Hdac Technical Whitepaper

HdacTech edited this page a day ago · 45 revisions

Hdac : Transaction Innovation - IoT Contract & M2M Transaction Platform based on Blockchain

Official Version 1.0.2 | Copyright @HdacTech.AG November 2017.

Please contact the authors with questions or comments at: support@hdac.io

▾ Pages 2

Home

Hdac Technical Whitepaper

Clone this wiki locally

https://github.com/Hdactech

Clone in Desktop

Executive Summary

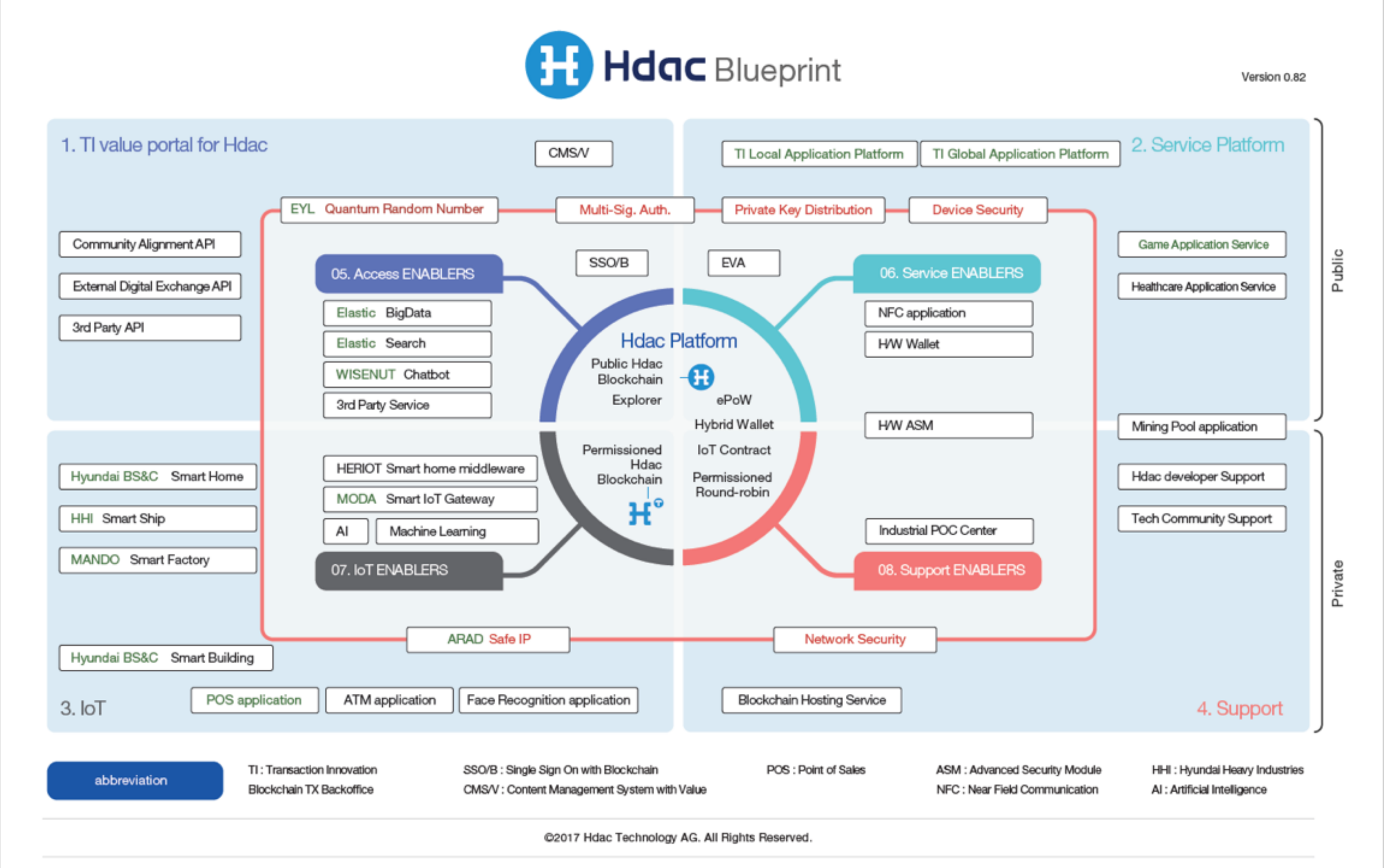
The IoT industry is on the verge of exponential growth. The Hdac platform provides the missing building blocks needed to enable IoT environments to thrive:

1. Authentication - devices can be correctly identified by one other
2. Mapping - once identified, they can connect seamlessly
3. Machine to Machine transaction - devices can then bill each other

Hdac will solve these three issues by combining blockchain and IoT, allowing automated, machine-to-machine, ultra-low cost transactions between IoT devices that are authenticated, mapped and verified through the blockchain.

In its architecture the Hdac system uses a combination of public and private blockchains, which allows for previously unattainable transaction speeds. The technology will use quantum random number generation to secure these transactions.

The Hdac system will ultimately ensure the efficiency and security of exponential growth of the IoT industry.



Introduction

Society in the future will be “hyper-connected” and digital innovation will be continuously reintegrated into global economic systems. New technology will be enabled by an appropriate combination of blockchain (which has its value as a cryptocurrency) and the IoT. The market and consumers will demand more reliable and more affordable industrial transactions. This will lead to the development of Machine Currencies which can be implemented using and within hybrid blockchain technology.

We believe that the future digital world will be a world where the Hdac platform operates a highly reliable blockchain network that can conveniently utilize the services of the world’s numerous IoT devices. It is said that “the currency of the new economy is trust,” and so it is paramount that new technologies be built on trust. The Hdac platform will be a key tool for implementing a more reasonable and efficient transaction system as the worlds of blockchain and IoT converge.

The technological philosophy underpinning Hdac is to dramatically improve M2M transaction environments in daily: economic activities should all be seamless and easy transactions. In addition, we believe it will be possible, using our technology, to promote reasonable consumption and accurate, smart management for all communication and utility expenditures.

Blockchains and cryptocurrencies are expected to serve as reliable, secure, and efficient transaction instruments for the Internet of Things [IoT] environment in the near future. Machine-to-Machine [M2M] transaction will be implemented with peer-to-peer [P2P] transaction that improves upon the high cost and low efficiency structure of the current centralized billing / deposit / settlement system used in such industries as apartment management and mobile billing.

However, it is also necessary to identify (authenticate) and connect (map) to the appropriate device to ensure everything is in a connected environment with pre-approved privileges, and to provide identification functions to handle requested tasks securely. These changes enable a payment culture that allows micropayments and transparent settlement in all economic activities, such as when purchasing consumer goods or using public services in daily life. For example, consumer goods can be purchased and consumed in needed quantities only. Transactions will be immediate with low transactional cost or risk for both private and public goods such as electricity, water, cable TV, and the Internet.

Society in the future will be “hyper-connected” and digital innovation will be continuously reintegrated into global economic systems. New technology will be enabled by an appropriate combination of blockchain (which has its value as a M2M transaction) and the IoT. The market and consumers will demand more reliable and more affordable various types of transactions. This will lead to the development of M2M transaction which can be implemented using and within blockchain technology.

Hdac Private Blockchain [Hdac*T], a blockchain based smart transaction method on the Hdac platform, is designed to perform a given task under the various commanding conditions in the IoT environment. Hdac*T provides these M2M transaction functions and a simple transaction service environment, and with the rationality and efficiency that the Hdac platform pursues, it will be the platform of choice for use and control with IoT devices.

In addition, Hdac will evolve into a hybrid blockchain platform by providing a hardware wallet for user security and transaction convenience in service of the aforementioned communication and transactions between IoT devices.

Blockchain and IoT

The Use of Blockchains to Support IoT Applications

In an environment such as a smart home or factory, various devices equipped with sensors, which are closely interconnected using a private blockchain, can be configured to operate more safely and reliably in accordance with each other’s conditions. A private blockchain is configured to perform not only user authentication but also mutual authentication between devices, generating and securely recording operation details and scenario-based IoT contracts.

We are creating a reliable ecosystem in which transaction services run across the general Hdac space and the private, purpose-built objective blockchains by configuring the private and public blockchains so they are interconnected.

The use of private blockchains is only practical if they are able to interact with a public blockchain which is already operating. In this regard, we provide Hdac ? a platform and cryptocurrency-enabled public blockchain that can be effectively used with multiple private blockchains. In other words, with our blockchain-by-use, transactions are possible beyond the P2P settlement of the public blockchain. In a controlled private blockchain network, we implement Hdac*T for mutual contracts and transactions between IoT devices, thereby enabling more accessible, reliable, and secure consumption and M2M transaction processes.

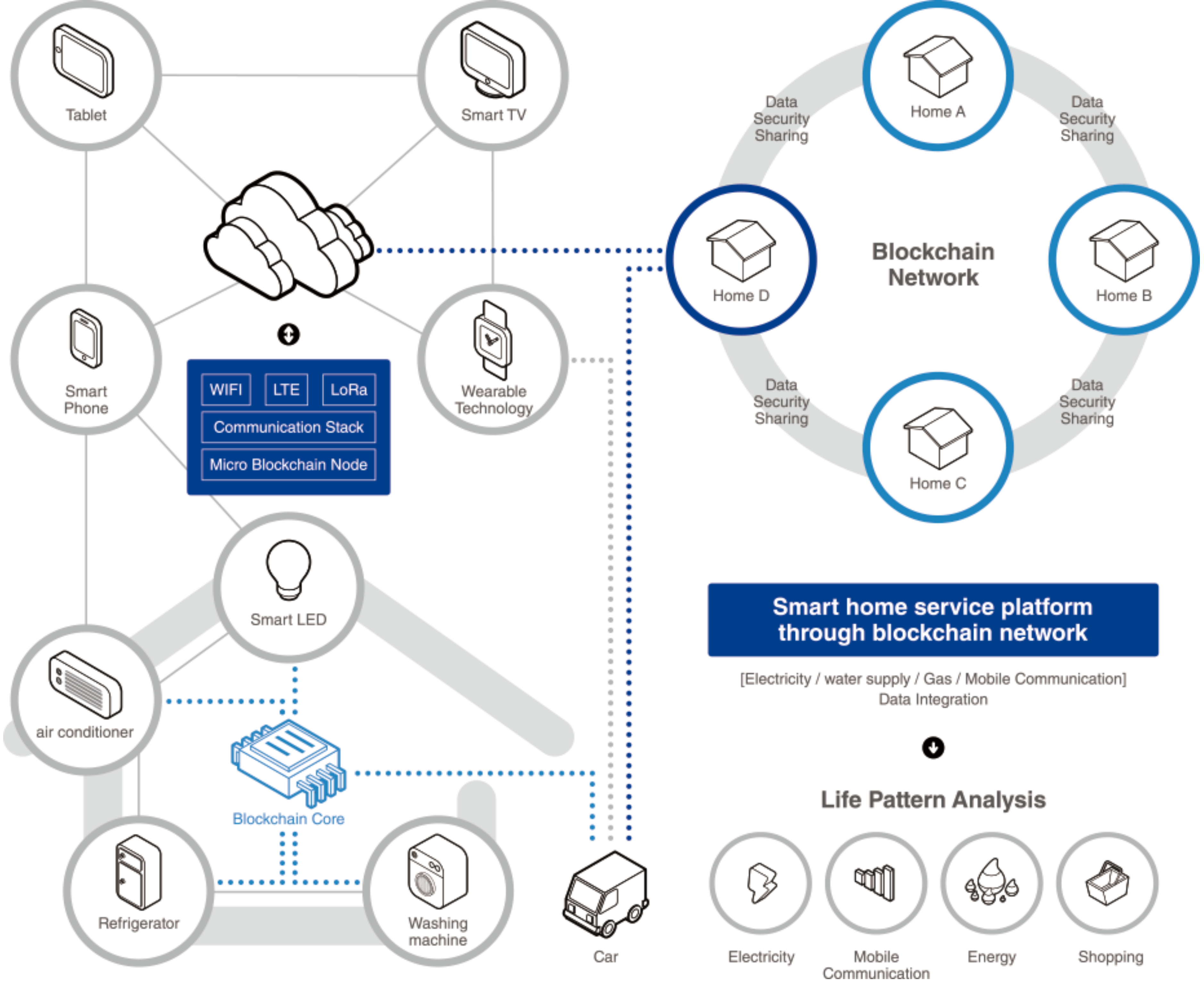


Figure 1. Example of private blockchain enabling IoT usage

For example, suppose that a user wants to operate a device within a specified capacity or budget. The user sets the designated value (capacity or amount; here, it refers to IoT contract value) in the control device mounted on a smartphone, a computer, a smart TV or a remote control and transfers the data to the corresponding device. Then, the measurement data processing part of the device transmits the IoT contract value to the measuring device and starts the operation. At this time, the activated device will operate until it transmits a signal indicating that the specified IoT contract value has reached the level as indicated by the measuring device. The operating device transmits data when a specified value is reached, or when the user control device requests confirmation of the current operating status so that the user can confirm the data. At this time, an authentication process is required to confirm communication processes among the user control device, the operating device, and the measuring device. If it is not an authenticated device, it can adopt a mutual authentication scheme that cannot send or monitor the IoT contract. In addition, an authorized IoT contract can be used to make a

M2M transaction and, in the case of a private blockchain, a user defined Hdac*T can be used as a transaction to activate the IoT device.

User defined Hdac*T can be assigned attributes to make transaction only for specific purposes in an IoT contract, and can prevent the user from being diverted to unwanted devices or uses. This plays a big role in providing transparency of using costs while maintaining the security described above. For example, Hdac*T can be a control method for specific uses under specific conditions such as shutting down electricity and gas for safely evacuating residents when an earthquake or a fire incident occurs.

Integration between Blockchain Networks

How Integration between Public Blockchains can be used?

As initial blockchain technology is becoming popular due to its features of decentralization, transparency, usability, and reliability, the applicability of the blockchain is expanding across industries such as cryptocurrency, attendance verification, forecast markets, and international finance. Therefore, as the amount of transactions and data increases, it is necessary to consider a case wherein public blockchains will exceed their natural capacity.

Connections between public blockchains are already implemented by exchanging data through exchanges. That is, in the case of a registered blockchain in exchanges, exchange can be performed in such a way that the exchange performs relaying. The advantage of this approach is that people can easily identify and use services because they are done in the same way as exchanges between fiat currencies such as the Korean Won and the US Dollar.

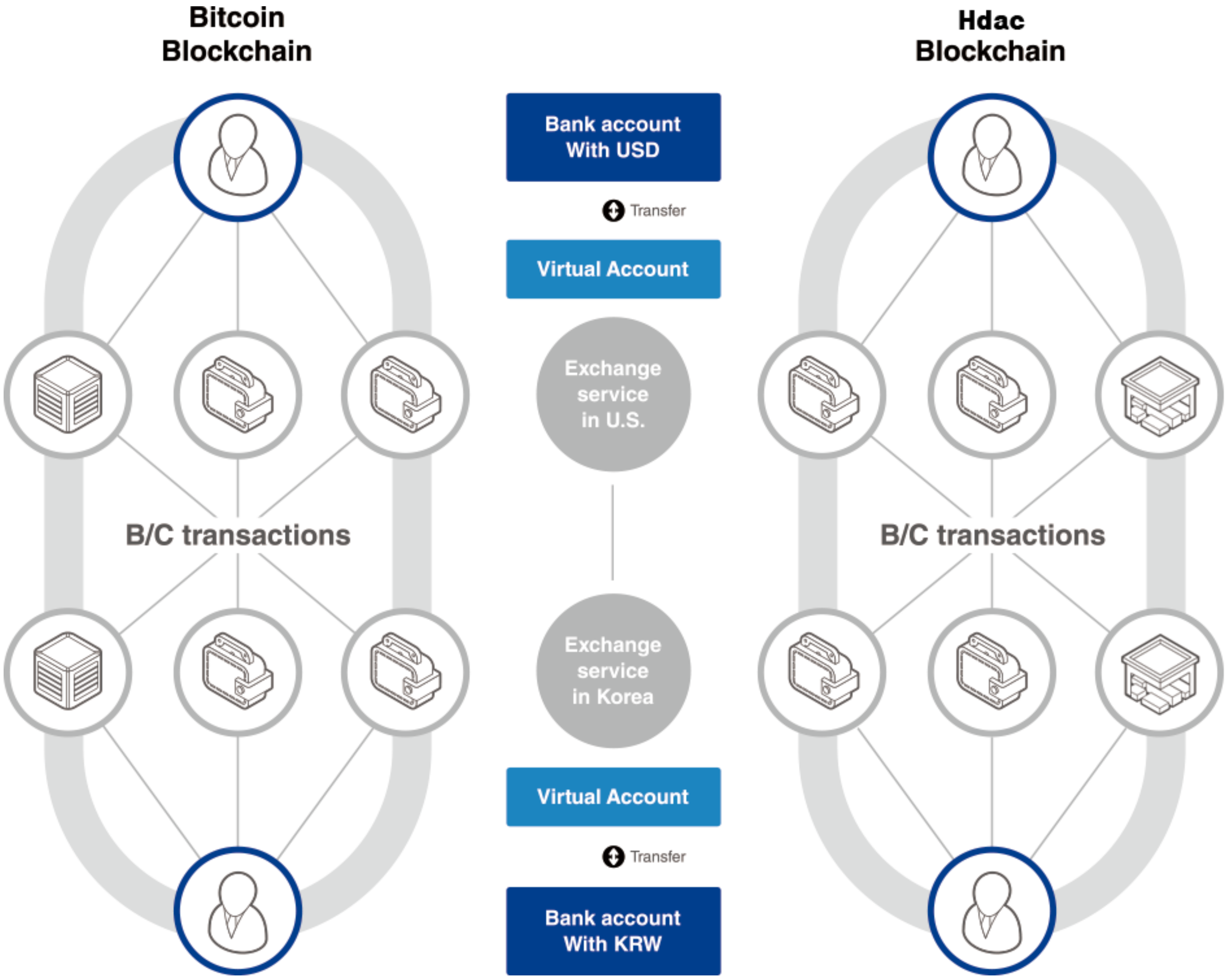


Figure 2. Example of Integration between public blockchains

Public blockchains can also can be linked hierarchically. For example, there are bottom-level blockchains that can be voted on by district or by county, and the results from these are integrated into a mid-level blockchain. In this case, the mid-level blockchain is the scale of a city/province, and can have multiple bottom-level blockchains. In other words, a summary of the transactions collected on the bottom-level blockchain is transferred to the mid-level blockchain. The upper blockchain can be regarded as a structure in which information of all bottom-level blockchains is integrated with a blockchain of a national scale. Although this is just a simple example, it can be applied in various forms on a blockchain network in the form of a tree.

In this specific case, interworking between public blockchains can be interlocked through a separate service acting as an exchange. And this formation can be a chaining of the blockchain.

Integration between Public and Private Blockchains

A private blockchain network or a permissioned blockchain is a blockchain with access privileges. Its configuration means it may not be accessed by every node freely unlike a public blockchain. Therefore, to access a private blockchain from a public blockchain, a bridge node or a relaying intermediary is required. This bridge node must have all of the configuration information of the private blockchain, to allow it the same level of access as its private equivalent whilst allowing it to post to the public chain. In summary, the private blockchain can be accessed only when the administrator of the private blockchain grants access through pre-authentication and registration.

Alternatively, in the case of a specific transaction, the administrator can grant a separate privilege and send it to the node or device. To use a private blockchain, fundamentally the user must be registered after the same authentication with that private blockchain.

In terms of financial transactions, when there is a transaction between Bitcoin public blockchain and Hdac private blockchain that does not change the value. Hdac*T transaction may possibly be used within a specific enterprise or for a specific purpose. In this case, the exchange ratio between those two can be determined/exchanged through the exchange.

In order to find out ways to effectively deal with transactions generated by large-scale IoT devices, the Hdac team have investigated IOTA's transaction processing structure/speed and Ethereum's next generation network. In our test network, making large transactions of tens of thousands, to hundreds of thousands of transactions per second, has proved that only a limited number of transactions were processed, depending on physical network speed/physical computing performance. Therefore, the best solution for managing high levels of transactions is processing with multiple, separate private blockchains and integrating the information through a separate root blockchain.

In particular, public blockchains in a global environment have very limited transaction speeds (Bitcoin=about 2 tx/sec and Ethereum=about 5 tx/sec) due to network problems and block synchronization problems for many nodes. Hdac is also unable to implement the optimal speed in the global internet environment, due to the changes of the network speed over time and delays for block synchronization. Therefore, in the future, a large transaction processing blockchain may be a network of blockchains of a hierarchical or distributed structure composed of multiple private blockchains for each purpose. We will continue to research and work to implement this type of blockchain, and strive to develop an entire blockchain ecosystem by sharing it online as the results are available.

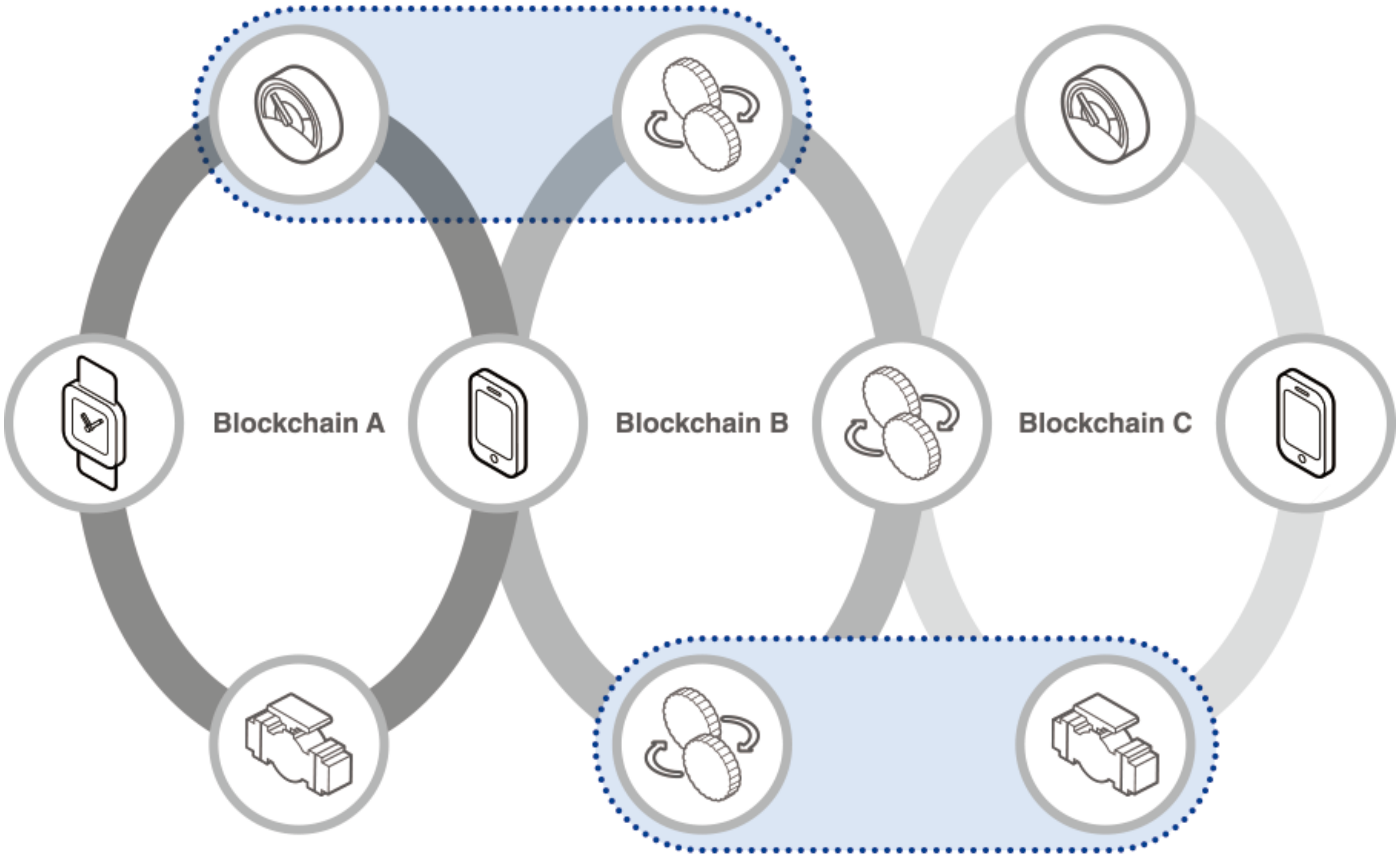


Figure 3. Hierarchically integrated blockchains

IoT and Security

ICBM (IoT, Cloud, Big Data, and Mobile) is regarded as the promising core technology of the next Industrial Revolution in the global industrial market; the IoT is expected to not only expand access to this market, but also to increase efficiency and convenience for users with various economic values.

However, in order to achieve such a positive outcome, the connectivity between devices and reliability must be ensured. In other words, eliminating the distrust and security threats implied by the convenience of Internet connection is the top priority.

The most attractive attributes of the IoT are that it enables devices to be both smart and connected. Devices that were not created for use on the blockchain will be neither smart nor connected, and all the threats and vulnerabilities that may occur in the existing Internet environment can be inherited. Meanwhile, apart from the security vulnerability due to external infringement, data collected in real time on an Internet-based service can lead to the invasion of privacy, and connection without security may be a social disaster. It is necessary that the basis of this hyper-connected society is able to contract and operate between a reliable P2P network system and the IoT devices we will be relying on everyday. Based on this, it has the capacity to evolve into a network that can support an ultra-advanced M2M transaction system which can function securely, reliably, and independently with customizable inputs from users.

Transaction Innovation & M2M Transaction

One of the most innovative aspects of the next Industrial Revolution is the IoT, which refers to intelligent technologies and services that connect all things based on the Internet and communicate information between people and devices, as well as between different devices. However, technologies such as networking, which connects devices to one another, processing technology suitable for various services, interface technology for communication, and distributed processing technology for storing and processing large amounts of data, are essential to the IoT, and all require security technologies to prevent against hacking and information leakage.

While various services based on this kind of Internet technology are emerging, many devices on the blockchain are operated by an IoT contract, and it is expected that this service will be possible in various industries. In particular, IoT contracts not only control devices, access, and help communicate between devices, but also assure anonymity, with all transactions recorded in the ledger. The recorded ledger is used as learning data for machine learning. The cost saving that this IoT big data is expected to provide through artificial intelligence [AI] is the ultimate goal of the IoT blockchain ecosystem.

Securing Trust between IoT Devices in the Blockchain

The connective structure of the IoT and the network structure of blockchains are very similar, as the Figure below shows.

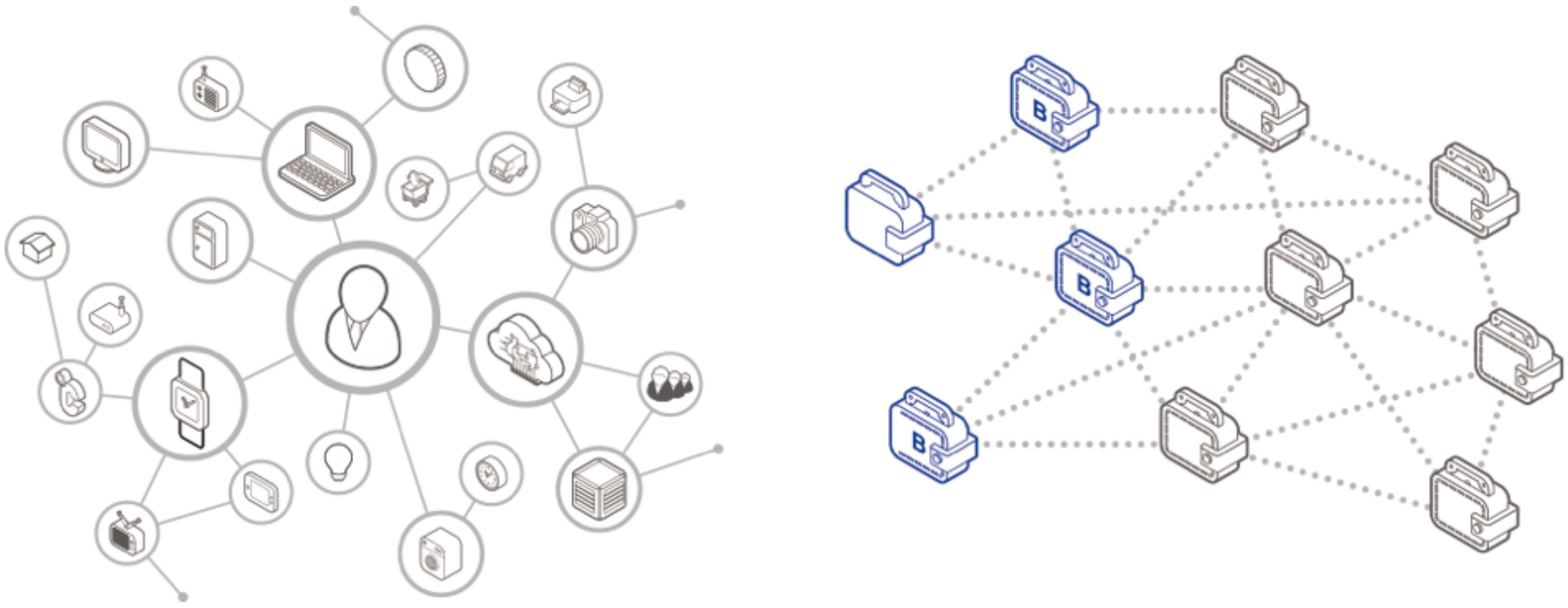


Figure 4. Comparison of network structure between the IoT and blockchains

Integrating blockchains with the IoT makes it easy to implement confidentiality with integrity, a necessary condition for ensuring reliable connections and secure processing between devices. To do so, the connected devices respond to fabrication and modification attacks, thereby enhancing the mutual reliability of communication. In particular, the blockchain contains an ability to cope with external attacks through complex mathematical encryption of the transaction ledger contained within the block. In addition, the blockchain uses a decentralized rather than centralized method, which has the advantage of making it difficult for hackers to determine the attack target. These features minimize the impact of individual attacks on IoT devices to the entire device.

Reliable services provided between IoT devices can be summarized as follows:

- P2P and a decentralized structure distributes attack targets, making it difficult for the hacker to identify individual users as targets.
    - In the case of a private blockchain, if the development of distributed computing becomes limited, the security problems can be solved by protecting the network through the “Safe IP” method, whereby the threat of external attacks is much diminished.
- It is possible to engrain transparency in all aspects of transactions by recording them on a distributed ledger like a blockchain, where they are readily accessible for future reference should the need arise
    - This guarantees the integrity of the transaction details to respond to counterfeit and tampering attacks, minimizing dispute resolution costs as all participants prove transaction details.

- Authentication and authorization procedures are required for IoT devices that are the subject of transactions.
- In the case of a public blockchain, it is possible to increase the efficiency of construction and maintenance according to the distribution. In addition, the widespread decentralization of the public ledger improves efficiency by reducing the transactional costs, therefore more efficiently allocating public and private resources.

As a result, the network using the blockchain will provide a reliable environment for both the administrator and the user to exchange a wide variety of data and value.

Features of Hdac

Main Features of the Hdac Platform

The main features of the Hdac blockchain are as follows.

Custom DAC can be created and used without limitations, and the name of the asset will be defined or freely created and distributed by an authorized administrator. This asset can be circulated and used similarly to the existing native coin.

In addition, assets that are generate for a particular business or for specific purposes may be exchanged with native coins at an appropriate ratio as needed.

There are various rights management functions, and an administrator who builds the first blockchain node can grant authority to other nodes. Types of authority can be access rights, permissions to transmit and receive, mining rights, rights to generate assets, etc., and can be changed effectively during operation.

The Hdac private blockchain provides convenient installation and configuration functions, and the blockchain can be easily configured as defined by the user. In addition, the new node configuration can be done simply with only a single line command to participate in the existing blockchain as a full node and all configurations are automatically copied and shared. In the case of a private blockchain, this can support mining in a more efficient way, as opposed to the relatively wasteful approach like a proof of work [PoW] system.

Enhanced multi-user signatures are provided to support services such as secure P2P transaction. It also provides the ability to communicate by creating encrypted channels between two specific users. Together with this, we are also planning to provide IoT control and functions for the private blockchain specialized in various application fields and ideas and infrastructure for connecting blockchains. Details related to the IoT are specified in the “Hdac Technology Roadmap” on page 21.

Hdac is based on blockchains and accommodates all the features of a typical blockchain. The limitations of the blockchain itself are evolving one by one over time. Hdac differs from other platforms based on blockchains by having modified or supplemented several functions to distinguish it in terms of capacity, security, functionality, and speed.

The limited capacity of the block and extra data part of the existing blockchain was modified to be used flexibly in the data loading part. This enables various applications using blockchains.

In the case of a private blockchain that is backed by the Hdac platform, security must be enhanced. By generating random numbers to create identifying keys through a quantum random number generator it is possible to eliminate the possibility of hacking through number pattern analysis, thereby greatly improving the security of the technology and associated transactions.

In addition, we propose an ePoW algorithm for the consensus algorithm to develop the existing PoW scheme to induce efficient use of energy and equitable distribution. Also, by adding a permission concept that can grant administrative rights, only a specific user in a private blockchain can participate as a full node of a blockchain. If the existing platform uses common units, Hdac can construct multiple blockchains according to usage, and furthermore, provides a service model that can be used to create units.

We have examined a number of blockchains that are suitable for implementing IoT environments developed for real-time processing. It is difficult to implement this with Bitcoin. Ethereum has a model more useful for IoT environments, but most devices are developed mainly in C, so we examined blockchain in C. However, it can be developed to be compatible with Ethereum in the future. IOTA has the potential to cope with large volumes of transactions, but it is not a standard blockchain technology that we are targeting, and therefore we excluded it. After reviewing many other platforms, we chose MultiChain, which can effectively implement private blockchains based on the most commonly used Bitcoin.

Hdac is based on and improved from MultiChain, which is a blockchain improved from Bitcoin. Hdac has specifically explored blockchains to efficiently support IoT environments and to provide various services quickly and effectively to private blockchains. We will also set up the appropriate blockchain as MultiChain and make improvements. Therefore, Hdac has some of the characteristic of bitcoin blockchain as well as MultiChain's optimized characteristics for private blockchains. Hdac will provide a basis for acting as a platform for the IoT. It can be applied to various service fields such as IoT, distribution, logistics, and public data management based on fast transaction processing speeds and transaction scalability.

Bitcoin generates one block every 10 minutes, and Ethereum generates one block every 12 seconds. When considering the time that is shared on the network, it takes one to two minutes or more to check the outcome of the transfer transaction.

Considering this, Bitcoin processes about 7 transactions per second [TPS] and Ethereum processes about 25 TPS. In particular, Bitcoin is limited to a maximum of 1MB in the current block size, and an alternative is proposed to increase the block size through SegWit2x.

Features	Bitcoin Blockchain	Hdac Blockchain	Ethereum Blockchain
Main Features	Financial Transactions (Bitcoin script)	IoT friendly blockchains, Public/Private blockchains	Smart Contracts (Solidity, Serpent etc.)
Consensus Algorithm	Proof of Work	ePoW, Trust-based	Current: Proof of Work Future: CASPER PoS
Transaction Speed	7 tx/sec	~160 tx/sec (public)* ~ 500tx/sec (private) 1000 tx/sec (target)	25 tx/sec
Block Time	10 minutes	3 minutes	12 seconds
Block Size	1MB	Dynamic (Max. 8 MB)	Dynamic
Extra Data	80 Byte (OP_RETURN)	Dynamic (Max. 4 Kb)	Dynamic (5 gas / byte)
		Private/Public	Public blockchain,

Topology	Public blockchain	blockchains, Permissioned blockchains	Permissionless blockchain

* This figure can vary depending on server performance and network environment.
Table 1. Comparison of cryptocurrency properties

Hdac has compensated for these shortcomings and allocated the block time to three minutes, accounting for the lagged traffic speed of the Third World. The maximum block size is up to 8 MB and is variable.

The reason for this figure is that the average Internet traffic speed in the Third World is only 1~2 Mbps. Therefore, if Hdac can accommodate only one fraction of this speed, it is suggested to create an environment that can operate a full node of the Hdac blockchain. Transactions through general wallets are also available in lower traffic environments. Testing in a limited internal environment has shown that stable transactions can be achieved in large transactions of about 20 times or more, which is closer to the theoretical value when compared to Bitcoin.

Hdac provides a way to store large amounts of additional data in a transaction as an IoT-oriented blockchain in the future. Also, transaction size can be dynamically adapted if required for IoT security and application service expansion.

Consensus Algorithm

Blockchain has the necessary basic conditions for all the nodes participating in the network to agree on in the step of verifying that the block is valid for connecting a new block. All participating nodes (full node) should be able to identify the same result with the same procedure, and all verification processes must determine the same value. In addition, the determined value should be that proposed by a specific node.

Hdac blockchain is based on the PoW method as a public blockchain. It also supports the mining method for a trust-based private blockchain: a trust-based consensus algorithm for a permissioned blockchain.

Here, the task of creating a block is referred to as "mining," and the nodes participating in mining are referred to as "miners" or "mining persons." When an Hdac transaction begins, it broadcasts to the miners informing them about the transaction and encouraging participation. Miners then perform arithmetic calculations to verify the generated block. The consensus algorithm of blockchain includes PoW, proof of stake [PoS], and delegate proof of state [DPoS]. Such a consensus algorithm determines those who will generate a block through performing a calculation process that takes a certain amount of time amongst numerous participants.

This consensus algorithm wastes energy by consuming hashing power to obtain one block compensation in the competitive mining process. In addition, the PoW or PoS method has the problem that the greater the hashing power, or more stake, the more the accumulation of compensation or wealth can be concentrated in one place. In fact, mining is concentrated in certain mining pool areas.

Hdac uses ePoW as a consensus algorithm for creating new blocks and connecting them to the blockchain. ePoW refers to "PoW based on equitable chance and energy-saving." The Hdac algorithm considers these two as its basic philosophy.

The ePoW consensus algorithm can reduce the number of nodes participating in PoW and motivates the participation of multiple mining nodes. As a result, we intend to prevent energy waste due to excessive hashing power for mining competition and distribute equitable mining opportunities.

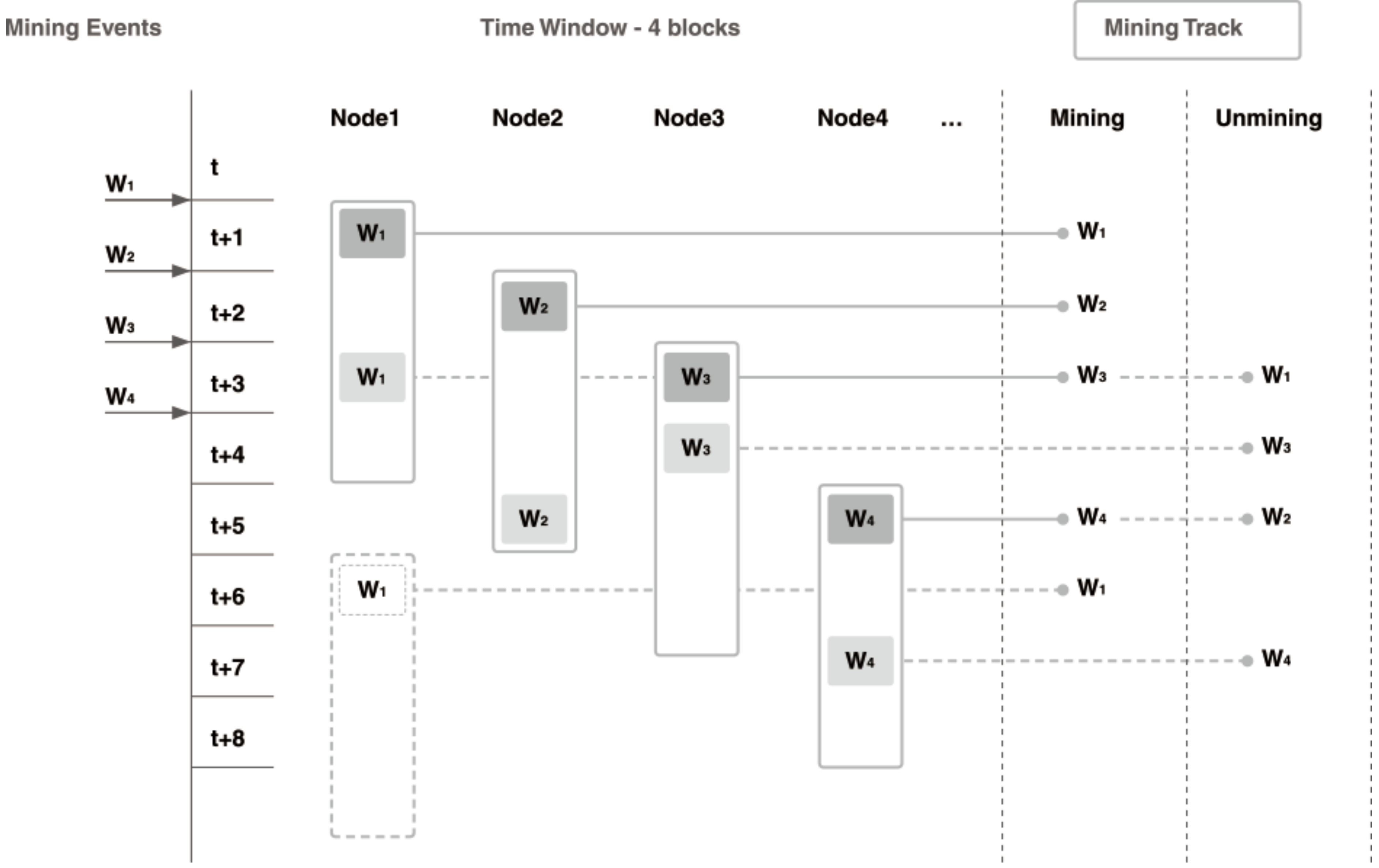


Figure 5. ePoW consensus algorithm

Hdac ePoW is a consensus algorithm that reduces the mining monopoly by applying the block window concept. It reduces the wasteful energy consumed in the hash calculation by avoiding spontaneous mining attempts during the block window application period once the mining is successful. If a node succeeds in mining, no new block can be mined during the block window application period. Even if a greedy node neglects this mechanism and succeeds in mining a new block, it will not be recognized as a valid block in the entire Hdac blockchain network, thus eliminating the need to try to find an invalid block.

The block hash must satisfy the data specification according to the degree of difficulty and should not be within a given block window (time spacing). This block window size can be expressed in the form of a time function, Ws = f(t). “F(t)” is a function that increases in proportion to time, and therefore the window size gradually increases with time. This means that there is a great opportunity for early participants, and over time, it becomes increasingly difficult for certain mining nodes to monopolize mining and more equitable distribution can be achieved.

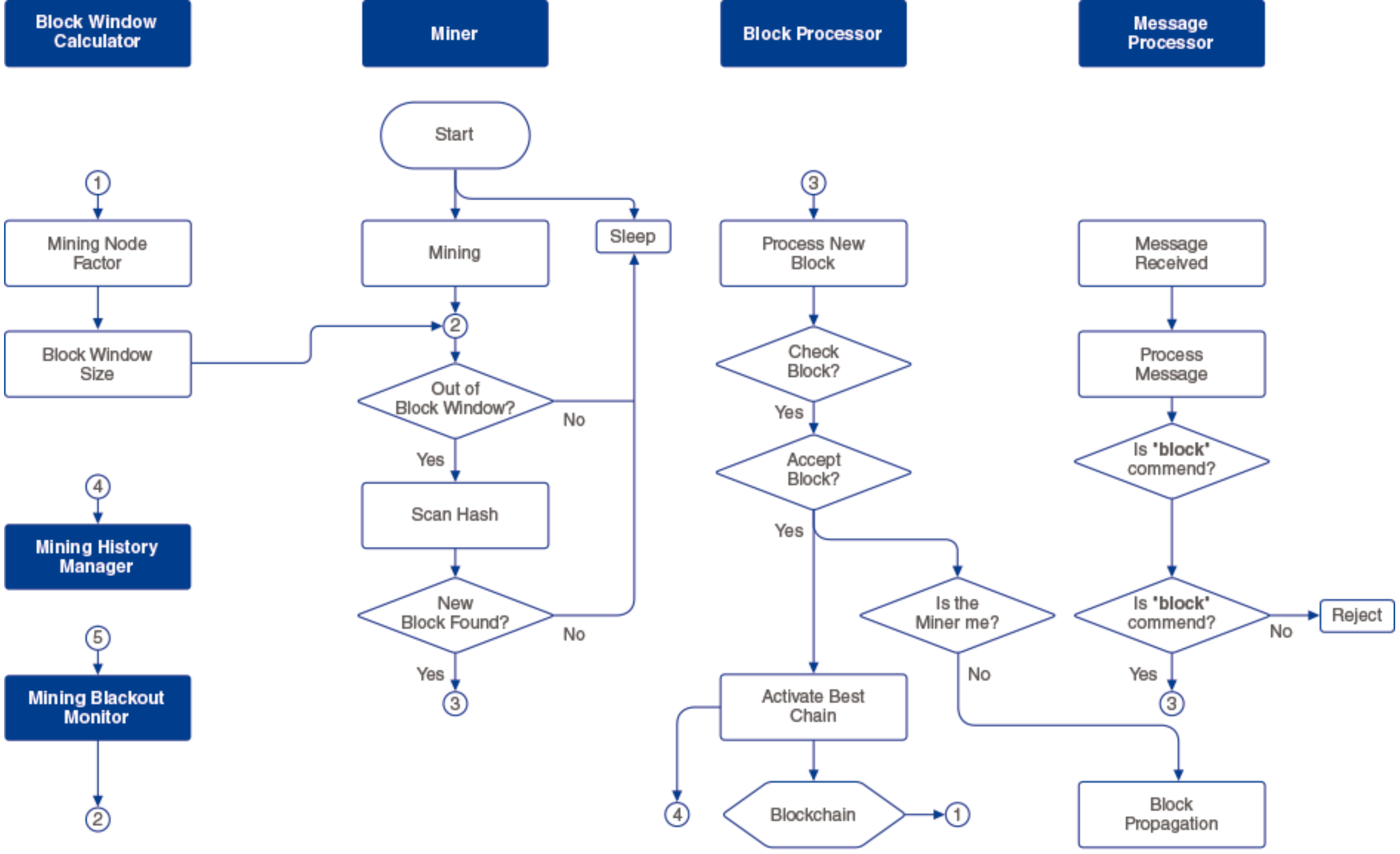


Figure 6. ePoW flow chart

Figure 6. ePoW flow chart

The ePoW block window is a system that gives certain constraints on mining attempts after succeeding in mining in a certain PoW cycle. The block window size (Ws) is defined as, f(t) = [(N*0.7) x (cumulative number of blocks currently (t))] / (cumulative block number for 10 years (tm)), and the node factor (N) is calculated from the list of recent successful mining nodes. The reason for the arrival time of the maximum block window size (Wm) being 10 years is because it is set to reach the point of more than 80% of the total block generation by that time.

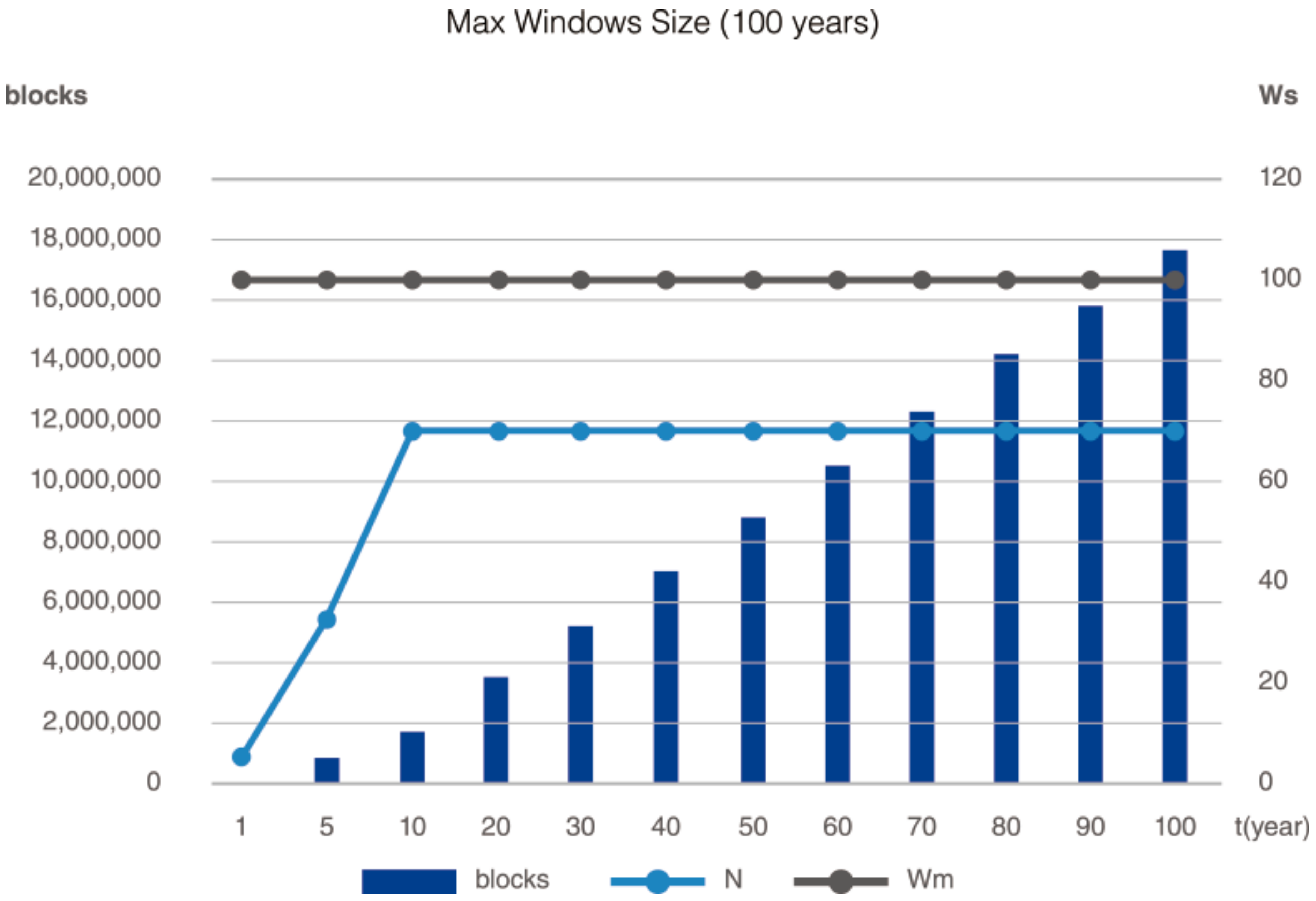


Figure 7. Block window simulation (100 years)

If the block window size is simulated for 100 years with a mining node factor of 100, it is as in the above figure. The block window gradually increases from the point of time when the genesis block is started, and the size increases or decreases according to the node factor after the point (tm) when the maximum block window size is reached.

We have completed the development of ePoW, and the results of ePoW's block mining distribution and energy consumption levels will be published separately on the website later.

The Hdac ePoW consensus algorithm will support a variety of technical methods for creating a healthy mining environment. A separate hardware security module [HSM] is being developed to enhance security of the mining node where this will be an available option to select.

Enhancing Quantum Random Number Security

Blockchain-based platforms have already been verified with high security. The private key, public key, and wallet address used in blockchain based transactions are created using a pseudo random number. In recent cases, a pseudo random number security vulnerability has been found by analyzing the patterns of pseudo random numbers and creating values for specific purposes. There have been various attempts to compensate for these weaknesses, and a quantum random number method has emerged that cannot be analyzed theoretically. Hdac proposes a method to replace random number generation with quantum random numbers for a private blockchains.

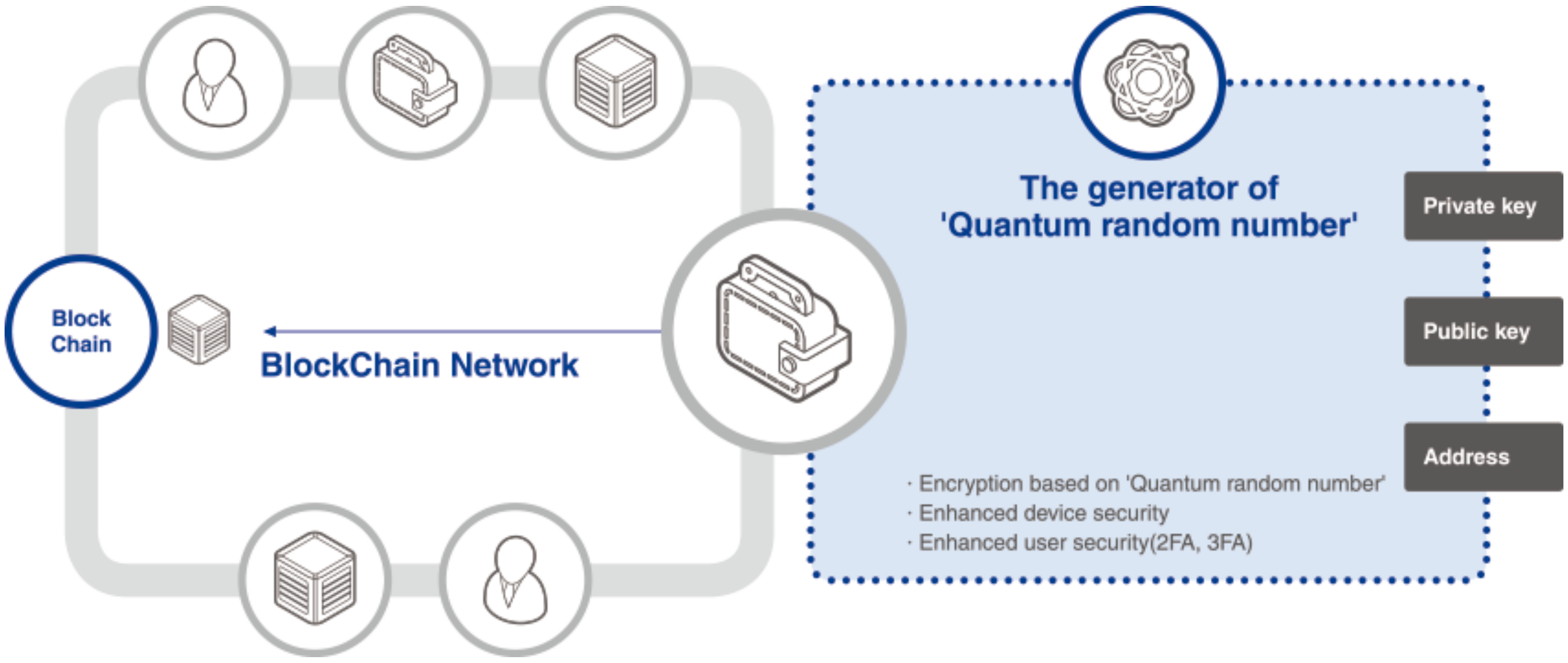

Block Chain
BlockChain Network
The generator of 'Quantum random number'
Private key
Public key
Address
· Encryption based on 'Quantum random number'
· Enhanced device security
· Enhanced user security(2FA, 3FA)

Figure 8. Enhanced device security using quantum random numbers

Blockchain-based platforms have already been verified with high security. The private key, public key, and wallet address used in blockchain based transactions are created using a pseudo random number. In recent cases, a pseudo random number security vulnerability has been found by analyzing the patterns of pseudo random numbers and creating values for specific purposes. There have been various attempts to compensate for these weaknesses, and a quantum random number method has emerged that cannot be analyzed theoretically. Hdac proposes a method to replace random number generation with quantum random numbers for a private blockchains.

DAC Generating, Mining and the Mining Result

Compared with Bitcoin, Hdac's issuance policy is as follows.

The total DAC amount of the Hdac blockchain is 12 billion. The first mining result begins with 5,000DAC before DAC halving. The block generation cycle is 3 minutes, and halving is set to reduce the mining result by half for every 1,032,000 blocks. That is, the mining result is reduced by half approximately every 71 months since the Genesis block is created. 7% of the DACs will be used for creating platform, and an ecosystem to implement Hdac technology, boost its transaction, and also for liquidity management. Another 7% will be distributed to participants who donated to the Hdac Technology AG.

Such a mechanism is a policy intended to maintain the intrinsic value of the DAC by reducing its supply. The total amount of DAC generated is fixed, rather than inflationary DACs where the generated asset increases to infinity and the asset value declines. It is important to see if the equilibrium price can be maintained at the point where the buyer and the seller’s stocking instincts meet.

Miners who want to mine by participating in the Hdac blockchain network, will receive a mining result and a transaction cost. The Mining result, which is halved roughly for every 6 years, gradually increases the number of transactions included in a block, thereby filling up the total cost.

Hdac Technology Roadmap

Configuration of IoT Blockchain Network

The IoT blockchain network is a permissioned private blockchain that is registered after being authenticated and can operate on a blockchain network. Therefore, it can be said that its personality is different from a public blockchain which access to the network.

The components of the IoT blockchain network are as follows.

- **Blockchain node**: Records all transaction blocks as a full node. Stores setting information related to user-device, device-device control, billing, and management performed by the administrator.
- **Administrator**: A person who registers users, gateways, and devices in the blockchain and grants access between them. The settings are safely stored in the full node of the blockchain and are transmitted to the following users, gateways, and devices through the network. Each user and device maintains the latest settings related to them. It can also be integrated systematically with the existing IoT operating environment.
- **User**: A person or device with a program running as a simple node that does not store blocks.
- **Gateway**: As it is, a unit used to control many dummy devices or sensors. It can analyze details of the IoT contract and then transmit to dummy devices or sensors. Each device or sensor is connected with an individual address.
- **Device**: As it is, a device that is connected to a gateway or a simple node which does not store blocks. It corresponds to individual addresses and it can also analyze the IoT contract details and operate.

As illustrated in Figure 7 below, the user sends the IoT contract which is attached with a program to the gateway or a device. The device analyzes and operates the received IoT contract. The user can send transactions that access or control explicitly authorized gateways or devices.

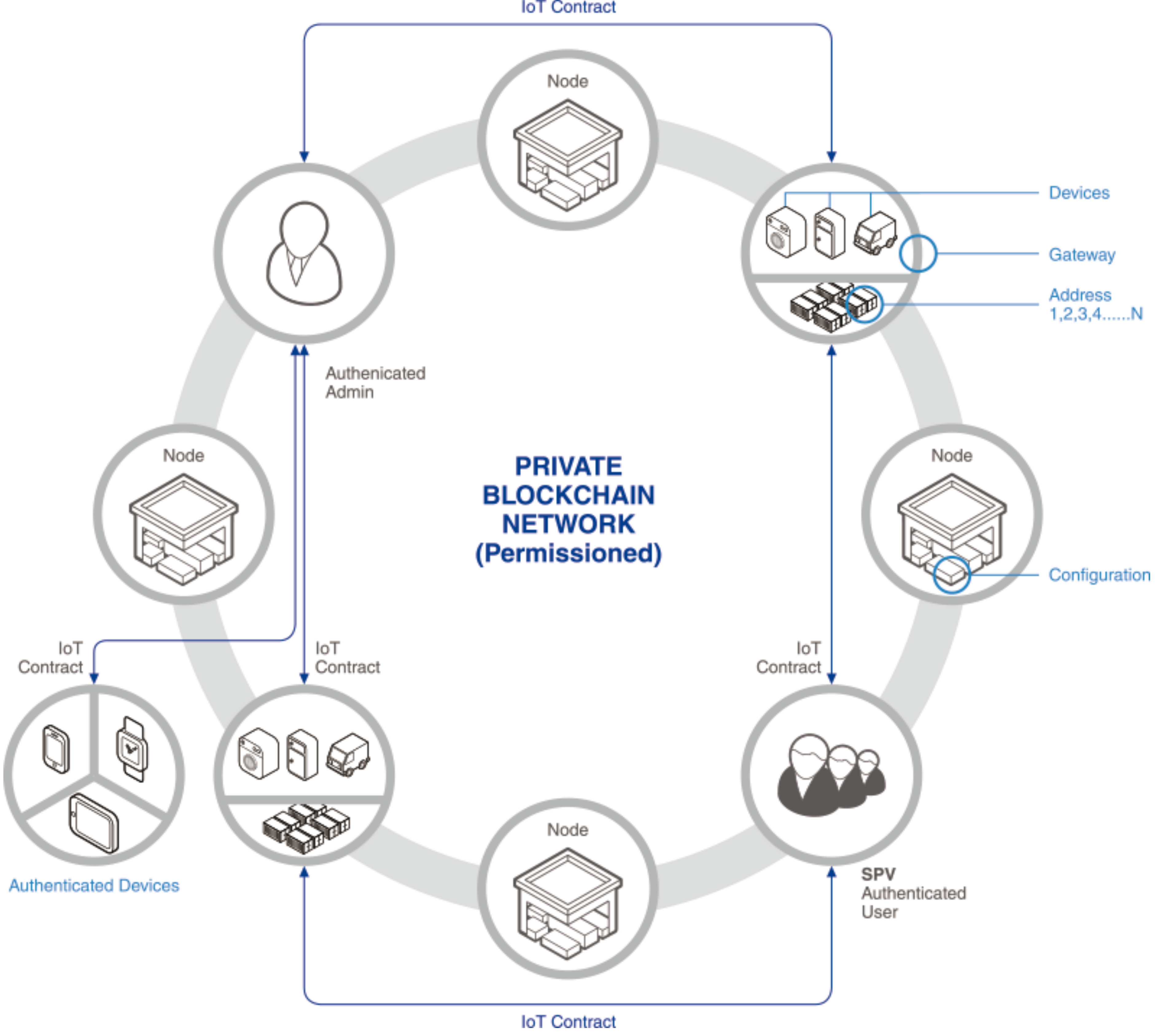


Figure 9. Structure of the IoT blockchain network

User-Device Mapping in the IoT Blockchain

The user on the IoT blockchain must be able to access the device according to clear access rights rules to control the device. The user should also be able to control the specific equipment according to the setting or to only read the status of the equipment, and it should be possible to make general users inaccessible to certain equipment. This allows the administrator to set access permissions by the addresses of the users, devices, or gateways. This access right setting is stored in all of the full nodes of the blockchain network, and is also shared among all nodes, gateways, and devices.

Access and control of users and devices, and transaction authority, are recorded securely in the blockchain. The IoT contract can be carried out after the authority is verified compared to this record when the transaction occurs.

In the general IoT operating environments, these permissions are often granted. Therefore the IoT blockchain may be useful to use in combination with the existing IoT environment.

The types of authority mapping are as follows.

- User-device/gateway mapping
- User-user mapping
- Device/gateway-device mapping The mapping rights are as follows.

- **Access rights**: Indicates the right to access the equipment. Will be able to specify a minimum access rating. A user or device will have a rating, meaning only a specific rating or higher is accessible. If access is not possible, all of the rights below are not available.
- **Right to read**: It is a right to read the current state, and detailed authority can be specified as a separate string, and it can be interpreted by the device to determine whether it is applicable or not.
- **Right to control/write**: It is the right to control the device or to change the state. Detailed authority can be specified separately, and it can be interpreted by the device to determine whether it is applicable or not.
- **Transaction rights**: Specifies configurable rights related to manual and automatic transaction. Detailed authority can be specified separately, and it can be interpreted by the device to determine whether it is applicable or not. The method of limiting the maximum transaction count and maximum one-time threshold during a specific period is effective.
- **Other rights** (specifying detailed rights by device): Other detailed rights can be specified as a separate code or string, and can be interpreted by the device to determine whether they are applicable or not. Since this detail is a method of depending on the device, no specific control measures for all devices are specified here.

All transactions using this blockchain network are determined to be transmitted according to the access right. That is, if a user A has no access to a device B but still a transaction from A to B occurs, device B and all blockchain nodes will reject this transaction. In this case, the error can be reported to the intrusion detection node in the blockchain, and the administrator can immediately check for the details.

After the administrator configures the authority between the first user-device or device-device, the rights of each user and device can be adjusted if changes are made to the blockchain network. In addition, when a device is added or deleted, a corresponding mapping must be performed. Basic rights may be specified in cases where a new device is added according to the setting.

The process of access rights mapping according to device can be quite complex in some cases. Therefore, it is possible to try to group users or gateways and devices into specific groups in order to effectively handle such rights mapping, and also, may provide a user application programming interface [API] or command in the form of a script to control complex mappings. In some cases, the user-device mapping may be expressed in more complex forms with respect to the location and state of time and space. In this section, only the generic form of device mapping is presented.

This user-device mapping method is already being used in the IoT industry, and it will be possible to operate the existing management system to have the maximum effect while minimizing the modification through appropriate business linkage with the blockchain.

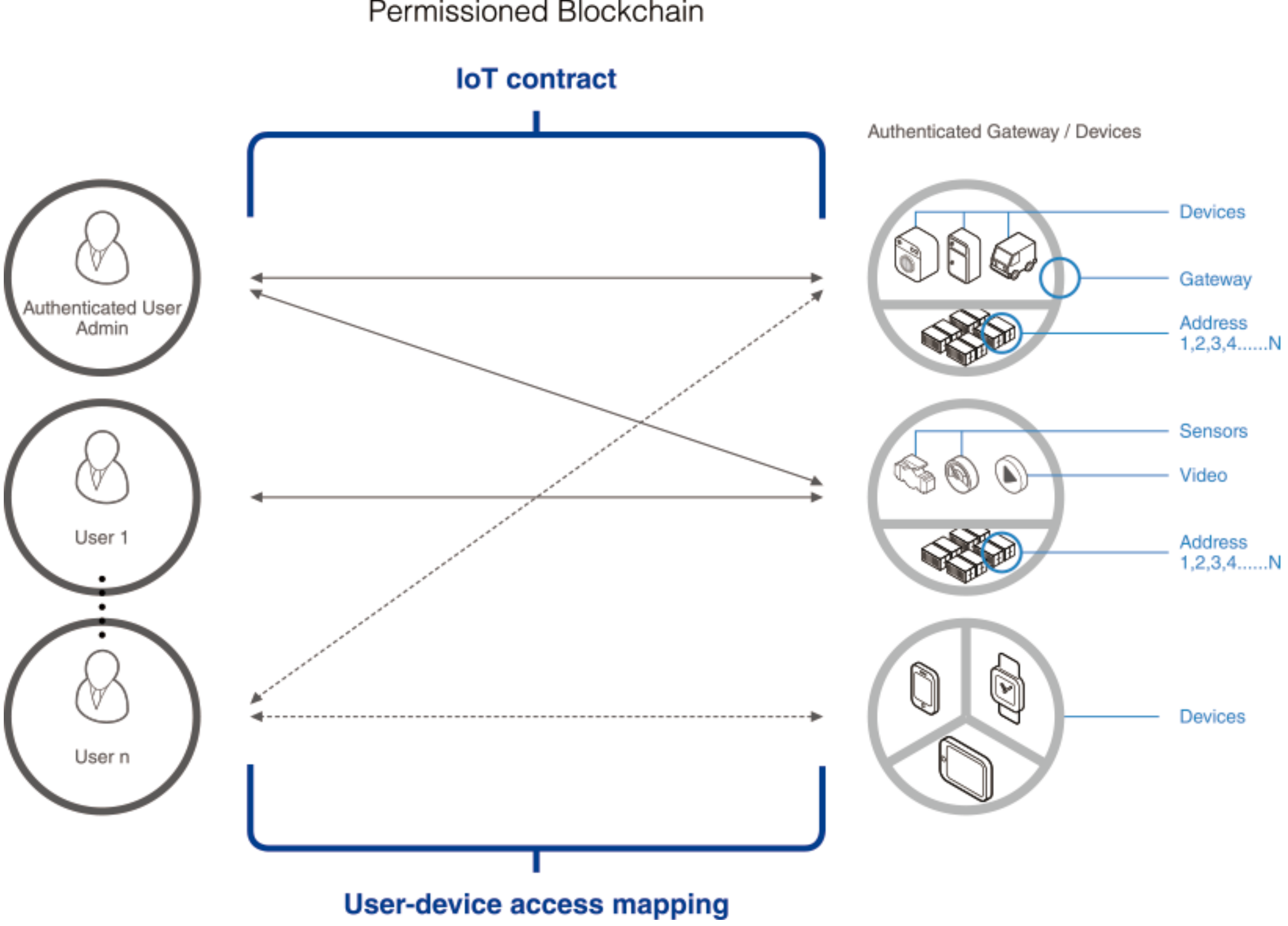


Figure 10. Example of mapping between user and device on the private blockchain

IoT Contract

IoT contract is a concept where the object of the smart contract is expanded to IoT devices. A programmer can create a program that controls the operation of the IoT device. That is, he or she creates a smart contract for the IoT, and sends an IoT contract to a specific device to perform machine-based automated work and operation. The IoT contract is a transaction that transfers control commands between user-device or device-device, and to use this transaction, user-device or device-device authentication, which will be described later, must precede.

Before using this transaction, the user and the device must first be registered in the blockchain network through the authentication procedure. In the case of the user, only the authorized user through two-factor authentication should be able to access the blockchain network. As the user authentication method, an ID, a password, a one-time password or a biometric authentication (fingerprint, iris, face recognition etc.) can be added, and verification is performed through these.

Since the device is difficult to register by itself, the administrator must first identify and register the associated device. Several methods are being considered to determine the unique ID of the device. First, there is no problem if the device has a unique ID (such as a security chip). However, if this is not the case, it can register the hash of unique response information, MAC address, CPU ID, disk ID, OS image, electronic wallet address, etc., so that the device can be automatically disconnected from the blockchain network and reported to the administrator whenever it is tampered with.

Depending on the IoT contract, when the status of a program running on the device changes, it can manipulate the device, perform automatic transactions between devices, or transmit status information or data to a predetermined location. At this time, automatic transaction between devices is called M2M transaction, and transaction can be made only to the addresses allowed to transfer in the user-device and device-device mapping in advance. The device A, which receives the commands, can transmit status or control information to another device B according to the program contents and may be able to control the device B.

Control is possible only when the setting is registered and has control rights in the blockchain network. By providing the IoT contract service through Hdac*T, state control, transaction and management between users and devices, as well as between devices, are possible. Through this, M2M transaction can be provided.

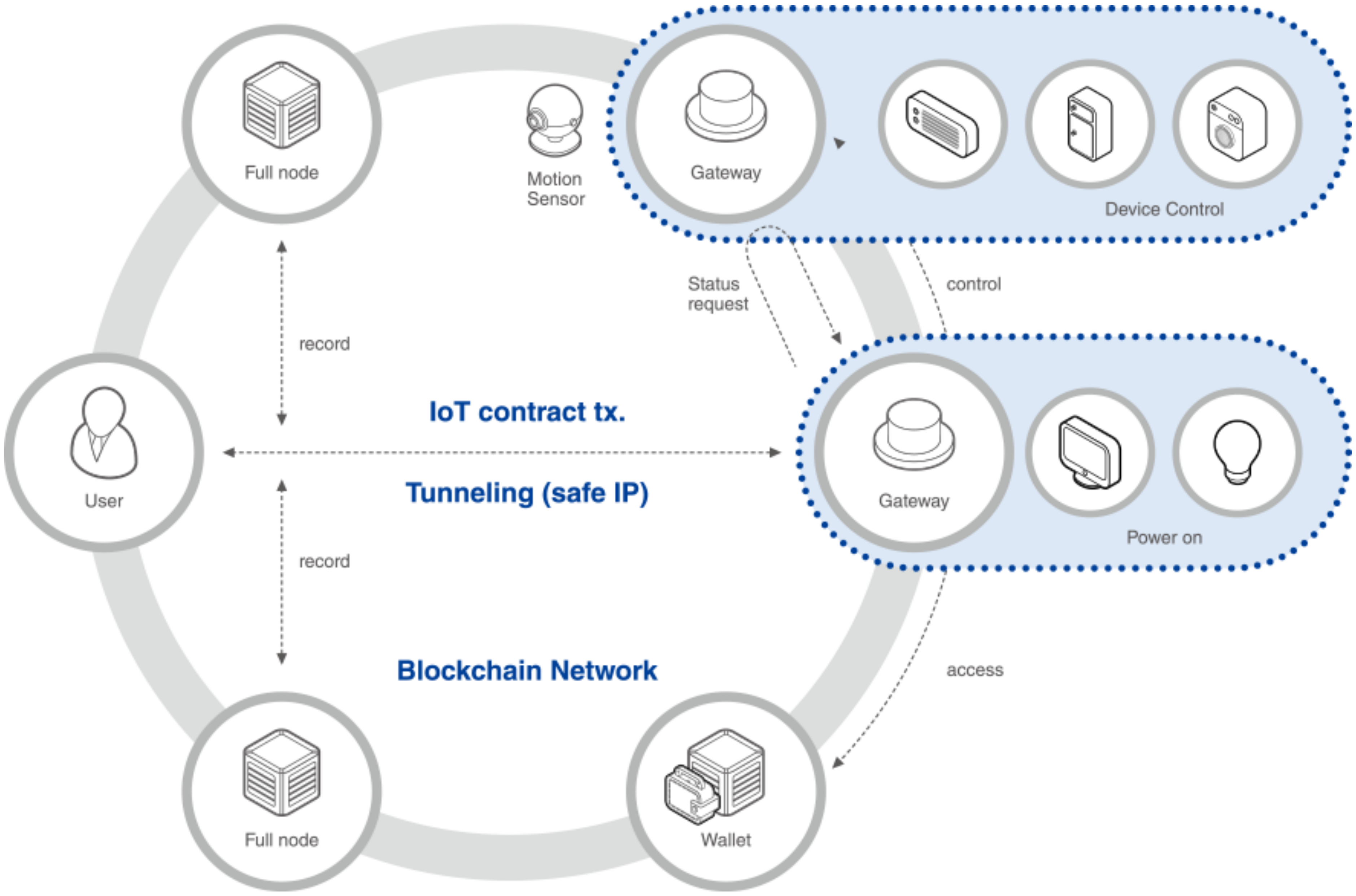


Figure 11. Structure of the IoT Contract Service

An automated program can be added to the IoT contract so that the device will operate for the user to control the device, be informed about the status of the device, automatically proceed with transactions if a certain condition is fulfilled, etc. This program can deliver simple JSON-formatted data according to the device’s conditions, and it can be provided with a programmable API type that can handle more complex information.

In higher performance devices, more complex and sophisticated high-level programming is added to the IoT contract and delivered to the device, and it may be interpreted and processed through an interpreter or virtual machine operating within the device.

The most effective and convenient way to control IoT devices in terms of speed and security is to use APIs to develop programming for the device. In terms of flexibility, an interpreter or a virtual machine can be effective. In the case of an interpreter or a virtual machine, it is not necessary to change the device only by changing the control program on the user side, so that it can be applied easily and flexibly. However, using an interpreter or virtual machine requires a relatively high level of computing power and memory, so it cannot be directly loaded into low-performance devices. For example, if there are 100 A-type devices and the policy to manage this device is changed, it is much more efficient and secure to change the user-side IoT contract, which has control rights, rather than to modify or update 100 devices.

In IoT, since a transaction must be performed in real time, an appropriate number of devices are registered in the blockchain. If it is the case where the network ensures appropriate processing performance, it can process about 500 tx/sec. The amount of transactions or response time that can be handled can be highly dependent on the performance of the network and the device.

In particular, where a transaction requires high security, it can be transferred to the device through a secure channel completely separate from the normal network, such as a VPN. In other words, it can be made inaccessible through the public network in-between. In the private blockchain, the device and the full node can be arranged in N:1 ratio where security devices are used to enhance security of the network segment. If necessary, the user program and the data block may be encrypted and transmitted due to device security matter.

Detailed specifications of IoT contract are as follows.

- Basic blockchain transaction
- User-defined JSON header
  - Consists of user information, type of user, authorized contents, processing command and data, response method etc.
- User program
  - Additional JSON data, or high-level programming language, or object information to carry out
  - It can be processed by API, interpreter, or virtual machine
- Data/stream to be used in the user program

Iot Contract	Default Blockchain Transaction	
	User Defined JSON Header (User Info., UserType, Permission, OpCode, OpData, ReplyType, ...)	
	User Program (Script)	User Data (Binary)

Table 2. Structure of IoT Contract

The user program is a high-level language, and the program may be interpreted through an interpreter or a virtual machine that have a syntax similar to C, which is familiar to IoT developers.

In this process, we will use a specific program interpreter/virtual machine to interpret user programs, but we will keep the source code and interface as simple as possible, so that the users can easily add a new type of interpreter or virtual machine.

Security for IoT Blockchain

The primary concern of IoT is a security issue for IoT devices. The majority of these security problems can be solved by adapting IoT blockchains. However, since denial of service [DoS], distributed denial of service [DDoS], and sniffing attacks cannot be solved by the IoT blockchain, connection with other security technologies should be considered.

For private blockchains, security could be improved by using a separate secure channel by separating the network between nodes and devices or between blockchain nodes and users. This method can be implemented through hardware or blockchain software, which can be mounted on a device. This method has an advantage that it is not necessary to change an existing blockchain node or device configuration. Those general devices which are not able to transfer blockchain code, can be controlled through a separate device adapter node. In this case, the transaction can be controlled by changing the signal to directly control the device.

Moreover, if necessary, other various security methods should be installed inside the server to prevent threats. Recently, smart devices have built-in protocols such as Transport Layer Security [TLS] or Secure Sockets Layer [SSL]. They also have various security systems against control signals. An IoT contract, which is an encrypted transaction between users and devices, can support devices by using TLS / SSL and various protocols. An IoT Contract, an encrypted transaction between users and devices, can support devices using TLS / SSL and various protocols. In addition, low-performance devices that have difficulty performing complex encryption can selectively use IDEA (International Data Encryption Algorithm) or ARIA (Generic 23-Block Cryptographic Algorithm with Involutional SPN Structure Optimized for Lightweight Environments and Hardware Implementation) or with the AES128 to AES256 standard symmetric key encryption algorithm, depending on the device.

Because the program inside the device needs to be changed, this method is difficult to apply to a device which has already been created. Therefore, these very low performance devices can be classified as dummy devices, and can be managed by gateways that operate over separate secure channels.

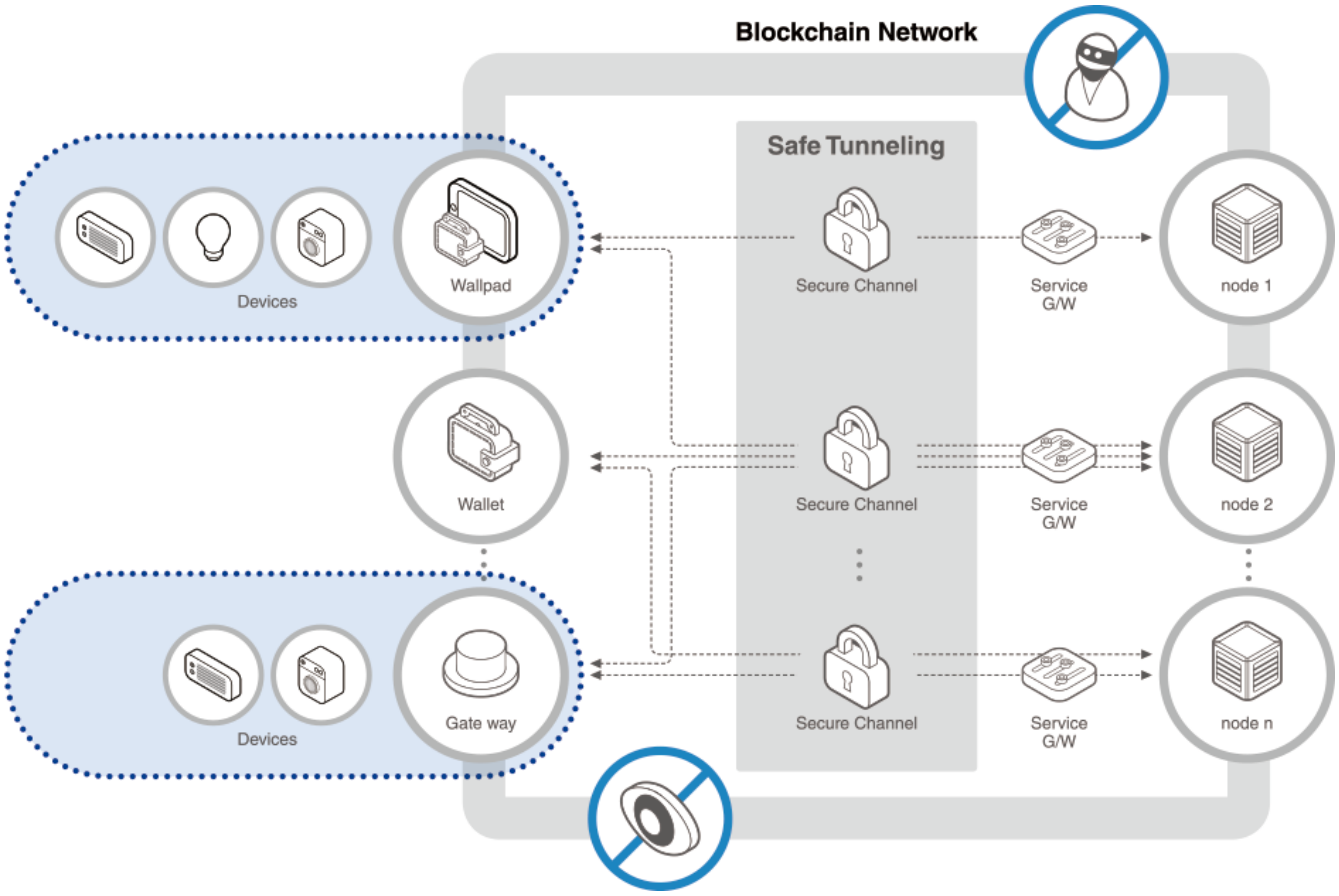


Figure 12. Enhanced network security in a blockchain

Even if the IoT blockchain is well integrated with existing security processes, there may still be unexpected security vulnerabilities. Therefore, it is necessary not only to constantly monitor user setting changes, device additions, setting changes, and mapping changes between user and device on the IoT blockchain, but also compare with previous settings when changing contents. This big data can be searched and analyzed by using tools equipped with machine learning.

Furthermore, if the main contents change, it is necessary to enact the process of attempting secondary authentication to the administrator, and it should be able to cope with various network attacks including DoS and DDoS performed in the network.

Therefore, one or more nodes should operate as watchdogs to detect abnormal transactions and generate events. In each node, the function of monitoring the status of the server may be inserted to notify the administrator, who can act before the blockchain becomes difficult to operate.

The following events can be detected by the watchdog node:

- **Abnormal transactions:** Transactions that do not have a destination address, and that cause abnormal excessive traffic, unauthorized transactions and IoT contracts
- **Detecting status of each node**: If it is a full node, it monitors the disk capacity, server status and network status, and notifies watchdog when it reaches a certain level.
- **User-device, device-device mapping change monitoring**: Detects when contents are changed. Tracks changes when mapping changes are prohibited.

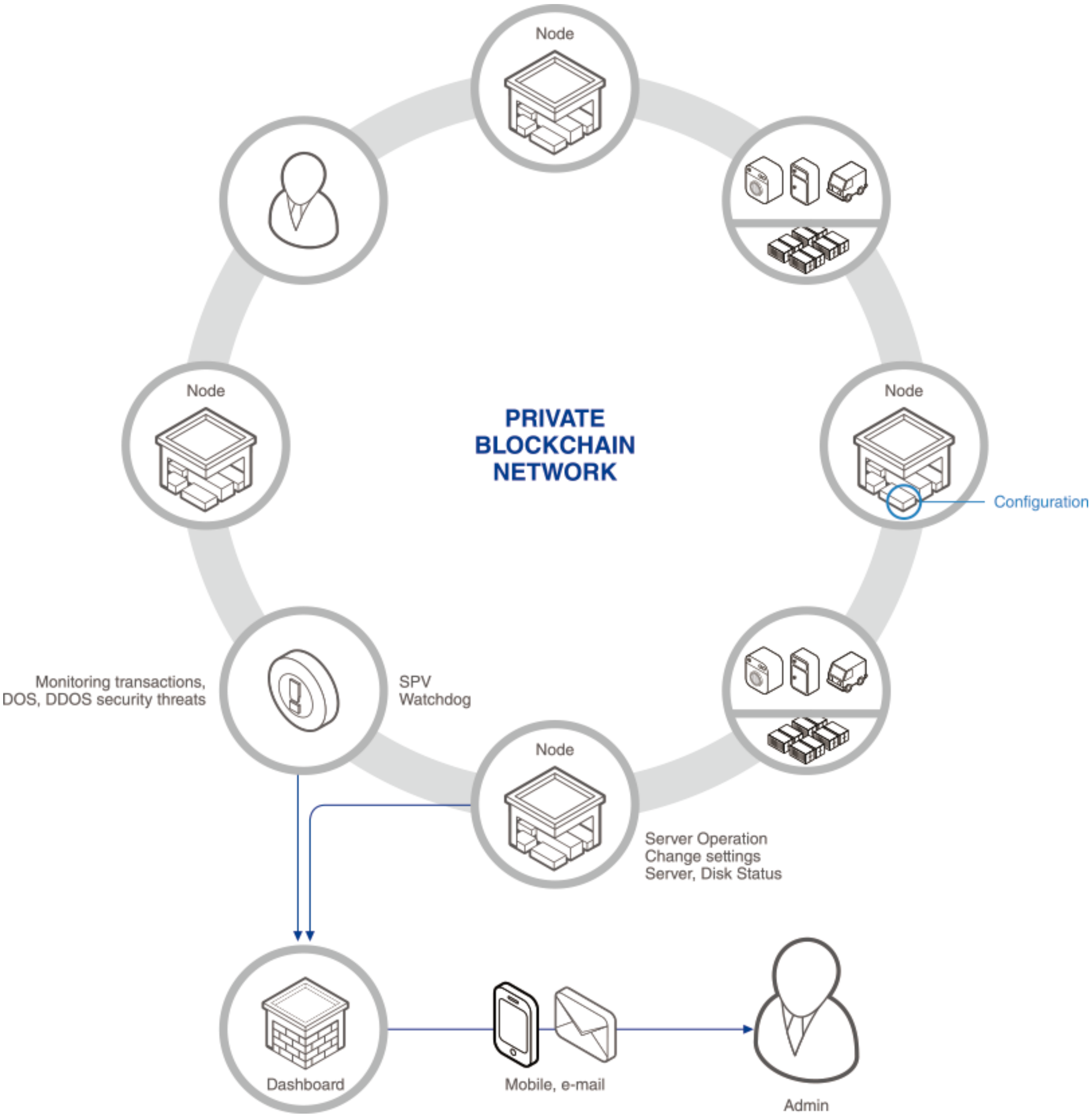
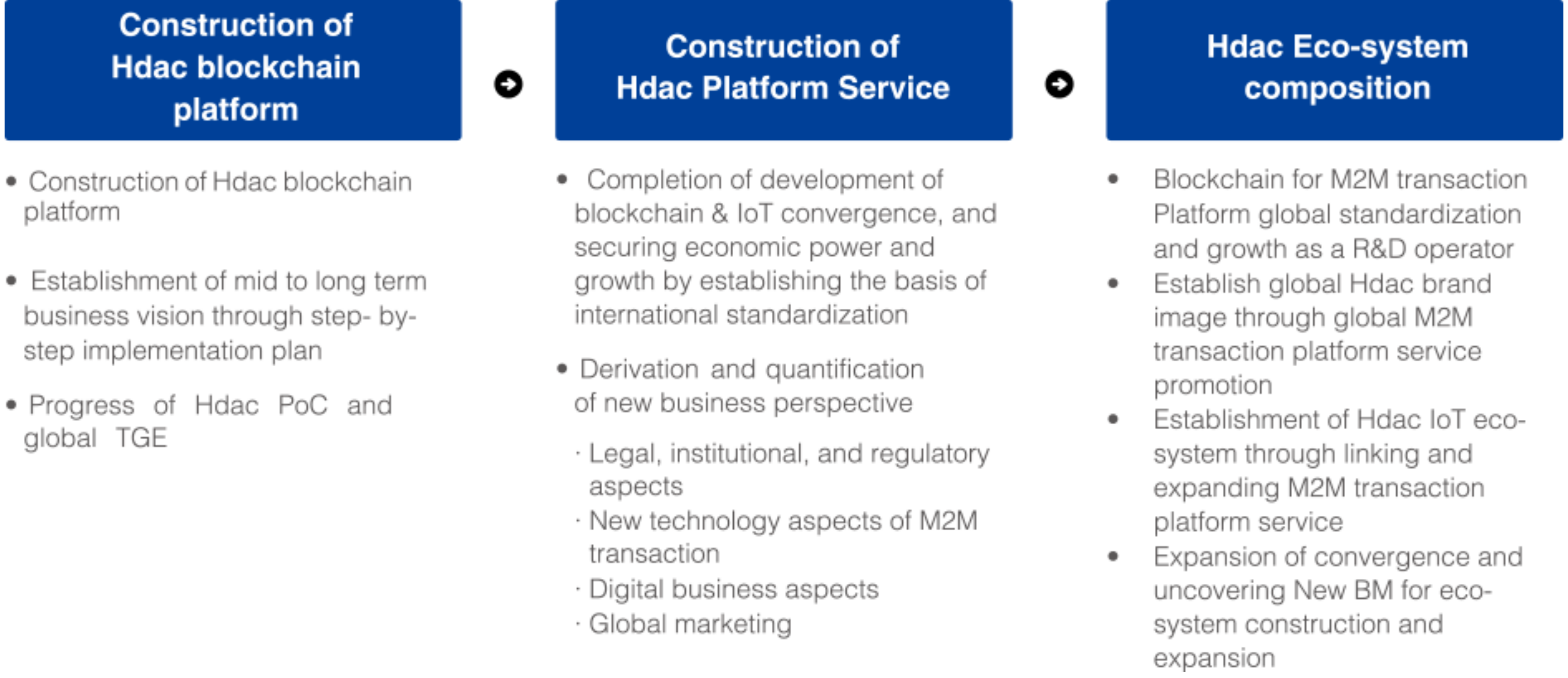


Figure 13. Threat detection in the IoT private blockchain

Hdac Ecosystem

Strategy of the Hdac Ecosystem Development

In order for Hdac to evolve continuously and stably, The Hdac Technology AG will conduct marketing, and public relation activities while HDAC Technology AG implements Hdac Platform Technology, developing the next-generation Industrial platform. These teams will strive together to develop technological progress and synergy ecosystem of Hdac in order to create a virtual circle environment for global technological development as shown below.



Construction of Hdac blockchain platform

- Construction of Hdac blockchain platform
- Establishment of mid to long term business vision through step- by-step implementation plan
- Progress of Hdac PoC and global TGE

Construction of Hdac Platform Service

- Completion of development of blockchain & IoT convergence, and securing economic power and growth by establishing the basis of international standardization
- Derivation and quantification of new business perspective
  - · Legal, institutional, and regulatory aspects
  - · New technology aspects of M2M transaction
  - · Digital business aspects
  - · Global marketing

Hdac Eco-system composition

- Blockchain for M2M transaction Platform global standardization and growth as a R&D operator
- Establish global Hdac brand image through global M2M transaction platform service promotion
- Establishment of Hdac IoT eco-system through linking and expanding M2M transaction platform service
- Expansion of convergence and uncovering New BM for eco-system construction and expansion

Figure 14. Strategy of the Hdac Ecosystem development

Ecosystem Players & Partners

Hyundai BS&C, Doublechain, HyundaiPay, and BLOKO have formed The Digital Transformation Community for the core technology/application development of Hdac as well as its activation. In addition, we are in the process of cooperating with various partners: such as WisBase, which specializes in large database design and tuning; PnP Secure, which is an information protection solution company; EYL, which is a developer of quantum random number chips; INTO Information, a developer of original technology and service development for various industries; logical closed network solution supplier ARAD; IOT device technology partner MODA; and Mill Corp. We are also collaborating with Intel to develop IoT and face recognition access security solutions.

In December 2016, Hyundai BS&C and Doublechain signed an MOU to launch a blockchain-based business. And we are pursuing a joint project to maximize the efficiency of blockchain-based platform development/operation, and developing the IoT and blockchain convergence solutions.

In June 2017, HyundaiPay was launched, the specialized blockchain-based company, for the advancement of blockchain technology and early launch of various services. On 20 July, 2017, HyundaiPay and Doublechain signed a strategic alliance with Elasticsearch Korea, a large data and machine learning company, for the co-development of an Hdac-based blockchain businesses.

EcoSystem	Partners	Agreement/Role
DTC	Hyundai Pay	DTC Hyundai Pay Blockchain core development support,Hdac value enhancement and activation
	Doublechain	Blockchain Core / Platform Development, Virtual account development
	Hyundai BS&C	Smart IoT (HERIOT, etc.), Smart IoT Home Technology Research Collaboration
	BLOKO	Research Blockchain and Managing Blockchain Technical Community
	EYL	Quantum random number technology, platform support
	INTO Information	Web Firewall, Security Compliance Support

Applied technology	MODA	IoT Gateway device development/manufacture
	WisBase	Large capacity DB/tuning
	ARAD Networks	Technical Support for safe IP
	Elasticsearch	Search engine, Big data preprocessing, Technical support for machine learning
	Mill Corp	Manufacturing IoT products and Industrial PC

A Timeline of the Development of the Hdac Ecosystem

Year	Plan
2017	- Hdac Generation Event - Release Hdac consensus algorithm - Completion of Hdac operating environment Field test (ASM mining pool, Wallet 1.0, Explorer, etc.) - Release H/W Wallet (KASSE 1.0) release, ASM (Advanced Security Module) Ver 0.9 - Release Hdac apps API (ASM mining, Wallet, Explorer)
2018	- Release Hdac operating environment (ASM 1.0 mining pool, wallet 2.0, etc.) release - Hdac IoT Contract PoC - IoT authentication and device control (Smart Home PoC) - Private Blockchain PoC (Game Application, POS Hdac*T site) - Smart IoT diffusion PoC (apartment, factory, etc.)
2019	- Release Practical application of Hdac IoT Contract & Smart Home (HerIoT) - Release Practical application of Hdac IoT Contract & Smart Factory (Mando case) - Hdac Public-Private Hybrid Blockchain Use-case development
2020	- IoT High Speed Transaction Distributed Processing Blockchain Development - Release Private Blockchain Security Enhancements, Advanced Security Module Ver 2.0 release - Hybrid (Public-Private) Blockchain Network Live Operation (M2M transaction)

Table 4. Timeline for Creating the Hdac Ecosystem

APPENDIX A - Examples

Example of a Smart Contract

JSON header may contain the following simple control commands. JSON data can be passed to user definition function, then users can control the device by interpreting those JSON data:

// Light on (if the IoT Contract comes to the address of the light)
{ “operation” : “on”, “rerurn” : “yes” } // If the response is returned after executing the command
{ “operation” : “off” }

// Turn on the air conditioner, set the temperature to 22 degrees Celsius, and set the wind to natural wind. Return temperature

```
{ “operation” : “on”, “temperature” : “22c”, “wind” : “natural”, “return” : “temperature” }
// Turn on the air conditioner, set the temperature to 70 degrees Fahrenheit, automatically turns off after 60 minutes
{ “operation” : “on”, “temperature” : “70f”, “timer” : “60 minute” }
```

Example of an IoT Contract Program

The following example is a simple IoT Contract program that activates the air conditioner when the user is at home, enabling them to limit the transaction automatically to cover only the amount of the service used:

```
#include "hdac.h"
NodeAlias AC = "75578a276a3b2d50a1b4ddae16724185ae2d6d25"; // Air conditioner
NodeAlias TV = "1BZDfv3gjrFi2YpZ4FnPWhgRovbyM5coFmAAEA"; // TV
NodeAlias IS = “Infrared Sensor”; // Infrared Sensor
NodeAlias MO = “Management Office”;

hdac_t *hdac = NULL;
time_t PowerOnTime = 0;

main()
{
  hdac = HdacInit();

  IS.AddEvent(hdac, ProcessISEvent);
  ExecuteContract(hdac); // Wait until the IoT Contract end signal

  HdacExit(hdac);
}

// Process Event
void ProcessISEvent(hdac_t *hdac, NodeAlias node, NodeEvent ev)
{
  if (hdac == NULL || hdac->disabled == true)
    return;

  if (ev.GetStatus("motion") == 0 && PowerOnTime > 0)
  {
    AC.SetStatus(“power”, “off”); // AC OFF
    TV.SetStatus(“power”, “off”); // TV OFF

    int elapsed = time() - PowerOnTime;

    if (node.balance > 1) // If the balance is sufficient, pay
      MO.Pay(0.0001 * elapsed / 60); // Pay exact amount
    else
      node.Alert("Low Balance"); // Notify the user
    PowerOnTime = 0;
  }
  else if (ev.GetStatus("motion") == 1 && PowerOnTime <= 0)
  {
    AC.SetStatus(“power”, “on”); // AC operation
    TV.SetStatus(“power”, “on”); // TV operation
    PowerOnTime = time();
  }
}
```

APPENDIX B - Legal Disclaimer

The information in this document is subject to change or update without notice and should not be construed as a commitment by HdacTech.AG. This document is for informational purposes only and does not constitute an offer or solicitation to sell shares or securities in Hdac.io or any related or associated company. Any such offer or solicitation will be made only by means of a confidential offering memorandum and in accordance with the terms of all applicable securities and other laws.

APPENDIX C - References

Antonopoulos, Andreas, Mastering Bitcoin: Programming the Open Blockchain, O'Reilly Media Inc. (California: 2017).

Arad Networks, "Why SPN Solutions?" http://www.aradnetworks.com/spn_why, (March 2017).

Banafa, Ahmed, "Internet of Things (IoT): Security, Privacy and Safety," Datafloq, https://datafloq.com/read/internet-of-things-iot-security-privacy-safety/948.

Beecham Research Limited, "IoT Security Threat Map," http://www.beechamresearch.com/download.aspx?id=43, (2015).

Belson, David [Ed.], "The State of the Internet / Q3 2015," Akami, https://www.akamai.com/us/en/multimedia/documents/report/q3-2015-soti-connectivity-final.pdf, (December 2015).

Boldt, Bill, "Without Security, is the Internet of Things Just a Toy?" Pubnub, https://www.pubnub.com/blog/2015-01-30-without-security-internet-things-just-toy/, (January 2015).

Buterin, Vitalik, "Ethereum: A Next-Generation Smart Contract and Decentralized Application Platform," https://github.com/ethereum/wiki/wiki/White-Paper, (2014).

Elasticsearch, "Heart of Elastic Stack," https://www.elastic.co/kr/products/elasticsearch, (2017).

EYL Partners, "Product Overview" http://www.eylpartners.com/index.php/product-overview/, (2017).

Greenspan, Dr. Gideon, "MultiChain Private Blockchain ? White Paper," Coin Sciences, http://www.multichain.com/download/MultiChain-White-Paper.pdf, (2014).

Intel Software, "Intel Realsense Camera SR300," https://software.intel.com/en-us/realsense/sr300, (June 2016).

La Marca, Daniela, "Gartner: hype in 2015 around the internet of things (iot) and wearables," Mediabuzz, http://www.mediabuzz.com.sg/asian-emarketing-latest-issue/210-asian-e-marketing/digi tal-marketing-trends-a-predictions-week-1/2504-gartner-hype-in-2015-around-the-intern et-of-things-iot-and-wearables, (Jan. 2015).

Modacom, "Smart IoT Gateway (Hub)," http://web.modacom.co.kr/ko/product/product_view.php?cate=IoT%20Products, (Feb. 2017).

Nakamoto, Satoshi, "Bitcoin: A Peer-to-Peer Electronic Cash System,” https://bitcoin.org/bitcoin.pdf, (2008).

P&P Secure, “Domestic DB Security # 1 'P & S Secure,'” http://www.pnpsecure.com/NEWS--NOTICE/page-4, (Sept. 2017).

Postscapes, “Internet-of-Things Software Guide: Find and compare the best IoT Software development tools, OS, language platforms, and frameworks,” https://www.postscapes.com/internet-of-things-software-guide/, (2017).

Sandoval, Kristopher, “Blockchain: Beyond Cryptocurrency,” NordicAPIs, https://nordicapis.com/the-uses-of-blockchain-beyond-cryptocurrency/, (May 2016).

Waterman, Shaun, “Report: IoT security products face huge challenges,” Cyberscoop, https://www.cyberscoop.com/forrester-iot-security-report-q1-2017/, (Jan. 2017).