DAVINCI PROJECT

TECHNICAL WHITE PAPER

The world's first blockchain ecosystem for
building and deploying decenterazed application

VERSION 2.2 (07/26.2018)

Category

1 Abstract

As digital asset has become diverse and increasingly difficult to manage, the emergence of integrated digital asset has been considered as a crucial topic. However, due to lack of comprehensive foundation, there is no consistency in the method of payment. Moreover, flow and security of transactions, convenience, and, even anonymity cannot be guaranteed. Currently the digitalization of real economic assets and their expansions have risen as a global issue. Digitized economic assets are expected to be significant part of future finance, but problems to solve still exist as well.

Our society is anticipated to enter a full-scale digital economy through active public participation and problem resolution via digital finance, which is based on digital asset. Centralized financial system has been dominated methods of payment, settlement, loans, stocks, derivatives, and inter-country transactions until now. On the other hand, forthcoming decentralized digital economy is expected to be structured with the collection of digital assets and number.

The main function of the blockchain is to settle disputes among network participants. Before the adoption of blockchain, multilateral consensus among several financial products is almost impossible to reach in financial transaction. With guaranteed transparency of blockchain, reliability of the structure increases along with participants' recognition of data transparency and anti-counterfeiting mechanism. Additional affirmative aspect of the blockchain is its resistance to modification of the data and making undue profit with asymmetry of information. Even with its transparency and efficiency, further discussion still exists between a payment processing company and a financial institution that serves as a gateway .

To settle above issue, Davinci platform, which is based on high-technology and proven marketing operation experience, gathers numerous information about asset, payment, insurance, society, credit, culture and medical care. By connecting accumulated information and asset, Davinci platform is able to bring down barriers of diverse field to provide a secure and convenient payment ecosystem.

2.1 Application of Blockchain Technology

2 Introduction

In 2009, Satoshi Nakamoto proposed peer-to-per(P2P) electronic transaction system, Bitcoin, generated by specific algorithm and calculation. Bitcoin economy is found on distributed database that is constructed

by numerous nodes, which all transaction is encoded and recorded to ensure the reliability of the monetary circulation. P2P's decentralized characteristic and algorithm prevent artificial manipulation of monetary value during the acquisition(mining) of bitcoin. Thus, transparency, ownership, and the anonymity of transaction are secured and ensured. By appending smart contract mechanism to bitcoin's decentralized blockchain system, Vitalik Buterin created Ethereum in 2015. As an open-source, Ethereum is a public blockchain platform with function of smart contract. Ethereum's ultimate goal is to allow variety of applications in programs or consensus protocol of blockchain by users.

Ethereum's script language, called EVM (Ethereum Virtual Machine), provides various modules to users. Its technology has been quickly recognized in the market by allowing users to construct their own applications. Along with the improvement of Ethereum, other blockchain technology also continuously pursues for further innovations. Blockchain is in its heyday with complementation of offline trading by implementing the 'lightning network' in the smart contract.

The major sources of blockchain's rapid growth are the simplification of existing transaction and its convenience. Moreover, anonymity and transaction transparency also have contributed to the development. Progress of blockchain shed a light on the possibility to decentralize the current centralized system. Reconstructing the centralized financial ecosystem from the understructure level is a significant innovation that is not bound by the regulation. It is certain that blockchain technology has brought a revolution in cryptocurrency, but various steps still exist in order to apply blockchain in real life and economy. For the actual application of blockchain, the linkage of decentralized blockchain is necessary to construct blockchain network. Furthermore, with its capability to dissolve a series of process such as funding, transfer, authentication into a blockchain, cryptocurrency will be ubiquitously applied, and finally achieved enhancement in its ecosystem.

2.2 Blockchain and Davinci Project

The world is assembled by numerous communities ranging from individuals to families, as a small community, and from workplace to society, as a big community. Each community is closely intertwined and organized by a close structural network environment where all modernized members of society coexists. In the future, these communities are expected to be linked to the decentralized blockchain, which also would be closely connected to another community's blockchain. The chain of network will allow communities to form a distinctive ecosystem. This unique ecosystem will assist self-development and freedom of all members, and the "Davinci Project" will be the significant component of the ecosystem.

Davinci Project has built highly efficient, fast, secured, and simplified payment system. The project also has strengthened global transaction to blur the currency boundary, and minimized the complexity of financial and accounting verification process. Furthermore, management of credit information will be more transparent, and this will allow insurers to alleviate dispute and justify a claim for compensation. Decentralization of encrypted network has reinforced security and reduced costs. Surplus resources are shared through network, and the record of food and product would be easily traced. Lastly, digitalization of the real estate transaction details will strengthen the transparency.

2.3 Background

Cryptocurrency market share of Republic of Korea has remained only 5 percent of its global market in 2016. Restriction policies of Chinese government on cryptocurrency such as the prohibition of ICO and Bitcoin exploitation cause diminishment of Chinese cryptocurrency market. As a result, the capital of cryptocurrency has pushed into countries where the transaction is allowed. Under this circumstance, Republic of Korea as the IT powerhouse seized the opportunity to expand the market share to 25 percent and became a huge shareholder of global market with its domestic exchanges.

As a new concept of currency, cryptocurrency has raised public's interest and concern regarding on blockchain. To prevent rash speculation, Korean government has restricted cryptocurrency exchange. However, with fast acknowledgement on its rich value, the government has presented policies for transparent transaction by legalization of cryptocurrency.

Republic of Korea, globally known as IT powerhouse, has formed a various collaboration project on blockchain and cryptocurrency. The innovative research and projects are expected to recover country's international finance status, which has lagged behind in the past. Also, in this important age of transformation in digital finance, Republic of Korea puts its efforts to become the international base of digital assets.

2.4 Start of Joint Project between South Korea & China and Arise of Korean Wave

Korean pop culture has gone viral in Asia since the introduction of Korean dramas to China in 1996 and the spread of Korean pop songs. Rapid cultural expansion in China and Taiwan naturally coined the term "Korean Wave." The Korean Wave has not only landed to China, but also propagated several countries including Taiwan, Hong Kong, Vietnam, Thailand, Indonesia, Philippines, and etc. Especially after 2002, Korean products such as food and electronic devices are largely preferred along with cultural media like drama, music, and movie. This cultural trends, in a comprehensive sense, refers to hanryu, the Korean Wave.

After 1996, Korean wave became one of the biggest contents in China and achieved great success in overseas markets. However, installation of Terminal High Altitude Area Defense (THAAD) caused the decrease in exchange between Korea and China and negatively affected Korean Wave as well.

According to trade statistic in 2017, the proportion of the trade with China accounted over 20 percent (24.8% for export, 20.5% for import) of total Korea trade, which ranked as the first in both exports and imports. China imported 9.9 percent of its total trade from Republic of Korea, which ranked as the first surpassing Japan. Korea is also placed as a 4th in China's export by covering 4.3 percent of total.

Compared to the trade growth prior to 2017, the large scale of the China-Korea trade has noticeably diminished. Unexpected diplomatic issues have negatively affected the inter-country exchanges between Korea and China, and public demands for the resolution at the civilian level have been raised accordingly. Therefore, beyond diplomatic barriers, companies of China and Korea have decided to join forces to find solutions in cultural sector. The Davinci Project was initiated to promote non-governmental exchanges between Korea and China through the blockchain technology of Korea, an IT powerhouse.

3 Davinci Project

With collaborations of diverse fields including cultural sector, Davinci project comprehends not only the domestic but also the international level exchanges as a non-governmental network. The project is expected to be the important communication hub while cooperating and linking people and organizations from all over the world. Similar to the invention of boat and plane, allowed people to travel any part of the globe, Davinci project exploits the trade route and the cultural exchange in digital ground as a pioneer.

Within Davinci network, the blockchain connection is cultivated through Davinci Token. The token can be traced and utilized as a payment method for any financial transactions including overseas' trade, shopping, insurance, house loan, or even cell phone charge. Even in this simple purchase, data and personal information movement and unnecessary confirmation are inevitable. These processes incur costs, and individual members of the society have to bear the burden. To guarantee people's right to receive better services, this inefficient steps and costs shall be reduced.

The blockchain system is composed of a six-layer structure: data layer, network layer, consensus layer, incentive layer, contract layer and application layer. The comprehensive design established with previous and Davinci's blockchain systems has two layers- the upper and lower layer. The upper, usually contains the presentation layer and the application layer, is mostly stable. Blockchain technology is applied in business layer and data layer, categorized as the lower part. The business layer specifically processes business logic, and data layer handles relatively complicated logic and stores all processed data under the chain.

Davinci Chain is a public blockchain that uses distributed ledger and storage in the absence of centralized hardware or regulatory authority. The right and obligation of each node are evenly sustained, and the data block in the system maintains its structure by managing and preserving functional nodes.

Utilization of 'timestamp' in the cognitive block structure introduces time dimension in the data during the storing process. This innovation provides strong traceability and verifiability. Moreover, a specific mechanism is adopted to ensure participation of all nodes in the distributed system to the verification process of the data

block. The new block also can be added to the blockchain through the preselected node of consensus algorithm.

The Davinci project is constructed based on the consensus derived from specification and protocol. In the environment, created by the project, all nodes in system maintain their reliability, and the data is freely and securely exchanged. The Davinci project can preserve its condition due to blockchain's resistance to any artificial modification of the data. This condition reveals the transition from the belief in "human" to belief in "technology."

Once the information is verified and added to the blockchain, it is permanently stored and not executable to alter the data in the single node level. Since it is public blockchain, except the encrypted information of the parties in transaction, the data is completely open to any individuals and groups, hence the overall system information is highly transparent. As mutual trust between each node is not a vital element of the transaction, exposition of node's identity is unnecessary. Therefore, each participating node in the system is possible to be remained anonymous.

3.1 The Combination of Davinci Project with Industry

The Davinci project combines blockchain technology on numerous fields including culture, asset, bonds, insurance, finance, and IoT. The project suggests optimal solution to complicated problems of specific industries and provides appropriate smart contract for each. Various information, data, and its mechanism created during its operation also are stored in the Davinci blockchain. This currency system that is combined with information, data, and authentication relations, promotes the development and convergence of this ecosystem while focusing on the payment. And the advancement of the ecosystem contributes to convenience in daily life.

<Cultural Aspect>

Due to the widespread of Korean culture in the global society, impact of Korean Wave in China influences not only cultural sectors but also diverse fields of industries. Yet, the numerous trade barriers in cultural and artistic areas have existed because of conflict of interest and technical inefficiency between nations. These problems, however, can be easily resolved by application of blockchain technology. It is possible since the technology allows the creation of decentralized blockchain ledger for each contents. And it creates a grounds for recording and updating all information and data of the contents. For instance, specific information of the content such as copyright, publication right, shares, transaction authentication, and document forgery prevention is categorized and stored in the blockchain ledger through decentralized blockchain technology. These information is accessible to only authenticated users with legitimate reason. Such transparent trading of cultural contents will prevent counterfeiting and contribute to the development of a clean culture and art market as well. In addition, this transparency enables to encourage cultural exchange between Korea and China beside other countries.

<Value Storage Aspect>

Reestablishment of real estate transaction into a 'digital credit society' can be achieved by connecting real estate to the blockchain and owners of assets with financial institutions. Theory of real estate transaction and ownership is dealt and managed by blockchain ledger and smart contract technology. Blockchain's trust mechanism prevents unauthorized alteration and sustains transaction transparency. Additionally, joint monitoring and tracking features provided by blockchain's systematic character serves as major advantage. In the real estate transaction, the cryptocurrency approved by Davinci project also is utilized. The transaction details are stored in each block and generated without real estate agent. The blockchain technology can reduce the unnecessary expense and improve the efficiency of the transaction.

<Internet of Things(IoT) Aspect>

Internet of Things, abbreviated as loT, refers to controlling things by maneuvering internet with frontend internet technology. The blockchain technology ensures secure one to one data communication of all devices connected to the network over the internet. The most important issue on loT are protection of data encryption, validation mechanisms, and the settlement and payment of reliable costs in a distributed environment. With application of blockchain technology, individual internet facility can transmit data via directly encrypted protocol and settle the transaction of each transmission. This can serve as the basis of practice the cryptocurrencies in the IoT blockchain and can be utilized as the currency among companies in the market to stimulate healthy competition.

To connect internet of things(IoT) to Davinci project, firstly blockchain consensus verification mechanism shall be remodeled. In the IoT applied environment, each sensor and microcontroller nodes become inactive because IoT's smart facilities are not participating PoW calculation and only concentrating on the data encryption and transmission. Instead, verification nodes are established with mainstream pc servers used by a company providing variety of IoT services, and these nodes function to achieve the objective of transaction.

Compared to the classic center-server architecture of internet of things(IoT), the input amount of small scale verification nodes required for the computation is significantly lower than the existing service cluster. Additionally, it is almost impossible to artificially change or data leakage, since verification nodes are not automatically storing the user's data.

<Financial Service Aspect>

In future, blockchain technology is expected to be the core infrastructure for the financial service. Existing financial institutions such as banks, insurance, trust companies, and etc. attempt to reform the ground by introducing blockchain to the financial models. Furthermore, the integration of advanced technology and finance created new financial system named Fintech. Information asymmetry among participants negatively influences the establishment of economic credit system.

This causes decrease in the transaction efficiency between centralized credit mediator and information intermediary and increase in the costs. Davinci Project has solved the problem of redundant information, and connected various field data and transaction channel.
Moreover, the project presented possibility of trust mechanism in decentralized system through blockchain's opened information and anti-counterfeit characteristic and potentiality to reform the base of finance architecture. Exchange and disbursement are the most fundamental concept of the finance. Prominent advantage of adopting blockchain in transaction is especially represented in cross-border payment. Along with participants' capability to perform transaction regardless of their regions, simplified processing procedures, efficient transaction via real-time settlement, and reduction in the cost make the blockchain system ideal for business models dealing with international transaction and small payment.

3.2 Davinci Project and Cross-border Payment

The payment system is currently divided into three main methods, which are bank settlement system, third-party settlement system, and cash payment. All of these methods have several drawbacks including high commission fee, inconvenient procedures, long settlement period, and unnecessary costs. Blockchain does not rely on intermediaries such as banks for trust patterns in financial systems due to its safety, transparency and unalterable feature. In cross-border payment, blockchain is able to exclude the role of intermediary banks. Based on the blockchain technology, payments would be made through person to person(P2P) rather than via bank. This will not only eliminate third party financial institution but also actualize real-time deposit, cash withdrawal, and all types of payment. Furthermore, transaction costs will significantly be reduced in B2B cross-border payment. The application model of the blockchain on cross-border payment utilizes its networks to build payment gateway among existing financial institutions. Through payment gateway, the real life currency can be converted into the digital currency for blockchain system which makes payment and transferring more convenient. The replacement of the actual transaction with the blockchain will accomplish fast and low-cost transactions.

Utilizing blockchain in payment has various advantages:

First Advantages: High payment efficiency

All transactions made by traditional online-payment are performed through complex multi-procedures since the intermediary of payment, usually a bank involved in the transaction, has to play a central role. In other words, banks that participated in the transaction are required to check the balance of and synchronize the commercial information of transactions. Moreover, final payment is made only to an account existed in participating banks. As a result, conventional centralized exchange and payment methods have to go through complicated process. Online payment via blockchain, the nodes, participating in the blockchain network, share the same verification information and ensure the consistency of the information. Consequently, the efficiency is greatly increased because it is not required to synchronize and settle complex information.

Second Advantage: Save banking resource

Among various blockchain cross border payments, bank-to-bank transaction is performed by utilizing agreed upon chain system. This transaction allows real time cross currency exchange without a role of intermediary bank. Therefore, the cross border payment based on blockchain technology saves possible loss of bank's resources.

Third Advantage: Low risk

In cross-border payment based on blockchain technology, participating nodes in all payment including importer and exporter, etc., are connected each other through blockchain technology. These nodes cooperate to share, verify and protect the payment transaction information. Therefore, if an importer set up the payment schedule and fail to receive delivery information from an exporter, the importer will not approve the payment confirmation during transaction validation process. Due to the importer's refusal, the transaction will not take place and the exporter cannot receive the money. Consequently, international trade risk can be significantly reduced by introduction of blockchain payment since all the participating nodes jointly manage transaction records and actively participate verification process.

Forth Advantage: Rapid speed of transaction

In conventional cross-border payment models, especially in the process of manipulating large amounts of artificial settlement, banks have typically handled the large amount of settlements process at the end of the day. While transaction through bank usually takes 24 hours to be completed, blockchain cross-border payment greatly shortens the payment period by reducing unnecessary procedures and providing 24/7 services for the international participants.

Fifth Advantage: Significant decline of transaction commission

According to Global Payment 2016: Strong Fundamentals Despite Uncertain Times by McKinsey Company, an average commission of cross-border payment through correspondent bank model was indicated between twenty-five dollars and thirty-five dollars, which is ten times more than commission of domestic payment. Conventional cross-border model contains various fees such as payment processing, requisition, financial operation, accounting and others. The utilization of blockchain technology can reduce the role of intermediaries in commercial transactions and increase the liquidity of funds, which enables to check and control the process in real-time. As the result, it is possible to effectively reduce direct and indirect commissions of each transaction.

Sixth Advantage: Ideas for a new transaction

Payment and settlement through blockchain provides a new idea regarding customer information and verification. According to anti-money laundering law(AML), financial institutions around the world must strictly enforce customer identification procedures during transaction and implement account name verification (Know-Your-Customer Rule, KYC). Existing financial institutions procedure and required documents of customer information verification have been complex. Therefore, a long process in confirmation of information is inevitable and, consequently, financial institutions face cost issue. By establishing trust with blockchain technology and storing electronic files of customer identification, blockchain technology actualizes safe management of identity information, fulfills core requirements of anti-money laundering law, and suggests a new solution to management regards to KYC process and anti-money laundering law.

3.3 Davinci Chain & AI

The mainnet means building a new platform out of the existing block-chain platform. The main net can attract companies that use various tokens. The mainnet will issue a coin directly to act as a kind of base currency. Davinci is a third-generation coin that builds a new mainnet. How do you count the generation? The first generation of blockchain is a Bitcoin. The second generation is Ethereum. Ethereum has implemented smart contracts and is capable of distributed applications(Dapp).

Davinci is a third generation blockchain. What does the third generation mean? At present, various cryptocurrencies are based on the second generation platform, Ethereum. These Ethereum-based cryptocurrencies are called 'ERC20 tokens'. The problem with the second-generation blockchains is that second-generation technology makes it difficult for people to create real-life technologies and services. The oxymoron of capacity and speed can be handled by blockchain technology, but the method of mining (consensus algorithm) is unclear. The solution to this problem is the third generation blockchain.

Davinci, as a third generation of blockchain, is capable of using a variety of DApp. In addition, it can speed up transaction processing in lower costs. As a result, the most practical blockchain is the third generation. The third generation of blockchain should increase transaction processing speed. Ethereum has a slow processing speed and limited transaction (transaction record between users) capacity. For this reason, Ethereum is rarely applied to business.

Let's look at the concept of velocity in blockchain. Ethereum's trading per second (TPS) is 20 TPS. It processes 20 transactions per second. It is better than Bitcoin’s processing speed(4TPS) but it is still not practical for business use.

The block generation time has a great effect on the blockchain speed. In a situation where there are not many transactions, TPS is meaningless. If the block creation time is short, the speed of the blockchain is fast. If the block creation time is long, the speed of the blockchain is slow. As a result of the agreement method in the blockchain, the transaction processing method and the overall performance of the system are different. "Do not agree if you have a completely reliable network. " The above sentence simply means that you do not need a blockchain that increases speed.

Blockchains were created because of the need for strong trust. If you have strong trust in your system, you do not need a blockchain. If you need trust in the system, the throughput will be sacrificed. This is the problem of current blockchain theory. Until now, blockchain's main focus were speed and security. However, enhancement of security was achieved at the expense of speed and vice versa. Resolution of this contradiction is DAI, Davinci project's AI technology. What role should artificial intelligence play in the block chain? Let's take the speed as an example. POS is faster than POW. Davinci adopted the POS system. The Davinci chain can support fast block creation up to 1000 TPS. The Davinci chain must limit the number of nodes to achieve maximum speed. The chain has greatly improved processing speed by introducing parallel processing using multi-thread.

Due to the limited number of nodes in the Davinci chain, attack targets become clearer. After securing 51 percent, the Davinci chain can be neutralized. The Davinci chain divides the blocks according to their importance. AI evaluates the importance of Davinci chain blocks. In the Davinci chain, machine learning can be used in networks.

Blockchain technology is an ideal tool for managing network transactions. However, the blockchain based framework must be designed so that AI agents can interact with external customers. Artificial intelligence should be used to automatically classify the importance of incoming customers. The Davinci chain must manage the creation cycle of the blocks through an external business.

DAI(DaVinciArtificial Intelligence)

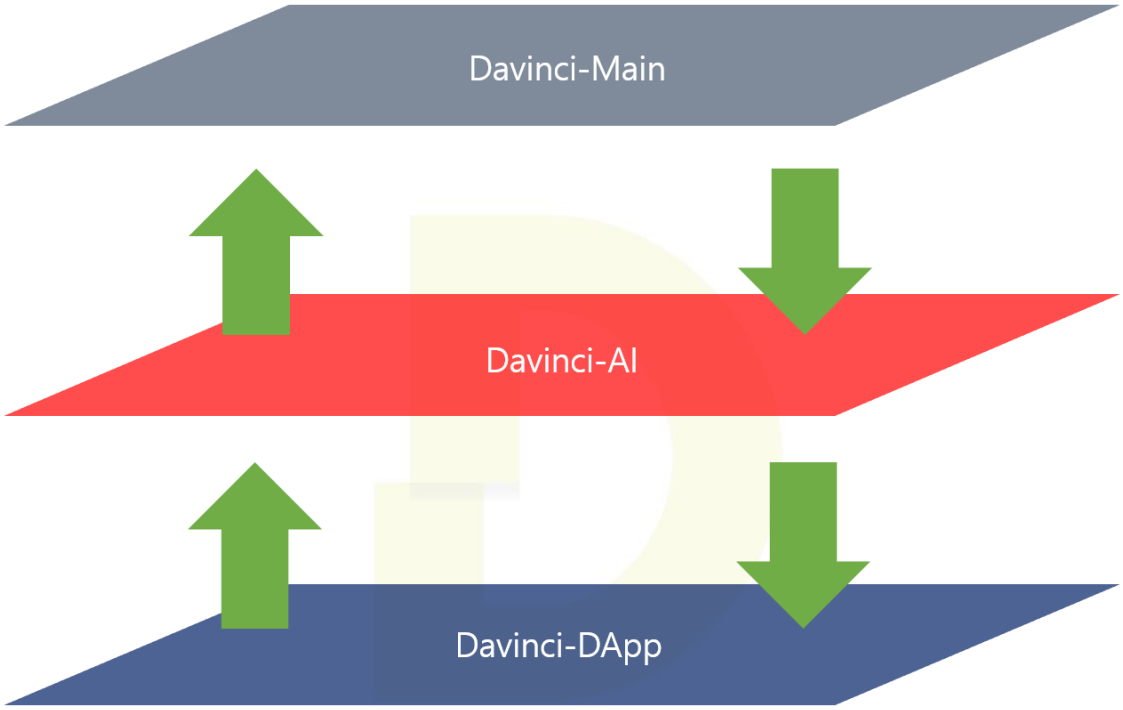
The Davinci chain must be vested to make mining possible. The mainnet defines mining which was justified based on the following data. (the hash of the previous block, the time it took for the previous block to be mined, the time it took for the current block to be mined, the address of the miner, the amount of DAC left by the miner in the vest contract)

DAI is the abbreviation of AI engine. DAI enables machine learning and manages the whole process of block verification of Davinci mainnet. Artificial intelligence learns the generation cycle of blocks. Artificial intelligence is to find out that dangerous events occur on the main net.

For example, if a person who withdraws $ 1 suddenly withdraws $ 10,000. If the artificial intelligence perceives these changes, it can stop the mainnet since DAI oversees the main net. Problems can arise with this system. It is the excessive intervention of artificial intelligence within the mainnet. Automation problems may arise too. However, this is a problem to be solved in the future.

Dapp is associated with blockchain technology. The existing centralized system and decentralization based philosophy are strictly different. It's impossible to build an app with only blockchain yet. Currently only a hybrid of app and blockchain is possible.

There is a server that hosts the DApp code and acts as a mediator between the user and the database. Data can be protected through a blockchain, but if the central server is disabled, the system will be broken down. The Davinci AI engine is responsible for the stability of the central server and the ability to control the connection to the block chain.



Artificial Intelligence Checkpoint of Davinci Chain

Scalability

The result of the aggregation of the seven extensibility factors is the actual transaction rate / throughput (TPS / throughput). In addition, the seven scalability factors go beyond simple throughput, and show how flexible they can be applied in real life.

Main checkpoint of scalability

1. DPS (Data processing speed)

The Davinci chain has a fast DPS(data processing speed). This is due to the appropriate block size. Assignment of block size is determined by artificial intelligence(DAI).

2. DVS(Data validation speed)

DVS(Data validation speed) in the Davinci chain Validation within POS systems is important. As the validation speed increased, it becomes less secured. It is a matter of the POS system as well as Davinci chain. To solve this problem, we construct an artificial neural network DAI.

3.DNS(Data network relay speed)

The problem of DNS (data network relay speed) is the problem of connecting to an external network. The network problem with the outside is important to understand. Moreover harmonization of inside and outside the chain is also necessary.

4. Increasing Data Size (storage)

Removal of obsolete data. To be able to use this function, artificial intelligence learning is required.

5. Number of nodes participating in consensus structure (The number of validators)

Adjustment of the number of nodes participating in the consensus structure (the number of validators) is related to stability.

6. Scalability on codes and applications

7. On-chain/off-chain governance

Davinci mainnet will combine the three methods to enhance the speed

1. Raiden Network

Raiden Network minimizes block-chain records and saves commissions through off-chain method, which does not record intermediate transactions between opening and closing payment channels. Since the Raiden Network does not wait for a block transaction, the approval is fast. We plan to apply it to highly reliable networks, which refer to network of nodes that verify data.

2. Plasma

Plasma is a technology that minimizes the recording of a block chain through a subchain in case of Leiden utilizes off-chain through the channel opening and closing process. Currently, DApp records all data in the Ethernet block chain (Main-chain). This causes speed problems and creates unpreferable conditions such as block size problems and increase of gas consumption due to data volume.

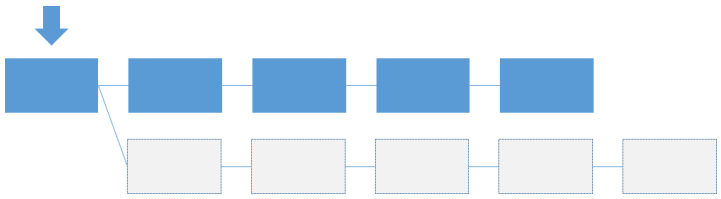
3. Sharding

'Shard + ing' means to shred data. In the conventional method, if all of the processing data have 1 to 10000 pieces of data, sharing stores 1 to 10000 pieces. The result is that the nodes are lighter and the transaction processing speed is improved significantly. In addition, plasma technology that utilizes subchain to minimize the recordings stored in the main chain is expected to be 100 times faster, which resulted in raising Ethereum's operating speed by 10,000 times faster than current. The problem is the forgery and falsification of data. Vitalik Buterin referred Sharding to an island. A new algorithm is required for each of these islands to be compatible.

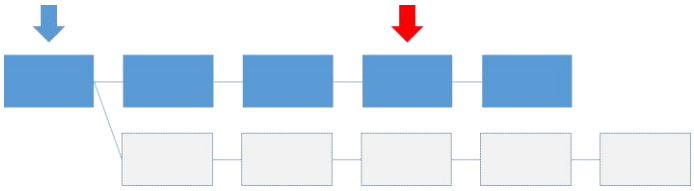
DAI makes a secure blockchain

Block chain is not a perfect system. It can be vulnerable to attack at any time. On May 15 in 2018, Monaco used Block Withholding Attack (BWA). The definition of BWA is that blocks are generated by mining to find the computed value. Normally, miners declare on the network as soon as they find a block. The first person who finds it is given a coin as a payoff.

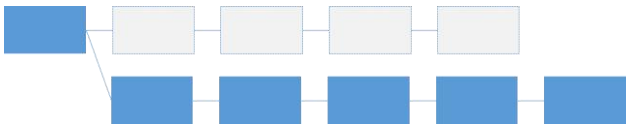
However, if the hash power (computation speed) is high, the block that has already been found may not be declared intentionally. It is then possible to mine the next block without informing the network



BWA is illustrated as an example. As the blockchain(blue) is created, the attacker secretly mines his own blockchain(gray). Because the attacker's hash power (computation power) is higher, the secretly mined block chain is also longer. At this time, the attacker deposits the coin to the targeted exchange. For example, if the exchange handles the deposit with the approval of 3 times, the deposit is completed from the red arrow in the figure below.



At this time, the attacker swaps the coin of this system to another coin and quickly withdraws it. After that, declare blocks from the behind that have been secretly mined.



When a new block appears, the chain is split into two bifurcations. In a blockchain of PoW (Proof of Work) method, since the chain is longer, the attacker's blockchain is justified and considered a legitimate chain. Existing chains are culled and disappear. This phenomenon is called block reorganization.

Transaction history existed (existing chain coin -> other coin) in coin exchange. If the existing chain disappears, the transaction history disappears as well. For this reason, the coin that was used to purchase another coin is returned. An attacker will vanish as soon as he or she moved the returned coin to the personal wallet. Coins of existing block chain and new block chain overlaps. At this time, the existing coin that had purchased another coin disappears and only the coin in the attacker's personal wallet is left. To become an attacker, the abundance of coin's liquidity is necessary. Next, high hash power is required for BWA. For this reason, PoS method is preferred in PoW method. But PoS is not fully secure.

In the case of PoS (proof of stake), 'Nothing at Stake' problem can occur. In PoS, there is a validator instead of a miner. The verifier has the authority to verify the blocks according to the assets. The validator adds a proof of own asset to the block, which is considered as a valid block, and places a bet. In the network, the block with the greatest sum of the betted assets is recognized as a legitimate block. Suppose an attacker made a fake block to attack a blockchain. The verifier must sign only the real block. However, since a fake block is able to camouflage as a legitimate block, both fake and legitimate blocks can be approved. Eventually, the whole network can be fall into chaos.

In the PBFT (Practical Byzantine Fault Tolerance) algorithm, there is no recurrence of the blockchain. However, if you have more than one-third share, you can attack against the blockchain. This is lower than 51% of PoW. Therefore, PoS is more vulnerable in terms of defending against malicious attack than PoW. In order to defend against malicious attacks, the number of nodes must be increased.

In PBFT, as the number of nodes are increased, the amount of traffic increases sharply. Therefore, additional time is required for block generation. In general, the block generation time (waiting time to complete the transaction) is shorter and faster. People preferred 5 minutes rather than 10 minutes, 1 minute than 5 minutes, 10 seconds than 1 minute.

However, since short block generation time and security are currently incompatible, the number of approvals must be increased accordingly. In order to improve the speed of transactions, new method should be developed.

The bottom line is that mainnet can be used well without increasing the block length as the transaction speed improves. Based on AI, Davinci chain offers to satisfy these conditions. Davinci's mainnet enhances the stability of block generation using artificial intelligence. Using the machine learning process of the smart contract and the block creation process, the stability of the mainnet improved.

The ether block explorer, Etherscan, can verify smart contracts. But even proven contracts tend to have bugs and vulnerabilities. Meaning of 'verified' means that only the source code provided matches what is distributed in the blockchain. It is difficult to guarantee mainnet’s security in this way. Thus, the security standards need to be established for Ethereum Smart contracts and conduct smart contract validation.

DAI is an automatic verification system of smart contract. Artificial intelligence automatically validates creators of smart contract and sends them to verifier nodes in real time. The learned artificial intelligence senses and analyzes the dangerous alteration of blocks. First, artificial neural networks learn the changes of smart contracts and blocks and then collect data. As a result, it learns the pattern of smart contract and block mechanically. Finally, the stability of the chain is maintained by using deep learning.

The deep learning is also called as 'Deep Neural Network' (DNN) that imitates a human neural networks. And DNN solves complex problems through iterative process of updating parameters which affects relations between layers. Davinci’s artificial intelligence system uses deep learning to create a pattern of repetitive process of blocks.

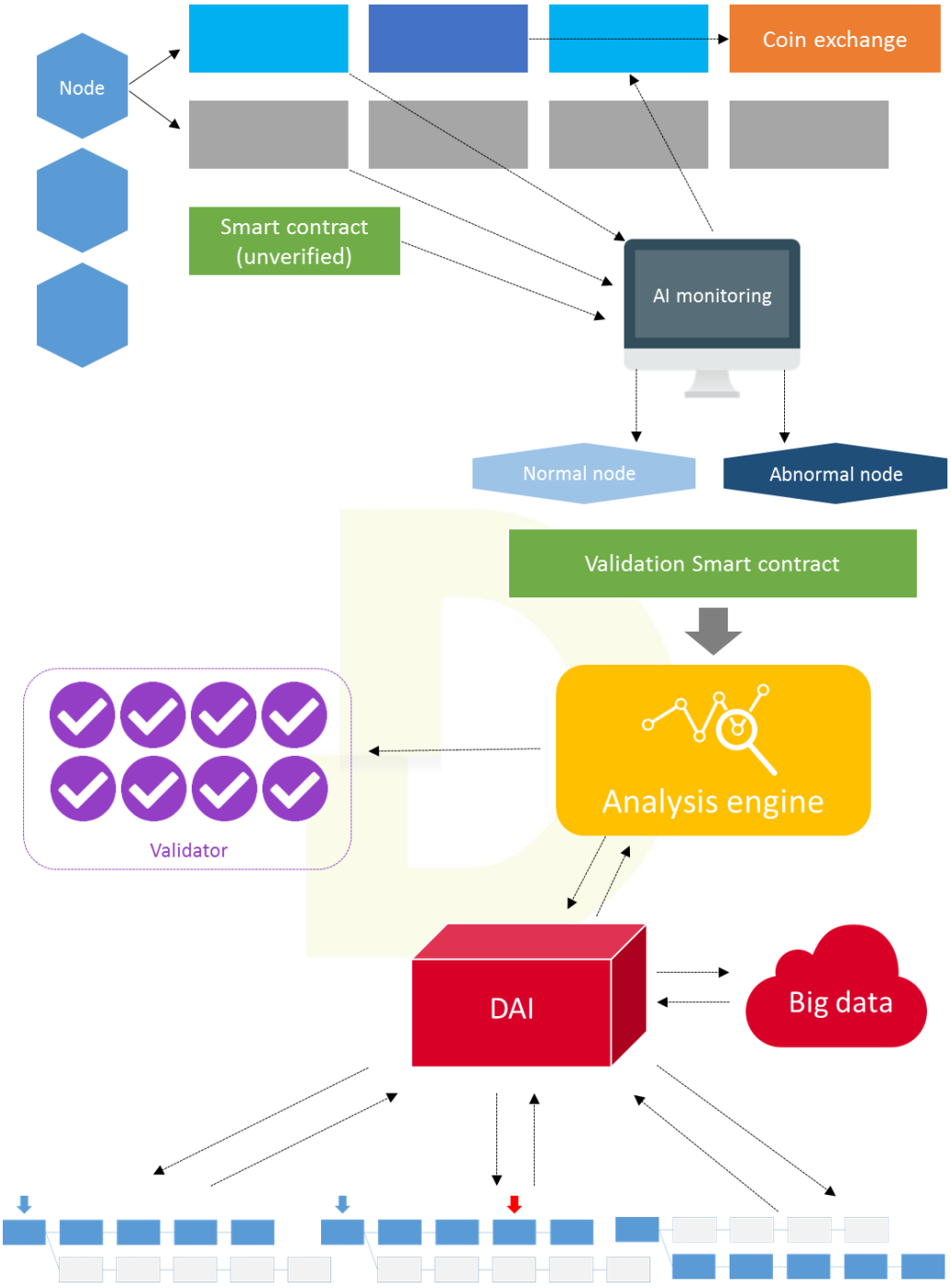
Davinci's Artificial Intelligence (DAI) automatically learns repetitive processes in block chains and Dapp. Therefore, AI itself is able to prepare for problems that may arise. Davinci AI engine aims to unsupervised learning. Unsupervised learning is a process in which the algorithm itself learns data’s the relationship and specificity without providing a solution to specific data.

Let's take an example of supervised Learning, which is the opposite of unsupervised learning! The photo materials given to us are "Joe, this is David, this is puppy ... "If you have a label for each picture, you can learn about it and find other photographs of Joe, David, and puppies.

On the other hand, unsupervised learning is something like automatic group categorization among mixture of several animal pictures. Even if you have not learned to categorize a 'dog', unsupervised learning is able to classify all of the similar species as puppies.

Davinci platform's Artificial Intelligence Engine (DAI) aims to use unsupervised learning. DAI’s unsupervised learning allows automatic detection of abnormal changes in block generation and to take action. In addition, it will be able to solve the problems automatically by learning and forecasting the problems that occur in the distributed environment.

Davinci AI recognizes dangerous patterns in the blockchain. This is similar to the way a self-driving car detects an obstacle and stops a car. For example, the artificial intelligence can automatically select and process the algorithm depending on the importance of the payment by itself. DAI is possible to recognize and control the process of $1 and $100,000 differently.


Node
Coin exchange
Smart contract
(unverified)
AI monitoring
Normal node
Abnormal node
Validation Smart contract
Validator
Analysis engine
DAI
Big data

4 Davinci Token (DAC)

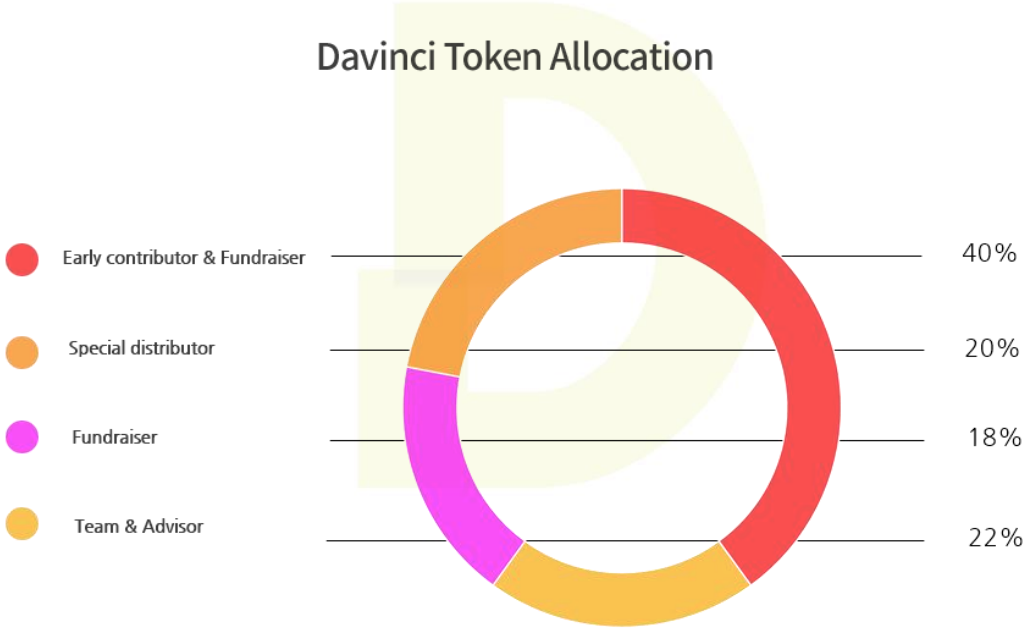
4.1 Token Sale

Term Summary

- Total Token : 8,800 , 000 , 000 DAC

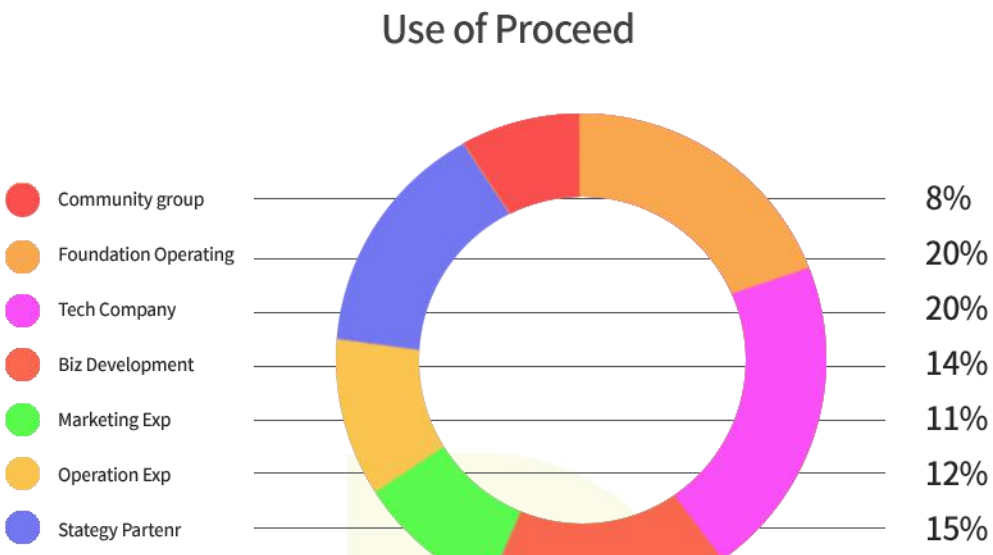
- Sale Token : 2, 640 , 000 , 000 DAC

4.2 Token Allocation



- 40% will be sold in accordance with the sales plan
- 18% will be managed by foundation
- 22% will be allocated to development team and advisors
- 20% of it will be allocated to special distributor
- 10% (880,000,000 DAC) are locked. From two months later, it will be unlocked 20 percent of each month over five months

4.3 Use of Assets



- IT Company 20%
- Foundation Operation 20%
- Business Development 14%
- Marketing Expense 11%
- Operation Expense 12%
- Strategic Partners 15%
- Community group 8%

It will be allocated to the foundation operations, business development, marketing, community group and strategic partners.

5 Davinci Member

5.1 Development Team

Minjae Kim
POSTECH Univ.
SAMSUNG Electronics
Software engineer

Sangwoong Cho
Sogang Univ.
LG CNS
Smart green Platform and IBK Banking system Dev.

Zachary Moon
Sogang Univ.
Novacos
Software Engineer

Jaemin Shin
Sungkyunkwan Univ.
SKK Software Developing Department: Doctor's

Singi Jeong
Sungkyunkwan Univ.
SKK Software Developing Dpartment : Master's

Sangyeol Nam
Tenspace project manager
Familiar recruitment platform, AI self-audition platform, etc.
Research Fellow, Weihai City, China

Taeho Kim
Tenspace IT Engineer Multiple Network Security Business PM and PL Linux based mail engine development

Sangyun Han
Tenspace Big Data Analysis Team Leader
IT Engineer Yonsei University Graduate s chool of Engineering

Jerry Gao
Graduated from Jinan University Master.
Software Engineering
THU Domestic famous block-chain developer

Wang han
PHD.
Computer Science MIT
Person in charge of the project named Big Data

Wo jiang
Master.
Computer Science THU
Main research directions are block chain and high

Kelvin
Senior blockchain Developing enginner
Who had worked in Many blockchain projects

5.2 Davinci Advisory Board

류 이

- 다빈치재단 이사장
- 재단 공동설립자
- 중국 윈단 사물인터넷 회장

한 승 재

- 다빈치 재단 공동 설립자 / 한국대표
- 다빈치 재단 부회장
- 연세대학교 졸업
- 전) 코스닥사장사 디지털옵틱 대표이사

이 금 룡

- 인터넷 쇼핑몰 "옥션" 설립자
- 도전과 나눔 이사장
- 코글로닷컴 회장

정 해 만

- 치프 어드바이저
- 자유한국당 부대변인 / 정당인
- 여의도연구소 부회장

김 시 현

- CMO / 경희대 졸업
- 153 프로덕션 대표이사
- TV 드라마"태양의후예"등 공급사

고 진 석

- CIO / 서울대학교 컴퓨터공학과
- 전) 아이러브스쿨 기술이사
- "텐스페이스" 대표이사
- 한국 AI 기반기술의 최고기술자

이 병 건

- 스페셜 어드바이저
- 전) 종근당 홀딩스 대표이사

김 호 경

- CLO / 법률전문가
- 전) 대한민국 특수부 부장검사
- 법무법인 "율촌" 대표변호사

함 철 만

- 건국대학교 의학박사
- 연세대학교 공학박사
- 전) 지식경제부 상근전문위원
- 전) 기획재정부 한국수출은행 기술전문위원

하 준

- 현대그룹 커뮤니케이션실 실장
- 현대그룹 전무이사

김 석 현

- 골든키 자산운용사 회장
- 파이낸셜 어드바이저

김 정 현

- 스페셜 어드바이저
- 솔리더스 인베스트먼트 회장

6 Roadmap


01
2017 Q4
문화교류를 위한 한.중기업인 모임
02
2018 Q1
싱가폴 기금회 설립
다빈치 프로젝트 ERC20 토큰 생성
03
2018 Q2
수석 고문 및 핵심 고문 영입
사모 펀드 추진
04
2018 Q3
AI 기반 블록체인
다빈치체인 테스트넷
05
2018 Q4
다빈치 플랫폼 1.0 발표
메인 체인 개발 완료
06
2019 Q1
생태시스템 완성

7 Davinci Organization Structure

7.1 Overview of Davinci foundation

Davinci Foundation (referred as "Foundation") is established in Singapore and focuses on the construction and dissemination of the overall Davinci's economic ecosystem. The foundation complies with laws and regulations of Singapore.

Foundation operates under the authority of community members. Cooperating with associated partners, which include service provider, market operator, business and client user, to promote the Dapp ecosystem. The Foundation is a nonprofit organization that oversees general operation of the entire system. The community is the highest authority and is managed by a voting system.

7.2 Purpose of Davinci foundation

The basic principles of the Davinci Foundation are open sharing and sustainable development.

1) Exercise the authority, granted by the community, with transparency, openness and impartiality.

2) As a non-profit organization, cooperate with participants of the system to stimulate market activities through commercial offerings and economic ecosystem construction.

3) Aim for balanced development of Davinci's commercialized ecosystem with rigorous management of the foundation and monitoring of the community.

8 Disclaimer

This document is for purpose of conveying information only and does not constitute any investment encouragement or proposal regarding DAC. It does not serve as any kind of contract or commitment.
To participate Davinci project, all investors must clearly understand the risks. Therefore, every investor who is involved in the investment is considered to contain full understanding of possible risks and ready to take full responsibilities of all consequences. Thus, Davinci Foundation clearly states that the foundation is not responsible for any direct or indirect damages that incurred.

The disclaimer of the project contains the followings (Other risks that were not mentioned may exist as well):

1. The foundation cannot guarantee the increase and fluctuation of the token value. The value may drop depending on the situation.

2. Definition of token is neither ownership nor control. The project cannot guarantee authorization to alter the project to any individual or organization with an associated business and utilization plan.

3. Token contains various types of risks such as lost or stolen.

4. Risk of judicial regulations may exist. Cryptocurrency is already subject to supervision by all countries around the world, thus the project itself and the token may be affected if the authoritative group is introduced to the ecosystem or regulate it.

If you are not familiar with the vision of this project and the risks associated with cryptocurrency, we do not recommend to participate in token pre-sales. Cryptocurrency is riskier and should be considerate about its investment. Participant cloud funding of digital assets will not be refunded if they participate in token pre-sales. This project has the potential for development and also development failure depending on legality, market technicality, or uncontrollable causes.

Furthermore, Davinci team will continue to conduct reasonable tests to ensure the reliability and accuracy of the information in the white paper. However, this white paper is written based on the status at the time of writing and does not warrant the accuracy and appropriateness of any content in the white paper, including the conclusions, performance of the project, roadmap and achievement. This white paper can be adjusted according to the team's policy or decision.

The team shall not make any representations or assurances about any matter in relation to this white paper and shall not be liable for any applicable liability. For example, whether this white paper (i) is written based on legitimate authority without infringing on the rights of a third party; ii) is commercially valuable or useful; iii) the content of the Davinci project described in the white paper are not in violation of the laws of investor’s country.

The object to which the Davinci project team is exempted from the responsibility is not limited to those illustrated above.

9 Davinci official community

 http://davinci.vision

 Instargram : https://www.instagram.com/davinci_foundation/

 Twitter : https://twitter.com/DavinciFoundat1

 Facebook : https://www.facebook.com/Davinci-coin-1688348254582102/

 Telegram : https://t.me/davincifoundation

http://davinci.vision