FirmaChain

WHITEPAPER

Version 1.1

Table of Contents

1. Overview

1.1 Importance of License Agreements for Intellectual Property (IP) Rights (Patent Rights, Trademark Rights, Copyrights, etc.)

Development of the internet has introduced an era of borderless information, and the protection of IP rights such as patent rights, trademark rights and copyrights, etc., and their commercial utilization through license agreements have become the key to the competitiveness of individuals and companies, and nations.

However, the protection of intellectual property rights and the traceability of their transfers do not reflect the highly advanced technologies, which have resulted in a wide range of domestic or international IP infringement and fraud or abuse of rights in the process of executing license agreements. We plan to utilize blockchain technologies to verify IP rights and record their transfers to promote the safety of companies' and individuals' IP in the course of executing international license agreements.

1.2 Need for Introduction of Electronic Contracts in License Agreements for Intellectual Property Rights

In the modern society, numerous contracts still retain the classic way of writing contracts. So far, many digital signatures and document-related services have been introduced, and electronic contracts have been legally recognized. However, even then, the majority of companies still continue to use written contracts and many of them are not aware of the usefulness of electronic documents.

'We thought.
Why do we prefer written contracts?'

Society still gives more trust towards written contracts over electronic documents. This is because writing takes the role of evidence wherein it provides an original copy. Also, most of the services that provide electronic contracts are centralized, so some factors, such as forgery, data loss or leakage of confidential information through hacking of servers, have made it harder to obtain trust than written contracts. The higher the trade price, the more it causes anxiety concerning forgery between the contracting parties. In addition, when it comes to international contracts, the taxes, remittance fees, and processing fees required to be received through overseas subsidiaries come as a huge burden to the parties.

Relevant problems can be highlighted through numerous real-life examples provided below.

Example 1.

I recently purchased a license from a user who holds an IP right (patent right). However, I am highly concerned as to whether I am not certain whether the seller is a real holder of the patent right, since the seller is a foreign user, and it is difficult to confirm that the seller has never granted an exclusive license to another purchaser. What if a third party uses the patent right I purchased without proper authority or in excess of the scope of the purchased license?

Example 2.

In order to enter into a contents publishing contract, Company A and Company B had exchanged word documents with revisions until the day before executing the contract. On the day of signing the contract, Company B brought the draft of contract including an additional provision concerning the copyright protection, which had not been previously discussed between the parties. It was an uncomfortable situation because time was limited and the Chairman was out of office. Although the person in charge promptly made the necessary corrections without approval of the Chairman and executed the contract, similar situations may arise any time.

As shown in the above examples, the introduction of blockchain-based electronic contracts in the field of license agreements for intellectual property rights will solve the foregoing problems by improving the transparency and the efficiency in contracting processes and eliminate potential inconveniences based on their broad application, including the protection and tracing of IP rights.

FirmaChain utilizes the decentralization of the blockchain. We plan to create an electronic contract management service where we can secure transparency and reliability of the transaction documents in license agreements for IP rights; fundamentally solve issues of verifying contracting parties and forgery of contracts; implement a reasonable contract-making procedure between parties using DApp; reduce the processing cost for international contracts through contract writing using less resources and simplifying the process; and ultimately create a service that overcomes the limitations of written contracts.

1.3 Decentralization of Data

Millions of personal computers all over the world are constantly operated for considerable time, but not all of a computer's resources are utilized to the fullest extent. This is especially the case with storage capacity and network bandwidth. If the remaining storage capacity and network resources could be lent to another person at a certain price, the user could save files at costs lower than other similar file storage services while the provider could generate a profit with the unused resources.

We have devised a decentralized distributed file storage system to provide reliable storage that protects the integrity and reliability of data. Decentralization means that the system is managed and operated by every participant in the system without the central management of the file storage system.

P2P distributed file sharing systems, such as BitTorrent, also allow individuals upload and store files by sharing data. These P2P file sharing systems, however, are a kind of file-sharing community based on the concept that 'individuals download as much as they upload.' Unfortunately, such system failed to adequately motivate the users maintaining seeds to continue uploading files without any compensations. As a result, P2P distributed file sharing systems do not guarantee sufficient availability of files because these files were always at risk of disappearing at any time.

In order to address the problem of users with files disappearing from the system for various reasons, we have adopted a market system through which users can buy and sell file storage space upon their individual needs. Further, this system does not require the users to maintain uploading the files in order to download the files from the system.

Further explanation of FirmaChain's key technology, Decentralized Data Storage, are provided in the following pages. A more detailed explanation of Decentralized Data Storage will be covered in FirmaChain's Technical Whitepaper to be disclosed in future.

2. A Decentralized Data Storage

FirmaChain's Decentralized Data Storage is used for storing and retrieving large amounts of data. Most blockchain platforms, including Ethereum, can store data, but only temporarily. In addition, these platforms require spending expensive resources such as computing power rather than space for physical storage to maintain the blockchain. If such blockchain platforms are used for the purpose of storing data, astronomical costs will inevitably be incurred.

In most cases, however, files do not need to be stored permanently nor does one have to expend huge resources to do so. FirmaChain's Decentralized Data Storage, therefore, has been designed to allow the users to store huge files for a specified period at a reasonable price. Moreover, in a separate blockchain network where FTC is issued, we have created a structure that further strengthens the integrity by storing only information that can specify the files stored in FirmaChain's Decentralized Data Storage.

Because FirmaChain's Decentralized Data Storage is based on a separate network from FCT's network, there exists a separate token called FDR (Firma Data Reward). Both the user who wishes to save a file (hereinafter, the "User") and person who wishes to provide storage space (hereinafter, the "Miner") can trade file storage space by using the FDR token in the file storage space market. If a transaction is executed between the two parties, the User will send the file to the Miner, and the Miner will duty store the file in compliance with the terms and conditions of their contract. The transaction process can be transparently verified based on a number of theories. Contents that need to be disclosed to the public, such as the transaction between the User and the Miner, the authentication by the Miner, the payment

of the User's service fee, etc., will be contained in a new block, transmitted to the network, and verified by all members of the network.

2.1 FCT (FirmaChain Token)

FCT is a token necessary for using FirmaChain-related services. FCT can be used (i) to pay the service fees for the DApp, developed using the Firma Network; (ii) to be exchanged as FDR, a currency needed to use FirmaChain's Decentralized Data Storage; and (iii) to store short strings that require a stricter integrity standard.

We contemplated about FCT's technical specifications for a long time. We had to decide whether we should establish an independent blockchain with infinite expandability considering the commission policy, block compensation, and transaction speeds suitable for DApp; or whether we should proceed with development for rapid commercialization using Ethereum, a technically stable and proven platform, which uses the Smart Contract of Ethereum Virtual Machine (EVM). After our developers' careful examination of Constantinople, the second update of Ethereum's Metropolis, we have currently decided to use the Ethereum Platform.

Considering the possible application of Ethereum's Smart Contract function, FCT is issued in the form of an ERC-20 token. FCT, as an ERC-20 token, can be used to store status data that is necessary for the DApp service. Unlike FirmaChain's Decentralized Data Storage that has a limited storage period, FCT makes it possible to semi-permanently store data while guaranteeing integrity and availability.

However, if any platform is developed as more suitable to achieve FirmaChain's goals in future, FCT may be issued on said platform's network, and said platform may constitute FirmaChain's independent main network, if necessary. Such considerations concerning various blockchain platform options will lead to the service's smooth and stable development.

2.2 FDR (Firma Data Reward)

FDR (Firma Data Reward) is a currency as well as a compensation that is used in FirmaChain's Decentralized Data Storage. The User must pay the Miner FDR, which is a fee that the User pays to store a file, and if the Miner successfully stores the file, the Miner receives the fee for his/her work from the User. Also, apart from the FDR that the Miner receives as a reward for storing the file, the Miner will receive a block mining reward by generating a block that contains the verification of the ecosystem's participants, such as the User and the Miner.

In order for the User to use the Decentralized Data Storage, he/she can exchange FCT for FDR. Also, the Miner can make a profit by exchanging FDR to FCT and can be used as a currency to use FirmaChain's various DApp.

During the initial state of the operation and in order for a smooth exchange, one gets allocated a fixed quantity of FCT and FDR from FirmaChain's smart contract wallet that is used for FCT-FDR exchange. Then, when the User deposits FCT and enters his/her FDR wallet address using the exchange smart contract, the User will receive the amount of FDR that equals to the amount of FCT deposited. The exchange ratio between FCT and FDR is always 1:1, and in order to prevent the tilting of an applicable wallet's FCT and FDR, one can restrict the exchange ratio per unit time.

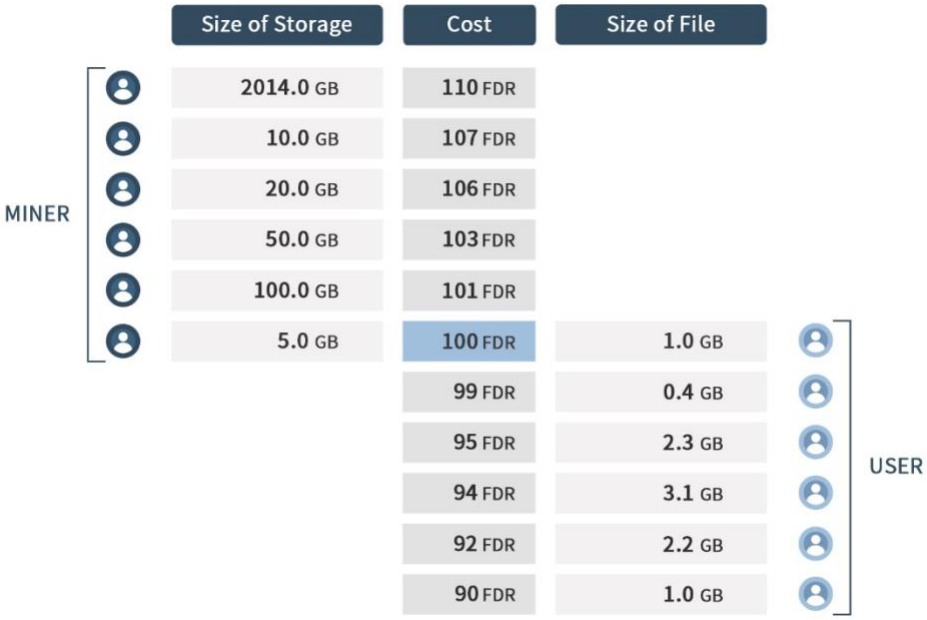
If the ecosystem operates stably, either the Miner or the cryptocurrency exchange that possesses a great quantity of FDR can play the role of the FCT-FDR exchange smart contract. However, unlike the exchange operated by FirmaChain, the exchange owned by these people is not verified and thus cannot be trusted. Also, the exchange ratio might not be 1:1, a separate fee might be charged during an exchange, and there might not be a restriction of the exchange ratio per unit time.

Later on, when FirmaChain's main network is perfectly constructed based on the roadmap, there might be an integration of FDR and FCT, along with the integration of the Decentralized Data Storage and token platform.

2.3 File Storage Market

2.3.1 Market and Orders

The Decentralized Data Storage provides a marketplace for trading file storage contracts between Users and Miners. If a User places a buy order or a Miner places a sell order, the order will be recorded on the single order book publicly disclosed to the entire network. If there is already an order in the order book that meets the conditions, then both orders will be completed, and the file storage procedure will commence promptly after the verification and signature of both parties. As such, in this open market, prices are determined according the law of supply and demand.



<Diagram of File Storage Market>

2.3.2 Rules for Completing Orders

Although a single order book is used, a trade transaction cannot be concluded by treating different orders the same. Therefore, the User may add conditions to the Miner when placing a buy order, and conversely, the Miner can also add conditions to either the User or the file. For example, a User may add a condition requiring a deposit from the Miner as part of ensuring accountability for the file storage, while the Miner can add a condition for the minimum file size to avoid storing small files.

The User and the Miner can demand various types of conditions from each other. Examples of conditions might be requiring the Miner's/User's geographical location, imposing a per unit price ceiling for file storage service of the Miner's choice, and requesting a guaranteed minimum storage period. Conditions will be smart contracted, and the types of conditions will be technologically designed to be composed only of the elements necessary within the decentralized file sharing market.

These conditions will be evaluated when the network node concludes the order. The values of some conditions are verified since the network formally confirmed the validity of them. However, for unofficial conditions used between the User and the Miner, the network node only evaluates whether the conditions satisfy the conditions inserted by the two parties and does not evaluate the truth of the conditions inserted by the two parties. Thus, after the order is completed, the two parties must confirm that the conditions imposed by the other party are actually satisfied.

2.3.3 Reputation System

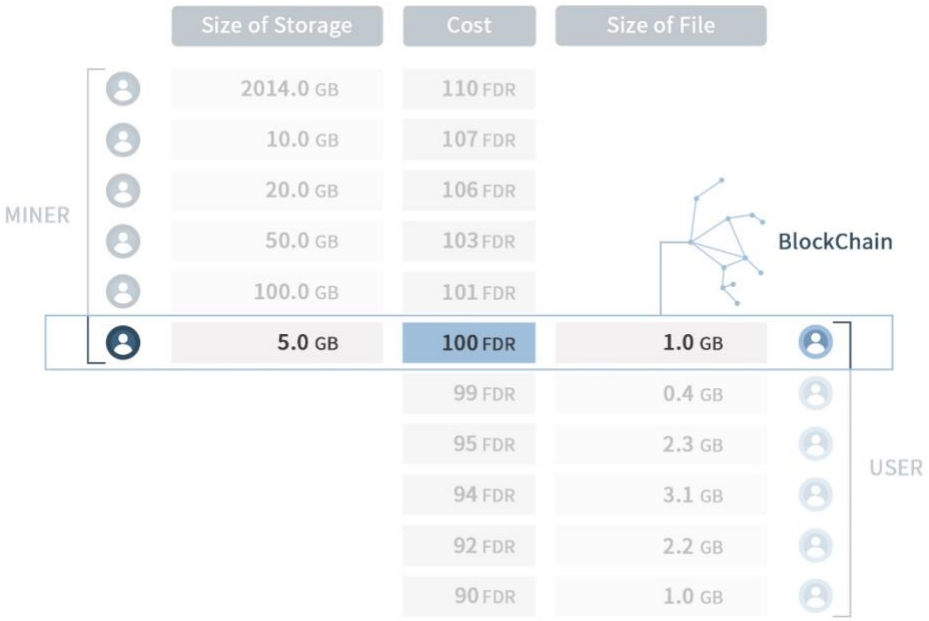
In order for the User to save the file in a more secure way, the User may consider the Miner's **reputation**. It is important for the User to consider the Miner's reputation because some Miners might not meet the obligation of file saving and might cause injury to the network enough to receive penalties. Although an official reputation score is not provided, the User can require conditions such as the cumulative value of the file volume stored, the failure rate for file storing, and a reasonable commission for file storing, so that the User is able to entrust his/her file to a Miner that participated in the network for a substantial period and contributed in creating a better ecosystem.

However, the blockchain network does not officially verify this information, so the User must double-check the miner's conditions after the conclusion of the order and before the signing of each party. This will be provided as a form of a side-service, and since the Miner's file saving history is public data within the blockchain system, anybody is able to view and calculate the values from the record. A function by a third party that provides elaborate calculation of Miners' reputation might be integrated into and used in the User's/Miner's client program stage.

2.4 File Storage Protocol

2.4.1 Storage Procedure

When orders of the User and Miner are completed, both parties will sign the order after confirming each other's conditions. After both parties to the transaction sign the order, a temporary wallet is created for the file-sharing contract, and the User's funds and Miner's security deposit are transferred to the temporary wallet. Following this, the User sends the file to be stored to the Miner, and after the transfer is completed, the Miner encrypts the file and transmits the proof of file storage to the blockchain indicating that the file has been successfully copied and encrypted. Once the transactions under the contract are successfully completed, the Miner can use the records of proof to transfer the file storage fee and security deposit from the temporary wallet to the Miner's wallet. If the Miner's credentials are missing, the User sends the Miner's proof of file storage failure to the blockchain network. The User can then use the proof of file storage failure to transfer the file storage fee and security deposit in the temporary wallet to the User's own wallet.



< Order Completion Process Diagram>

2.4.2 Return Procedure

When the User wishes to get his/her file back, the User needs to put in a request for file return with the Miner. During this process, the User has to pay the Miner a return fee that was decided when initially making the order. The Miner must transmit the file back to the User upon receiving the request for file return. Although the Miner may refuse to transmit the file, such refusal will be recorded on the blockchain, making it possible to gain a negative reputation with later market participants.

2.4.3 Proof of File Storage

As the User is relying on a Miner he/she cannot rely upon with full confidence to store the file, the User wants continuous proof that the Miner is safely storing the file during the promised storage period.

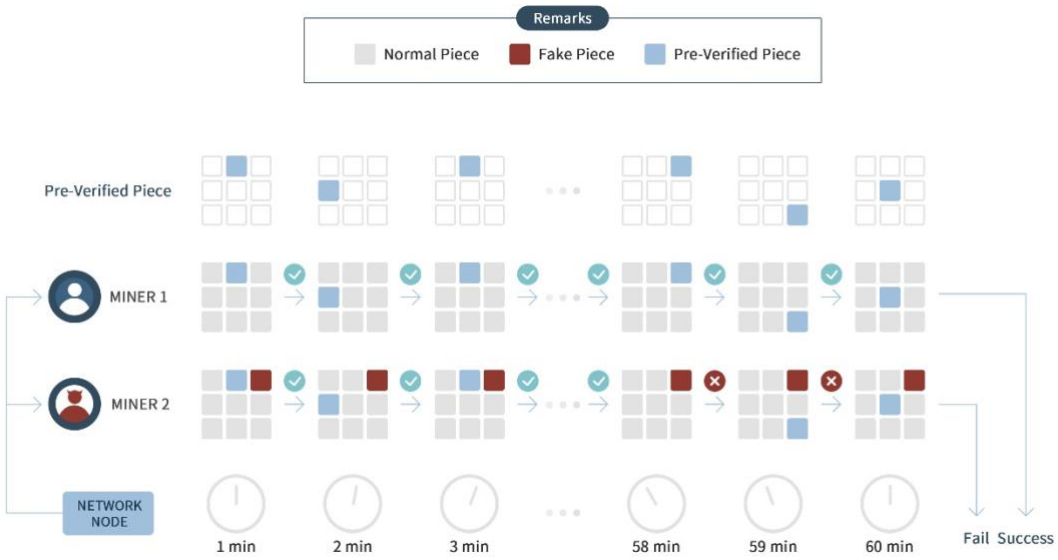
One easy method of proof is having the User who is in possession of the file request the contents of the file from the Miner and checking whether the contents of the files match. If the User continuously compares the contents of the file during the file-sharing contract period by requesting the contents of the file from the Miner, then the User will be able to confirm that the Miner is safely storing the file during the file-sharing contract period.

However, this method would overload the network bandwidth and reduce the file verification speed when the User and Miner share files that are larger in size and greater in number. Therefore, to maintain a minimum verification speed required by the system, there would be no other choice but to restrict the total file sharing size.

In order to improve the overload issue, instead of having the Miner send the entire file to the User, the User may extract file pieces at random, request the contents of the file pieces from the Miner, and then compare their contents. This method allows the Miner to prove with high probability that he/she has the entire file as the number of verifications increase.

However, problems still exist with this method. The User has to first maintain storage of the entire file, and also has to consistently request verification from the Miner. Users who are not Miners rarely operate their computers for 24 hours straight. Further, the method of proof requiring the User to maintain storage of the file is not consistent with the purpose of utilizing the Decentralized Data Storage.

The problems of the above-mentioned methods of proof are that the User has to continuously communicate with the Miner for verification and that the User also has to possess the original file. There needs to be a method of proof for continuously proving that the Miner is in possession of the file without such problems. One concept of proof that meets such requirements is zk-SNARKs.



< Verification Process Diagram>

If we apply zk-SNARKs, or "Zero-Knowledge Succinct Non-Interactive Argument of Knowledge," word-by-word to the situation of proving file storage for the Decentralized Data Storage, first, "Zero-Knowledge" means that the person requesting verification (User) does not have any information about the file that the verifier (Miner) has in his/her possession. "Succinct" means that no matter how large the file, the Miner must establish proof as fast as possible, and the result also has to be as small as possible. "Non-Interactive" means that the verifier only needs to unilaterally send final proof to the person requesting verification upon completing the verification process, without having the two parties simultaneously transmit proof to each other online during the verification. process. "Argument of Knowledge" means that the Miner needs to actually know the contents of the file. Instead of having the User directly verify the Miner's method of proof, zk-SNARKs is a verification method where any person on the blockchain network can verify the Miner's method of proof by using random seeds.

2.5 Blockchain

2.5.1 Orderbook

In the file storage market, when a User or Miner places a new order, it is transmitted to the blockchain network nodes. The received orders are recorded in a single order book / ledger. This order ledger / book is shared by all network nodes, and the contents of an order are relayed to all other nodes. Orders placed on the order book will be deleted from the order book after a certain period of time if the order fails to conclude. If an order is concluded, it is deleted from the order book and is signed by the User and the Miner and then sent to the network in the form of a transaction.

2.5.2 Transactions

Among the various types of actions that take place in the Decentralized Data Storage, transactions refer to those public actions that need to be recorded in the Ledger. Once an order of a User and Miner are concluded and signed by both parties, a transaction for **File Storage Contract** is created. After concluding the transaction for File Storage Contract, the Miner must generate a transaction for **Proof of File Storage** on fixed intervals during the file storage period. If the Miner does not generate a transaction for Proof of File Storage for the fixed interval or fails to do so, any participant of the blockchain network may create a transaction for Proof of File Storage Failure and transmit this to the network. If a User requests the contents of a file, a transaction for **Request for File Return** is created, and the Miner returns the contents of the file to the User. As such, when a Miner successfully responds to a request to return a file, or when it is necessary to transfer FDRs based on the success or failure of file storage, the User or the Miner records the transaction history for **FDR Claim**, combines it with the former transactions and transmits it to the blockchain network.

2.5.3 Pending Transaction Queue and Fees

When the User and the Miner makes a new transaction, the transaction is transmitted across the blockchain network. Before being transmitted across the blockchain network, however, the transaction is first included in the Pending Transaction Queue. The Pending Transaction Queue is shared among all market participants, and the transaction received by one node is also transmitted to all other nodes. A block Miner refers to the Pending Transaction Queue when making his/her next block. If the total size of data accumulated in the Pending Transaction Queue is greater than the maximum size of the creatable block, the block Miner takes into consideration the type of the block and the transaction fees to structure transactions with the most efficient combinations and includes those transactions in a block and transmits them across the blockchain network.

2.5.4 Blocks

Different transactions are included within the block data. A block miner is selected based on a mutually agreed algorithm and gets to mine blocks. However, if no block miner exists for the pertinent period, block is not generated. Transactions are selected from the transaction waitlist ((based on conditions)), and the block miner includes the selected transactions into the block. Newly generated blocks are disseminated into the entire network and receive confirmation from all network nodes. As a reward, the block miner receives awards for block generation and also receives commissions included in the block transactions.

2.5.5 Block Creation Consensus Algorithm

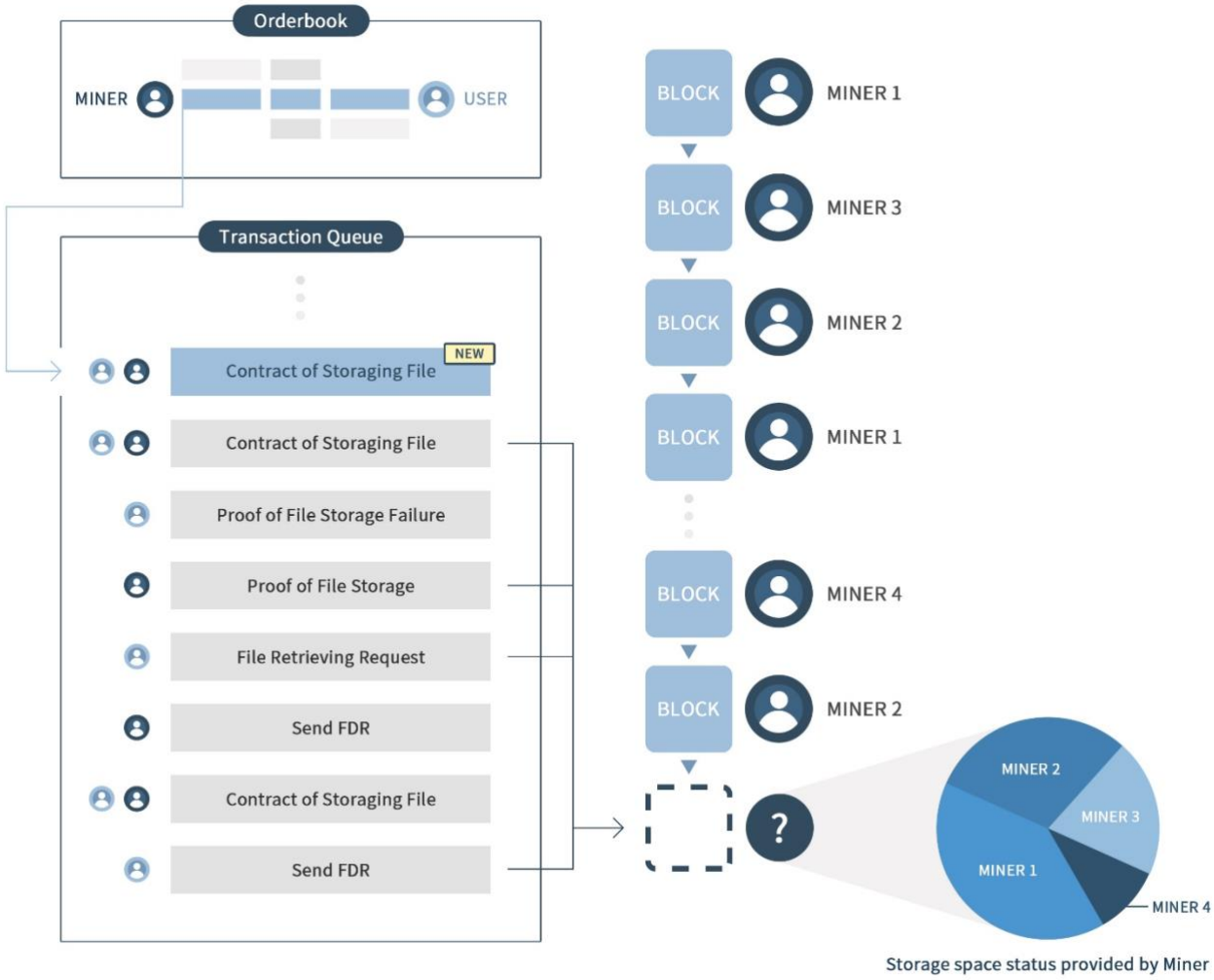
Most cryptocurrency such as the Bitcoin create blocks by using the Proof-of-Work method. In order to create a new block, the Proof-of-Work method requires repeated cryptographic work until the cryptographic hash function meeting a certain requirement is acquired. Therefore, a person who has greater Mining Power is more likely to mine new blocks.

In the alternative, other cryptocurrencies create blocks using the Proof-of-Stake method. In case of the Proof-of-Stake method, a person who has a larger stake on the blockchain network is more likely to mine new blocks. One example of Proof-of-Stake is providing opportunities to mine blocks pro rata to each Miner depending on the share of cryptocurrency in their possession.

Storage space is the most important resource for the Decentralized Data Storage. In case of the Proof-of-Work method, Miners have to possess not only storage space, but also Mining Power. High-performance CPUs and GPUs make it possible to increase the data process rate, but does not contribute to increasing the size or quality of storage space. Further, process rates above a certain rate is not required for dispersed data storage, which is one of the advantages of the Decentralized Data Storage.

The Proof-of-Work method is therefore not compatible with the blockchain we wish to implement. We will be using the Proof-of Storage method, which uses the total storage capacity of the currently concluded orders and provides Miners with great amounts of storage space, as our Block Creation Consensus Algorithm.

This concludes our brief introduction of FirmaChain's key technology, Decentralized Data Storage. From the following page, we introduce the management service for E-Contracts procedures, which uses Decentralized Data Storage to store contracts.



<Blockchain Diagram>

3. FirmaChain's DApp : E-Contract

3.1 Problems of Existing License Agreements for Intellectual Property Rights and Solutions Based on Blockchain Technologies

Contracts exist in every corner of our lives as an indispensable element in the modern society. Among the various types of contracts, written international contracts require at least one of the parties to travel abroad, as the parties should execute a contract in-person. As the entire process is very time- and cost-consuming, the execution of a written contract requires significant efforts.

When transmitting, modifying and executing a license agreement for IP rights electronically, there have been issues on forgery and security as well as verification of contracting parties. Exchanging drafts several times via emails or messengers has also caused many inconveniences. In particular, those who execute a contract for the first time with an unknown counterparty had no way of verifying the counterparty's identity, authorities or rights to execute the contract, or had to verify those in an extremely complicated way. However, the advent of blockchain technologies will solve all these problems.

Thus, **FirmaChain** and **E-Contract** combine the fundamental elements of a contract with blockchain technology to achieve our goal of creating a smooth process of contract execution and implementation between parties, and is also doing its best in tackling the aforementioned social problems.

The advantages of **FirmaChain**'s E-contract based on blockchain can be maximized in license agreements for IP rights such as patents, trademarks and copyrights (games, characters, animation, etc.). Therefore, such IP license agreements will be the first target of the new platform to be established by

FirmaChain.

The problems of the current license agreements are as follows:

It is difficult for a licensee who intends to execute an agreement to verify the actual holder (including exclusive licensees) of IP rights (patent, trademark, etc.). Their names or addresses can be identified in the official publication of patents issued by the Korea Intellectual Property Office, but the traditional way of executing international agreements did not have a clear mechanism to verify whether a licensor who claims to be holding the right is the actual licensor registered on the official publication of patents. Furthermore, in cases where an IP right has been transferred to a third party or licensed to an exclusive or non-exclusive licensee, it was more challenging to confirm the identities of those licensees and trace the actual licensor.

Licensors, too, were exposed to risks of fraud because they could not confirm the identity of a person who intends to execute a license agreement without meeting the person face-to-face.

Purchasers of a product to which a patent right was licensed or a trademark right was attached were not able to verify whether the product had been manufactured by a person legitimately holding the right. It was difficult for a third party to obtain information on the period of the patent rights and trademark rights, and the accurate coverage of the licensor (including exclusive licensee).

Even if there was a known IP right holder, it was difficult to actually execute an agreement with that person because of the vast amount of time and cost required to sign a written agreement. An IP right holder also faced a wide range of practical problems (time and cost) in finding a person who desires to use his or her IP in another country. The process of cross-border remittance of fees and payment of taxes, etc. was at all times exposed to risks of fraud and caused inconveniences and nuisances.

In order to address the abovementioned problems, FirmaChain will offer a solution as follows:

1. As long as accessible to the internets, the users can confirm the details of IP rights, including the type of IP rights, the titleholder, and the coverage (geographic coverage).
2. The introduction of blockchain-based electronic contracts in the entire process of contract execution will enable the users to record and verify the whole contracting process, such as negotiations and transaction history, etc.
3. A licensor of an IP right who has been confirmed to be the legitimate titleholder and a licensee whose identity has been verified can execute an international contract online rapidly and free from any risk of fraud using the electronic contract platform (E-Contract) without physically meeting each other. In particular, the platform will secure the reliability in executing a contract with an unknown counterparty.
4. Various useful functions, e.g. dashboards, provision of standard contract forms, real-time translation, etc., will be provided to facilitate rapid and convenient execution of contracts. IP rights will be protected in a prompt and affordable manner since lawyers provide real-time online reviews for final drafts and patent attorneys will register the exclusive license in the relevant country after execution of the contract.

5. FirmaChain platform will allow the IP holders to easily locate the potential licensees and thereby facilitate the execution of diverse license agreements at lower costs.

FirmaChain's solution will expand the international license market and improve the transparency in relevant transactions.

3.2 Problems with written contracts and advantages of E-contracts

There are many problems in our society due to people's preference for written contracts, and this includes the problems mentioned earlier. On the onset, each party share 1 copy each of the written contract, but it is difficult to synchronize any subsequent revisions, and it can also easily give rise to fraud issues. Numerous companies try to follow the content modification timeline by using external elements such as emails and voice recordings, but this is difficult to manage. Even if the problem of forgery in writing is a huge problem that may lead to a legal battle, there is no way to prevent it. In order to solve these problems, electronic contracts emerged in our society.

Electronic contracts are a way to digitize contractual agreements between companies. Electronic documents of a similar concept (Electronic Transactions Act) are recognized as having the same legal effect as paper documents. In domestic and overseas laws related to commercial transactions, it is stipulated that electronic signatures (Digital Signature Act) have a legal effect. As a result, electronic contracts have also become legally valid.

Currently, the efficiency of electronic contracts is superior to written contracts. However, it is not preferred over written contracts because certain problems are unavoidable, such as contracts by unauthorized people, burdens that come from transmission risks due to system failures, and so on. In addition, companies that have yet to advance are taking the position to adhere to these traditional methods, so the position of the technology of electronic contracts is still under-estimated and is regarded as an unnecessary technology.

FirmaChain has the goal of making electronic documents and contracts transparent and reliable by using the characteristics of the blockchain, and thereby solving the current problems.

3.3 Why E-Contract?

<Create and implement a rational contract with e-contracts>

From an advanced modern society perspective, we are using fairly primitive methods when making and implementing large and small contracts. For example, we go through several email exchanges to send and receive contracts, or sometimes we would exchange contracts on the day itself. Some don't check the contents of the contract properly before implementing it, use legally inaccurate seals or stamps with no information, or even try to proceed with work without making a contract at all because it costs time to create one.

In addition, many companies undergo contracts with large transaction costs and long contract period, and by doing so, they only manage the contents, such as the contract's progress, status, additional work, modifications to the contract, etc. in writing, so the timeline becomes difficult to manage.

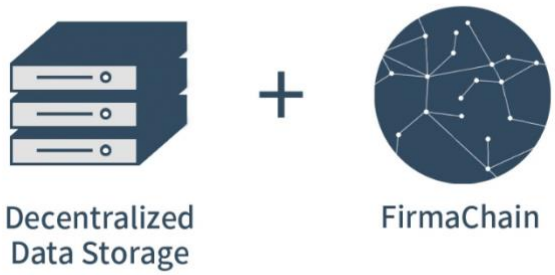
The **E-Contract (DApp)**, which uses **FirmaChain**, provides a trans-parent ledger through a smart contract and public chain, which means both legality and stability can be assured. It is convenient in managing the contents needed when creating contracts, and allows users to work efficiently by using the necessary functions. In addition, it can reason-ably solve the problem on transaction fees by replacing the currency used for the contract with cryptocurrency. In particular, it can solve problems when creating multinational contracts such as double taxation, overseas corporation establishment problems, overseas remittance, etc., so it can allow people to carry their business plans efficiently.

As described in the service structure, E-Contract will provide several functions. (Enforced security parameters for electronic contracts, form presets for standard contracts, contract edit and management)

4. Structure of E-Contract

E-Contract is divided into: **1) The core layer** where encrypted contract data is stored, and the contract transaction is saved; **2) The application layer** which creates and manages the contracts using DApp; **3) The service layer** which verifies and processes electronic contracts, and connects the core layer and application layer.

4.1 Core Layer (FirmaChain)



FirmaChain is used to transfer and collect transactions, distribute the finite-state for the entire contract procedure, verify the integrity of electronic documents, and protect the contract data from forgery. The contract will have a finite-state for each phrase, and the details are as follows. The states that will actually be implemented are going to be broken down further.

Establishment of contract

In order to confirm the payment ability of the party paying at the time of the contract creation, a certain percentage of the initial transaction price shall be set as the deposit under the agreement of the parties. The transaction price will be in local currency or **FirmaChain Token (i.e. FCT)**. If the transaction price will be in local currency, the deposit will not be necessary.

After the contract is written, the contract will be written in the Decentralized Data Storage once the parties have reviewed and confirmed its details. In this "waiting to upload" stage, the paying party should have money more than the deposit amount in their wallet, and they must remit the money in case they need to pay for certain fees in advance, such as a deposit. Once this process is complete, the status is changed to "in progress." Once the contract is in this stage, the transaction history containing the ***Hash String** is uploaded in the Smart Contract. All parties involved can now implement the contract. When using local currency as the transaction price, the party must create a transaction in the Smart Contract without FCT, and must include a proof of transaction in the electronic documents of the corresponding contract, such as a passbook transaction history or transfer document.

Progress of contract

The contract will be processed, and the transaction amount will be remitted either in FCT or local currency depending on the agreement. In the blockchain and service layer, check the transaction of the remittance to determine the progress of the contract.

Completion of contract

When the payment of the transaction amount written in the contract is completed, the status of the corresponding contract is changed to "waiting for completion." Once the contents of the contract are verified and confirmed between the parties, the status is changed to "completed" and the settlement cost will be given to the party that receives the contract.

Destruction of contract

The contract may be destroyed due to circumstances mutual to both parties while the contract is in progress. A contract that has already been uploaded cannot be deleted, and can only be destroyed by creating an additional contract to override the original. In this case, the information of the destroyed contract will be entered on the E-Contract, and a settlement agreement between both parties, or a refund or additional payment request according to the contract will be settled by creating a new payment contract based on the destroyed contract.

When the contract is cancelled due to certain reasons between the parties, the E-Contract service actively supports the technical part so that the data stored in the Decentralized Data Storage regarding all the details that took place in the contract process can be easily browsed.

Modification of contract

If there is a sudden problem unforeseen at the time of the contract process, the parties may change the contents of the contract through a special contract. Once the parties create a special contract and all persons involved agree to such, the corresponding special contract will be attached as a subcontract of the main contract. In addition, the Hash String of the subcontract will be uploaded to the Smart Contract, and the contents of the subcontract will be uploaded in the Decentralized Data Storage.

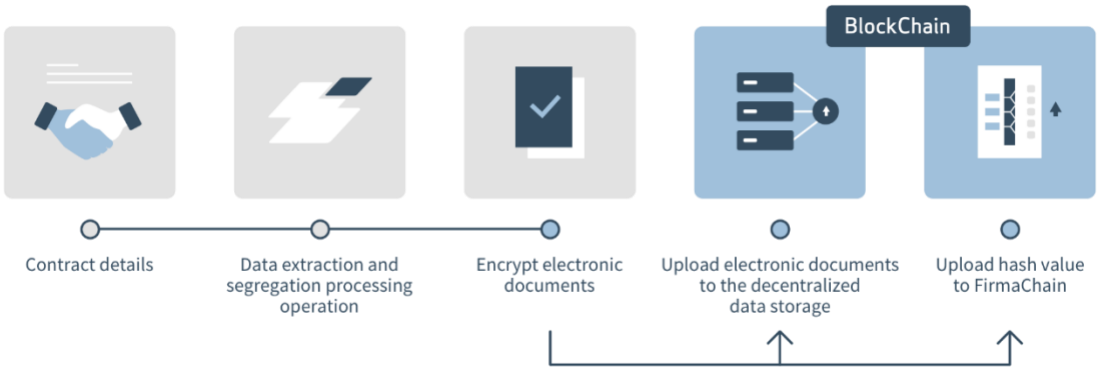
If there are any changes to the transaction amount when amending the contract, the amount of the new deposit will be additionally remitted or refunded depending on the deposit amount set previously.

***Hash String**

A **Hash String** uses a cryptographic hash function to map a data of arbitrary length to a string of fixed length. This function is a unidirectional function, so it cannot obtain the original data from the Hash String. Even a slight modification to the original will create a completely different Hash String, so it can check the integrity of the data and is used as the unique identification value of electronic documents at FirmaChain. For cryptographic hash functions, proven algorithms such as SHA256 or SHA512 are used.

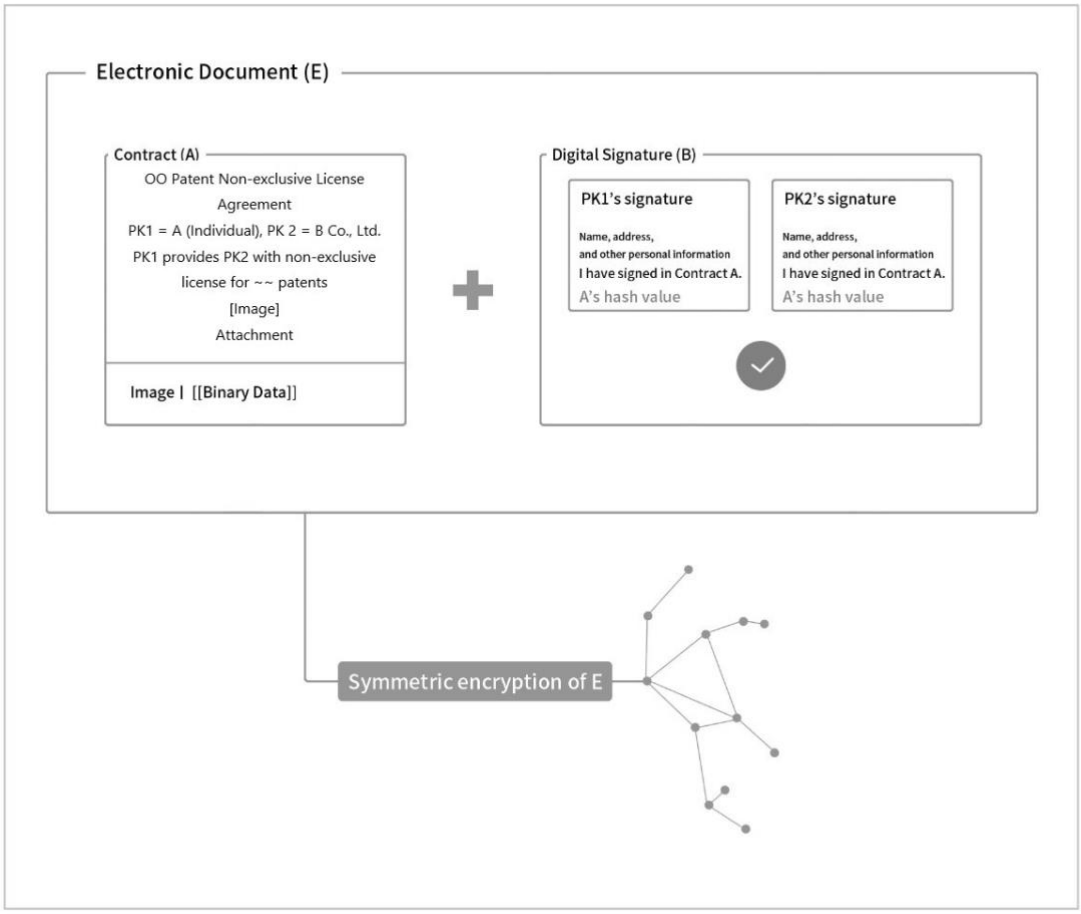
4.2 Service Layer (Firma Network)

The Firma Network acts as a processor and inspector between the application layer, which is the E-Contract service, and the core layer. The contract is created through the E-Contract, and it needs to undergo a processing operation in the middle before it can be uploaded on the **FirmaChain**.



The processing operation refers to processing the text data and other data (such as images, music, recordings, etc.) found in the electronic contract document and uploading it to the Decentralized Data Storage. Generally, users are recommended to make the contract data composed of a text data only.

However, there are contacts in which non-text contents are necessary. For these types of contracts, if the electronic documents produced using the Markdown syntax, which is supported by the E-Contract, are transferred to the Firma Network, the images and other files part of the contract are included in the electronic document. Also, in the case of electronic signatures, they are replaced with ***digital signatures** (using a public key cryptographic method, e.g. RSA, Merkle, Signature, etc.). With this, a unified document is uploaded to the Decentralized Data Storage once the processing operation is finished.



The contracting parties will receive a public key (PK) and a secret key (SK) created by the RSA method upon signing up on the E-Contract service, and each contracting party will have one key pair.

In the contract section, the contracting parties' PK are included. Before we jump into the explanation, let us assume that there are 2 contracting parties, and we will refer to each pair of keys (SK and PK) as (SK1, PK1) and (SK2, PK2). In the digital signature section (B), the message that includes the personal or company information as well as the agreement to fulfill the contents of Contract A are encrypted with their own SK for both contracting parties. The Hash String of Contract A is included in the message in order to identify Contract A.

An electronic document , E , containing both Contract A and Digital Signature B is created, and the keys are issued only to the contracting parties using a symmetric password cryptographic system. This is uploaded to the Decentralized Data Storage. The Hash String of the document is uploaded to the Smart Contract of FirmaChain, and the contract is implemented.

Patent Right Licensing Agreement (for Exclusive License)

This Agreement is made and entered into by and between A Co., Ltd. ("Company A") and B Co., Ltd. ("Company B") as follows:

Article 1 (Purpose)

Company A shall grant an exclusive license for the patent right held by Company A as specified below (the "Patent") to Company B:

Patent Number	No.
Title of Invention	

Article 2 (Registration of License)

Upon execution of this Agreement, Company B may register the establishment of the license indicated in the preceding Article at its own expense. Company A shall cooperate therefor.

Article 3 (Coverage of License)

The coverage of Company B's use of the Patent is as follows:

1. Region: Republic of Korea
2. Period: X years from X X, 20XX
3. Type of use: Manufacturing and sale

...

Article 13 (Non-refund of Licensing Fee)

In no case shall Company B return the licensing fee that it has already received.

Article 14 (Termination)

Upon the occurrence of one of following events, Company A may terminate this Agreement immediately without giving notice to Company B:

1. Company B fails to pay the licensing fee in a timely manner;
2. Company B fails to use the Patent within X months from the date of execution of this Agreement without a justifiable reason; or
3. Any of the notes or checks that Company B has issued or endorsed is in default.

...

Attachment. Contract Contents

[[image::Binary Data...]]

Digital Signature of Company A:
[[Digital Signature::0GCSqGSZKjeGcjDlb3D...]]

Digital Signature of Company B
[[Digital Signature::DOL5Ulsuulb3DQEISaC...]]

< Example of an electronic document before encryption after the processing is complete>

The example shown above is an electronic document that has been processed. This electronic document consists of a text data that includes the contents of the contract; a binary or base64-encoded data, such as images, music, recordings, etc.; and a Public Key that can verify the digital signature of the parties at any time.

The above example may be subject to some revisions after reviewing it with our partner law firm to ensure the effectivity of legal evidence of the electronic documents and electronic contracts.

$A = Contents\ of\ a\ contract$

$E_K(M)$:*Encrypt M by using key K*

$HASH_A = SHA256(A)$

$S = Secret\ key\ of\ A$

$SK, PK = KEY\_GENERATE()$

$M1 = "Information\ about\ PK1,\ I\ agree\ with\ this\ contract(HASH_A)'$

$M2 = "Information\ about\ PK2,\ I\ agree\ with\ this\ contract(HASH_A)'$

$S1 = E_{SK1}(M1)$

$S2 = E_{SK2}(M2)$

$B = S1||S2$

$W = A||B$

$C_W = E_S(W)$

$HASH_W = SHA256(C_W)$

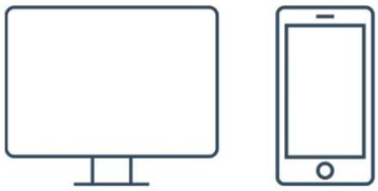
$HASH_W \rightarrow Smart\ Contract$

$C_W \rightarrow Decentralized\ Data\ Storage$

The above formula illustrates the process of creating an electronic document that is uploaded to the Decentralized Data Storage by combining the contents of the contract and the digital signature. As E-Contract development progresses, changes may occur if a more efficient and more secure algorithm is discovered.

These types of processing operations are only used in E-Contracts. Other DApps using the Firma Network can create various processing algorithms to suit the nature of the service. This allows us to create a variety of services through the efficacy of the contract, and this will become the basis for producing various electronic document-based services.

4.3 Application Layer (DApp)



The basic role of the **E-Contract (DApp, Decentralized Application)** is to write contracts, make necessary modifications under the agreement of the parties, receive confirmation from all contracting parties, and upload this state to the blockchain. In addition, the E-Contract will carry out all core tasks required for the contract such as confirming and changing the status, by connecting the Smart Contract code of the Ethereum. The parties may check the contract before signing, and all of the contract processes after signing can be managed using the E-Contract. In addition, as mentioned in the introduction, many functions are available to assist in the contract writing and implementation process, some of which are described below.

Markdown and Visual Editor that help in writing contracts

You can create a contract using DApp. The content creation should be done according to the Markdown syntax as defined by the E-Contract in order to textualize the data. Of course, it supports Visual Editor (WYSIWYG) for those users who have trouble using Markdown syntax. In addition, it also provides a conversion function to enable the use of existing contract formats such as doc and hwp.

Security enhancement system for digital signatures

Most electronic signature services are written directly on the digital canvas above the contract. However, this can easily be done by someone else as a proxy, and one cannot expect to have the same non-repudiation effect as an authorized certificate. Signatures affixed in written contracts are also exposed to such risks. Even if this may have legal effect, in case this happens, it is difficult to determine who actually affixed the signature. E-Contract allows users to use a **digital signature registration system** provided by Firma Network after signing up. This system makes it easier to have proof when a legal dispute arises. The details are given below.

Standard contract preset support

You may receive legal advice from E-Contract and retrieve various standard contracts in the industry that were reasonably prepared by E-Contract before the time of writing. If the contract is not significantly different from the standard contract, users can immediately create a contract by changing only the parties to the transaction, contracting entities, project name, transaction amount, date, etc. In addition, users may edit the standard contract and save the contract they have created.

Identifying progress and revision history of contract

Users can determine the progress of their agreement through the E-Contract. In addition, when the contents of the contract are changed, users can add DiffTool to compare which parts have been modified or deleted and they will be able to see the changes at a glance. This tool will help the contracting parties recognize the modifications that took place in the contract.

Legal advice on international contracts

There may be cases wherein it is difficult to draft international contracts due to differences in customs and laws between countries. Upon comparing and analyzing such cases, we are now able to provide a Tooltip for legal advice when creating contracts. In addition, we are also planning to provide one-on-one legal advisory services in the future for contracts with large or frequent transactions.

Besides this, various convenience functions will be added to make it easier to implement the contract.

For the E-Contract web services, we are planning to build a server with Node.js Framework using JavaScript (ES7 standard). For the web, we plan to apply the ReactJS library. The reason why we chose ReactJS is that it is a library optimized for creating a view that is easy to see and understand so that the parties may implement the contract in an easier way.

The mobile services are in the planning stage. The main service will be done via web, and we are planning to provide various functions such as chatting between the contracting parties, notifications of the contract progress, etc., on mobile. We will be using React Native, or build it using the native language of the platform (iOS and Android).

The technology to be used in the service development has been chosen on the basis of our goal: to develop as quickly as possible while allowing us to have a stable and efficient development.

In addition, we will create and distribute an SDK, which will allow users to use electronic contracts and signatures, one of the core functions of the E-Contract service, in a modular format for all web and app services that require contracts. We are also planning to produce various electronic document services using FirmaChain.

5. Token Economy

5.1 Ecosystem Structure

As mentioned before, Firma Chain's token economy on the application layer consists of E-Contract customers and professional service providers within E-Contract. The token economy of Firma Chain's DDS and the token economy of Firma Chain's application layer exists separately and will be explained below. FCT is the basic currency within Firma Chain's economy and FDR is a form of bonus that can be obtained through using Firma Chain's services. FDR can be exchanged for FCT, but also be used to increase credibility score which comes with several benefits within the platform. Credibility score is applied to both users and service providers and is a measure of loyalty and credibility within the platform.

5.2 Application Layer Bonus Structure for Service Provider

5.2.1 Credibility Score

Service providers (hereinafter the provider) receive bonuses in the form of FDR depending on their contribution. Providers can switch in their FDR to FCT, but can also hold their FDR to increase their Credibility Score (CS) which is calculated for the purpose of differentiating quality service providers. Providers who hold their FDR to increase their Credibility Score are benefited for their loyalty and quality service by obtaining for example; a higher hourly rate. The form of which providers who have higher credibility scores may change according to market responses. Naturally the demand for providers with higher credibility scores will rise and according to the demand, the provider will be able to benefit from the high demand. This is mainly to build a stable community of providers and users, but also to reward returning providers with higher bonuses and users with higher quality services. The determining factor, credibility score, is calculated by the equation below

$$CS_{r,n}(L) = \frac{\sum_{i=1}^{n} L_k(1-r)^{k-1}}{\sum_{i=1}^{n}(1-r)^{k-1}}$$

(r,n is a constant determined by the service provided and Li within the equation L = {Li} is the average sum of FDR held over time i, 30 days. (ex: L1 would be the average number of FDR held over 30 days)

5.2.2 Application Layer Bonus Structure for Customers

Firma Chain's first DApp E-Contract is an electronic contract platform that also provides legal opinion within the service. Customers are rewarded FDR for using these services according to the equation below.

$$FDR_{a,b,r}(c) = ar^{[log_b c]}$$

$$(a > 0, b > 1, 0 < r < 1)$$

. (a,b,r are constants that are determined by the service provided while c is the frequency of which the service has been used over a short period)

Customers can exchange the FDR they have received to FCT and use services within the DApp or exchange their FCT to fiat currency through an exchange. Customers are also benefited for holding on to their FDR. According to the sum of FDR that the customer has received from using services within Firma Chain's DApp, they are awarded with monthly loyalty programs at different tiers. Customers are rewarded with discounts and other benefits depending on their tier. The sum of FDR that the customer holds is calculated by the equation below.

$$\text{Net Gain} = \text{Gross Gain} - \text{Converted to FCT}$$

5.3 The Circulation Ecosystem of FDR and FCT

FDR and FCT may have a close relationship, but are not directly related. In the beginning, Firma Chain will reserve FCT for the sole purpose of exchanging the FDR users request. An equal amount of FDR is issued according to the FCT reserve the company sets. This newly issued FDR is used as bonus within the application layer.

When a user requests for an exchange of their FDR to FCT, Firma Chain will exchange this FDR to FCT from the reserve pool that has been made for the sole purpose of exchanging FDR to FCT. Firma Chain will keep a portion of the FCT users pay in order to use Firma Chain's services and designate it into the reserve pool to always have enough FCT to exchange.

To prevent issues like exchanging a very large sum of FDR at once, Firma Chain will limit users of how much FDR they can exchange in a period of time. This is calculated by the equation below.

$$CAP_T(D) = \min\left(M - a \cdot \max(0, T - D), \frac{D}{b}\right)$$

$$\left(M, T > 0, b > 1, 0 < a < \frac{M}{T}\right)$$

(D is the reserve of FCT for exchange purposes while T is the total circulation supply of FDR)

By setting a cap on the amount of FDR swapped over time, this can prevent from shortage of FCT and failing to exchange FDR to FCT for all users. However, if the cap does not satisfy the users expectations, this system will fail to operate normally. For example, if there is a gap between how many FDR is issued and how many are in circulation, the system will fail. In situations like this, Firma Chain will burn FDR to close this gap within the range of the amount of FCT in reservation for exchange. Additionally, the constants which are factored into how much FDR users receive within the platform will be adjusted accordingly.

6. Roadmap

2018

02 FirmaChain R&D

04 Whitepaper version 1.0 release

11 Launch of E-Contract prototype

Q4 Launch of E-Contract Main Service

2019

Q1 IPFS applied E-Contract service release

Q2 Target 100+ Enterprise Solution Contracts

Q3 Decentralized Data Storage Test-Net Activated / Launch of Test-net based E-contract

Q4 Finalize Updates & Release Firma Network

2020

Q1 Decentralized Data Storage Main-Net Activated /
Target 1000+ Enterprise Solution Contracts on Firma Network and SDK release

7. Token Generation Event (ICO)

Total capacity : 600,000,000 FCT (FirmaChain Token)
Sales Cap : 300,000,000 FCT

There will be no additional tokens to be issued from the total issue volume. Company-owned tokens will be locked up for 1 year to maintain the Firma blockchain. In addition, community and promotional tokens will be used for marketing purposes, such as the promotion of Firma community and/or having an air drop event once the FCT is listed on exchange.

8. Team

Young Yoon

Chief Executive Officer

Jack Lee

Chief Technology Officer

Bullisay Park

Chief Architect Blockchain

Jason Yoon

General Manager UI / UX & Marketing

Simon Lee

Global Business North America

Alex Sangwon Ye

Global Business North America

Justin Wee

Global Business India

Wan Kim

Global Business China

Timothy Kim

Marketing Manager

Jason Park

Blockchain Developer

Ben Park

Blockchain Developer

Jason Piao

Blockchain Developer

Juchan Park

Front-end Developer

Dana Kim

Digital Media Designer

Robert Han

Community Manager

Sanghyeok Lim

Marketing

9. Advisor

Ju Young Song

Lawyer
Milbank, Tweed,
Hadley & McCloy LLP

By utilizing smart contracts with blockchain technology, complication procedures can easily be streamlined and simplified. Due to this, costs related to legal disputes or forced enforcement can also be minimized. The implementation of this process into various fields of our society can bring about revolutionary and innovative change to everyday lives.

FirmaChain uses blockchain's transparency and reliability to create a contract management service that remedies the current shortcomings of written contracts. In addition to reducing risks from contract defaults, we believe that time and costs will be optimized. FirmaChain will open the potential of smart contracts and we firmly believe that it will elevate smart contracts to a new level. We are excited and looking forward to the positive changes that FirmaChain will bring to our future.

Han Jong Lee

CEO
Goodtimewith.me

Firma chain's vision is to reform the basis of our modern society, the written contract, by eliminating its various complications through the decentralization, transparency and credibility that block chains offer.

Especially in the case of multinational contracts, issues of conflict such as country-by-country double taxation, overseas incorporation, remittance abroad, and fee arrangement can be resolved transparently and effectively with our technical skills that are basd on a framework of economic growth. With hopes to materialize such vision, along with our prolonged teamwork, and quick, flexible executions, Firma team invites you to join us on a challenge that seeks

Jihwan Won
Managing Director
KJ DNS

The name FirmaChain is derived from a combination of the word 'Firma', which means signature in Italian, and 'Chain', which is short for blockchain technology. It represents the concept of an innovative technology for public ledgers through the decentralization of all documents that require signatures, including contracts.

We are gradually moving away from the analog era and towards the future, a digital era, so it is only natural for a sudden rise in blockchain technology within the large-scale sharing network between peer to peer users to increase transparency and reliability in lowering the possibilities of information change. Within the construction industry, we expect blockchain technology to be the key to improving potential factors for unfair transactions such as unfair unit price fixation, contract change and more that are made by the contractor/subcontractor's abuse of their superior status. In 2018, the beginning of the New Information age, we hope FirmaChain becomes a leading industry in offering services that will change the world.

Hyeonwook Jeong
CEO / Founder
beSUCCESS

There are still lots of spaces that can be improved in the blockchain-based data storage, especially in the form of electronic documents and contracts. I have seen and worked with the FirmaChain team from the early stage.

Based on my personal experience, I believe FirmaChain will keep growing and will remain strong in the future, because it is handled by a solid team with a realistic road map. Due to its strong development team, FirmaChain also has a high potential for producing solutions that can bring more innovation to the transaction and can add even more speed to it. Personally, I am excited to be joining as an adviser and am happy to support the global expansion of this project.

Guho Son

CEO
Monument Company
Former Managing Director of
SoftBank Ventures,

Starting with the financial industry, blockchain has been leading the 4th industrial revolution and is believed to be the leading technology. The numerous count of devices and the skyrocketing trade volume has caused traditional cloud based centralised systems various problems such as system maintenance, and security.

FirmaChain's solution will create a more transparent and secure resolution not only for the financial industry, but in retail, manufacturing, and in resolving social-cultural issues, ultimately bringing a positive impact to our economy.

Jiwook Kim

Attorney at law
Partner at Yoon & Yang LLC

Blockchain technology, based on the responsibility of the participants within the network, verifies transactions and decentralizes encrypted information allowing for better transparency and security. FirmaChain utilizes these aspects of the blockchain and has formulated a blockchain-based electronic contract platform. This allows for simplified contract procedures (drafting, negotiating, closing) and by uploading to the blockchain network this contract can be verified by those participating in the network, eliminating the risks of forgery and emphasizing transparency for safe contract management. FirmaChain is the solution to the disadvantages we experience with traditional contracts.

Joonwoo Kang

COO

Hexlant

2018.01 ~	Hexlant COO
2017.01 ~ 2017.08	BuildIT CTO
2014.08 ~ 2017.01	Samsung Electronics Software Engineer

Seongsan Lee

CEO

SPIN Protocol

2018.09 ~	SPIN Protocol CEO
2018.06 ~ 2018.09	Director of Global Sales and Business Development. SOOM -Foundation
2018.02 ~ 2018.08	International Business Development Manager. Minds Lab, Inc
2014.05 ~ 2018.02	Senior Manager, Trade / Investment and Business Development. KOTRA

10. Partnership

Strategic Partners

Ecosystem Partners

Press

11. Disclaimer

The Firma team (collectively referred to as "Firma Solutions" and its stakeholders, employees, and affiliates) has written this white paper to the many people who have shown their interest and love towards FirmaChain for reference purposes only so that we can provide a more detailed information about the chain and team that the Firma team is planning.

In other words, this white paper is not meant to invite you to invest in the Firma team or the chain, and it has nothing to do with such purposes. Also, the Firma team is writing this paper "as is" for you and it does not guarantee that any of the contents of this paper, including its conclusions, will be accurate until the future.

The Firma team does not declare or guarantee the accuracy of any information on this white paper, and assumes no legal responsibility for such. For example, the Firma team does not guarantee (i) that this white paper is written based on legal rights and that it does not infringe the rights of a third party, (ii) whether this white paper is commercially valuable or useful, (iii) whether this paper is appropriate for a particular purpose you may have, and (iv) that there are no errors in the contents of the white paper. Of course, the range of exemptions to liability is not limited to the previous examples.

If you use this white paper in your decision-making and actions (including, but not limited to, using this white paper as reference or as evidence), the consequences thereof are entirely your responsibility, whether it results to profit or loss. In other words, please note that if any damages, losses, debts, or any other damages occur by using this white paper, the Firma team will not be liable for any reparation, compensation, etc. to you.