Anduschain Whitepaper

Version 1.0

August 2024

The Era of the Blockchain Revolution (The Birth of a P2P World)

- Bitcoin demonstrated to us that a P2P world is possible through the concept of Distributed Ledger
- Ethereum opened up the P2P world for us through Blockchain technology.
- The philosophy and ideology of the Blockchain revolution are fundamentally about a decentralized world
- However, both Bitcoin and Ethereum reveal limitations in achieving a sustainable decentralized world due to the characteristics of their underlying consensus algorithms (PoW, PoS)

A new consensus algorithm is needed to maintain sustainable decentralized characteristics

2. Analysis of Sustainable Decentralized Characteristic

Proof of Work

- Consensus algorithm relying on the computing power held by miners
- Centralization of mining
- Unnecessary resource waste due to computing power competition

Proof of Stake

- Consensus algorithm relying on the amount of cryptocurrency stake held by miners
- Centralization of mining and the emergence of the rich-get-richer phenomenon

Delegated Proof of Stake

- Debate arises on whether it is truly a public blockchain
- Loss of mining opportunities and concentration of power in the hands of a few due to stake delegation

Establishing a blockchain with sustainable decentralization characteristics within the concept of fairness

Concept of fairness

- Anyone can mine, and the probability of a miner successfully mining is the same, regardless of the miner's conditions (computing power, stake, etc.)
- Mining probability of the miner

$$\text{Mining probability of the miner} \fallingdotseq \frac{1}{\textit{Total number of nodes}}$$

The world's only fair public permissionless blockchain satisfying fairness

Comparison of fairness

- Equity of mining probability regardless of the conditions of mining nodes
- First proposal and implementation of the concept of mining fairness
- In the DEB consensus algorithm, nodes have a higher probability of mining compared to other methods

✓Mining probability of nodes in Proof of Work (PoW) systems

$$\textbf{Mining probability of the miner} \fallingdotseq \frac{\textbf{Computing power held by a node}}{\textbf{Total computing power}}$$

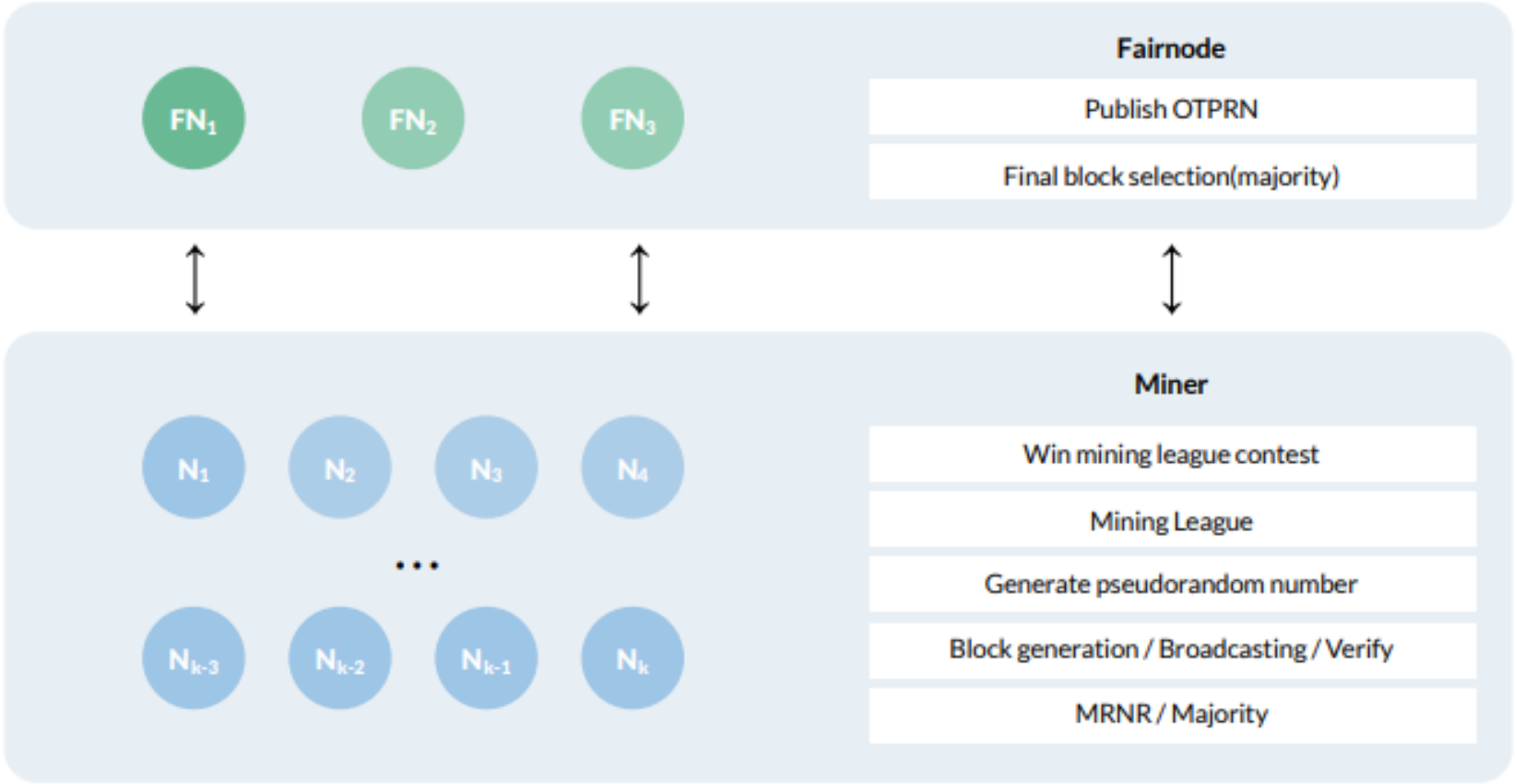
✓ Mining probability of nodes in Proof of Stake (PoS) systems

$$\textbf{Mining probability of the miner} \fallingdotseq \frac{\textbf{Amount of cryptocurrency held by a node}}{\textbf{Total cryptocurrency supply}}$$

✓ Mining probability of nodes in the DEB consensus algorithm

$$\textbf{Mining probability of the miner} \fallingdotseq \frac{1}{\textbf{Total number of nodes}}$$

4. deb Consensus Algorithm (Overall Architecture Diagram)



4. deb Consensus Algorithm (Three-Stage Process)

① Formation of the Mining League | ② Block Generation | ③ DEB Consensus Algorithm

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

4. deb Consensus Algorithm (Three-Stage Process)

① Formation of the Mining League | **② Block Generation** | ③ DEB Consensus Algorithm

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

   difficulty={0≤n≤JoinNonce | 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

4. deb Consensus Algorithm (Three-Stage Process)

① Formation of the Mining League | ② Block Generation | ③ DEB 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

① Formation of the Mining League | ② Block Generation | ③ DEB Consensus Algorithm

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

4. deb Consensus Algorithm (Step-by-Step Detailed Process)

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 ÷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

4. deb Consensus Algorithm (Step-by-Step Detailed Process)

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. deb Consensus Algorithm (Step-by-Step Detailed Process)

① Formation of the Mining League | **② Block Generation** | ③ DEB Consensus Algorithm

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.

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

* ***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.

$$difficulty = MAX(0\le n\le \textbf{\textit{JoinNonce}}\{\textbf{\textit{difficulty}}_n\})$$

4. deb Consensus Algorithm (Step-by-Step Detailed Process)

Block creation and broadcasting

1. The mining node generates random numbers by referencing their block headers OTPRN.rand, Join-Nonce 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

4. deb Consensus Algorithm (Step-by-Step Detailed Process)

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. deb Consensus Algorithm (Step-by-Step Detailed Process)

① Formation of the Mining League | ② Block Generation | ③ DEB Consensus Algorithm

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.

4. deb Consensus Algorithm (Step-by-Step Detailed Process)

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 : $Tx.Join_{Nonce} = Tx.Join_{Nonce} + 1$

“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 de-centralization 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:

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

The Andus Chain is fundamentally based on Ethereum, embodying the philosophy and principles of blockchain (Ethereum Equivalence). The architecture of Andus Chain is largely similar to that of Ethereum, with most components mirroring Ethereum's architecture. However, to maintain sustainable decentralization, the consensus algorithm has been enhanced.

The changes made to apply the DEB agreement algorithm are summarized as next 2 pages

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

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*

Performance comparison of major public blockchains

	Bitcoin	Ethereum	AndUsChain
Consensus Algorithm	PoW	PoS	deb
TPS	7	12~15	500 over
Finality	10min	About 3min	13sec~15sec

Beyond Ethereum : A Fair fast secure Ethereum!!!

Technical Strength 1: A Public Permissionless Blockchain that Maintains Sustainable Decentralization and Fairness

Technical Strength 2: The World's First Public Permissionless Blockchain with Fork-Free Single Block Finality

Technical Strength 3: The World's Highest Speed Among Public Permissionless Blockchains

Technical Strength 4: Maintaining the Lowest Transaction Fees in the World

7. Coin Issuance and Distribution Policy

Coin Issuance

- 1 Billion

Coin Distribution Policy

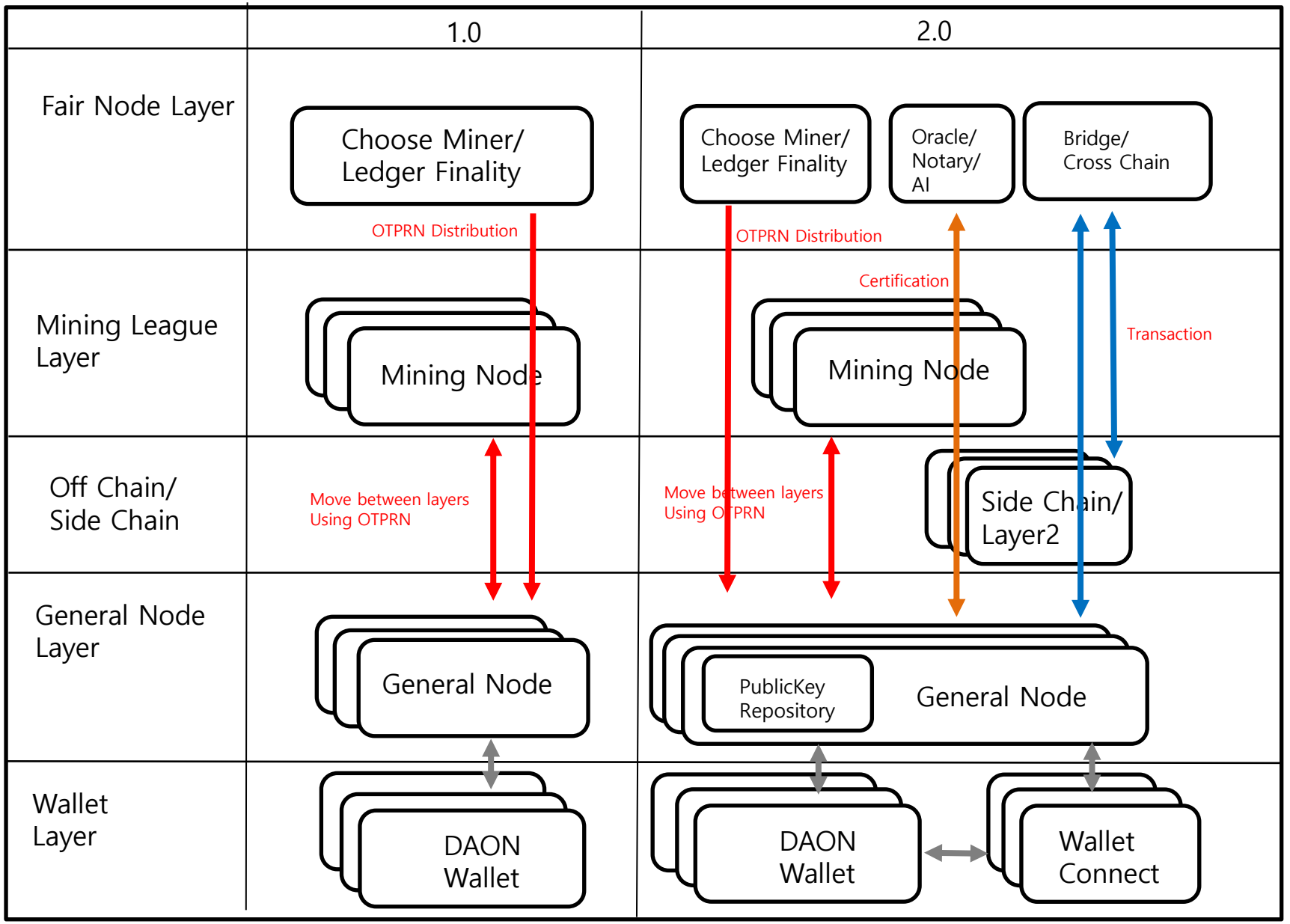
- Pubic Sale : 30%
- Team & Advisior : 5%
- Partner : 5%
- Development : 10%
- Marketing & Promotion : 20%
- Ecosystem : 30%

7. Coin Issuance and Distribution Policy

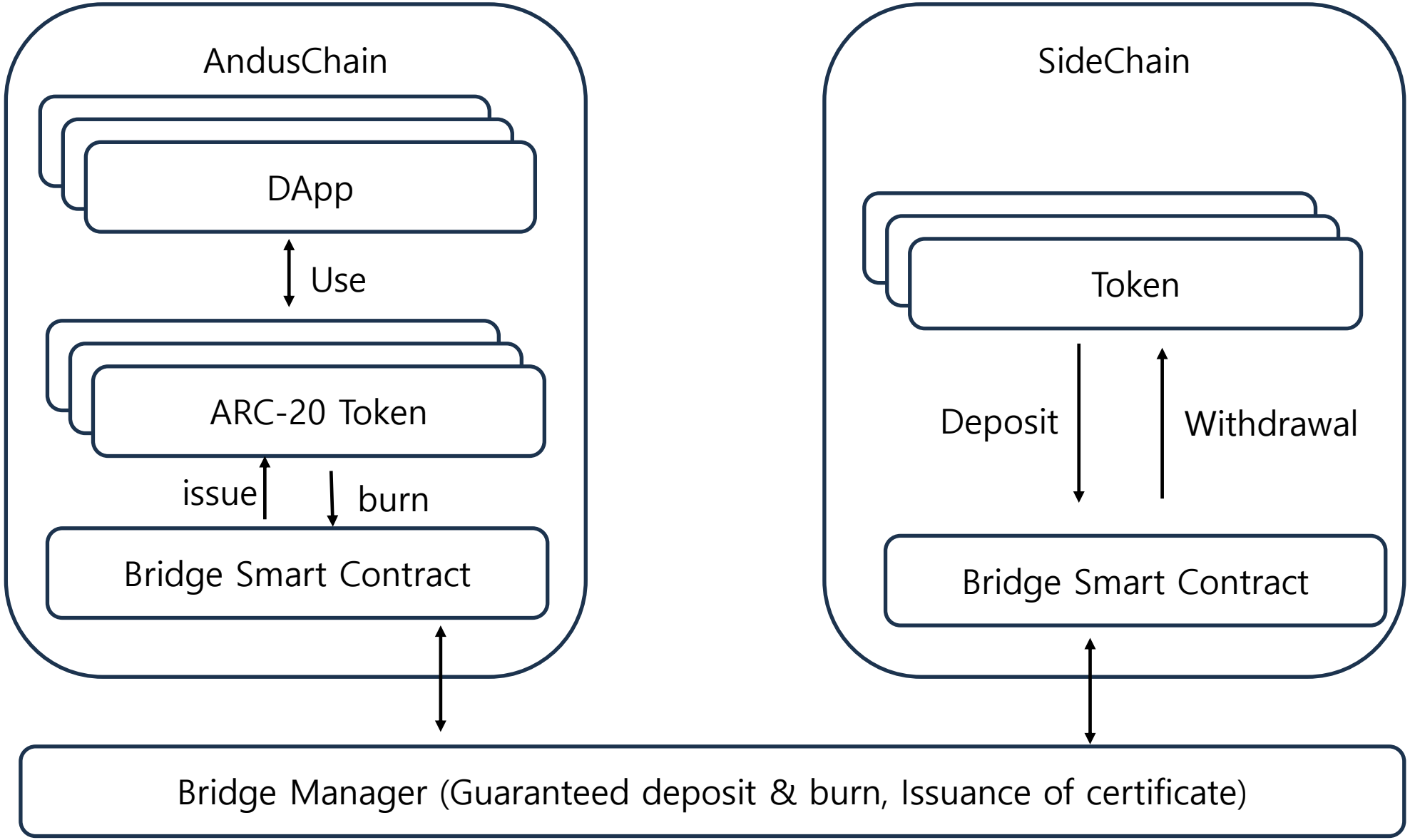
Vesting Plan

Date	Ecosystem	Marketing	Develop.	Team	Advisor	Public Sale
Token Allocation	30.00%	20.00%	10.00%	5.00%	5.00%	30.00%
Token Amount	300,000,000	200,000,000	100,000,000	50,000,000	50,000,000	300,000,000
Before August 2024				50,000,000	50,000,000	300,000,000
Aug-24	50,000,000	20,000,000	30,000,000			
Sep-24	9,000,000	4,000,000	3,000,000			
Oct-24	9,000,000	4,000,000	3,000,000			
Nov-24	9,000,000	4,000,000	3,000,000			
Dec-24	9,000,000	4,000,000	3,000,000			
Jan-25	9,000,000	4,000,000	3,000,000			
Feb-25	9,000,000	4,000,000	3,000,000			
Mar-25	9,000,000	4,000,000	3,000,000			
Apr-25	9,000,000	4,000,000	3,000,000			
May-25	9,000,000	4,000,000	3,000,000			
Jun-25	9,000,000	4,000,000	3,000,000			
Jul-25	9,000,000	4,000,000	3,000,000			
Aug-25	9,000,000	4,000,000	3,000,000			
Sep-25	9,000,000	4,000,000	3,000,000			
Oct-25	9,000,000	4,000,000	3,000,000			
Nov-25	9,000,000	4,000,000	3,000,000			
Dec-25	9,000,000	4,000,000	3,000,000			
Jan-26	9,000,000	4,000,000	3,000,000			
Feb-26	9,000,000	4,000,000	3,000,000			
Mar-26	9,000,000	4,000,000	3,000,000			
Apr-26	9,000,000	4,000,000	3,000,000			
May-26	9,000,000	4,000,000	3,000,000			
Jun-26	9,000,000	4,000,000	3,000,000			
Jul-26	9,000,000	4,000,000	3,000,000			
Aug-26	9,000,000	4,000,000	1,000,000			
Sep-26	9,000,000	4,000,000				
Oct-26	9,000,000	4,000,000				
Nov-26	9,000,000	4,000,000				
Dec-26	7,000,000	4,000,000				
Jan-27		4,000,000				
Feb-27		4,000,000				
Mar-27		4,000,000				
Apr-27		4,000,000				
May-27		4,000,000				
Jun-27		4,000,000				
Jul-27		4,000,000				
Aug-27		4,000,000				
Sep-27		4,000,000				
Oct-27		4,000,000				
Nov-27		4,000,000				
Dec-27		4,000,000				
Jan-28		4,000,000				
Feb-28		4,000,000				
Mar-28		4,000,000				
Apr-28		4,000,000				
May-28		4,000,000				
Total tokens	300,000,000	200,000,000	100,000,000	50,000,000	50,000,000	300,000,000

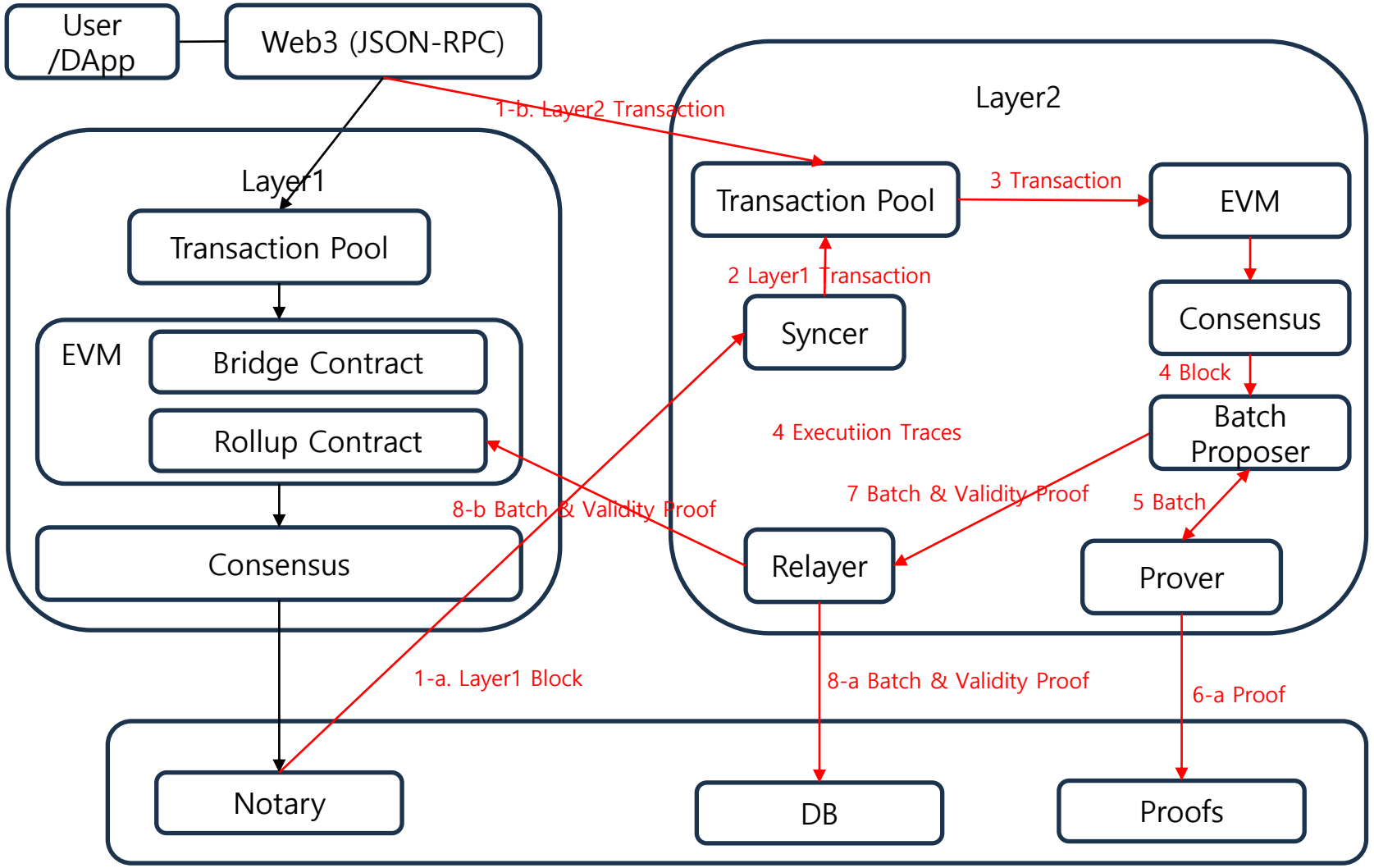
8. AndusChain 2.0



9. Bridge Service



10. Layer2 Architecture



11. Raodmap

May 2021

Launch of AndusChain Mainnet Commercial Service

September 2022

First Hard Fork Implementation

- Added precompiled contracts related to zero-knowledge proofs and EVM (Ethereum Virtual Machine) OP codes
- Improved AVM (AndusChain Virtual Machine) in accordance with changes in Ethereum EVM
- Added PoA (Proof of Authority) consensus algorithm and completed enterprise-grade AndusChain
- Enhanced security of DEB consensus algorithm and updated external libraries due to Go language upgrades

November 2023

Advancement of AndusChain Layer 2 Project (Addressing Privacy & Scalability Issues)

- Progressing with the Andus Chain Layer 2 project to solve privacy and scalability challenges
- Andus Chain ZK Rollup Project

First Half of 2024

Layer 2 Launch (Andus Chain ZK Rollup)

Second Half of 2025

Development of 'A Global Trust AI' (Concept of Integrating Blockchain and Artificial Intelligence)

12. Introduction of CEO Park, Sung Jun

Current CEO of Andus Co., Ltd. (AndusChain)

Current CEO of Davious Co., Ltd. (Real Estate NFT)

Current Director of the Blockchain Research Center at Dongguk University's Graduate School of International Information Security

Current Professor in Cryptography and Blockchain at Dongguk University's Graduate School of International Information Security

Former CEO of BC Secure Co., Ltd.

Former Team Leader of the Basic Technology Team at the Korea Internet & Security Agency (KISA)

Former Senior Researcher at the National Security Research Institute (NSRI)

12. Introduction of CEO Park, Sung Jun

Current National Standard Expert Committee Member for Blockchain at TTA (Telecommunications Technology Association)

Current Director at the Korea Blockchain Association and Federation

Former Member of the Ministry of Education's Intelligentization Promotion Committee (Chairman of the Private Sector Members)

Former Blockchain Advisor for Incheon City and Jeju Province

Former Chair of the Information Security Research Committee at the Korean Blockchain Society, under the Ministry of Science and ICT

Former Expert Advisory Panel Member for Blockchain Future Tasks at the National Security Research Institute (NSRI)

Former Blockchain Advisor for Seoul City

Former Technology Development/Information Security Subcommittee Chair at the Blockchain Open Forum, under the Ministry of Future Creation and Science

Former Expert Committee Member for the Intelligent Government Mid-term Plan at the Ministry of the Interior and Safety (Blockchain)

Former Advisory Committee Member for Blockchain Services in the "Softpower Korea 2015" Internet Services Division

Former Practical Committee Member for the Blockchain National Roadmap, Ministry of Future Creation and Science, 2016

Former Research Consultant for the Law on Small-Scale Transactions Based on Blockchain, Ministry of Strategy and Finance, 2016 (Korea Financial Research Institute)

Former Project Leader for the G4C Online Document Issuance

Former Technical Director for the Digital Signature Act (KISA)

Former Lead Developer of the SEED Cryptographic Algorithm for National and International Standards (KISA)

Author (Co-author): Coin Wars (Transformation of Wealth), May 28, 2021

Editor: Job? I Will Become a Blockchain Expert!, August 28, 2020

Editor: Don Tapscott/Alex Tapscott, Blockchain Revolution, January 20, 2017

Speaker: Over 950 lectures including the EBS Classⓔ on Cryptocurrency and Blockchain (October 2016 - Present)