Abstract

Decentralized forum application platform using smart contract

Bitcoin, of which the blocks were first generated in January 2009, brought up global currency innovation. This was the first case to actually utilize blockchain and to move away from the traditionally non-reliable network to trust-based innovation using blockchain as the Bitcoin ledger, and eventually to bring about currency innovation. Since then, the use of Bitcoin has been steadily growing along with its technology development.

Whereas Bitcoin focused on the most basic functions of blockchain, the stable transfer and storage functions as a currency, Ethereum of which the first block was generated in 2015, added private contract on top of its transferring function. The first smart contract function was used to enable private contract on blockchain without the intervention of a third party.

Ethereum, also called blockchain 2.0 following Bitcoin, is a blockchain with a perfect turing-complete programming language embedded. This programming language allows users to directly build private contracts according to given rules. This contract not only includes literal contracts but also the generation of contracts in the concept of 'generating tokens' under conditions that meet the rules of ERC-20. By using the condition of being an Ethereum contract, it is possible to issue and transfer other coins on the Ethereum blockchain network, and already countless numbers of tokens are run on the Ethereum platform.

Ethereum is a continuously developing blockchain that demonstrates tremendous advancement. However, there are still many limitations for general users and application developers to actually apply its functions. Also, it is very much complicated for various social networks, communities and game websites to develop their own coins.

EtherSocial provides management tools that can generate tokens complying with the ERC-20 smart contract rules with a couple of clicks as well as API functions that are applied to various services. Through EtherSocial, website administrators can plan, make, create, transfer, manage and burn their own tokens.

Table of Contents

History

Introduction of Bitcoin

The first digital currency, Bitcoin, was first suggested in the thesis of Satoshi Nakamoto in 2008 under the title 'Bitcoin: A Peer-to-Peer Electronic Cash System'. ^{<1>}Nakamoto realized the transfer and storage of coins adopting the blockchain technology. Blockchain was suitable to be used as a financial transaction ledger, as previous data could not be modified and the issue of double spending could be prevented. It is difficult to forge or falsify blocks as hash information that requires lots of computing power for calculation is recorded in each block. Time is also recorded in each block and as blocks refer to the immediate previous block, all blocks would have to be forged, making it realistically impossible. There are opinions that implementation of a quantum computing could pose a serious level of threat to Bitcoin, however this would only be possible after more than a decade, meaning that this is a fully safe system at least for the foreseeable future.
Despite the absence of a central administrator for Bitcoin, about 500,000 blocks have been generated since the creation of the genesis block on January 9, 2009 without any hacking on

the Bitcoin itself, boasting a sound level of security. A daily average of 230,000 transactions take place through Bitcoin and a market capitalization of more than 200 trillion Korean Won was recorded.
As for Bitcoins, new blocks are generated through Proof of Work (PoW). The first cryptocurrency was made through the collaboration of voluntary miners even without the existence of central control or intermediary. To use the credit card, the most popular payment method in the modern society or for overseas remittance, a central server was required. A reliable institution such as a 'bank' or 'credit card company' that can prove that I have sent the money, was essential. Bitcoin enabled the transfer and storage of coins without a third party, making it truly a breakthrough innovation never imagined before.

Limitations of Bitcoin

There have been upgrades of the Bitcoin through continuous modification of codes. However, as it has been quite a while since the development of the Bitcoin and because it is the first cryptocurrency, Bitcoin has some obvious limitations.
It takes more than ten minutes for the transfer of Bitcoin, as a block is generated once every ten minutes. Also, because the value of 1BTC is excessively high, it is not easy to use it as a means for payment in actual life.
Bitcoin is a public blockchain and its transaction list is open to the public. As it is open to the public, Bitcoin is transparent and cannot be manipulated, but its weakness is that it cannot hide secrets. Many users who own large amount of BTCs may not want to expose their BTCs. Also, there are people who want to hide their transaction details. To overcome such limitations, coins with anonymity functions such as the Zcash or Monero have emerged.
Another important limitation would be that it is difficult to use the Bitcoin in areas other than the transaction of coins. The language called 'Script' used in Bitcoin only allows limited functions as there are no repetitive statements. Against this background emerged Ethereum, to go beyond its limits and to be expanded to other domains, not confined to the transaction of cryptocurrency.

Introduction of Ethereum

ICO (Initial Coin Offering) of Ethereum took place in 2014 and the first version was released in 2015. Ethereum was a platform that actually realized the concept of 'smart contract' using blockchain. The concept of smart contract is that when a contract is created with digital commands, the terms of the contract are automatically executed according to the conditions. DApps or decentralized applications that extend blockchain to various domains can be made easily than before using Ethereum. ^{<2>}
Ethereum users can generate a 'token' and use it for whatever purpose of the user. Once a new token is generated, the blockchain will be easily generated as well and transaction, wallet and explorer is given to the user who generated the token. The major difference between a token and a coin is that a coin has its own network whereas a token is made and run on top of a network of another coin. The common thing is that both have the transaction function and are recorded in the blockchain.
Currently 443 tokens are made based on the Ethereum platform and those account for 81% of the token market based on the types of coins. Tokens utilizing Ethereum enabled crowdfunding with multiple investors without an intermediary, and for the first time in June 2017, the amount invested through ICO into blockchain surpassed the amount invested through venture capitals, demonstrating the energy of ICO. Through ICO, small investors who were not able to participate with small amount of investment could invest in high-tech IT venture companies and projects and realize profits. Also, individuals and groups that already had ideas and technological know-how but insufficient capital found a new way of financing.

The most substantial risk to Ethereum was the DAO hack. Although smart contract was a double-edged sword that gave versatility, the rapid speed of development lowered the level of overall security. This resulted in the DAO hack and eventually led to the Hard Fork of Ethereum. Many of such security weaknesses are now substantially improved. Since the DAO hack in 2016, numerous ICOs took place on the Ethereum platform but no crucial security issues have ever occurred since then. Therefore, it is safe to say that the current Ethereum code has gone through years of stabilization and testing, and is now reliable.

Limitations of Ethereum

The most important issue of Ethereum is that it is difficult to directly introduce Ethereum to the general forum. To introduce a reward system using Ethereum, one needs to be capable of fluently using the smart contract programming language called 'Solidity' and also have a good understanding of blockchain. APIs exist in Ethereum, but are not specialized for forum websites. Therefore, web developers with less understanding of blockchain have relatively lower accessibility. Therefore, if one would want to introduce Ethereum to the forum, additional time and expenses for development will follow. After all, if there is a need for a forum-specialized cryptocurrency, there may be no substantial difference between developing it using Ethereum and developing new coins from scratch.

Introduction of Steem coin

Steem coin is a forum-specific coin of 'Steemit', of which sales began in 2016. The purpose of Steem coin is to generate coins that can be used across the forum. Steemit is composed of personal blogs and comments, and users who give good comments to postings obtain rewards. Individual users who frequently use Steemit can be rewarded through Steem coins. If the value of the user's Steem coin increases in the exchange, the user is bound to acquire additional profits as much as the amount of Steem coin the user owns.
^{<3>}
The Steem coin forum service itself was successful enough to have acquired more than 600,000 users. The value of Steem, the digital currency used in the Steemit forum, increased by more than six times for a year and eight months, since its launch in April 2016.

Limitations of Steemit

However Steemit also bears many issues. First of all, the subjects uploaded on Steemit are quite limited. Based on Google's related search results, most of the postings of users that appear as related search results for Steemit were subjects related to coin or investment. It is because of the difficult accessibility for first-time Steemit users. However, people interested in cryptocurrency actively join Steemit to get its rewards despite the inconveniences.
Another shortcoming is that Steemit is not specialized for Korean forums. In Korea, forums tend to use bulletin boards rather than blogs. But Steemit has its roots in an overseas website and only supports personal blog formats, making it difficult to introduce Steemit as it is to Korean type bulletin boards. Another issue is that most of the rewards are determined according to the opinions of a few, who own large amount of coins. Those who own lots of coins are the so-called 'whales' on Steemit and their one click of 'like' could lead to a coin reward equivalent to 300 USD.
If one would search 'Steemit' on Google, the first related keyword that appears would be 'haejin'. It is not sure whether the user of this ID is a Korean, but this user usually posts ten postings a day and receives a profit of about 300 USD for each posting, resulting in 3,000 USD worth of coin rewards a day. Earning a reward of 300 USD for a single posting with one simple illustration and one line of text seemed impossible to the general Steemit users, which in turn

made Steemit users to furiously click on the ‘un-vote’ tab. Nevertheless, 'haejin' keeps on with the posting and some users express concerns that 'only one whale is taking up everything. Steemit is getting out of order'. Another issue is that it has already been two years since the transaction of Steem coins, but there is no official launch of the API yet. Moreover, issuance of the SMT tokens which were planned to be released in 2018, did not happen either. SMT tokens are similar to the ERC 20 tokens and have a function of creating token for one's own forum. Eventually, the current Steem coin remains as a coin just for the Steemit forum. In summary, Steem coin became a coin just for the users who are interested in cryptocurrency, particularly for those using the Steemit forum.

Bitcoin and its basic concept

Basic concept of reserves

To complete the concept of digital currency, basically two goals have to be achieved. First is the safe storage and transfer, second is the verification of altered contents. Also, cryptocurrency is only complete when it is safe and anonymous at the same time. To satisfy these requirements, simple and complete security was achieved without being subordinate to specific groups. This was enabled through the nodes of the ledger called blockchain and a security process called Proof of Work (PoW) on top of the ownership management algorithm based on public key encryption.
Participants can take part in cracking down the codes of such blockchain only through 'computational capability' and this is the so-called 'mining' process. Mining creates a unique structure in which it deals with basic security and processing of transactions and also enables blockchain rewards to all participants. Therefore, transaction or transfer will not take place or be extremely slow on a blockchain (excluding the PoS) without a miner.

Mining

The structure of blockchain is very simple. The concept is about 'whether the first block is normal' and 'whether every subsequent block is normal'. All we need to do is to check whether the newly created blockchain is created normally, and if this process is continued, we will be able to have all our assets and transactions in one blockchain.

1. The first block and previous blocks agreed by all parties
2. Verification of a mix of transactions without errors
3. Generation of a whole block
4. Appropriate level of verification and relevancy of verification

Starting from a block of which past verification is completed, a miner just has to do the best to generate a complete and safe block. To obtain coin rewards, the miner is willingly providing his or her computational ability, and at the same time maintaining the security level of the blockchain. To hack the blockchain, one needs to deal with the computational ability of mining. Of course such mining consumes lots of energy and resources. Although this is an issue to be improved in the long-term, it still is the most effective security maintenance method.
EtherSocial follows the GPU mining method.

EtherSocial

The purpose of EtherSocial is to create APIs and management tools that could be applied to actual services using the decentralized application protocol. Ethereum itself is a developing blockchain that provides an essential and fundamental platform of blockchain embedded with the turing-complete language, but the following shortcomings make it hard to apply it to actual services.

1. Constant development
    - Constant development is a good phenomenon. But because development happens constantly, there were many times when security issues related to Ethereum account and others occurred in the meantime. It is important to have a stable version without any of these security issues.
2. General users or developers do not have easy accessibility
    - Since development is done mainly focusing on the functional improvement of Ethereum core, there are major shortcomings in the user environment. This is why it is almost impossible to apply it to general services as of now.
3. Too much network traffic
    - The network is always crowded with endless development and various tests going on. This is why the various smart contracts on the network are not successfully transferred in many cases.
4. Expensive fees
    - As the price of Ethereum itself has increased, the costs to realize smart contracts have become too high.

The EtherSocial coin which aims to solve these issues have the following features.

1. Only functions from the stable version are chosen out of the Ethereum functions.
    - Only the superior functions of the stable version are chosen and further developed.
2. Convenient usage
    - GUI management tools are provided to enable easy access to general users. Also, applying a language frequently used by general developers in the development allows the convenient use of APIs and the coins to be actually applied to various types of services.
3. By specializing in the token functions of ERC-20, usage of other smart contract functions are reduced and therefore the network runs more smoothly.
4. Token management can be done with less fees and at a lower price than Ethereum.

EtherSocial account

ESN is used to pay the transaction fee as a fee to run the smart contract of EtherSocial. There are two types of accounts. The first is an external account that is controlled by a private key and the second is the contract account controlled by the contract code. The external account does not have any code, so to send a message from this account would require a new

transaction and a signature. As for the contract account, whenever a message is received, a personal code will be activated to read and internally store the message. Afterwards, messages can be sent or contracts be generated.

Message and Transaction

Transaction refers to the transferring details of EtherSocial and includes information of who sent what to whom.
Transactions include the following information. ^{<2>}

- Recipient
- Signature of the sender
- Amount of ESN the sender is sending
- Option data
- Permitted calculation frequency
- Calculation fee

Recipient, sender or the amount to be sent are items commonly used in most cryptocurrencies. Items such as the permitted calculation frequency and calculation fee perform the roles of blocking DDos attack in EtherSocial.
To prevent repetitive execution of transactions caused by mistake or limitless arithmetic carried out maliciously, ESN should be paid as a fee at each step when executing the code in the transfer of transactions. The basic unit is 1gas and if the transfer takes up more time or is complex, more fees should be paid. In this way, a malicious hacker would need to consume too many ESN for an attack which is less tempting for someone who holds lots of ESN. Thus, malicious attacks can be prevented more efficiently.

Messages

Transfer contract can call out other contracts using messages and then deliver information. In other words, smart contracts can be delivered using messages.
Messages include the following information. ^{<2>}

- Sender
- Recipient
- ESN
- Option data
- Permitted calculation frequency

Messages are similar to transactions except that messages are not from external accounts. Like transactions, messages will execute the relevant codes in the recipient account. The gas allocated to the transaction or contract is applied to the total amount of gas consumed due to all executions related to that transaction. For example, if an external account A sends 1000 gas and a transaction to B, and B sends a message to C after consuming 600 gas, and returns after consuming 300 gas for internal execution of C, B will be able to use 100 more gas before all gas is depleted.

Blockchain and Mining

EtherSocial blockchain is similar to the previously explained Bitcoin blockchain, but is also different in many ways. The major difference is that unlike Bitcoin, EtherSocial blocks include the most recent state of the account, block number and difficulty. Since Bitcoin blocks do not

have block numbers, one needs to start counting from the very first block to know the block number.

The following explains the basic methods of verifying EtherSocial blocks. ^{<2>}

1. Check the existence and validity of the current block.
2. Check whether the timestamp of the current block is greater than the previous block and does not exceed 15 minutes as of the current time.
3. Check the block number, difficulty, transaction route, uncle route and gas limits.
4. Check the validity of Proof-of-Work (PoW) of the block.
5. Assume that S[0] is the final state of the previous block.
6. Check errors on the transaction list and whether the amount of consumed gas did not exceed the gas limit.
7. Verify the reward block paid to the miner.

It is very efficient to put all information into the block. Information will be stored in a tree structure and only a smart part of the tree behind all blocks will be altered. Unlike Bitcoin, as most contents of the tree are the same between the two adjacent blocks in EtherSocial, once stored data can be re-used again in the next block. On top of the concept of the Merkle tree, data can be input and deleted efficiently, and since information on the account's change of state is included in the last block, it is not necessary to store the whole blockchain information.

A smart contract is created when contract code of each transaction is executed at the same time when the blocks are being verified.

Applications

Token Systems

The blockchain token system has applications that realize many types of transaction systems on the network, from the sub-currency linked with US dollars or gold, smart property (assets of which the ownership is controlled/managed on the Bitcoin blockchain), secure and unforgeable coupons to other token systems (for example, point system to provide incentives) not linked with conventional value. The token system on EtherSocial can be realized in a surprisingly easy way. The following are the core parts in understanding the token system. ^{<2>}

- Currency and token systems execute only one function.
- Currency/token of unit X is deducted from A, and the deducted currency/token of unit X is paid to B. However, A should have held a minimum unit of X before the transaction.
- A approves the transaction.

In EtherSocial, the user just has to reflect the above logic to the contract. The basic codes that execute the token system in the Serpent are as the following.

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

In this case, the 'state transition function' of the banking system explained in this white paper is applied per se. To define the unit of the currency and do the initial work for distribution, or to enable other contracts to process information requests on the balance of accounts, additional lines of codes could be written. But that is all we need to make a token system. Theoretically,

the token system as a sub-currency system based on EtherSocial may have an important feature the MetaCurrency (currency linked to the Bitcoin blockchain) based on Bitcoin does not have. It is that payment can be directly made with the currency used when trading the transaction costs. Such feature can be realized through the following process. To execute a contract, the ESN balance should be as much as the costs to be paid to the sender. And the internal currency that is received as a fee when executing the contract, can be immediately exchanged and charged as an EtherSocial balance. Although users have to 'activate' their accounts through the ESN, the amount obtained through each contract can be exchanged to ESN every occasion. This implies that a once-charged ESN can be re-used.

Application process of incentivized communities

Requirements for commercialization of coins

EtherSocial was designed for the pay-type contents forum. It also brings contents creators of blogs to the forum. Coins can be applied to click-type reward, recommendation based reward and direct purchase for the contents without the server or DB approval, and can bind the contents from different servers working in different portals together.
Numerous coins are released with more than one role. Through the white paper that can utilize blockchain technology and various types of application software, we can observe the possibilities of that blockchain contributing to other fields. However, out of the vast number of coins, there are only a few that are commercialized according to the white paper, which arouses serious suspicions regarding the commercialization of coins and blockchain. We need to consider why there are less coins applied in the daily lives, despite the already verified and abundant security and transfer technologies in place and the possible distribution of numerous application software and contents.

1. First would be the gap between the blockchain ecosystem and the developers of general contents/software. Up to now, blockchain is considered to be in the realm of virtual currency and it is mainly the miners or investors who are interested rather than other software developers.
2. Also, most of the investments in coins, like the ICO, are mostly interested in the stable launch of coins through effective marketing rather than the stable settle down of actual application software. Eventually the tendency is to first focus on the profits of existing investors by creating coins and going public on the market.
3. There were a couple of efforts, however since blockchain is mainly focused on the owning and transferring aspect based on security, there is some animosity towards lowering the speed or reducing network resources by adding other functions. Nevertheless, coins should not only be owned or traded but more widely used by transacting with various application software and systems. There are concerns that continuous ICO and the flood of investment into new coins amid this situation could make the entire cryptocurrency ecosystem into a speculative ground. Therefore, this is the time when we need a case of integration and operation of actual software.

Based on the existing cryptocurrency forum 'DDengle', EtherSocial begins its service from providing modules required for running an actual forum and collecting cases applied in the operation of forums. This is the outcome of excluding means to raise funds such as ICO, and transparently opening up all processes from mining to generating/distributing coins, as well as deriving the direction based on the agreement of collective intelligence.

Coin features to vitalize forum

Forum administrators can set up a more extended reward system from the existing concept of mileage. Coins can be used as existing points or mileage within the forum and as rewards for external partner companies or advertising and marketing. Each forum coin that is made as a token provided by EtherSocial can be freely distributed, listed and traded. Further expansion is possible based on such liquidity.

1. Rewards can be provided directly to other forums and advertisers. In other words, a certain amount of coins will be distributed to the advertisers in advance, and the advertiser can provide the rewards directly to the customers.
2. Escrow services appropriate for P2P or secondhand trades can be provided. In other words, the deposit amount can be provided with the tokens, and as soon as the deal is approved, the tokens can be liquidated or the tokens can be traded again.
3. In particular, providing additional rewards for game ranking is also possible. By using tokens when partnering with external game companies, forum users can be easily brought to the game company, or user activities from the game company can be brought to the forum.
4. Such functions can be immediately applied without having to modify existing mileage, points or levels. Like the example of 'DDengle', existing points can be converted, paid and used.

Basically, if a forum wants to distribute, transfer and manage coins, it needs other coin controlling parts along with the wallet. These parts would be similar to the roles played by existing 'exchanges'.

Essential factors of the forum to utilize coins

1. The user can create an own wallet for deposit, and through this wallet the user can receive external coins or tokens on the blockchain network.
2. The forum can create deposit wallets by users subordinate to the user's hot wallet, and forum coins coming in at the same time from externally can be received.
3. The address of the coin will change if there is a behavior of the user creating a trading rule for coins and executing the rules. Although mutual deals accompanying cash are mostly used in exchanges, address of the coins will change in the forms of recommendation, donation and entries in the forum.
4. If these occur in the forum (in this chapter 'exchange'), direct transfer to the DB will be done without using an external blockchain network.
5. Every user can create a wallet for withdrawal which can be used for direct remittance to an external forum, personal wallet and if listed, to a local or overseas exchange.
6. Within the forum, the administrator can provide coins according to internal rules of the forum based on activities such as login, writing comments and recommendation.
7. Every member can donate coins to other members or give coins as a return for the comment and also receive coins from other users based on their activities.
8. To prove the transaction, certain parts of coins of a certain user can be locked in. Such lock-in can be used not only for the escrow function but also for the coin to be proof of various transactions and for betting processes, and also can be led to actual approval by linking with subsequent actions.
9. Coins can be used not only for conditional events but also for bets or betting between users, and even be applied to simple games within the forum if stronger modules are utilized.
10. The forum has been designed to introduce its own fees. The administrator of the forum can define a certain fee rate for the transactions between users in advance, and can collect certain portion of the coin profits.

11. Since EtherSocial and coins based on it both use blockchain, if there are deposit/withdrawal with parties outside the forum, there will be fees for blockchain miners which become profits for them.
12. The forum can decide on its own fee rate, however a very low fee rate can be rejected by miners like other blockchain coins and the forum can experience lots of delays. This is not something an EtherSocial company should be involved in.
13. Coins can be used instead of cash to apply for various events within and outside the forum, and a limit per person will prevent the tyranny of certain users holding large amounts of coins.
14. Moreover, the use of EtherSocial or token as a reward for user actions such as recommendation is encouraged, as the purpose is to enable actual contents creators to make profits.
15. As small forums can experience difficulties in developing their own coins because of the blockchain technology and difficulties in the verification process, it is recommended that those forums issue tokens on EtherSocial.

Expansion functions to various forums such as games

EtherSocial especially is designed to be firstly applied to contents reward-type forums, and modules will be continuously expanded to be applied to game forums and social network services moving forward.

1. External advertisements can be purchased through EtherSocial or EtherSocial based tokens.
2. Such advertising reward can be provided to the contents producer.
3. By restricting recommendation or donation per person, a more democratic voting can be enabled.
4. The same reward is provided to blogs and forums within the forum. (Rewards can even be transferred to a blog outside the forum. In this case, the blog should have an EtherSocial wallet.)
5. There are functions such as exposing the ranking of coins and recommendation, however it is encouraged to disable the contents producer from checking such information. (With the right of the forum administrator, owned coins can be exposed, and marketing or contents can be provided to members above a certain amount of coin). However, as long as the coin is permitted to be transferred externally, it is better not to be exposed due to security reasons.

APIs required for actual application

The forum defines the functions of core items and explains how to realize each modules. To apply the coins to actual software, there needs to be a system in place that distributes the wallet to each member. Beginning from security, such a barrier is a similar difficulty existing exchanges had. Although coins are designed to protect copyright and to be distributed, if the user still has to program the wallet, it would remain as a concept that cannot be eventually used. To solve this fundamental issue, EtherSocial provides a solution by providing additional APIs for the parts where application software control the wallet and the coins. Initial APIs are basically limited to the forum, and APIs to utilize blogs and game item trades will be continuously added.

List of basically required APIs

1. Lock-in

- Definition: Lock-in is to fix the change of state of the users' coins for a certain period or until a certain event takes place.
- This function is basically set up to guarantee behaviors after the transaction or to provide escrow functions.
- Most of the lock-in takes place due to the action chosen by the user, but some lock-ins are automatically given by the system.
- Types of lock-in defined by the user: preparation for transaction, auction, cancellable transfers
- Types of lock-in defined by the system: block condition of the account, preparation for transaction approval
- Cancelling lock-in

2. Generating coins (an act of distributing to users from the forum)

    - Definition: Actual coins are not created, but coins owned internally by the forum are distributed to members)
    - Basically, coins are paid together with the internal mileage system of the forum or points.
    - Coins can be continuously distributed through participation in events, writing comments and recommendations.
    - There is a high possibility that the distribution of APIs can be 'misused'. Other than functional hacking, issues such as repetitive membership subscription, help in recommendation can continuously occur. It should be kept in mind that if an appropriate cap is not created to the application of API, a very serious problem might occur, coins might evaporate overnight and there could be a rapid increase of inflation within the forum.
    - Manual distribution of coins is supported. Automatic distribution of coins is possible, but it is better to manage the overall amount of coins through manual distribution.

3. One-sided provision

    - Definition: The act of a user transferring coins to another user or an entity(business member etc.) within the forum
    - One-sided provision is used as paid recommendation, applying to events and donations etc.
    - Promises(such as an agreement to receive money when the novel is published) that have not been further confirmed or cannot be received, are considered as one-sided provision even though they might look like transactions.
    - One-sided provision is different from the 'withdrawal from wallet', of which coins go out through the wallet.

4. Mutual transaction

    - Definition: The act of trading between users that include coins
    - As a forum is not an exchange, such trading can be acted as secondhand deals or digital contents transactions, although it does not happen that often.
    - Very limited APIs will be provided. To use this part more extensively, it is recommended that development is done with a comparably qualified programmer. Basic APIs that are provided do not include all of these commercial purposes, and such commercial usage includes broader security issues and responsibilities. Basic APIs do not guarantee the service itself and these parts should go through additional programming under the responsibility

of each forum.

5. Creating a wallet address for deposit and withdrawal

    - Definition: Creation and management of the forum's wallet address to receive coins of individual users
    - Although the coin wallet is in the form of a 'token', a personal wallet can be created and managed. However, a forum member does not need a wallet as it can be almost unnecessary. The forum will create and manage the address of the wallet by members of which deposit and withdrawal is possible, so that the wallet can easily receive or send external coins.
    - Managing the balance between coin deposit/withdrawal and internally owned coins, is very crucial. This is not only an item of which it is difficult to provide a separate API, but also very closely related to the forum policy. For this matter, balance of other parts of the forum should be well adjusted based on the balance of the wallet or adjusted by creating an arbitrary balance adjustment account.
    - For blockchain related issues regarding actual deposit and withdrawal, if possible, EtherSocial Explorers provided by EtherSocial or external developers should be used.

Development plan for reward-type contents forum

General forms of current forums

1. DDengle is a forum in which discussion takes up the main part. Because of that, there is less burden for producing contents, as comments or participation of other users complete good contents. Production of contents is followed by discussion and verification, different opinions from different positions, making this whole process into good information and contents.

    - DDengle is a bulletin board type forum in which contents are not subordinate to the writer but to the forum, and there are no separate profits to be provided.
    - Support, criticism and verification are inevitable.
    - Although the writer might be a famous person, users generally depend on recommended articles rather than searching the writer's name.
    - As the bulletin board is standardized, continuous management is required. Equal forums are not always the good forums. It is vital to manage various newcomers and inappropriate articles.

2. Individual blog type forums. Individuals can produce their own contents and provide high quality contents, as series can be posted on the blog for a long-term. However, difficulties in advertising and exposing oneself could aggravate the 'rich-get-richer and poor-get-poorer' phenomenon. As the forum is about personal services, actual sales or profits of advertising or partnership expenses can be generated. Such motivation can always be substantial help to the creator.

    - The issue with the blog format is that the blog is proportional to the creator's ability, but it is also possible to do greater and diverse directing and expressions.
    - Therefore, lots of efforts are required for creation of contents, and there could be a huge gap in terms of quality.
    - Various profit models such as advertisements can be deployed, and stable

provision of contents to followers or neighbors that are continuously added up, will eventually increase profits.
- Copyright is clear.
- Arrangement and classification of contents is clear and relatively easy.

Development direction

Advantages of the discussion forum composed of bulletin boards and blogs should be combined, and coins should be used as intermediaries for profit distribution and contents vitalization to make users intervene more actively. To this end, general creators should use the application software APIs of EtherSocial that are applicable.

1. Articles posted on the bulletin board should be able to be grouped in the form of a blog.
    - Basically, the format of the forum should be the bulletin board where discussions and verification are possible.
    - Articles posted by users can be grouped and made into blogs, or linked and categorized.
    - Information on advertisements or clicks of the article should be shared.
2. 'Paid recommendation' and democratic recommendation using coins should all be permitted and direct profits should be generated.
    - By applying EtherSocial to advertising expenses or recommendations, rewards should be directly paid to the creator.
    - By purchasing coins, advertisers should be charged using more improved filters.
    - By utilizing 'paid recommendation' for both article and comments, readers can reward the creator.
    - By setting limits per person for the number of recommendations, democratic decision-making on ranking can be enabled if necessary.

Active profit sharing

When using EtherSocial, we can receive advertising expenses or donations through our wallets not only from our own forums, but also from external partner websites or individual homepages. There could be benefits such as additional profits being generated utilizing existing contents and importing one's blog into a new forum.

Our goal is the update of a new reward type contents forum in the fourth quarter of 2018.

Reward program for EtherSocial developers

Scope of reward program

From its beginning, EtherSocial was created based on the collective intelligence of the forum and contributions made by an extensive range of participants even not only developers. Therefore EtherSocial includes a reward program for developers who participated in the development starting from coin distribution, marketing and for all other participants who have

contributed to the improvement and development of blockchain and cryptocurrency. This does not necessarily have to be improvement of EtherSocial coin but includes active participation for the Crypto-Community Forum DDengle or our own development other than GitHub. These would include hardware or management software for mining, suggestions for actual use of existing coins, but are not related to profits. However, such reward programs exclude the development of new coins for the purpose of ICO. ICO itself is still closer to a profit-making model but has the possibility to be changed in the future. Detailed standards regarding the scope of the reward program are described as the following.

1. Contributors for the development of EtherSocial
    - Contributions to the development, modification and stabilization of sources for GitHub of EtherSocial
    - Contributions to the addition, modification and supplementation of contents of Wiki excluding the program itself
    - Contributions to the improvement of languages and policy directions of each countries
    - Contributions to local and foreign partnerships for the actual use of EtherSocial
    - Contributions to the development of individual contributions evaluating algorithm
2. Improvers of the mining system
    - Contributions to the development and maintenance of local and foreign EtherSocial mining pool
3. Application Software Developers
    - Contributions to the development of EtherSocial based DApp related to the forum, social network service, game and media
    - Contributions to the development of APIs for the development and improvement of application software
4. Individual who strived for the development of cryptocurrency and improvement of its image using marketing and social network services
    - Contributions to EtherSocial marketing and its vitalization providing qualitative and quantitative contents
5. Individual who contributed to considering the drawing up of policy or its direction
6. Individual who contributed to the new concept and its possibility
    - Contributions to the technological and applicable expansion of EtherSocial

Reward program

The challenges of EtherSocial are to assess the level of contribution on a fair basis and provide rewards thereof. EtherSocial's development forum will continuously discuss about additional contributions and rewards, and the discussion outcomes will be applied henceforth. The details of the support plan are as the following.

1. Plan to vitalize individual donation
    - Contents creators or programmers and marketing people can register on the EtherSocial creators' forum and create anonymous accounts for donation.

    - This account does not expose personal information and includes the address of EtherSocial internally.
    - If anyone from the registered account makes a donation, EtherSocial managers will make an additional donation equivalent to the donated amount.
    - Of course, there is a donation ceiling per person to prevent the operational funds from being depleted due to excessive donation of a single person. Also, adjustments will be made for fairer execution.
    - The modules provided by EtherSocial are designed to enhance stability of donation and meet the interest of contents providers by additionally providing an amount almost equivalent to the donated amount.
    - Individual donation will be vitalized by providing benefits worth the donated amount to the donator.

2. Reward plan according to contribution rankings based on voting

    - As it is almost impossible to objectify rewards for individual contribution, periodical or non-periodical voting is done to release the ranking reflecting collective intelligence and to provide the corresponding reward.
    - A list of candidates is drawn up every month or occasionally by getting recommendations through EtherSocial’s website.
    - Details of actual activities and support provided by the candidates are released and online voting is carried out.

Roadmap

1. The first ESN was mined on December 26, 2017.
2. A beta test carried out by selecting members of the forum 'DDengle' on January 15, 2018.
3. 5million coins allocated to the forum 'DDengle' in the fourth week of January 2018 (to be used for the next ten years).
4. The first ESN coin mining pool opened in the fourth week of January 2018.
   Direction of batch coin distribution announced to the members of 'DDengle' in the fourth week of January 2018.
   (Existing member ratings and activity index reflected)
5. Formal launch of the EtherSocial coin in the fourth week of January 2018 (official launch).
6. Additional coin distribution to members of 'DDengle' in February 2018.
7. Release of official ESN White Paper in February 2018.
8. Announcement for joint development with external forum based on ESN in March 2018 (technological support for token development of external forum).
9. Official announcement of APIs for the use of external forums in April 2018 (application cases of DDengle etc.).
10. Meetup to be held through the mining conference in April 2018.
11. Launch of coins for the use in overseas forums in the third quarter of 2018.
12. Listing of ESN on foreign exchanges in the third quarter of 2018.
13. Launch of coins for two to three local and overseas external forums in the fourth quarter of 2018.
14. Launch of integrated operational tool that combines forum and coins in the fourth quarter of 2018.
15. Overseas launch of 'contents reward type forum' in the fourth quarter of 2018.

Other issues

Introduction of uncle blocks

EtherSocial introduced uncle blocks for the following reasons. ^{<2>}

EtherSocial has a very short block generation cycle compared to the ten minutes of Bitcoin. This causes weakened security due to the following reasons. Let us assume that miner A generated a block. A generates the block and transfers the block to the network. In the meantime when A's block has not yet arrived to miner B, B might have generated a block too. Since EtherSocial provides numbers to blocks, the block of miner A and miner B will have the same block numbers. In Bitcoin, only the block of miner A would be recognized and the block of miner B would be discarded, which means that the resources of miner B is wasted and did not contribute to the network security.

Also, there is the issue of centralization. If miner A has a hash power of 30% and B of 10%, the risk of A producing a stale block will always be 70% (as for the other 30%, since A created the last block, A would immediately get mining data), and B will always have 90% risk of producing a stale block. Therefore, if the block cycle is short enough necessary for the high stale rate, A would have much higher efficiency just by the fact that its size is large. As these two effects are combined, there is a high possibility that in a blockchain of which the block cycle is short, a single pool with a high hash power share will have actual control over the mining process.

This is why we do not only provide rewards to the blocks of longest chains but also to blocks that are almost generated at the same time but have slightly less hash power. Those subordinate blocks are called as uncle blocks derived from the word 'uncle'. These uncle blocks also get 87.5% of the original rewards and ‘cousin’ blocks that include the uncle blocks receive the remaining 12.5%. However, transfer fees are not given to uncle blocks.

EtherSocial provides rewards up to the seventh generation of uncle blocks. This is because if rewards are given without any limits, uncle blocks can increase tremendously and calculation will become much complicated. Secondly, if uncle blocks are given limitless rewards, instead of mining the main, miners will intentionally mine from the uncle blocks.

Fees

As all transactions included in the blockchain require computing resources to download and verify the transactions, a cost for using the resources, the so-called transaction fees need to be paid. Transaction fees are definitely required, because if not, excessive amount of transactions would consume computing resources and transaction issues could arise. Likewise, transaction fees need to be paid for the transaction of ERC-20 tokens to prevent the abuse of transferring tokens. In Bitcoin mining, as the sender voluntarily sets the fees and higher fees are prioritized in mining according to the principle of market competition, transaction fees and generation of blocks are determined based on the principle of supply and demand.

However, one issue is that there are always miners who want to maximize profits when generating blocks through transactions. This is why the following problems can occur.

First, to generate a block, numerous transactions need to be verified and a hash that generates the blocks need to be made. However, as it takes time to verify the transactions and there is higher possibility that block generation is delayed, miners might not be able to make profits. Also, as much as the time is delayed, there will be less time for preparation to generate the

next block, which eventually lowers the possibility of generating a block.
Second, miners only want to include transactions that require less time for verification and that can maximize fee returns.

Because of these reasons, if a rational fee structure is not in place, transactions of EtherSocial and ERC-20 tokens might experience difficulties.

Currency and Issuance

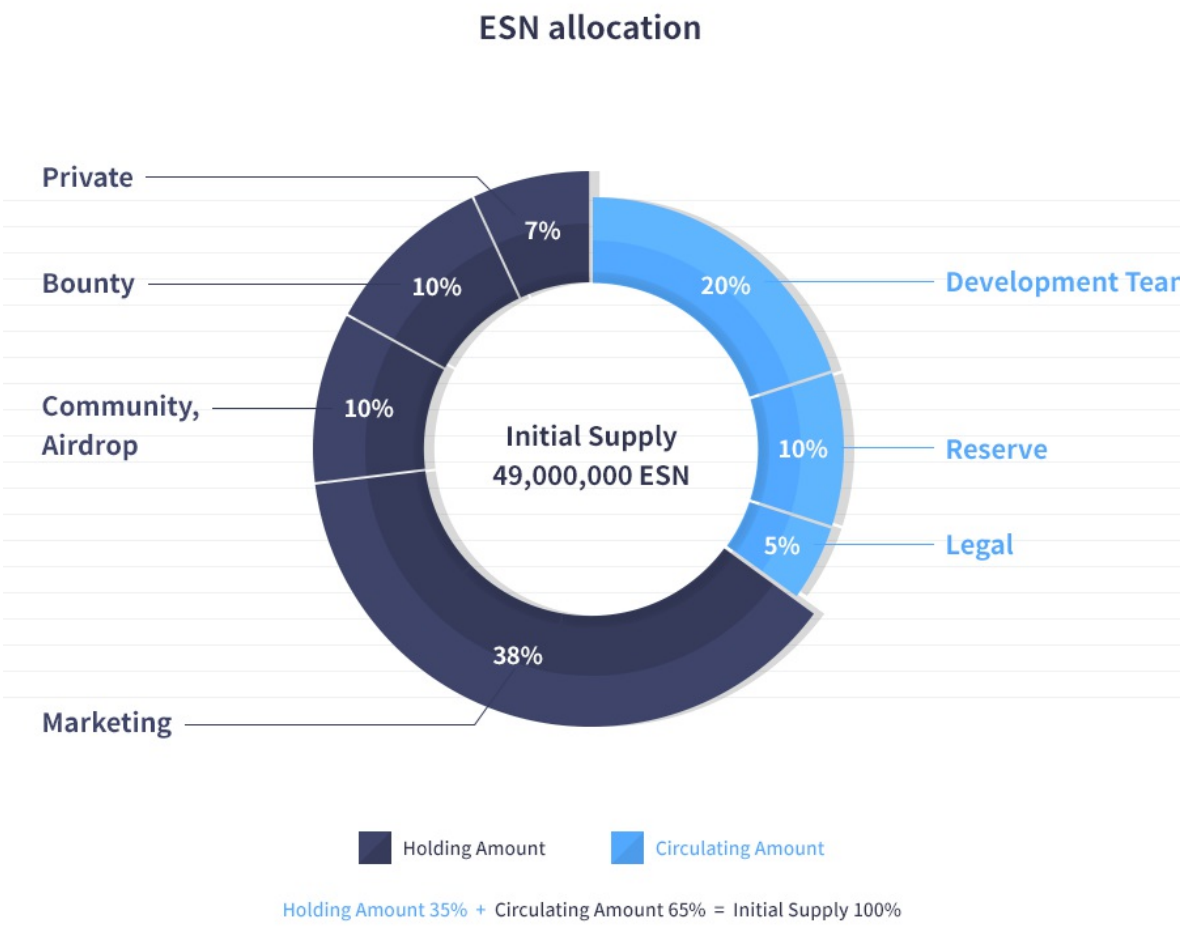
The EtherSocial network has its own currency called 'ESN' which is used internally. ESN is an intermediary that enables efficient exchanges between various digital assets, and also provides ways to pay transaction fees. For the convenience of users and to prevent any possible disputes, the names for each unit of ESN are already defined as the following. (Refer to arguments about the naming of Bitcoin)

- 1: wei
- 10¹²: szabo
- 10¹⁵: finney
- 10¹⁸: ESN

It will be easier to understand, if the above names are thought as extended concepts like 'dollars' and 'cents' of the American currency, or 'BTC' and 'Satoshi' of Bitcoin. Other names are not included in the client as of now.

Currency issuance model:

- ESN is used to financially support the EtherSocial organization, to collect funds necessary for development, to give rewards to developers and as an investment fund for various profit-making and non-profit projects related to EtherSocial.



- Initial EtherSocial amount which has been secured before making public was owned by the ‘Development Team(Geminis)’ and the initial supply amount is 49 million ESN. This amount is divided into Holding Amount and Circulating Amount, Holding Amount is long-term internal ESN for Development Team, and Circulating Amount is for public circulation towards general users.

❇ Holding Amount

- Holding Amount is 35% of the initial supply amount, and it is used for ‘Development’, ‘Reserve’, and ‘Legal’. ESN allocated for ‘Development’ can be used directly for ESN core and ecosystem development and supports the development team, which is about 20% of the initial supply amount.
- Among ‘Holding Amount’, the Reserve is about 10% of the initial supply amount. The reserve will be kept for a long period, and if an unexpected situation happens, this amount can be used. Besides, ‘Legal’ amount, which is about 5% of the initial supply amount, will be used for such as legal advisory expenses.

❇ Circulating Amount

- Circulating Amount is about 65% of the initial supply amount. This amount will be circulated externally. As for Marketing, 38% of the initial supply amount, can be used as marketing expenses such as active advertisement and promotion. For community and airdrop, about 10% of the initial supply amount will be allocated and so more users will use ESN.

- ‘Bounty’ means ESN rewards for special mission participants or contributors of development and design. It is also about 10% of initial supply ESN is allocated for ESN development and spread. ‘Private’ amount, which is 7% of the initial supply amount, can be exchanged by Ethereum.

❇ ESN supply after initial issuance.

- After the time of mining, 18,709,078 ESN are newly issued for the first one year and after that every year a total of 15,626,576 ESN are newly issued to miners.
- After that, depending on the level of block and mining difficulty, mining amount can gradually decrease.
- Mining algorithm can be changed by developers depending on the level of mining difficulty and the use of a mining equipment.

The following explanation is about the legitimacy of the 'EtherSocial forum's reserve'. For example, EtherSocial can be constantly distributed every year for ten years and contribute to increasing the user base. A certain portion will be distributed according to the contributions of the forum's members and another portion can be distributed through specific events. Also, EtherSocial can be distributed if necessary, as a basic asset for using EtherSocial tokens in other forums or websites. If there is no such reserve, EtherSocial cannot be easily acquired and the user base will inevitably become smaller.

Legitimacy of the 'distribution to EtherSocial's development organization (Geminis)' can be explained as the following. Many development human resources, planning and marketing manpower are required to develop blockchain and various APIs as well as for repair and maintenance. As expenses are accompanied in running an organization, to cover such expenses, EtherSocial has to be distributed to the EtherSocial development organization. For legitimacy of the 'long-term reserve', the following explanation can be applied. This long-term reserve is not to be distributed to the market for at least one year (or more than a year). For the first one year, mining reward is 18,709,078 ESN, meaning that the proportion of the mined amount to the initially issued amount is much higher than other cryptocurrencies. However, if initial issuance is increased too much, then ESN may not become a widely used cryptocurrency. Therefore, initial issuance should be kept at a level lower than the half of Ethereum but not too low, and distribution for the first one year should be prohibited.

For comparison

- Initial issuance of Ethereum is 70,002,436 ETH and mining reward for the first one year is 15,626,576 ETH
- Initial issuance of EtherSocial is 49,922,490 ESN and mining reward for the first one year is 18,709,078 ESN. Afterwards, mining reward per year would be 15,626,576 ESN.

Permanently issuing new coins from a set amount of ESN could relieve the 'concentration of wealth phenomenon' currently Bitcoin is experiencing. Also, it provides opportunities for current or future participants to acquire EtherSocial through mining and not through the market. By increasing initial mining more than Ethereum, 9 ESN shall be set as the mining reward until 300,000 blocks and 5 ESN for the blocks afterwards.

Mining Centralization

Bitcoin mining is done by repeatedly hashing the sha256 block header until a value lower than the target value is acquired. However, there are two weaknesses in this method.

First, the barrier to participate in mining has become much higher. Currently mining has been completely encroached by ASIC. As the mining ASIC can have thousand times more efficiency compared to the general GPU mining equipment, mining through GPU has become less effective in terms of competitiveness. If mining activities were decentralized in the past, now centralization due to ASIC is intensifying.

Second is the method of mining. It is not that participants from various regions take part in the generation of blocks like the past. Nowadays they participate in mining depending on block headers provided by the mining pool. There are significant side-effects arising from this situation. As of now, three mining pools have been transferred with the computing power of individuals and are indirectly controlling almost 50% of the hashes. Of course, as individuals can move to smaller pools before the share of those pools exceed 50%, those pools cannot arbitrarily abuse resources,. However, this still remains a major issue.

EtherSocial mining works slightly different. Each miner brings random information from the state, hashes details of randomly selected recent blocks and comes up with the result value. There are two advantages in this method.

First is that Ethereum contracts can include calculation methods of all types of computers. Naturally, ASIC would have to be designed to fit for all calculation methods, but then it would become a high performance CPU rather than an ASIC. In reality, ASIC (Application Specific Integrated Circuit) itself will become useless.

Second, miners would have to verify all transfer details by downloading the whole blockchain. In this case, there would be no need for a large and centralized pool. Of course large pools have the effect of equally distributing rewards to participants for generating new blocks, but that effect can also be sufficiently realized through the P2P type pool. There is no need to use a centralized pool.

However, at some point, ASICs designed for Ethereum mining can be released. Therefore at this time, decentralized mining should be enabled by applying a new hash algorithm difficult for the ASIC to use.

Conclusion

EtherSocial provides token management tools that comply with the general-purpose ERC 20 rules based on smart contract, as well as APIs that can easily be combined with various services. EtherSocial also provides administrator management tools that enable applications with 'escrow, setup of withdrawal limit, financial contracts and other advanced functions' to be used in various services through a very general programming language. EtherSocial also provides support to theoretically create all types of transfer methods or applications through the turing-complete language. Through these features, forum hosts or administrators of all services that have accounts can use these services more easily and universally.

References

1. Bitcoin Whitepaper https://bitcoin.org/bitcoin.pdf
2. Ethereum Whitepaper https://github.com/ethereum/wiki/wiki/White-Paper
3. Steem Whitepaper https://steem.io/SteemWhitePaper.pdf