PROTOCON

A Window into the Protocol Economy

PROTOCON

Whitepaper | v.1.0

PROTOCON

Contents

Contents

01 Abstract

One of the hottest topics in the 21st Century is the Digital Transformation of the human society. The term ‘Digital Transformation’ connotes two definitions: one refers to the digitization of every information produced and processed analog, that is, based on paper; and the other refers to the automation of the entire process of producing and processing information based on digital infrastructure. And by automation of production and processing of information, it means that the entire social system is being automated. Before long, with the large-scale automation of the entire social system, an economic system which operates based on protocols, namely a pure digital economy will hit the stride. Digital transformation of not only digital currencies but also traditional assets such as real estate, works of art or musical copyrights have begun based on blockchain technology, and protocol economy was implemented through DeFi. However, automated economic and social system does not necessarily mean there’s only gloomy pessimistic Sci-fi fears ahead of us; if the economic and social system operates in accord with the originally agreed and pledged protocol, those who have monopolized power of decision-making and arbitrarily exercised the authority would be put on the downside. Instead, we believe that under protocol society the power of the individual will become stronger. And the blockchain will guarantee the impossibility of forgery during the individual’s collective consensus and contracting process, and that the agreed terms are implementd as protocols and operate without fail, ultimately strengthening the power of independent individuals. ProtoconNet[1]is a mainnet project aimed at providing trust infrastructure. ISAAC, the core algorithm, was designed to be suitable for large scale data processing for practical industrial application, the versatility of which is secured for use in all fields which require blockchain technology. Also, ProtoconNet greatly enhances blockchain UX through user participatory financial model named Feefi, and distributes added value created by blockchain network throughout the entire ecosystem. Moreover, its decentralized network and governance over the entire ecosystem will promote a protocol-based pure digital economy. But at the same time, we must understand: the future does not come at once. There is no correct methodology for digital transformation of offline data and values. Digital transformation of analog reality is bound to take a fairly long time, and so the early models of pure digital economy will first emerge in game industry and metaverse which was made up of pure digital data in the first place. Taking this into regard, we take game industry and metaverse as the primer of the coming digital economy and the starting point of ProtoconNet 1.0.

02 Introduction

After Bitcoin's appearance in 2008, the blockchain industry had its ups and downs. During more than a dozen years of "verification period', tons of questions were raised against Bitcoin and blockchain technology alongside sharp-looking yet useless criticisms. On the other hand, attempts to break in Bitcoin and decentralized networks through strong regulation and control also existed. Despite the challenges, Bitcoin proved the solidity of blockchain architecture and eventually stepped up to the position of a global asset, standing beside gold. Ethereum, a 2nd generation blockchain, is also evolving from a token issuance platform into a decentralized asset management platform, giving birth to a new industry called DeFi despite having encountered several unfavorable incidents including the DAO Hack and Hard Fork. Following the footsteps of Bitcoin and Ethereum, the 3rd Generation blockchains are steadily hacking their way through to the solution to the problem they defined. Unfortunately, it is too early to say that any of these projects have come up with answers to problems faced by the blockchain industry.

However, a technology which proved its value does not turn back its time and deteriorate. While the blockchain industry hardened its foundation through bubbles and pitfalls, various efforts to extend the application of the technology took place. Thanks to these efforts, blockchain has transgressed the boundaries of generic technology for digital tokens and positioned itself as the essential technology for proving existence of digital data, preventing forgery, ensuring uniqueness, and verifying authenticity. As blockchain technology is indispensable in order to protect digital data with 'value', blockchain will be used as an essential trust infrastructure in digital society.

DeFi (Decentralized Financing) which started off with MakerDAO in 2017 and boomed all of a sudden in 2020 proved that protocol-based automated finance with minimized representative or broker intervention does operate. Implemented through a methodology named 'Smart Contract', DeFi protocol includes pledge or contract, which operates on the blockchain without fail or forgery. While still a bit loose and underdone with repeated trial and error, DeFi is trying to prove that unforgeable protocol-based automated economic system with minimized intervention of representatives or brokers – that is, the Protocol Economy – is operable, and that the establishment of protocol-based social system is not impossible, just as Bitcoin proved that it is able to create unforgeable digital tokens and developed blockchain into an industry.

In fact, significantly automated economic and social system is an intrinsic attribute of digital technology itself, not blockchain. Amid all-encompassing Digital Transformation

of the society, we are witnessing automated digital systems in our daily lives through autonomous vehicles, robots, drones and AI products. Moreover, a large-scale automation is expected to take place throughout the overall social system in the near future. However, it was difficult for existing digital technology to deal with 'valuable data' due to the possibilities of infinite duplication, hacking and forgery. If automated economic system could be duplicated infinitely, hacked or forged, that is, if the automated social system did not operate as agreed by the community, its outcome will surpass the consequence of a simple accident; man-made catastrophe with the consequences similar to natural disasters may occur. As blockchain provides impossibility of forgery of digital data and irreversibility of contract execution which general digital technologies cannot guarantee, it supplements weak points of digital technologies and exerts the potential and possibility of digital economy. If Bitcoin began as a token but ultimately led to the development of blockchain industry, the protocol economy which sprouted from DeFi will expand and extend to restructure the overall politics, society and economy into protocol-based digital system, and blockchain will serve as the trust infrastructure which allows safe operation of automated protocol economy and protocol social system. Now, we are only near the start of the transition.

The entire process of transformation will probably take a great deal of time. Above all, the technological resource for the transformation is insufficient. Currently, the imagination, will and demand for blockchain technology is overfull, but the implemented technologies are not enough to live up to the expectations. In order to establish the protocol economy, where pledges, consensus and contracts between individuals of the community and authorities operate with minimum intervention of brokers or representatives, and protocol-based society in which the system operates as agreed by the community, the following details need to be dealt with.

First, data processing performance should be enhanced to the level that is sufficient or close to sufficient to operate the current economic or social system.

Second, the cost of continued blockchain servicing should be relatively inexpensive and stable. If the cost of blockchain fluctuates sharply, a predictable and sustainable service cannot be provided. After all, high variability of the cost is what hinders the spread of blockchain.

Third, an execution environment which guarantees safe treatment of various digital data and failproof operation of protocol should be provided. Generally, this condition is implemented through the methodology named 'Smart Contract' proposed by Ethereum, but time has repetitively taught us the vulnerability of Ethereum-proposed Smart Contract. Therefore, an enhanced methodology which can supplement the security

vulnerability of Smart Contract.

Fourth, the network should be decentralized, in which its management authority is not vested in a specific person or group. For some time, governments and corporations have carried out various projects with private blockchain. While these attempts are meaningful in some sense, the market already made the conclusion that private blockchains cannot exceed the level of trust provided by decentralized blockchains. In blockchain, decentrality is not a lofty ideal, moral superiority or splendid propaganda of idealists; it is a structural instrument which restricts a specific person or group from dominating or exerting exclusive control over the blockchain network, thereby significantly overcoming the Single-point Failure problem. Therefore, securing decentrality is a task directly related to ‘trust’, the purpose of existence of blockchain.

Lastly, the fifth, UI/UX issue of services with blockchain applied should be addressed. The issue can largely be categorized into two. First, when using blockchain the individuals are forced to learn how to manage security key or private key by themselves and bear the risk of management. For those new to blockchain, it is quite unfamiliar, inconvenient and burdensome. Second, when using dApp service token, the mainnet token must be paid as fee. Metaphorically, this is not different to having to acquire dollar for fee when one wishes to pay using Korean Won. While it may look insignificant, problems caused by fee is one of the biggest factors in making blockchain difficult to use and hindering the expansion of dApp services and the blockchain ecosystem.

The five problems mentioned above have been acknowledged by the blockchain industry as ‘challenges’ since long ago. In ProtoconNet, we will provide comprehensive solutions to these problems. Moreover, technological development and securing usability, or having excellent technology and developing into a successful blockchain project are very distinct objectives. However excellent the technology may be, the technology itself does not guarantee extensive use or adoption by the society. Therefore, an elaborate plan is needed for blockchain to secure usability or be adopted by the society. In particular, with Ethereum cementing its position in the industry following its transition from token issuance platform to asset management platform and other numerous blockchain projects opting to compete with Ethereum, a solution on how a new project can enter the mainnet market was needed.

As a solution to this, we chose game industry and metaverse. Based on the experience and analysis results acquired from the blockchain industry, we seek to provide a blockchain service specialized for (online) games and metaverses. Considering that blockchain technology verifies and protects ‘valuable digital data’, various types of data created from games or metaverse are a great fit. At least in games or metaverse, the

transformation of analog data to digital for storage in blockchain is not needed, and one can only focus on implementation and need not waste time worrying and thinking about regulation. The industry already has a somewhat unstable and immature market in which digital items are traded. Also, when game is combined with blockchain, fraudulent activities in the game industry can be prevented, and the acquired items and game records can be maintained and stored even if the game service is closed or the game developer shuts down so that the items can be used in other games. This will allow protection of assets and rights of users who were originally neglected and violated, thereby activating a new digital economy ecosystem in which a variety of digital items produced in games or metaverses are distributed in the market. There already exist various attempts to combine game and blockchain such as NFT. By proposing a methodology for linking various game data to blockchain, ProtoconNet will aim to enhance the assets and rights of gamers and establish a user-based metaverse ecosystem.

03 Technology

ProtoconNet is a mainnet operated with Mitum blockchain. Mitum is based on ISAAC+ Consensus Protocol, which is a PBFT [2] implementation. Mitum is a code written twice. During our previous project, BOScoin, our team had developed and launched Sebak[3], a PBFT-based blockchain implementation. Based on the experiences of developing and operating Sebak, Mitum was completely rewritten, and was developed from scratch just like Sebak. Our team carefully reviewed the critical mind, strengths and weaknesses of algorithms and source codes of previous PBFT implementations such as Stellar, Tendermint, Hyperledger and EOS, based on which we built a product with processing performance and stability sufficient for application in the industry. In particular, a lot of effort was put into building a network closer to the goal of decentralization based on PBFT algorithm. Also, the concept of 'Model' which corresponds to the Smart Contract of blockchain platforms was adopted. 'Model' is Mitum's unique development methodology through which various data formats and logics can be implemented to accept and fulfill business demands using Mitum blockchain core as framework. While model's purposes and features are similar to the Smart Contract of other blockchain platforms, it is a new methodology which can secure high level of safety and greater freedom in terms of implementation.

Various new technologies and techniques were applied to Mitum. keccak 256, keccak 512 etc. Several features which guarantee blockchain performance and stable network operation were supplemented including: supporting various hash algorithms; feature allowing as-is use of addresses (private key and public key) used by Bitcoin, Ethereum or Stellar; account management feature allowing separation of the account and address with public key so that the account can be managed separately; data structure which can accommodate all types of data; feature allowing grafting of various databases depending on the purpose; adopting AVL Tree to increase blockchain internal data search speed; adopting Acting Suffrage Group concept which is the technological foundation of decentralized network; node voting feature through which nodes can put on vote to adopt models or reflect code or policy changes on blockchain; and, network designer feature which allows network to operate in excelsis without having to stop operation even in cases of changes in network environment and components. In particular, the Acting Suffrage Group concept is an instrument which monitors the soundness of network and separate nodes and automatically expel or add nodes which meet certain conditions from or to the consensus node while guaranteeing finality, which is a distinct characteristic of PBFT. This is a methodology newly adopted by Mitum to implement permission network based on PBFT. Also, network designer feature allowed key operations related to network

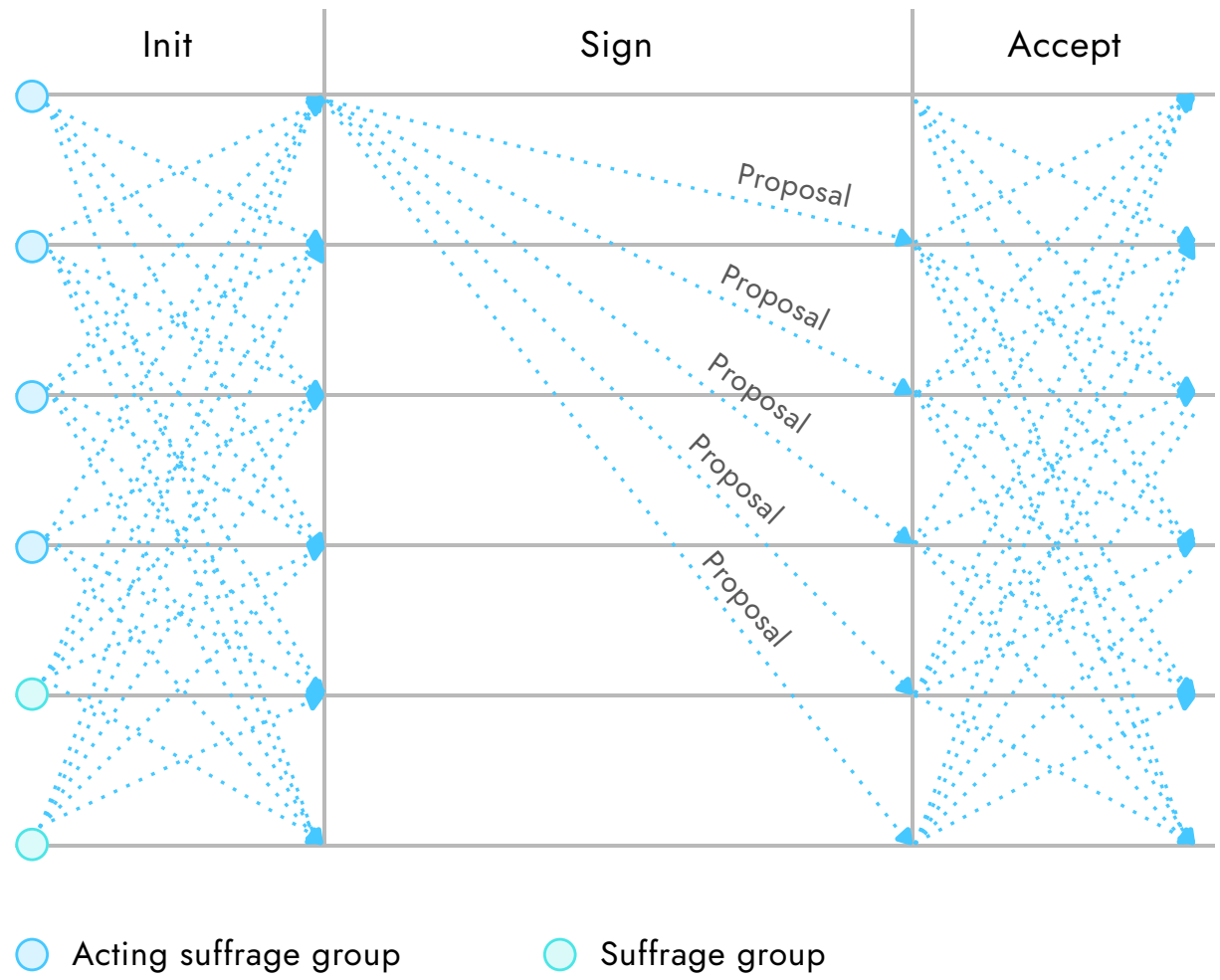
management such as join and expulsion of nodes, changing block generation speed or model update without having to stop network operation to maintain the constancy of the blockchain network. All of the features have been optimized several times and were repeatedly tuned to create the best performance using the minimum number of codes.

A good part of the abovementioned features has already been implemented. The details on new technologies newly introduced by Mitum will be provided in a separate Technical Paper. This Whitepaper will describe core elements of Mitum and their characteristics.

01 Consensus Algorithm

ISAAC+[4] is a consensus protocol which modified and enhanced PBFT (Practical Byzantine Fault Tolerance) algorithm, guaranteeing block finality, and liveness and safety within a limited fault tolerance.

The reason why we chose PBFT-based consensus protocol was that large-scale service with fast processing speed had to be provided for the blockchain to be applied to the industry. Also, as data finalization takes at least a few minutes and up to an hour with PoW, it is not suitable for industrial and business settings which require almost real-time data processing. For blockchain to be used in industrial settings, almost real-time data finality is required, and PBFT is the most suitable algorithm for such. ISAAC+, a consensus protocol which improved PBFT also guarantees data finality and liveliness and safety within a limited fault tolerance (3f+1, f=the number of faulty nodes). Below is a figure of message delivery and consensus process among nodes in the ISAAC+ algorithm.

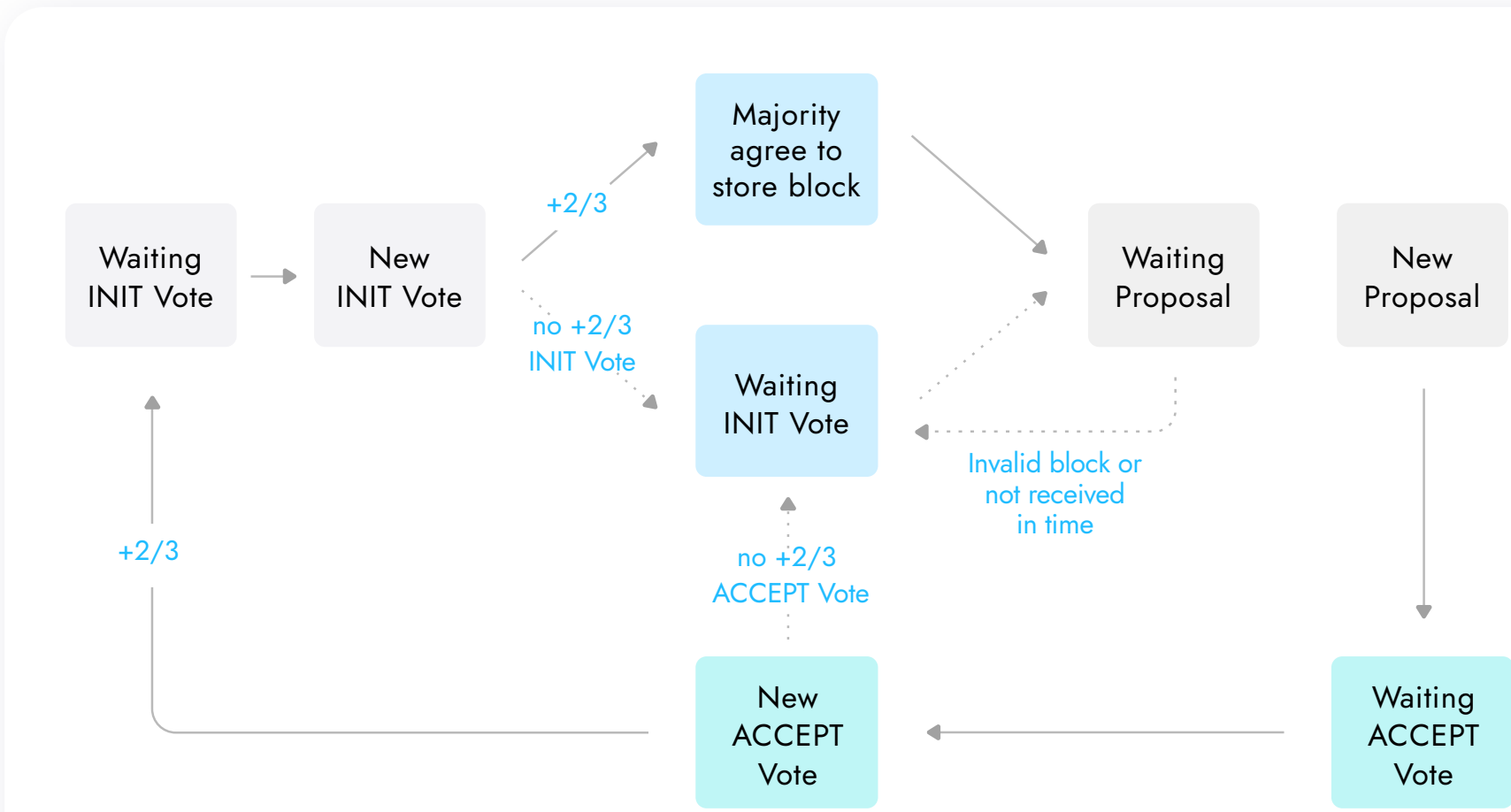


The node groups which participate in the consensus process of ISAAC+ are called suffrage groups. They elect acting suffrage groups composed of random nodes every round. That is, the consensus process of the original PBFT was restructured by randomly electing a certain number of acting suffrage group among the suffrage group at every consensus round, and then electing a leader which proposes a new block among the acting suffrage group. The reason for adopting Acting Suffrage is to check the actions of a certain number of nodes every round and monitor node soundness at all times. The consensus process of ISAAC+ algorithm consists of the three stages of Init -Sign - Accept.

During the Init stage, all nodes participating in the consensus (Suffrage Group) verify agreement on the block generated in the previous round, contain the result in the ballot and send it to the suffrage group. If the result is not above threshold, the Init stage for the next round begins and the voting for the block is carried out again. If the agreement is made, the block generated from the previous round is recorded on the blockchain and a new round begins. At this moment, the suffrage group records the agreed block on the blockchain and moves to Sign stage. At the Sign stage the Proposer who will propose block generation for this round and the acting suffrage group members are elected using random function. Acting suffrage group validates the Proposer’s proposal and sends the result to the entire suffrage group. Regardless of the voting result of acting suffrage group at Sign stage, the suffrage group conducts voting for the Accept stage, and if the

agreement is made a new INIT stage is opened.

The process of Init-Sign-Accept is as follows.



The reason why a certain number of acting suffrage group is elected is to randomly sample nodes in electing the Proposer to rule out faulty nodes. If a certain node shows irregular patterns exceeding the limit, the node is expelled from the suffrage group. So, the process exists to constantly monitor faulty or unsound nodes in the suffrage group which performs consensus and replace nodes below threshold so that the soundness of the entire network is maintained. Through such process, faulty nodes can be screened out from the suffrage group. Only the nodes which meet certain standards set by the protocol are given the chance to participate in consensus building in order to support the stability of the network, and random participating nodes are given the opportunity to be active in the blockchain network so that permissionless network is secured while guaranteeing stability.

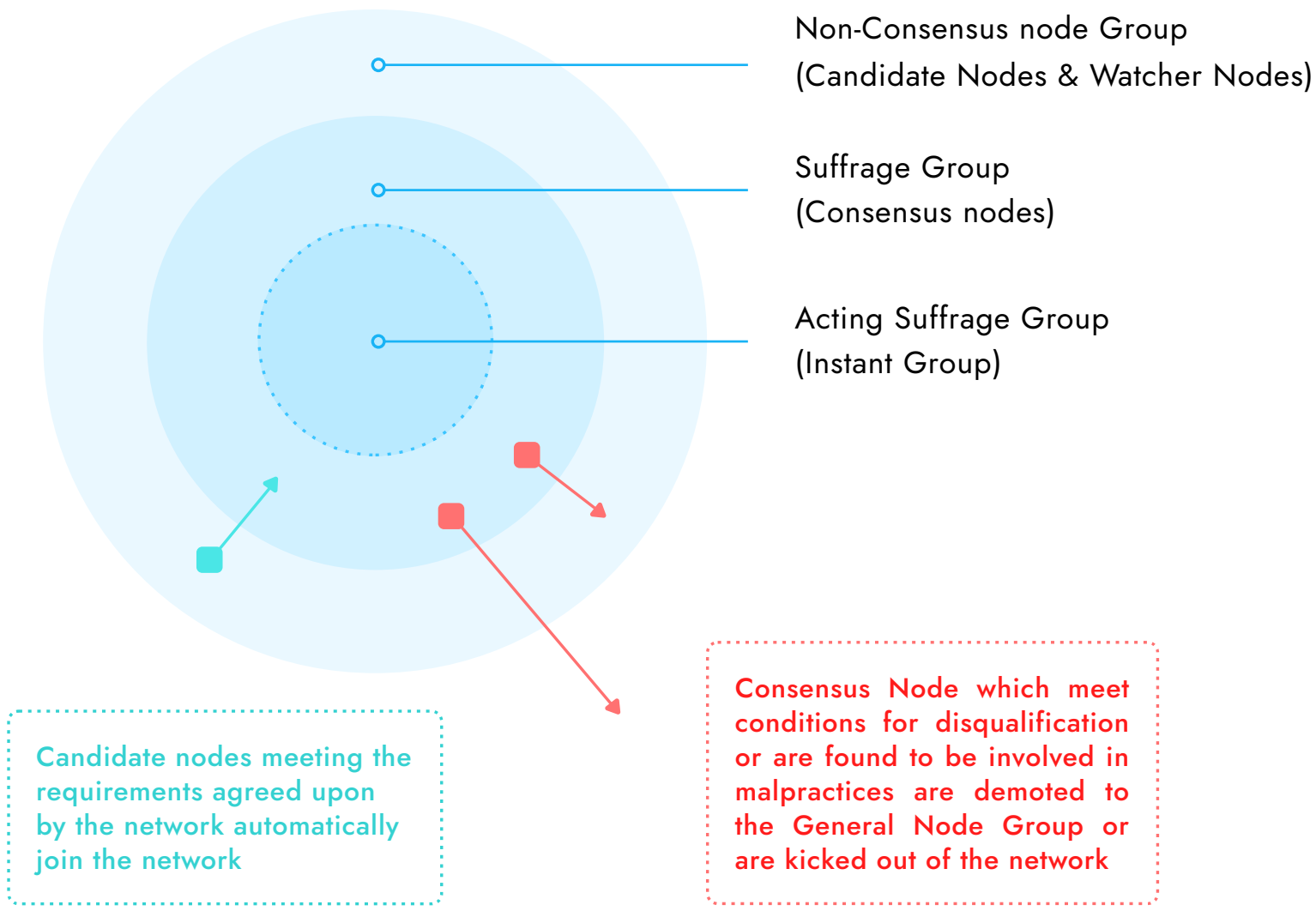
02 Node Operation Structure

There exist three types of nodes in ProtoconNet. First is suffrage group node, and we call them workers as they are in charge of building ‘consensus’, the most crucial element in blockchain. Due to the characteristics of PBFT algorithm, the number of suffrage group nodes is limited. Under PoW there’s no limitation on the number of nodes but the

but the processing performance is limited, while under a well-implemented PBFT algorithm the processing speed can reach up to several thousand fps, but the number of nodes cannot be increased infinitely. As under PBFT the number of nodes and performance are generally inversely proportional, an optimized combination of the two factors is required considering the stability, economics and decentrality. We aim to secure an appropriate number of nodes by carrying out various tests and optimization while gradually expanding the network in BetaNet phase. Also, ProtoconNet aims to provide network performance sufficient for application in industrial settings, and so the processing performance exceeding a certain level and stable network bandwidth must be secured to operate suffrage nodes. That is, certain performance and stability conditions should be met to operate nodes. The information on the requirements for node operation shall be provided separately.

The structure of ProtoconNet is as follows:

ProtoconNet Node Ecosystem Structure



Outside the suffrage group exists multiple non-consensus nodes. These group of nodes back up the agreed blocks and at the same time provide data in case of external data retrieval, and so the suffrage group can focus on consensus and model data processing and the processing performance of the entire blockchain can be enhanced. As we expect that the increase in blockchain use will lead to the explosive increase in requests on not only the consensus but also data retrieval, the role of non-consensus node group will become more important over time. Non-consensus node group is generally open to nodes with lower performance, less strict security environment and less stable network environment than those of suffrage group nodes. Also, nodes wishing to participate in the consensus process may wait as candidate node in non-consensus node group and replace nodes expelled from the suffrage group. The expulsion and joining process of nodes will be carried out through node votes in the earlier stage and will be automated using algorithm in the near future.
However, we cannot reach the ideal state at one go. In order for the project to grow mature, a substantial amount of effort, time and accumulated management expertise will be needed. In this regard, we choose to pursue a strategy which starts off by creating a network close to private blockchain, establishing business ecosystem and progressing into a decentralized network step by step.

03 Node Group Operation Policy

As nodes can freely be accepted to and expelled from ProtoconNet without having to stop the network, up to one-third (⅓) of the entire ‘worker’ node can be replaced any time if they fail to fulfill their duty. Figuratively speaking, the ground rule of Protocon ecosystem’s node operation policy is to select solid and loyal workers among those volunteered, assign them the role of operating and managing the network and provide them with sufficient compensation. For someone to participate as a worker, he/she must sign up on the worker list and serve the role of non-consensus node on standby. Nodes which are qualified for participation in suffrage node group are approved by the network and are designated as candidates, to whom a certain amount of node compensation is provided. The number of candidate nodes may range from ⅓ ~ ½ of suffrage nodes so that these candidate nodes can immediately replace nodes which have stopped operation or withdrawn themselves from the network for a certain reason.

Generally, many PBFT algorithms have adopted PoS or DPoS structures which combined stake structure with PBFT algorithm. Behind this decision is the assumption that those with higher share are generally likely to participate more actively in network operation than others and not engage in actions which hinder the growth of the network in order to maximize their financial gains. Also, PoS or DPoS structure considers economic interest of large shareholders by allocating the probability of block generation in

proportion to the share ratio, hence granting them the chance to gain block generation reward in proportion to the share ratio. However, there exist concerns that under this structure large shareholders may collude to gain control over the entire network, and also criticisms that the economic interest of small number of large shareholders are excessively reflected, posing negative impact on the development of entire ecosystem or long-term project plan. Also, the weak point of these structures is that if a certain node with excessively high share ratio is attacked, the entire network may be influenced. Considering the fundamental aspects of PBFT algorithm, it is favorable in terms of security to distribute probability of block generation as randomly as possible, and so in terms of stability and reliability of the entire network, PoS or DPoS which affects the randomness of block generation by combining consensus algorithm and share ratio is not a great fit. Taking this into regard, we did not choose PoS or DPoS, but adopted PoC (Proof of Capability) structure which selects nodes based on the processing performance of nodes and network safety.

Blockchain algorithm structures such as PoS or DPOS do not only affect block generation or block reward, but also influence ecosystem composition method and reward structure of participation in the ecosystem. Therefore, under PoS or DPOS structure, staking is structured with nodes as the center because the share ratio of nodes is important. In such structure the token holders tend to depend on node operators, thereby strengthening their authority. However, by choosing to adopt PoC in which all nodes share the same amount of authority, responsibility, and reward, we became free from having to select node-centered token staking structure. We could also break free from node operator-centered governance structure and build a governance system where every stakeholder in the ecosystem partakes in. (In relation to this, we propose FeeFi, through which token holders contribute to the enhancement of usability of the entire network and be rewarded, which is explained in further detail in Chapter 4.) Nonetheless, as nodes serve critical roles in the ecosystem taking charge of maintaining and managing the network, they will be provided with sufficient financial compensation.

On these premises, the operation policies of suffrage node group – or workers – which maintain and manage the network are as follows.

1. All nodes participating in the suffrage group shall stake the same amount and be rewarded the same. Also, their probability of block generation shall be near-even.

2. The initial stake of suffrage nodes is five million PEN, but the amount of stake may be adjusted by the governance depending on the changes in the price of PEN token. Nodes on standby for participation in suffrage node group, also known as candidate nodes, shall also stake five million PEN.

3. We aim to establish a structure in which the nodes are compensated for node operation with the fee received from providing the services in the long term. Until the network reaches this stage, the network shall provide subsidy to nodes so that they can cover node operation cost. Node reward shall be procured from a portion of network usage fee and a portion of inflation coin generated during node generation. The network shall provide node reward sufficient enough to operate the node.

4. The network shall select nodes based on the stability and capability of nodes. Node operators shall fulfill the minimum hardware performance and network performance required by the network and prove that the node has sufficient operational capacity. Should a node be repeatedly confirmed to be of low quality or unstable according to certain standards, the corresponding node may be expelled from the suffrage group through node voting or automated algorithm. Here, low quality includes but is not limited to: 1) node's hardware performance is not up to the standard; 2) network performance is not up to the standard or consistently unstable; or 3) node is found to be intentionally negligent of its duties.

5. Should a node be found to have engaged in malicious activities such as double signature, the corresponding node shall be penalized. Penalties include fines deducted from stake or expulsion from the network with the entire stake confiscated and shall be imposed in the strictest manner as a rule. The network shall provide sufficient reward for the contributions, but sternly penalize any malicious action as a warning to other nodes. Further details on the penalty shall be provided in a separate node operation guide.

6. The PEN tokens staked by nodes shall be unlocked approximately four weeks after the stake withdrawal request is placed. This is to prevent a large number of tokens from entering the market at the same time and causing market disturbance.

7. New nodes shall be added to the group when 1) the existing node is expelled from the group (for some reason) and the group has to be reinforced, or 2) new nodes need to be added due to the increase in size of the network, in which cases the node in the best condition among the candidate nodes shall be added to the group. In the early stages a new node shall be added to the group through voting of nodes, and once the node management technology is mature, the network shall automatically select and add an optimal node among the candidate nodes based on its own judgment.

8. Node operators retain the authority to approve various programs and policies such as consensus algorithms and models distributed in ProtoconNet through voting. Nodes shall serve as primary administrators for items related to security, safety and performance which greatly influence the network and the ecosystem. However, every node operator shall submit to the decisions made by the 'Congress'.

The abovementioned operation policies will be verified and supplemented through a sufficient number of tests in testnet and mainnet Phase 1. In particular, node operation subsidy policy is bound to be modified, as node operators will have to almost fully depend on the subsidy in the earlier stages during which the collected fee would be too small, and the amount of subsidy will have to be adjusted as the total value generated through fees increases. These modifications will be drafted and introduced in accordance with node operation reward guidelines and will be finalized upon Congress approval.

04 Model

Bitcoin proposed the concept of blockchain and is considered a pioneer of a new field called 'cryptocurrency', and Ethereum is praised for presenting the concept of 'worldwide decentralized computing infrastructure through blockchain and Smart Contracts' and expanding the scope of application of blockchain. Fueled by the innovativeness of Smart Contracts [5] which began with Ethereum, most mainnets implement smart contracts structured similar to that of Ethereum.

However, a question on whether it is right to allow 'anyone' to generate transaction on blockchain if the fee is paid is raised. In the existing smart contract operation structure, the existence of inappropriate or malicious smart contracts is discovered only after the contract is executed in the blockchain network and the accident or problem takes place, and so the distribution of a bad smart contract jeopardizes not only the creator of that contract but also the entire ecosystem including node operators, Dapp operators and users. While the structure may seem to have high degree of freedom, it is extremely vulnerable in that the network cannot take any measure against unstable or malicious projects from posing negative impact on the entire ecosystem. Taking this problem into regard, we choose to renounce the smart contract's 'freedom to distribute' to enhance blockchain security and protect the entire ecosystem. Instead, we propose a new concept of 'Model' through which minimum quality control centered on node groups is allowed and higher degree of 'freedom to implement' is guaranteed through direct use of blockchain core features in terms of development. The 'Model' we propose can be defined as <a program which handles operations required by various businesses through a framework which leverages the capabilities provided by Blockchain Core>. A 'Model' has the following features.

1. ProtoconNet provides ‘Model’ development framework to allow free-for-all development. Any developer can refer to the model-related document and develop a unique model.

2. Multiple models can be operated simultaneously on a single network.

3. As a minimal instrument to manage security issues which repeatedly took place in the existing Smart Contracts, the adoption, operation, supplementation and update of models is allowed only after the approval of node operators. It was also defined that policies be approved after nodes complete the review if the policies affect the overall stability and value of the blockchain.

4. ‘Features’ and ‘policies’ within the model will be separated to ensure maximum amount of freedom of implementation.

5. Even when applying new models or updating existing models, the network operates without downtime.

Let us cite Mitum Currency Model which provides coin issuance feature as an example. If a project wishes to issue a new coin using Mitum Currency Model, it must set parameter values (coin name, quantity, fee, etc.) and submit the token issuance proposal, and upon approval of nodes the new coin will be issued. During this process, the nodes will review the policies and codes of the new project to see whether the leading agents of the projects are obvious and reliable, whether the submitted codes are okay, or whether the project can contribute to the development and expansion of the ecosystem in the long term, and approve the proposal so that it can be uploaded on the network.

Here, blockchain functions as a special type of database that safeguards data integrity, and the model provides features to define and process different types of data and policies including tokens. Thanks to its expandability, the model can be used to develop all types of services which require blockchain in ProtoconNet such as token transaction, data management or other blockchain-based application services. The development of different models in the future will allow users to use diverse features.

We are currently developing the following Models deemed essential for using Mitum blockchain, among which the development of the Token Model is complete. For the Data Model, we are currently developing a prototype version which can be used in linkage with ‘Blockchain’, a blockchain-based digital document and data management service described below. Furthermore, various models including Fee Model specially designed to solve fee related UX issue (FeeFi) and Voting Model will be developed. The Models below

will be distributed on the blockchain network by consensus of nodes after strict security check. The types of model we aim to implement in the early stage are as follows.

Token Model

In general, Token Model includes features which allow issuance and transmission of tokens on the mainnet. Currently the development of a model corresponding to Ethereum's ERC-20 is complete, and other token models with various characteristics will be developed one by one. All models including token models use fee model to pay for network fees. ProtoconNet uses PEN Token issued by the network as the key currency and governance token of the Protocon ecosystem which operates through the Token Model. dApp service providers may also issue tokens of their own using the Token Model. As described in the figure below, a dApp token can easily be issued by setting several values including the amount issued, fee policy and currency ID and running the operation.

[dApp Token Generation Operation]


```
"operations": [
    {
        "hash": "98Qu7EytGVZMHW7ujDWbwPh1uYGhWS7RKQip7eEUyHvx",
        "fact": {
            "_hint": "a028:0.0.1",
            "hash": "25panwZiZ7KLLdjrRgZ6HW5YT4vW86NaHUSYtJN51utG",
            "token": "MjAyMS0wMy0yNlQxNTo0ODozOC42NTE2MyswOTowMA==",
            "currency": {
                "_hint": "a030:0.0.1",
                "amount": {
                    "_hint": "a022:0.0.1",
                    "amount": "99999999999999999999",
                    "currency": "PEN"
                },
                "genesis_account": "4UM4CN8MZNyv26TK84486CX5X8bu9EUYbsWz5ovRsp1M-a000:0.0.1",
                "policy": {
                    "_hint": "a036:0.0.1",
                    "new_account_min_balance": "10",
                    "feeer": {
                        "_hint": "a032:0.0.1",
                        "type": "fixed",
                        "receiver": "4UM4CN8MZNyv26TK84486CX5X8bu9EUYbsWz5ovRsp1M-a000:0.0.1",
                        "amount": "3"
                    }
                }
            }
        },
        "fact_signs": [
            {
                "_hint": "0150:0.0.1",
                "signer": "skRdC6GGufQ5YLwEipjtdaL2Zsgkxo3YCjp1B6w5V4bD-0113:0.0.1",
                "signature": "AN1rKvtJhUbbZAEtqQ7g7R8R1iyz64Yxq4GTQDrZZE2yDBJZ1Vc6xr1fKtxven7ZZraHr5BW8QvXVw6CD5SwKzM3JavTMszps",
                "signed_at": "2021-03-26T15:48:38.652382+09:00"
            },
            {
                "_hint": "0150:0.0.1",
                "signer": "ktJ4Lb6VcmjrbexhDdJBMnXPXfpGWnNijacdxD2SbvRM-0113:0.0.1",
                "signature": "381yXZL5jLng9CTHKLywBVdFegFNRaW12AE7wzsHpLphF28JZVuA1LzpVETy7ZDeBWFRv7sMP7wiSqvEHZVYwL7TAksgmpKe",
                "signed_at": "2021-03-26T15:48:39.12282+09:00"
            },
            {
                "_hint": "0150:0.0.1",
                "signer": "wfVsNvKaGbzB18hwix9L3CEyk5VM8GaogdRT4fD3Z6Zd-0113:0.0.1",
                "signature": "AN1rKvtX5DJGPjUG6NJwYviozrpfERfF1NemwH1SPWJ3Uqj5zbRM8zwcDLiWr9hYWPRcr6WAaDrpxnUXdZfcH4GTRjorjMkHi",
                "signed_at": "2021-03-26T15:48:39.265779+09:00"
            },
            {
                "_hint": "0150:0.0.1",
                "signer": "vAydAnFCHoYV6VDUhgToWaiVEtn5V4SXEFpSJVcTtRxb-0113:0.0.1",
                "signature": "AN1rKvtgkDFxZibobzNvqaARiVNikbXh56XyjqZZJLMsJmJQ61fBz2Y25jVUQLBXRgueZa7efHHWP4AJNgy4wSHkroSqB2u9X",
                "signed_at": "2021-03-26T15:48:39.279463+09:00"
            }
        ],
        "memo": "",
        "_hint": "a029:0.0.1"
    }
]
```

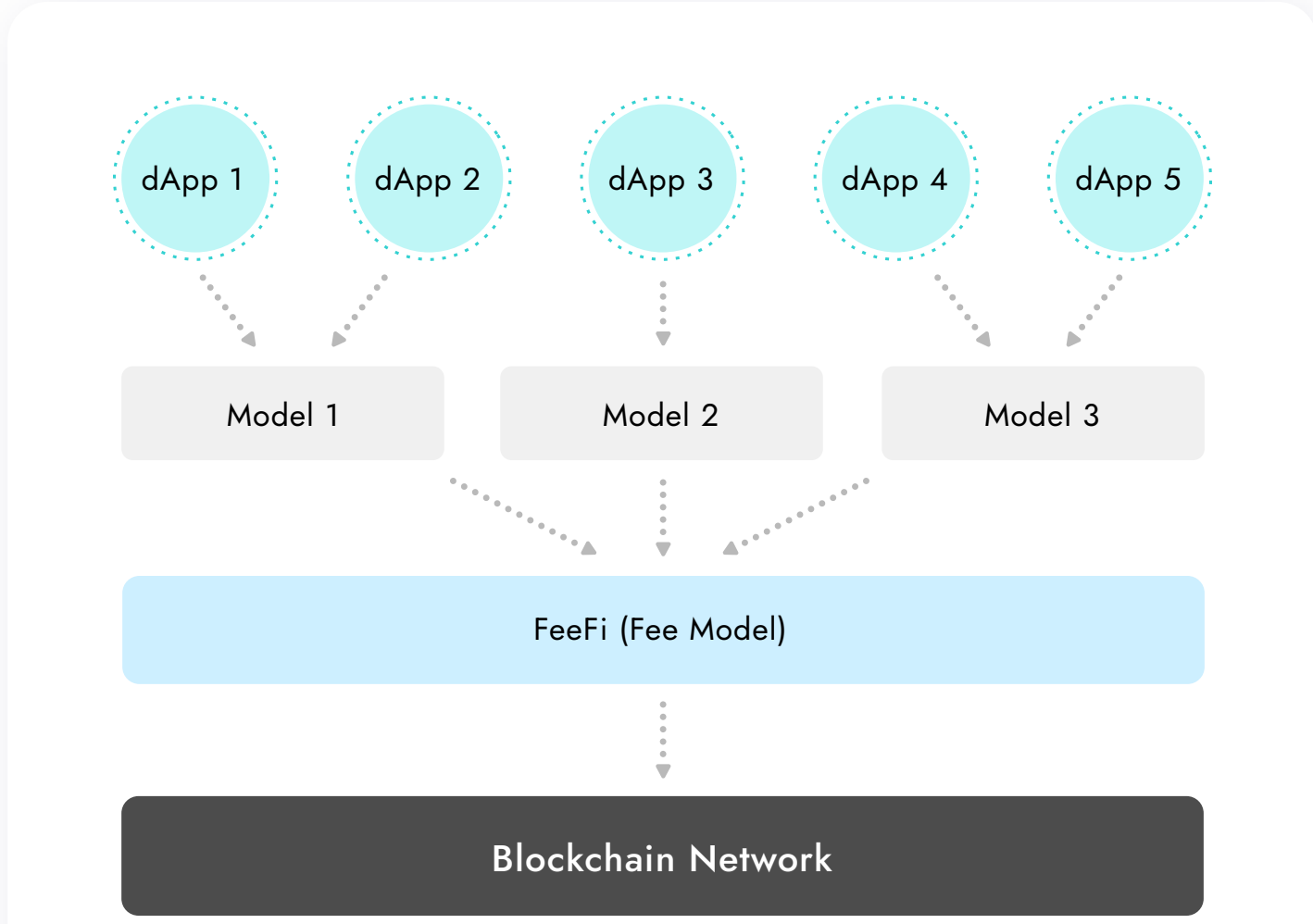

check. The types of model we aim to implement in the early stage are as follows.

Fee Model

We believe the fee related UX issue must be solved in order to enhance the usability of blockchain. For general mainnets, the users will have to purchase mainnet token to use dApp tokens or give up using them. In fact, many potential users give up using blockchain services at this stage. While some blockchains pay a portion of the fee for the users, pre-purchase system resources or provide the service for free for a limited period, we believe these stopgap measures cannot contribute to a fundamental solution, as paying fee for

users or fee-free policy may lead to DDoS attacks, and pre-purchasing system resources may induce infinite competition over the resources, leading to violent fluctuation of network use expenses.

To solve this, we propose to implement a fee market model in which token holders participate to enhance fee usability and share the reward, namely FeeFi (Fee Financing). In ProtoconNet, users can pay fee in two methods: one is paying with PEN, and the other is paying with dApp tokens. That is, ProtoconNet allows users to pay for network fees using dApp tokens, not PEN, the key token of the mainnet. The first method is for paying fees when the user is using ProtoconNet while not holding a separate dApp token, and the second method is when the user is using dApp tokens. This will be explained in further detail in ‘Chapter 4. Token Economy and Fee’ below. The figure below is a diagram of the relationship between general models and the Fee Model.



DID Model

One of the areas that is emerging importantly/significantly in relation to blockchain utilization is the DID area. DID is an infrastructure service that secures individual identity and uniqueness in decentralized networks or global economic activities beyond the boundaries of individual countries, and further manages ownership and disposal of various assets, certification records, and works stored in the blockchain. We will provide more convenient usability by building a DID model that is based on ProtoconNet and compliant with global standards.

Data Model

One of the most important features of blockchain is storing the original form or hash value of digital data in an unforgeable way and guaranteeing the originality, uniqueness and singularity of digital data through verification of original copy, non-repudiation and management of document modification history. Also, as corresponding values can be retrieved and verified outside, document publication history and originality can be openly verified. Like this, the Data Model is a model which implemented various features required to manage digital data or document. This model will directly be used in Blocksign (https://blocksign.ai) service and continuously be upgraded as per the requests of the service and its users.

Digital Asset Model

Recently, attempts to manage digital assets based on blockchain such as NFT are hitting the stride. As the society at large is nearing digital transformation, generation of unique digital assets which correspond to real assets or management of digital assets which were digital from the outset have just begun. NFT is an extremely elementary model for defining digital assets, and the task of discovering ways to manage digital assets using blockchain is before us. We are developing a number of ideas related to this internally, and we will release them to the market one by one when we are ready. We plan to formulate various methodologies for managing different digital assets required in-game through Blockcity.

Voting Model

Voting Model is a model which can be commonly used for general on-line voting and allows open and secret voting on blockchain. We plan to use this model as a voting tool for decision-making on ProtoconNet Governance. The model can also be used as blockchain based voting system by communities, local administrations, government institutions or cooperatives, and as a decision-making tool in the methodology used for developing user decision-making-based games. As ProtoconNet retains sufficient performance, the model will be good for use in not only small community-level votes but also at local-level votes and national-level referenda.

The network will require much more models. As the blockchain industry is still in its waking phase, we cannot possibly be aware of the detailed needs of the industry and businesses. And so, we will continue to actively interact with the industry and the ecosystem to update safe and convenient models to allow as many people as possible to extensively utilize blockchain technology. Also, as we plan to provide a detailed methodology on developing models using blockchain in our Technical Documentation, any developer can develop their own model. However, as ProtoconNet is not structured to update and operate a random source, a self-developed model should pass strict security test and decision-making process of ProtoconNet Governance for it to be run on ProtoconNet.

04 Decentralization Strategy and Governance Structure

In his writing 'The Meaning of Decentralization'[6], Vitalik Buterin examined various aspects of decentralization. Taking his opinions and other discussions and opinions related to decentralization into regard, the concept of decentralization can be defined as 'a state in which a particular individual or minority cannot dominate or control the network'. And, as blockchain network is not fixed and is alive, a decentralized network, in practical and substantial terms, can be redefined as 'a network which is maintained and managed to be in a state which a particular individual or minority cannot dominate or control, and can enhance and scale itself'. Then, how can one establish a network and ecosystem that is decentralized but still continue to maintain and develop?

While ISAAC+ provided the technological instrument for decentralization as previously mentioned, technological elements do not ensure decentralization. In order to establish a decentralized network, a complex composition of technological elements, financial elements and governance structure is needed. Even the PoW algorithm, which is generally considered to be decentralized, has a logical and critical weak point named 51% attack, and there exist projects on which the 51% attack was successfully launched. Bitcoin and Ethereum secured its decentrality by growing slowly but surely to reach the level that avoids attacks as targeting them has become too costly. So, it can be said that for PoW financial safeguard is serving as an element which helps the algorithm maintain decentrality alongside technological safeguard. Therefore, in order for PBFT - in which the entry and exit of nodes is limited - to maintain decentrality, the token economy which deals with financial interests and governance structure which can hold back the dominance of a specific individual, group or force should be considered at the same time alongside technological safeguard. In this regard, it is necessary to define the types, characteristics, authorities, risk factors and managerial factors of blockchain ecosystem participants.

Participants of Blockchain Ecosystem

There exist various types of participants in the blockchain ecosystem such as project leader group with the Foundation as the center, node operators who operate and manage blockchain network, developer community which participates in open-source development, community consisting of token holders, or dApp service partners. And the ecosystem operates based on explicit or tacit cooperation, competition and checks and

balances among these participants who serve different roles. A group of individuals formed with cryptocurrency as the center in a decentralized network is called Crypto Community. Crypto Community is a global economic community which operates voluntarily based on trust of the project's vision and faith in its technology. While Crypto Community participants all serve different roles, authorities and responsibilities, a structure where every participant cooperates with and hold each other in check to contribute to the growth of the entire ecosystem should be established for the ecosystem to operate in a sound manner. To design a blockchain ecosystem which continuously develops in the long term, we need to explore deep into the roles and responsibilities of the participants.

01 Leader Group

Almost every blockchain project has a project leader group. Even for Bitcoin whose first developer is currently not present, there existed a project leader group with Satoshi Nakamoto as the center. Leader group is in charge the initial designing, proposing, raising necessary funds, developing technologies and actively driving the activation of the ecosystem. Also, leader group leads the project with the support of the entire ecosystem including node operators and token holders, and after the project has developed to some degree, supervises technological development and sets overall direction of the project. Without the leader group, the project wouldn't be able to survive or even exist in the first place, and so in the earlier stages of the project their roles and responsibilities are of the essence. As they are crucial for the initiation and existence of the project, they occupy a somewhat special position in the ecosystem, and so currently these project leader groups tend to possess absolute power in most projects. While this tendency is unavoidable in a sense, the monopoly of decision-making rights from excessive dominance of power sometimes causes backfires in the invigoration of the ecosystem due to selfish and dogmatic decisions and one-sided execution of policies. Also, such structure sometimes induces the leaders to commit criminal activities such as privatization or extortion of assets. In short, there exist risks that project leader groups may cause single point failure, one of the biggest problems caused by centralized power. Therefore, while the importance and roles of the leaders in the ecosystem should be recognized, their power should also be controlled and monitored to some extent.

02 Node Operator

A blockchain ecosystem exists based on the aggregate of alive nodes. In most cases, node operators provide their computing resources in compensation for node operation rewards. They also occupy a special position in the ecosystem because they retain the authority to control hardware and software which execute nodes. While this authority is exercisable not on the entire network but only on the node (computer) he/she operates, possible monopolization of node operators may on a certain agenda may wield strong influence over the network and the entire ecosystem, and even take over the control of the entire network. It is not impossible for a single individual to seize control of multiple nodes through anonymity. While blockchain networks have to distribute ownership and control over each node as much as possible to maintain decentralization, preventing monopolization of node operators in pursuit of joint interest is not an easy task. This is why there were cases when the opinions of node operators were strongly or unilaterally reflected over the opinions of all other participants in the ecosystem when there was conflict of interest between the common interest of the entire ecosystem and the interest of node operators, such as the failed attempt to reduce Bitcoin transaction fee due to the objection of Bitcoin node operators and Filecoin miner strike leading to the stoppage of the network. Therefore, structure-wise technological and political instruments to control the monopolization of node operators is required.

03 Community

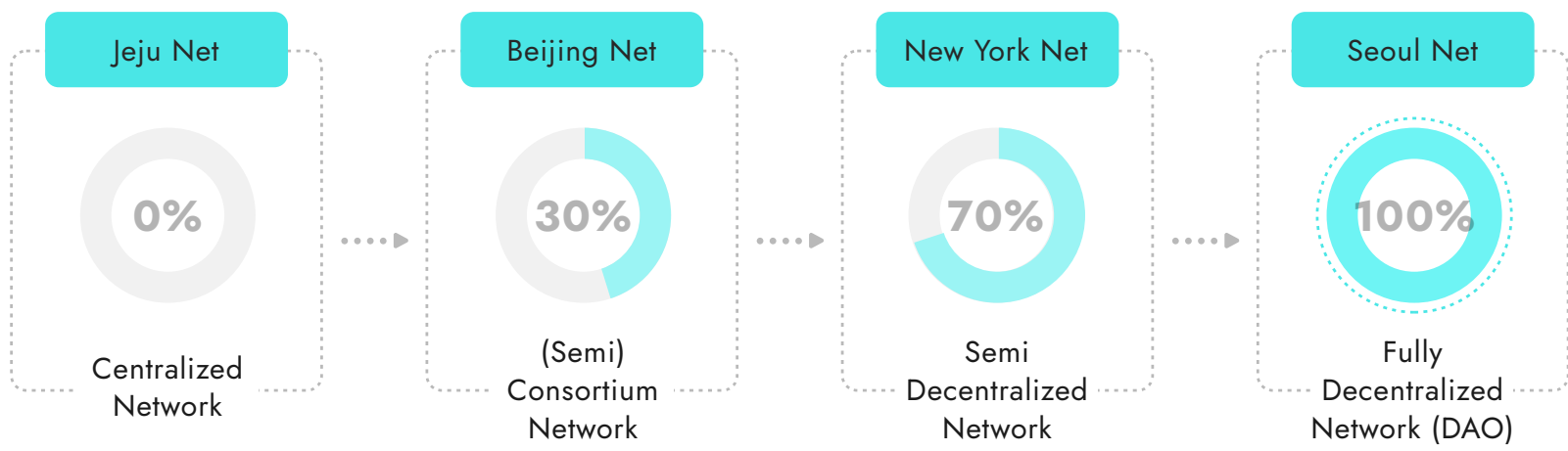
Token holder group, or token community, is also one of the important stakeholders alongside project leader group and node operator group. They possess tokens and act as voluntary supporters, invigorating and advertising the project. There also exist other types of participants such as open-source developer community or dApp service partners who are jointly referred to as ‘token holders’ in general or ‘community’ in broader terms. In the early blockchain projects, token holders were simply passive subjects who only purchased tokens looking for economic profit. While most in numbers, they were often neglected from the decision-making for the actual project. However, recent projects have been attracting token holders’ active participation by giving them rights to participate in governance and leading them to stake tokens to control token flow in the market. More and more efforts have also been made to attract token holders to participate more actively in governance by granting them direct decision-making rights. This is because higher diversity and bigger number of participants in the ecosystem and their active participation leads to higher value of the entire ecosystem.

All participants share a common interest of sharing financial benefit created from the growth of the network and the ecosystem. And the total amount of benefit tends to

increase rapidly as the project grows and develops. If the participants of the ecosystem understand and believe in the long-term vision of the project and cooperate for the project's growth, it can see rapid growth. However, if they only focus on their short-term benefit, the project's growth will be delayed or even stopped in some cases. Therefore, establishing the governance structure in which the participants can cooperate for the common benefit while maintaining decentralization is of paramount importance. Also, as under this type of governance it is difficult to force participation and the level of participation rapidly fluctuates depending on the rise and fall of the project, various supplementary instruments such as incentives to continuously encourage participation in activities to sustain and develop the governance are also needed. We aim to design the decentralized governance structure in full consideration of these experiments, efforts and trials and errors of the cryptocurrency ecosystem.

Stages of Decentralization

Decentralization strategy and governance structure are closely connected with node decentralization. In the early stages of the product, we plan to launch our mainnet in a form close to a private network, at which point a small number of partners will be participating in node operation. That is, the Foundation will operate most nodes and hold control over the governance. We have already started operating alphanet internally, and is planning to link Blocksign service and Blockcity game service at BetaNet phase to develop and test related fefatures. Once the establishment of the token economy including FeeFi is complete, Jeju Net, our mainnet 1.0 will be officially launched. During Jeju Net phase, the Foundation will be obliged to serve a leading role in decision-making, and the project will ultimately develop into a DAO (Decentralized Autonomous Organization) through several steps of gradual decentralization of the governance. For this, we plan to execute a four-phase strategy as follows.



Phase 1: Jeju Net

In Phase 1, ProtoconNet begins with the Foundation mainly in charge of nodes. Also, early-stage partners will be participating in suffrage node operation. We have already secured more than two early partners who will be participating in the operation of suffrage nodes. As the network gradually expands and the number of partner nodes increases by gradually making business partners participate to a level in which the number of nodes operated by non-Foundation operators exceed ⅓+1 of total node, the project will move on to Phase 2. In theory, the Foundation will no longer be able to unilaterally control the network once the number of partner nodes reach ⅓+1 of the total node. Important tasks during Phase 1 include network stabilization, development of essential model features and accumulation of experience in operating nodes and the entire network. When Phase 1 network is launched, Blocksign and Blockcity will be linked and serviced as the first application services. Furthermore, services under preparation in cooperation with several early partners will also be linked once preparation is complete. Depending on the readiness of partners, some services may be accessible from BetaNet phase.

In Phase 1, we will be developing standard models of application technologies required for Digital Transformation of the society at large and the implementation of protocol economy. In particular, Blocksign and Blockcity which are currently being developed will serves as the Living Lab where the cases of blockchain's application on actual services are established. In this regard, Blocksign and Blockcity will not only serve as a laboratory for verifying the excellence of ProtoconNet but also as a technological showroom. A lot of experiments will be carried out in Phase 1. For instance, network operation cost and other incidental expenses will be calculated and whether the values created from node operation cost and fees are reasonable enough to guarantee long-term business feasibility will be verified in order to find optimal fee structure. Through such process, we will establish a detailed model regarding network operation and economic system. Technically, new nodes can join the network in phase by being accepted through voting of those currently participating as nodes, but as the network will be operated as a private network for a certain amount of time, ProtoconNet Foundation, the initial project proposer, will lead the decision-making as an earnest supervisor in Phase 1 in reflection of opinions within the ecosystem. Therefore, in Phase 1, the Foundation will supervise overall project and business development, sort out and select dApp services for Protocon and expand the ecosystem.

Phase 2: Beijing Net

he goal of Phase 2 is to increase the number of those participating in node operation, reducing the number of nodes operated by the Foundation and increasing the number of external node operators to ⅔+1 of the entire node, expanding the network to a level just below decentralization. Once the number of nodes managed by participants from outside reaches ⅔+1, the foundation cannot exercise any control over the network. At this phase, the results of the experiments carried out in Phase 1 are reflected on the network to toughen the ecosystem and the community, and the initial model of a substantially decentralized governance structure starts off. As substantially decentralized node network operates, the node reward structure will start its operation in earnest, and the participation of multiple non-consensus nodes which are not a member of the suffrage group in network operation will further stabilize the network and provide a basic framework toward decentralization. The governance will also be decentralized accordingly. During this phase, a feature which allows new nodes meeting the standards to automatically join the network will be tested.

In Phase 2, we plan to activate a insufficiently elaborate yet somewhat institutionalized governance, through which the Protocon Governance will be equipped with two decision-making bodies. One is Node Committee, an exclusive decision-making organization of the suffrage node group, and the other is the Congress, where token holders exercise their decision-making rights using the Vote Model. However, the ‘final’ decision-making right for the ProtoconNet belongs to the Congress, the decision-making organization of token holders.

1. In Phase 2, the Foundation shall yield its decision-making rights for the ecosystem to the Congress, a governance organization of token holders. Therefore, ProtoconNet’s final decisions shall be made through voting of token holders. However, in order to facilitate efficient decision-making, decisions on some agenda, in particular the agenda not directly related to the entire ecosystem or economic interests of most token holders but are related to node operation shall be made in the Node Committee. Also, for the execution of routine and continued duties, the Foundation and the development team shall submit yearly proposal to the Congress and execute business activities specified within the proposal upon approval of the Congress.

2. Node Committee, in which suffrage node group participates as members, shall have the right to vote for ordinary issues related to node operation and enhancement such as network updates (e.g., bug fix or improvement of features) or model updates. The committee shall also have the rights to approve the entry of

new nodes or expulsion of faulty nodes until automatic node update feature is adopted. Considering PBFT rules, Node Committee's voting rule shall be two-thirds supermajority. However, should conflict of opinions occur regarding agenda related to common interest of the entire ecosystem, the suffrage node group shall follow the decision of the Congress.

3. The Congress refers to the gathering of token holders, and shall hold final decision-making rights over ProtoconNet. Here, token holders are defined as the aggregate of people who staked tokens in the system. There exist two types of staking: one is the fund staked by nodes as collateral, and the other is the fund staked by token holders in FeeFi. Token holders shall exercise one vote per token based on the total amount of tokens staked to the two funds, and suffrage node operators shall also obtain the right to vote in proportion to the number of tokens staked as collateral. However, one-token one-vote system was often abused to steamroll the interest of heavy token holders. Therefore, the Congress shall have two decision-making rules. For agenda which do not provoke acute conflict of interest, the agenda shall be ruled in favor if the total votes for reaches the majority of total votes calculated based on total stake. Should the agenda provoke acute conflict of interest or be sensitive, the agenda shall be ruled in favor if the total votes for reaches 80% supermajority of total stake. Here, agenda which provoke acute conflict include: 1) Expulsion of a certain node from the Congress due to actions against the entire ecosystem, 2) Opposition of the majority of token holders to the decision made by the Node Committee, and 3) Any other agenda which were petitioned to the Congress to be dealt as acute conflict of interest by token holders whose aggregate stake is one-fifth or larger. A more detailed operation plan on this shall be drafted during the operation of Phase 1 network and shall be put to the first vote of the Congress.

4. Should the Congress make decisions against the decision made by the Node Committee, the Committee shall follow the decision, and if not, the Congress holds the right to take the vote to expel nodes which oppose the decision. Should the vote pass, the node shall be automatically expelled from the network effective immediately. The reason for such strong authority is because in other projects, the opinions of node operators have usually been ruled in favor in case of conflicts of interest between node operators and the entire token holders. To prevent this, the Foundation chooses to establish a strong control system so that the interest and decision-making of the Node Committee ultimately coincides with the interest of all token holders and the ecosystem.

5. Node Committee and Congress voters shall be offered a certain amount of voting reward which is paid out from Commons Budget. This is to prevent decline in participation which often observed when operating a governance system similar to that of Protocon, and also because it is logically appropriate to reward those participating in the growth of the entire ecosystem. A detailed reward policy shall also be finalized during Phase 1.mittee ultimately coincides with the interest of all token holders and the ecosystem.

The idea of 80% supermajority originates from Tezos' [7] governance. One-token one-vote structure's disadvantage is that those with larger number of tokens exercise bigger decision-making rights, and therefore it is possible for a small number of people to use voting as a means of plutocracy to represent their interest. One of the alternatives would be one-person one-vote system, but from our experience the participation and operation process of this system is extremely complex and costly. However, as 80% supermajority is based on overwhelming expression of favor of the entire ecosystem, the result of the voting will represent almost the same result as voting carried out under one-person one-vote system. In other words, by combining a simple instrument of 80% supermajority to the one-token one-vote system, we can produce the result similar to one-person one-vote pure democracy.

The principles suggested above are rough guidelines for the Congress, and a more elaborate designing will be needed to operate the decision-making body smoothly and to the point. For instance, an instrument to prevent imprudent petition to the Congress is required, as some may abuse petition out of malicious or mischievous intent. An example of such would be confiscating vote reward for abusive petitions or imposing petition deposit to verify the petitioner's veracity. These are only examples, and we aim to implement a more elaborate and on-point Congress model in Phase 2 using the operation experiences obtained during Phase 2.

Phase 3: New York Net

Phase 3 marks the network's entry into the early stages of decentralized network. In this phase, the Foundation operates only a small number of nodes just enough to take on a symbolic meaning, and will have most nodes be operated by external participants. As can be seen in <Figure x : Protocon Node Ecosystem Structure>, there exists a group of multiple non-consensus nodes in the outermost area of the structure, in which nodes meeting sufficient conditions to be accepted as consensus nodes form the suffrage group to process data. If for a specific reason a node in the suffrage group repetitively causes problems or intentionally disrupt normal operation of the network, the node will be automatically expelled from the suffrage group using a predefined algorithm and become a general node. If the case is severe, all pledged assets may be confiscated, and the node may be permanently expelled from the network. Also, non-consensus nodes wishing to participate as consensus nodes are put on standby and are given the chance to be become consensus nodes when the existing consensus node is expelled.

Phase 4: Seoul Net

In Phase 4, a DAO with completely decentralized node operation and governance structure will be established. In this phase, the Foundation's intervention will be minimized, and decentralized global community will operate the network. In Phase 4, an exquisite governance ruleset will be established based on prior experiments and experiences, and a more elaborate and systematic governance structure will operate.

The expected dates, main decision-makers and major plans of the ecosystem of each phase is schematized as follows. The expected dates in the following table are subject to changes depending on the development progress and business conditions.

Phase	Expected Date	Main Decision-maker	Node Operator	Node Entry and Expulsion Method	Application Services and Major Events	FeeFi
Alphanet	In operation	Foundation	Foundation	Node voting	Blocksign Test Version	X
BetaNet	Q4, 2021	Foundation	Foundation+ partners	Node voting (Decision made by the Foundation)	Linkage and pilot operation of Blocksign, Blockcity and other dApp services	X
Jeju Net	1st Half, 2022	Foundation	Foundation+ partners			
Beijing Net	1st Half, 2023	Congress	Foundation+ partners + random participants	Node voting (Decision made by nodes)	PEN coin issuance and operation of various dApp services	FeeFi adopted
New York Net	1st Half, 2024	Congress	Foundation+ partners + random participants	Protocol-based automation (Pilot operation)		
Seoul Net	1st Half, 2025	Congress (DAO)	Foundation+ partners + random participants	Protocol-based automation		

05 Token Economy and Fee

For last 10 years, cryptocurrency has experienced intense changes since the beginning of Bitcoin Network. Although some still insist that public blockchain industry is unsubstantial, it is them who do not understand the actual state of cryptocurrency industry. Converted into the fiat money, the total sum of Bitcoin fees has exceeded $1B as of 2020. As of March 2021, monthly sum of Ethereum fees is equivalent to approximately $698M, and it means the annual sum is over $9B. Blockchain industry is gradually becoming a mature business.

Blockchain Economy System

The economy system in the blockchain mainnet works largely around two pivots. One is the token price formed in the market, and another is the fee the network charges as the return for provided services. Most of the blockchain projects are mixing up those two while securing resources for the economic survival of the project. However, those two aspects have distinct characteristics while they are closely related. First, we will look at the characteristics of token price. Most of the projects cover the project costs and induce participation in their ecosystems by issuing new coins when a block is generated and distributing them to the network participants. If the token price is high, additionally issued tokens themselves become sufficient economic reward to cover the costs of maintaining the network. Market price of the token is determined by the combination of diverse aspects, including the leader of the project, fame of the team, technological capacity of the team known to the market, actual traffic of the network, feasibility and beauty of technological vision, marketing capacity, size of the community supporting the project, and sometimes, almost scam-like decoration and exaggeration. Second, the fees which the blockchain network receives for providing services are relatively more practical and clearer because they are based on the number of operations using the blockchain network (ops) or the number of transactions (tps). In other words, the fees are measured depending on the actual usability of the blockchain. Once a blockchain reaches a significant data throughput, the token price of the project sharply increases.

As for most of the coins except few, their future values, which are the values their technologies are expected to create in the future, have more influence rather than the actual usable value, because their uses have not been acknowledged by the market. Although many projects have strived and spent great amounts of funds to make an actual usable value, obvious success has been extremely rare. However, Ethereum has proved its value of existence as recent growth of DeFi services rapidly raised traffics in the Ethereum

network, and Terra[8], which is a Korean project, has rapidly grown from the top 40 to top 10 based on sharp increase in blockchain throughput. Those phenomena are quite inspiring in that they indicate that blockchain projects have started to be assessed based on the actual usability rather than their future values.

[Status quo of sum value of fee of each mainnet projects as of March 18, 2021]

Project	24H Revenue	7D Revenue	30D Revenue	1 Year Revenue (Estimated)
Ethereum	$26,835,163	$184,533,658	$698,045,626	$8,376,547,512
Bitcoin	$6,206,822	$50,124,904	$196,436,318	$2,357,235,816
Terra	$19,214	$182,472	$776,554	$9,318,648
Filecoin	$5,396	$45,722	$152,722	$1,832,664
Polkadot	$4,247	$35,449	$125,899	$1,510,788
Tezos	$412	$3,648	$13,316	$159,792

Source : https://www.tokenterminal.com/

Table above is an estimation of daily, weekly, monthly (30 days), and annual sum of fees each mainnet network has made as of March 18, 2021, converted to the fiat money. According to the table, Ethereum is making fess worth approximately $698M (annually, over $1B) monthly, and Bitcoin is making approximately $2.3B annually. Terra, which have grown fast recently, is generating fee value worth approximately $9.3M annually. Sum value of fees all the blockchain mainnets make is almost $15B. From this, we can see that blockchain industry has now become one of the meaningful Internet businesses creating a substantial level of usable values. In other words, public blockchain industry has advanced beyond mere abstract discussion or slogan like unstable future value or decentralized value and grown into a significant business. This means that operation of the network sustain itself with the values created by the network fees alone once meaningful number of transactions are secured, and this can serve as a dynamic to

invigorate the token economy. For example, if we assume the fee of the network to be $0.03 and average number of transactions processed per second to be 1,000 transactions, the annual fee value of the network is almost $1B. Because data processing speed of ProtoconNet is 5,000ops at most under the ideal condition and the network is capable of handling from 1,000 to 2,000 transactions per second in average, ProtoconNet can sustain its network and blockchain ecosystem with the network fees as long as there are enough paying transactions.

However, the fee issue is not limited to business aspects only. It is the key topic widely related to service accessibility and mass adoption of blockchain, as well as business.

Fee Issues

Three most significant reasons that impair usability of blockchain and hindering so-called mass adoption are as follows: 1) Difficulty in private key management; 2) inconvenience of purchasing the mainnet token to use a dApp token; and 3) high volatility of the fee itself. As for the issue regarding the private management, occurrence of incidents such as losing the private key has significantly reduced thanks to recent advance in wallet technology and biometric technologies such as fingerprint or facial recognition and spread of smartphones. Nevertheless, the fundamental problem that losing the key is losing every authority and asset still remains. In regard to that problem, we decided to wait for another excellent project to suggest the solution. The very problem we are focusing on in regard to the usability of blockchain is the fee. Fee issue in the blockchain industry is never a simple problem. It is not just an problem about economic cost but the one directly related to users' usability or user experience. To summarize pending issues of the blockchain business regarding the fee, they are as follows.

1. Issue regarding the appropriateness of the blockchain fee
2. Issue regarding the volatility of the blockchain fee
3. Issue regarding the difficulty in paying the blockchain fee (fee UX issue)

The first one is about how much would be appropriate as the price for using the blockchain. As DeFi grew recently, Ethereum fee had increased to USD 200. It was higher even than Bitcoin transfer fee. Because most mainnets, including Ethereum, are designed to use limited resources through competitive bidding, their fees increase as the demands on the blockchain increases.

This causes the second problem. For example, if a businessperson has been using the blockchain expecting the fee to be $0.1 at most but the fee suddenly increases to dozens of dollars, the person can no longer use the blockchain. If the service highly depends on the blockchain, it directly leads to termination of the service. This is the actual problem that many Ethereum-based dApp services are experiencing. Plus, if skyrocketing of the fee in the midst of the service is expected, designing stable and persistent service become impossible. In other words, the attempt for a universal service utilizing the blockchain becomes unavailable.

If only few people use the blockchain for a special purpose or the blockchain covers highly valuable assets only, cost of using the blockchain being expensive or rapidly increasing would not have been a problem. Actually, people are paying expensive financial cost (fee) for asset transactions though Bitcoin or Ethereum network. However, the expensive fee and intense volatility are great hindrance to the mass adoption of the blockchain. The expensive fee becomes a great obstacle in the growth of the blockchain industry, considering that this is the epoch of omnidirectional digital transformation.

If the appropriateness and volatility of the blockchain fee are economic issues, the third one, difficulty in payment is about the service usability, in other words, UI and UX. A mainnet token is an essential aspect because it is the internal payment system of the mainnet. However, the dominant fee structure force the users of dApp services or dApp tokens to pay fees in the mainnet token. Someone familiar with the token economy will be able to purchase the mainnet token from the exchange and pay the fee easily, but a first-timer will hardly acquire the mainnet token. Such a structure becomes a great barrier to dApp service providers who wish to deliver popular services through the blockchain. This problem is a common thing among most of mainnets because the mainnet projects have either copied the fee structure of Ethereum or made few modification or improvement while maintaining the fundamental premise.

The key point of the UI and UX issue related to the fee structure is that the users are forced to acquire the mainnet token in order to use dApp services and tokens. To take Ethereum for example, there are three ways to acquire Ethereum: 1) Mining; 2) receiving from other user; and 3) purchasing from the exchange. However, these three ways are all difficult for most of the potential users, except ones familiar with the blockchain and cryptocurrencies. How can we expect the services based on Ethereum to be invigorated when acquiring Ethereum itself is too difficult? For further notice, growth of DeFi cannot be an excuse in this case because it is a service where users familiar with the cryptocurrencies participate solely with the cryptocurrencies.

In regard to this issue, projects like EOS have conducted a few experiments. EOS established its logic to make the users pre-purchase the resources by auction. In other words, the team has built a structure where the users do not have to pay fees personally by allocating a certain volume of the system to those who purchased the resources by staking the EOS Token. This certainly is an improvement in that the users can use the blockchain service without purchasing the mainnet token. However, because each service provider has to compete over limited system resources, the cost of using the network rapidly increase if the competition become too heated. Moreover, even if I have already secured the necessity amount of resources first, they may reduce if another service provider stakes even more EOS Token. In other words, if other service providers take over the resources by staking more tokens, the service provider has to stake additional EOS Token to secure the same amount of resource. Hence, burden of the service providers rapidly increases.

One of the fundamental cause of this problem is that most of mainnets have adopted ‘competitive resource model.’ In particular, EOS tried to improve the blockchain usability by suggesting a method that does not force the users to pay the fee, but it created a structure where the service provider must compete over resources infinitely. In such a case, only service providers who can afford the fee which may skyrocket any time can use the blockchain network, and there are few such service providers. Hence, the utilization purpose of the mainnet become very limited.

As a way to bypass such a barrier, there have been attempts to provide the blockchain service for free or pay the fee by proxy. However, those were possible only as a temporary marketing policy or promotion policy in the early stage of the service, and constantly paying the fee by proxy or providing the service for free is impossible. Because a blockchain network requires a great amount of cost for its operation, assuming that the network can be sustained without a proper rewarding structure is irrational. Also, providing the service for free or fully depending on payment by proxy bears the risk of being exposed to DDoS attacks.

We believe that mass adoption of the blockchain will become possible only when the dApp users can easily use the mainnet, in terms of both cost and UX. Hence, this is not a matter of choice but a problem that must be solved for the sake of the mass adoption of the blockchain. Fortunately, we could adopt the strategy that allows more users to use the blockchain services while paying the appropriate fee, thanks to the excellent performance of ISAAC+. Because we can build a considerable volume of token economy with the blockchain fee alone as we have discussed hereinbefore, we hereby suggest a new concept, FeeFi (Fee Financing), which is a kind of fee market that builds a token economy that works based on the added value generated by the blockchain network, the fee.

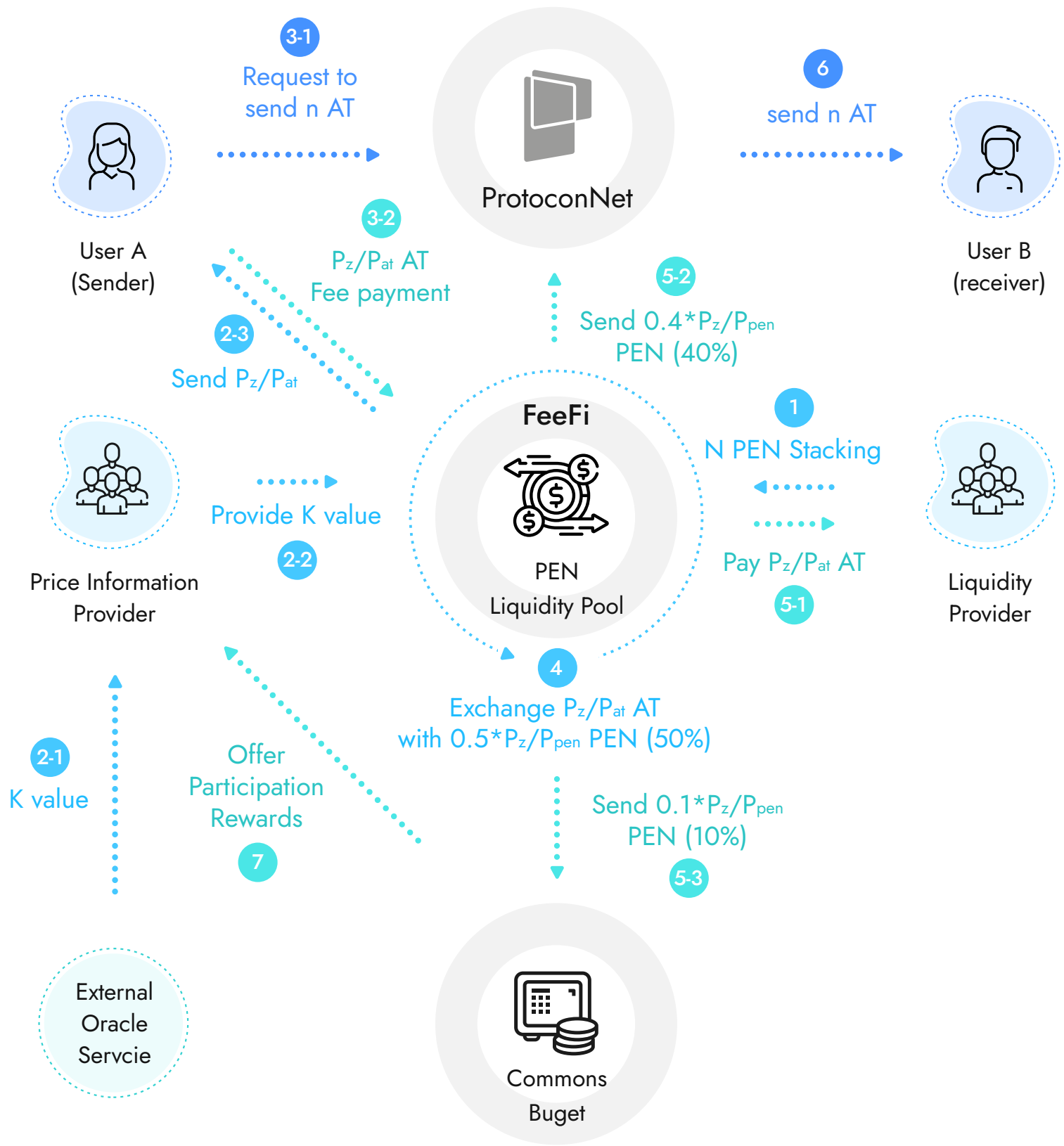
FeeFi (Fee Financing)

Fee Financing, or FeeFi, is a new methodology that solves diverse problems about the fee by applying the DeFi financial method to the fee. In the ProtoconNet, FeeFi serves two roles. One is distributing the added value generated by the network while the users participate in solving the issues regarding the fee. Another one is making the users participate in the market regulation by staking the tokens. However, tokens issued in inflation will be provided as the incentive to induce the user participation because the value acquired through the fee would be slight in the early stage of the project. We are aiming to provide the potential solution for the three issues regarding the fee, appropriateness, volatility, and usability in payment (UX), which have been suggested by the blockchain industry.

Solution 1 : FeeFi

Acquiring the mainnet tokens and paying them as the fee to use a dApp service or transfer dApp tokens is one of the worst UX that hinders the mass adoption of the blockchain. The key is allowing the dApp token holders to pat the fee in dApp tokens.

Let’s take an example. First, assume there is AT, the token of a dApp service named A. Some users holding AT, which is a kind of dApp token that works in the ProtoconNet, must hold PEN Tokens and know how to pay the fees in PEN Tokens, but the majority will have AT only, not having any PEN Token. If the service provides the proper usability, AT user must be allowed to pay the fee for using the blockchain in AT alone. To solve this problem, we suggest FeeFi (Fee Financing), which is a kind of internal DEX to exchange dApp tokens paid as the fee with PEN Token in which the token holders participate. Structure of FeeFi is as follows.



Market Price	Exchange Rate	FeeFi Fee	Fee Correction Value
1 PEN = P_{pen} (USD) 1 AT = P_{at} (USD)	PEN:AT = P_{pen}:P_{at} AT = P_{at}/P_{pen} PEN	Constant price P_z (USD) (P_z/P_{at} AT or P_z/P_{pen} PEN)	K = $f(c,t)$

First of all, we defined the fee distribution ratio, market price of the token, and the transfer fee as follows.

Node Operator 40%, Liquidity Provider 50%, Commons Budget 10%

P_z (USD) := x USD (x is the fee) (1.1)

P_{pen} (USD) := 1PEN (1.2)

P_{at} (USD) := 1 AT (1.3)

$Fee_{at} = P_z/P_{at}$ (AT) (1.4)

$Fee_{pen} = P_z/P_{pen}$ (PEN) (1.5)

(P_{pen} :Price of 1 PEN in USD,Pat : Price of 1 AT in USD, Pz:Price of the fee in USD)

The figure above indicates the operation flow of FeeFi architecture by step. First of all, the liquidity providers stake N PEN in the FeeFi. If any transaction occurs because of an AT user, the liquidity providers can receive a part of the fee paid by the AT user as the reward. Then, the actual value of the fee the AT user shall pay may differ greatly depending on the fluctuation of the market prices of AT and PEN Token. In the FeeFi architecture, an external oracle, K, has been adopted to solve such a fee volatility problem. We will cover K in a separate section below, and the relevant descriptions will be omitted as of now.

AT users shall pay AT equivalent to Pz/Pat to FeeFi, regardless of the transaction volume. Later, the fee paid in AT by the user is exchanged with PEN Token at FeeFi. The exchanged two tokens shall be in the equal value.

Fee_{at}(AT) = Fee_{pen}(PEN)=P_z(USD) (1.6)

However, Fee_{at} is exchanged with 0.5*Fee_{pen}(PEN) at FeeFi. Originally, Fee_{at}(AT) shall be exchanged with Fee_{pen}(PEN), which has the same value, but we can enjoy the effect of providing the half of the paid fee, 0.5*Fee_{pen}(PEN), to the liquidity providers staking PEN Tokens by exchanging it with PEN Tokens equivalent to 50% of the paid fee. Out of the exchanged 50%p of Fee_{pen}, 10%p is saved as the commons budget and 40%p is provided to the node operators. Lastly, Fee_{at}(AT) exchanged with 0.5*Fee_{pen}(PEN) is distributed to the liquidity providers who provided the PEN Tokens to FeeFi, according to the staking share. Therefore, the liquidity providers can provide 0.5*Fee_{pen}(PEN) and receive Fee_{at}(AT), which is a double, consequently purchasing AT with 50% discount. We will call this process and the result the ‘fee farming’ or FeeFi (Fee Financing).

In addition, dApp tokens are divided into ones with the public market price and ones without a market price yet. The fee market works as above if the token has the market price, but one of the following two ways is applied if the token does not have a market price. A way is creating an account exclusively for the fee and paying the fee by proxy from the account whenever a transaction occurs. However, the users will be

recommended to pay the fee in the dApp token even in a small amount, in order to prevent DDoS attacks. As for another way, even when a stable coin is not listed yet and does not have a public market price, a fee market for the coin can be formed as long as the coin has or is expected to have a constant price and the participants of the market acknowledge the price. In other words, a fee market can be formed autonomously by the users even when there is no market price at the moment.

Because Ethereum has proved the blockchain fee market worth approximately $8.3B (approximately 10 trillion KRW), the fee market can operate as an independent financial system if we can secure sufficient transaction volume. In that context, we have named this FeeFi (Fee Financing). Such a structure has several strengths in regard to the ecosystem. dApp service providers participating in the ProtoconNet can easily secure the initial users by distributing the token to the PEN Token holder pool. That is, dApp services share the PEN Token liquidity provider pool and become able to secure the initial participants of their ecosystems naturally. We may also promote participation in the dApp ecosystem by offering an unique incentive model for dApp services in addition to the fee the users receive. PEN Token liquidity providers can acquire dApp tokens while participating in the work to provide a better blockchain UI and UX and directly contributing to the growth of the ProtoconNet. If dApp tokens operating on the ProtoconNet largely grow, the PEN Token liquidity providers may share the outcome together. Like this, as an economic symbiotic relationship between PEN Token holders and dApp service providers where they share the outcome of the project's growth is established, PEN Token holders become the supporters of not only PEN Token but also every project related to the ProtoconNet.

In addition, we can clearly identify the contributors to the ecosystem through the 'PEN Token staking' process and grant them the right to participate in the governance votes. Moreover, when FeeFi is well established, we will further develop more diverse financial models based on the staked PEN Tokens and additionally generated fee rewards. We will authorize those contributors to participate in the initial funding for PEN-based dApp projects. Through this, we will show that the protocol economy functions from the inside of our mainnet. The minimal staking amount for FeeFi participants shall be 10,000 PEN initially, but the specific guideline will be determined by the governance considering the time when FeeFi starts to operate and the PEN Token price at that moment.

Solution 2 : Controlling the Fee Volatility

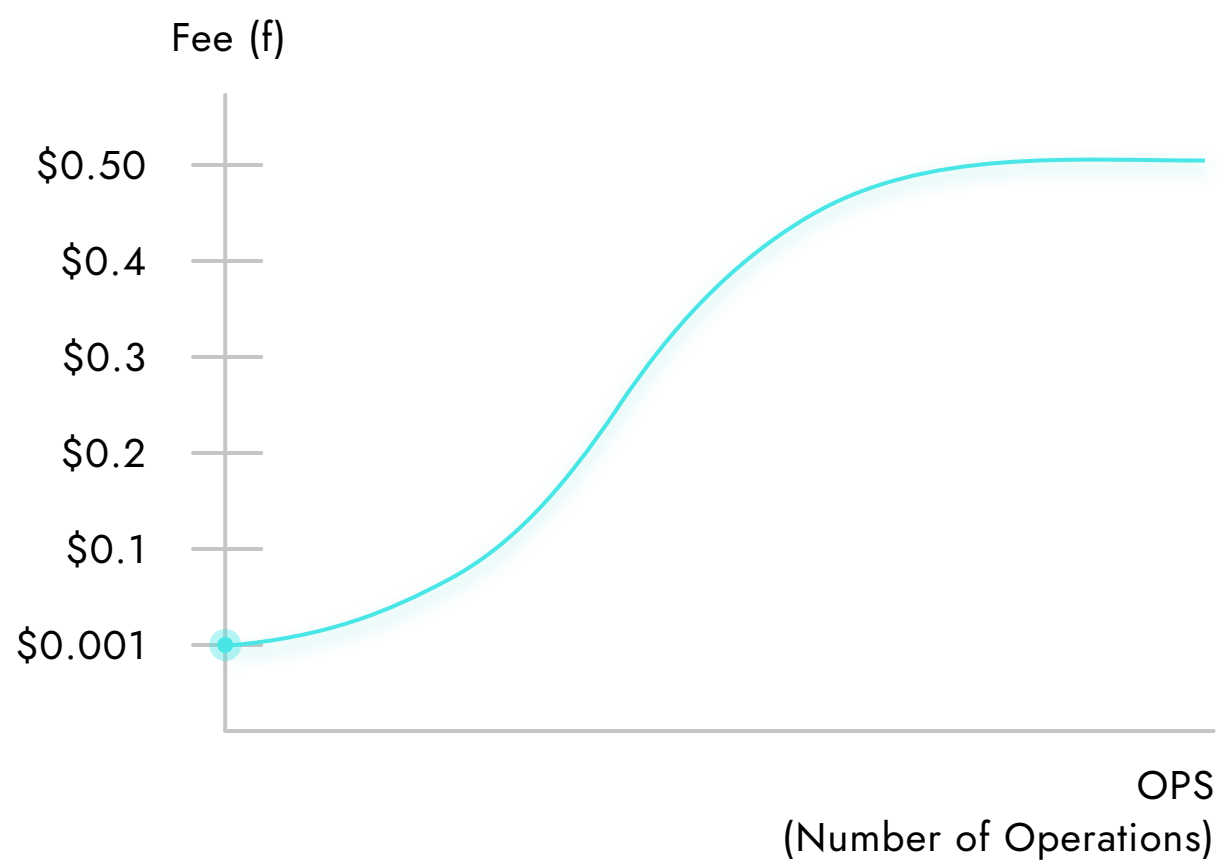
To summarize another issue, the fee for using the blockchain network shall be reasonable and not too volatile. However, this is not a simple problem too. Above all, there has been no sufficient consideration upon the fee-oriented network operation in the public blockchain industry. Hence, we lack the evidence on how much is the appropriate and reasonable price to use the blockchain service. However, we can make an estimation based on the following three aspects to consider: First, the total expenditure or cost to operate a blockchain network that functions with the fee alone, without any incentive such as additional coin issuance; second, in terms of mass adoption of the blockchain, the range of the maximum price that is appropriate or psychologically acceptable for the users when they store a piece of data onto the blockchain; and third, the fee as the minimal barrier necessary to prevent DDoS attacks to the blockchain network.

Considering those aspects, we have assumed the minimum value and the maximum value of the price of a processing fee per unit operation or transaction (Pz) to be $0.001 and $0.5, respectively. If the user wants to process the multiple numbers (N) of operations or transactions to process a piece of data, a higher cost (Pz * N) will be needed. While $0.001 is a rather strategic price considering the entrance to the market at the time of the initial booting of the network, $0.5 is the estimated maximum price that the popular Internet service can pay or accept to protect valuable data. If the processing cost of an individual operation exceeds a certain price, only expensive financial transactions will be processed, as in the case of Bitcoin or Ethereum. That is, too expensive fee restrains the extension of the blockchain's usability. However, it is not necessarily good that the fee is low, because a too low fee gives room for DDOS attacks.

Although ProtoconNet also process expensive financial operations in a cheap and reasonable price, we believe that the fee shall not exceed a certain level to allow the application of the blockchain technology to our daily lives and overall industries, including securing the uniqueness of data, verification of the original document, provision of nonrepudiation feature, and registration and verification of certified copy of registration. In the point of view of the blockchain as a 'service,' structure competitively increasing the fee in proportion to the increased network traffic will seriously harm the sustainability of the service. Because of such reasons, we will implement the management mechanism to begin with $0.001 and gradually increase the fee up to the reasonable level as the network traffic increases. Of course, $0.001 and $0.5, the current minimum price and maximum price, are just our assumption, and we do not yet have enough information to estimate the appropriate level of the fee and the upper limit of fees that blockchain users can tolerate. Because the assumption of $0.001 at least and $0.5 at most is also an estimation based on the experience so far and the current fees of

other blockchains, it will be adjusted by checking the cost and the marginal utility through the actual network operation during the Phase 1 of the mainnet.

In addition, high volatility of the fee is an aspect that harms the quality of the blockchain as a ‘service.’ If the minimum and maximum fees are set at $0.001 and $0.5, respectively, and the fee intensely fluctuates from $0.001 to $0.5, it is extremely difficult for ordinary Internet service providers to provide services because they cannot predict the cost of using the blockchain. In this respect, we are introducing a fiat-money-based 'base price fee'. As blockchain usability is enhanced, the base price will gradually increase as shown in the graph below.



The base price of the fee is determined by the foundation in the initial stage, and the Congress determines the base price since the Beijing Net Phase. Because the token price continuously changes in the market, we shall prepare special tools to fix the fee at the base price.

Decision making for the policy regarding the fee will take place as follows. At a certain time of each quarter, the Congress of the ProtoconNet determines the appropriate price or the base price of the fee in dollar (P_{z0}). Because market prices of the PEN Token and a dApp token (hereinafter AT) are volatile, the amount of AT a dApp token user shall pay constantly changes depending on the time of payment (t). In here, we shall make exchanging values of Fee_{at}(AT) provided as the fee and Fee_{pen}(PEN) exchanged with the fee to as close as possible to the base price set by the Congress. For this we should know the market prices of PEN Token and AT at the time of payment and the exchange ratio of PEN Token to AT. Hence, we can calculate the fee closer to the base price if we can make the time we get the market price closer to the real time and better reflect the average market price.

First of all, it is defined as follows for the future explanation.

P_{z0}:= **Base Price.** (2.1)

$P_{z,\,t}$**(USD) :=fee in USD at time t,** $0 \le t$**.** (2.2)

(t=0 is the time when the market created)

Let's assume that an AT user is transferring n AT at a certain time, t. Then, the exact market prices of PEN Token and AT shall be Pexact pen, t(USD) and Pexact at, t(USD), respectively. If we know the exact prices of PEN Token and AT, Feeat, t(AT) and Fee pen, t(PEN) shall be exchanged as follows.

$Fee_{at,\,t}(AT) = P_{z0} / P_{exact\ at,\,t}(AT) = P_{z0}(USD)$ (2.3)

$Fee_{pen,\,t}(PEN) = P_{z0} / P_{exact\ pen,\,t}(PEN) = P_{z0}(USD)$ (2.4)

$1(AT) = P_{exact\ at,\,t} / P_{exact\ pen,\,t}(PEN)$ (2.5)

However, if the acquirable market price is not updated in real-time, the actual prices of PEN Token and AT in which the user purchases the tokens will differ from Pexact pen, t(USD) and Pexact at, t(USD). Another chance is that the externally derived market prices themselves are inaccurate. To distinguish the differing price from the exact market price, the derived prices will be written as follows.

$P_{der\ x,\,t}$ **:=Externally derived** $P_{x,\,t}$ **at time t,** $0 \le t$ (2.6)

$P_{der\ y,\,t}$ **:=Externally derived** $P_{y,\,t}$ **at time t,** $0 \le t$ (2.7)

$Fee_{at,\,t} = P_{z0} / P_{der\ at,\,t}(AT) = P_{z,\,t}(USD) \approx P_{z0}(USD)$ (2.8)

$Fee_{pen,\,t} = P_{z0} / P_{der\ pen,\,t}(PEN) = P_{z,\,t}(USD) \approx P_{z0}(USD)$ (2.9)

Like the above, it is not easy to calculate the fee with similar value to the base price in the actual situations. Hence, we are trying to reduce the disparity from the base price occurring during the exchange between AT and PEN Token by introducing a compensating value K. (K_t =K at time t, $0 \leq t$)

c_t :=Externally derived state at time t, $0 \leq t$ (2.10)

K_t := f(c_t,t) at time t, $0 \leq t$ s.t f is a correction function. (2.11)

$1\ (AT) = K_t * P_{der\ at,\ t} / P_{der\ pen,\ t}(PEN)$ (2.12)

Combining this with the description mentioned hereinbefore while explaining about the architecture of FeeFi, the fee converted into PEN at the time t is as follows.

$$Fee_{pen,\ t} = (P_{z0}/P_{der\ at,\ t})*(K_t*P_{der\ at,\ t}/P_{der\ pen,\ t})(PEN) \quad (2.13)$$

Consequentially, we can calculate more accurate fee because we can compensate the exchanging rate between $P_{der\ at,\ t}$ and $P_{der\ pen,\ t}$ with K_t.

Although it is the best if $P_{z,\ t}$ are close to the fixed base price P_{z0}, they do not have to be as same as P_{z0} at every t, and it would be acceptable if the average price during a certain t interval either approaches or is close to P_{z0}. If we properly implement oracle data Kt (=f($c_{t,\ t}$), which is a compensation value for the exchange rate, we can adjust the fee exchange rate so that exchanging value of AT and PEN Token at time t become the same.

We can use two mechanisms for the oracle data. The first is importing the external market prices through oracle data services like Chainlink and Band Protocol, and the second is operating internal decentralized oracle production system that makes the fee to approach a certain price, like FTSO used in the Flare Network. However, because there are many variables in utilization of oracle data and we cannot fully depend on a single method, we are reviewing the decentralized oracle production system through the first method to import credible external oracle data (data acquisition) and the second method, internal oracle production system (compensation), to generate even more elaborate data. By doing so, we will be able to build even more stable and complex fee system.

ISAAC+ is a high-performance algorithm which can stably process 5,000ops at most under the ideal condition. As ISAAC+ has achieved the best stability and speed compared to other existing blockchains, it is expected that the added value generated by the ProtoconNet in the form of the fee will be immense once the ProtoconNet become saturated. We have designed our token economy to provide every participant of the ProtoconNet ecosystem with benefits generated by the operation of the network, and will implement FeeFi, a methodology reflecting that intention, so that the entire ecosystem share the added value generated by the blockchain network. Plus, before the network become saturated, processing thousands of instances of data every second, we will find sufficient alternatives to accommodate even more traffics.

Fee Distribution and Incentive Policy

We regard the fee as the fundamental economic resource that operates the blockchain network and designed the token economy of the ProtoconNet around the blockchain fee. However, we will support the node operation by providing the incentives in the initial stage because some time is needed until the network sufficiently grows, and the incentive will be provided in the tokens issued additionally for each block. (Additionally issued tokens and incentive policies by year are currently under the review, and they will be added to the finalized version of the Whitepaper.)

Based on the fee income and additionally issued incentive tokens, the fees and incentives in the initial ProtoconNet can be allocated to: A) the node operation reward; B) the FeeFi reward; and C) commons budget reserve. (A+B+C=100%) (A) The node operation reward is the fund provided to the node operators for operating the nodes. (B) The FeeFi reward refers to the return for FeeFi stakers who contribute to improving the usability of the overall blockchain network. (C) The commons budget reserve is a kind of reserve saved for the funds spent for the advance of the entire ecosystem. We do not know which ratio would be the fair reward for the contributions. Plus, the fair ratio will change as the token price changes. For such reasons, the distribution ratio among A, B, and C will be set to the proper figures by the foundation depending on the actual operation of the nodes after several tests and experiments during the BetaNet phase, and the congress will determine it thereafter.

Commons Budget

Commons budget is a fund saved on the blockchain for the sake of the development of the entire ecosystem. Commons budget will be allocated to initial funds by the initial token allocation policy, and commons budget will be built by continuously accumulating a certain percentage of fees (e.g., 10%) after the mainnet FeeFi operation. The commons budget can be utilized for diverse purposes regarding the development of the entire ecosystem, including voting reward, support on marketing activities, support to the ecosystem partners, and support on R&D. The common budget shall be spent by the vote at the congress, and the detailed plan will be announced separately.

06 Market Entrance Strategy

Applying the blockchain to the actual social systems is not very fast. Governments and companies around the globe have been working on projects to utilize the blockchain since 2016 [9], but there are not many clear achievements. There are four main reasons for this: First, lack of technology; second, lack of experience; third, incomplete digital transformation; and fourth, various regulations and social management skills formed in the analog society. Combination of these four reasons are hindering the full-fledged digital transformation. These obstacles will continue to exist for a considerable time.

In relation to this issue, we are confident that we have solved some of the technical part of the problem. However, applying the blockchain technology to the actual industry is bound to undergo a number of trials and errors. To largely evaluate the experience the blockchain industry has gained, it seems that people have only learned a lesson that it is useless to apply blockchain to some things and the blockchain should not be applied to them. They approached it as if everything was going to be done, but now they are only at the stage of distinguishing between what they should not do and what they cannot do. Methodologies on 'how' to apply the blockchain to a particular industry or business have not yet been much developed. It is no wonder considering that it has not been long since the blockchain-based cryptocurrency or digital assets formally entered the social system, and digitization of assets, represented by NFT, is underway in a very rudimentary form. Therefore, most of the works we have to do in the future are things that no one has ever done yet, so we have no choice but to try by ourselves to accumulate experiences and find answers.

The unfinished digital transformation and regulation and social management techniques from the analogue epoch also created a great barrier. To apply the blockchain technology properly, the target data shall be in a digital format but most of the physical data are in the analogue form. Hence, the problems of determining to which the blockchain shall be applied first and how the digital transformation shall be done must be solved first. Applying the blockchain shall come after that, but most of project teams double their difficulty by hastily trying both application of the blockchain and digital transformation simultaneously. In that process, ignorance of what is the right way to utilize the blockchain technology. Moreover, issues regarding diverse regulations on the real data also become a great barrier in proceeding with the project. Because so many things are prohibited, a project team is forced to spend substantial resources and time to consider how they shall avoid the regulations and how much regulatory risk an action would cause even before making any attempt, instead of focusing on their actual tasks.

From Game to Reality

For those reasons, we believe that the market entrance strategy which can wisely solve various barriers we face at the moment and further accelerate the realization of the blockchain technology is needed, and the most appropriate and efficient way for that is to apply the technology to the games and metaverse. This is because we do not have to agonize about the regulations or have difficulty in determining how the data shall be digitized at least in a game or metaverse. When it comes to the online game or metaverse, we can postpone the third and fourth issues mentioned above and focus solely on the third and fourth issues. Furthermore, we can use most of the verified technologies that are implemented and work in the game as they are. We aim to increase the utilization rate of the blockchain network by applying the blockchain technology to the game and enhance the fee revenue until FeeFi can actually work. Then, we will expand the technology built there to economic and social systems. That is why the market entrance strategy of the ProtoconNet can be summarized into ‘From Game to Reality.’

Combining a game with the blockchain is not a new attempt. As for the attempts in the market, diverse attempts, including guarantee of item ownership and facilitation of trades, verification of digital estate ownership, and proof of transaction history using NFT, are underway. There are several projects, including Engine Coin, Decentral Land, and Flow, are already working on combining a game with the blockchain for years. Once gaming data is accumulated on the blockchain, a new industry of trading game items or digital assets will appear naturally. The gaming industry is still suffering from typical problems every digital technology faces, including item theft, misappropriation of the item, and item hacking and copying. This is why we expect the blockchain would lead a new industry of management and transaction of digital assets. Metaverse, which has arisen recently cannot work without mentioning the blockchain.

If someone asks what is the closest precedent model to identify the specifics of a fully digitized economy, it must be the gaming industry. In this respect, the online game industry is a space where we need to go beyond simple means and strategically focus on to actively experiment and discover new models. However, we believe such attempts around the Ethereum network can hardly promote significant industries because of slow speed and expensive fees. In this respect, we believe that it is necessary and possible to strategically support all the functions needed for the game at the mainnet level. So we will execute the growth strategy of the network around the game as follows.

Roadmap

Phase 1 : Building Model House (Blockcity)
Phase 2 : Implementing Game Data Platform
Phase 3 : From Game to Reality

In the Phase 1, we will develop diverse methodologies to apply the blockchain to game data, through Blockcity. We will implement the Blockcity game using Minecraft by ourselves and develop diverse modules for the guarantee of the item ownership, proof of the digital estate ownership, verification of transaction history, verification of game experience points, issuance and distribution of digital badges, and management of digital copyrights and apply them to the Blockcity. In addition, exclusive plugins or mods for the blockchain will be developed to allow the entire Minecraft ecosystem to enjoy the features implemented in the Blockcity. Once the usability of the game features created through the Blockcity will be verified and the data model is fixed, they will be provided to the market as modularization features so that the entire gaming industry can utilize them. In the Phase 2, we will build a kind of game data platform using the blockchain as the medium to provide the blockchain features specialized in gaming so that diverse games can freely use the necessary feature. In the Phase 3, we will work on applying diverse features built in the game to the real world. For example, digital badge or digital copy right management feature can be utilized to operate the digital badge system or build digital copyright management system in the real world. Although all of those phases will be processed in the order, some works can be done at the same time. For example, if the verification during the Phase 1 was enough, we may proceed with Phase 2 and Phase 3 simultaneously.

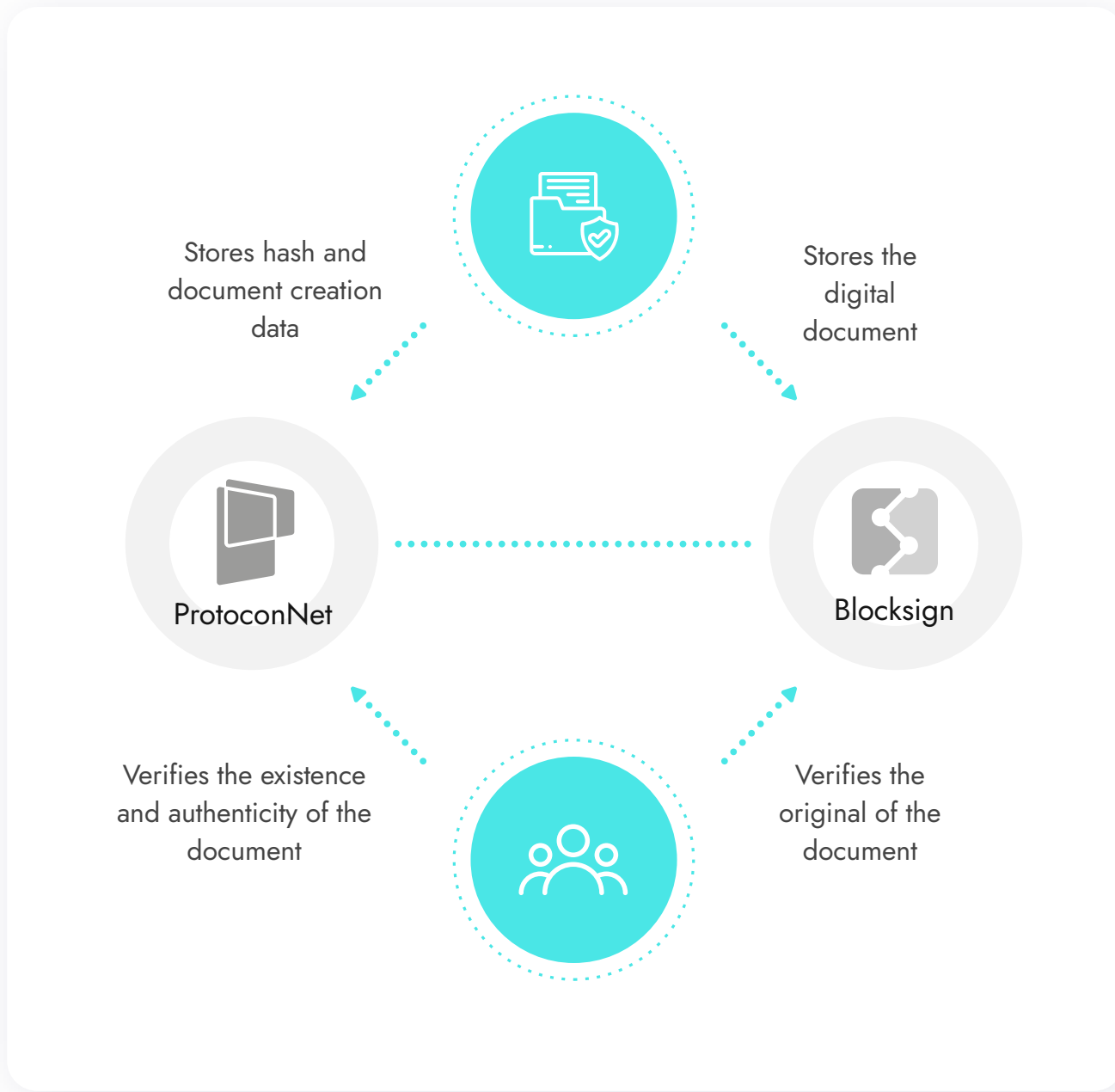
07 Application Service

We had numerous thoughts on how to apply the blockchain technology to the industry. We confirmed that utilizing the blockchain technology would not be easy because the blockchain still is a difficult technology to handle and we are in the midst of solving the problems suggested by the industry. The reason why most of the utilization cases of the blockchain are focused only on tokens, which is the simplest application, is this. Plus, because the blockchain is still in its early stage, it is not easy for a project team to refer to the existing results if the developer of the original technology does not build sufficient application cases.

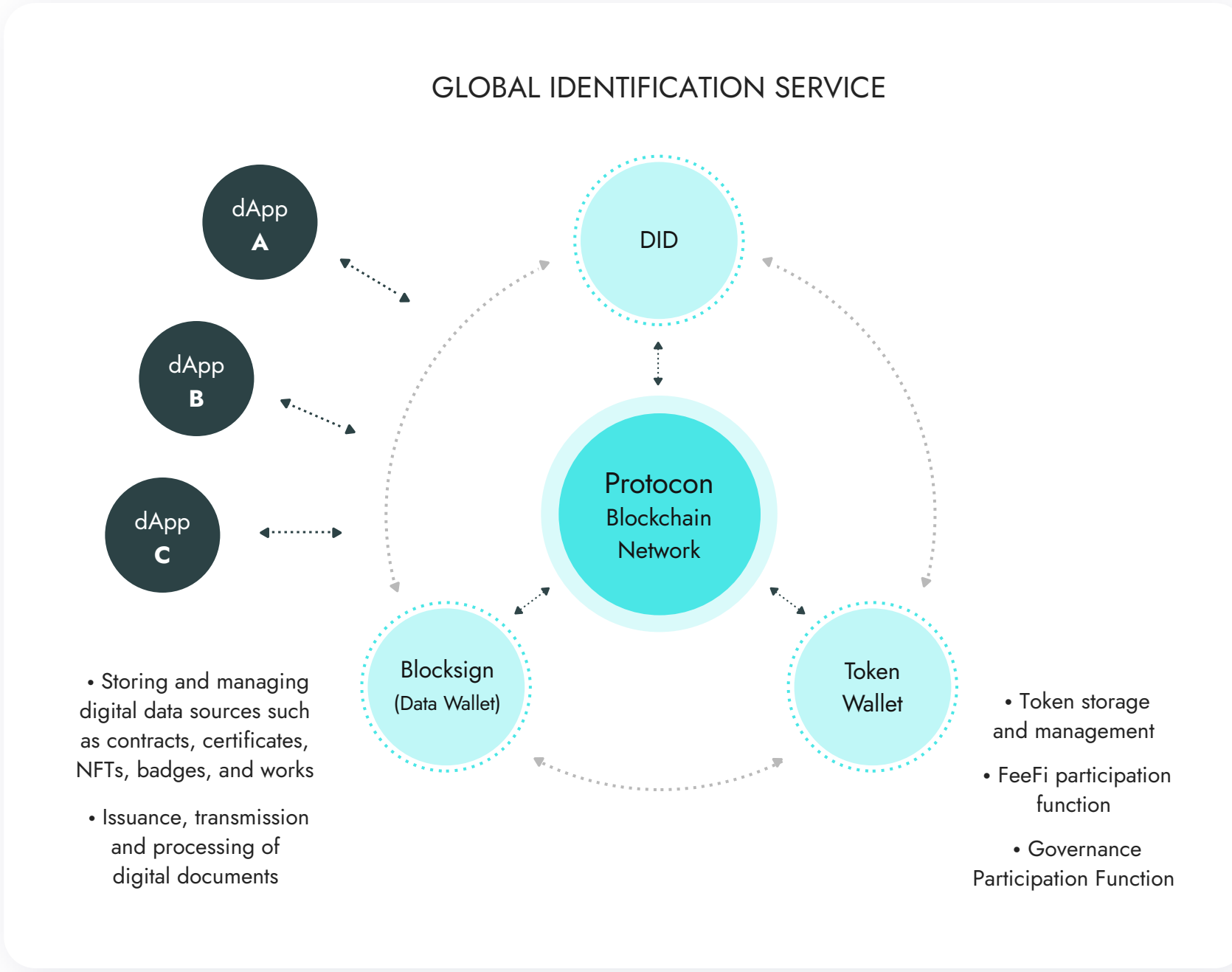
In addition, the blockchain alone cannot provide every service necessary for the digital transformation. The blockchain is a highly expensive solution needed to guarantee the credibility of digital data. Hence, the blockchain shall be utilized in an optimized and minimized way, as a methodology to guarantee the credibility, and in combination with the methodologies of providing the existing IT services. This is why we have implemented and operated ‘Blocksign,’ which the document and data management system linked with the blockchain, and ‘Blockcity,’ which is the model house of the blockchain technology and data production factory, while developing the original technologies. If we do not conduct such works personally, we cannot generate the usability of our blockchain network or build a proper example of utilizing the blockchain technology in the actual industry effectively.

Blocksign

To deal with blockchain-based data and documents properly, we need a cloud service that stores and handles them according to the process as well as the blockchain network, apart from the digital token that we are already familiar with. In other words, although we have focused on the blockchain itself to utilize it for industrial uses, that cannot let us handle diverse digital data. Hence, we have created a data cloud service called Blocksign along with the ProtoconNet. In the ProtoconNet’s perspective, Blocksign is a blockchain-based application. However, it is a kind of infrastructure service in terms of digital data management.



In particular, if industrial use of blockchain expands in the future, and data such as works based on individuals' NFTs, certificates and badges such as graduation certificates and vaccination certificates begin to be produced in full scale, the need to manage the original data increases. In that respect, if we call a wallet containing tokens as a token wallet, BlockSign has a kind of data wallet feature. Schematic illustrations include:



Digitization of documents are seriously lagging compared to other highly advanced digital technologies. The reason why documents could not be digitized is that a document is not just a combination of texts printed on paper. 1) A document is created through specific processes; 2) a document is handled (amended, modified, or discarded) through specific processes; and 3) sentences or numbers recorded on the paper have actual binding power in the real world. However, a proper methodology to handle those unique characteristics of documents in a digitized way has not been established. In other words, methodologies to digitize conventional analogue documents and handle them with methods suitable to digital environment have not been developed sufficiently. Hence, we are developing Blocksign, in order to manage diverse formats of digital data, including documents, effectively and efficiently. Especially, it will serve as the re to store the digital original of documents regarding items produced in games and relevant ownership.

Blocksign will be developed in 4 phases in total. Phase 1 development is completed at the moment, and phase 2 development is under way.

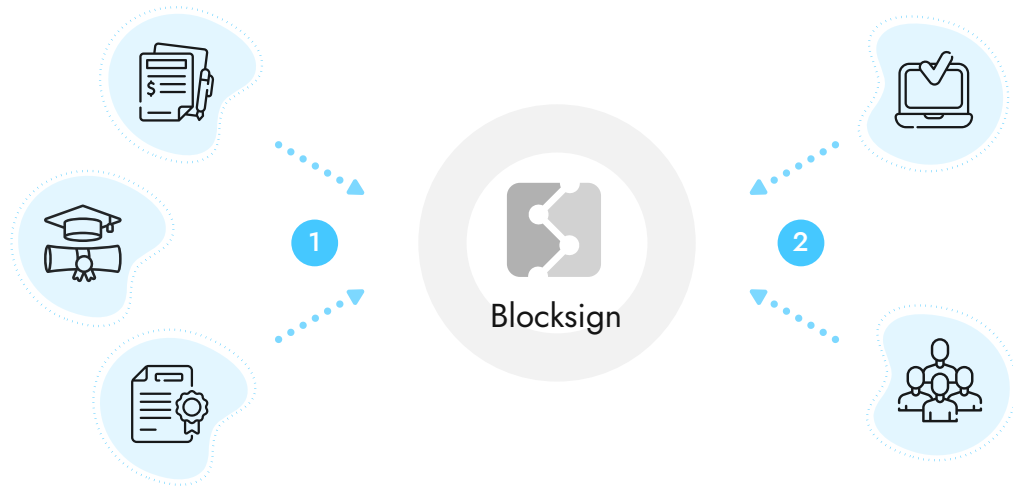
[Blocksign service implementation plan of each phase]

Phase 1 (Beta version completed)

Blockchain-based My data management function

Personal data storage, mutual signing, sharing, and document source verification

1. Store in Blocksign such as diploma, contract, etc.
2. Third party validates documents at Blocksign

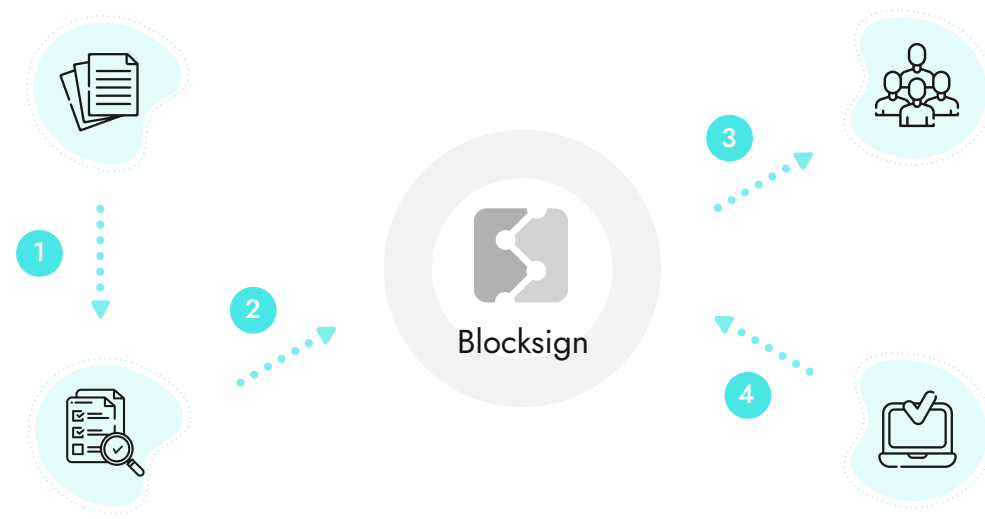


Phase 2 (In progress)

Issuing and sharing digital original documents

Issuing digital original documents, implementing document mutual authentication and sharing functions

1. Document issuance and recipient authentication request
2. Document recipient authentication and blocksign storage completed
3. Sending documents stored in Blocksign to third parties
4. Third party checks document validity in Blocksign

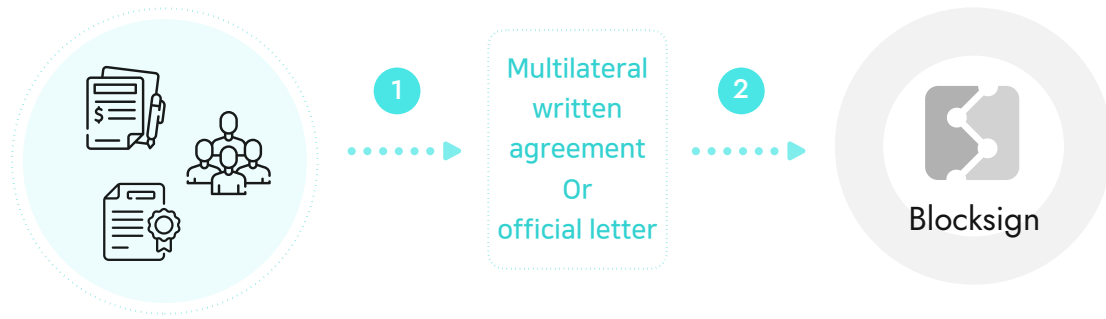


Phase 3 (To be developed)

Ability to create and manage multilateral agreements

Implementation of agreement document management function containing contracts of multiple individuals

1. Multiple individuals agree on the creation and modification of the terms and conditions (E-signature or voting)
2. Record the agreed documents and personal information participating in the agreement on the blockchain

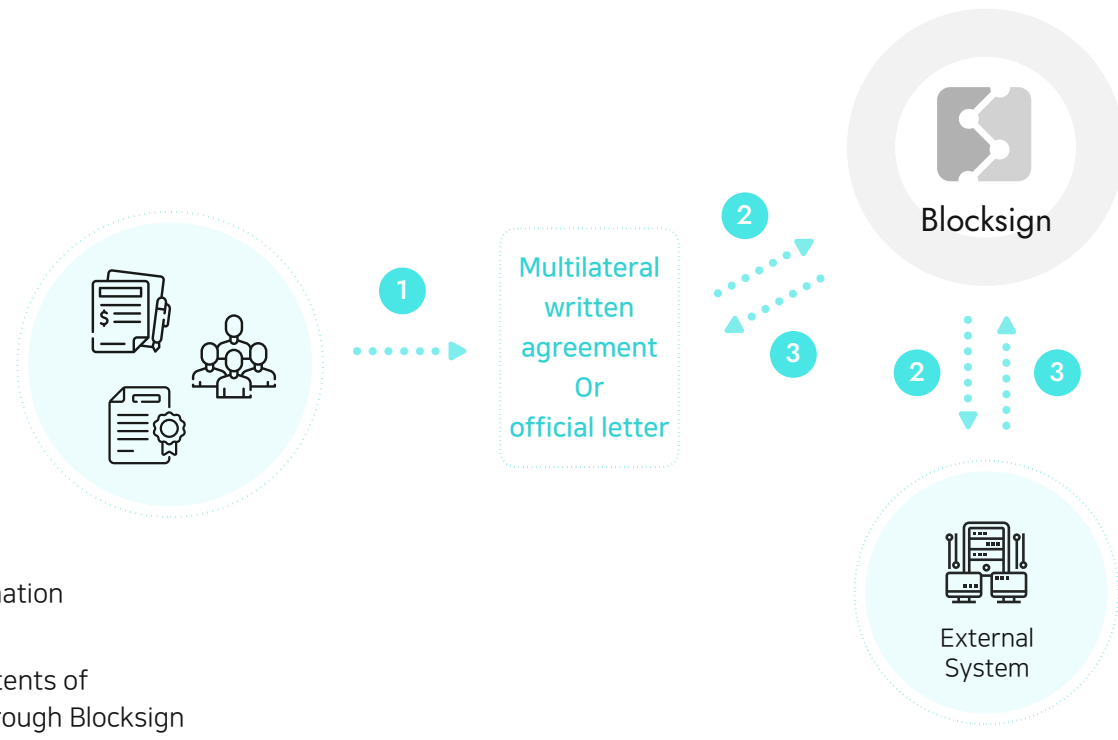


Phase 4 (To be developed)

Ability to manage external system-linked documents

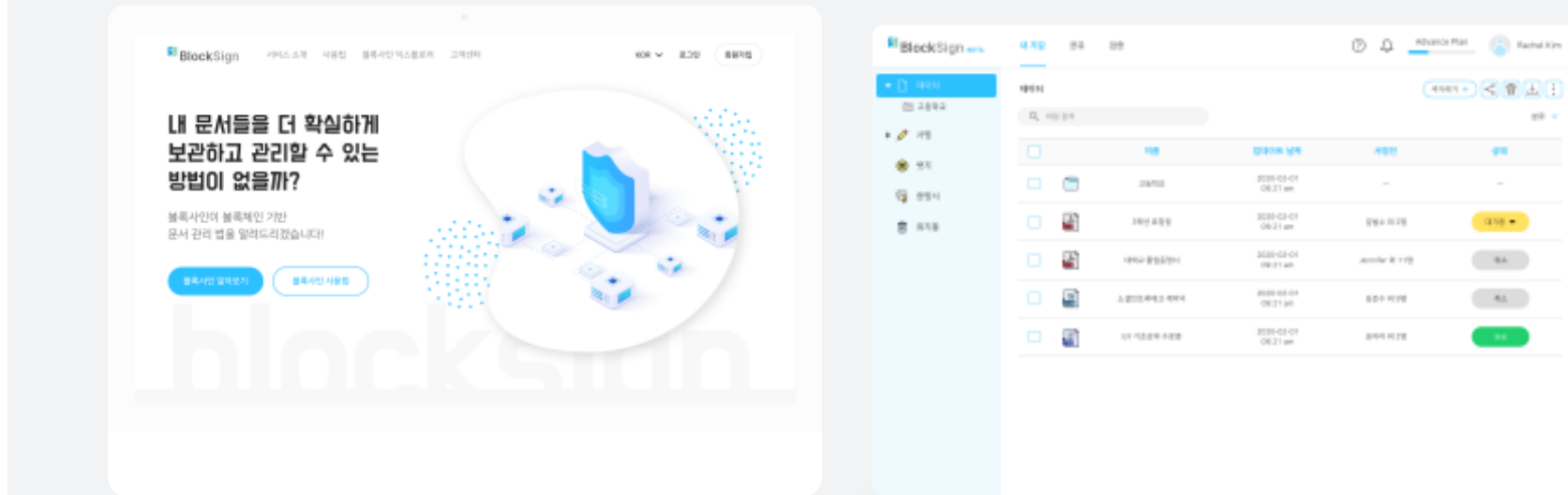
Implementation of external system controls by consensus of multiple individuals

1. Joint management of multilateral or public documents
2. Record agreed documents and personal information on Blocksign and control external system
3. External events systematically change the contents of consensus documents or public documents through Blocksign



The Phase 1 of Blocksign is the digitization of document management, which implements cloud storage to manage personal Mydata. Individuals can store the documents the one shall keep or verify to prove the original of the document and signature history. In other words, documents requiring verification, including graduation certificates, award certificates, and diploma, can be stored and managed easily, and simple interindividual contracts can be processed through mutual signatures. Improvement work to launch the service is currently underway, and the launching will be in the first half of 2021.

[Service page of Blocksign phase 1]



The phase 2 of Blocksign is the digitization of document creation and issuance, which can issue the digital originals of documents issued by schools or institutions and receive, share, and verify the digital originals. Our goal is completing the development and launching the service by the first half of 2022, and the developed service will be linked to BetaNet. The Phase 3 is implementation of digital management of documents based on or created by multilateral consensus, including laws, articles of association of corporations or cooperatives, municipal ordinances or conventions, and board resolutions of companies or organizations, which are created and modified by consensus of multiple individuals. The Phase 4 is implementation of the feature to grant digital documents created based on the consensus with power to control or regulate the actual digital infrastructures in the real world. For example, when a community makes a consensus to change the speed limit within the school zone from 30km/h to 20km/h, the road traffic control center automatically sets the new speed limit in accordance with the consensus, either in real time or at the designated time. To display the Blocksign's usability, we will document the certified copy of land registration, item ownership, and badges users purchased in the Blockcity, and enable storing the generated documents in the Blocksign and sharing them. In addition, it will implement concepts of the Phase 3 and the Phase 4 Blocksign that actually work through the establishment of rules by consensus and the automatic application of the established rules in the game.

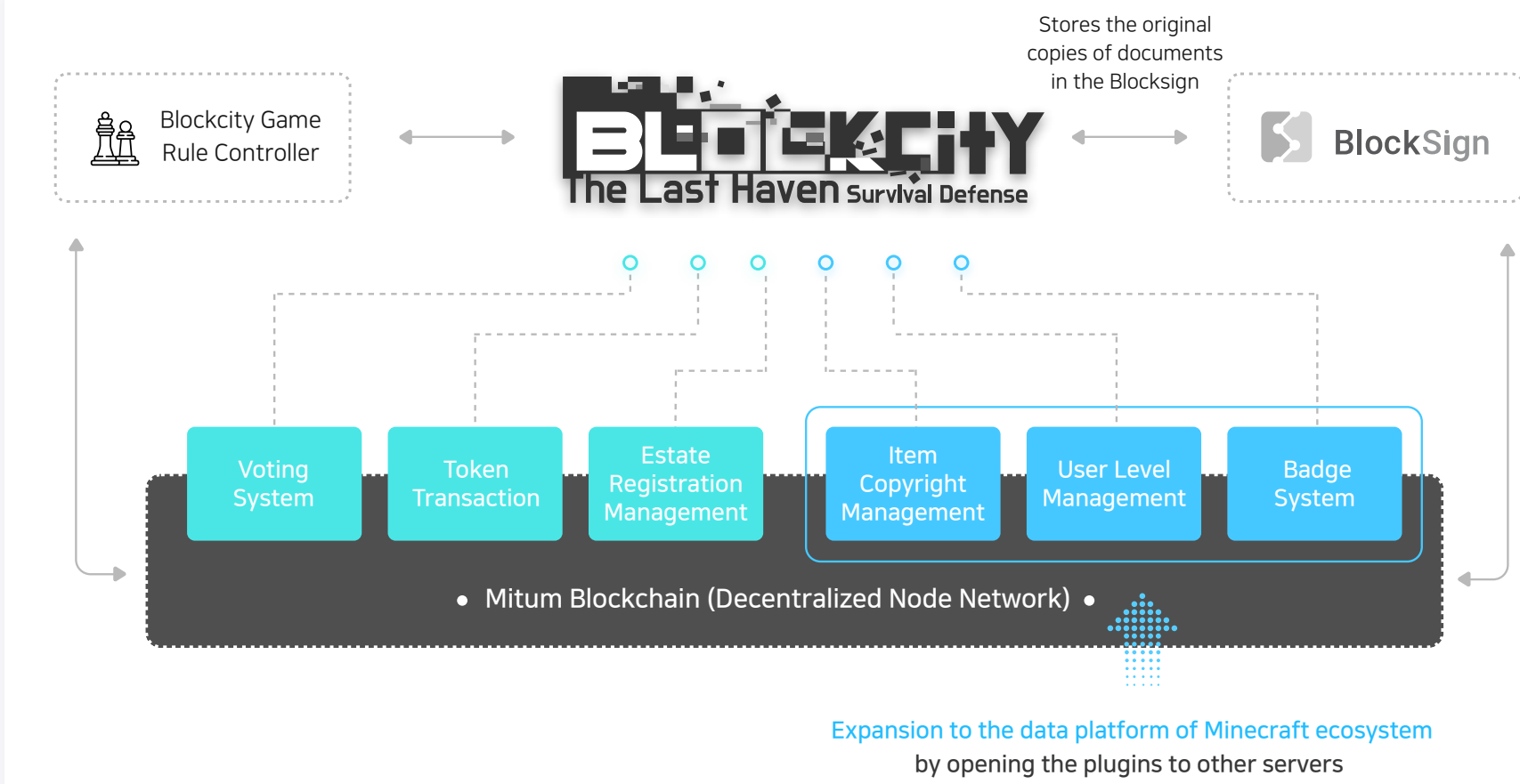
In a long-term point of view, we are considering linking data in the Blocksign to decentralized storage when decentralized cloud storage technology, such as IPFS, is sufficiently advanced. However, decentralized storage is available only at an experimental level, and much time is necessary until stable industrial use of decentralized storage become possible. Furthermore, it would become even more difficult if processes and operational features needed for data and document processing are included. For users, losing the private key of IPFS means losing every material stored in IPFS. That is, non-fungible loss may happen to the user. That is why we are trying to develop the Blocksign service based on existing cloud services, and we will aim to link with IPFS as our long-term objective.

Blockcity

To prove the applicability of ProtoconNet in industrial uses and build profitable mainnet business model, we have created the “Blockcity” where blockchain is fused into a game, Minecraft. In addition, we connected the Blockcity with Blocksign to store the original copy of documents and badges related to land registration, ownership, and copyright, proving the necessity and utility of the Blocksign service and generating its usability.

Minecraft is an open-world indie game developed by Markus Alexej Persson and taken over and distributed by Microsoft Studios. The 200 million copies of the game were sold, and 120 million users are accessing the game server monthly. As the first sandbox game, it allows the users to modify the game freely with diverse mods and plugins, and the users can create independent custom game server to enjoy games of diverse genres. We will utilize the Minecraft that have a global fandom to operate Blockcity game in which blockchain technology is applied.

[Structure Diagram of ProtoconNet, Blocksign, and Blockcity]



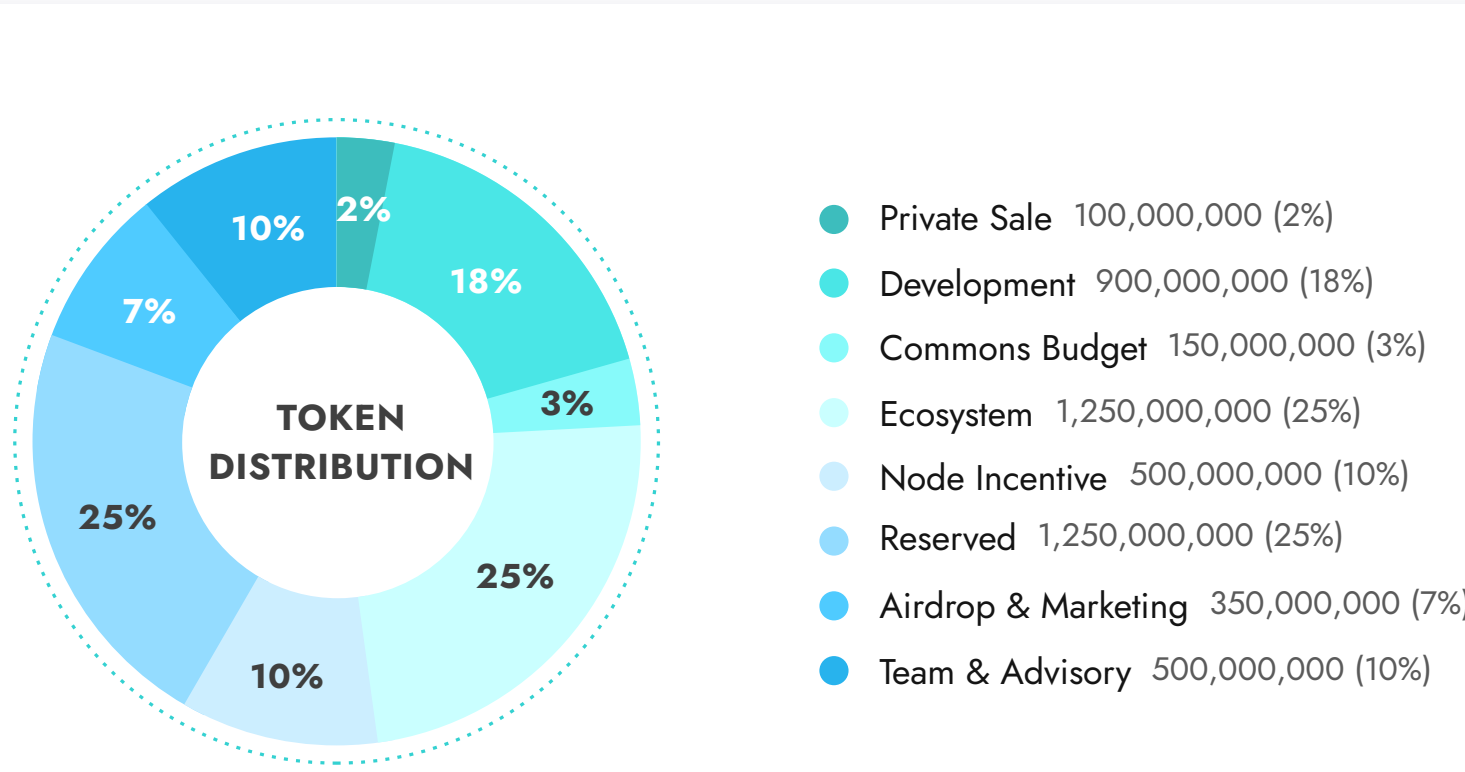
Blockchain technologies that we are applying in games like Blockcity are as follows.

1. Voting system (Citizens of the Blockcity participate in determining the rules of the game through the vote, and the determined rule is implemented in the game as blockchain codes. Linked to Blocksign phase 3 and 4)
2. Blockchain-based in-game point (game money)
3. Granting ownership of the virtual land, registration of estates, and management of estate transaction records
4. Registering and managing item ownership/copyright and trade history (linked to Blocksign phase 1)
5. Managing the game portfolio data, including gaming history, level, and experience point (linked to Blocksign phase 2)

We will expand our application of blockchain technologies to other games based on the ones applied to Blockcity and build a blockchain-based gaming ecosystem as our long-term objective. Plus, we are aiming to apply the blockchain technologies in the abovementioned game to public and industrial sectors as they are.

08 Token Allocation Plan

A total of 5 billion PEN tokens will be issued, and will be allocated as follows in consideration of securing continuity of development, mainnet operation and ecosystem construction.



The above 5 billion tokens are allocated sequentially over a total of 15 years, with the initial yearly allocation plan as follows. (Unit, 1 Million)

Items	2021	2022	2023	2024	2025	2026	2027	2028	2029	2030	2031	2032	2033	2034	2035
Private Sale	100	0	0	0	0	0	0	0	0	0	0	0	0	0	0
Development	0	100	100	90	80	70	60	50	50	50	50	50	50	50	50
Commons Budget	0	10	20	10	10	10	10	10	10	10	10	10	10	10	10
Ecosystem	0	100	200	150	150	120	100	90	80	70	50	50	30	30	30
Node Incentive	0	50	50	50	40	40	40	40	30	30	30	30	30	20	20
Reserved	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0
Airdrop & Marketing	30	30	25	25	25	25	25	25	20	20	20	20	20	20	20
Team & Advisory	100	30	30	30	30	30	30	30	30	30	30	30	30	20	20

The above plan is designed with a top priority on ensuring that ProtoconNet is stable in the market and that token prices do not fluctuate dramatically. The reserved volume has not been specified for its current use yet but is intended to be assigned to areas that may be added in the future, areas that are insufficient compared to the initial plan, or token usage required after 2035. When using a reserved volume, it must be approved by congress. In addition, each year's quota is subject to a separate lockup policy for each item to prevent tokens from being distributed to the market at once. Devices have been introduced to prevent moral hazards among key developers. For instance, even if the team and advisory portion is allocated in 2021, the lockup will be one and a half years after the token's first listing. Therefore, the number of tokens allocated per year in the table above does not necessarily match the actual market volume. In addition, some of these supplies will continue to accumulate in commons budget via FeeFi, and the accumulation in commons Budget will be approved by congress to maintain the mainnet and ensure ecosystem sustainability. In addition, when the actual mainnet is operated and the ecosystem starts to work, the actual reality will be different from the original plan. After the official operation of mainnet and congress, we will submit an annual plan to congress and adjust the token distribution plan to suit the market environment through approval from congress.

Conclusion

We have included aspects that we have realized or are going to update in a nearby future. We will gladly accept new methodology and way for the sake of our goal of applying decentralization and blockchain to our real lives, and the Whitepaper will be continuously updated accordingly.

09 References

[1] ProtoconNet is short for Protocol Economy Network.

[2] Miguel Castro and Babara Liskov at 1999, [Practical Byzantine Fault Tolerance] (http://pmg.csail.mit.edu/papers/osdi99.pdf)

[3] https://github.com/bosnet/sebak

[4] The plus sign (+) on ISAAC+ means that it is the upgraded version of the existing ISAAC Consensus Protocol. ISAAC Consensus Protocol divided the consensus process into four stages of Init - Sign - Accept - All Confirm, which is similar to the four stages of PBFT. The name ISAAC originates from the first letters of each stage, I-S-A-AC.

[5] Andreas M. Antonopoulos, Gavin Wood, Mastering Ethereum: Building Smart Contracts and DApps', O'Reilly Media, 2018

[6] https://medium.com/@VitalikButerin/the-meaning-of-decentralization-a0c92b76a274

[7] https://tezos.com/

[8] https://terra.money/

[9] Myungsan Jun, 'Blockchain Government: A next form of infrastructure for the twenty-first century', CreateSpace Independent Publishing Platform, 2018

