and the signature can be acknowledged by the node on the network that receives it. Each block refers to the previous block, and the block-formed blockchain can be used to trace to the history of the transaction that is known to the network, all of which can be traced all the way back to the genesis block.

3.4 Transactions

Calculating the balance of each WCG account requires to scan the entire blockchain. Although this sounds very inefficient, it is not a big amount of computation for the current network and CPU speed. Working with these tasks requires lower energy consumption and therefore mobile devices can also become a node for WCG.

Details of the WCG transactions are shown below:

1. The sender specifies the parameters of the transaction. There are many types of transactions (sending coins, creating aliases, sending information, issuing assets, or placing orders on assets), but several parameters for any transaction need to be specified.

- Send user's password
- Transaction fees
- Transaction deadline
- Random "reference" transactions

2. The input values for all transactions are checked. For example: Mandatory parameters must specify: transaction fee must not be less than zero, the transaction deadline must not be less than one minute.

3. If the results of the verification of the parameters appear as expected:

- The public key of the generated account is calculated by the provided password.
- The account information for the generated account can be restored and the transaction parameters should be further validated.
    1) The balance of the account sent cannot be zero
    2) The confirmation balance of the sending account cannot be less than the sum of the transaction amount and the transaction cost
- If the trading account has sufficient funds to provide for the transaction amount
    1) It generates a new transaction whose type and subtype value are set to match the type of transaction that has been generated (send money, create alias, send message, etc.) All specified parameters are included in the transaction object. The only transaction ID is also produced with the creation of the object.
    2) The transaction is signed with the key to send the account.
    3) The encrypted transaction data is placed in the information, which is used to guide the network node to process the transaction.
    4) The transaction is sent to all nodes on the network.

4. The server feedback with a result code: the transaction ID, if the transaction is successful; if the parameter validation fails, it will feedback error code and error message.

3.5 Transactions Confirmation

All WCG transactions are considered "unconfirmed" unless they are already included in the active network block. Newly created blocks are distributed to the network by creating their accounts. And the transactions contained in the blocks will be confirmed. Because the subsequent blocks are added to the existing blockchain; therefore, each additional block will be added to the existing transaction to confirm once again.

After 10 confirmations, the WCG transaction is considered credible. If there is a problem, the network may reorganise the recent 720 blocks, so a transaction is irreversible after 721 confirmations. A transaction is considered to be eternal transaction after it has been confirmed 1440 times.

3.6 Proof of Stake (POS)

In previous obsolete POW models, cyber security has ensured by the "work" of the nodes, and they borrowed their resources (computer/processing time) to strengthen the network and prevent malicious attacks. These nodes are rewarded for some of the coins because of their "work", and these numbers and their duration are based on a particular network. The drawback of this approach is the need for more and more time to deal with (and the continuous energy) because as time goes by, the designated node to support the operation of the network is particularly important.

In other words, as the network grows faster, the enthusiasm of individual nodes to support the network is getting lesser because their potential bonuses are divided by more and more nodes. Some nodes continue to invest in resources with professional, proprietary and expensive hardware, and increase energy consumption. As time goes by, it is ironic that the network will become more centralise, and smaller nodes (very small nodes) will quit because their bonuses will flow to larger nodes (for those who can afford of more resources and energy of the node).

Speaking of this point, the recent calculation of the GHash.io mining pool has been very close to 51% of Bitcoin computing power. In this case, the blockchain has been controlled by a single individual, and the concept of centralisation has completely disappeared. In the POS model used by WCG, the security of the network is maintained by nodes with "shares".

3.7 Network

WCG's network is made up of nodes. A node is essentially a device that contributes to the network. Any device that runs WCG's client (WCG Reference Software) is a node, and because the source code can develop costly local clients, they also become nodes. Nodes can be divided into two types: "marked" and ordinary. Each marked node inherits the weight of the WCG based on the marked account, which can be only 1 WCG, or 5 to 10 million WCG, with no upper limit. The greater of weight of marked node, the higher the credibility.

If an attacker wants to mark a node in order to obtain the credibility of the network, and then use this credibility to attack, access to the obstacles (consumption of WCG) will limit such abuse. Once the voting system is implemented, other nodes can initiate a vote to ban or punish malicious nodes on the network.

3.8 Transparent Forging

In order to understand the transparent forging, we must first understand the process of forging. For an activated forged account, the opportunity for forging to the block is proportional to the number of WCG it holds and the number of activated WCG on the network. Also, a certain degree of randomness is required to eliminate the relative to the known forging of the attack, relatively to be as accurate as possible to reduce the use of network bandwidth.

The rule of thumb determines the amount of block that an account can forge up to every day (account balance/1000000000)*1440. The assumption is that all WCG are forging and 1400 blocks generated per day. However, the two changes in the data within a day are big.

Since the forging opportunity can be calculated, it is possible to expect which account to forge the next block with and when to forge it. As the hit value has been determined, people with multiple accounts can calculate which account is most likely to forge the next block, so you can transfer all the WCG to that account. This is why you want to choose a valid balance rather than an actual balance. The time delay for an account to be credited and the time delay in the transfer of funds will reduce the effective number of WCG attacks.

By storing the hit value from all accounts, if each node knows which account is actively forging, it is possible for all nodes to predict which account will forge the nearest block.

Because each node has a different network topology based on the visible node and the changes in forged account activation, it is not 100% accurate as this is only a pre-design. Of course, some of the wrong factors are needed to prevent an attacker from attacking the WCG network by calculating the nearest block forge. As long as the prediction accuracy is close to 100%, the problem of network congestion will be reduced, thus allowing thousands of real-time transactions.

Transparent forging allows centralised operations in a decentralise network. This is the most basic breakthrough of WCG. Transparent forging allows each user client to automatically decide who will produce the next block, and then they can send their transactions to that node. In order to achieve real-time transactions, an additional fee is allowed. Another important feature of transparent forging is its outstanding security of the protocol, which can temporarily reduce the forging capability of nodes that produce one block to zero.

This feature is designed to prevent nodes with 90% WCG from diverging. Therefore, if a node has 90% of the WCG and does not plan to generate the block, the system will temporarily reduce its forging ability to 0 to prevent possible forging. Its forging ability is allocated to the remaining nodes in the network, so the capacity of the network is still 100%. Therefore, regardless of what the potential opponent does on other diverge, it will be offset by a high-level consensus mechanism (not yet disclosed).

What does transparent forging mean? It means that everyone can predict (great chance) who and when will the next block. This gives WCG a lot of advantages:

1. The transaction can be sent directly to the forging of the next block (if he is willing to disclose its address on the network), thus saving the transaction traffic and quickly approaching the VISA / MasterCard transaction volume.

2. Blocks can be generated in advance and sent to most of the forgers before they take effect (timestamps), thus reducing the probability of isolated blocks to a large extent.

3. It is possible to predict the future block time (block rate), it is possible to set the appropriate fee to ensure that the important transaction can be quickly confirmed (do not spend too much in a block).

4. Perhaps most importantly, the network can detect who are not involved in the block generation and take appropriate measures.

As a 100% POS cryptocurrency, WCG can prevent the intervention of government and obtain more from ASIC consortium, and having transparent forging characteristic, and even can prevent some people from buying the majority of such cryptocurrency. So what exactly does WCG become the next generation of currency? It is not only its beautiful features, such as a decentralised deal, a DNS, or a centralised app store, but a transparent forging mechanism that contributed to it.

3.9 Transaction Fees

The transaction fee is how WCG is recycled to the network. The existing transaction funds are generated by sending WCG, creating an alias, or sending a message.

The transaction fee is currently set to pay at least 0.01 WCG at a time, until the number of transactions is filled with a block. And with the increase in WCG prices, the minimum transaction fees will be reduced to the user acceptable level. The transaction fee for Bitcoin is 0.0001 BTC, and the transaction fee will become more and more unrealistic as the price of Bitcoin increases. With the rise in WCG prices, transaction fees will gradually decrease, WCG will be very suitable for micro-payment. By that time, even if smaller units such as milli-WCG, micro-WCG and even femto-WCG are needed, we can issue colored coins to represent anything.

3.10 Recycle disk space

The expansion of the blockchain is a great deal, it is related to any cryotpcurrency, especially for those who trade a lot like WCG. Often, the operations added to the blockchain are charged according to the size of the space they are using, which is also intended to limit the node's intentional expansion of the blockchain.

However, as time goes by, it is inefficient to recalculate all the content from the source block. WCG plans to conduct annual checkpoints, which will create a starting point for all nodes to use, the frequency of which allows WCG shareholders to vote. By using an electronic signature, the validity of the annual checkpoint can be ensured. A network node with more resources (such as a dedicated server) can continue to support the entire blockchain and be rewarded as a service provider.

For example, on mid-2012, Bitcoin's blockchain is still remained within 1GB. And now, with the increase popularity of Bitcoin and more transactions, the blockchain has expanded to nearly 13GB in size. Obviously, it is not feasible for the vast majority of devices to provide such a large capacity of blockchain. Even if the entire chain of transmission will take a lot of hours, but it also depends on the network connection speed.

3.11 Device Portability

Because it is a Java code, a POS hash column, and ability to trim and reduce blocks, WCG is well suited for running on small and low-power devices. Android and Apple's applications are also being developed, and WCG client has been running on low-power ARM devices, such as RaspberryPi.

Applying WCG to low power or networking equipment is easy, for example, in smart phones. These devices support most of the network. Because millions of people around the world already have smart phones, WCG can quickly get applications in these devices to support the network without having to spend a lot of money as traditional cryptocurrencies.

WCG features, such as instantaneous trading, make smart phones an ideal platform for everyday use in the use of WCG (food, fuel, etc.). In this area, other cryptocurrencies also have solutions (such as Bitcoin), but because of the large amount of resources needed to maintain the network, the use of these devices does not help the health or stability of the network. For WCG, any device that has the ability to send and accept transactions and has a certain amount of computing power can increase the stability of the network and decentralization.

4.0 WCG Creation

4.1 WCG Creation (Forging)

The opportunity to forge a block depends on the base target value Base Target (same to everyone), time since the last block (same to everyone), and user account balance.

$T = Tb \times S \times Be$

where:

T is the new target value

Tb is the base target value

S is the time since the last block, in seconds

Be is the effective balance of the account

4.2 WCG forging calculation

We discuss WCG's forging mechanism from the perspective of probability theory, calculation of several important parameters, such as the possibility of an account forging to a block, an account forging to the longest sequence of consecutive blocks, and the possibilities of current blockchain is better than others.

5.0 WCG Features

5.1 Alias System - Similar to DNS

5.2 Arbitrary Messages - Anyone can send any form of information

5.3 Asset Transactions - Currency / Stock Trading

5.4 Distributed Computing

5.5 Distributed Storage

5.6 Instantaneous Trading

5.7 Mixed Service

5.8 Multiple Signatures

5.9 Service Providers - Services outside the blockchain

5.10 Reduction - Reduced expansion of the blockchain

5.11 Smart Contract

The expectation of a smart contract is to embed the contract in a valuable and electronically controlled asset. WCG's contract only can be used to distribute distributed autonomous organisation DACs. DAC can be used as WCG pool.

5.12 Two-way payment

5.13 Voting system

The most important thing for WCG's scalability is the ability to add new features. The new feature makes WCG more dynamic and attracts a larger user base. It is also highly anticipated that the more features that are added, the more transaction fees will be created - the increased enthusiasm for forging, and thus the security of the network. To achieve this, WCG has established a voting system that allows the community to vote to determine which characteristics should be implemented and what order to implement. But the voting system itself is not a rigorous technological innovation, because it is possible for each region to be implemented - but WCG has implanted it into the system, hoping to become a reality soon.

Anyone can vote according to their own needs. The person who initiates the poll must determine the voting content and the voting period (associated with the number of blocks). Users can use it to solve all the problems, such as selecting a new icon. Adding new features must be decided by voting by WCG shareholders. Shareholders can also vote for the decision to alias transfer and WCG smaller units. You can also vote to decide to destroy (freeze) specific coins, especially thieves or hackers' coins. Or even through the main vote to decide to stop malicious attacks on the node. Furthermore, the community can vote to decide whether or not to initiate a vote to consider individual users or nodes.

Voting is based on the number of WCG held by the calculation. Users with larger trading accounts have greater voting capacity in this system. In order to prevent this situation, the network needs to have a healthy number of trading accounts for the user to choose from. In addition, with the implementation of decentralised transactions, the centralised problems in voting system can be resolved.

WCG's voting system is one of the important components of the decentralised currency. There is no leader here, no centralised entity, all decisions are determined by the democratisation of the vote. In addition, in order to solve the global problems, the voting system can also be used by asset shareholders for asset trading functions. It can help the assets shareholders to reach a consensus.

5.14 The total number of WCG's

The total amount of WCG's total coins is 900 million, of which 600 million are distributed in multiple re-signature repositories, which will be distributed by WCG Global to all the accounts of gold collectors, for a reliable decentralised asset management transactions. In addition, there are 300 million WCG as a reserve income, each eligible account must have at least 100 WCG. For each 172,800 blocks (about 120 days), each account will receive an additional 3% of the proceeds. This design in addition to attract collectors, while ensuring the rewards of the supporters, effectively control the flow of the market, creating a long-term value protection. WCG definitely has greater advantages as compared to other cypto assets!

6.0 Conclusion

WCG will bring revolution to the electronic economy, as they will replace a large proportion of global GDP. With all the strong features to consolidate it together, WCG is able to become the top digital investment tool. Bitcoin investment and development is based on blockchain 1.0, and its return on investment is massive. But with the coming of more and more cryto-products, Bitcoin is no longer the sole digital asset. In the coming days, the investment in innovation agreements and blockchain applications will be the hot topic. An investment with 10 times or even 100 times return on investment opportunities is achievable so long as the investor is able to spot on the valuable digital assets with good growth potential. With solid gold as the backing, WCG will be the most promising investment in the digital asset market.

Bitcoin has created a lot of legend, and the next would be WCG.

WCG

WORLD CRYPTO GOLD

华克金