CGA COIN
WHITE PAPER V1.1

Version 1.1

Initial Draft : June 2019
Final Edit : May 2020

www.cgacoin.net

CGA COIN (CGA) White Paper 1.1

Cryptocurrency

For past few years, the biggest topic among investors and creative programmers including software developers must be blockchain. And the real initiator who enabled emphasis on blockchain based on the technology is a cryptocurrency which is based on the blockchain.

Exponential market expansion and investment boom of cryptocurrency is as big as any economic and social phenomena we have experienced. For the movement of the real economy, the social impact of cryptocurrency which is led by Bitcoin, affects how capital is invested and all forms of investment transactions. It is now a reality, not a phenomenon.

With a new computing system called blockchain and the future it pursues, it has been considered a turning point of network which can be labeled as a revolution. Cryptocurrency has become a driving force that rapidly drives the development speed and verification of the value of blockchain technology.

However, other than its positive aspects, negative phenomena which are different from the core purpose of cryptocurrency have occurred as well.

For example, Bitcoin's advantages including fast transmission speed, fee restrictions, decentralization and P2P transactions which are all pursued by cryptocurrency have become ineffective, and the stakes of the ecosystem have been unequally distributed in proportion to the size of capital and resources.

Even in the collapsed ecosystem, many only have prioritized technological and informational values of the future that pursue economic benefits rather than physically proven values. As a result, problems of imbalances, such as unnecessary resource consumption and damage from speculation have occurred.

For a short period of time, numerous coins and tokens have been issued. They have been criticized for being a fictitious value market because future businesses with unforeseeable results are misrecognized as special value that can succeed only because it uses blockchain.

The direction that CGACoin pursues returns to the origin of the reason for the birth of cryptocurrency using blockchain technology. And it presents alternatives based on the problems we have learned in the ecosystem until now.

Problem

Absence of practical use

It may be considered that the current Bitcoin has proven the reality and future value of blockchain technology, and as a result, some of the goals pursued by the developer have been accomplished. However, the question of the practical use of cryptocurrency remains a challenge.

Where can I use it? Can I actually use it? Is it useful? Efficient? Do we really need it? We need practical answers for such questions.

Structural limit

Each block of Bitcoin can only store limited amount of data, and it means that Bitcoin can only process the transactions as much as stored amount of data per second. Creation of the blocks has become a product which have made the block itself into an unequal product.

Problems of mining

For blockchain, mining (proof-of-work) and rewards for mining have been a means for individuals in the blockchain to form blocks with good will and accelerate the development of the P2P system.

However, the mining compensation system which should act upon decentralization, has been dominated by few specific groups with powerful computing power, and it caused problems such as high fees and slow proof-of-work. In addition, the proof-of-work (POW) used by several coins has been consuming lots of increasingly meaningless and inefficient power.

Limits of scalability

Large platforms have contributed a great deal for increasing accessibility of cryptocurrency and blockchain development and lowering the entrance barrier. However, each token and DAPP developers are bound to the limits of the platform they belong to.

For Ethereum, instability in the supply of 'Gas' used for transaction fees has led to difficulties in DAPP development. In some ways, even in EOS platforms which is more advanced, the fluctuation of RAM prices is considered as obstacles in DAPP development and operation.

Speculation

In a situation where capital power had already affected the hash power, the recognition that the value of blockchain technology was equal to cryptocurrency has led to sharp increase and decline in the market value, and it has resulted in hindering its growth as a practical function of the currency.

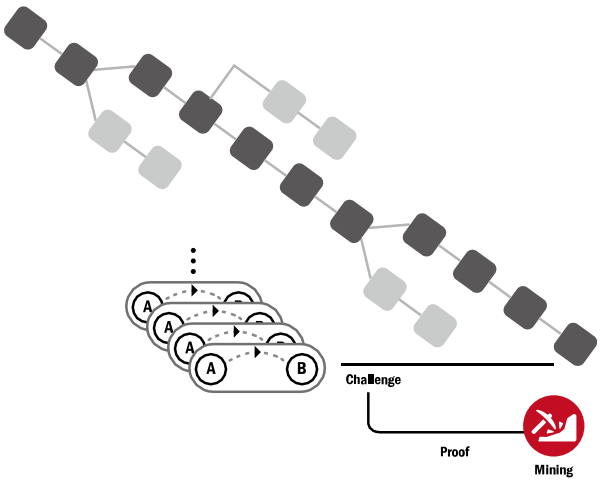
CGA Coin

As a means of value exchange, irreversible characteristics, forgery-proof as well as fast transaction speed, optimization of P2P transactions, selective anonymity, and transparency of transaction details are the core of CGA Coin blockchain technology.
It can be understood that all technical requirements for long-term persistence and the role of cryptocurrency are equipped thanks to the addition of technology optimized for integration with the ecosystem.
Raiblock introduced by Nano, shows irreversible uni-directionality by using DAG algorithm. At the same time, with a method of verifying multiple blocks in one block, it has the advantage of being differentiated from existing blockchain.

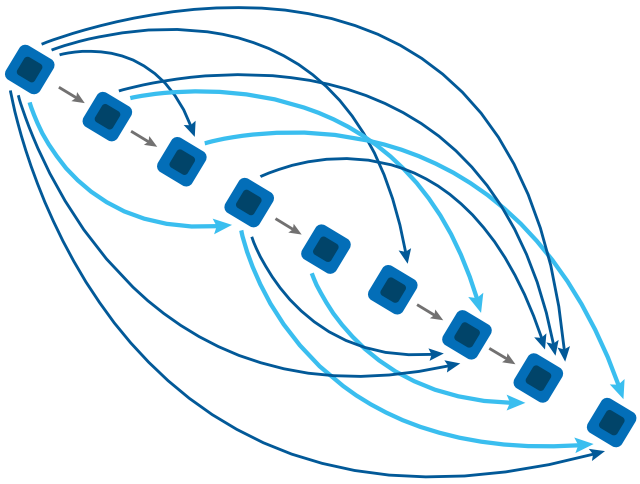
First, let us explain the excellence of DAG algorithm based on CGA Coin.

DAG (Directed Acyclic Graph) Algorithm

DAG algorithm is the core algorithm of the block lattice technology that enables the fastest transaction while conforming to the uni-directionality and non-circularity, which are the blockchain's technical definition.
With following Figures, let's take a look at two structures of blockchain.



[Figure 1] General blockchain structure



[Figure 2] Blockchain structure using DAG algorithm
DAG does not have circulating cycle. It only shows uni-directionality for a certain direction.

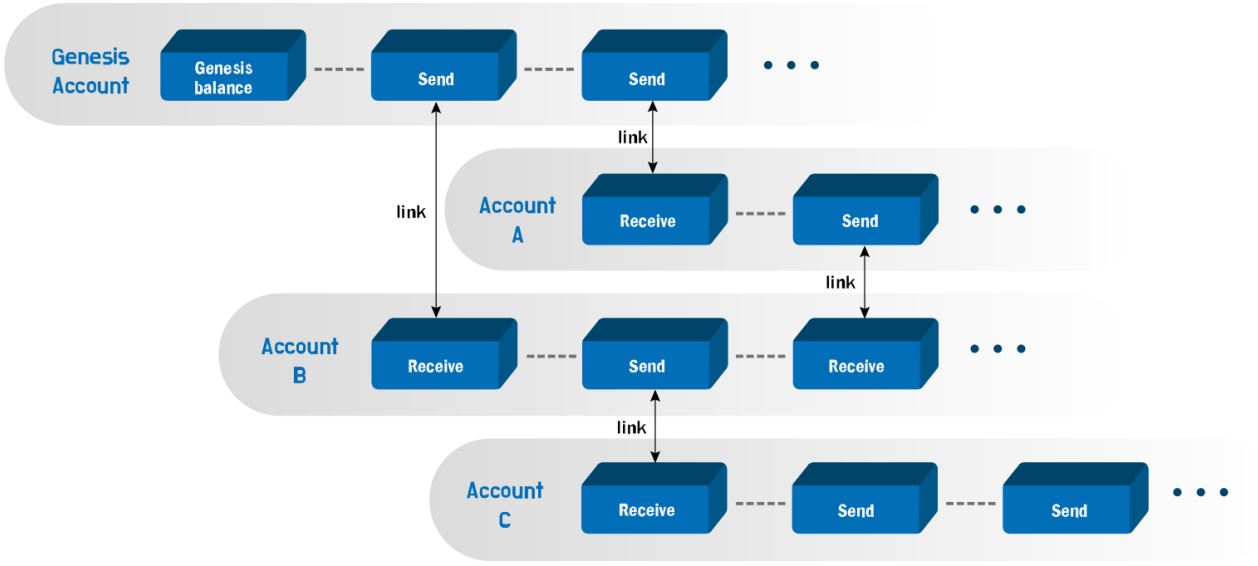
As indicated in above Figures, once a block is created, it does not allow another block to be created. It shows that all processes connecting the chain are performed in parallel at the same time.
DAG algorithm is a method in which an arrow indicating transaction processing has a certain direction, and a single transaction verifies another transaction without creating a cycle.
Since the generated block immediately verifies the next block, the transaction processing speed has become faster exponentially. In addition, as transaction request increases through parallel and asynchronous nature, bottleneck issue that delays transaction approval does not occur. It is an advantage for the popularization of blockchain technology.

Block Lattice

CGA Coin uses block lattice technology different from the blockchain technology used by most cryptocurrencies. Conventional blockchain cryptocurrencies are all listed and connected to each other in a row. To join the row, cryptocurrencies compete against each other using hash power, and only blocks adopted through the entire consensus process join the listed blocks to be chained. Such process leads to delays in synchronization between nodes, and causes delays in transaction time, unnecessary energy waste used to join the chain, and increased fees as a result.
When sending CGA Coin to another account using block lattice technology, the following two transactions take place.

1 SEND Block	Transaction deducting the remittance amount from the sender's account
2 RECEIVE Block	Transaction increasing the recipient's account balance.

[Figure 3] below expands the part of above DAG algorithm [Figure 2] and explains.
All account ledgers minus the Genesis account, begin from SEND block derived from the Genesis account block and RECEIVE block that receives and processes it, and vertically extend account-chain in their accounts.



[Figure 3]

Simple looking lattice-shaped ledger and block system enable various facts and technical verification. Each account created and started by linking SEND block and RECEIVE block of Genesis ledger has its own blockchain that cannot be changed by anyone. And it directly connects to the target account to send and receive transactions only when a transaction occurs. It refers that each block does not need to compete for adoption using hash power, and it enables amazingly fast transaction process.
Each transaction occurs individually in the blockchain of the account that the sender and the receiver hold arbitrarily, and the incoming transactions are ordered and processed asynchronously. Because only blocks related to incoming and outgoing in each blockchain are

created and stored in the ledger, transactions with a small size suitable for UDP packets and data capacity are possible and it can minimize storage and network usage.
In addition, as explained above, ledgers of all accounts begin from Genesis account. The genesis balance was a fixed quantity and can never be increased. Because another ledger is created from a remittance transaction derived through Genesis account chain, the sum of the total balances of all ledgers will never exceed the initial genesis balance.

Use of UDP protocol

Protocol of CGA Coin is extremely light. Each transaction fits in minimum UDP packet size for transmitting to internet. Hardware requirement to execute nodes also is minimized, because nodes only record and retransmit blocks for most transactions.

dPOS

Pos (Proof-of-stake) has been introduced to improve inefficiency of PoW which consumes enormous amount of energy, and it reduces energy waste of PoW and replaces miners with verifiers. According to the stakes they own, they have rights to verify the blocks and vote. In other words, accounts with more stakes have more voting rights and priorities. PoS shuns wasteful calculation capability competition, and it only requires lightweight software which operates in low-spec hardware.

Further, CGA Coin has selected dPoS method which allows delegation of voting right exercise to other account. It is almost similar to PoS, however, it has improved its downside which requires online status at all times to exercise voting right of the stakeholders. As long as prearranged delegation in online, stakeholders can always exercise voting rights equally even the holders are offline.
Delegations can only vote per delegated stakes, and other than the voting rights, they do not have rights to access the delegating party's account or transaction of balance.
PoW method has been used partially as a part of proof of work method. This, unlike Bitcoin, is only used for means of preventing SPAM, and calculation is completed within few seconds. Since even this is pre-calculated using the information of the last sent transaction, it is difficult to notice at the end-user level and looks just like it is processed immediately.

Centralization of computing power and assigning a Representative

As we configure CGA Coin system, we have selected centralization of computing power to maintain technical value at higher performance and stabilize the ecosystem where coin is used. As CGA Coin directly manages computing power for main net and PoW and operates full nodes, business activators and users do not have to operate or maintain nodes directly. Further, it does not require consumption of resource or large storage space.

Delegation of each account is appointed as a lead node that is directly managed by CGA Coin, and it maintains performance of main net and speed of network storage at certain level while maintaining the account user rights and guarantees stability of blockchain nodes and fast transaction speed.

This is a temporary measure until stabilization of network speed and computing power is accomplished above a certain level anywhere in the world.

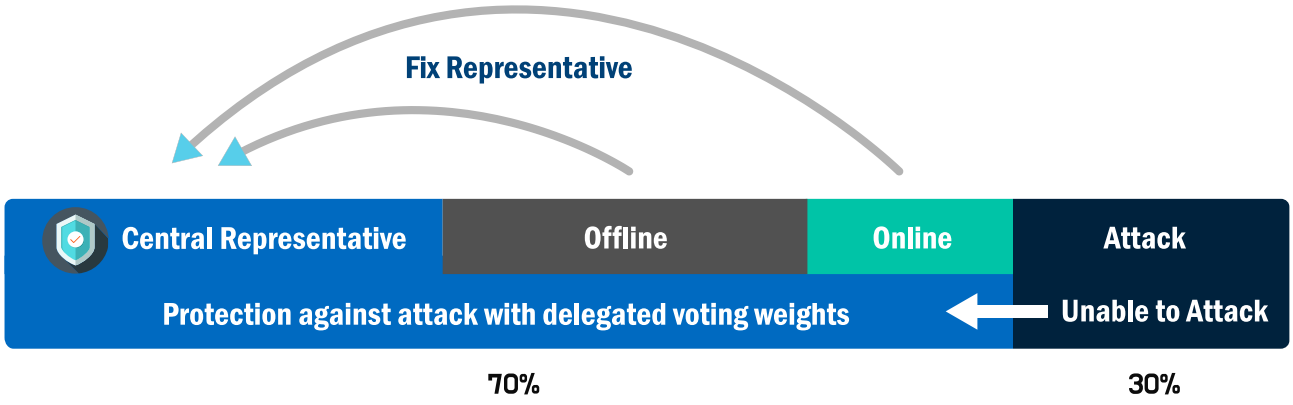
As mentioned above, each account can assign a representative who can vote on the account's behalf while they are offline and can quickly and easily change to a new representative at any time.

```
...
mdb_dbi_open (env.tx (transaction), "pending_v1", MDB_CREATE, &pending_v1) != 0;
mdb_dbi_open (env.tx (transaction), "blocks_info", MDB_CREATE, &blocks_info) != 0;
mdb_dbi_open (env.tx (transaction), "representation", MDB_CREATE, &CGArepresentation) != 0;
mdb_dbi_open (env.tx (transaction), "unchecked", MDB_CREATE | MDB_DUPSORT, &unchecked) != 0;
mdb_dbi_open (env.tx (transaction), "checksum", MDB_CREATE, &checksum) != 0;
```

Example of code edit to fix delegation appointment method.

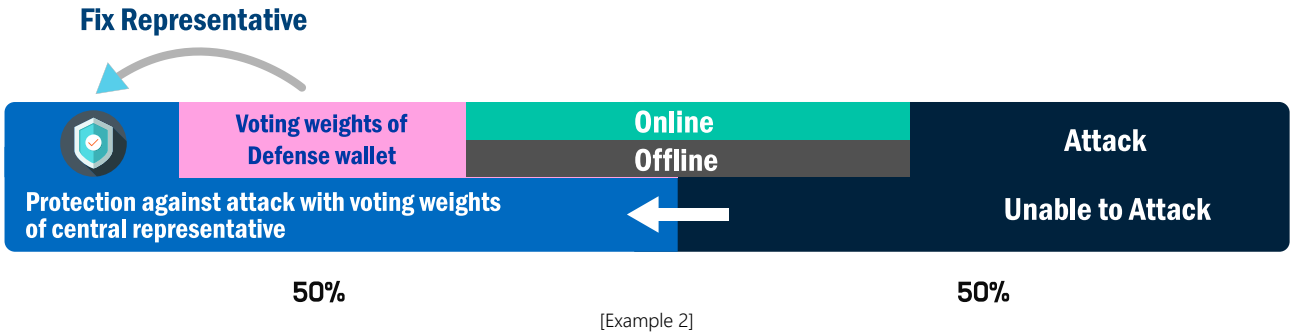
Protection against >50% Attacks through changes in delegation appointment

Delegation appointment method as above can easily respond to attacks called >50% among many risk factors. There can be many types of attacks, but it is as below if we imagine a few scenarios. Below scenarios explain the most extreme and meticulous methods where >50% attack can take place in a diagram.



[Example 1]

[Example 1] If there are offline and online accounts in which the voting rights are delegated to the central delegation accounts under CGA management, and an attack is attempted using the majority of the stakes using the remaining stakes, the attack has no chance of succeeding because the central delegation accounts have already been delegated the majority of the voting rights.



[Example 2]

[Example 2] If an attacker attempts to attack by purchasing unspecified on/offline stakes after system stabilization and the restriction on agent fixation was lifted, the attacker's possession of 50% or more is completely blocked by the defense wallet issued for defense at the time of coin issue.

Use of CGA

We are trying to dramatically solve the problem where most coins and platform tokens have not reached the creation of direct value and practical use. In all examples of use below, characteristics of blockchain where hacking or forgery is not possible is maintained. As a result, each business model can experience excellent scalability and stability.

Means of Value Storage

The characteristics of the value of the coin can be specified and used as volatility, minimum volatility, stability, etc.
Through the link with payment guarantee system per nature of the business being used, it can be used as a stable coin, half stable coin, minimum guarantee coin, and bonus reward coin.

Value transfer medium

Transferability of CGA Coin for the basic feature of cryptocurrency is superb.
For now, it can process at least 18,000 transactions per 10 seconds, and for maximum, it processes 6,000 transactions per second. Such performance is equal to the performance of most financial system based on data transfer financial system. In addition, it can be improved in proportion to physical capability of the system and development of the circuit.

Payment method

With a simple application installation, users can use general purpose wallet for payment for goods or service, and transaction history can also be verified. It can be used for payment in online and offline shopping as well as donation or fundraising for less fortunate neighbors, and equal level of stability to general financial transaction can be easily adopted.

Use in game

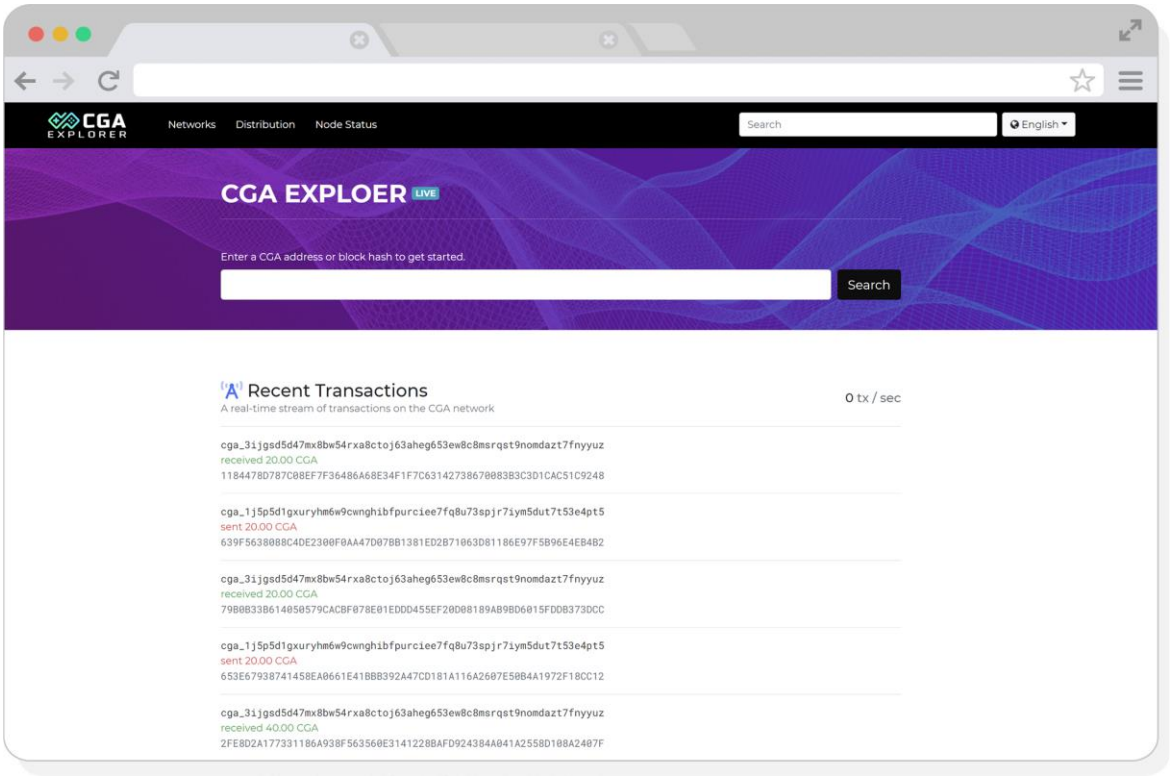
Combination of the game and blockchain coin makes it easy for users to pay or donate fees for the service to the creator of the content. As a result, it can become a medium for game developers to enter the market easily.

Future update

For the improvement of performance and features, both nodes and wallets are continuously updated, and block explorer feature update is scheduled. For nearly perfect protection, upgrade of encrypted protocol is under review, and the efficiency of improving security against the decrease in processing speed from the update is intensely under test.

CGA Block explorer

Through CGA node explorer (**https://www.cganode.com**), anyone can see and verify all activities of CGA network. When a user enters and searches CGA account or hash value, detailed block information regarding the account and transaction history is available.



CGA Coin Wallet

Official CGA wallet application

It is available in both iOS and Android app stores for all users for immediate account creation and use.

- CGA Coin is an edited cryptocurrency which has been hard-forked from << NANO (https://nano.org) >>
- At a github linked in the website (https://www.cgacoin.net), entire CGA node sources are available.