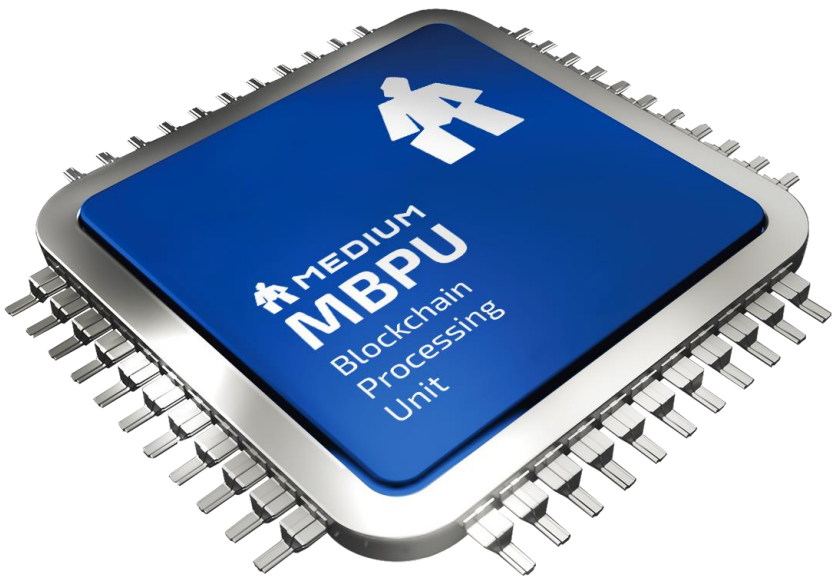
MEDIUM

MEDIUM

4th GENERATION BLOCKCHAIN

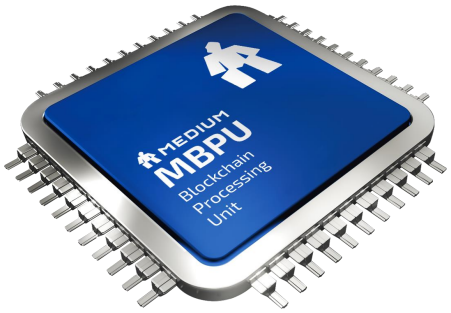
H/W BLOCKCHAIN PLATFORM & MBPU TECHNOLOGY

POSITION PAPER | VERSION 1.0



Contents

Abstract



4th GENERATION BLOCKCHAIN

H/W BLOCKCHAIN PLATFORM & MBPU

TECHNOLOGY

Bitcoin, that was first introduced through the paper of Satoshi Nakamoto in 2008, received worldwide attention with the expectation for being decentralized "alternative for legal tender" with no central bank. The requirement for such decentralization is a core technology called "blockchain," and blockchain is regarded as a technology for both economic values of bitcoin and leader for the 4th industry. Hence, there is a global trend in which various countries and companies worldwide attempting to synthesize traditional business and blockchain.

However, realistically current blockchain technology does not successfully satisfy TPS (Transaction per Second) required by enterprise system, with lower data transaction speed compared to traditional network service. Hence, current blockchain technology has achieved little compared to high social expectations and demands.

To overcome the limits of performance of blockchain, we aim to not go through the traditional method of striving for increase in performance through improvements of software architecture and algorithm undertaken by many researches on blockchain, but design unique H/W solely for blockchain and develop our own MBPU(Medium Blockchain Processing Unit) that performs core functions for commercialization level of blockchain platform designed for enterprise. Services operated on MEDIUM blockchain platform realized by such approach are guaranteed hundred thousands of transaction per second. As of July 2019, when this document is distributed, we realized 100,000 TPS through independent development, and the number is increasing consistently.

MEDIUM guarantees Hyperledger fabric, the De Facto Standard of traditional enterprise market, and interoperability for establishing blockchain platform for commercial-level enterprise service. Through this, it aims to guarantee stability and convenience for developers around the world developing various blockchain services by allowing easy access to global enterprise market and providing verified software specifications of Hyperledger and various libraries.

Furthermore, the limited number of MEDIUM coins issued can be used as fee for using platform that can arise from using MEDIUM blockchain platform by various services and solutions in the future. Also, MEDIUM coin will be used in general MEDIUM token economics such as consumption with in MEDIUM blockchain network, reward for registering on marketplace, and transactions of solutions.

We are sure that we can achieve new innovations and visible results by using fundamentally different approach from other blockchain researches focusing on improving performance such as Bitcoin, Ethereum, and EOS. Through this, we hope to realize successes of blockchain service model based on enterprise that was impossible in the past.

01 Introductions

1) The emergence of blockchain and possibility for utilizing it for enterprise

After the release of Bitcoin in 2008, various countries and companies worldwide are attempting to apply blockchain, the core technology of Bitcoin, to various areas of industry. Global ICT industry, which saw the possibilities of currency transaction with no central system, became excited about the technological and industrial values of "decentralization," and attempt to utilize blockchain technology in every method that saves and transfers data. If decentralization occurs in an information system environment with enhanced availability and confidentiality, and integrity for distributed data can be guaranteed, blockchain technology will become the necessary technology in every industrial area in the 4th industrial revolution.

IT environment of most companies is divided according to various criteria. Systems are often separately established among affiliates, headquarters, and departments of the same company. Adding security procedures creates various processes in transferring data between department, and a credible third party is required to exchange data internally and externally. Through this example, it can be confirmed that systems for companies and finance have similar structure in relation to data exchange, and that "decentralization" for company system in data transfer is possible similar to decentralization in financial system with the emergence of Bitcoin.

When data is encrypted and saved in distribution for individuals wishing to exchange data, and when who took data for what purpose and where it has been used is recorded on distribution ledger, an integrated system can be constructed without involvement of a third-party system. This will cut the expense by effectively merging systems distributed due to the credibility among organizations, solve the problems of overlaps of data, and reduce the time to request and transfer data.

Furthermore, if the blockchain in which such data are stored as one enterprise-level data platform, the compatibility issue in integrating existing solutions can be solved as well. Data to be referenced by the solutions on the platform is saved as blockchain in lower data platform level, and the solutions can request the data for reading and writing. Then, the overlaps of data disappear, and because there will be no need to exchange data in the solution, it is expected to replace the existing integration project.

Based on this expectation, IBM was the first company to show interests in the blockchain among the companies that provide enterprise-class solutions, co-founded Hyperledger Foundation with Linux Foundation and unveiled the Hyperledger fabric. Microsoft, Oracle, and SAP also started to develop blockchain related technology and launched the service.

2) Who is the blockchain platform for?

According to Coinmarketcap.com, the representative cryptocurrency information site, about 2,500 blockchain projects are currently registered, and aggregate market capitalization totaling approximately 32 billion US dollars. There are hundreds of platform projects that aim to establish independent cryptocurrency ecosystem based on blockchain technology, and it is also easy to find thousands of decentralized app service projects realizing independent cryptocurrency business model. These are only a fraction of multiple blockchain projects in progress around the world, and numerous researches are being conducted and released to create new value in each area at this moment.

Then, for whom is a truly meaningful platform being researched and invested with astronomical amount of money in blockchain industry like this new IT Big Bang?

Platforms cannot exist independently and can only realize their values as platforms when someone provides functions operating on the platforms. Blockchain platform should be able to accommodate every type of system that can be serviced over an internet network capable of high-speed communication, and if we wishes to realize any type of service using the characteristics of the blockchain the service

provider should be able to reduce the time, effort, and cost to develop and study all the technology necessary to realize blockchain system.

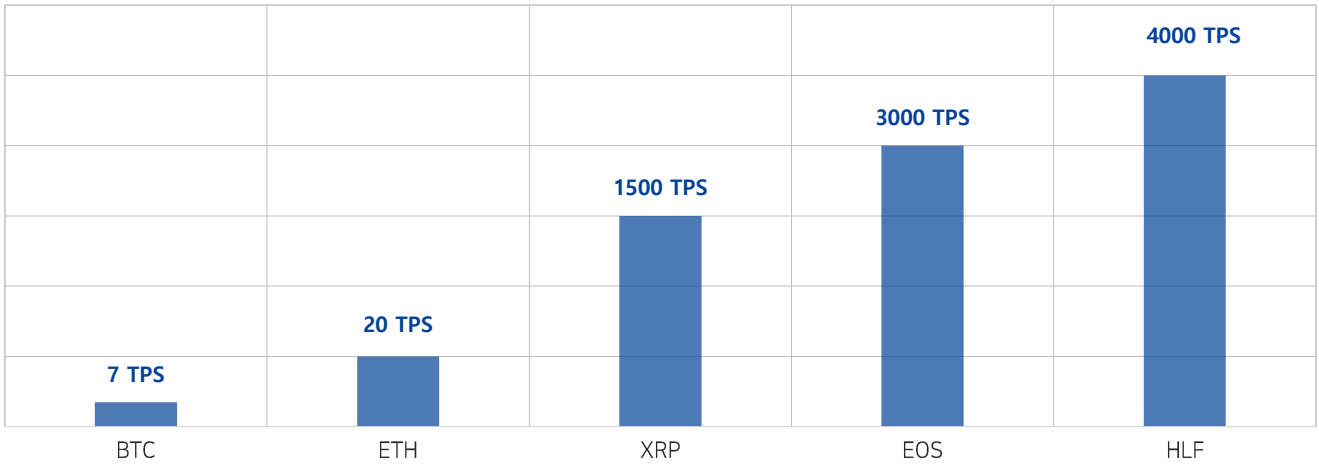
3) The problems of blockchain until now

(1) Blockchain performance issues

The possibility of applying blockchain to enterprise as aforementioned gave people the impression that blockchain is "The Next Cloud" or "the core technology of the 4th industrial revolution," but it is hard to find cases that are perfectly applicable in real industry. Blockchain enterprise systems require high-speed data input and output to distributed ledgers, and at the same time require high computing power. However, at present, several technical difficulties have prevented successful blockchain enterprise systems from being implemented, and the main causes are remarkably slow consensus structures and data processing performance.

Because of the nature of the enterprise environment where system outages or slowing down can significantly impact the business, companies typically require a certain level of SLA(Service Level Agreement). The most representative index is TPS(Transaction Per Second), and this is the basic measure to ensure stable response time without slowing down even when a certain system requests a large amount of work from multiple users simultaneously.

While TPS of Bitcoin or Ethereum, excluding EOS, fails to reach 100, the TPS desired by the companies is significantly higher. VisaNet uses average of 2,000TPS, but it requires 56,000TPS in case the number of users rapidly increases[1], and AliBaba, the standard payment system in china, is already working on a project to allow tens of thousands of TPS[2].



[Diagram 01] TPS of Bitcoin, Ethereum, Ripple, EOS

As seen above, the current blockchain fails to reach the demands of the companies in terms of TPS and research institutes and companies that want to apply blockchain to technology are studying various ways to improve this, but have not found any clear measure yet.

In addition, the blockchain has become more interested in improvement of TPS as the applicable areas of smart contracts and the like are expanded beyond the simple distributed ledger. Some projects, such as EOS, are faster by 28 times than Ethereum, and are planning to develop further with the goal of reaching 1,000,000 TPS, but they are not suitable for enterprise platform because they are still in thousands TPS levels and are fundamentally difficult to control data ownership, such as private network desired by companies.

1) visa-fact-sheet-Jun2015 at https://usa.visa.com

2) https://www.alibabacloud.com/blog/when-databases-meet-fpga-achieving-1-million-tps-with-x-db-heterogeneous-computing_594147

As more and more commercial platforms are developed based on Hyperledger Fabric, the limits in processing
As to what specific portions of the blockchain platform must achieve to be recognized as a high-performance platform, we MEDIUM's many case studies and analyses have led to the following items.

(2) Performance evaluation criteria for blockchain platforms

TPS(Transaction per Second) is a typical quantitative indicator that expresses the performance of blockchain platforms, but it is regarded now as fragmentary category, as blockchain platform have to process multiple functions. Therefore, the following items should be analyzed when measuring performance in various aspects.

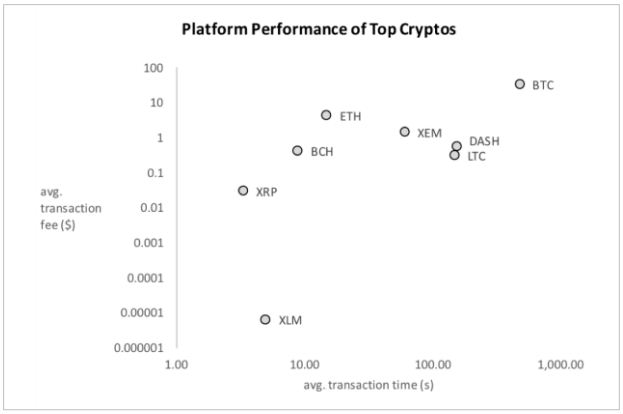
Classification	Category	Description
Transaction	Transaction per Second– TPS	The number of transaction completed and recorded per second
Smart Contract	The number of smart contract completed per second	The number of smart contract completed and recorded on the block per second
	The number of smart contract completed that are processed in parallel per second	The number of two different smart contract completed that are processed in parallel per second
Expandability	The maximum number of node that ca ne be increased (Target TPS Fixed)	Measure on how many nodes can be increased when demanded TPS is fixed
	The number of consensus algorithm processed as the number of node increases	Measure on throughput of consensus algorithms completed in unit time as the physical number of nodes increases.
	The speed of consensus algorithm processed as the number of node increases	Measure on the speed of process per consensus algorithm requested as the physical number of nodes increases.
Response Time	Response time of transaction	Measure on the response time of transaction when transaction is requested from End-point(Web, App I/F) and is completed

[Table 01] Performance evaluation criteria for blockchain platforms blockchain platform by MEDIUM

(3) Cost issues of blockchain platform

The problem narrate along with the performance of blockchain is the cost of using blockchain platforms. Although a Bitcoin system designed from the awareness of the problem of expensive fees for overseas remittances being used worldwide, ironically, the money transfer system, developed using Bitcoin networks, faces a situation where the existing centralization system is much more expensive than it would have been in the bottleneck section due to the overload of Bitcoin networks.

This is not only a problem for Bitcoin, and its relatively early blockchain platforms, such as Ethereum, NEM and DASH are struggling to expand ecosystem due to high network fee policies. The expensive network commission policy is not only a burden on the developer who wants to develop the service by using the platform, but also forces to make middleware or complex UX designs to reduce the cost, which is inconvenient and time consuming for the user. This leads to new problems. Efforts have been made to add additional nodes and improve consensus algorithms to improve network bottlenecks that cause these problems, but the cost of doing so has not led to a significant total cost savings.



[Diagram02] Transaction fee by avg. TPS of top cryptos[3)]

EOS and Tron, which emerged as a relatively advanced blockchain platform, developed their systems to achieve "no-fee model," but commercial services based on each platform must secure smooth transaction processing bandwidth in order to provide traffic to thousands to tens of thousands of users and hold a large amount of platform tokens in the process.

When data communication was introduced based on phoneline, it revolutionized the world by bringing a world where using PC and communicating with text possible, but the expensive fee refrained from people to experience the Internet service.

However, with the rapid introduction and universalization of high-speed network technology, the Internet itself is no longer recognized as an expensive paid service. Therefore, various high-definition contents services such as real-time broadcast, personal broadcast, and multi-channel broadcast are changing the world. The blockchain is also expected to become popular as a new concept of decentralization services that will lead the trend and lead the era if it guarantees high processing performance to establish itself as a platform and achieves cost level close to that of public goods.

4) Why does blockchain platform need to be high-performance?

MEDIUM emphasizes performance among the many features that blockchain platforms should have. To maximize the value of decentralization, which allows the use and confirmation of network resources freely without policies and restriction of central authority, many services must be operated at once, and it must be global service where millions of people can use them without limits of borderlines and time and space.

5) The efforts of the industry for increased performance of blockchain platform

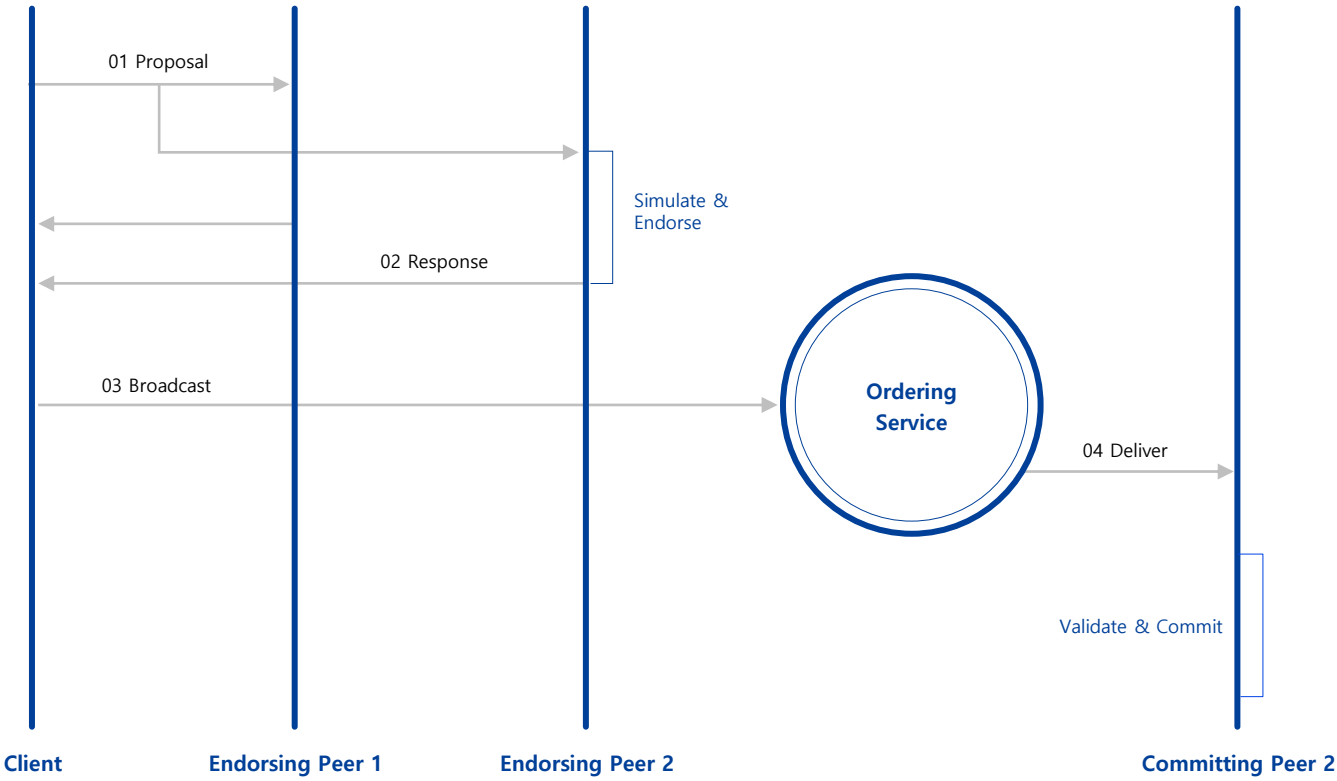
(1) Permissioned blockchain platform

The first element mentioned in elevating the function of the blockchain is the form of blockchain. There are many suggestions such as public, private, hybrid, and side chain, but many papers by blockchain research institutes report that permission blockchain, which has clear and consistent standards for participation of node, is the most efficient in terms of performance[1]. This research is designed for blockchain platform specialized for independent organization such as companies or agencies, and includes Hyperledger, EEA, JP Morgan Quorum, and R3. Hyperledger Fabric, led by IBM through Apache Foundation, has positioned itself as De Facto Standard of enterprise market.

(2) Research on improvement of performance based on Hyperledger-Fast Fabric

3) https://www.stellar.org/blog/Q1-2018-stellar-and-state-of-crypto/

transaction and expandability became recognized. There are many researches to improve the functions of platforms based on Hyperledger Fabric, and research about 4 improvements methods based on causes of limits in performance mentioned importantly by traditional transaction flow[4].



[Diagram03] Hyperledger fabric's transaction flow [2]

Causes of limiting performance	Solutions
Separation of data and Meta data	Redesign fabric's transaction ordering service to work with only the transaction IDs, resulting in greatly increased throughput.
Parallel processing and caching	Increase overall throughput by some parallelization of Transactions validation or by data caching.
Improved data access method using hierarchical memory structure	Redesign to optimize the data management layer for faster access to the data on the critical transaction-validation path.
Transformation of the resource management architecture	Separate hardware of the resources for the peer roles of committer and endorser.

[Table02] Diagnostics cases of fast fabric study

4) Fast fabric : Scaling Hyperledger fabric to 20,000 transactions per second

6) MEDIUM's suggestion

MEDIUM is a blockchain platform designed to meet the needs of the enterprise market. It will provide enterprise-class, high-performance and high-speed blockchain systems, as well as solutions that are compatible with existing blockchain markets.

For this purpose, MEDIUM has developed Medium Blockchain Processing Unit (MBPU), which is dedicated hardware for blockchain, with parallelization technology for executing instructions for transaction processing and concurrent processing threads for block creation. The MBPU is a result of the MEDIUM technology that innovatively increases the processing performance of the blockchain platform, in which the hardware is configured for each module independently to perform the main functions of the blockchain independently.

MBPU is designed to modularize and efficiently handle bottlenecks and complex structures of the processing which are the main causes of speed delay in the blockchain. In addition, MEDIUM will benchmark and redesign the architecture of Hyperledger fabric, currently De Facto Standard in the private blockchain market, and fully reconstruct the Hyperledger fabric with C++, the language that uses H/W and CPU most efficiently, to realize the fastest theoretically feasible speed with MEDUM MBPU.

As of July 2019, which is the date of this document's distribution, we confirmed about 100,000 TPS, and this performance measurement results will be published after measuring the official performance figures in the research and development department from the certification expert organization which is in collaboration with MEDIUM.

7) MEDIUM blockchain's policies and directions

MEDIUM blockchain platform aims to implement the technology based on the following policies and directions to ensure ultra-fast performance.

(1) H/W Oriented improvement with MBPU enhancement

As the blockchain platform runs, many bottlenecks and processing delays occur in the creation and processing of the transactions and smart contracts. This phenomenon is a fraction of the software that processes the commands of the requested program, the method of processing the memory structures of a general computer which is designed for bottleneck purpose is the main cause of the processing delay which is an inevitable problem, currently, this is the same phenomenon that occurs to all blockchain platform providers. MEDIUM will design and develop our own MBPUs optimized for blockchain platform specific functions and command processing structures, and to improve processing performance of the entire platform.

(2) Permissioned blockchain: Consortium blockchain

In order to ensure high-speed throughput, MEDIUM aims to establish a permissioned blockchain network, which sets specific criteria for participation in blockchain nodes and only some users are authorized to participate in the nodes. A node operation organization that meets the criteria given by MEDIUM will be selected to represent each continent, and the MEDIUM blockchain platform will be established by the consortium of the representatives of each of the organization of each continent.

(3) MEDIUM Appliance® use exclusively

In principle, participants must use MEDIUM dedicated H/W equipment developed by MEDIUM if they want to participate as nodes on the MEDIUM blockchain platform or if they want to build a separate platform based on the MEDIUM blockchain. MEDIUM H/W equipment is a hardware device made up of dedicated chipset and board specially designed / developed to maximize the performance of MEDIUM MBPU, ensuring the optimum environment in which the operating system and software architecture of MEDIUM block- chain can be operated. If only the software package of the MEDIUM blockchain platform is applied to general intel series PCs or servers or other machines, it may not operate normally and smooth performance will not be guaranteed.

(4) Large bandwidth permissioned network environment: Co-location service

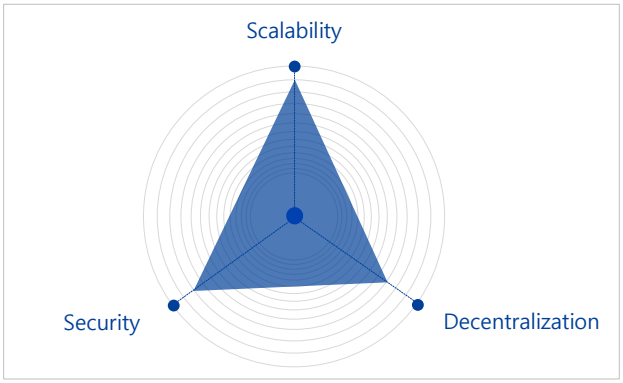
All node devices participating in the MEDIUM consortium network will be brought in and operated in a data center that is as close as possible to the Backbone network and is always pleasantly available to the high-speed Internet network.

Recently, data centers around the world, including Korea, have high-quality fault-handling and monitoring systems as well as 24 hours a day, 365 days a year, non-stop, uninterruptible, constant temperature and humidity, and are managed under very strict conditions. Ensuring a high bandwidth network environment to provide an enterprise-class performance platform is essential and is considered a necessary and sufficient condition for a high-speed blockchain platform.

8) MEDIUM blockchain's identity

As mentioned above, we are concentrating on maximizing the platform performance by redesigning and optimizing all the systems needed for platform implementation from H/W step to back bone inter-working structure in order to implement the block-chain platform as commercial level enterprise system.

The MEDIUM blockchain aims not only to improve the throughput and scalability that are simplified by TPS, but also to realize integrated technology that can guarantee decentralization and security.



[Diagram04] MEDIUM blockchain trilemma goal

9) MEDIUM blockchain's final goals

MEDIUM already well knows for whom to commercialize the platform and for whom to upgrade the technology, while looking deep into the nature of the blockchain platform.

In the first half of 2019, when this document is being written, there is no blockchain based decentralization service that has become common to the general public. However, if blockchain and network technologies continue to evolve in the future, and if decentralized network services become generalized, and cryptocurrencies becomes commoditized for daily life services, we think it will be the result of technologies that have evolved through the transformation of ideas and approaches such as our MEDIUM.

For the upcoming worldwide project to develop thousands and tens of thousands of blockchain services, MEDIUM aims to eventually implement the 1Million TPS, and it will be a prime indicator of ensuring the performance of the fastest platform and the lowest cost.

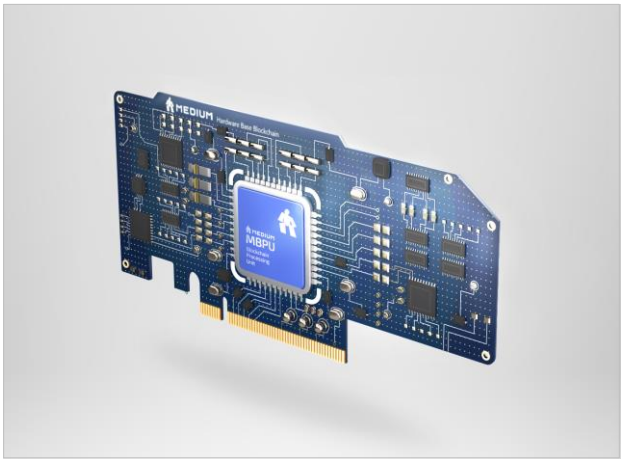
Medium will also provide the best environment and tools for developers around the world to easily and quickly access the MEDIUM network to realize their ideas and achieve their desired goals. Thereby we want to contribute the true value of decentralization to take root in the global IT industry.

02 MEDIUM's core technology

1) MBPU (Medium Blockchain Processing Unit)

MBPU is a hardware information processing unit for the world's first blockchain platform developed by MEDIUM, consisting of crypto engine, enhanced DB, SC Engine and NIC engine module. It modularizes the operation type that is repeatedly performed by the blockchain platform, and is designed according to the characteristic of the data processing pattern for each module part.

This pattern modular design approach can fundamentally improve bottlenecks that inevitably occur on data computations and memory control mechanisms that operate on CPUs designed for traditional categories, and is optimized for data patterns such as transaction and smart contact data that usually occur on blockchain platforms.

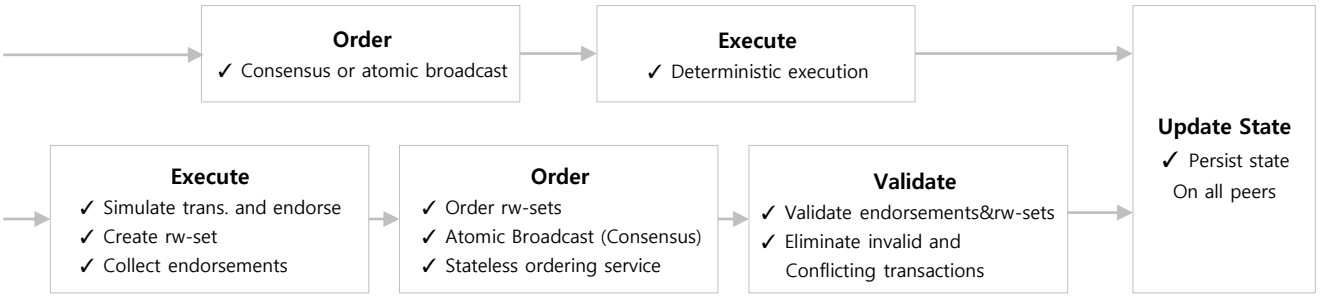


[Diagram05] MEDIUM MBPU (Medium Blockchain Processing Unit)

This MBPU is a study that upgrades blockchain technology in a fundamentally different way from the thousands of traditional blockchain studies, and it is the first ones we've tried worldwide. These attempts at MEDIUM are just the beginning, and we will continue to innovate to set the standard for high-performance blockchain platforms.

2) MEDIUM architecture

MEDIUM has benchmarked Hyperledger fabric's idea to improve the performance constrains revealed by various consensus methods including Order-Execute and their architecture. The fabric is aimed at the Execute-Order-Validate architecture, which is a step in which some nodes execute the transaction first, then verify the result value, and separately apply the steps applied to all the nodes. This design is fundamentally different from the Order-Execute method in that the fabric executes the transaction before it reaches the final agreement on order.

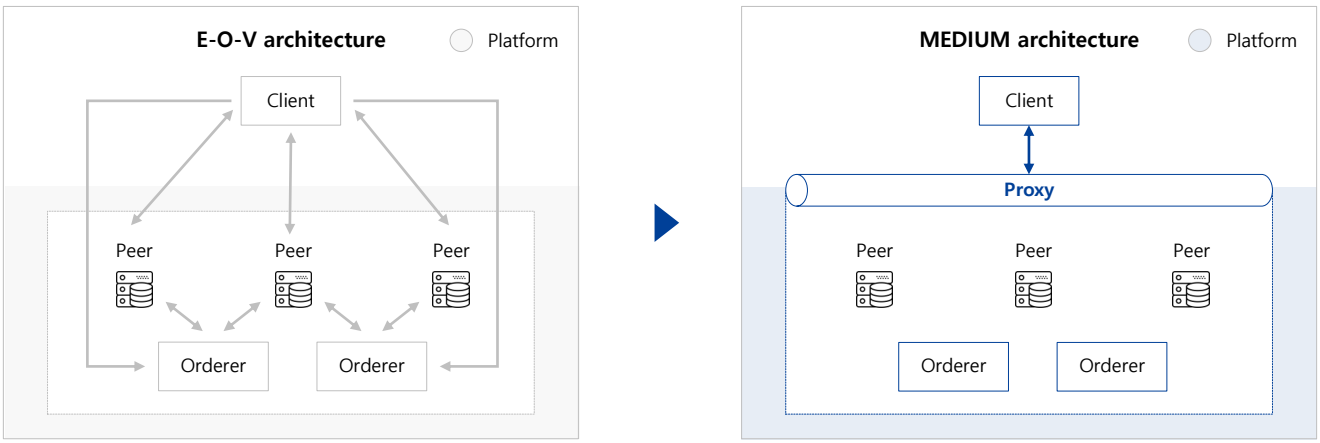


[Diagram06] Order-Execute and Execute-Order-Validate architecture process comparison

MEDIUM has designed and applied its own architecture by benchmarking the EOV architecture mechanism and consensus algorithm of Hyperledger fabric and implemented an architecture that maximizes performance by modularizing and structuring the process of identifying and verifying transaction information.

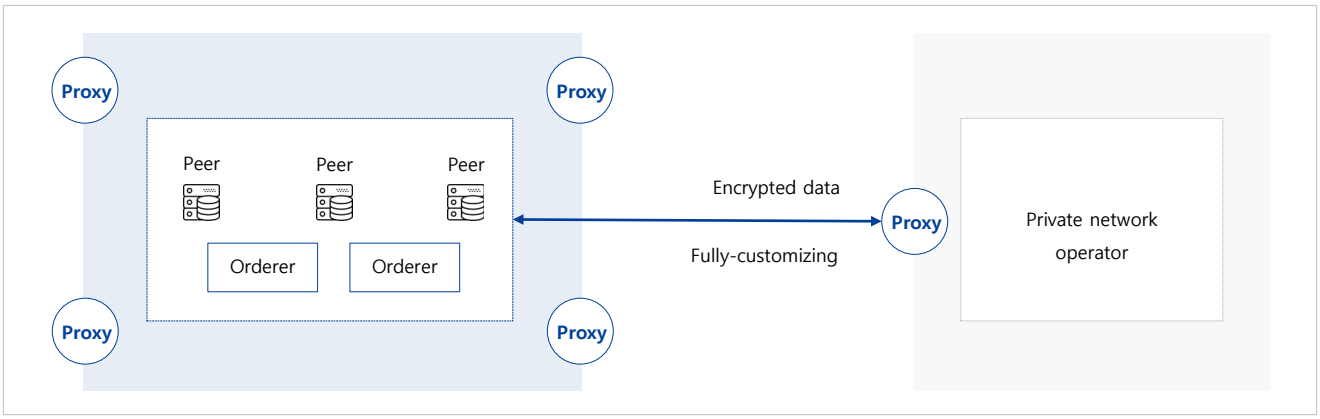
3) MEDIUM proxy

When operating the decentralized service using E-O-V architecture, the client is responsible for accessing the platform and using the resource. The client communicates directly with peers and orderers existing in the platform to perform authentication and data recording of the node. The client must know information for connection and communication such as peer's and orderer's IP address, and the client will go through multiple communication processes with nodes directly at various stages such as signing, verification, and request. This structure can also affect the final processing performance of client and it can be an architecture that requires improvement in the sense that Peer and order's information is exposed to all clients. To improve this, MEDIUM introduces the concept of proxy to create a structure that allows clients to access the platform or use resources efficiently through proxy. Through MEDIUM proxy system, client does not need to communicate separately with individual nodes such as peer or orderer, and can perform communication with only proxy node for request and management of data. This is an improved architecture in terms of procedural efficiency, but it also enhances security in that it prevents client accessing the platform for the service from unnecessarily obtaining sensitive information about the platform configuration.



[Diagram07] MEDIUM proxy system's structure

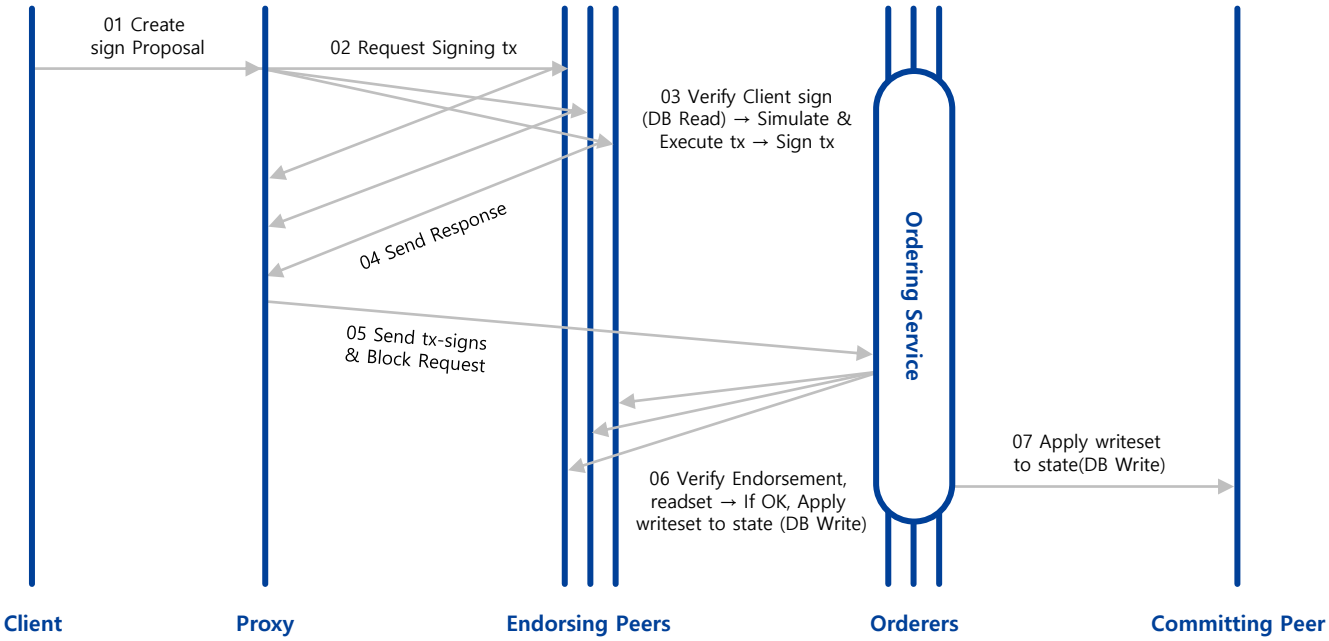
While the above case described an example of a general case in which a decentralized service (DApp) accesses a blockchain platform and uses resources, the following case shows a structure that enables the MEDIUM public platform to be used safely and efficiently through the MEDIUM proxy node when the operators (government agencies, financial institutions, other organizations, etc.) operating a private network want to use only high-speed blockchain platform functions separately. At this time, the proxy node can be fully-customized according to the environment and requirements of the private network operator, and ensures the security through the encrypted data communication method.



[Diagram08] Private network operator's proxy node structure

4) MEDIUM's diagnosis and solutions for increased performance of platform

MEDIUM analyzed the consensus algorithm and transaction processing of enterprise type blockchain platforms including Hyperledger fabric and popular public blockchain platforms, and found that it is converged to five issues in which factors restricting performance improvement are commonly derived, and want to propose 7 models that can improve the performance by direct processing through MEDIUM MBPU.



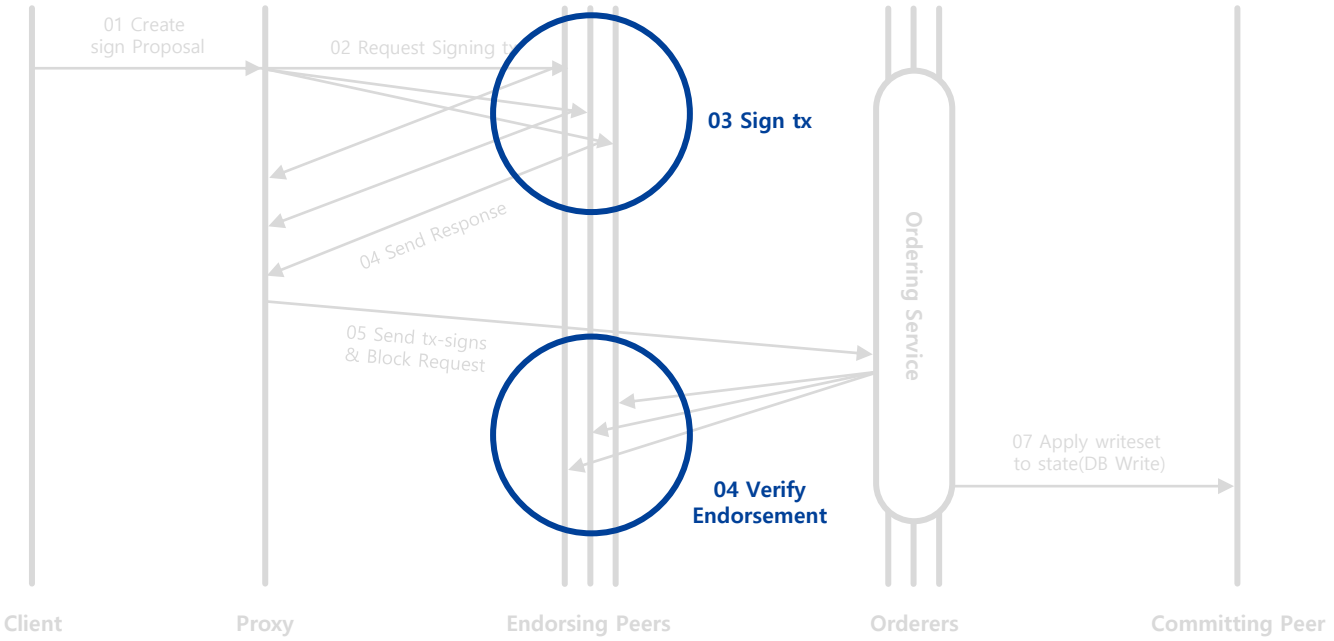
[Diagram09] MEDIUM blockchain transaction flow

Elements limiting the increase in performance	Solutions
[Issue1] Sign & Verification Process	[Solution1] Accelerating for sign & verification by crypto engine
	[Solution2] Sign algorithm for peer's scalability
[Issue2] Data processing	[Solution3] Data serialization by data processing engine
	[Solution4] High performance Key-Value storage
[Issue3] Operation process of smart contract	[Solution5] Increase smart contract parallelism
[Issue4] Network overhead	[Solution6] TCP offload engine
[Issue5] Ordering consensus	[Solution7] H/W based ordering consensus

[Table 03] Elements limiting the increase in performance and solutions by MEDIUM

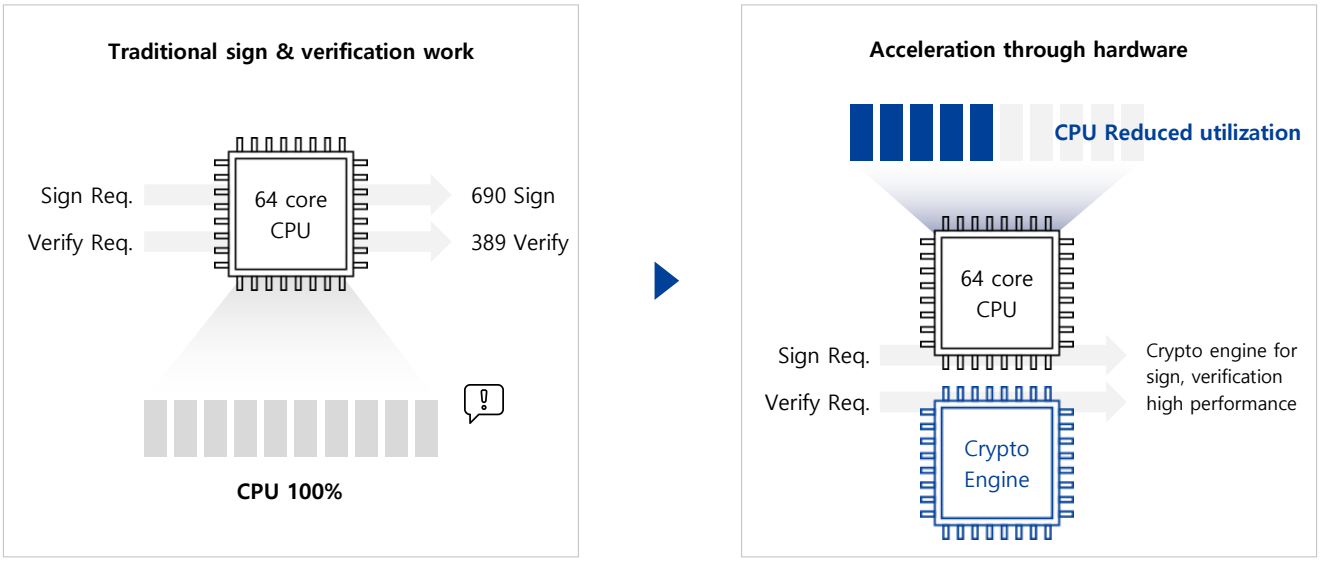
(1) Issues of sign & verification process and two solutions

a. Causes of speed reduction in signing and verification process
- In the process of sign tx and verify endorsement, the bottleneck increases and speed decreases as the Tx request approaches 1M.



[Diagram10] Causes of slowing down during sign & verification process

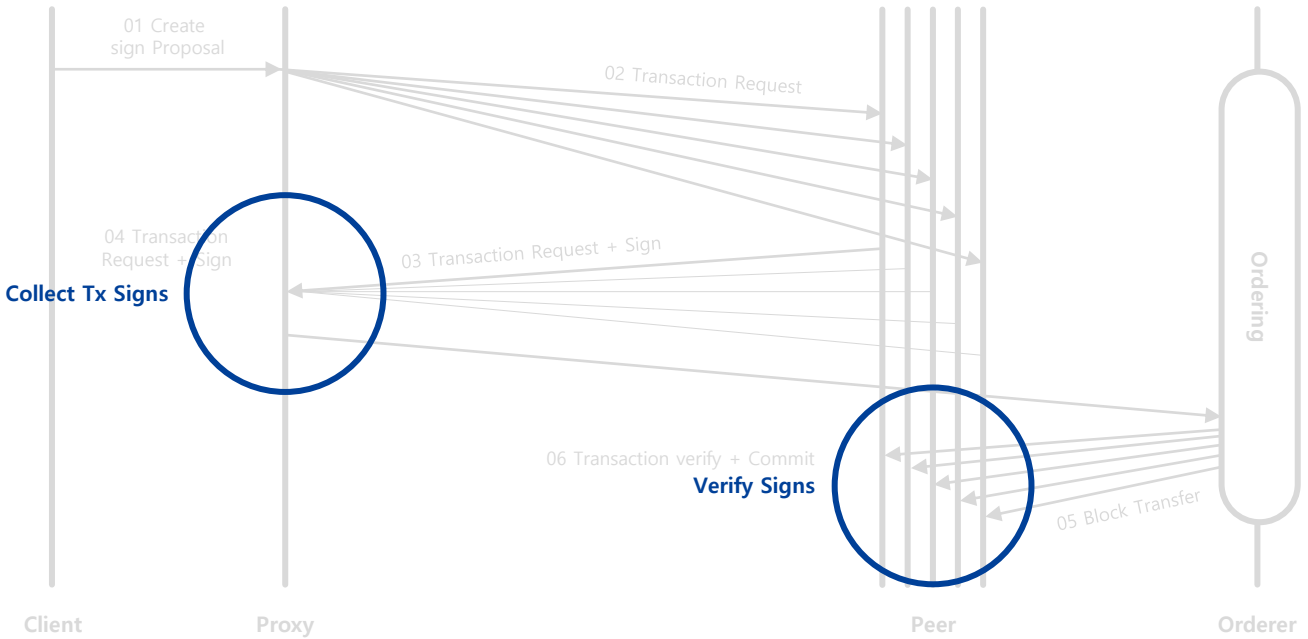
b. Solution1 : Accelerating for sign & verification by crypto engine
- In performing existing sign & verification operations, we confirmed the processing of 690K sign request and 380K verify requests based on 100% CPU availability (based on 64Core CPU)
- Increase the performance through using "Crypto Engine Chip," a dedicated H/W for sign & verification



[Diagram11] Accelerating for sign & verification by crypto engine

c. Causes of slowing down as the number of peers increase

- When a new node(peer) is added/extended in the entire node, the number of sign tx and verify endorsement is increased exponentially, which is a direct cause of speed degradation.



[Diagram12] Causes of slowing down during sign & verification process

d. Solution2 : Use an algorithm dedicated for verification for peer scalability.

- When Peer is expanded, CPU load for verifying signs also increases because sign per transaction also increases in proportion. Improve performance by using an algorithm dedicated for sign that converges the number of signs to be verified to a specific number even if the peer increases.

Traditional Sign Algorithm

	Peer 1	Peer 2	Peer 3	Peer 4	Peer 5	...	...	...	...	Peer N
Tx 1	Sign 1	Sign 2	Sign 3	Sign 4	Sign 5	...	...	...	...	Sign N
Tx 2	Sign 1	Sign 2	Sign 3	Sign 4	Sign 5	...	...	...	...	Sign N
Tx 3	Sign 1	Sign 2	Sign 3	Sign 4	Sign 5	...	...	...	...	Sign N
⋮	Sign 1	Sign 2	Sign 3	Sign 4	Sign 5	...	...	...	...	Sign N
Tx 300,000	Sign 1	Sign 2	Sign 3	Sign 4	Sign 5	...	...	...	...	Sign N

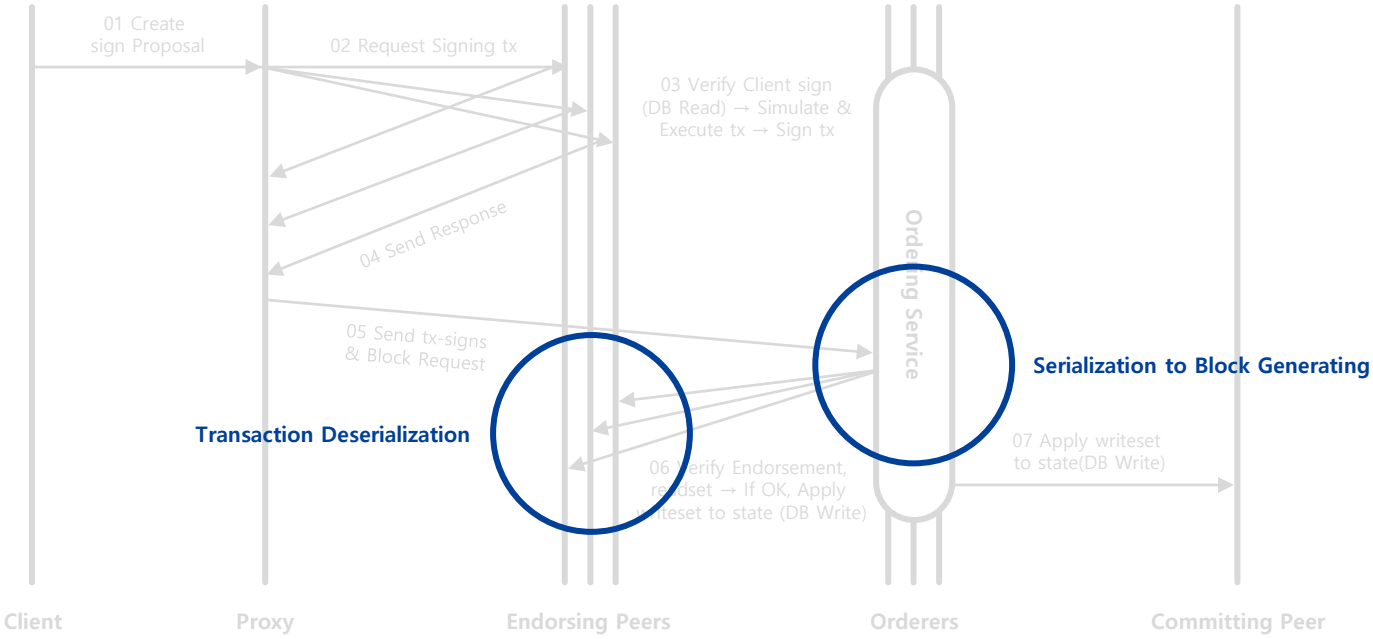
Acceleration through sign algorithm

Tx 1	**Peer 1**	**Peer 2**	**Peer 3**	**Peer 4**	**Peer 5**	...	**Peer N-2**	**Peer N-1**	**Peer N**
Tx 2	X Signatures								
Tx 3	X Signatures								
⋮	X Signatures								
Tx M	X Signatures								

[Diagram13] Effectiveness of improvement of algorithm specifically for sign

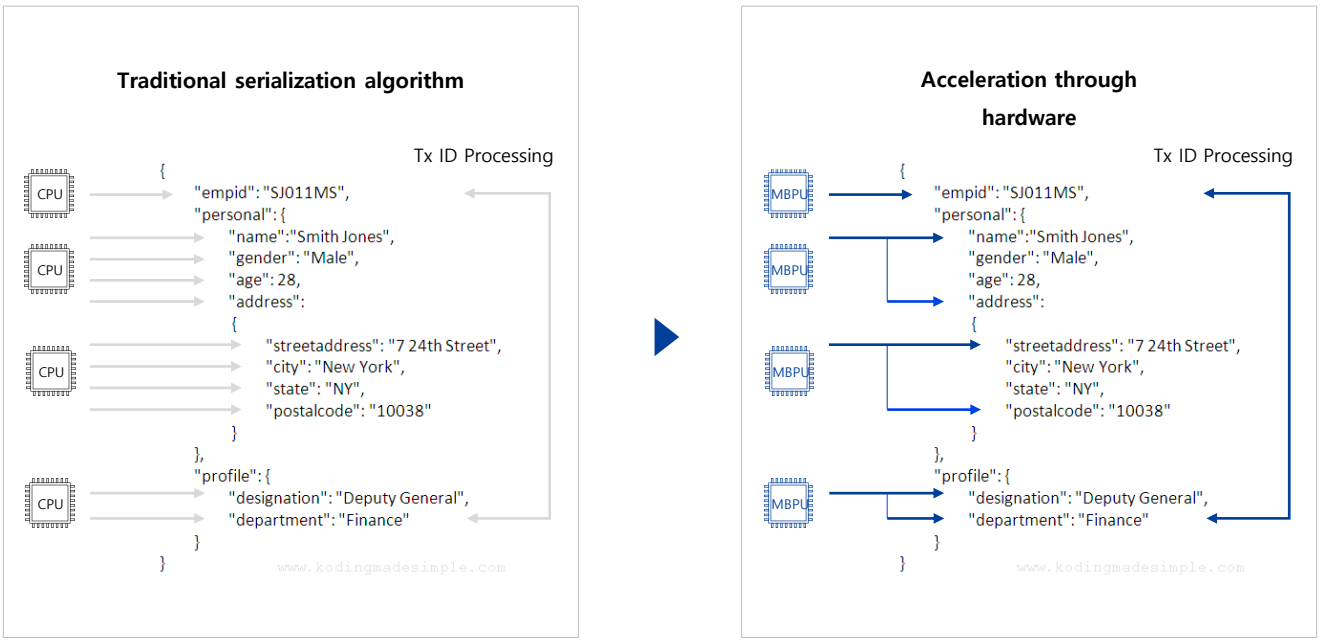
(2) Data processing issues and 2 solutions

a. Causes of decrease in performance in data processing
- In the transaction flow process, it takes a lot of CPU resources to serialize and record the received data during the process of receiving data and generating blocks, which makes it difficult to process a large number of transactions.



[Diagram14] Causes of slowing down in read / write process in DB flow

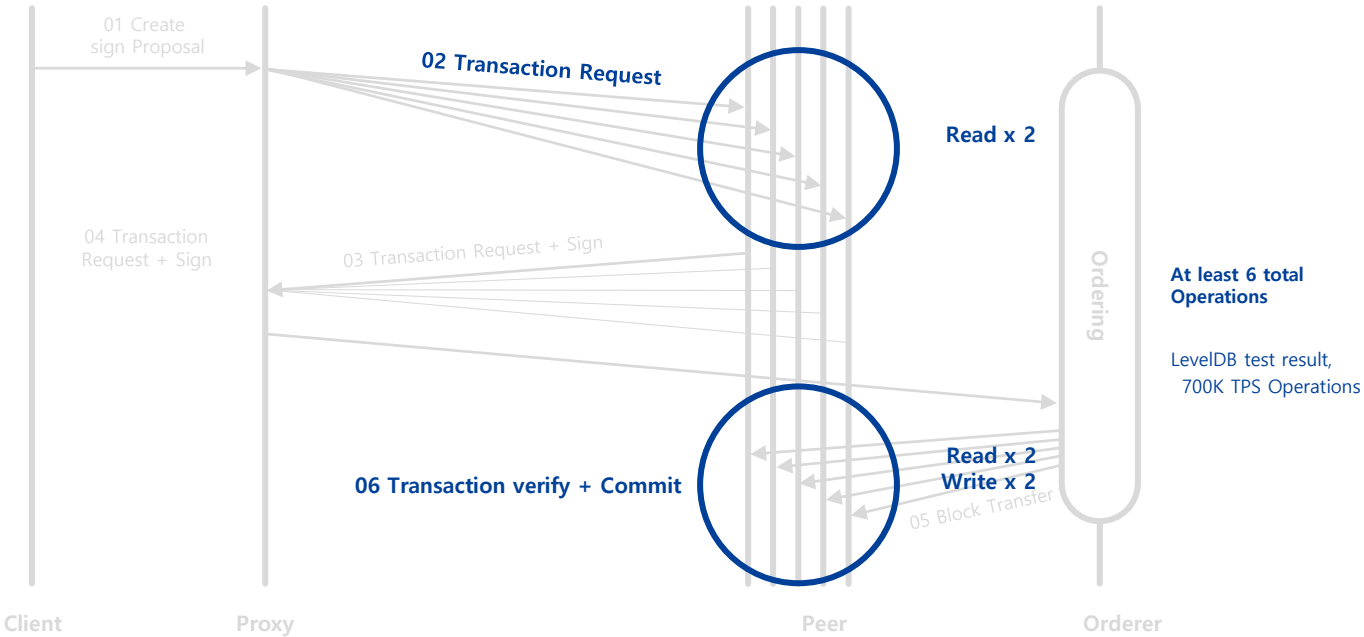
b. Solution3 : Add H/W for serialization and deserialization
- Improve the performance by adding separate H/W for serialization and deserialization



[Diagram15] Causes of slowing down in Read / Write Process in DB Flow

c. Limitations of existing key-value store

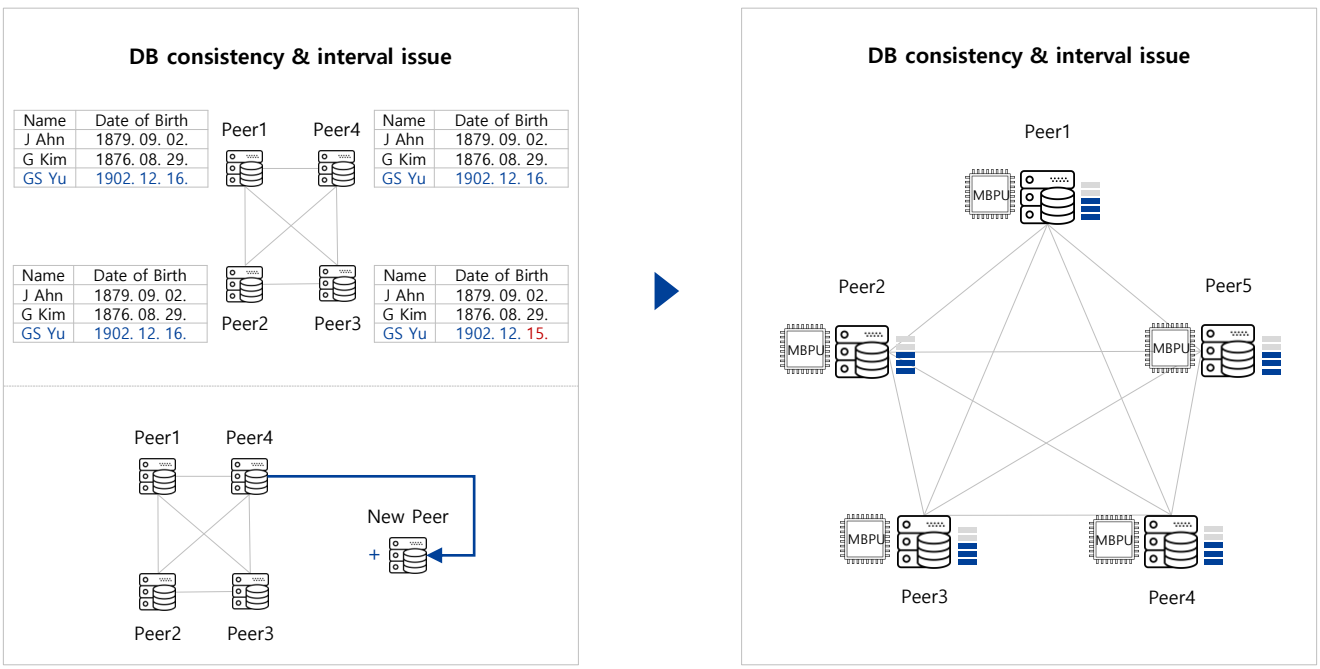
- Overall performance degradation due to limitations of existing database performance during Tx Read / Write
- Occurrence of problems where the consistency of data between peers cannot be maintained
- Data replication issues to added peers



[Diagram16] Problems of functions in transaction Read / Write DB

d. Solution4 : Key-value storage

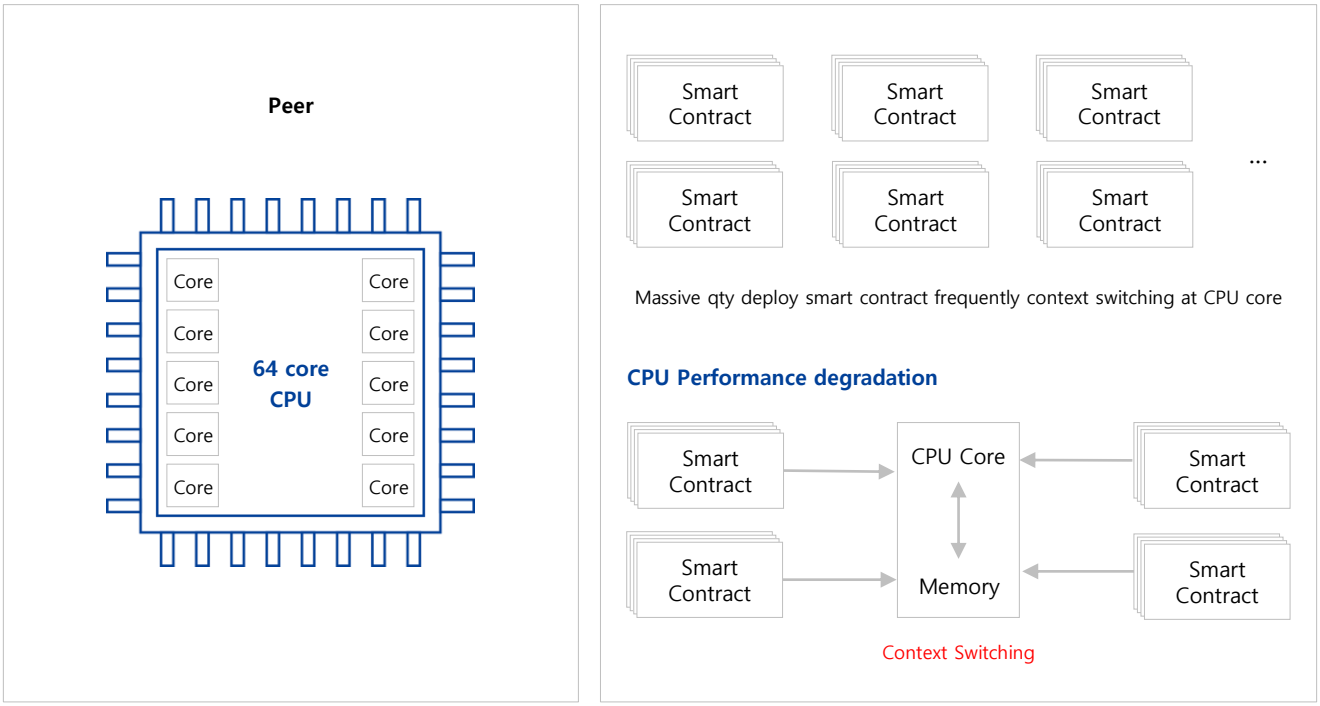
- Groundbreaking performance improvement through structure improvement of hardware-based key-value storage.
- Add hardware that regularly confirms the consistency of entire data for maintaining consistency
- Use a fast network and add data processing hardware to speed up DB replication.



[Diagram17] Key-value storage for db consistency & interval problem

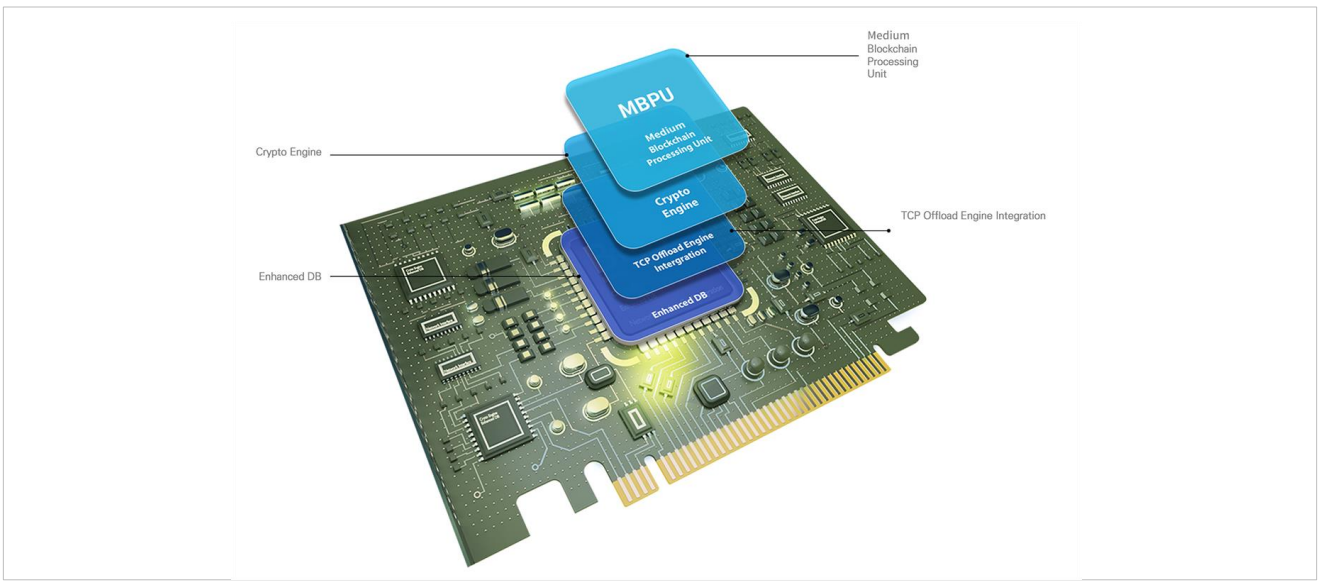
(3) Issues of operation process of smart contract and the solution

a. Smart contract operation issue
- System performance degradation due to frequent context switching in CPU core when distributing large amount of smart contract.



[Diagram18] Smart contract operation issue

b. Solution5 : Increase smart contract parallelism (install smart contract processor board to peer)
- Multiple dedicated processors are placed on a single server, allowing multiple smart contracts to run at the same time.
- A smart contract runs in a standalone os to increase security level.

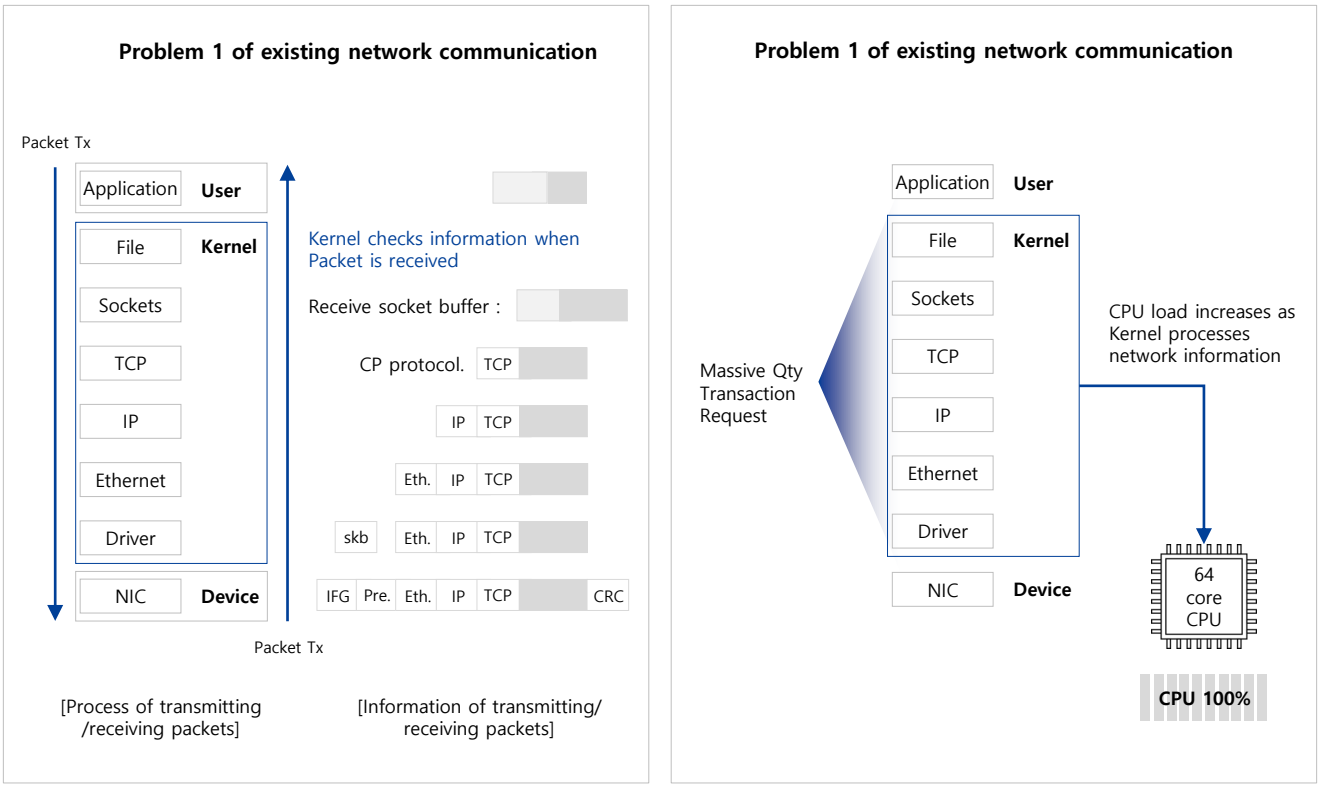


[Diagram19] Smart contract processor board key map

(4) Network overhead issues and the solution

a. Network overhead issue

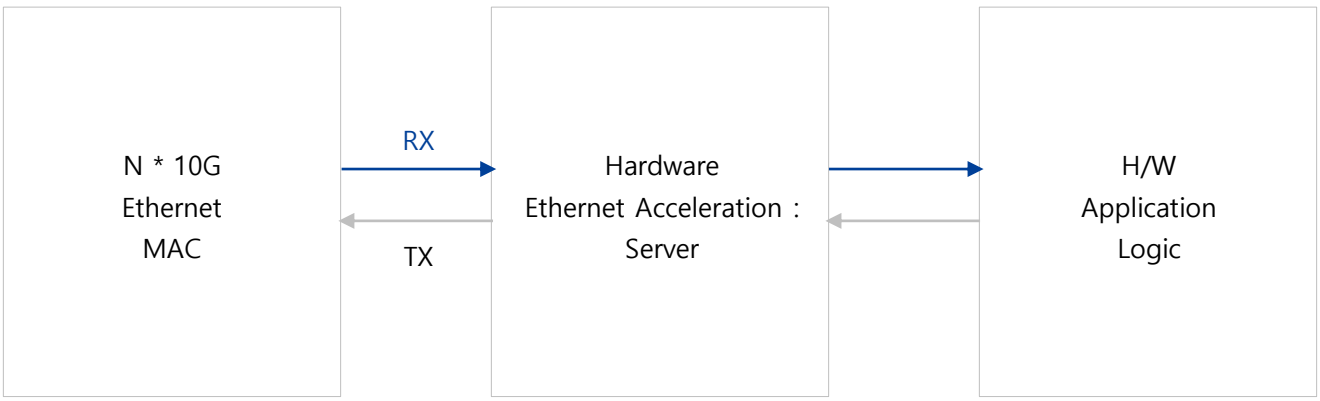
- The process of receiving packets through a network module and interpreting packet information in the kernel will result in heavy CPU load, and if the network module receives more than hundreds of thousands of requests per second in a moment, it will cause severe bottlenecks.



[Diagram20] Network overhead flow diagram

b. Solution6 : Add network H/W module

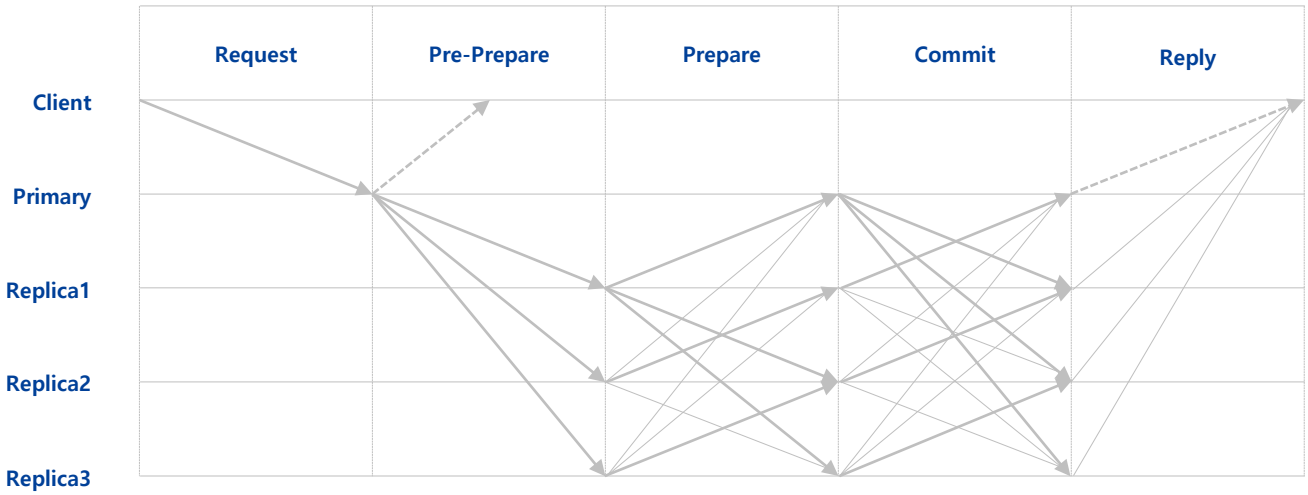
- Develops an H/W chipset for Network Modules to perform parallel processing of packet information.
- Study on reduction method of kernel usage load using existing hardware such as TOE (TCP Offload Engine)
- Secure high bandwidth for processing large transaction requests.



[Diagram21] Network module concept diagram

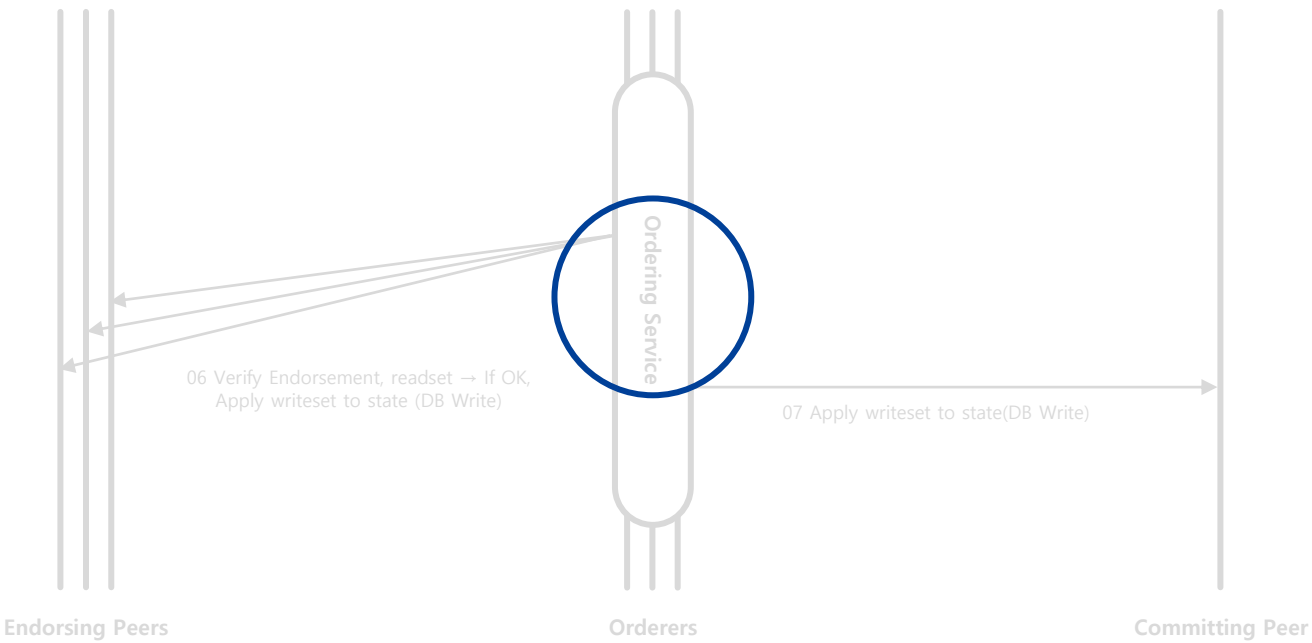
(5) Ordering consensus issues and the solution

a. Problems of existing BFT type algorithms
- BFT(Byzantine Fault Tolerance) family algorithm (ex> PBFT) requires high performance to handle hundreds of thousands of transactions because of the nature of the consensus.



[Diagram22] PBFT consensus algorithm example

b. Solution7 : Accelerating by H/W
- Use dedicated H/W and H/W based high speed, scalable algorithm for BFT in orderer.



[Diagram23] Network overhead flow diagram

5) MEDIUM's core technology and development roadmap

The blockchain technology, which was first started from Bitcoin, introduces a new concept of storing, generating and managing transaction data in a P2P network, and implemented a confidence-building method in software that has not existed before. MEDIUM regards MBPU as its core technology in order to apply and distribute the blockchain technology represented by Bitcoin to all ICT industries, and intends to develop it through continuous innovation and improvement.

(1) Commercialization of MEDIUM appliance® with MBPU performance enhancement

The research results of the MEDIUM blockchain platform will appear as the performance of the core MBPU and will be commercialized as MEDIUM Appliance® combined with the MEDIUM platform architecture. As the global application of blockchains to the business world is becoming commonplace, MEDIUM's Appliance® products will be reviewed first and will be rapidly commercialized to meet the direction of market development if government agencies, corporations and organizations want to deploy high-performance platforms individually.

(2) 1M TPS realization

As previously mentioned in the final goal of MEDIUM Blockchain, MEDIUM continues R&D effort to develop dedicated H/W as well as improving the software performance in order to implement 1M TPS. The most important part is the MBPU, and now we focus on making the four parts of crypto engine, enhanced DB engine, SC engine and NIC engine as H/W. In the future, we will realize the final 1M TPS through R&D of MBPU dedicated cache memory and core.

(3) Expansion of the application fields

Blockchain technology will evolve so that it can be used in various areas of promising technologies in the fourth industries such as smart city, AI and shared economy in the future. We, MEDIUM will also upgrade our blockchain platform accordingly, and in particular, as it is expected that MBPU will be widely used in various fields, plans to add various functions as well as its performance.

As IoT technology becomes more common in the near future, blockchain technology will be used to verify trust and consensus between devices in communication methods and data exchange, and micro MBPU that can be attached to various IoT devices will also be developed and commercialized.

In addition, we believe that as new means of communication emerge and spread in future modern people's lifestyles, mobile MBPU and application MBPU will be developed so that blockchain technologies and services can be utilized directly in future smartphones, so that blockchain smartphones can be commercialized. If the blockchain smartphone is commercialized, it is expected that cryptocurrencies will be applied to more application services, and that the identification and authentication methods of individuals will evolve one step further and the utilization of smartphones will be maximized.

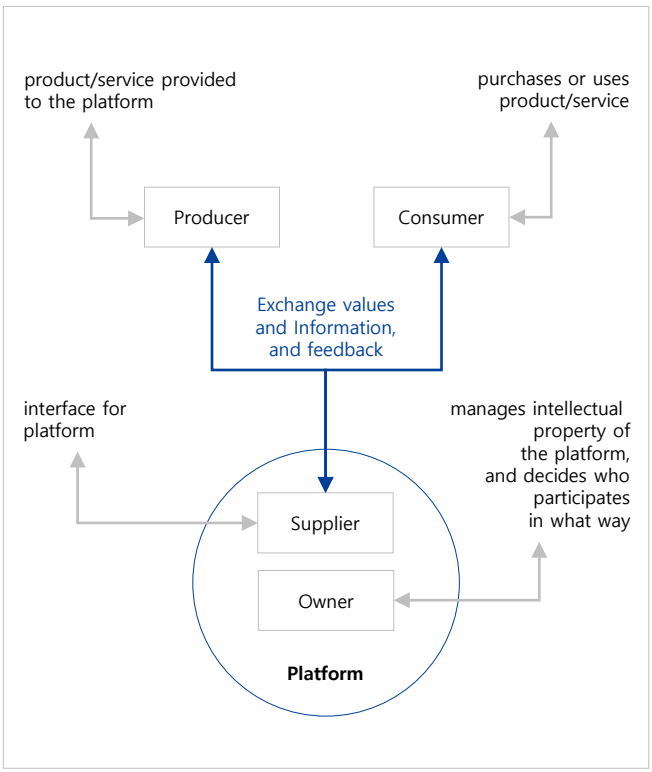
03 MEDIUM blockchain's ecosystem

This chapter describes the key components and value chains of the platform to illustrate how ecosystems can be implemented based on the MEDIUM blockchain platform technology described above. In addition, we will explain the cryptocurrency-based economic system and money flows to be issued in MEDIUM blockchain.

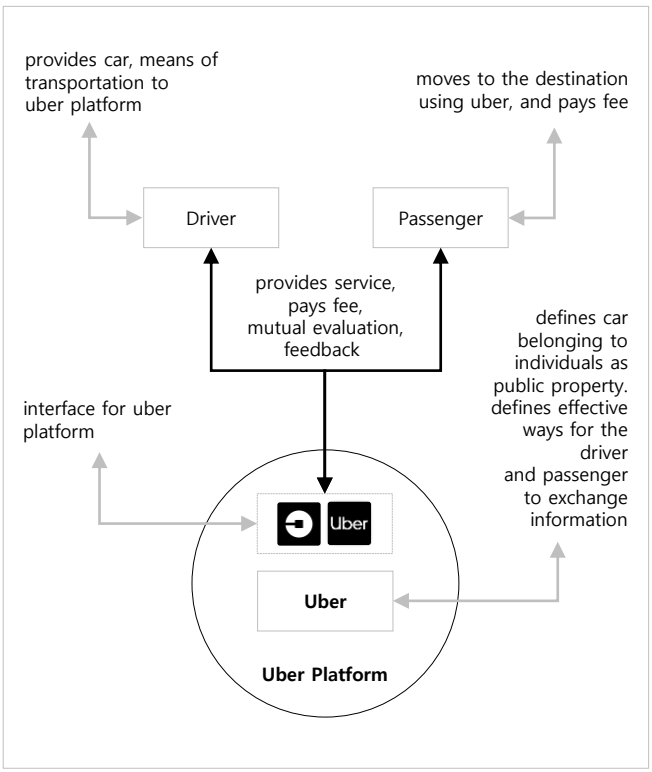
1) About blockchain platform and the business ecosystem

Before explaining the structure of the blockchain platform ecosystem, we should reconsider the meaning of the platform from the modern view that digital business is generalized and think about what value the platform technology should prioritize.

As ICT technology becomes commonplace, at the present time when global business is generalized, a platform is basically a link that enables business integration by making valuable goods interchangeable between producer and consumer. In these platform businesses, platform operators/owners control the intellectual property of the nature and core of the platform, and how the platform is managed, and coordinate the interests of the components. Provider acts as an interface/channel that connects the platform to the user. Producers are those who provide goods and services that can be provided to users on the platform. Taking this as an example of Uber, a global shared platform, the diagram below shows.



[Diagram24] Application pipelines, platforms, and the new rules of strategy[5)]

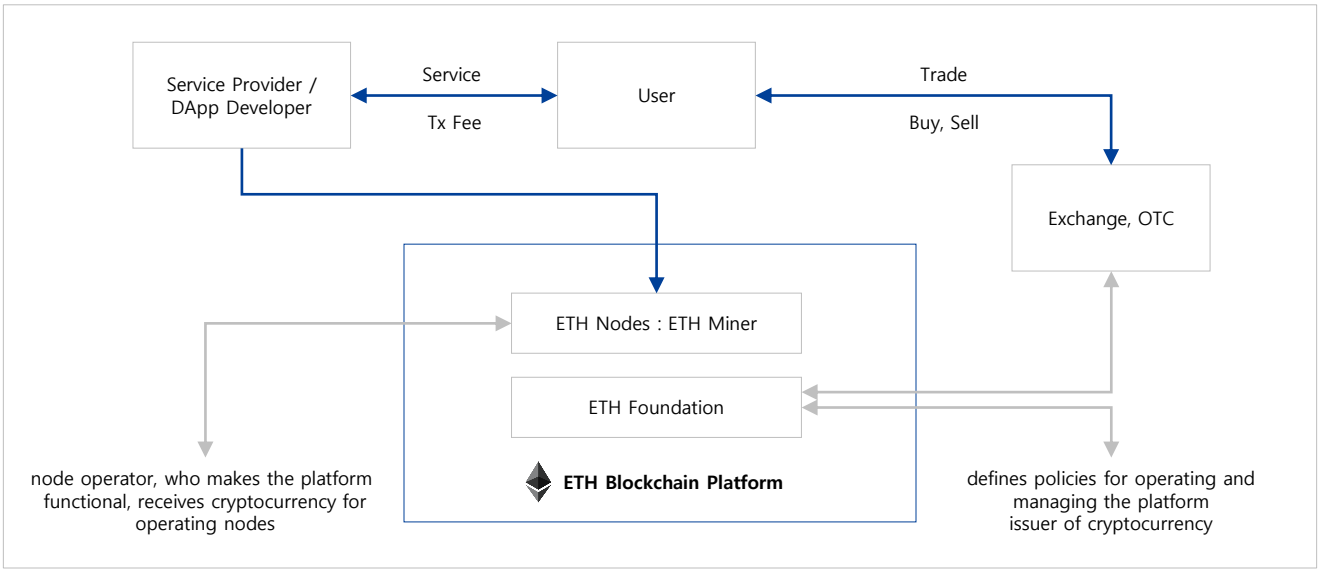


[Diagram25] Key map on platform, supplier, provider, and user on uber platform

5) Pipelines, Platforms, and the new rules of strategy at hbr.org : https://hbr.org/2016/04/pipelines-platforms-and-the-new-rules-of-strategy#comment-section

2) Properties and features of blockchain platform ecosystem

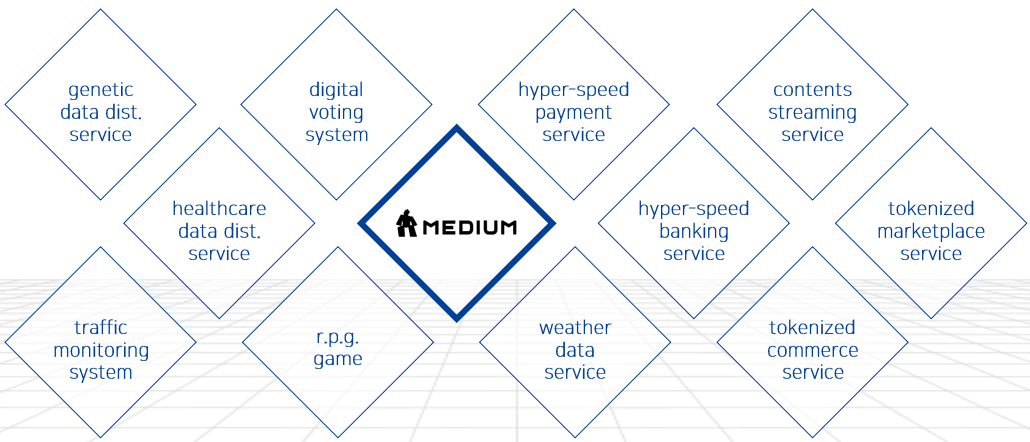
Then, it is necessary to look at how the structure and characteristics of the blockchain platform's ecosystem differ from the ecosystem of the platform business, which is seen in the Uber example above. Etherium was used as an example to help understand.



[Diagram26] Value chain of Ethereum platform's ecosystem

The biggest difference between a blockchain platform ecosystem and a platform business ecosystem so far is that, among other things, each entity's interests are formed based on cryptocurrency. When the foundation defines the operation principle, operation policy, management rules, etc. and issues the corresponding cryptocurrency, the node operators who operate the platform provide computing resources to help the platform operate stably. And cryptocurrencies can be obtained as a reward for the operation of the corresponding node. Service providers/developers can use the platform's resources to develop/operate the services to provide to the users, and the users can obtain cryptocurrencies by exchanging or purchasing to pay the fees (transaction fees) incurred in using the service, or can participate in the operation of the node directly.

3) MEDIUM blockchain platform ecosystem's vision



[Diagram27] Key map of MEDIUM blockchain ecosystem

Various decentralized services, which have been attempted in many R&D since Bitcoin's emergence, have failed to develop further in the development verification phase due to the limitations of the platform's environment and performance. Payment system that require real-time processing and large amount processing, weather forecasts that need to calculate millions of big data in seconds, transportation service, online games that need to process millions of simultaneous log-in requests, and digital voting system, etc. areas that require high performance decentralized system covers all areas where ICT services are currently common.

MEDIUM blockchain platform guarantees ultra-fast performance and the lowest cost environment when all existing ICT services want to implement services using decentralized network resources. We are confident that the high-speed blockchain platform environment will bring innovation in various decentralized service areas on the basis of the new economic system that will be newly created with cryptocurrency.

4) Forms of MEDIA blockchain platform

We will provide the MEDIUM blockchain platform in several formats to address various types of infrastructure environments.

(1) MEDIUM public(permissioned) blockchain platform model

In the public blockchain platform model, the resources of the platform can be utilized in the same way that many other projects generally provide. Because MEDIUM public blockchain platform, as defined in "01-7) MEDIUM blockchain's policies and directions, will be constructed as nodes of MEDIUM in the form of a consortium of operating organizations around the world, permissioned blockchain is the correct expression. However, in order to classify it according to the usage pattern of the user, we will all it public blockchain model. Service providers or developers wishing to utilize the resources of the MEDIUM public network may develop their own services in accordance with the proposed interlocking specifications and SDK.

(2) Cloud-Type blockchain platform model

The cloud-type blockchain platform model is a model that can use the same level of infrastructure as the MEDIUM blockchain infrastructure in the form of cloud service. Since the platform operates on a MEDIUM H / W-based cloud infrastructure, the deployment and other resource management of blockchains on demand can be individually defined and updated through web-based consoles and dashboards, and you can freely create an independent private blockchain platform, a common blockchain platform, a consortium blockchain platform, etc. In addition, since the architecture can be freely defined, it has the advantage of designing governance and control policies that are not dependent on the MEDIUM platform when issuing platform-based cryptocurrency to be deployed.

(3) Private blockchain platform model

Private blockchain platform model is a model that is introduced when it wants to be used by organizations that want to build their own, decentralized network systems without sharing resources with systems in any external environment. In other words, the MEDIUM H/W equipment is placed inside the private network of the organization to operate a separate platform. Organizations can receive direct and intensive technical support related to the platform technology and DApp interlocking from MEDIUM in accordance with the their requirements.

(4) Hybrid blockchain platform model

Hybrid blockchain platform model is a model that can be used in conjunction with the MEDIUM public blockchain model if the organization already has a private blockchain or decentralized service. When an organization wants to use the resources of the MEDIUM public blockchain model despite the fact that there is a private blockchain platform that is operated separately from the external network, the organization can interoperate its system with the MEDIUM public network using a proxy system.

The proxy system is basically produced by MEDIUM and provided with the relevant library, and will be

continuously updated according to the trend of blockchain industry and distribution level. Medium provides the technical support to be fully-customized to maintain consistency with the internal policy of the organization and the platform it is running.

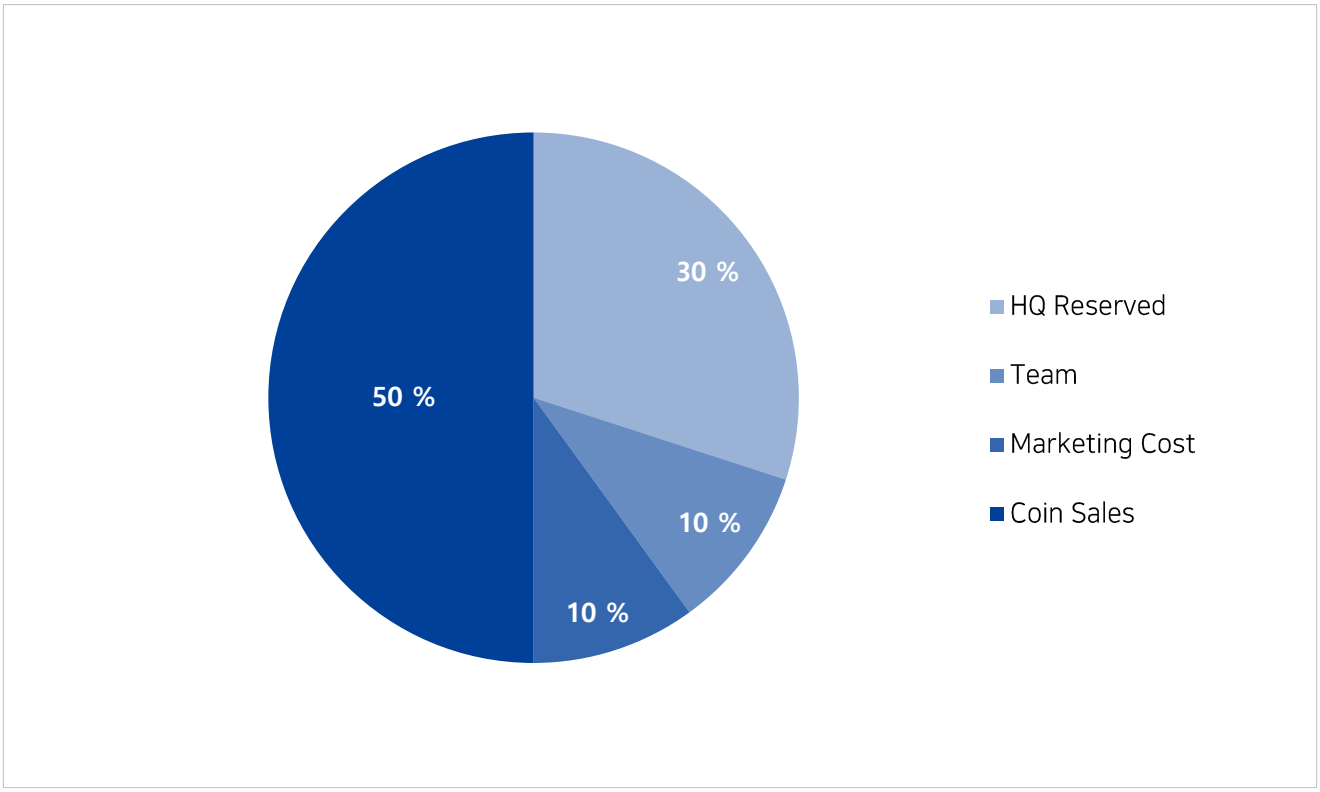
In addition, as mentioned several times earlier, the MEDIUM blockchain platform ensures compatibility with the Hyperledger platform, so if the organization running the Hyperledger fabric-based private platform or DApps needs to use a separate high-speed network, you can freely use the resources of the MEDIUM public blockchain platform by linking with a proxy service.

5) Definition of MEDIUM cryptocurrency – MDM coin

MEDIUM coin is issued with limited quantities with the MEDIUM project release, and it can be used to pay all costs incurred within the MEDIUM blockchain platform and can be used as the platform resource usage fee.

(1) MDM coin information

a. Total generating coin : 1,000,000,000 MDM
b. MDM coin distribution : Coin Sales 50% | HQ Reserved 30% | Marketing Cost 10% | Team 10%

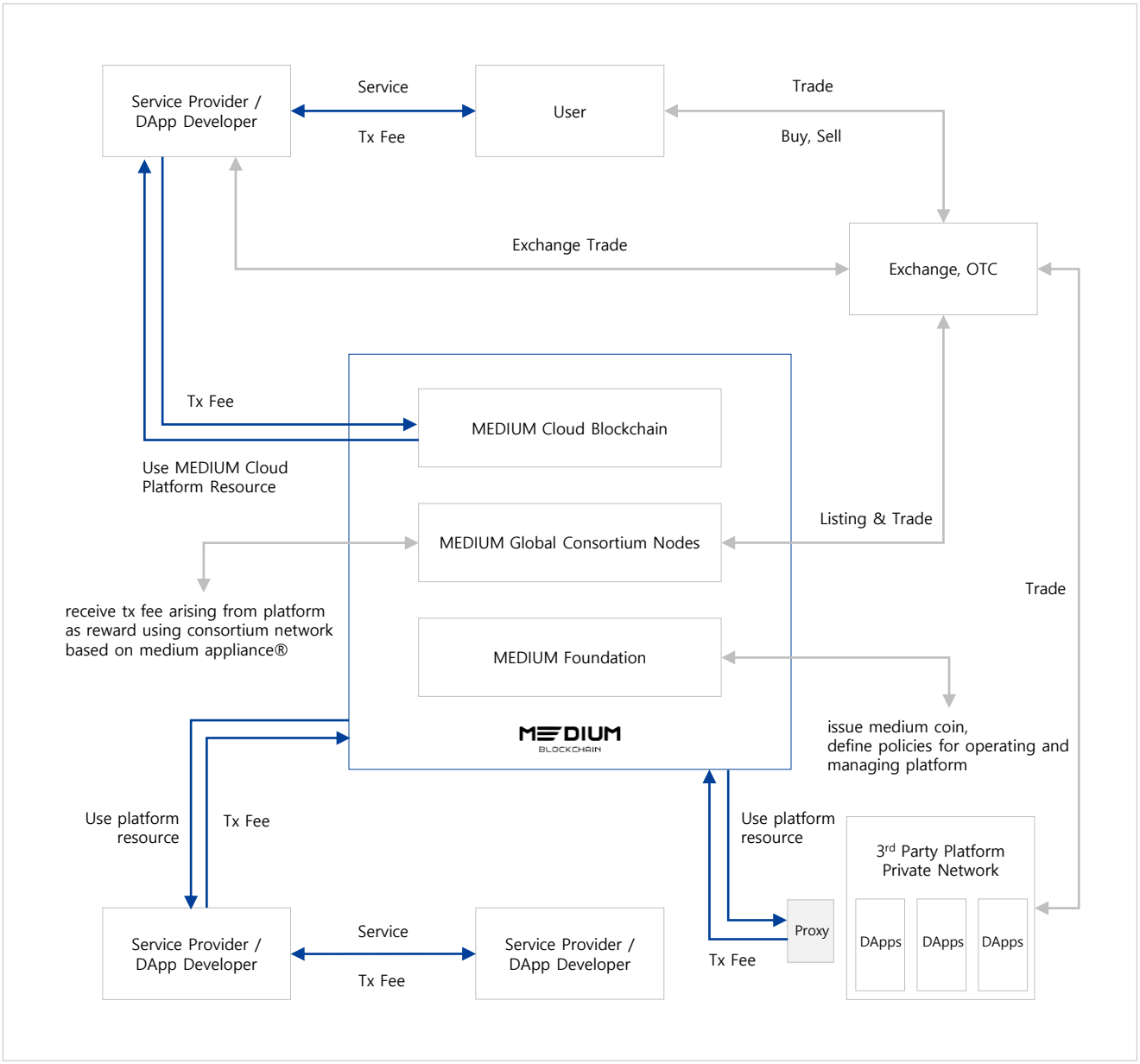


[Diagram28] MEDIUM token distribution

6) Overview of MEDIUM coin / Token economics

(1) MEDIUM coin / Token economics introductions

MDM token economics will be applied to all types of platforms except private type, which is the third of the four types of delivery methods described in section 3- (4) above, and will begin with the integration of the MEDIUM consortium network. To use the resources of the MEDIUM consortium network in all types of services except private type, payment must be made with MDM tokens, which are paid to consortium members.



[Diagram29] MEDIUM blockchain coin / Token economics chart

(2) MEDIUM platform network usage fee

Usage fee have to the paid in proportion of use of all types of service running on the MEDIUM platform, and every purchase occurring inside the platform can be paid by MDM token. In MEDIUM platform, the network resource usage fee will always be calculated in TPS unit, it will follow the information tailored to the global average transaction information of MDM token at the moment of settlement, in order to prepare for the volatility of MDM token's price, we will use the key currency of global fiat market, which is the dollar(USD) as the standard for the network usage fee.

(3) MEDIUM platform models' policies

The policies applied to users by MEDIUM platform are as follows. This policy is a guideline at the time of distribution of this paper, and detailed policy and governance rule will be distributed separately when MEDIUM's mainnet is released.

* MDM token hold
Policy in which user who selected model used for each platform must retain certain number of MDM tokens for certain number of days to use the system

Category	Private	Cloud type	Public (Permissioned)	Hybrid	Participation in consortium (node)
Introduce MEDIUM H/W	Required	N/A	N/A	Choice	Required
Co-Location service of data center	Choice	N/A	N/A	N/A	Required
MDM token hold *	To be agreed	Applicable	Applicable	Applicable	Required
Independent platform (governance Rule)	Possible	Possible	Impossible	N/A	N/A
Individual consortium	Possible	Possible	Impossible	Impossible	N/A

[Table04] Policies for each MEDIUM platform model

04 Reference

[1] Harish Sukhwani, Performance Modeling of Hyperledger Fabric (Permissioned Blockchain Network) Chrysoula Stathakopoulou IBM Research – Zürich, On Scalability and Performance of Permissioned Blockchain Systems

[2] Linux Foundation, "Hyperledger Architecture", Linux Foundation, 2017

* Other reference

1) Accenture 2018 - Connecting Ecosystems: Blockchain Integration

2) Performance Modeling of Hyperledger Fabric (Permissioned Blockchain Network) - Harish Sukhwani

3) EY GLOBAL BLOCKCHAIN BENCHMARKING STUDY - Dr Garrick Hileman & Michel Rauchs 2017

4) hbr.org - Pipelines, Platforms, and the New Rules of Strategy

5) IBM Research Blog - Behind the Architecture of Hyperledger Fabric