ANDUS Chain

Fair & high-speed public blockchain:

Version 0.95 August 2021

Fair & high-speed public blockchain: AndUsChain version 0.95

Subtitle: Secure, fair & high-speed next generation Ethereum

No doubt that Blockchain is the core technology for the Fourth Industrial Revolution. It's also known as the second Internet (Value added Internet). Currently, computers and Internet are the main infrastructure for cyber world; then, blockchain technology will be the infrastructure moving forward.

Actually, blockchain implies more meanings than just simple distributed ledger technology. Obviously, blockchain is a sort of brand-new computer as well as entirely new network. As we know, the definition of Ethereum is global trusted computer. Based on this blockchain technology, every current ecosystem such as politics, economy, finance, medicine, energy, logistics and education will be transformed. The transformed new ecosystem shall be, what we called, blockchain world.

The basic philosophy of blockchain is to realize a decentralized P2P based world. In other words, it is an attempt to innovate the P2P-based world without a third-party trusting agency or intermediary that assumes reliability. The blockchain that reflects these philosophical ideas is the public blockchain. Ethereum is the one of the most representative public blockchains and aims to realize blockchain's philosophical ideas. It is the reason why we have named AndUsChain, the Fair High-Speed Next Generation Ethereum.

AndUsChain is the public blockchain based on Ethereum; however, there has been many debates on the sustainability of Ethereum due to its PoW(Proof of Work) and PoS(Proof of Stake) methods given that PoW and PoS have a sort of centralized characteristics rather than decentralized ones.

Except for sustainable decentralized consensus algorithm, there seems to be many solutions for Ethereum due to the significant progress of lots of researches. Still, there exists big gap on sustainable decentralized consensus algorithm.

Obviously, AndUsChain developed the public blockchain which applies the ‘deb’ consensus algorithm. The ‘deb’ consensus algorithm will enable public blockchain to maintain sustainable decentralized characteristics. The main purpose of ‘deb’ consensus algorithm is to develop much faster public blockchain than Ethereum by enhancing sustainable decentralized characteristics.

Table of Contents

Table of Contents

1. Overview

With the concept of distributed ledger and PoW(Proof of Work) consensus algorithm, Satoshi Nakamoto introduced Bitcoin, a decentralized P2P crypto currency system in 2008. In 2014, Vitalik Buterin developed Ethereum, "A trust world computer", which resolved some limitations of Bitcoin such as Turing Imperfection.

Since the most critical technology of blockchain is a consensus algorithm between nodes that do not trust each other, PoW (Proof of Work) method is used in both Bitcoin and Ethereum's consensus algorithms. However, for the consensus algorithm using PoW method, the mining probability is determined by the computing power possessed by the node, it means the decentralization characteristic of the blockchain is reduced, and a major problem of bitcoin concentration is identified. For these reasons, Ethereum is currently switching its agreement algorithm to PoS (Proof of Stake) method with processing certification. However, since this causes the stake held by the node to determine the mining probability, a fundamental question of whether its decentralization characteristic is sustainable. For the same reason, an argument has emerged that PoS based system essentially has the problem of capitalism.

We first try to define and analyze the decentralization characteristics of a consensus algorithm, which is the core source technology of a blockchain, as a fairness concept. Briefly, the fairness of the consensus algorithm can mean the proportionality of the probability depending on the target node's conditions (computing power, holding stake, etc.).

Then, we propose a DEB consensus algorithm that maximizes fairness and tries to develop a public blockchain, AndUsChain, that maintains sustainable decentralization characteristics.

AndUsChain is based on Ethereum. In other words, AndUsChain is a public blockchain that maintains the structure of Ethereum, which is a typical public blockchain with sustainable decentralization and increased speed. To date, many blockchains have been proposed, including public blockchains and private or consortium blockchains, but it is Ethereum blockchain that satisfies the essential philosophy of the original blockchain because creating the infrastructure for decentralized P2P business ecosystems (ecosystem) is the primary purpose of Ethereum.

On the other hand, the distinction between the DEB agreement algorithm, the PoW information used in the existing public blockchain and PoS method can be related to mining and issuance of cryptocurrency. For existing consensus algorithms participating in mining. It is how a cryptocurrency issuance right is given as a reward to a successfully minded node.

However, in the case of the DEB agreement algorithm, mining and cryptocurrency issuance are not related. In other words, mining and issuance of cryptocurrency are mutually independent algorithms, which are a total algorithm for developing the first public blockchain. It is a system that consists of nodes that want to participate in mining, and compensates for transaction fees with a part of participation fee of the paid mining league, instead of giving the necessary compensation money for miners with cryptocurrency issuance privileges.

There is also a key reason for this configuration is also linked to making the node mining conditions independent for sustainable decentralization. In other words, to ensure the fairness of the mining operation, the mining process is such a low cost that it can be fair to all nodes, so a high-reward system would not be necessary.

In particular, the DEB agreement algorithm has an advantage of no fork being generated, unlike other public blockchains. It ensures that the creation of the block immediately guarantees the finality of the block.

2. Vision and Goals of AndUsChain

The vision and goal of AndUsChain are, in principle, same as the vision and goal of the public blockchain, Ethereum that realizes the philosophy of blockchain. However, we have managed to solve the problem of the decentralization of the consensus algorithm while having maintained a high-performance of the next-generation Ethereum.

Vision :

- *To create a Fair and high-speed public blockchain platform*
- *To realize a fair and reliable world*

Target :

- *Realization of crypto economy and blockchain economy*
- *Infrastructure for constructing DAPP ecosystem with maximized convenience*

AndUsChain is also an open blockchain platform for decentralized P2P business ecosystem like Ethereum. In other words, it has all the token issuing functions, smart contract functions, smart asset functions, and DAO functions Ethereum has.

In particular, AndUsChain is a blockchain based while enhanced the ability to support a convenient ecosystem for users to activate the decentralized P2P open ecosystem (DAPP ecosystem).

Differentiated features from Ethereum

1. *Debating a fair agreement algorithm that maintains sustainable decentralization characteristics, and applying the algorithm*
2. *No linkage between mining and cryptocurrency issuance (that is, password mining function is not included in mining function)*
3. *The best performance among public blockchains: over 1,000 TPS*
4. *Finality is guaranteed at the same time as creating a block without a fork*
5. *Strengthen the ecosystem support function of Dapp service*

3. Fairness of Consensus Algorithm

Before explaining the sustainable decentralization characteristics of the AndUsChain, we explain the fairness of the consensus algorithm.

The purpose of the DEB consensus algorithm is to maintain sustainable decentralization characteristics by ensuring fair mining probabilities for all nodes regardless of the mining node's conditions. (computing power, holdings, etc.)

For this reason, we first define the fairness of the consensus algorithm and analyze the fairness of the existing public blockchain.

Definition: Fairness of consensus algorithm

The fairness of the consensus algorithm is defined as the correlation between the mining probability of a node and the conditions. (computing power, stock, etc.)
For example, with PoW in Bitcoin and Ethereum, the probability of becoming a mining node is determined by the computing power of the node. It means the probability of successful mining is proportional to the total computing power of nodes.

$$\text{Mining Success Probability of Node} = \frac{\textit{Owned computing power}}{\textit{Sum of computing power held by all nodes}}$$

In the case of Bitcoin, which employs PoW method, the probability of a general node succeeding in mining due to the birth of a mining factory or group is almost zero. This has created a controversy on Bitcoin.
For Ethereum, which employs PoS method, the mining probability of the node is determined by the stake held by the node. This means node's mining success probability is the share of cryptocurrency held.

$$\text{Mining Success Probability of Node} = \frac{\textit{Owned stake}}{\textit{Total amount of cryptocurrency}}$$

In the case of the PoS method, the fact that typical capital logic is applied, when the mining probability of the stake held is determined, has already been pointed out.

Fairness of Consensus Algorithm

4. DEB Consensus Algorithm

In the case of the current PoW and PoS agreement algorithm, the mining node's mining probability is proportional to the mining node's computing power and the possessed stake. It indicates to the miners that it is not fair.

The DEB consensus algorithm is a consensus algorithm for solving such a problem while ensuring a fair mining opportunity. First, to secure a fair mining opportunity, it is necessary to give a fair mining opportunity regardless of the conditions (computing power, shares held, etc.) given to all nodes to be mined.

For this reason, the DEB agreement algorithm introduces the concept of fair nodes (hereinafter used in combination), unlike the PoW and PoS schemes. Of course, we do not assume a fair node's reliability to maintain the characteristics of the P2P-based DEB agreement algorithm. In other words, a fair node is not a third trusted party (TTP), just a special node that supports the agreement algorithm in cooperation with nodes in the P2P network. We will explain the role and security of a fair node in the future.

The DEB consensus algorithm operates on three basic principles: Paid Mining League, Maximum Random Number Rule (MRNR), and Majority Rule. A paid mining league is a group of a specific number (for example, 100 people) of nodes for mining. Of course, a node wishing to participate in the mining league must pay the participation fee which is as small as practically possible (for example, 100 won) to participate in the mining league. The maximum random number rule is a rule that is composed of nodes that participate in the paid mining league, and each node in the group generates a block. The method for determining the final miner determines the last block, consists of the principle of majority voting through cooperation between fair nodes and nodes participating in the mining league.

Overall configuration diagram of the DEB Agreement Algorithm is as follows.

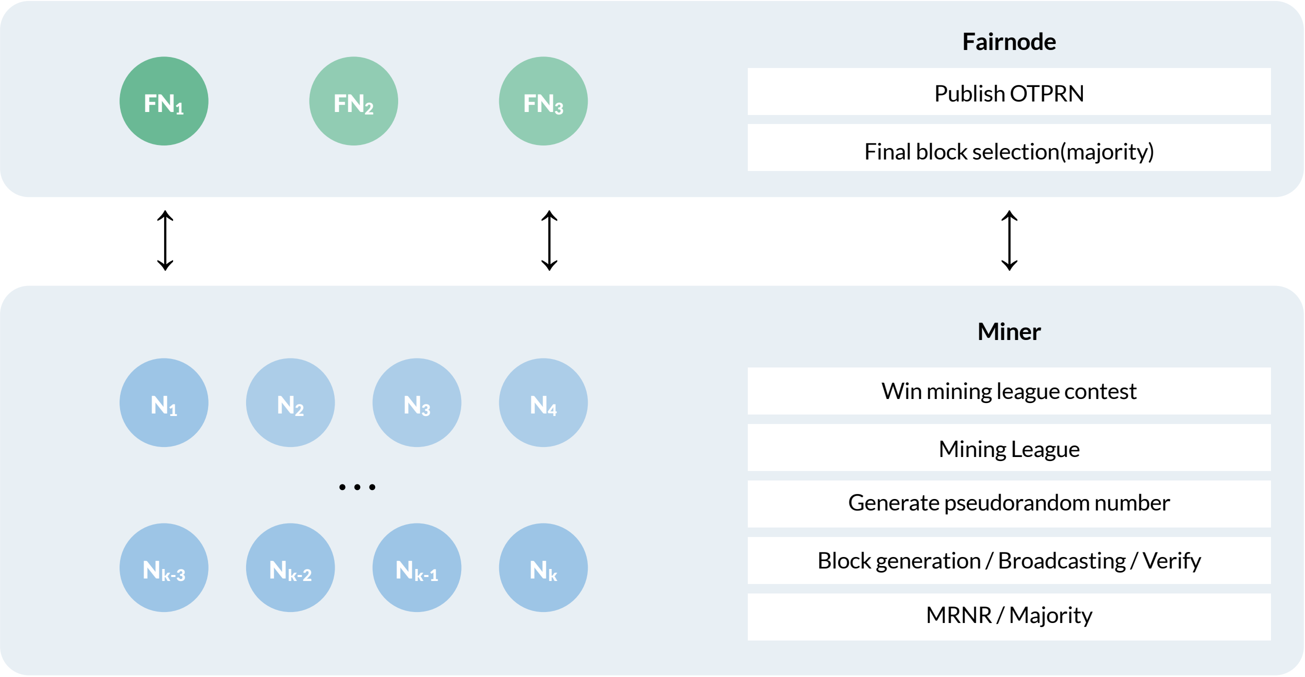

FN1
FN2
FN3
Fairnode
Publish OTPRN
Final block selection(majority)
Miner
N1
N2
N3
N4
...
Nk-3
Nk-2
Nk-1
Nk
Win mining league contest
Mining League
Generate pseudorandom number
Block generation / Broadcasting / Verify
MRNR / Majority

Figure 4-1 Consensus Agreement Diagram

A fair node can be composed of clusters.

4.1 deb consensus algorithm full process

The entire process of deb consensus algorithm consists of three phases: paid mining league configuration, block creation(mining), and final block consensus.

Organized a paid mining league

1. *The node that wants to mine provides its own access information to a fair node.*
2. *Fair nodes are distributed to all OTPRN nodes for mining rig configuration.*
3. *Nodes who wish to participate in the mining league shall OTPRN determine whether they are eligible to participate in the mining league by referring to the distribution of the fair node.*
4. *Mining nodes selected as participants of the Mining OTPRN JoinTx League will be created, including for the construction of mining leagues.*
5. *Broadcast to all JoinTx nodes.*
6. *Refer to only mining nodes JoinTx selected as participants of the Mining League.*

Block creation (mining)

1. The mining node participating in the mining league creates difficulty the basis for the final block selection.

$$difficulty=\{0 \leq n \leq JoinNonce \mid MAX(CSPRNG(n,OTPRN.rand,coinbase,P\_blockHash\ ))\ \}$$

** If you have applied for a mining rig to equalize the probability of mining, but have not been selected as a miner, you will generate difficulty multiple numbers if you are not selected.*

2. The mining node generates a block, difficulty including in the block header.

3. Broadcast blocks created for all nodes.

Consensus algorithm

The basic principle of block consensus is the final block consensus process by majority resolution, in which the largest number (MRNR:Maximum Random Number Rule,the largest random number) rule and the node and the fair node work together.

1. The node selects and signs the largest block of the block difficulty that it receives and sends it to the fair node.

2. The fair node decides and signs the most selected blocks of the blocked sent in accordance with the majority resolution principle and sends them to the nodes.

3. The mining node broadcasts to the entire node after verifying that the block received from the fair node is a block selected by a large number.

4. Each node recognizes a fair node and a block signed by a majority as the final block and adds it to the blockchain.

4.2 Paid Mining League Configuration Detailed Process

For safety and efficiency, the method of organizing a paid mining league is conducted by adjusting the number of fair nodes and nodes themselves and applying for participation in the mining league.

Selected as a participant in a paid mining league

1. Nodes that want to be mined provide node information to a fairnode.

Field name	Description
enode	Enode value of mining node.
coinbase	The address of the account to participate in mining.
port	Port number to communicate with fair node.

<Table 4-1> enodeCoinbase structure

2. A fair node distributes a transOTPRN structure to all nodes, depending on the block creation cycle.

Field name	Description
OTPRN	The structure that mining nodes refer to when mining
Sig	*OTPRN* The signing of a fair node for

<Table 4-2> transOTPRN structure

Field name	Description
num	*OTPRN* issue number
rand	One-time pseudo-random numbers that fair nodes periodically deploy
CMiner	The number of nodes that are maintaining a fair connection to the mine to perform mining.
Timestamp	Local time for fair nodes

<Table 4-3> OTPRN structure

3. Mining candidate nodes refer to the structure deployed by the fair node OTPRN to determine if they can participate.

A. Set the system setting variable Mminers to the number of participants in the maximum mining

B. The mining node sets OTPRN the Cminers as an avoiding water, indicating the total number of mined nodes that the fair node propagated, which indicates the intention of mining.

C. Set the amount obtained by computing two values to Div

$$Div=CMiner \div MMiner$$

D. enodeCoinbase.coinbase Using the sum of the OTPRN.rand XOR operations as the seed of the random function to derive random values* is a random function.

$$rand=RAND(\sum_{i=0}^{19} enodeCoinbase.coinbase[i] \quad OTPRN.rand[i]))$$

* RAND is a random function

E. ***rand*** modular operations to determine that mining participation is possible when the following conditions are met. ***div***

rand % div==0

Organized a paid mining league

1. Mining nodes that can participate in the mining league create ***OTPRN*** a structure, including the structure, ***JoinTx*** and broadcast it to all nodes.

* ***JoinTx*** : Application transactions for participation in mining leagues that result when a node wants to participate in a mining league

Field name	Description
Tx	Same as Ethereum transaction structure except for the field below *to: Fiarnode' s address* *data: JoinTxData*

<Table 4-4>　JoinTx structure

Field name	Description
JoinNonce	Add 1 to the account *JoinNonce*
OtprnHash	Hash value received from a fair node *OTPRN*
FairnodeSig	*transOTPRN.sig*
Timestamp	Local time for mining nodes
NextBlockNum	Number of blocks to be mined

<Table 4-5>　JoinTxData Structure

2. Collect only mining nodes that JoinTx have participated in the Mining League.
3. The mining node organizes its own JoinTx mining rig by listing the collected ones.

4.3 Block creation process: mining process

Use fair nodes and pseudo-ins for fair and efficient Difficulty mining.

Difficulty generation

1. The mining node generates difficulty using a reference to the OTPRN structure received from a fairnode in the participant selection process.

$$\text{difficulty}=\{0 \le n \le \text{JoinNonce} \mid \text{MAX}(\text{CSPRNG}(n,\text{OTPRN.rand},\text{coinbase},P_{\text{blockHash}}))\}$$

* ***JoinNonce*** : ***JoinNonce*** for other purposes of, As the mining node participates in the mining rig, it performs the function of increasing the probability of mining. To achieve this goal, ***JoinNonce*** As many as different ***difficulty*** can be generated and the largest value of which can be used to create blocks. ***JoinNonce***

* ***OTPRN.rand*** : A one-time pseudo-random number deployed by a fair node prevents mining nodes from generating any value that is favorable for mining ***difficulty***

* ***coinbase*** : To have the mining nodes create differently by the address used to mine ***difficulty***

* **P_BlockHash** : Hash value of previous block (i) To prepare for the distribution of a fair node favorable to a particular mining node, and ***OTPRN.rand*** (ii) to allow the mining node to create one that is dependent on a particular block. ***difficulty***

2. The mining node creates a difficulty transaction by selecting the difficulty largest of its own creations.

$$\text{difficulty} = \text{MAX}(0 \leq n \leq \textit{JoinNonce}\{\textit{difficulty}_n\})$$

Block creation and broadcasting

1. The mining node generates random numbers by referencing their block headers OTPRN.rand, JoinNonce and other data, and then records the random number and its own in the block header. Exist within a block and is recorded by a fair node in the future FiarNode.Sig and Voters.

Separated	Field name	Description
Header	*UncleHash*	Remove
	JoinTxHash	*JoinTx* List hash value
	GenTxHash	*Tx* List hash value
	JoinReceiptHash	*JoinTx* Receipt hash value of
	GenReceiptHash	*Tx* Receipt hash value of
	Difficulty	Random value generated by utilizing the mined node received from a fair node *OTPRN*.rand
	nonce	*JoinNonce* The value of the mining node
	FairNodeSig	A fair node is a value signed by a number of mining nodes, including selected blocks and proof data.
	VoterHash	*Voters* Hash value
Body	*JoinTxs*	*Tx* List
	GenTxs	*JoinTx* List
	Voters	Address and signature of nodes that voted on the block (multiple)

<Table 4-6> Block structure

Field name	Description
addr	The address of the mining node that voted for the block.
sig	Signature of mining node
difficulty	*difficulty* Used to verify that the value created by the mining node is correct, selected by a *difficulty* future majority.

<Table 4-7> Voters structure

2. The various transactions collected by the mining node are included in the block, and then the block is created.
3. The mining node broadcasts the generated blocks to other mining nodes.

4.4 Consensus algorithm

Block consensus is basically MRNR based on the principle of majority resolution. In other words, Originally, mining nodes broadcast their own created blocks. Select the largest designated block of the block received to you difficulty(MRNR) and then sign and send to a fair node.

A fair node selects a block selected by a large number of the blocks it receives (majority resolution principles) and includes the address and signature of the mining nodes within the block and then signs itself. And if a fair node propagates the block to the mining node, the mining nodes will have the block in accordance with the principle of majority resolution., Verifies whether a fair node has been signed, and then add it to the ledger. As a result, the block is determined as the final block., Mining nodes propagate the block to the network.

Validation phase

1. Make sure that the *OTPRN* propagation cycle and the block creation cycle match.
2. Verify the *OTPRN* integrity and signature of fair nodes.
3. Make sure that the mined node is eligible to participate in the mining league.
4. Make sure that the mining node can pay for the mining league.
5. make sure that *difficulty* is created correctly.

Block agreement

1. The mining node selects the block (MRNR) that is the largest *difficulty*, signs it, and sends it to a fair node.
2. A fairnode is selected and signed as the final block and then sent to the nodes in accordance with the principle of majority resolution of the sent block. For future verification, a fair node will include and sign the addresses and signatures of the mining nodes that voted on the block.
3. The fairnode broadcasts the block to the mining node. Mining nodes are sure that the received blocks meet the principle of majority resolution., Verify that a fair node's signature is included, then add it to your ledger and broadcast the block.
4. Similarly, the general nodes that received the above block nodes (that did not participate in mining) also go through the same verification procedures as the mining nodes performed, and then add the block to the ledger.
5. Miners are provided with incentives as follows:
   Incentives= Transaction fees + Total participation fee for mining league participants
6. Adjust the mining probability of mining league participants.
   - Mining Success Node : Tx.Join_Nonce =0
   - Mining Failure Node : $\text{Tx.Join}_{\text{Nonce}} = \text{Tx.Join}_{\text{Nonce}} + 1$

4.5 The role and fairness of fair nodes

Consensus algorithms in Bitcoin and Ethereum do not use fair node concepts. However, deb In the case of consensus algorithms, the concept of fair nodes was introduced to maintain sustainable decentralization characteristics. Of course, deb consensus algorithm does not assume the reliability of a fair node in order to operate.

The Fair Node is only responsible for the efficiency, block consensus, and finality cooperation of the paid mining league configuration.

The role of fair nodes

1. Random selection of paid mining league participants
2. Final block consensus cooperation through mutual checks with nodes

Most importantly, the deb consensus algorithm does not depend on the reliability of a fair node. Through mutual checks between fair nodes and blockchain nodes, the safety of the blockchain can be secured without ensuring the reliability of fair nodes.

The fairness of the deb consensus algorithm using a fair node can be thought of as follows:

$$\text{Mining Probability of Node} = \frac{1}{\textit{Total number of nodes desired to be mined}}$$

DEB Consensus Algorithm

4.6 Performance

The performance of the deb consensus algorithm can be dynamically determined by the number of paid mining league configurations and block creation cycles.

For example, if you have 100 mining leagues, the expected performance is as follows:

	deb consensus algorithm
Block Size	4.5MB ~ 9MB
TPS	1000 TPS
Creation cycle	30sec ~ 1min

<Table 4-8> deb Consensus Algorithm's Performance

In particular, reducing the network connection load between fair nodes and paid mining league nodes to reduce block creation time can further reduce the block creation time. For example, the number of blocks generated by a paid mining rig that is configured once 10 block creation time 10 will be shortened in seconds.

4.7 Features of deb agreement algorithm

The purpose of the deb consensus algorithm is to solve the problem of centralization of blockchain consensus algorithms that can be caused by the unfairness of the current consensus algorithm. In other words, Proof of work, an existing consensus algorithm is to prove your stake, and the biggest difference between the consensus algorithms is that sustainable decentralization can be maintained. This means that it is a fair consensus algorithm that does not depend on the conditions of the nodes that want to be mined.

In addition, in the case of the consensus algorithm of the existing public blockchain, but the mining and crypto currency issuance to generate the block is linked, in the case of deb consensus algorithm, mining and crypto currency issuance is irrelevant. In other words, this means that the amount of crypto currency issued earlier is the total amount of currency.

This is the first consensus algorithm that allows the public blockchain to be configured while monopolizing the right to issue crypto currencies.

On the other hand, the advantage of deb consensus algorithm has the advantage that the fork does not occur if the finality is one block.

Deb consensus algorithm features

1. Maintaining sustainable decentralized characteristics (fairness)
2. No mining and cryptocurrency issuance (cryptocurrency issuance can be exclusively available)
3. Finality guarantee of one block without fork
4. High-speed performance over 1,000 TPS

5. AndUsChain

Since the AndUsChain is based on Ethereum, many of the architectures, etc., are the same as Ethereum and appear to have improved the consensus algorithm to maintain sustainable decentralization characteristics. In this chapter, we will deal with the parts modified in the existing Ethereum and the aspect of personal information protection.

5.1 Ethereum Correction Area

The changes made to apply the DEB agreement algorithm are summarized as follows.

Account status

Add : *JoinNonce*
√ Mining probability by the value increased to the increased value every time you participate in the mining league

And lead voluntary mining league participation

Transaction structure: *JoinTx* type

Correction : *to*
√ Replaces the field with the fair node address

Add : *JoinNonce*
√ Number of dredging sent by mining nodes (initialization when mining is successful)

Add : *OptrnHash*
√ Hash value received from fairnode

Add : *FairnodeSig*
√ Signature value included in transOTPRN structure sent by a fairnode

Add : *Timestamp*
√ A local time when mining the mining node

Add : *NextBlockNum*
√ Block number to mine

Block structure

Add : ***JoinTxHash***
√ List hash value

Add : ***JoinReceiptHash***
√ receipt hash value of

Correction :*difficulty*
√ Enter the mining league with OPTRN structure with fair nodes deployed Contains necessary information

Correction : ***nonce***
√ Mining node value

Add : ***FairnodeSig***
√ A block with proof data from a number of mining nodes selected by fair nodes Signed value including

Add : ***votersHash***
√ *voter's* hash value

Delete : ***uncleHash***
√ Fork does not occur, and a block is not generated, so No field needed

Delete : ***mixHash***
√ Pow Agree algorithm is not used, so these fields are not required

Add : ***voters***
√ Address and signature of the node that voted for the block

Add : ***JoinTxList***
√ *JoinTx List*

In particular, the AndUsChain uses the deb consensus algorithm to perform best while maintaining the sustainable decentralization of public blockchains proposed to date.

	Bitcoin	Ethereum	AndUsChain
Consensus Algorithm	PoW	PoS	deb
TPS	7	12~15	300 over
Finality	10min	About 3min	10sec ~ 1min

<Table 5-1> Performance comparison of major public blockchains

In conclusion, the AndUsChain is based on the deb consensus algorithm, which maintains a sustainable decentralization that has the same mining probability in fair conditions while being a High-speed public blockchain.

5.2 Information protection functions such as personal information protection

The information protection function uses a function built in the Ethernet. The information protection function that exists in the Ethereum can verify P2P encrypted communication and zero-knowledge proof data.

This is done via a saved smart contract.

Encryption of the transmission section

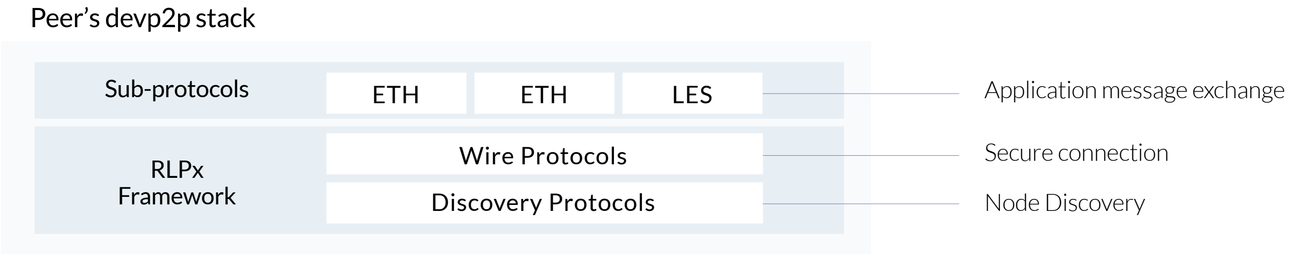
The set of protocols that make up the Ethereum P2P network is called “devp2p”. Devp2p is not only used in the blockchain but is designed to be used in all network applications related to Ethereum. This is another node on the network
Used to detect transactions and exchange transactions and blocks.
Devp2p consists of two layers, as shown below.

RLPx framework

√ Enables communication between nodes. This framework can be divided into a Discovery protocol that detects other nodes and a Wire protocol that allows each node to establish an encrypted and authenticated connection to each other.

Sub-protocols for user area

√ Ethereum (ETH), Whisper (SHH), Swarm (BZZ), Light Client Protocol (LES)

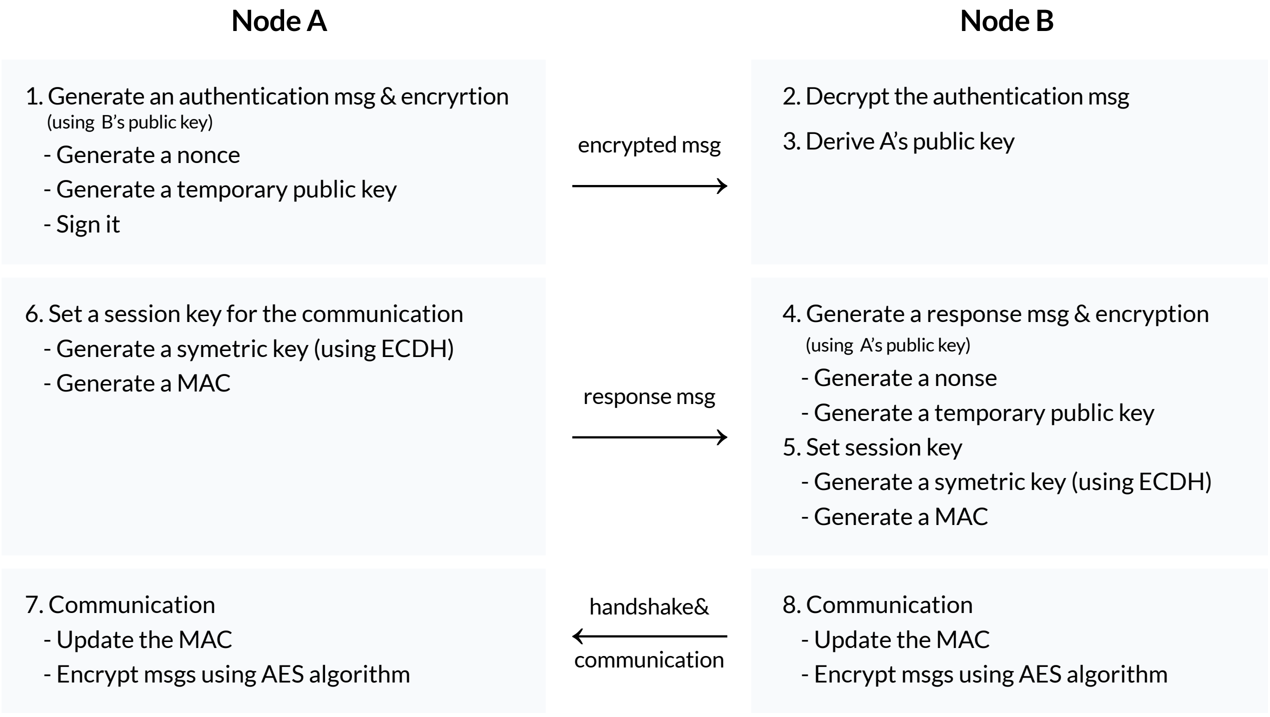


<Figure 5-1> **DEVP2P STACK**

The part we deal with here is the encryption method of the communication section provided by the devp2p protocol. The Devp2p protocol uses an “Elliptic Curve Diffie Hellman (ECDH)” key exchange protocol in the process of handshaking for encryption of a communication section to generate a key used for data encryption. A brief description of (Figure 5-2) is as follows.

Node A attempting to connect the first session generates an authentication message (encrypts authentication data using the public key of node B, the recipient). The authentication message includes the shared secret data created using the node A dog ink and the node B public key, non-XOR operation data, a temporary public key, and the like. Receiving this, the node B decrypts its private key data and then extracts A's temporary public key. The node B generates a response message (encrypts the response message using the public key of the node A) for the received authentication data.

The answer message includes Node B's temporary public key and nonce. When the message exchange is complete, Node A and Node B use the ECDH algorithm based on each other's temporary key to generate new secret shared data, perform additional operations on that value, and extract the symmetric key become. The symmetric key generated in this way is used for encrypting data in the course of communication. Further, in the calculation of nonce and MAC secret data created by the nonce created by the other party, after generating a MAC (Message Authentication Code), it is added every time data is exchanged, and message authentication proceeds simultaneously.



Node A

Node B

1. Generate an authentication msg & encryrtion
(using B's public key)
- Generate a nonce
- Generate a temporary public key
- Sign it

encrypted msg

2. Decrypt the authentication msg
3. Derive A's public key

6. Set a session key for the communication
- Generate a symetric key (using ECDH)
- Generate a MAC

response msg

4. Generate a response msg & encryption
(using A's public key)
- Generate a nonse
- Generate a temporary public key
5. Set session key
- Generate a symetric key (using ECDH)
- Generate a MAC

7. Communication
- Update the MAC
- Encrypt msgs using AES algorithm

handshake&
communication

8. Communication
- Update the MAC
- Encrypt msgs using AES algorithm

<Figure 5-2> Secure channel

The AndUsChain also uses the devp2p protocol to enable secure communications encryption.

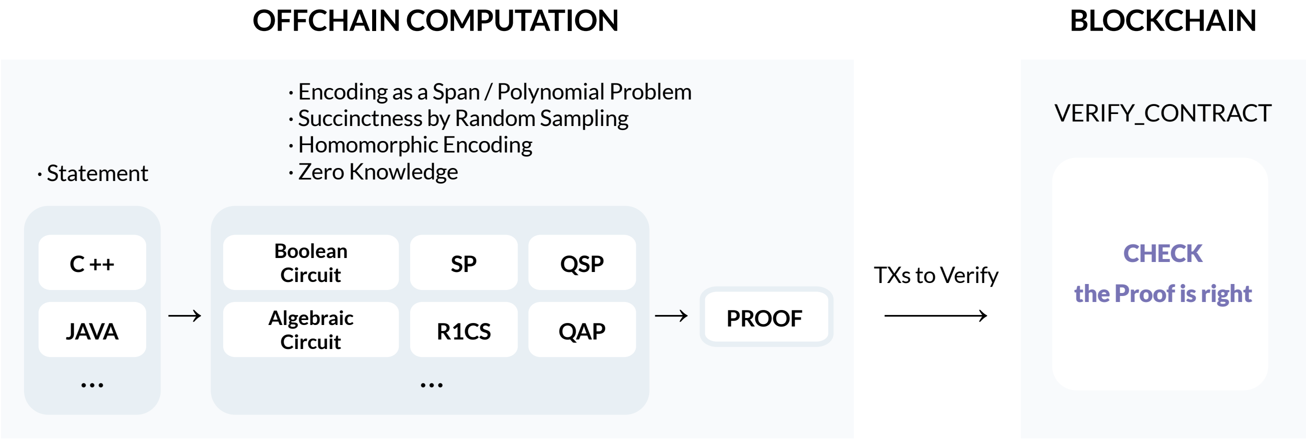
Protection of personal information (zero-knowledge proof)

The information recorded in the blockchain length is generally impossible to delete, and it is not desirable to store personal information in plain text to share everything. Ethereum provides a special contract for this property of the blockchain. This contract is provided pre-compiled to complement these characteristics and provide personal information protection functions within the blockchain network.

The personal information protection law used in Ethereum uses zk-SNARKs, a zero-knowledge proof method. It translates and saves specific information so that it can be proved instead of being saved directly to the director. Since it is challenging to extract the source data from the converted data (certification data) in practice, it is possible to ensure the confidentiality of specific information even if the proof data is entered in the director. (Of course, due to the possibility of development of new technologies and algorithms, we cannot guarantee that confidentiality is guaranteed at the same level in the distant future). The verifier uses the proof data generated in this way to the compiled contract provided by Ethereum.

However, the process of generating proof data is computationally intensive and has the potential to disclose personal information, so it is not performed on the blockchain. Only the procedure for verifying the generated data is performed in the blockchain. (Figure 5-3) explains these processes.

A simple explanation (Figure 5-3) is as follows. Disassemble/reassemble high-level language such as C and adequately express it in zk-SNARK. An expression (calculation/condition, etc.) expressed to be compatible with the prover zk-SNARK trying to prove that the expression is true can be referred to, but proof data is generated as data. Utilize public parameters provided by Ethereum when generating certification data. The proof data generated in this way is verified by sending the proof data to the verification contract (VERIFY_CONTRACT) (verification is also possible with OFFCHAIN). The verification contract is implemented using the compiled contract provided by Ethereum.

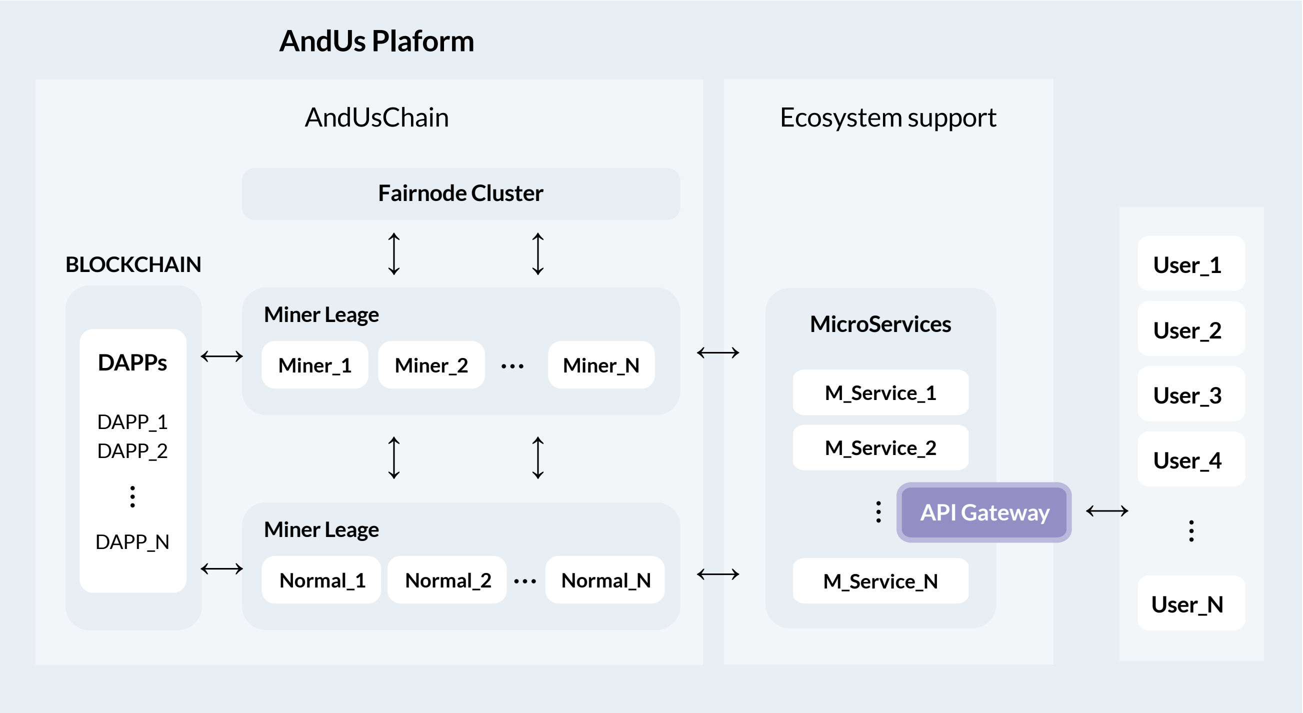


<Figure 5-3> zk-SNARK progression

AndUsChain also protects users' personal information in the manner described above.

6. Provide Key Functions to support AndUsChain Ecosystem

AndUsChain has established an ecosystem support layer to enable users to enjoy various aspects of service. We use the AndUsChain platform as a mixed form of the AndUsChain and the ecosystem support layer. In other words, users of the AndUsChain platform can receive services that are a fusion of several technologies, without receiving only the services made available by the blockchain.



<Figure 6-1> AndUsChain platform configuration

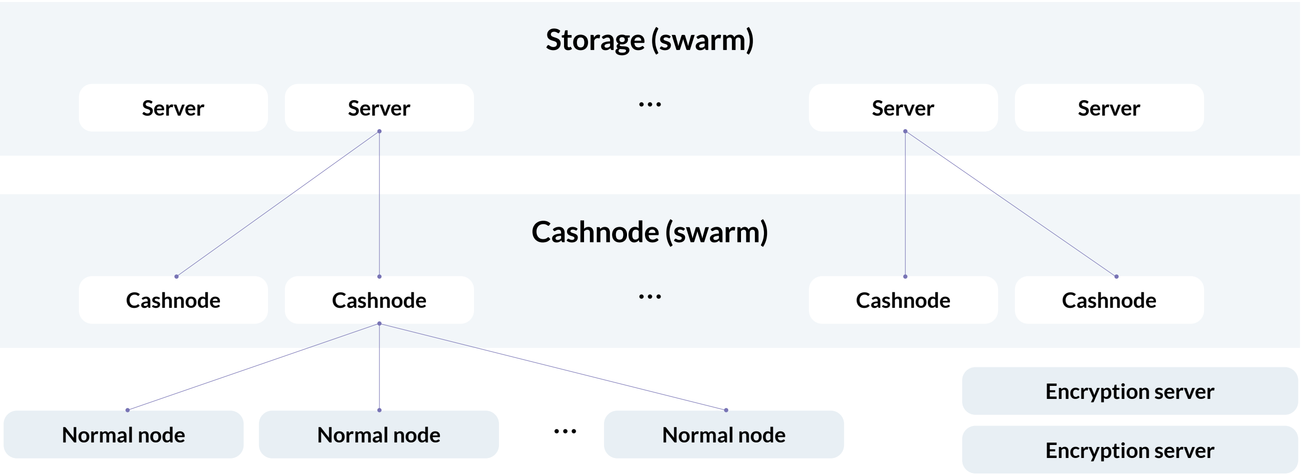
Of course, AndUsChain does not monopolize the role of the service provider. Any user who wishes can act as a service provider on the AndUsChain platform. Service providers can provide services primarily as DAPP and microservices. Also, one service provider can provide services with more enhanced functions by mixing Dapp and microservices provided by other service providers with services provided by itself. The service provider can obtain a profit by presenting a usage fee for the service provided by the service provider.

Here, we explain how to support the ecosystem with big data provided by AndUsChain.

6.1 Big data

Existing Ethereum proposes Swarm as a data store, and IPFS is gaining popularity for other distributed repositories. However, both storages have insufficient incentive provisions for storing and managing data. In addition to this, it is not enough to use it as actual service in various fields such as sharing maintenance, stability, security, deletion, and method. Therefore, we, AndUsChain body, wants to propose a new storage mechanism for data storage.

The proposed storage mechanism has a structure in which a storage and password-only server and a node search server that can efficiently search a working node are added based on the Ethereum Swarm. When another delete pool is managed with a hash is registered, it is decided that the hash is deleted, and the download is stopped. Only the user who uploaded the first data can register the hash in the deletion pool.



<Figure 6-2> Ecosystem support: the composition of big data services

Explanation of the composition of big data services

- A general node finds a cache node adjacent to itself through a node search server and uses the cache node to store and play data.
- The node search server is enabled and manages the cache node, and general nodes use the Kademlia algorithm at the time of the request to know the cache node closest to the requesting node.
- If a cache node can process a general node request directly, it should process it directly (if the re quested cache node manages the data)
- If a cache node cannot process a general node request directly, it requests the adjacent cache node and processes a general node request (when the requested cache node does not directly manage data).

- Storage group servers are responsible for data storage and manage data using the Swarm protocol between servers in the storage group.
- The encryption server is responsible for cancer and decryption of data when storing and querying data from general nodes.
- Deletion pool is configured in a Merkle tree format. Hash of deleted materials is recorded, and in the case of materials registered in the pool, the download is stopped, and when the stop is completed, the data saved by the garbage collector is automatically Deleted.

Storage structure

- Existing Swarm data structure

Field name	Description
Chunk	Consists of data up to 4KB size, save and query materials Is the basic unit for explaining 'chunk'
Reference	A value assigned exclusively to play a saved file. Swarm is stored in an encrypted file format, so it consists of 128 bytes including a 32-byte content address and a 32-byte decryption key. The system automatically generates the generated encryption/decryption key, and the decryption key is stored in the field.
Manifest	Manifest in the form of a URL as a data structure to represent the file store Used for searching matererials (composed of a hash to display the file name and actual location).

<Table 6-1> Existing Swarm data structure

- Create a "manifest" when saving the file, and generate a transaction that stores the hash that specifies the location in the block format.
- Transaction structure

Field name	Description
Receiver	store
ExData	Manifest hash is recorded

<Table 6-2> Swarm transaction structure

- For personal files, save the Manifest content so that you can decrypt the private key of the node where you want to save it.

- Data encryption based on the publication policy (public, personal, permission) of materials, independent of Swarm self-encryption, using a separate group of encryption servers, Perform decryption.
- When data is uploaded to the store, the data is broken down into "chunks," and each chunk can be accessed via a chunk hash.
- Configure a Merkle tree using Chunk hashes.
- Caches the distributed content when searching for cache nodes, Minimize connection time.
- The biggest difference with Swarm of Ethereum is that there is an encryption server group that is different from the data storage period. Data with low access frequency in the case of Ethereum is automatically deleted from Swarm. This service is maintained until the storage period expires, and another encryption server group is responsible for encrypting the material.

Cache node and storage server

- Basically, it uses Ethereum's Swarm protocol.
- Uploaded data is broken down into chunks at the cache node and distributed to other nodes in the same address space based on the chunk hash.
- The cache node is always connected to one or more storage servers, and the material disassembled into chunks is transmitted to the storage server in addition to being synchronized between the cache nodes in units of chunks.
- Unlike the cache node, the storage server maintains / stores data by storing all chunks and synchronizing the storage servers.
- Uploaded data is broken down into chunks at the cache node and distributed to other nodes in the same address space based on the chunk hash.

Data security

- General nodes can set public policies (public/permit/ private) when saving data. The general node includes a hash in the transaction so that the stored data can be queried and saves it in the blockchain so that the transaction's hash can be used to query the data.
- When specified for personal use, encrypt the data with the public key of the node that saved the data when saving it so that only the node that owns the private key can play it.

- For authorization, provide an API that can generate an arbitrary key on the encryption server, encrypt the data, and query its contents. The API, encrypted with a public key of the node in the chapter, is provided, and is stored in a block. The node can query the information by decrypting the secret key information and confirming the API information.

- For public use, save without having another encryption process.

Virtual network distance

- In a P2P environment, the physical distance between nodes cannot be measured, so the distance is measured assuming a virtual network. This service uses the Kademlia algorithm, which is one of the algorithms for measuring distances in this way.
- The calculation of the distance of the virtual network can be obtained by converting the value obtained by performing the bitwise XOR operation based on the node address into the big-endian.

√ Maximum distance (M): If the number of digits in the address is N, the maximum N
√ Distance between nodes (D): Log value of XOR of address values of both nodes ($log_2 D$)
√ Proximity: Maximum distance minus the distance between nodes (M-D)

Incentive (fee) rules

- When a user tries to use a big data service, a fee is paid in proportion to the size of the stored file. This fee is distributed to the cache nodes at a fixed rate, and the remainder is periodically distributed to the storage group servers.

- The period during which users use the service is set to basic one year, and the storage server group is responsible for storing during that period. If the period is basically exceeded, it can be renewed on a yearly basis, and an additional fee must be paid each time. The fee is also distributed to the storage server group.

- When a user saves data, the user can set a reference fee (existing/free) for other users accessing the data. If the inquiry fee is set to be paid, the fee paid for data inquiry is distributed to the cash node at a certain rate, and the remaining amount is distributed to the user who uploaded the material.

- The inquiry fee distributed to the cache node is paid to the cache node that responds to the request regardless of the data storage location.

6.2 Blockchain AI

Key technologies in the future are blockchain and artificial intelligence. In particular, blockchain and artificial intelligence are the most important technologies that will enable Korean Green New Deal policy to be successful. AndUsChain was developed to serve as a blockchain platform for the future world. Now, we are going to propose the vision and goal of blockchain convergence platform with artificial intelligence, another key technology in the future.

So far, many blockchain and artificial intelligence companies have put the utmost efforts to combine these two core technologies.

AndUsChain proposes " AndusChain artificial intelligence" that will reconstruct AndUsChain with artificial intelligence technology to achieve the goal of next generation blockchain platform.

In particular, our research has started from the end of 2019 for the convergence of blockchain and artificial intelligence. The blueprint of architecture was completed by the end of 2020 and we're planning to complete the technical development of "AndUsChain AI" by the end of 2021.

" Anduschain Artificial Intelligence" is an innovative method of building blockchain with artificial intelligence, not just integrating existing blockchain and artificial intelligence.

Looking at the current research trends of blockchain and artificial intelligence convergence, most of them have been studied in terms of blockchain for AI and AI for blockchain, which are complementary aspects to overcome technical limitations of blockchain and artificial intelligence.

With blockchain based data storage technology, artificial intelligence can enhance the improved quality, security of services and new AI business model development. In terms of AI technology usage for blockchain, this will support detection of hacking, minimizing the damage, expansion opportunity, operational efficiency and secure customized individual services.

However, complimentary application is NOT real convergence of these two technologies. When these two technologies become a sort of ONE synthetic body, that's the true meaning of convergence.

It's necessary to expand our way of thinking in order to make sure "Blockchain AI".

- *Phase 1: Conceptual Understanding Phase*
- *Stage 2: Structural Understanding Stage*
- *Stage 3: Completion stage*

The meaning of each step to implement blockchain artificial intelligence is as follows.

- *Phase 1: Conceptual Understanding Phase*

First, the conceptual understanding stage requires the accurate understanding on the blockchain concept. Blockchain experts understand blockchain from their respective point of view. Typically, most people (including experts) understand blockchain as a distributed ledger.

However, blockchain contains more concepts rather than only a distributed ledger. Actually, blockchain is a global computer as well as network. In other words, many different computers become the global computer connected by P2P network.

Based on this perception, the concept of "Blockchain AI" can be automatically determined. Having said that, many different AI will become "Global AI" connected by P2P network. In conclusion, "blockchain artificial intelligence" means that AI constructs its own blockchain platform by learning blockchain.

- *Stage 2: Structural Understanding Stage*

To understand the structural stage, it's necessary to understand basic architecture of blockchain.

There are 3 main architectures in blockchain. The basic architecture consists of accounts, transactions, and blockchain.

- **Account**
  An account is an entity that generates transactions. It is usually indicated by the address (owner) of the wallet.
- **Transaction**
  Transaction means the operation that an account creates. Works include cryptocurrency transactions, generation and execution of smart contracts
- **Blockchain**
  A block means a set of legitimate transactions, and a blockchain means that each block is connected by a certain rule

The blockchain platform is also configured on a P2P network basis.

- **P2P Network**

Based on this, the second stage of constructing blockchain artificial intelligence is as follows.

The first step is building up P2P network by each artificial intelligence that consists of blockchain platform. Network can be regarded as mutual communication network for the computers. So, artificial intelligence network means substitution computers as node with artificial intelligence.

If so, what innovation will happen from network point of view?

- ***Stage 3: Completion stage***

In the final stage of completion, it is a step to understand how blockchain platforms can be innovated through artificial intelligence.

- First of all, innovation from network perspective
- Innovation at the transaction stage
- Innovation from blockchain (consensus algorithm) perspective

In conclusion, "blockchain artificial intelligence" means that a "blockchain (artificial intelligence) platform evolves itself", which is fundamentally different from the existing method. In order to provide optimal platform services for each blockchain-based service (Dapp), it will have capability to change platform characteristics by itself. It also means that the "blockchain artificial intelligence" platform will continue to be a self-evolving platform that strengthens the various characteristics of the platform (decentralization, performance, scalability, etc.).

Perhaps in the near future, our lives and all services will be running on "blockchain artificial intelligence" platform and we'll take lots of benefits from these services.

7. Low-cost Ecosystem for New Ventures to create High-quality Jobs

The most important purpose of the AndUsChain is to provide the platform that enables to develop sustainable and decentralized P2P-based services. Therefore, it is a public platform that all current services are switched to blockchain based services, which is actually the objective of Ethereum. Thus, AndUsChain ecosystem includes all different industries and services. In conclusion, AndUsChain is the basic infrastructure for cultivating and accelerating blockchain related business.

Currently, in Korea, one of the most important agenda is the creation of high-quality jobs. In addition, reduction of the youth unemployment problem related to this is truly critical. The government, therefore, invests a lot of money to support new venture foundation ecosystems for job creation. However, the traditional new venture foundation ecosystem has failed given the fact that it didn't reflect to the Fourth Industrial Revolution related environment appropriately. Also, it was such a high-cost ecosystem. Actually, despite of great new business ideas, it has been really challenging for young people to implement actual business due to the difficulties on funding, pre-business valuation and so on. Obviously, traditional new venture foundation environment was NOT flexible and NOT relevant to create high quality jobs.

AndUsChain will transform this high-cost ecosystem to low-cost ecosystem to prepare for the fourth industrial revolution and for the future proactively. AndUsChain can reduce foundation as well as operation cost significantly.

By leveraging AndUsChain platform, many young people can proceed pre-valuation on their business through P2P-based business services. Even if they fail, significant cost reduction will enable them to be in much safer position for the recovery.

Despite of the advantages of blockchain ecosystems, there has been NO blockchain based ecosystem. Currently, many start-ups and large corporations are engaged in blockchain business, but most of them are limited to developing blockchain-based services.

The AndUsChain platform is an open platform that anyone can easily use at low cost.

Basic foundation ecosystem issues

- Foundation cost Issue: System development cost to realize own business ideas

* The average foundation cost related with IT industry is about KRW 300 million [8].

- Fund Raising Issue: Significant challenges due to no effective pre-evaluation

- High probability of failure: In case of failure, there's no safer system. Thus, it causes founder's significant burden such as endorsement during fund raising

Low-cost foundation ecosystem based on the AndUsChain platform

- Resolve the cost of foundation costs: Reduce system construction costs by utilizing blockchain platforms
- Resolve fund raising issue: Easier fund raising with open pre-evaluation
- Low failure probability: Innovative safer infrastructure with low-cost structure

The current blockchain-based open new venture foundation ecosystem model is Ethereum. Anyone can build up P2P business services on Ethereum platform, and more than 2,670 blockchain-based services are being operated and developed as of April 2019.

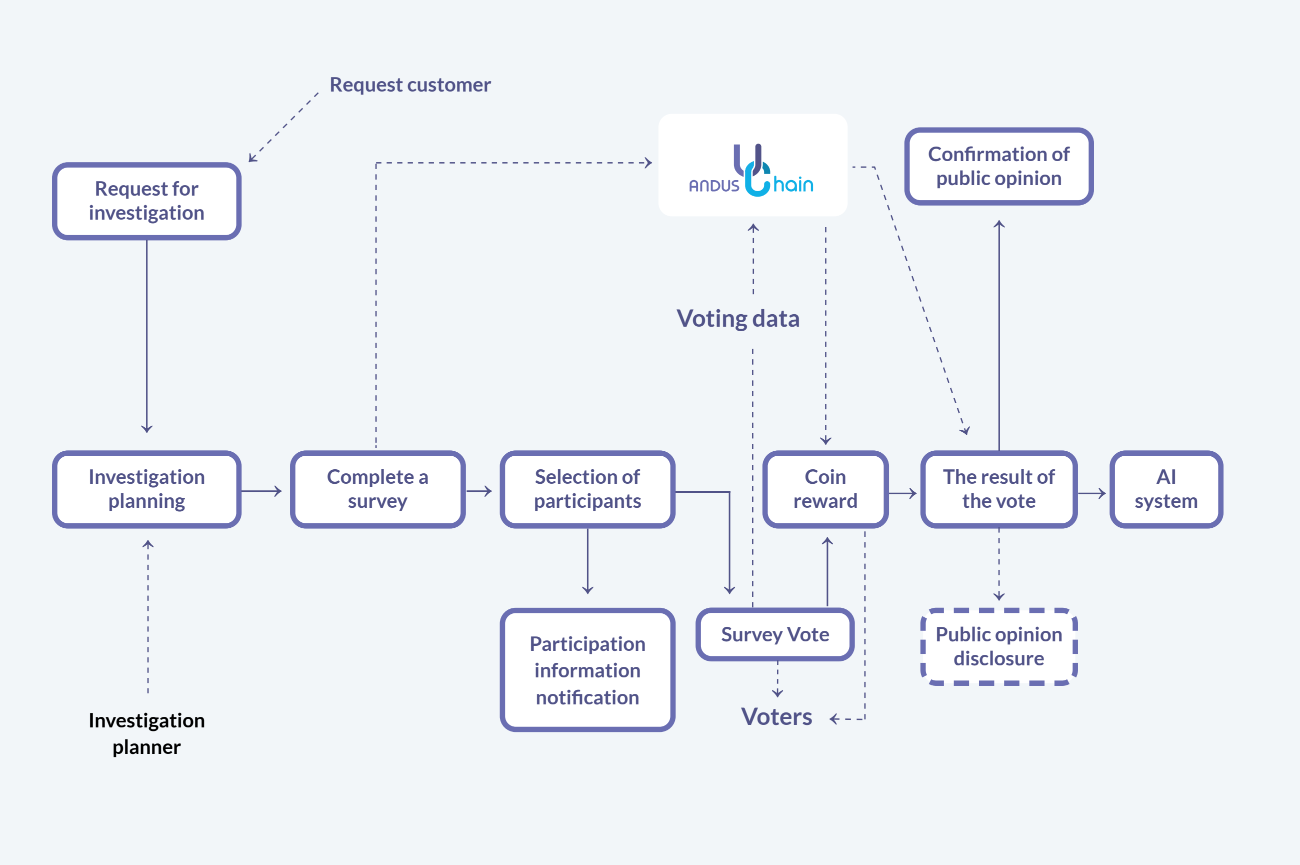
AndUsChain will play the critical role in providing a low-cost new venture foundation ecosystem to create high-quality jobs by maximizing user convenience which will exceed Ethereum based ecosystem.

8. Planned Projects

8.1 Public Opinion Poll

The process of public opinion poll can be built on the blockchain, and the reliability of the survey results can be improved innovatively. Blockchain based opinion poll system can be proceeded actively with relevant reward program for the participants. Our aim of public opinion poll project is open poll services that embedded above mentioned benefits.

Service configuration diagram for public opinion survey in (Figure 8-1)



<Figure 8-1> Service configuration diagram for public opinion survey

Main processes

- Survey request
  Register information such as survey purpose, survey group, survey period and consign survey execution an information collection

- Survey planning
  Anyone can enhance the authority of survey planning through relevant procedures, and proceed overall planning and actual survey and collect the final results.

- Create Survey Questionnaire
  Once survey questionnaires are registered, survey web page is automatically generated and recorded in blockchain simultaneously.

- Participant Group Selection
  Generate a participant list of unspecified majority or specific group depending on survey requirement.

- Participation Guidance Alarm
  Survey notice will be sent out to participants and encourage the participation.

- Questionnaire voting
  Participants can access the questionnaire directly via email, SMS and site login. The voting information for each question is recorded on the blockchain. Depending on the situation, an interview researcher can conduct a telephone survey.

- Voting results
  Aggregate voting data of participants, analyze the range of error and validate meaning, and derive the final result.

- Result inquiry and Disclosure
  Survey requester can inquire the result at any time. The result can be open to participants, third party, or other systems (AI, Big Data etc.) depending on situation.

- AI system
  Continuously accumulate voting results for similar survey questionnaire. AI systems infer and predict related public opinions indirectly.

- Incentive policy
  Provide coin compensation to questionnaire participants, interview investigators, participation recom mendations, and service evaluators.

Expected effect

- By applying the voting system to the blockchain, the risk of counterfeiting and alteration of votes is eliminated and credibility will be enhanced

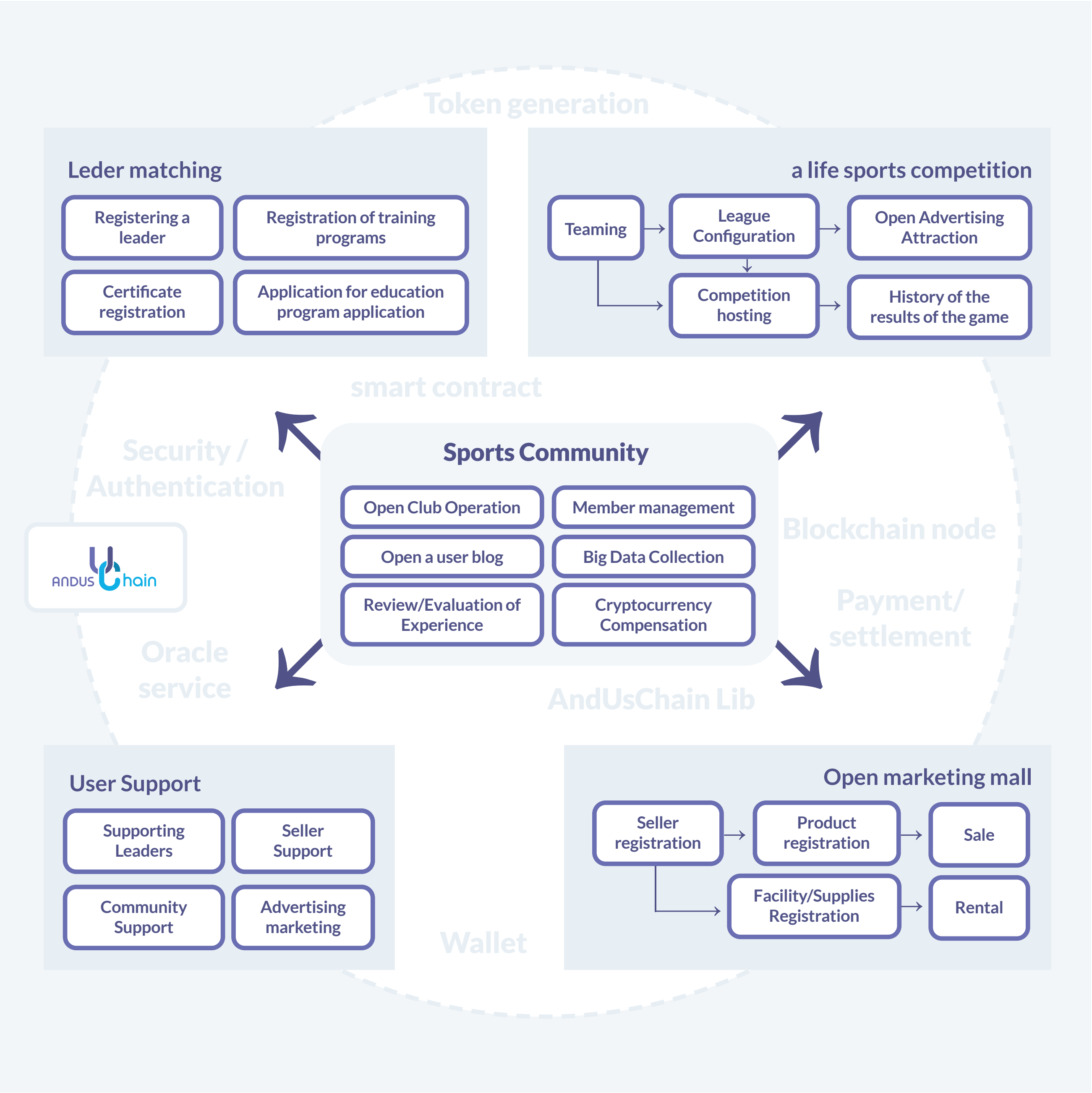
- By providing coin compensation for each participant (questionnaire participant, interview investigator, participation recommendation, etc.), open voting system will be vitalized actively.

- By preventing counterfeiting and alteration of votes, it will enhance credibility. Also, open system will enable everyone to request or participate in survey, which will lead activation of system. Finally, these benefits will contribute to various decision-making process with more credibility.

8.2 ATA Club

The ATA Club service aims to provide various blockchain based sports-related services. First of all, it will provide matching services, which will connect outstanding coaches and trainees for various sports clubs and blogs. This service will provide open market that will sell sports facilities and equipment. In addition, it'll provide team building and amateur sport tournament operation services as well.

The ATA Club service will be set up on the blockchain to ensure reliability and fairness and drive the expansion of the daily sports market.



<Figure 8-2> ATA Club service composition (life sports-related services)

Planned Projects

Main processes

- Open Sport Club Operation

  Any member of an open group can create a group and invite new members. In addition, users can utilize the program that support sport club activities conveniently.

- Opening a blog

  All members can open and manage their own blogs. They can submit various opinions to the blog based on predetermined conditions, and share many opinions with multiple members.

- Experience Sharing & Evaluation

  Various experience on education program, shopping, sport clubs can be shared and multichannel evaluation system will support effective evaluation process for service improvement.

- Incentive policy

  Cryptocurrency will be rewarded to all members as the return of activity and participation.

- Membership management

  Instructors, students, and team members can register various participants such as group members and general members, perform authentication, and grant authority for each role.

- Big data collection

  Various Service experiences and data derived from services itself (Game results, evaluation, etc.) are aggregated and analyzed for better services.

- Instructor registration

  Anyone that has sport expertise can register as an instructor and provide educational program and share them with others.

- Instructor registration

  Users with registered teaching authority for education programs can inform students about education programs and recruit students.

- Education program application

  Applicants for educational programs can review the profile of the instructors when applying for the program. Apart from this, specific instructor's programs can be recommended to the applicants depending on required condition and pre-educational requirements.

- Team organization
  Teams can be organized (inviting team members and applying for team members) according to the sporting event's team composition. Once the teams are organized, authorization on tournament participation and individual team activities is provided.

- League organization
  Teams can organize the tournament or league. Teams can take advantage of additional services (organizing competition schedule etc.) and enjoy the league conveniently.

- Public Advertisement
  Once league or tournament is organized, event home page is automatically set up. Online commercials can be uploaded on the website, which will create cryptocurrency compensation.

- Tournament
  Facility and equipment can be rented depending on competition schedule. Referee, event related progress and game result can be registered.

- Game result history

- The results of each game, opinions, and singularities that are derived from each game are recorded on the blockchain and can be shared among the team members. It can be benchmarked for the next game and tournament.

- Sales member registration
  When a member is registered for sales, the authority to open his/her own shopping mall page is granted.

- Product registration
  Members registered as seller can upload product information on shopping mall.

- Facility/equipment registration
  Information on sports facilities and rental equipment can be uploaded

- Sales / rental
  Sellers can generate revenue through sales of sports goods, facility reservations, equipment rentals, and so on.

- Instructor support
  General instructors and premium instructors can get services that support instructor's activities such as educational program management, educational application reception, storage, checkout, late experience, bulletin boards, and public relations.

- Seller support
  Sellers can get the services that support store PR, product display, management, order taking, facility reservation, Payment and reconciliation process, which is essential activities for the sales.

- Community support
  Blog management or community management service that supports group management and activities.

- Marketing
  Service modules required for educational program, products, facilities, banner, advertisement application, ad contents registration and so on.

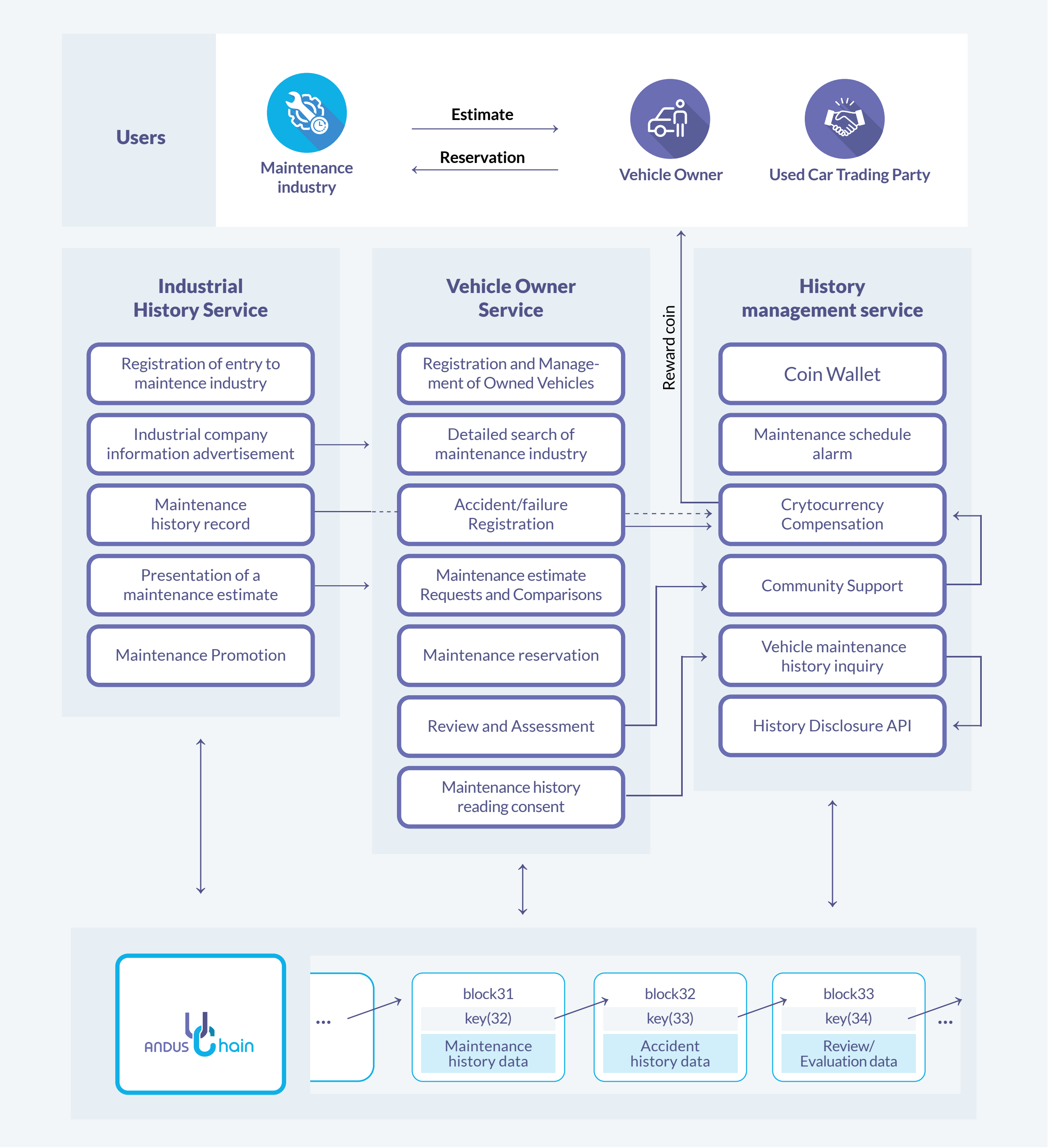
Expected effect

- Blockchain based various sport services will guarantee the operational transparency.

- Will enhance better customer experiences with the analysis on accumulated ideas, evaluation, and various data.

8.3 Used car trading

In order to ensure the credibility of used car trading, used car trading services with automobile history tracking system are being developed.


Users
Maintenance industry
Estimate
Reservation
Vehicle Owner
Used Car Trading Party
Industrial History Service
Registration of entry to maintence industry
Industrial company information advertisement
Maintenance history record
Presentation of a maintenance estimate
Maintenance Promotion
Vehicle Owner Service
Registration and Management of Owned Vehicles
Detailed search of maintenance industry
Accident/failure Registration
Maintenance estimate Requests and Comparisons
Maintenance reservation
Review and Assessment
Maintenance history reading consent
Reward coin
History management service
Coin Wallet
Maintenance schedule alarm
Crytocurrency Compensation
Community Support
Vehicle maintenance history inquiry
History Disclosure API
ANDUS Chain
...
block31
key(32)
Maintenance history data
block32
key(33)
Accident history data
block33
key(34)
Review/ Evaluation data
...

<Figure 8-3> Structure of used car trading service

* Details will be released in white paper version 1.0

8.4 Key milestones of AndUsChain ecosystem

AndUsChain based Dapp services are as follows;

- ***BSEEBOX(http://www.bseebox.io/)***

- Real-time video service (Live Commerce) blockchain-based offline and online convergence store platform

- ***Eirlab(https://www.eirchain.io/)***

- Blockchain-based beauty business

- ***DesignCell(http://www.designedcells.com/)***

- Blockchain-based stem cell ecosystem development project

- ***FinMart(http://www.finmart.co.kr/)***

- A project to establish a blockchain-based financial transaction platform between individuals

- ***FirstVentures(https://www.firstventures.ac/)***

- Blockchain-based startup investment attraction platform

- ***PowerCall***

- Blockchain-based overseas ecosystem development project

- ***Korea Small and Medium Business Development Association(http://www.ceo-maxvalue.org/)***

- Business agreement for the revitalization of the Anders chain ecosystem

9. Cryptocurrency: DAON

AndUsChain has issued crypto-currency “Daon (Unit DEB)” for platform operation.

- Total number of cryptocurrency issued: 1 billion DEB
- Cryptocurrency distribution policy (planned)

Category	Ratio(%)	Where to spend
Founder	5	incentives
Developer and Advisor	5	incentives
sales	30	√ AndUsChain platform operation √ AndUsChain ecosystem support function enhancement cost √ Deliver distributed protocols and development tools to the world
Ecosystem support	20	√ Education center management √ AndUsChain-based next-generation distributed application support to be able to develop (dapps) √ Founding expenses support etc.
Marketing	10	√ Public relations and marketing
reserve	30	
TOTAL	100	

<Figure 9-1> Crypto-currency distribution policy (planned)

Planned Projects

10. Roadmap

AndUsChain's technical development and ecosystem roadmap is as follows.

Timeline	Key Milestones
April 2019	white paper (version 0.7)
April 5, 2019	Test Net release
April 2020	White Paper (Version 0.7): Convergence of Big data
December 2020	Artificial Intelligence Convergence(Version 0.9)
May 1 2021	Main Net release
October 2021	√ Securing 5 ecosystems (self) √ Securing 10 ecosystems (joint)
December 2021	√ white paper (version 1.0) √ Blockchain AI
December 2022	√ Securing 10 ecosystems (self) √ Securing 30 ecosystems (external) √ Dapp ecosystem activation support

<Table 10-1> AndUsChain roadmap

11. Conclusion

AndUsChain is the infrastructure for the future blockchain world. AndUsChain will play the critical roles in accelerating blockchain economy and ecosystem. In particular, AndUsChain will focus on building up low-cost new venture foundation ecosystem which will actively drive high quality jobs in the marketplaces.

However, the final destination of the AndUsChain is to build up the next-generation Ethereum, which will surpass Ethereum that has enhanced lots of ecosystems. To make the long story short, AndUsChain is fair and fast next-generation Ethereum (A fair & fast & secure next Ethereum). AndUsChain team will actively contribute to lead our country to be world's most advanced blockchain country.

Moreover, AndUsChain team will prove that cryptocurrency as well as blockchain ecosystem can improve our daily life with actual performance.

In particular, AndUsChain team has been the World's first team to define the concept of "Blockchain Artificial Intelligence" and will complete self-evolving blockchain platform with utmost efforts of planning and development. AndUsChain team strongly believes that Blockchain Artificial Intelligence will play the tremendous roles in build up the world where everyone can be successful and win-win.

- **Reference Materials**

[1] Ethereum official website, https://ethereum.org/

[2] Ethereum White Paper, A Next-Generation Smart Contract and Decentralized Application Platform, 2018.08.

[3] Ethereum Huang, ETHEREUM: A SECURE DECENTRALISED GENERALISED TRANSACTION LEDGER BYZANTIUM VERSION e94ebda, 2018.06.

[4] Bitcoin white paper, Bitcoin: A Peer-to-Peer Electronic Cash System, 2008.

[5] V. Buterin, On Settlement Finality, https://blog.ethereum.org/2016/05/09/on-settlement-finality, 2016.09.

[6] V. Buterin, On Slow and Fast Block Times, https://blog.ethereum.org/2015/09/14/on-slow-and-fast-block-times, 2015.09.

[7] C. Decker, R. Wattenhofer, Information Propagation in the Bitcoin Network, In IEEE International Conference on Peer-to-peer Computing, 2013.

[8] Small and Medium Enterprise Agency, Founding Agency, 2016 Survey of companies founded in 2016.

History of changes

2020.07.31. - White Paper Version 0.71

- Cause of change: Mining participation transactions are not included in the block due to the lower priority of including blocks compared to regular transactions because there is no fee.
- Solution: Prioritize the processing of mining participation transactions as a priority
- Changed location: Block structure

2020.04.30 - White Paper Version 0.75.

- Cause of change: Speed improvement (over 1,000 TPS)
- Solution: Changes in the composition of mining leagues and suggestions for improving speed performance (more than 20,000 TPS when applying shading technology)
- Changed location: 4.6 Performance

2020.07.31. - White Paper Version 0.8

- Causes of change: Cryptocurrency issuance, distribution policy, and business promotion schedule adjustment

2020.09.07. - White Paper Version 0.81

- Cause of change: Add advisor

2020.12.05. - White Paper Version 0.9

- Cause of change 1. Change in cryptocurrency issuance and distribution policy
- Causes of change 2. Adding an ecosystem of end-like chains and adding “blockchain artificial intelligence” parts

2020.12.10. - White Paper Version 0.91

- Causes of change: Change of cryptocurrency issuance and distribution policy

2021.07.30. - White Paper Version 0.95.

- Cause of change 1. Added concept of “blockchain artificial intelligence”
- Cause of change 2. Adding token ecosystem status

AndUsChain Whitepaper

Fair & high-speed public blockchain:

Version 0.95 August 2021