



JCOIN

WHITEPAPER

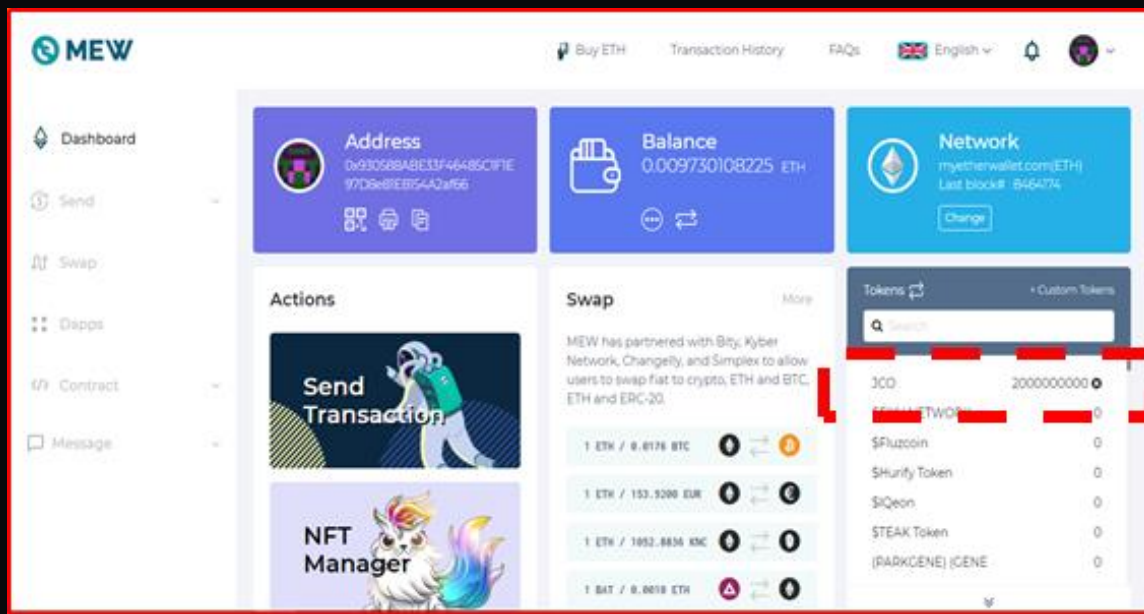
Ver 1.0

Consumer market shopping mall-based
Purchase reward type digital payment
point blockchain token

Table of Contents

- 1 Properties of J-COIN
- 2 J-COIN's E-Wallet
- 3 J-COIN's operating concept
- 4 J-COIN allocation structure
- 5 Technical background of J-COIN
- 6 J-COIN's policy
- 7 Future technology reflection
- 8 Reference
- 9 Legal notice and liability limitation

1 Properties of J-COIN



[Fig. 1. J-COIN's initial establishment E-Wallet-Address
0x930588ABE33F46485C1F1E97D8e81E8154A2af66]

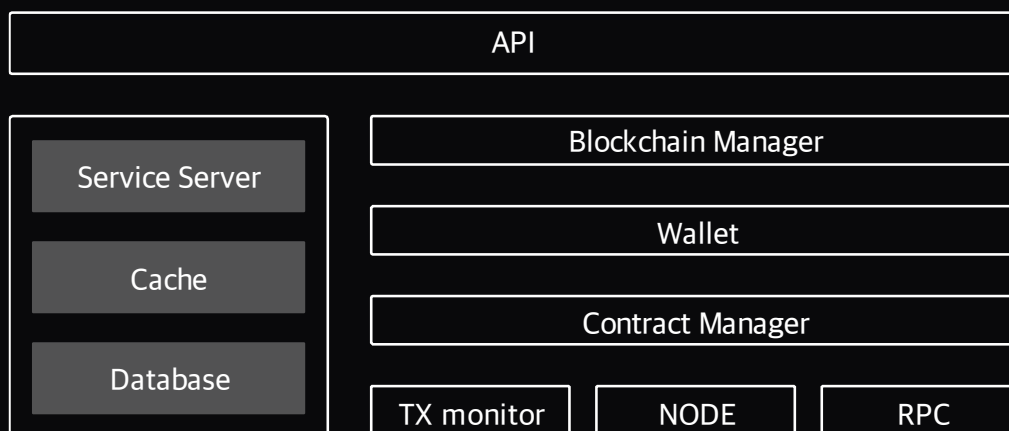
J-COIN complies with the ERC-20 standard and has the following properties.

- ✓ Basic system: Ethereum (Ethereum) blockchain (ERC 2.0 standard)
- ✓ Name: J-COIN, Symbol: JCO
- ✓ Supply: A total of 8 billion (8,000,000,000) J-COINs issued
- ✓ Balance: Announced to Ethereum
- ✓ Account: Use of Ethereum address
- ✓ Mining: Shopping mall jmall.bz linked type
- ✓ Owner: Multi-signature wallet
- ✓ Special agreement: The issuer of J-COIN does not issue additional coins arbitrarily but may issue additional coins, approve the purchase of J-COIN, and sell J-COIN after notification according to market trends.

2 J-COIN's E-Wallet

J-COIN E-Wallet is a space to store coins and can handle all financial commerce activities such as purchase, use, and transaction on the Ethereum blockchain, and the smart contract is illustrated in the bottom layer.

J-COIN Layer



[J-COIN's upper/lower layer structure]

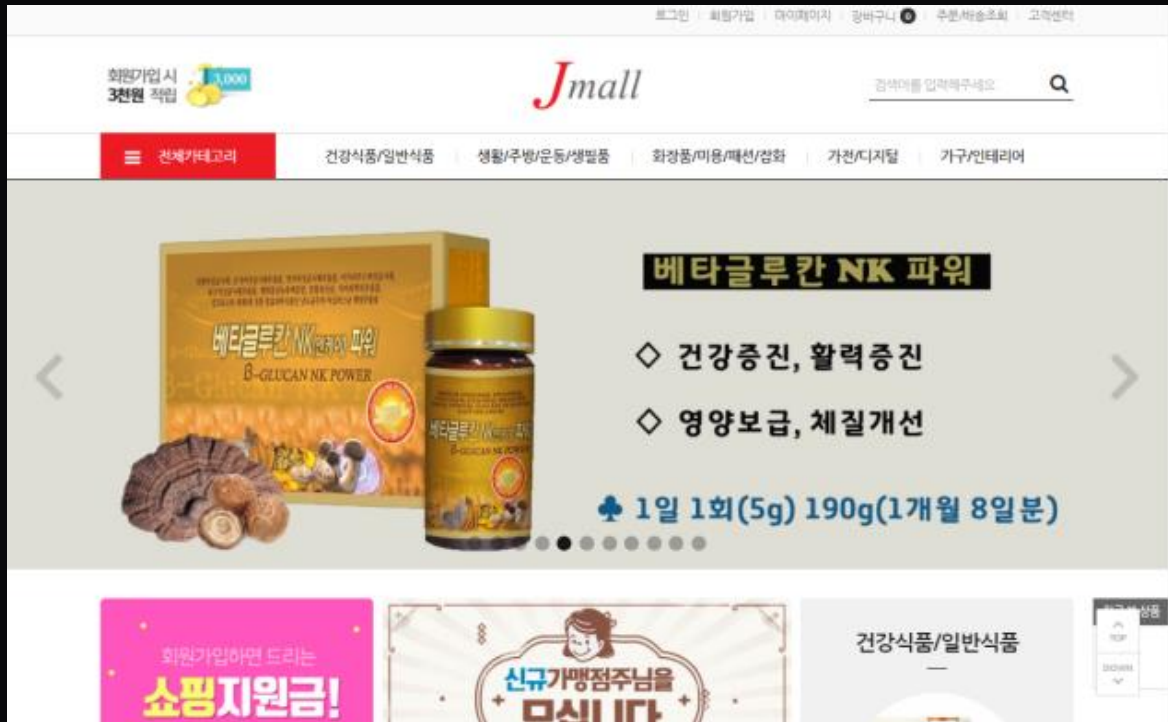
Blockchain Layer



[Blockchain upper/lower layer structure]

J-COIN's E-Wallet is built as a web mobile-based responsive page composed of HTML5 language and supports iOS and Android, allowing easy transaction on all commercial smartphones at home and abroad.

3 J-COIN's operating concept

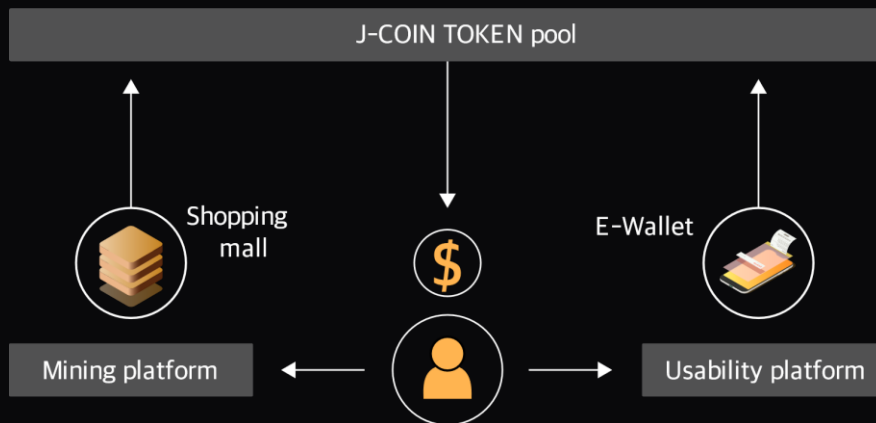


[jmall.bz shopping mall initial screen]

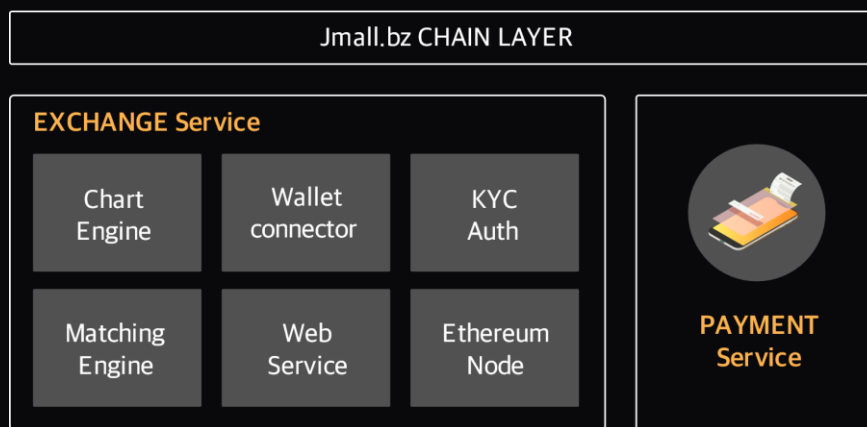
When purchasing and paying for products at Jmall Biz (www.j-mall.bz), the JCO in the wallet is recognized for its value according to the exchange market price, and J-COIN operates as a virtuous cycle of 'use→ recovery' and can be used for the purchase and use of the product at Jmall shop for actual payment purposes. I think the diagram below should be revised according to the contents above.

The above is put into the diagram below.

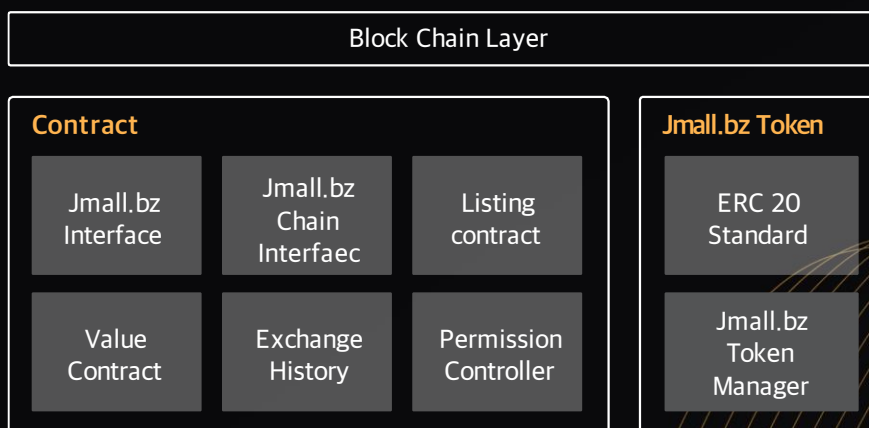
| J-COIN virtuous cycle mechanism overview



| Jmall.bz chain layer structure



| Blockchain layer structure



As shown above, J-COIN is adopted as the basic structure for the product purchase at jmall.bz, and the value of J-COIN is recognized according to the exchange market price of the day.

This has the aspect of solving the lack of economic incentives, a chronic problem of the previous first-generation cryptocurrency, and it will also satisfy the digital transaction real payment method that the fourth-generation future cryptocurrency aims for.

Trade mining includes compensation to future points, so the market price on the exchange becomes the size of the profit. This results in potential deflation of the coin, affecting real interest rates, consumption, and production like the Fisher equation.

$$r = i_{LT} + [\text{Deflation}]$$

[Deflation] : Expected rate of deflation
(expressed as a positive number)

$$r = i_{LT} - \Pi^e$$

r : Real interest rate

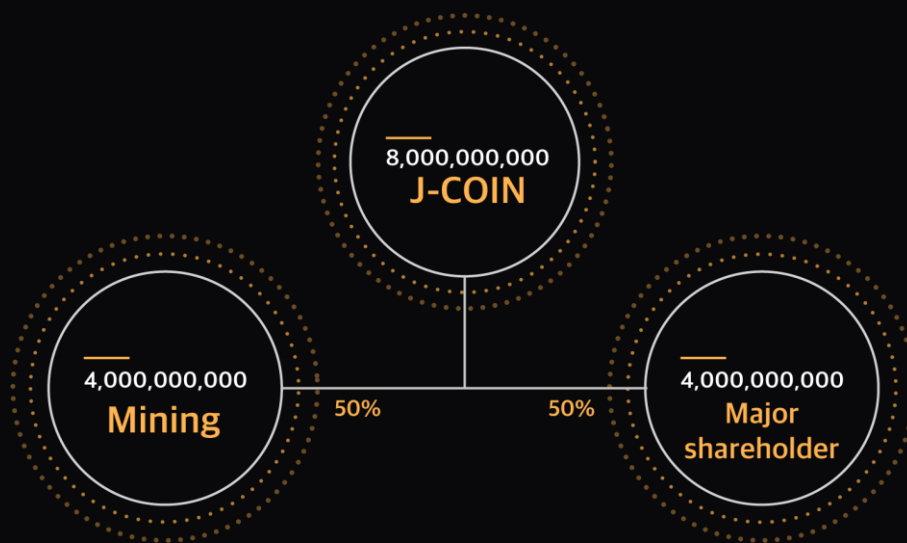
LT : Long-Term nominal interest rate

[Fisher equation]

Accordingly, J-COIN actively introduces jmall.bz, the medium for economic incentives, to create a catfish effect, and operates J-COIN as an asset that connects the cryptocurrency market in the cycle of use.

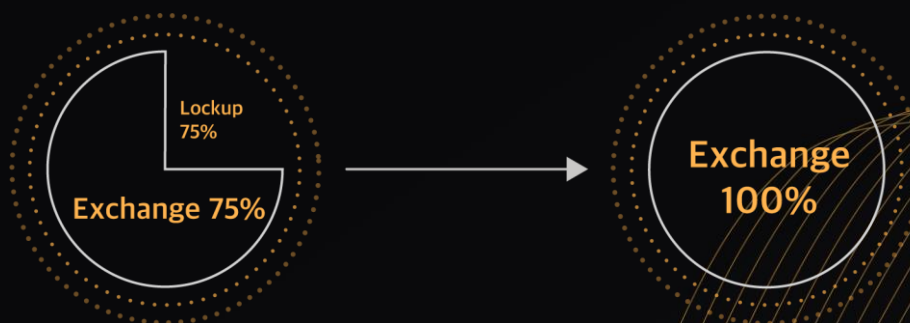
4 J-COIN allocation structure


Prior to the coin's listing on the exchange, a total of 8 billion coins are allocated by 50% (4 billion) for product purchase mining and the remaining 50% for the major management shareholder group.



The coins of the major management shareholder group are used for stable operation and upgrade of coins and shopping malls. In particular, the coins of the major management shareholder group are used for stable operation and upgrade of coins and shopping malls. In particular, the coins of the coins of the major management shareholder group are used for all listing costs and aggressive marketing expenses to boost the value of the coin.

In addition, a total of 2 billion coins in each group are locked up for 2 years to stabilize the coin value.






After listing, the allocated coins are collectively converted into 50% (4 billion) listed coins and electronically distributed to the exchange, and 50% (2 billion) are locked up for two years. After two years from the listing date, the remaining 50% (2 billion) will be automatically released from the lock-up and the corresponding coins will be listed as coins according to the above procedure.

On the other hand, listed coins can purchase products at jmall.bz in accordance with the value of the transaction price, and changes in value will be reflected in the payment in real-time.

When purchasing a product using the listed J-COIN at jmall.bz, the coin users will receive an additional discount of 5% of the product price so that the 5% value of the product price will function as an interlocking guarantee to receive collateral at least, independent of market price.



5 Technical background of J-COIN

| Ethereum base token

J-COIN is a technology-based upgrade blockchain for Bitcoin that facilitates the creation of distributed applications (DApp) and is programmed using the Ethereum Virtual Machine (EVM)-based working-specific language Solidity, which provides Turing-completeness.

5-1. Use the same data structure as Bitcoin

The safety of the Bitcoin data structure has already been verified, and it is actively utilized and the structure is as follows.

The decentralized consensus process that make up the bitcoin data structure must attempt to continuously generate the so-called blocks, which are transaction packages, therefore needing a node to help with this.

Each block has a timestamp, nonce, hash of the previous block, and a list of all transactions that occurred immediately after that, and a blockchain is formed and extends its scope in this process, and it continues to update to show its current states

In order to check whether this update is appropriate, an algorithm to check the validity of each block is required, which is as follows.

- A. Check the existence and validity of the block immediately preceding the block referenced
- B. Check whether the timestamp value is greater than the timestamp value of the previous block and within a specific valid time
- C. Verify validity of PoW
- D. Align $S[Q]$ to be the last state of the previous block
- E. Prioritize TX to a list of block transactions with n transactions, return a false value and escape from the repeating sentence if at least one of the $S[i+1]=APPLY[S[i], TX[i]]$ sets for i of the closed section Q to $n-1$ is found to be an error.
- F. Return true value and set $S[n]$ to the last block state

As above, each transaction in the block must have a valid state displacement, and it can be seen that all transactions from the Genesis State to the corresponding block are applied and calculated in order.

At this time, as PoW is applied, the double-SHA256 hash value of the block must be smaller than the dynamic custom target value, and the reason is to avoid artificial interventions in the entire blockchain.

In order to satisfy the unpredictable Pseudorandom Function, the nonce value of the block header is increased to ensure that the new hash value meets the above.

The block is stored in the Multi-layer data structure, where the block header contains 200 bytes of data from Merkle Tree's root hash, including time stamps. The Merkle is a binary tree, referring to a set of a number of leaf nodes reflecting the underlying data in, the middle node, which is a hash of two child nodes below itself, and the root node at the top of the upper middle node.

5-2. Ethereum account method, the core of an E-Wallet

The account consists of four fields: nonce, which is a counter that allows each transaction to be processed only once, and ether balance, contract code, and storage space.

Ether is a crypto-fuel and is used to pay transaction fees. Account is made up of Externally Owned Accounts controlled by a private key and Contract Accounts controlled by a contract code.

5-3. Message and transaction method, the core of the transaction

The transaction consists of six fields: message destination, sender confirmation signature, amount of ether sent to destination, optional data field, STARTGAS value, and GASPRICE value.

Of these, STARTGAS and GASPRICE are important defenses for anti-Dos. They prevent malicious overcalculation to paralyze the system by limiting the number of steps to the calculation. The unit of fuel in the calculation is the gas, which varies from time to time depending on the amount of calculation.

In other words, maliciously paralyzing the system requires a significant amount of computation, so the gas has to be paid proportionally, so disabling the unnecessary calculation.

On the other hand, a message consists of five fields: message sender, message destination, ether, optional data field, and STARTGAS value. It is a fairly similar structure to the previous transaction.

5-4. State transition

Confirmation of the transaction form, confirmation of the signature validity, and the matching of nonce sender's account with nonce can be defined as functions of $APPLY(S, TX) \rightarrow S$, the core function of Ethereum state transition.

The transaction fee is calculated as $STARTGAS * GASPRICE$, and an error occurs if the sender's balance is insufficient.

5-5. Block verification algorithm

It checks the existence and validity of the block just before the reference, and checks whether the size of the current block timestamp exceeds the block just before the reference and whether the size is smaller than 15 minutes after the current point.

After that, it checks whether the block number, transaction route, uncle route, gas limited, etc. are valid, and the validity of the proof of work included in the block.

$S[i]$ takes precedence over the last state of the previous block, and when applying $S[i+1] = APPLY(S[i], TX[i])$ from i to $n-1$, it returns an error, or if the total gas consumed by the block exceeds $GASLIMIT$. Simply attach the paid reward block to the work participants $S[n]$ and make sure that the block header in the Merkle tree is in the final state, enabling the block validation by the final procedure.

5-6. Token system

The token system of the temper-proof blockchain is based on J-COIN, and the token corresponds to the concept of a database that performs one operation.

[Code applied to the state transition function of the token system]

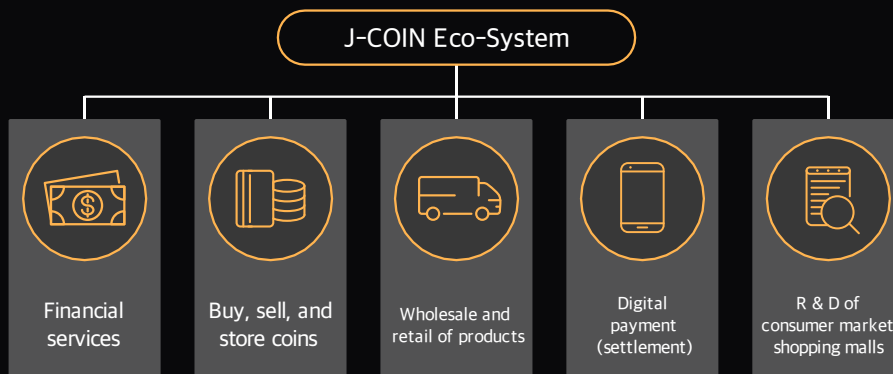
```
def JCOIN Send(to, valuse):
    if self.storage[msg.sender] >= value:
        self.storage[msg.sender] = self.storage[msg.sender] - value
    self.storage[to] = self.storage[to] + value
```

6 J-COIN's policy _____

6-1. Eco-System establishment

J-COIN operates in a blockchain-based decentralized ecosystem across various levels of individuals, companies, and national boundaries. It provides equal information, access rights and, equal opportunity for transactions, and guarantees usability as a practical payment method.

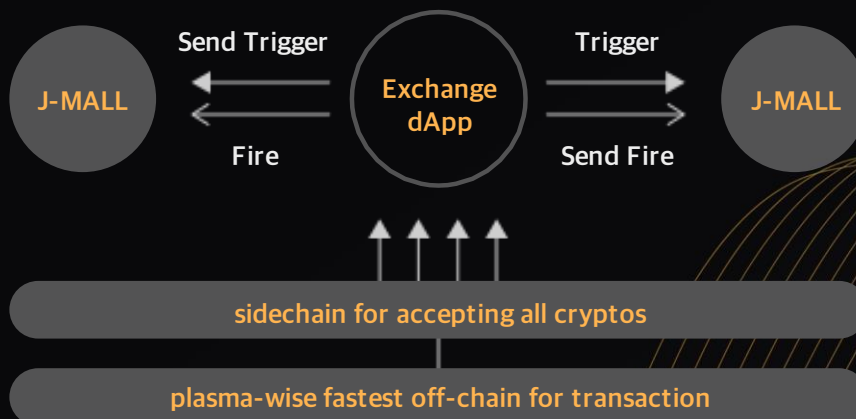
Diagram of J-COIN ecosystem



6-2. Mainnet

Ethereum has advanced Bitcoin's stack language to Turing-completeness, which has developed into the concept of smart contract, exponentially expanding the world of blockchain usability.

J-COIN의 메인넷 도식



6-3. Transparency (reliability)

Of the total 8 billion coins, 4 billion coins are listed, and a total of 2 billion J-COINs (each ratio is decided by approval of internal meetings) of the related parties and major shareholders are locked up to ensure reliability. Protect users of J-COIN by locking up major shareholders to prevent excessive profit-taking after the exchange listing.

Meanwhile, through the listed exchanges, announcement of quarterly audit reports, settlement reports, and annual business plans are mandatory.

6-4. KYC authentication

Through KYC authentication, J-COIN complies with transparent operation and money laundering prevention, and those who went through ID authentication are lifted of their limit on transaction size step by step and are required of minimum information such as name, email address, ETH address, and ID card for ID authentication.

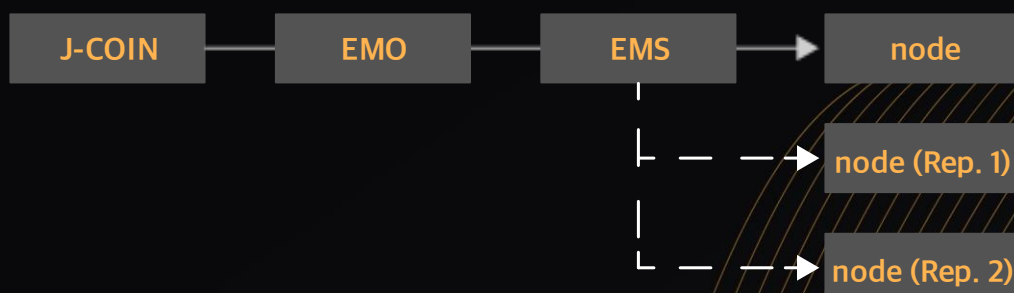
6-5. Circuit breaker

Coin volatility is very dynamic, and we can activate Circuit Breaker, a safety device for J-COIN users to absorb and control market shocks caused by various external factors.

6-6. Security through EMS, EMO

When new weaknesses are discovered due to market trends and technological advances, the coin's commercial policy EMS (Emergency Stop) and EMO (Emergency Off) functions are reflected in the smart contract to cope with emergency situations and prevent arbitrary manipulation. It is based on Multi Sig so to prevent arbitrarily manipulation and is transparently approved by Legal Advisor.

J-COIN의 보안정책 도식



7 Future technology reflection

7-1. POST consent mechanism

It is an improvement of the former PoS (Proof of Stake) consent mechanism and a post consent for the next progressive generation of the PoW (Proof of Work)

PoW consent participating nodes infinitely decode the nonce value and work on the hash value of the block until certain conditions are met, and when a successful block is created, the record ledger is immediately written.

However, at this time, since the excellent record ledger node may exercise control of other record ledger nodes, it is necessary to grant credit to the node, and it is possible to guarantee the reliability of the consent by presupposing only consent with the node by adjusting the difficulty of PoW based on the credit information of each node.

This is called POST (Proof of Stake + Trust) and will be reflected in J-COIN in the future.

7-2. Multilateral consent safety algorithm

- A. Arbitrary number of sets is set in the core node
- B. Divide the number of randomly generated sets by N (N=integer, over 60% of all users)
- C. The number divided by N above is designated for each of the N passwords.
- D. All users calculate N passwords using the password above
- E. Authorization is granted as soon as all data is received from the core node

- PBFT (Practical Byzantine Fault Tolerance)

As a Practical Byzantine Fault Tolerance Consent Mechanism, it verifies the consistency of three steps in the process of communicating news and meets certain conditions.

8 Reference _____

| Types of previous consent mechanism

- PoW (Proof of Work)

It drives block creation as a PoW consent mechanism, and nodes constantly calculate block hash values corresponding to all block ledgers and meet certain conditions.

- PoS (Proof of Stake)

As an Asset proof consult mechanism, it meets certain conditions in the PoW mechanism, prioritizing nodes based on assets held by nodes

- DPoS (Delegated Proof of Stake)

As a Consent Mechanism, it meets certain conditions by votes to select a certain number of nodes

- PBFT (Practical Byzantine Fault Tolerance)

실용 비잔틴 장애허용 합의 메카니즘으로서, 소식을 전달하는 과정에 3단계의 일 치성을 확인 후 일정조건을 만족시킵니다.

| Literature

- S.Nakamoto, Bitcoin : A peer-to-peer electronic cash system, bitcoin.org, 2009

- Tapscott, D.Tapscott, How blockchain is changing finance, Havard Business Review, 2017.

9 Legal notice and liability limitation

This white paper is intended to provide information on Consumer market shopping mall-based Purchase reward type digital payment point blockchain token that J-COIN(JCO) Project (JCO) wants to promote. Herein whitepaper is not intended to encourage investment in our platform and has nothing to do with it. In addition, the J-COIN Team has prepared and provided herein whitepaper as of the time of writing. It does not guarantee that any content on the whitepaper, including conclusions, will be accurate in the future.

The J-COIN Team will not state and guarantee any accuracy in relation to herein whitepaper, and will not be liable for it. For example, J-COIN Team does not guarantee i) whether the whitepaper is written on the basis of legitimate rights and does not infringe on the rights of third parties, ii) whether the whitepaper is of commercial value or useful, iii) whether the whitepaper is suitable for achieving the specific purpose you might have, and iv) whether the whitepaper is error-free. Of course, the scope of liability exemptions is not limited to the previous examples.

If you use (including, but not limited to, cases based on or referring to the whitepaper) herein whitepaper according to your decision-making, the other consequences, whether profit or loss, are entirely at your discretion. In other words, please note that even if damages, losses, debts, and other damages occur to you by using herein whitepaper, the J-COIN Team will not be liable for compensation, reparation, or other liability for them.

Warning for the forward-looking statements

(a) Certain expressions in herein whitepaper contain forward-looking statements about the future, future events, and prospects of the project. These are not statements based on historical facts but are identified by similar expressions such as 'scheduled,' 'estimated,' 'believed,' 'expected,' and 'prospected.' In addition to herein whitepaper, presentations, interviews, videos, and other public materials may include this forward-looking statement. The forward-looking statements contained in herein whitepaper include, but are not limited to, future results, performance, and J-COIN achievements and its affiliates.

(b) The forward-looking statements contain a variety of risks and uncertainties. These statements do not guarantee future performance and should not be relied upon too much. When risks and uncertainties materialize into reality, the actual performance and development of J-COIN

and its affiliates may differ from the expectations set by forward-looking statements. Even if there are changes to these circumstances in the future, J-COIN and its affiliates are not obligated to provide an update to the forward-looking statement. Suppose you act based on the forward-looking statements in herein whitepaper, J-COIN 's and affiliates' homepages, and other materials. In that case, you are solely responsible for the non-realization of the content of the forward-looking statements.

(c) The J-COIN platform is not complete or fully operational as of the date herein whitepaper was created. Although the explanation was written on the premise that the J-COIN platform will be completed and fully operational in the future, this shall not be construed as a guarantee or promise for the platform's completion and full operation.

Anti-Money Laundering Act (AML)

The buyers shall agree not to participate in any form of money laundering, illegal currency transactions, and other restricted activities through J-COIN Team's J-COIN Coin (JCO) and other related derivatives if any. Each participant shall be aware that J-COIN Coin (JCO) and other related derivatives cannot be directly or indirectly sold, exchanged, or disposed of for money laundering purposes.

Important matters

Due to frequent changes in related policies, laws, regulations, technologies, economies, and other factors, the information provided herein whitepaper may be inaccurate, unreliable, or not final and may change several times. This material is provided for informational purposes only. Our Team is not responsible for the accuracy and legitimacy of the information provided. Those who wish to participate shall not rely solely on the information in herein whitepaper. We encourage participants to do their research prior to the support. Basically, herein whitepaper is a business proposal or business promotional document and is not legally binding under any circumstances. What is stated in this document is for reference only, and the J-COIN Coin (JCO) buyer must take extra care of himself.

Language interpretation

This document is available in Korean and English. In the event of disputes, the issues will be resolved based on the Korean version. Please refer to the Korean version for a more accurate interpretation of the herein whitepaper.



THANKS

FOR WATCHING

© 2020. J-COIN. All rights reserved.