Internal cryptocurrency platform for the settlement, reward and transaction of online and mobile services



MECON CASH

BLOCKCHAIN CRYPTOCURRENCY

White Paper Draft Ver. 1.1

Date: August 19, 2019

CRYP2NOVA

Archived copy · cryp2nova.com

TABLE OF CONTENTS

1. INTRODUCTION 3

PROBLEMS WITH THE CURRENT REWARD SYSTEM 3
EXPANDED APPLICATION OF MOBILE CONTENTS USING THE BLOCKCHAIN 3
ISSUES AND PROPOSAL OF A SOLUTION 4

2. MECONCASH BUSINESS PLATFORM 5

INTERNAL CRYPTOCURRENCY PLATFORM FOR THE SETTLEMENT, REWARD, AND TRANSACTION OF ONLINE AND MOBILE SERVICES 5
MOBILE APPLICATION: BUSINESS CARD TO INTERLINK PEOPLE - LINKU 6
CARICATURE & EMOJI SERVICE: AN OPEN MARKET PLATFORM FOR ORDERS FOR THE PRODUCTION OF CARICATURES AND EMOTICONS 9
MOBILE GAME 12
ECOMMERCE: MOBILE COUPON SERVICE FOR VOICE MESSAGE THROUGH AN AVATAR 12
P2P EXCHANGE: COIN25 FOR THE TRADING OF CRYPTOCURRENCY 13
MECONCASH WALLET 16
MECONCASH OPENAPI 16

3. MECONCASH BLOCKCHAIN 17

BLOCKCHAIN 17
BLOCKCHAIN BUSINESS AND DISTRIBUTED LEDGER 17
HYBRID DESIGN OF MECONCASH 20
POW ALGORITHM IN MECONCASH 22
POS DESIGN OF MECONCASH 22
BLOCK GENERATION UNDER POS 22
PROTECTION OF HISTORY IN MECONCASH 23
BLOCK SIGNATURES AND DUPLICATE STAKE PROTOCOL OF MECONCASH 23
MECONCASH BLOCKCHAIN EXPLORER 23
MECONCASH INTEREST PAYMENT SYSTEM 24

CRYP2NOVA

Archived copy · cryp2nova.com

4. MECONCASH ISSUANCE 26

INITIAL DEVELOPMENT BUDGET 26

EARLY MINING REWARDS 27

POW MINING REWARDS 27

POS REWARDS 27

5. ROADMAP 28

CURRENT PROGRESS 28

ROADMAP 29

6. DISCLAIMER 30

REFERENCES AND EXCERPTS 31

CRYP2NOVA

Archived copy · cryp2nova.com

1. Introduction

Problems with the current reward system

With the advent of the digital business era, the industrial paradigm is shifting from manufacturing to services, while economic power is moving from the supplier to the consumer. When experiencing goods and services, consumers value emotional consumption more than rational consumption, which highlights quantitative advantages such as price and performance. In an age that values user experience, membership services have continuously expanded their domain as they are the closest customer contact services as well as consumer-centered integrated services that affect customer awareness.

Many of us are already registered with many reward programs of one form or another as we use services in our daily life. With the recent growth of the smartphone market, countless people view advertisements through a variety of reward apps that serve as a means of corporate marketing, and purchase products or game or app items using mobile coupons with and the points accumulated by installing apps on their mobile devices or by other means. Point-based services have moved beyond the concept of loyal customer marketing and are now evolving into a “second currency” combined with electronic payment. However, points are available only with services that offer them as a reward, and will expire if the service is either deleted or unused for a certain period. Thus, the rewards that users earn from investing their time and effort are easily lost and lose their value over time.

Expanded application of mobile contents using the blockchain

As there have been active attempts to apply blockchain technology to mobile services worldwide, a new business in which blockchain and virtual currency are applied to contents such as music, photographs, and personal broadcasting has emerged. As a result, there are growing expectations that the mobile contents market, which is easily accessed by the general public, will become a success case in which new business models are discovered by combining with blockchain technology.

Game companies, which are aware that users assign monetary values to in-game items, are paying close attention to blockchain technology. In fact, they are considering adopting the blockchain technology in order to use virtual currency to sell game items or game user records. Moreover, the blockchain technology can open up new possibilities for the production and distribution of contents such as videos and music. The following cases are examples of potential applications in the contents industry.

Archived copy · cryp2nova.com

- Game: Users can save game items or game records with blockchain technology and exchange them for virtual currency.
- Video: Users of video files can be directly linked with uploaders of video files and pay a fee to creators.
- Music: Creators and users can be directly linked to maximize income from music copyrights.
- Personal broadcasting: The service could introduce a feature to enable viewers to send virtual currency as a gift to personal creators.
- Blog: The service could provide income to creators who post articles on a blog platform and reward users who read articles and post comments.

Issues and proposal of a solution

Before proceeding with the blockchain-based platform, we developed character-based smart applications, an AI-based avatar business card called LinkU, character electronic business card called MeconTong, a gift mall called JangBoGo, a mobile game service, and an emoticon service.

Our internal services already feature an individual reward system according to the target and characteristics of the service. Although our services carry out cross-marketing, the reward points are integrated and managed only in some services, and individual services separately offer the remainders. We want our loyal customers to be able to use the points they have accumulated while using our services for other services.

We believe that a virtual currency that enables reward, transaction and settlement through blockchain is the ideal solution to the problem of trading reward points between our internal services. Existing points generally expire after a set period, but rewards with cryptocurrency can gain value over time and be exchanged and traded for other currencies.

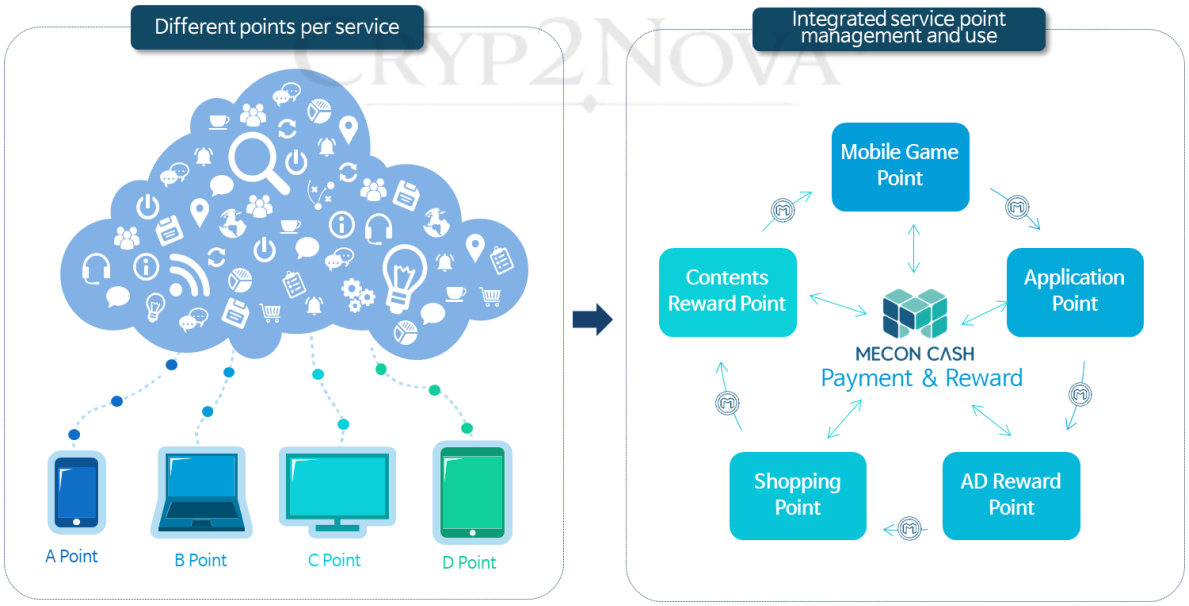


Figure 1. Blockchain connection of MeconCash

Archived copy · cryp2nova.com

2. MeconCash business platform

Internal cryptocurrency platform for the settlement, reward, and transaction of online and mobile services

We intend to develop MeconCash into a platform that allows user's assets to be transferred and traded between different types of services by integrating point reward systems, contents purchase, and settlement, which are currently operated separately between existing services and those under development. To that end, we will build the reward and settlement system, develop the API to connect it with other services, and build an ecosystem that can be used in the on- and off-line real economy. All this will ensure the usability, connectivity, and sustainability of MeconCash.

We will develop a variety of mobile-based applications, games, and contents on the platform and link it with such services as online marketplaces where users can purchase products. The reward system used by a service generally invalidates the rewards owned by users when the service is terminated. MeconCash, however, can transform the rewards obtained from using our services into valuable assets. As such, users will be able to fulfill the demand for new services with MeconCash even when the services they use are terminated, make transactions between them, and use the assets in the real economy.

We will stabilize the MeconCash ecosystem by developing new blockchain-based businesses and linking it with external services.



Figure 2. MeconCash business platform

Archived copy · cryp2nova.com

Mobile application: Business card to interlink people - LinkU

Mobile business cards are created, transferred, and stored by smartphones to maximize personal relations. Conventional paper business cards usually contain basic affiliation and contact information such as name, address, phone number, company, and position, whereas mobile business cards have the additional benefit of providing multimedia contents such as video, document, website, and SNS. A mobile business card stores all information in a digital form, and can be easily transferred via text message or messenger, and stored in smartphones. Most mobile business card services use the OCR function or manual input to save and manage the information.

We intend to develop the blockchain-based platform so as to interlink people using LinkU, which the AI-based Avatar business card that can be the PR and marketing tool as well as a personal assistant.

LinkU was launched in the Google Marketplace as the world's first avatar business card and personal assistant on March 1, 2017. The electronic business card platform allows users to promote themselves and their businesses using an elaborately created 3D or 2D avatar.



Figure 3. LinkU service

Archived copy · cryp2nova.com

Easy and simple operation and convenient functions

Users can design avatars, upload images and files, and even create a video with just one touch, and there is no limit on data volume or capacity. Users can also present company PR, a business plan, or their personal PR with the sheet of a mobile business card. The built-in avatar can explain the information and automatically play video files.

Linky, an AI avatar assistant

The avatar in the electronic business card is both the perfect agent and secretary to solve the PR, advertising and sales requirements of users who have difficulties with their business operations due to time constraints, personal reasons, or location in a remote place.

Linky can inform you of life information and schedules, while its AI-based avatar secretary can play music, take memos, manage your schedule, and notify you of items of interest through voice recognition.

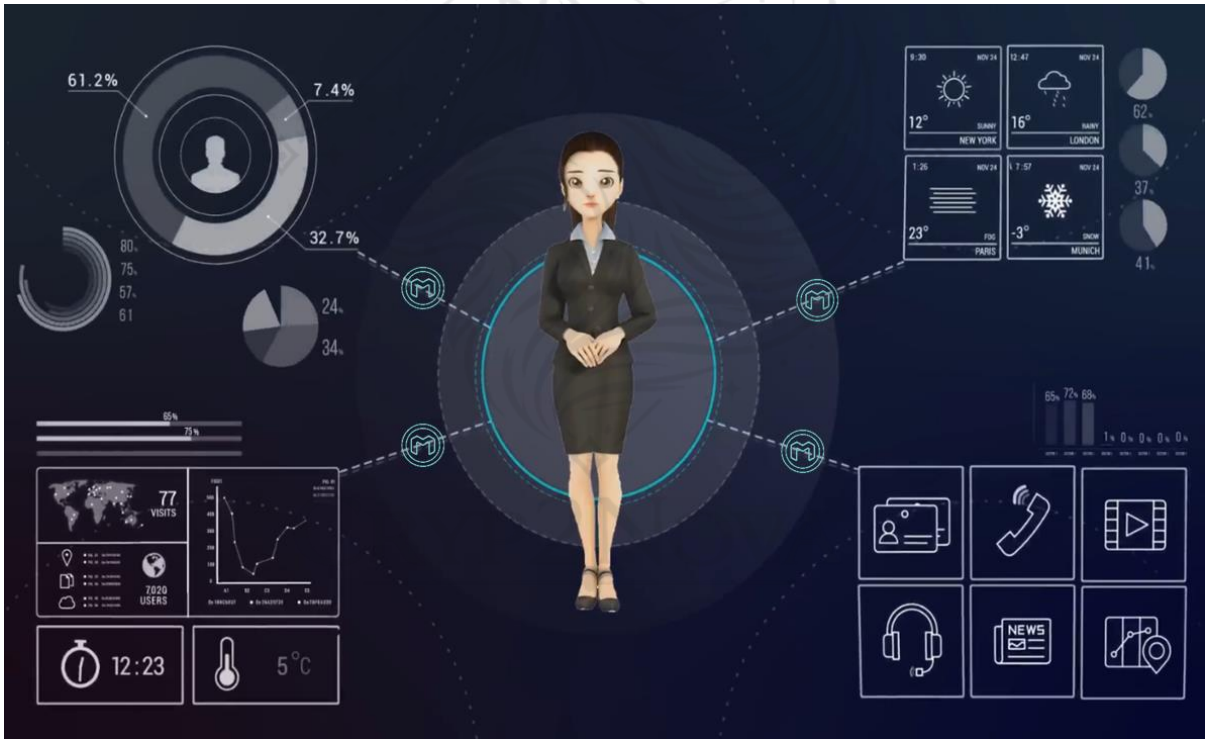


Figure 4. Linky, an AI avatar assistant

Call decline message by an avatar

Call decline messages are commonly used worldwide. However, a typical decline message may make the calling party feel rather uncomfortable or misunderstood. LinkU's call decline message is very sincere when authenticity is needed and can be great fun too if that is needed. It is designed to provide characters and behaviors appropriate to various situations and use the user's

Archived copy · cryp2nova.com

own or another person's voice recording. The automatic answering feature improves user-friendliness.

Spam call function to filter unwanted calls

The differentiated spam blocking function automatically filters calls you do not want to answer, calls from unknown numbers, or Smishing calls. You can register a number as spam to be blocked, block all unknown or unregistered numbers, or make a call using your preferred text or character message.

LinKet, an intelligent autonomous market with a visiting service

All platforms force consumers to search and find the seller they want. LinKet, however, is a service that enables sellers to find consumers by what they search and post. The service also allows consumers to consult sellers and compare prices to find the lowest price for the highest quality. It links stores, businesses, and entrepreneurs with consumers through categorization, and provides 1:1 chatting for inquiries and reservations for visits in real time.

Avatar and customized advertising for each customer

LinkU plans to introduce a service that will create avatars for business customers and provide customized advertising.

MeconCash reward and transaction

All service users will receive MeconCash as a reward for purchasing contents, advertising, and using the services. The MeconCash thus distributed will be the means of payment for all of our services and will become the user's asset. The following explains how users are rewarded for using LinkU:

- Users receive MCH rewards for disclosing their business cards, sending, linking, commenting or clicking on advertisements, and registering spam in the DB.
- Users can consume the MCH when using paid services such as avatars, contents, and the functions that they want.
- They can send the reward MCH to the integrated wallet for transactions or purchases.
- Business members can pay advertising costs with MCH. MCH paid by business members will be given to users as a reward.
- MCH will be safely transferred and stored with the Integrated MeconCash Wallet.

Archived copy · cryp2nova.com

Caricature & emoji service: An open market platform for orders for the production of caricatures and emoticons

Emoticons (stickers) are a fun way for users to interact visually with their friends and family on messaging apps and social networking sites. They are known to increase participation by a wide range of generations and social groups regardless of age or gender. Mobile communication using emoticons or stickers has gained popularity as it can easily convey a person's emotions while creating a bit of fun, as well as fulfilling the growing needs of users. The sticker and emoticon features of messenger services such as Line, KakaoTalk, Facebook, and WeChat have been extended to the character business.

KakaoTalk has grown by around 40% per year for the past six years. More than 2 billion messages use emoticons each month, and some creators have recorded annual sales of over 1 billion won. We launched the emoticon creator market service with Emoticon Open Studio in April, and the artist pool has been growing as a result. We also provide a personalized emoji service based on face recognition to the animoji service featuring moving emoticons introduced by Apple's iPhoneX and the AR emoji service provided by Samsung's Galaxy S9. Although users' desire to use unique characters to represent them has been increasing, it is difficult to find platforms for caricature and emoticon creators other than through large platforms such as KakaoTalk and Line.

AnotherMe open market platform

The open market platform provides a very convenient channel for promoting and distributing contents to artists who create customized caricatures and emoticons, while allowing users to freely use emoticons by matching actions to caricatures that convey a diverse range of emotional expressions. The AnotherMe platform is based on free and voluntary participation by many artists such as the designers and creators of caricatures and emoticons.

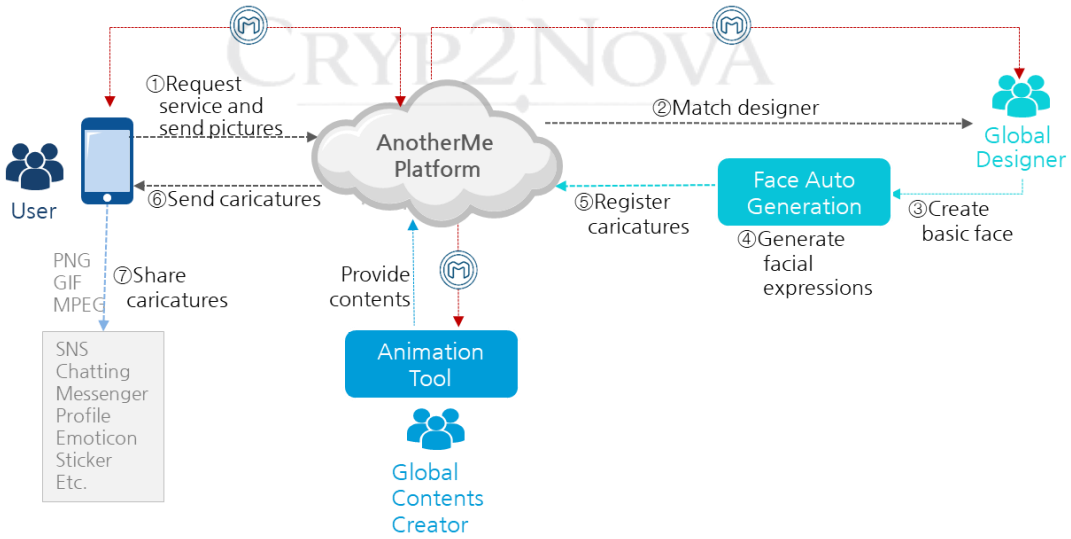


Figure 5. AnotherMe service flow

Scope of the AnotherMe service

Archived copy · cryp2nova.com

The user provides his or her picture and receives caricatures of various facial poses. We will develop a caricature facial expression auto-generation tool and animation tools that any designer familiar with graphic tools can use easily. We will also provide a system in which domestic and foreign designers can participate freely.

The platform will consist of an architecture designed to increase and recycle usability by allowing users to purchase contents with MeconCash and by paying MeconCash to creators and designers as a reward for their work.

- Windows-based tools to automatically generate facial expressions and animations for designers.
- A mobile app service that allows users to use unique animated emoticons freely.
- A system for customer order management, item management, creator management, and income settlement.
- A service for mobile coupons that contain emoticons with the user's voice message

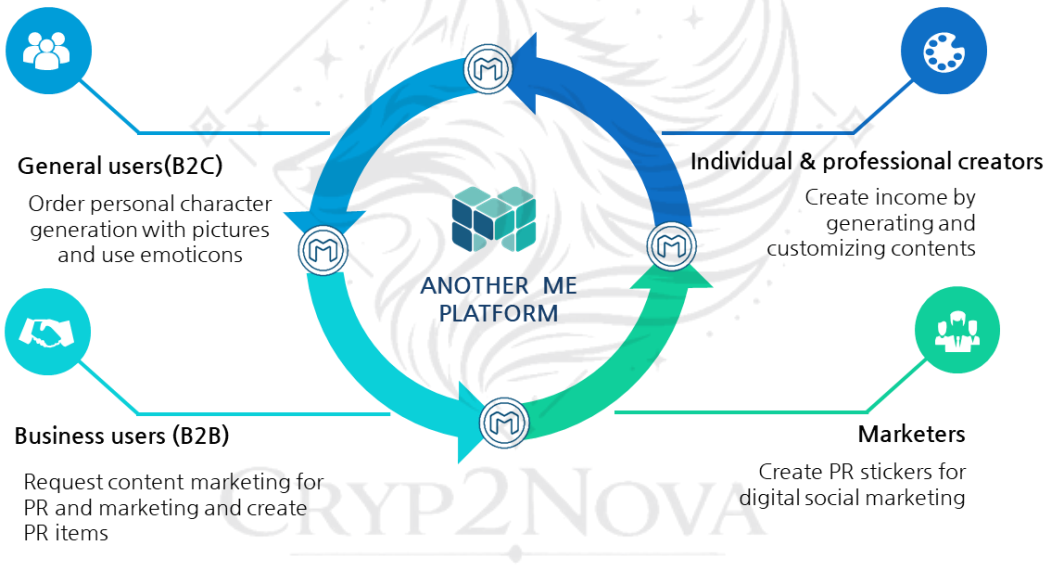


Figure 6. AnotherMe platform participants

Face auto-generation tool

This tool allows designers to create basic facial features such as face shape, hair style, eyes, nose, and mouth based on a picture, and automatically generates facial caricatures that express the user's emotions by combining them in various ways. It is a hybrid production tool that integrates the analog method of design work with the digital method of using an automation tool.

Archived copy · cryp2nova.com

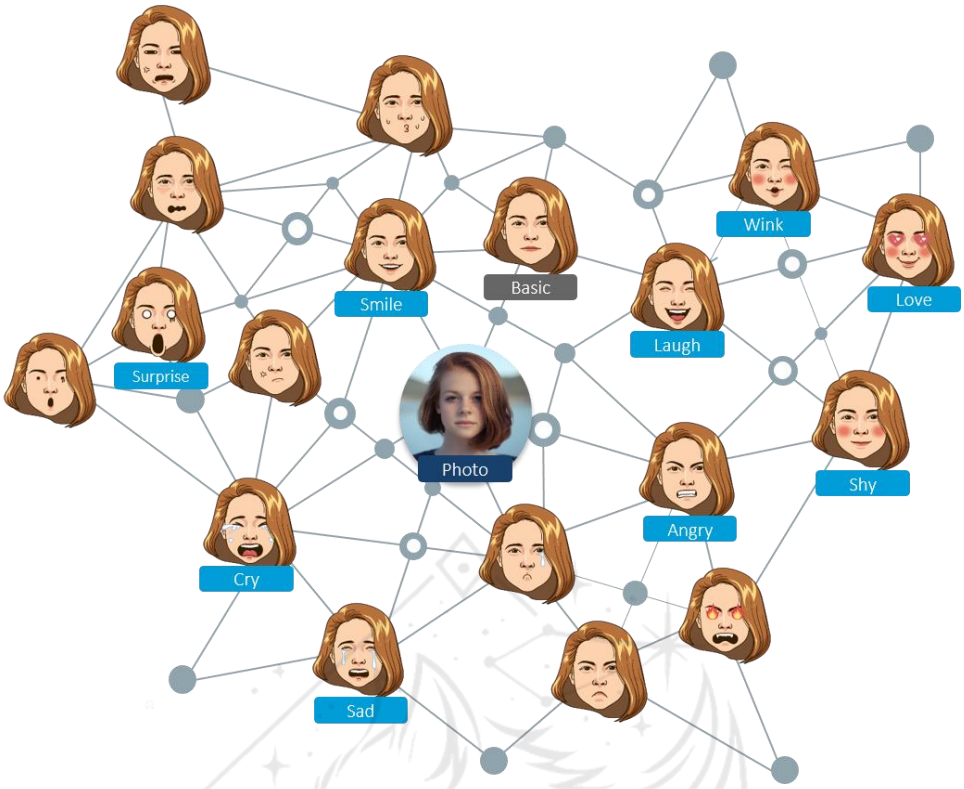


Figure 7. Generation of facial expressions

Animation tool

This animation tool allows content creators to animate actions to suit a generated caricature expression in the format required by the system. It automatically generates data such as expressions, coordinates them when the creator selects the expression that fits the action, and then creates the animation. It then uploads the generated file so that the user can use the automatic matching function to caricaturize an expression.

Mobile application

Users can order emoticons that match their caricatures with Android and iOS smartphones. The app provides a wide range of modes (personal facial expression, refined edge, and illustrated caricature) and decorative items to increase usability. The created emoticons can be saved in the png, gif, and mp4 file formats. We plan to expand its usability even further by adding a message function.

Archived copy · cryp2nova.com

Mobile game

Game users within the platform can earn MeconCash by playing games and then transfer it to other users in the same way as they transfer game money. They can trade their assets with other users just as they trade items, use them like cash for purchasing paid services in the game, and use them as a method of payment when trading assets.

The MeconCash platform provides a function for storing and transferring assets securely, and applies concurrency in asset transactions to enable reliable transactions without the need for intermediaries.

The design allows the user assets stored in the database of the app and game services to be transferred to the external blockchain DB so as to facilitate the transfer of assets from a third-party game and to allow app users and to trade with other users. We have published a strategic RPG game and will develop the link the MeconCash reward system and item trading system to the game. We plan to disclose the open API so that third parties can use it to apply their games to the platform.



Figure 8. Project Kingdom Heroes

eCommerce: Mobile coupon service for voice message through an avatar

Companies offer coupons which provide various benefits or price discounts to consumers in order to stimulate or promote the purchase of goods. Digital culture has recently become more popular with the development of information and communication technology, and new forms of coupons such as Internet coupons and mobile coupons have emerged as new promotional techniques. Mobile coupons in the form of bar codes that are sent as part text messages have mainly adopted gifts as a means of inducing the intention to purchase and improving customer satisfaction. These coupons compensate such shortcomings as inconvenient storage and/or the risk of loss of existing paper and print coupons by allowing customers to receive a variety of useful benefits including immediate and timely discounts and value-added services. Conventional coupons have a problem in that they only send the product shape, name, and barcode, and thus it is difficult to share emotion between coupon senders and receivers.

Archived copy · cryp2nova.com

We intend to provide a mobile coupon service that can stimulate the emotions of the recipient by allowing senders to generate their avatar, along with a voice message, whenever they purchase or send a mobile coupon. The mobile coupon system includes a function that allows the user to select a product, select the recipient of the coupon, add images or voice to the coupon, and request the coupon server to send the coupon to the recipient's handset. In other words, it allows the user to send his or her avatar or voice message as part of the coupon.

P2P exchange: COIN25 for the trading of cryptocurrency

Issues with centralized exchanges

Many cryptocurrency transactions have moved to the over-the-counter market due to problems with the existing cryptographic exchange, including security, limited availability, the inconvenience of trading, and government regulations. In addition, they are focused on specific coins such as Bitcoin and Ethereum.

Whenever there is a report about problems with centralized exchanges, such as the hacking of the Coincheck exchange in Japan or suspected illegal recording at a top domestic exchange, experts mention the decentralized exchange (DEX) as the alternative. The DEX differs from centralized exchanges in that it only links sellers and buyers of cryptocurrency through person-to-person (P2P) transactions, whereas centralized exchanges also keep investors' assets. The assets are stored in the user's personal wallet and transferred directly through P2P, and thus there is no need for the exchange to keep them. Even if an exchange is hacked, no assets are lost since the exchange itself does not keep any; and there is no risk of illegal booking as the assets move directly between wallets.

The face-to-face transaction, which is currently called "P2P transaction", is a way for a seller and a buyer to meet in an offline space to exchange cryptocurrency. Although there are information sharing sites for such face-to-face transactions in Korea and abroad, there is a problem in that it falls to the individuals themselves to deal with and resolve a transaction accident.

Decentralized P2P exchange as the alternative

We will build a P2P cryptocurrency exchange, COIN25, to promote safe cryptocurrency trading. COIN25 is a secure exchange platform for P2P trading of cryptocurrency. It has a built-in escrow function to minimize disputes and damages that may occur during person-to-person transactions, and protects personal information comprehensively so as to increase safety and reliability. It also provides features such as registration of virtual currency, market price trend, and transaction

Archived copy · cryp2nova.com

records and reputation so as to allow the trading parties to check each other's credibility and trade both listed and unlisted coins with confidence.

The key features of COIN25 are as follows:

- It guarantees the safety of trade between individuals.
- It is a simple trading system based on the application of wallet address input matching.
- It guarantees the credit rating of trading partners and the confidentiality of personal information.
- It guarantees the safest transaction through escrow and assurance of risk responsibility during brokered transactions.
- It increases sellers' profits by introducing the first coin bidding system.
- There is no possibility of hacking as the seller is paid from the escrow account only after confirmation of coin transfer from the seller to the buyer.
- It supports the trading of all coins and the simple registration of new coins.
- It supports safe transactions in each country by operating overseas branches.

Purchase and trading of cryptocurrency

Trading cryptocurrency with COIN25 is described below. The system notifies the users of each step in real time and ensures safe transactions.

1) A user registers to sell or buy a cryptocurrency.
2) A seller or buyer requests to trade by entering the quantity and amount.
3) The buyer or seller approves or rejects the trade upon notification of the trade request.
4) The system notifies the seller or buyer that the trade has been matched or rejected.
5) Upon matching of the trade, the system requests the buyer to deposit the purchase amount.
6) After confirming the buyer's deposit, the system notifies the seller of the buyer's wallet address and related information.
7) The seller sends the cryptocurrency to the buyer's wallet address and provides the record of the shipment to the system.
8) Upon receiving the cryptocurrency, the buyer provides the receipt record to the system.
9) The system verifies the sending of the coin by the seller and the receipt by the buyer, and then deposits the transaction amount - minus the fee - to the seller.
10) The transaction is completed when the seller confirms the deposit of the transaction amount.

Archived copy · cryp2nova.com

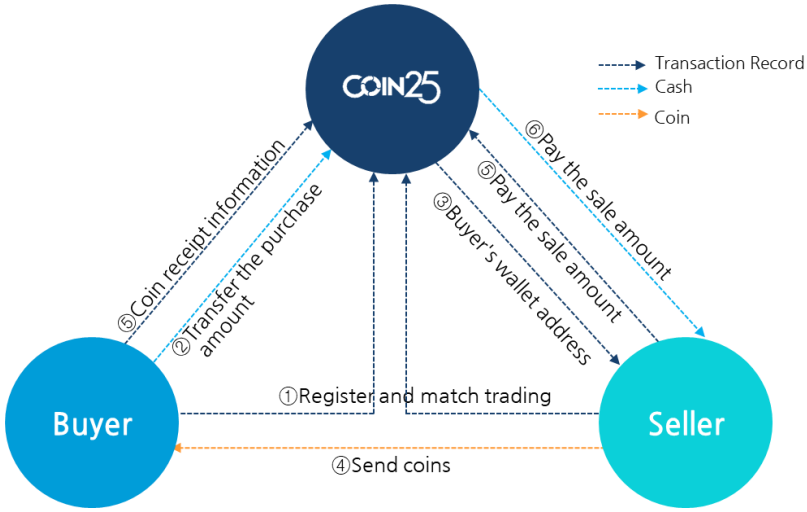


Figure 9. P2P cryptocurrency trade flow

Cryptocurrency auction

An auction is a buyer-centered trading method that allows the seller to register the quantity and terms of sale so that multiple buyers can bid. Upon the auction is completed, the same procedure as the P2P cryptocurrency transaction is followed.

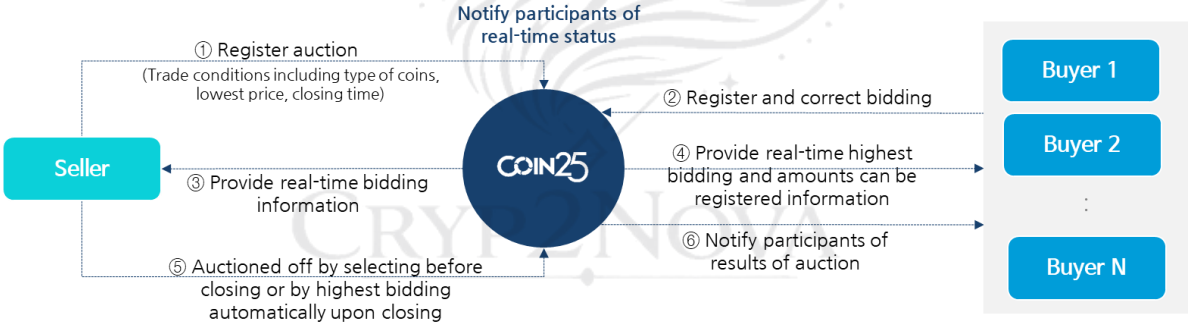


Figure 10. Brokered P2P trade

Value of MeconCash in P2P exchange

MeconCash can be used for P2P trade on COIN25 until it is listed in the exchange. Once the interface to the wallet becomes available in the second half of this year, it will be possible to use it for advertising payments during registration of selling, purchase, and auction. Moreover, users will be able to exchange the rewarded points for MeconCash and spend it on third-party services in the ecosystem.

Archived copy · cryp2nova.com

MeconCash Wallet

The wallet provided by the MeconCash platform is the service through which cryptocurrency can be used. MeconCash Wallet includes a function for securely trading MCH coins issued by the MeconCash platform; and it will be upgraded to a unified wallet service that integrates all reward MCH coins generated from services within the MeconCash Platform in the future. The MeconCash Wallet service will be launched in the following steps.

- It was first released on May 11, 2018 in the form of a hybrid app, and is currently undergoing an update.
- We plan to release a native app for Android and iOS with improved user-friendly features and a safer storage system around June or July 2018.
- The integrated wallet for the MeconCash platform services will be distributed in Q2 2019.

MeconCash OpenAPI

MeconCash OpenAPI provides an API that links the services of our business partners with the integrated member management, reward, transaction, and settlement functions of the MeconCash platform. The MeconCash Standard Open API will be applied in phases according to the development of our internal services, and will thereafter be continuously upgraded to establish an easy interface with the MeconCash ecosystem. It will also be defined and developed in accordance with the nature of our business partners' services.

CRYP2NOVA

- API for MCH reward generated by services.
- Wallet API for MCH exchange and trade.
- MCH settlement API for paid contents services.
- API for integrated member management.
- API for the use of MCH by exchange.
- API for MCH partner services.
- MCH payment module for MCH partner services.

Archived copy · cryp2nova.com

3. MeconCash Blockchain

Blockchain

A blockchain is a list of links of blocks ranging right from the initial block (genesis block) to the last block. Since the blockchains are distributed and stored across multiple nodes, and since each block contains the transaction information, the blockchain, which is an aggregate of all the blocks, is a huge distributed book that contains all the transaction records.

Blockchain business and distributed ledger

Role of ledger

In today's tightly connected world, economic activities occur in business networks that cross national, geographic, and legal boundaries. Business networks typically converge into the market where producers, consumers, suppliers, partners, market makers, market enablers, and other stakeholders own, control, and exercise rights, privileges, and authority over valuable subjects otherwise known as “assets”.

Assets can be tangible physical assets such as a house or car or intangible virtual assets such as securities and patents. In a business network, the ownership and/or transfer of assets create value, and such activity is called a “transaction”.

A transaction generally involves many participants such as seller, buyer, and intermediaries (i.e., bank, auditor, and authenticator), and their business agreement and contract are recorded in the ledger. Businesses typically use multiple ledgers to track asset ownership and transfers between participants in multiple business lines. A ledger is a system of records (SOR) of the economic activities and interests of an enterprise.

Problem with business ledger

The business ledgers that are currently in use have several disadvantages in that they are inefficient and costly, and can be subject to fraud and misuse. Such problems occur due to dependence on centralized and trust-based third-party systems such as financial institutions, clearing houses, and financial institutions.

These centralized and trust-based ledger systems can cause bottlenecks and delays in the settlement of transactions. In addition, disputes can arise from vulnerability to fraud and corruption and a lack of transparency. Moreover, it is costly to resolve disputes, cancel

Archived copy · cryp2nova.com

transactions, or ensure transactions, and thus many business opportunities can be lost as a result of such risks and uncertainties.

Finally, it is possible to make the wrong business decisions due to temporarily inaccurate data if there is an asynchronous copy of a business ledger in an internal system of a network participant. One urgent problem that can arise before resolving a discrepancy in ledgers is a delay of the ability to make decisions based on correct information.

Block

A block is an element of a blockchain that conceptually means “a bundle of transaction information”. A block is composed of a block header, transaction data, and other information.

The block header consists of the version, previousblockhash, merklehash, time, bits, and nonce.

The transaction data comprise various data related to deposit and withdrawal, while “other data information” refers to information in the block that does not correspond to the block header and transaction data, and is not used for block hash calculation.

Blockchain network operation

The member nodes in a blockchain network use a consensus protocol to consent to the ledger content instead of relying on a third party, such as a financial institution, to mediate transactions, and to assure the integrity of the transaction using a cryptographic hash and a digital signature.

The consent guarantees that the shared ledger is an accurate copy and lowers the risk of illicit transactions. This is because the alteration of a record requires the alteration of multiple blockchains exactly at the same time. The cryptographic hash (e.g., SHA256 encryption algorithm) calculates another hash value if there is even the slightest change in the transaction input to indicate that the transaction input may have been corrupted. A digital signature guarantees that the transaction has been generated not by an impersonator but by the sender who has signed it with the private key.

The distributed P2P blockchain network prevents a single participant or a group of participants from controlling the underlying infrastructure or compromising the entire system. All network participants are equal and must comply with the same protocol. The participants may be individuals, regulators or organizations, or any combination of these types of participants.

The key to a blockchain system is to use a selected consensus model to record in chronological order the transactions whose validity all of the nodes have agreed to. As a result, a transaction cannot be canceled and remains in a state of agreement by all members of the network.

Archived copy · cryp2nova.com

Proof of work (POW)

You can understand POW as the proof or evidence that you have completed the task of adding a new block to the blockchain. To add a new block to a blockchain, you must calculate the block hash of the new block, and then calculate the nonce value, which is an item of the block header data of the block, to compute the block hash.

In conclusion, calculating the nonce value is POW.

Problem with POW

The POW algorithm is the Byzantine consensus algorithm proposed in the paper “Bitcoin: A Peer-to-Peer Electronic Cash System” written by Satoshi Nakamoto, the founder of Bitcoin. The block hash computed by the hash function of the block header data is inserted into the block to connect the block data hash, and it verifies the hash connectivity to confirm that the data have not been forged or tampered with.

However, the critical problem with the POW algorithm is that it is very slow and wastes much energy. One needs hash more than 5,000,000 TH/s (1 TH/s = 1,000,000,000 hash operations per second) of hash power to generate a Bitcoin block.

Proof of stake (POS)

The POS algorithm is a consensus algorithm that was first proposed by the cryptocurrency called PeerCoin. It was created to resolve the problem of energy waste as well as the “Nothing at stake” problem of the POW algorithm.

POS generates a block with a stake without wasting computing power. It is determined by the stake and the date on which the stake is generated. The date of the stake used for a block generation is initialized.

The current POS algorithm refers to all types of consensus algorithms that use the stake, including the algorithm proposed by PeerCoin. Although the algorithms are the same in that they use the stake to represent the leverage, their inner workings are very different.

Archived copy · cryp2nova.com

Ethereum switching to the POS algorithm

Ethereum, which was developed based on Bitcoin, also uses a POW algorithm. Therefore, it is preparing to switch to the POS algorithm to solve the problems of slow speed and energy waste inherent to the POW algorithm.

However, we are not sure if the transition to a POS algorithm will be successful for the following reasons. First, there is a possibility of hard fork caused by the change of mining method, which is likely to lead to a decline in the value of Ethereum as a currency since an Ethereum coin would be divided into three. Second, the new unproven programs could contain bugs and hacks, in which case Ethereum might return to the POW algorithm, which could in turn cause considerable confusion in the Ethereum ecosystem. Finally, even if a successful transition is made, the problem of what to do with the existing high-priced mining equipment will be more difficult to solve.

Hybrid design of MeconCash

MeConCash has adopted the blockchain technology for its internal cryptocurrency, which is used in payment, reward, and transaction on online and mobile services, in order to take advantage of its technical maturity and outstanding security features.

We stored and synchronized all of the transactions that occur on the network in the distributed ledger and thus made sure that all records contain the correct data. Moreover, we maximized the security with the SHA-256 hash algorithm technology to assure the safety of transactions through the blockchain.

Coin Name	MeconCash
Coin Abbreviation	MCH
Coin Type	PoW + POS
Hashing Algorithm	SHA-2(SHA-256)
Coin Issuance Period	UNDETERMINED
Block Reward	1000000/1000/100/0.001
Pre-Mined Amount	200,000,000(20%)
Total Coins Issuance	1,000,000,000
Coin Generated Per Day	No limit

Table 1. MeconCash Specifications

Archived copy · cryp2nova.com

POW & POS hybrid design

We solved the difficult problem related to energy efficiency in blockchain generation and network verification by applying and enhancing the POS algorithm used in PeeCoin as an alternative to the POW algorithm, which had the problem of consuming excessive amounts of energy for mining.

However, it was designed as a hybrid proof method that uses POW and POS together to generate the blockchain and maintain the network mining ecosystem. As the POW mining process becomes inefficient after a certain amount of time has elapsed and the blocks have been mined, the POS mode maintains the network and approves transactions by rewarding mining after that time.

(1) Securing stability of POW

The mining process of the POW algorithm generates the genesis block and the network that will be used by companies and other users of the platform. It also continuously generates blockchain data in the main network.

(2) Entering maturity of POW

We distribute MeconCash to our members through the platform and continuously record the transaction information and holding information of MeconCash - which is gradually distributed through continuous mining into the blockchain - in the blockchain in order to increase maturity and protect the blockchain data. The block reward during the “entry to maturity” period is accumulated in the network memory pool each time a block is generated, and the transaction fee (minimum of 0.01) accumulated by each transaction facilitates seamless network operation.

(3) Switching to POS

Holders of MeconCash will receive up to 1% of POS interest through the full node wallet at the end of the MeconCash distribution and POW data block maturity period. MeconCash must be stored in the wallet, and cannot be used during this period. The concept of our POS is to assure that all stakeholders are guaranteed a minimum level of benefit.

Some 500 million POW coins will be issued in total, of which 200 million will be mined in advance. Afterward, the holders of the coins will receive up to 1% POS interest based on the minimum maturity period for POS of 30 days and the maximum period of 90 days.

Archived copy · cryp2nova.com

POW algorithm in MeconCash

MeconCash uses the POW technology of BitCoin, which has proven its stability over the past ten years, and the SHA-2 algorithm, a set of cryptographic hash functions designed by the United States' National Security Agency (NSA). A cryptographic hash function operates mathematically with digital data and allows users to determine the integrity of data by comparing the calculated hash (the output of the algorithm) against the known and predicted hash value. MeconCash uses SHA-256, which belongs to the SHA-2 series.

SHA-256(M):
  (* Let M be the message to be hashed *)
  for each 512-bit block B in M **do**
    $W = f_{exp}(B)$;
    (* Initialize the registers with the constants. *)
    $a = H_0$; $b = H_1$; $c = H_2$; $d = H_3$; $e = H_4$; $f = H_5$; $g = H_6$; $h = H_7$;
    for $i = 0$ **to** 63 **do**
      (* Apply the 64 rounds of mixing. *)
      $T_1 = h + \Sigma_1(e) + f_{if}(e, f, g) + K_i + W_i$;
      $T_2 = \Sigma_0(a) + f_{maj}(a, b, c)$;
      $h = g$; $g = f$; $f = e$; $e = d + T_1$; $d = c$; $c = b$; $b = a$; $a = T_1 + T_2$;
    (* After all the rounds, save the values in preparation of the next data block. *)
    $H_0 = a + H_0$; $H_1 = b + H_1$; $H_2 = c + H_2$; $H_3 = d + H_3$;
    $H_4 = e + H_4$; $H_5 = e + H_5$; $H_6 = e + H_6$; $H_7 = e + H_7$;
  (* After all 512-bit blocks have been processed, return the hash. *)
  return concat(H_0, H_1, H_2, H_3, H_4, H_5, H_6, H_7);

Figure 11. SHA-256 algorithm

POS design of MeconCash

The POS algorithm of MeconCash is stable because it uses the same proven technology as PeerCoin, which was issued on August 19, 2012 as the first cryptocurrency to use the POS algorithm.

Block generation under POS

In the hybrid design, a block is divided into POW and POS, i.e. two different types.

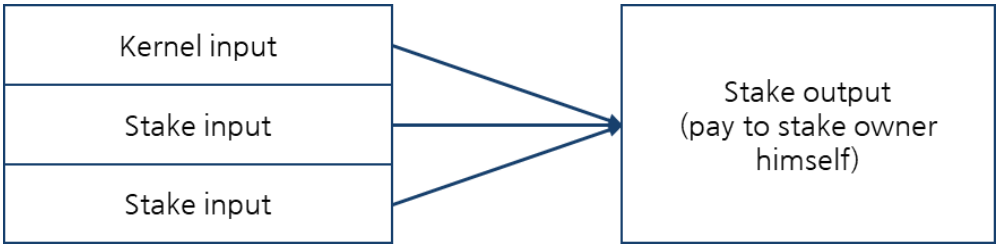


Figure 12. Transaction architecture of coinstake

Archived copy · cryp2nova.com

Coinstake (The name is borrowed from the “coinbase” used in Bitcoin.) is the trading structure of the new block type of POS. It secures the minting authority for generation of the block and the POS, while the block holder pays himself according to the age and quantity of the currency he holds. The first input in coinstake is called the kernel, which uses a specific hash target protocol to calculate the probability of generating a proof block similar to POW.

A significant difference here is that a hashing operation is performed through a limited search space (i.e. one hash being associated with a wallet output that is not consumed per second to be more specific) instead of an unlimited search space such as POW. Therefore, it does not consume much energy. For the hash target which the kernel stake must meet, the key (kernel) is the currency age spent per unit, i.e. the coin-day of the currency. Unlike the POW of Bitcoin, our POS system does not change the target value applied to all nodes. Therefore, more blocks can meet the harsh target protocol more easily when the kernel has a more prolonged retention period.

Protection of history in MeconCash

One of the main disadvantages of generating blocks according to the age of the currency is that the time needed for blockchain hacking decreases. Although the transaction records are protected with a powerful security scheme, Nakamoto announced the Checkpoint mechanism, which is designed to eliminate any possibility of transaction tampering, in 2010.

Moreover, the system performs the task of freezing prior blocks and completing transactions to prevent blockchain tampering by holders of large amounts of coins. A series of tasks periodically complete the previous transactions and blocks, and then add them to the checkpoint to ensure the stability of blockchain transactions.

Block signatures and duplicate stake protocol of MeconCash

Each block requires the signature of the block holder to prevent copy attacks. The duplicate stake protocol is designed to defend against attacks that generate multiple blocks using a POS, such as a Denial of Service (DoS) attack. All nodes collect the kernel and timestamp data of all possible coin steak transactions. If a block has kernels and timestamps, the “duplicate stake block” is ignored until the block has been confirmed as an orphan block

MeconCash blockchain explorer

MeconCash explorer is an explorer of blockchains. Currently, any user can query the latest block in the MeconCash blockchain, the transaction that has been consented to and verified in the block, and the wallet that contains the cryptocurrency. It uses components that are similar to those of generally well-known blockchain explorers of Bitcoin.

Archived copy · cryp2nova.com

MeconCash interest payment system

POW-based coins such as Bitcoin, BitcoinCash, and Litecoin perform complex algorithms utilizing the operational power of computers to prove the accuracy of transactions and record the blocks in the blockchain to secure safety.

It is necessary to have at least 50% of all coin network operational capacity to counterfeit a transaction; and, even if one has such operational capacity and succeeds in counterfeiting, it is likely that users will notice that someone is counterfeiting because of the characteristic of the coin network wherein all blocks are visible. People will not use the cryptocurrency if it does not guarantee the stability of the coin network, and the value of the coin will drop tremendously. As such, counterfeiting a transaction is not only physically difficult but is also economically unprofitable even if it succeeds.

However, the POW method requires a large amount of computation each time a block is recorded, and thus it takes too much time and consumes too much energy to verify the transaction. As a matter of fact, it takes at least a few hours and sometimes as much as a few days depending on the load of the coin network to send a Bitcoin, which is a POW-based coin.

On the other hand, the POS system does not require huge computation. While the POW is based on computational capacity, the POS grants the authority to generate blocks in proportion to the stake, i.e. the amount of coins held. Anyone who owns a coin can contribute to the coin network even if that person does not have a high-performance computer. A user verifies the transaction of a block by recording his or her stake in the block. Here, the stake is like the collateral of the block. It becomes more difficult to counterfeit the coin when more stakes are recorded in the block. As mentioned above, 51% of the total amount of computational capacity is required to counterfeit a POW-based coin network, but 51% of the total coin stake is required to counterfeit a POS-based coin network. It would require an astronomical amount of money to hold a 51% stake; and the value of the coin would decline and the asset value decrease if a counterfeit were attempted. If someone had a 51% stake, his or her intention would be to maintain the coin stably and in a valid status rather than counterfeiting the network.

Minting

MeconCash interest is the reward a coin holder receives upon generating a block successfully. This reward is the same as the reward received for mining, and is the compensation received for generating a block and contributing to the coin network. Minting refers to a coin holder's contribution to a coin network to generate a block.

Archived copy · cryp2nova.com

Minting uses the coin age value to determine how coins can contribute to the network. The coin's age can be calculated with the following formula:

Coin age = (Amount of coins held * No. of days the coins are held - 30)

The reason 30 is subtracted at the end is that the coin can only be used for minting after at least 30 days have elapsed since receiving the coin. The interest can be calculated using the coin's age as shown below.

Reward = ((Coin age* 33) / ((365 * 33) + 8)) * 0.01

Assuming steady minting, the above formula guarantees annual interest of around 1%.

You will receive the reward + principal when the reward is generated. It may take some time before you can actually use the coin since the coin network must verify the minting first.

Moreover, the date of interest is recorded as the last transaction date of a coin when it receives interest, and therefore it cannot be used for minting right away. You must wait at least 30 days.

It is not clear exactly how long it will take to receive the interest after beginning the minting. Although the coin wallet calculates and shows the probability of receiving the interest within 30 to 90 days, it is only a probability, and the interest payment may be delayed if you are not lucky. It is because minting, like mining, generates blocks through calculations, which means that it involves an element of coincidence. However, unlike mining, minting calculates within a very limited scope based on the amount of coins and the age thereof, which is an indicator of coin holding rather than dependence on computational capacity. Therefore it can be calculated on low-power devices such as smartphones and Arduino. For the same reason, minting does not guarantee that interest will be paid more often when using a high-performance computer. The number or period of interest payments is irrelevant to the total amount of interest, and there is only a difference in how many times you receive them.

Archived copy · cryp2nova.com

4. MeconCash Issuance

We will issue MeconCash in the following four stages: Initial Development Budget (200 million coins, 20%); Early Mining Rewards (33 million coins, 3%); POW Mining Rewards (267 million coins, 27%); and POS Deposit Rewards (500 million coins, 50%). We plan to issue a total of 1 billion coins over the next years. The max supply of MCH until the year 2050 is expected to be 236,000,000 by the current difficulty.

	Initial Development Budget	Early Mining Rewards	PoW Mining Rewards	POS Rewards
MeconCash	200,000,000	33,000,000	267,000,000	500,000,000
Share	20%	3%	27%	50%
End of Issuance	Genesis Block~200	Year 2018	Undetermined	Undetermined

Table 2. MeconCash Issuance

Initial Development Budget

The initial development coins will be issued after generating the genesis block and supporting the completion of software development. The amount of 100 million coin (50 %) will be kept for company's reserved share for a service, content compensation and transaction within the Mecon cash platform and the other 100 million coin will be used for development for app, game, P2P exchange service(25 %), domestic and oversea service operations (10 %), domestic and oversea marketings (10 %), consulting and strategic partners (5 %). Thus, 200 million MeconCash coins will be issued from the genesis block to the 200th block.

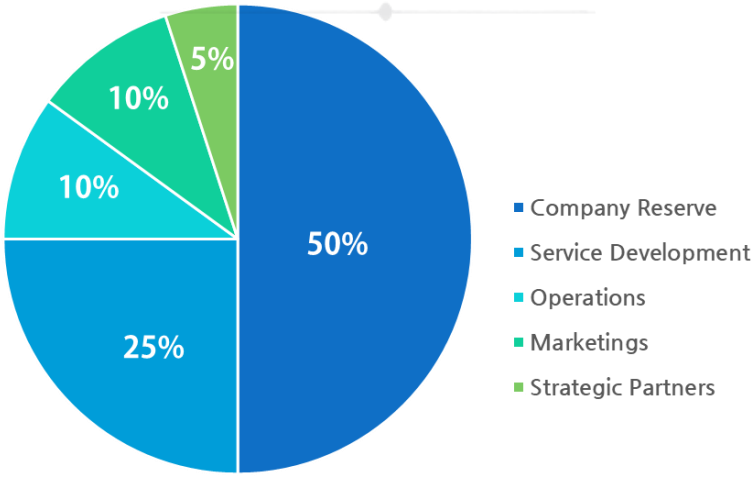


Figure 13. MeconCash Coin Allocation

Archived copy · cryp2nova.com

Early Mining Rewards

Early Mining Rewards is a reward by which 1000/100 coins will be paid at a time up to 33 million coins in order to generate initial blocks. Including the initial development budget, a total of 233 million coins will have been issued by the end of this stage.

POW Mining Rewards

PoW Mining Rewards is a reward by which 0.001 coins will be paid at a time up to a total of 267 million coins. Greater difficulty is involved at this stage than at the preceding early mining rewards stage. Including the initial development budget and the early mining rewards stages, a total of 500 million coins will have been issued by the end of this stage.

POS Rewards

The rewards for aging coins will be distributed in proportion to the number of MeconCash coins deposited in each node. They will be issued when minting begins, and the block will be generated. POS compensation will be based on the following formula: ((Coin age * 33) / ((365 * 33) + 8)) * 0.01; with 30 days as the earliest possible minting date, and 90 days as the latest. The total number of coins to be issued is 500 million, which is the total number of coins issued minus the number of POW minted coins. (Please refer to the section on the MeconCash interest payment system for more detailed information on interest payment.)

CRYP2NOVA

Archived copy · cryp2nova.com

5. Roadmap

Current progress

Prior to proceeding with the blockchain-based platform, we developed character-based smart applications, an AI-based avatar business card called LinkU, a character electronic business card called MeconTong, a gift mall called JangBoGo, a mobile game service, and an emoticon service. Our specialization in IT helped us to be selected as one of the “K-Global 300 companies” in December 2016.

We have more than 5 million members V, Thailand, and Vietnam. Our global members will become participants in the MeconCash platform and build the ecosystem for rewards, settlement, and transactions.

We are executing MOUs with domestic and foreign companies to expand the MeconCash services and business models, and preparing the necessary technology development and related services.

Patent	Registration Number
SYSTEM FOR PROVIDING MOBILE COUPONS AND METHOD THEREOF	10-2017-0008743
SYSTEM FOR PROVIDING MOBILE COUPONs AND METHOD THEREOF	10-2017-0008744
SYSTEM AND METHOD FOR MEDIATING CRYPTOCURRENCY DEALS	10-2018-0047906

Table 3. List of patents

Archived copy · cryp2nova.com

Roadmap

Schedule	Description
Oct. 2017	Began the development of the MeconCash blockchain coin
Apr. 2018	MeconCash pre-mining
May 2018	Distribution of MeconCash Wallet V1.0 Release of MeconCash Blockchain Explorer
Jun. 2018	Launch of domestic service of Coin25, P2P exchange for cryptocurrency Listing on the domestic exchange
Q3 2018	Distribution of MeconCash Wallet V2.0 Interfacing of Coin25 with MeconCash Wallet Signing of MOU for Coin25 operation in Indonesia Entry into Indonesian and Vietnamese markets with Coin25 Upgrading of AI of LinkU business card
Q4 2018	Development of ordered caricature and emoticon creation platform Development of MeconCash OPEN API
Q1 2019	Signing of Service Interface Agreement with Indonesia Telcomm Integration of service reward system with MeconCash OPEN API Launch of strategic RPG mobile game service and construction of reward system
Q2 2019	Distribution of Integrated MeconCash Wallet V3.0 Integration of the mobile coupon payment system within the services

Table 4. Roadmap

Archived copy · cryp2nova.com

6. Disclaimer

This white paper is intended to provide information on the business model and related technologies of MeconCash, a platform designed for multiple purposes, to those who are interested in the project related to the internal cryptocurrency platform used for payment, reward, and transaction on online and mobile services ("MeconCash Project").

This white paper is not intended to recommend investment in the MeconCash Project. We consider the opinions and feedback of MeconCash holders but do not grant them the right to participate in the development of the MeconCash platform.

This white paper is based on the current status of the platform at the time of writing. We cannot guarantee the accuracy and appropriateness of any content of this white paper, including the schedule and outcome of the project planned in the roadmap at the time of reading this white paper or in the future, and shall not bear any legal liability for such. For example, we cannot guarantee anything in relation to income or profits, the creation of contents on a legitimate basis without infringing the rights of a third party, error in contents, and legality of creation and distribution. Furthermore, we cannot guarantee that the MeconCash Project described in the white paper does not violate the national laws and regulations of the holder. Moreover, the subject to the disclaimer of the MeconCash Team is not limited to the above examples.

Please note that you shall be solely responsible for the consequences of any decisions that you make on the basis of the information contained in this white paper. In other words, the MeconCash Team assumes no liability for any damages, losses, debts or other consequences sustained by you in connection with your use of this white paper.

This white paper may be modified in accordance with the policies or decisions of the MeconCash Team. Please use the white paper as an overall reference for the business plan and vision as the project progresses, and check the final version for the official contents.

Archived copy · cryp2nova.com

References and Excerpts

[1] IBM developerworks / https://www.ibm.com/developerworks/cloud/library/cl-blockchain-basics-intro-bluemix-trs/index.html

[2] Bitcoin / https://bitcoin.org/bitcoin.pdf

[3] Peercoin / https://peercoin.net/

[4] Wikipedia / https://wikipedia.org

[5] NamuWiki / https://namu.wiki

[6] Darakbang, Lee Chel-hwan, Cryptocurrency Economics

[7] https://www2.deloitte.com/us/en/pages/financial-services/articles/making-blockchain-real-customer-loyalty-rewards-programs.html

[8] A study on the development of the evaluation model for the customer-centered membership service, Sungshin Women's University, Graduate School of Convergence Design and Art, 2014, pp.10

[9] Financial News, “Will the ‘blockchain revolution’ shake up the contents market?” http://www.fnnews.com/news/201805201755508539

CRYP2NOVA

Archived copy · cryp2nova.com