Insight Chain

Technical White Paper V1.0

A Big Data Ecosystem Public Blockchain with Infinite Scalability

Insight Chain Founding Team

February 1st, 2019

ABSTRACT

The TPS of public blockchains such as BTC and ETH is not high, which makes it difficult to support a large-scale application. Therefore, more and more public blockchains have tried to make technical explorations to improve TPS in 2017 and 2018. For example, EOS uses the DPoS consensus algorithm to increase TPS to a multi-thousand level at the expense of a certain degree of decentralization. Security, scalability and decentralization are known as the "impossible triangle" of the blockchain, which means that, in the same blockchain system, it is impossible to achieve all three properties and meet high requirements at the same time. And this is an essential issue to be solved. As a result, we define two core goals of Insight Chain: to achieve transaction data processing capability of 100,000+ TPS and business data processing capability of 1,000,000 + TPS by improving scalability and meeting requirements of more applications to store business data on blockchain under the premise of decentralization and security. Insight Chain will realize these two goals through following core technologies:

- VDPoS consensus algorithm, introducing validation nodes to increase decentralization and safety degree;
- Multi-Main chain + Multi-Child chain architecture, realizing almost infinite vertical scalability and horizontal scalability;
- INB Utilization Model (IUM), using self-adaptive sharding technology to increase processing capability of public blockchain;
- Structural storage on blockchain of business data, supporting data's preservation, encryption, decryption, transaction and etc.;
- Visible smart contract, introducing transaction engine to simplify the issuance and transaction of Token;
- Usage of the Floyd algorithm, improving Kademlia network;
- Random validation mechanism based on VRF;
- Supporting to cross blockchain through state channel smart contract, commission and public notary mechanism.

Catalogue

1. Background

1.1 From Cryptocurrency to Public Blockchain Data Ecosystem

Since the birth of Bitcoin [2] in the year of 2008, currency items have been the main body of the blockchain domain. Currency items are represented by Bitcoin, Litecoin, etc., and are based on single-dimensional value transfer. The birth of Ethereum [3] means that the blockchain domain has broken through the concept of pure digital currency and opened up a trend to develop into a more complex universal development platform. With the development of blockchain technology, the large demand of blockchain in the industry will be gradually realized, and the combination of blockchain and specific commercial application scenarios is also rapidly advancing, which is laid the foundation by the development of a universal development platform.

Considering the complexity of practical commercial scenarios, we believe, the use of "blockchain + a specific industry" will definitely lead to a corresponding public blockchain data ecosystem supported by that multi-dimensional value transfer providing digital currency market with a higher level and more diversified real value. As a result, blockchain industry could step into phase 2.0 of public blockchain data ecosystem from cryptocurrency.

1.2 Implementation and Operation of Public Blockchain Data Ecosystem

In the digital currency stage, storing transaction on blockchain has been able to meet most of the needs of fund flow, while within the public blockchain data ecosystem, the data produced by the interaction of various characters are necessary materials for maintaining the system operation and rationally operating economic distribution mechanism. In some scenarios, data information itself is also a carrier of value, and

therefore, it is an inevitable trend for the development of public blockchain data ecosystem from simple storage on blockchain of transaction to that of data. In addition to the demand for data credibility and data value protection, large amount of data produced in the ecosystem calls for higher requirements of processing ability of blockchain. Most public blockchains existing now have fallen behind actual demands in aspects of block packaging, confirmation speed, etc.

2. Insight Chain Technical Architecture

Insight Chain is abbreviated as INB Blockchain. In order to cope with the growing demand for blockchains, we define the core goals of the INB Blockchain as two: under the premise of decentralization and security, to improve scalability and meet the needs of applications on business data's storage on chain to achieve the transaction data processing ability of more than 100,000 per second (100, 000 + TPS) and the business data processing ability of more than 1 million per second (1,000,000 + TPS), and to lay the foundation for blockchain implementation for numerous practical scenarios.

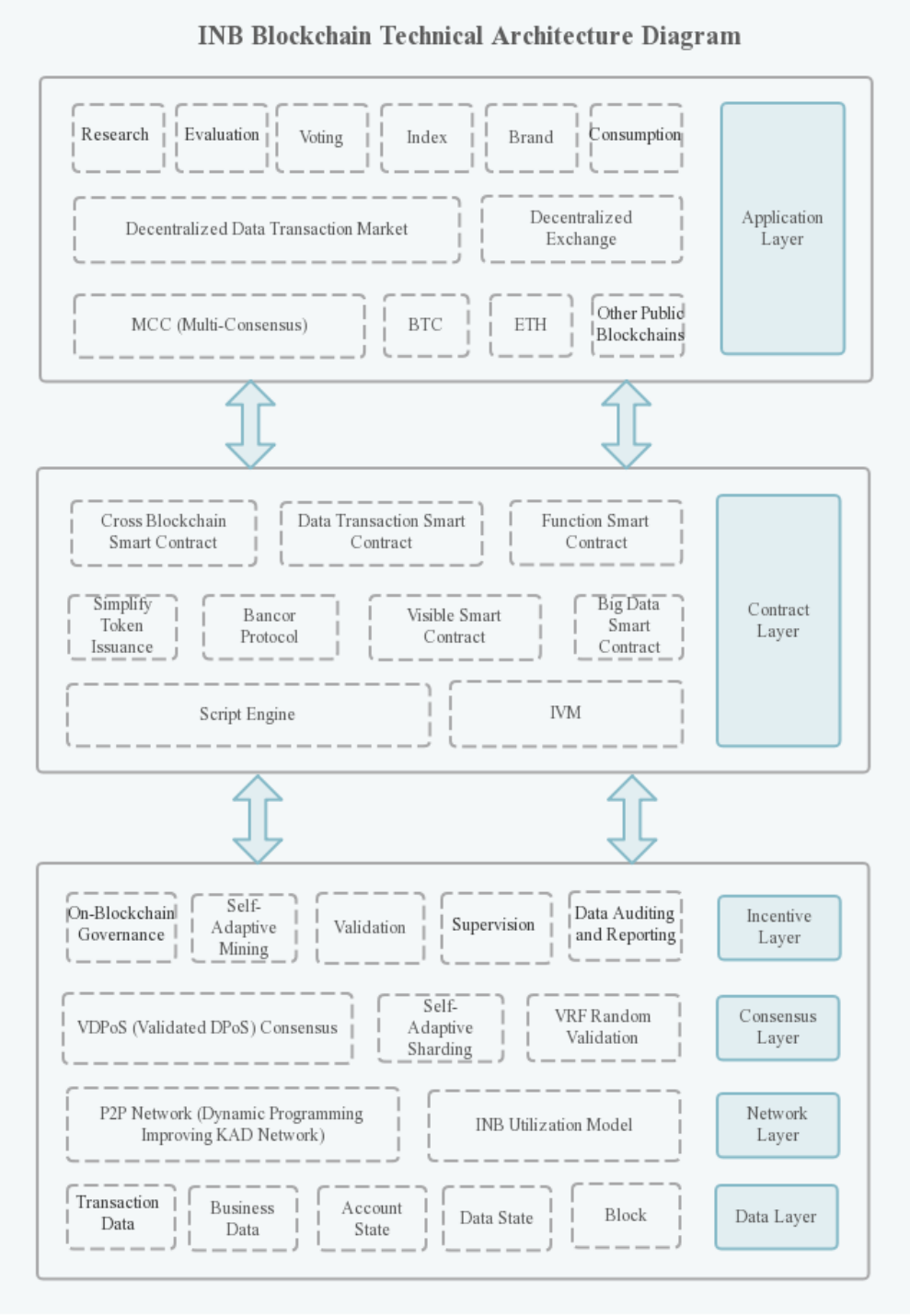
INB Blockchain proposes the consensus algorithm of VDPoS, which introduces validation nodes into traditional DPoS [4] consensus mechanism to solve problems of decentralization and securities, realizes vertical and horizontal scalability of public blockchain through Multi-Main chain + Multi-Child chain structure, conducts hierarchical storage of data to store global data state, and supports business data storage on blockchain and transaction. Its goal is to establish the very first global data ecosystem public blockchain with infinite scalability to truly support operation on the blockchain of high currency Internet applications.

The terms involved in the INB Blockchain are explained as the following table:

Terms	**Explanation**
Main Chain	Main Chain of public blockchain, saving high-value data including transaction, child chain validation data, etc.

Child Chain	Side blockchain of public blockchain, saving transaction data and business data with such rather low value
Super Node	Block producing node and validation node of main chain
Validation Node	Validation node of main chain
Supervision Node	Taking charge of supervision and feedback of public blockchain and data
Common Node	Synchronizing public blockchain data and providing public blockchain API to the public
Business Data	Data information except for transaction stored on child chain
Child Chain Service Provider	Service Providers providing child chain with nodes
Smart Contract Service Provider	Writing smart contracts for algorithms such as big data and collecting user fees for smart contracts
Credible Data Resource	Trusted data resources that users can save to the blockchain

The technical architecture of the INB Blockchain is as shown below:



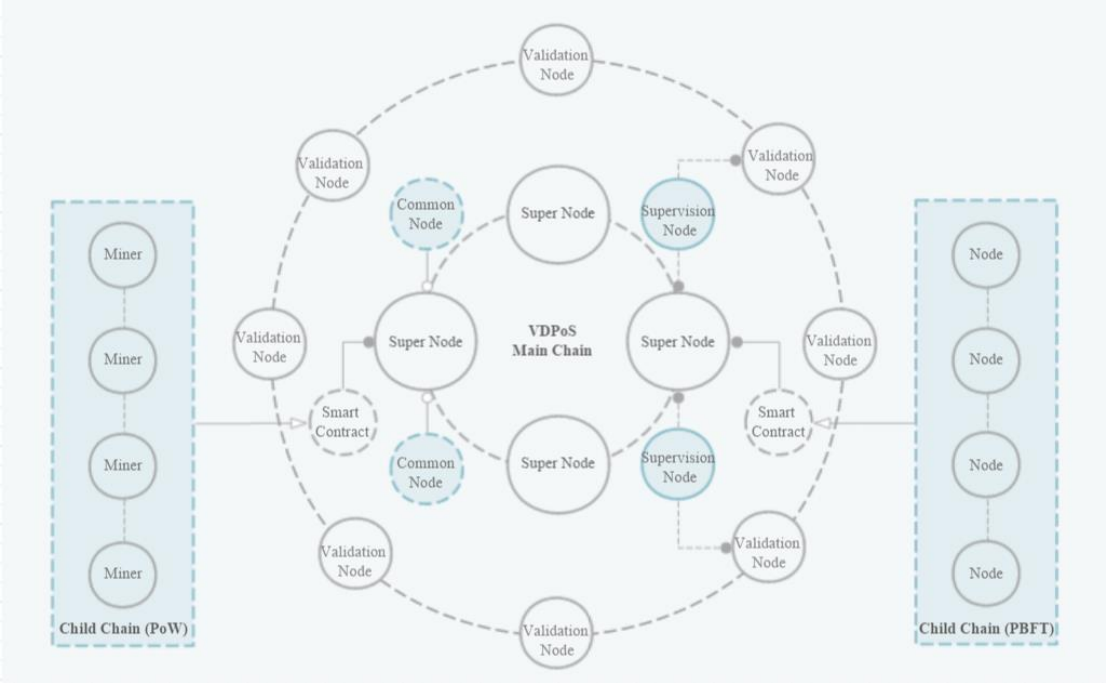
Technical Architecture of INB Blockchain

2.1 Consensus Algorithm: VDPoS

In order to solve the contradiction of blockchain impossible triangle, INB Blockchain proposes a brand-new consensus algorithm: VDPoS (Validated DPoS)

algorithm, which is an organic combination of “DPoS + BFT [7] + validation node". Each main chain in the public blockchain uses this consensus algorithm. The voting in the DPoS algorithm solves the problem that PoW algorithm resources are consumed by a large amount of uselessness, and the use of INB's mortgage and penalty mechanism has largely limited the evil of nodes. After the block is produced, the BFT algorithm is used to perform rapid validation within the super node at first. At the same time, the super node uses the VRF algorithm to find multiple random validation nodes, with which validation nodes perform asynchronous validation of the block data through BFT algorithm to prevent the joint evil of the super nodes and validation nodes, greatly improving the degree of decentralization and security of the public blockchain.

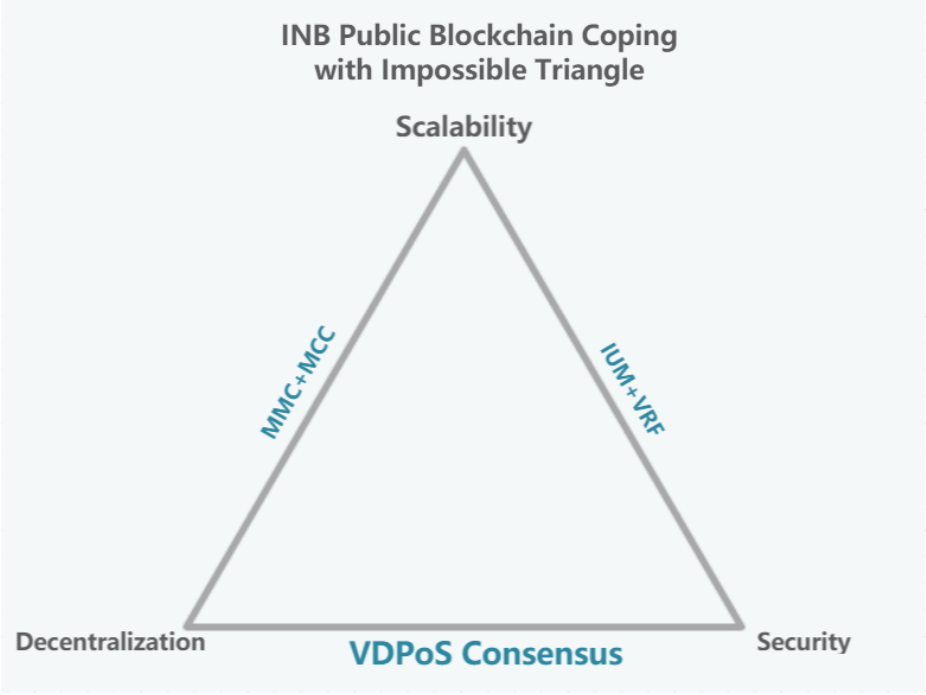
The child chain is a sub-blockchain network attached to the main chain. Each child chain has its own consensus algorithm. The child chain can use the consensus mechanism of the BFT type league blockchain, and it can also take advantage of public blockchain consensus mechanism such as PoW, PoS [3], DPoS, etc. According to different DApp requirements for the efficiency and security of the data’s storage on blockchain, different consensus algorithms are picked, and the public blockchain will not limit the consensus mechanism of the child chain. After a certain number of blocks being produced, the roots of Merkle tree corresponding to these blocks are stored on the block of the main chain to ensure the security of child chain. The blocks on the corresponding child chain are called validation blocks. The storage height intervals of validation blocks will be automatically adjusted according to the resource utilization of the main chain. When the resource utilization of the main chain is low, the hash value of each block may be stored to the main chain. However, when the resource utilization of the main chain is high, the storage height interval of the validation block is relatively large.



Nodes Ecosystem Map of Main Chain and Child Chain

2.2 Impossible Triangle Balance of Blockchain

The INB Blockchain is designed to fully consider coping with the problem of impossible triangle balance in the blockchain, as discussed in detail below.



Impossible Triangle Diagram

2.2.1 Scalability: Vertical Scaling and Horizontal Scaling

Many public blockchains and media confuse the scalability of blockchain with TPS. In fact, it is not rigorous. In the field of software engineering, scalability means that "in the process of system extension and growth, software can ensure strong vitality. With few changes or even the addition of hardware equipment, the linear growth of the entire system's processing ability can be achieved, and high handling capacity and low latency performance can be achieved." Generally, scalability can be divided into two types: horizontal scalability and vertical scalability. The former means that the processing ability of the system can be increased by adding new equipment, and the latter is to increase the processing ability of the entire system by increasing the processing ability of the existing equipment.

The INB Blockchain introduces INB utilization model to measure the use of the entire public blockchain. When the public blockchain is underutilized or the public blockchain resources are enhanced, for example, the processing ability of the super node is enhanced, and the network speed is increased. The public blockchain will automatically increase the number of sharding for each super node to increase the number of bars of the main chain, thus increasing the block production speed of the main chain and realizing the vertical scaling of the public blockchain. When the number of DApp on the public blockchain increases and thus the demand for storage on blockchain of data increases, DApp can apply to the super node to start a new child chain. After the voting of super node votes, the child chain will be initiated to store new DApp data, and therefore the horizontal scaling can be realized.

2.2.2 Decentralization: Introduction of Validation Node

Due to relatively small number of super nodes, DPoS consensus algorithm is often criticized for its insufficient decentralization and low security. In order to make up for these defects, INB Blockchain introduces the role of validation node and stimulates a

large number of validation nodes participation through INB's incentives to implement asynchronous validation of the data on the public blockchain through BFT algorithm and to prevent the super nodes from jointly cheating, which greatly increases the degree of centralization and security of the public blockchain. At the same time, the INB Blockchain selects the validation node through the VRF (Verifiable Random Function)[8] random drawing mechanism, which guarantees the random verifiability of the validation node and prevents the super node and the validation node from joint evil.

2.2.3 Security : Usage Principles of Resources and VRF Random Validation

For INB Blockchain, security is embodied in two aspects: security of traditional public blockchain and security of data on blockchain.

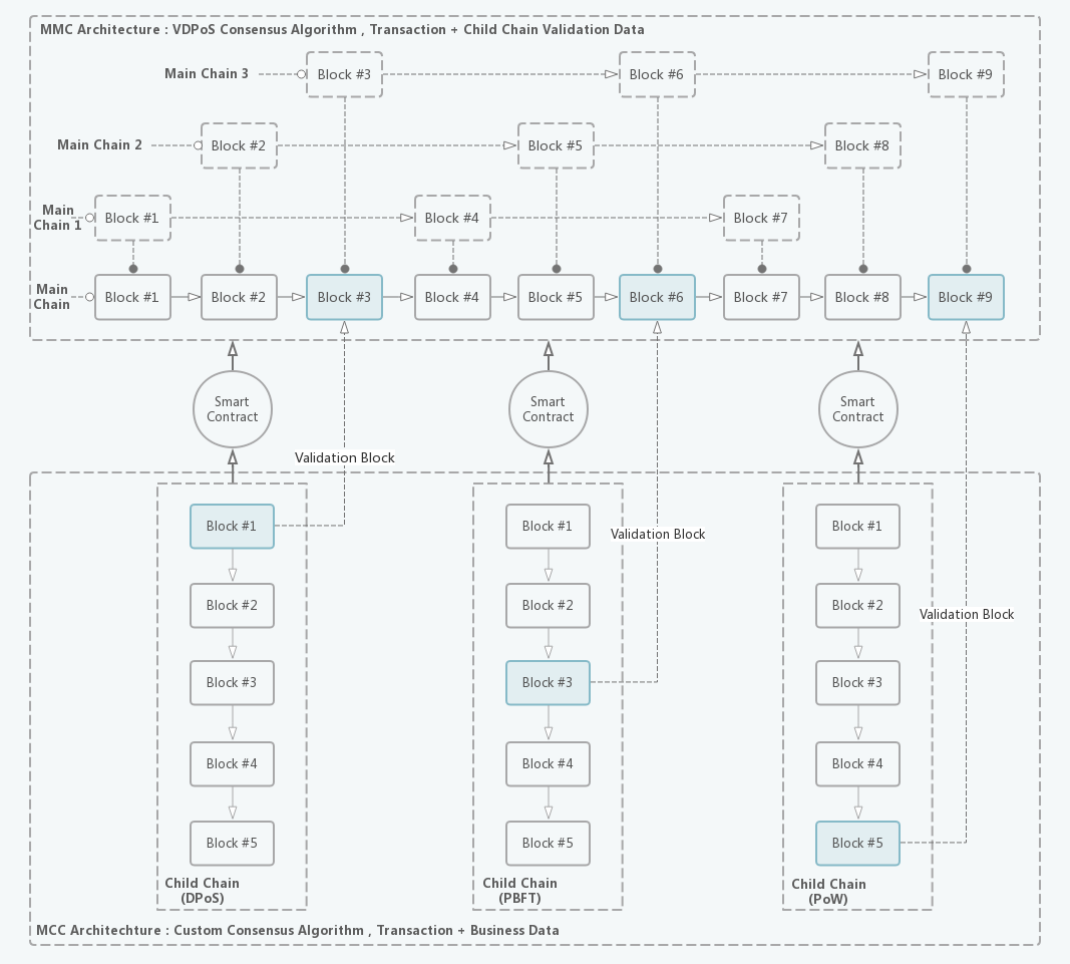
INB firstly takes advantage of algorithms and mechanisms such as Hash algorithm [11], asymmetric encryption [16], and MPT (Merkle Patricia Trie) to ensure the normal logic security of the public blockchain. For the prevention of malicious attacks, the INB Blockchain uses the INB issued on the mortgage blockchain in exchange for the right to use the resources on the main chain: including the right of using CPU and network, which could avoid hackers from attacking the public blockchain network through DDoS [28] and other methods. In the meanwhile, for child chain data storage resources, DApp needs to pay according to the amount of data stored, and it can also prevent malicious attacks. In addition, the INB Blockchain uses a random validation mechanism based on VRF to verify the selection of nodes, the validation of sharding and other mechanisms to prevent super nodes and validation nodes from evil.

For the security of the data on the blockchain, INB Blockchain will perform encrypted storage for data users who need to keep it confidential, and the user's private key or private keys of other authorized accounts are needed for decryption and observation. As well, both data storage and property changes require encryption by the

owner or authorized user's private key.

2.3 Core Architecture: Multi-Main Chain and Multi-Child Chain

The INB Blockchain uses the mixed architecture of Multi-Main Chain + Multi-Child Chain (short for “MMC + MCC”) and is the first public blockchain in the world to use this mixed architecture. According to the resource utilization of the entire public blockchain, the super node is automatically got sharding to form a multi-main chain parallel block producing mode, and the network resources are fully utilized to greatly increase the block production speed and the vertical scalability of the public blockchain; in the meanwhile, multi-child chains can be started on the main chain according to the use of the application to support more DApp business data blockchains to be stored on blockchain and increase the horizontal scalability of the public blockchain. The INB Blockchain consists of super nodes, validation nodes, supervision nodes, common nodes, and child chain nodes.



MMC + MCC Architecture Diagram

INB introduces INB utilization model (IUM) to measure resources usage situation of the entire public blockchain, including the use of CPU and memory resources usage of super nodes, resources usage situation in the network within the public blockchain, etc. to quantify and assess resources usage situation of the entire public blockchain. According to the resource utilization rate, the INB Blockchain will automatically divide sharding of super nodes. After the sharding of super nodes, multiple parallel main chains will be formed. The system will control the sharding at different nodes in the parallel main chain produce blocks in turn to form a multi-main chain parallel block production mode. It makes full use of the resources of the public blockchain and super nodes, and the distribution and validation of the block after the block production also occupies the network connection between different nodes, and therefore, the resource utilization rate of the entire public blockchain is maximized. When the node or network

is upgraded, the number of sharding will automatically increase, thus automatically realizing the vertical scaling of the public blockchain.

INB introduces a data tiered model to realize tiered management of transaction and business data. Rather huge valuable transaction data and child chain validation data are stored on the main chain while business data is stored on the child chain, and global data state is introduced at the same time. Data such as data version, price, number of purchasing, and number of views can be structurally stored on the child chain. Child chains are initiated by nodes or communities and be started after super node voting. Different DApps can use different child chains to store data, forming a multi-child chain parallel model, which increases the horizontal scalability of the public blockchain to nearly infinite.

2.4 Vertical Scaling: Multi-Main Chain Architecture

The main chain of the INB Blockchain uses VDPoS consensus algorithm (DPoS + BFT + validation node), among which 21 super nodes run the DPoS algorithm and produce blocks in a fixed order, and the principle of fixed order is adjacent to the node near it, that is, the nodes with short network transmission time are adjacent to each other to minimize the network transmission time after each block production, and the order will be determined before each round of block production. BFT algorithm is responsible for rapid first-level validation of the main chain block production. At the same time, INB Blockchain will automatically divide shards of the super nodes according to resources utilization rate of the public blockchain. The maximum number of sharding is equal to the number of super nodes. After sharding division, each shard is equivalent to an independent super node, which is called super node shard. Take one shard from each 21 super nodes to form a main chain, thus form an architecture of multi main chain parallel running. The formula can be expressed as:

$$Num(M) = Num(S) = 1 / Max(IU(Net), IU(SNode)) <= 21,$$

among which, Num (M) represents the number of main chains, Num (S) represents the number of sharding, IU represents the utilization rate, IU(Net) represents the utilization rate of network, and IU (Node) represents the utilization rate of super node.

In INB Blockchain, the block production time of each main chain is 0.5 seconds. In order to save the use of network, in each sharding, super node will continuously produce a certain number of blocks (for example, 6 consecutive blocks), and then turn to the next node. This continuous block production mechanism also prevents bifurcation. Multi-main chains will produce blocks under the same mechanism, but there is a difference of 0.5/Num (M) in block production time, and within 0.5 seconds, super node sharding of each main chain will production block once, forming a multi-main chain continuous block production mechanism. The sharding generating blocks within the 0.5 seconds are at different super nodes, thus maximizing the use of network and super nodes resources. For example, in the case of 20 sharding for each super node, the entire main chain will produce block once every 0.025 seconds, which is 20 times higher than TPS of traditional DPOS algorithm and greatly reduces latency time. The diagram is shown below. Taking advantage of this mechanism, main chain will achieve transaction data processing ability of more than 100,000 per second (100,000+TPS) under existing conditions, and will gradually increase with nodes and network capabilities improving.

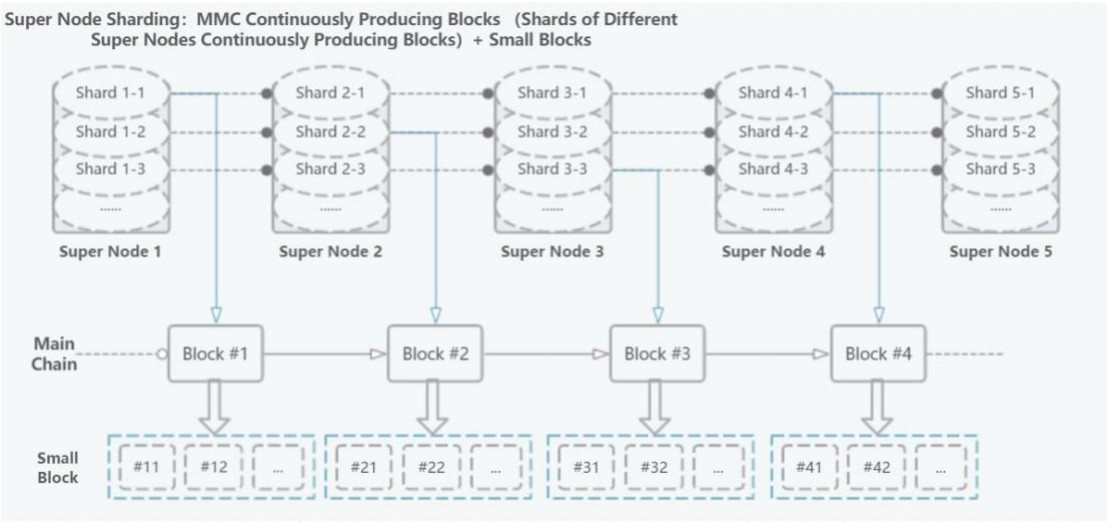


Diagram of Super Node Sharding

2.4.1 Dynamically Planning to Determine Block Producing Sequence

As mentioned above, before each round of block production, the sequence of super nodes sharding must be determined in advance to enable synchronization of block data as soon as possible. This problem can be described as: as the distance between any two nodes is known, please find out the shortest path of traversing all nodes from one node, what is TSP [34] (Travelling Salesman Problem). INB Blockchain introduces dynamic planning [29] algorithm to deal with the TSP problem.

2.4.2 Self-adaptive Multi-Main Chain Architecture

2.4.2.1 Self-adaptive Shards of Super Nodes

The Auto-Shading Algorithm of super nodes will be executed automatically at regular intervals according to the utilization of super nodes and network utilization to maximize the use of network and super node resources, which is also called the self-adaptive vertical scaling mechanism of INB Blockchain. In general, the number of sharding will be more than 10, which means that TPS of traditional DPoS is increased by 1-2 orders of magnitude.

2.4.2.2 Node Self-adaptive Rewarding Mechanism

In addition to the main chain self-adaptive sharding mechanism, INB Blockchain rewards different numbers of INBs based on the node's processing speed, network latency, etc., which is called the node self-adaptive rewarding mechanism to motivate nodes to increase configuration and perfect network with the load of the public blockchain increasing, thus realizing the vertical scaling of the entire public blockchain without investing a lot of resources in the early stages, which is called self-adaptive multi-main chain architecture in the INB Blockchain. This is a great breakthrough. For example, the continuously upgrading of CPU and memory, the popularity of 5G, etc.,

will bring great improvement to the performance of the main chain.

2.5 Horizontal Scaling: Multi-Child Chain Architecture

The INB Blockchain stores transaction data on the main chain and structurally preserves business data on the child chain. The storage on blockchain of ordinary non-transacted business data is a key factor of many DApps' implementation. INB Blockchain uses a multi-child chain structure to store business data on blockchain, encrypt and decrypt the data necessarily, which is the first public blockchain to realize structural storage on blockchain of business data.

2.5.1 Mechanism of Child Chain

Child chains are initiated by DApp or communities to initiate proposals of child chains, and to select a suitable consensus algorithm. Child chains can use the consensus mechanism of the BFT type league blockchain, or they can use the public consensus mechanism such as PoW, PoS, and DPoS. According to different DApp requirements for the efficiency and security of the data being stored on blockchain, different consensus algorithms are selected, and the public blockchain does not limit the consensus mechanism of the child chain.

The child chain initiation proposal is voted by super nodes. After agreeing to vote, the public blockchain will automatically start a child chain smart contract to manage child chains, and then wait for the addition of child chain nodes satisfying conditions to initiate child chains.

2.5.2 Child Chain Service Provider

DApp's using resources of child chains will pay through INBC, which is the abbreviation of INB Child Chain Coin. There is a smart contract based on the Bancor [37] protocol on INB Blockchain. The smart contract can be exchanged between INB

and INBC. INB can be converted into INBC through this smart contract. Similarly, returning INBC to the smart contract will be obtained at the current price of INB. This child chain resource payment mechanism will stimulate specific individuals or institutions to join the entire public blockchain ecosystem, providing child chain nodes for DApp, called child chain service provider. To become a service provider, certain an amount of INB must be mortgaged to the public blockchain to prevent evil.

2.5.3 Data of Child Chain

The data that can be stored on the child chain can be divided into three types: INB's transaction data, Token's transaction data and business data. The first two types are collectively referred to as transaction data and are similar to the data stored in existing public blockchains. The third type is an innovative business data structural storage method for INB Blockchain. In addition to various versions of business data, various properties of business data will be structurally stored.

As for business data, the data may change and the property will change accordingly. All these changes will be stored in the form of data versions and property changes, ensuring that records are searchable and traceable, realizing structural storage on blockchain of data. It has laid the technical foundation for the large-scale application of DApp.

2.5.4 Validation of Child Chain Data

Child chains will run under certain a consensus algorithm, the data is stored on nodes of child chains, and in order to ensure security and credibility, the child chain will store validation information of the data to the main chain for validation of the child chain data. After the production of a certain number of blocks, the roots of the Merkle tree corresponding to the part of blocks will be stored on the block of the main chain to ensure the security and credibility of the child chain. The blocks on the corresponding

child chain are called validation blocks.

Not all blocks on child chains are validation blocks, and there may be a certain height interval. INB Blockchain will automatically select the interval according to the resource utilization situation of the main chain. When the resource utilization rate of the main chain is comparatively low, the hash value of each block may be stored on the main chain, but when the resource utilization rate of the main chain is high, there will be more heights at intervals, and the number of intervals has no influence on efficiency of child chains. Only when selecting main chain to verify child chain blocks, the efficiency would be affected. The main chain verifies the data on child chains at regular intervals.

2.5.5 Anti-fraud of Child Chain

With a child chain being opened by many service providers, the risk of cheating may occur due to the low degree of decentralization. The supervision node should take the responsibility and obligation to supervise the operation of the child chain and submit the certificate on cheating to main chain for voting validation once a node's cheating is found. After voting, the supervision node will be rewarded by INB Blockchain and cheating service providers will be penalized.

2.6 INB Utilization

In the existing consensus, an important means to improve the TPS system is to find the bottleneck of consuming resources and then to import or to optimize of existing algorithms and logic so as to improve the utilization of the whole blockchain resource. INB Blockchain, focusing on existing problems, has put forward several means discussed below to improve the utilization of resources.

2.6.1 INB Utilization Model (IUM)

In order to measure the resource utilization of the whole public blockchain, INB Blockchain puts forward a concept of utilization model: INB Utilization Model, referred to as "IUM", which includes: CPU, memory resources and network resources of the super node. IUM model will provide public blockchain resource utilization: INB Utilization, referred to as "IU", including the Utilization rate of blockchain, and blockchain network (IU (Net)) and super node (IU (SNode)).

If we set the distance between any two super nodes for D (I, j), network bandwidth for B (I, j) and the current network usage for O (I, j), the IU (Net) = Max (O (I, j) / B (I, j)).

If we set each super node resource utilization for RU (i), the IU (SNode) = Max (RU (i)).

2.6.2 IUM Applications: Self-adaptive Sharding of Super Node

Due to the positive relation between running efficiency of the whole public blockchain and IU, when IU is very small, public blockchain resources should be made full use to improve the scalability, based on which INB Blockchain puts forward to according to the size of the IU automatically adjusting shards of super node number and the height of the child chain validation block interval, so as to make full use of the resources of the whole blockchain and improve the TPS.

Using VDPoS consensus algorithm, IU still cannot reach the maximum with a main chain operating with full TPS. Therefore, the INB Blockchain puts forward the architecture of multi-main chain operation to make full use of the public blockchain resources, improve TPS of public blockchain and reduce the time of block producing. In multi-main chain operation, it should be prevented that multiple shards of one node produce blocks continuously and that the net between same nodes is taken up repeatedly,

so as to improve utilization of network.

At the same time, INB Blockchain puts forward a series of mechanism to bring down the utilization of public blockchain resources and improve the processing ability of public blockchain. The following is the discussion from these two aspects: improving network efficiency and reducing consumption of node resources.

2.6.3 Improving Network Efficiency: Improving Kademlia Network with Floyd Algorithm

In INB Blockchain, the main chain will be made up of 21 super nodes, which forms a super node, Kademlia [43] (hereinafter referred to as KAD) network, keeping other super node location information in all super nodes. Different from the traditional KAD, INB Blockchain preserves the distance information of any two nodes, and introduces the Floyd [32] algorithm to improve the efficiency of data transmission between nodes.

Data transmission between nodes is a time-consuming operation, directly impacting on the block producing time of public blockchain. Thus, INB Blockchain will improve network efficiency through introducing Floyd algorithm. When a node transmits data to another one, Floyd can be used to choose the shortest path towards other nodes for communicating and improving the network efficiency.

If we set the distance between any two super nodes for D (I, j), then the data transmitting from one node to other nodes can be regarded as a problem, that is to find the shortest path in the whole situation, which can be solved by Floyd.

INB Blockchain will re-calculate the distance D (i, j) between arbitrary two nodes every once in a while, and update the corresponding distance information in KAD network. When transmitting data, compared with “directly linking to all nodes to transmit data”, it can be time-saving to transmit data through the shortest path found by

the Floyd algorithm.

2.6.4 Reducing Consumption of Node Resources

The consumption of resources such as CPU and memory of node is also an important indicator in the INB Blockchain utilization. First of all, using VDPoS consensus algorithm in INB Blockchain, not like mining of PoW, largely reduces resource consumption; and then, INB Blockchain offers two kinds of methods to reduce the consumption of node resources.

2.6.4.1 Transaction Engine of Public Blockchain: To Simplify the Issuance and Transaction of Token

INB Blockchain puts forward another way to reduce the consumption of node resource significantly: to separate smart contracts of Token in traditional public blockchains from smart contact business and to implement with simple scripting language, which is called INB transaction engine (ITE, INB Transaction Engine). On the Ethereum, a large proportion of smart contracts are issuing contracts of Token, more than half among which are transaction of ETH and Token implemented by starting virtual machine to call smart contracts. Such methods consume much system resources. If it is in INB transaction engine, the resource consumption can be reduced largely, and time will be saved in the transaction and validation of Token.

As INB Blockchain will acquiescently support protocols like ERC20, ERC721 and ERC223, ERC621 and ERC827, users can apply token conforming to these protocols through visible methods, and therefore, smart contracts cannot be called in the transaction process of Token and less resource can be consumed. INB Blockchain also will update its supporting Token issuing protocols in order to support most of protocols and then simplify the issuing and execution of Token thoroughly.

2.6.4.2 Sharding of Block Package and Validation

INB Blockchain is going to use a kind of method for sharding of block package and validation. If the data volume of each block is huge, the block package and validation are both time-consuming. INB Blockchain will conduct sharding towards each block with VRF random drawing mechanism and then give out to various nodes to package and validate, which can improve the utilization of nodes maximumly and reduce the processing time. Meanwhile, this kind of random drawing will be validated by other nodes to prevent cheating.

2.7 Smart Contract

Smart contracts of INB Blockchain can be divided into two kinds: visible smart contracts and Turing-complete smart contracts based on IVM

2.7.1 Visible Smart Contract

The design of INB Blockchain is to simplify scenarios in which users utilize smart contracts and to reduce the occurrence of errors, trying to modularize common smart contracts. Based on this concept, INB Blockchain will provide a visible smart contract creation method, including:

- Simplifying issuance: a token can be produced after filling key parameters, maximumly providing convenience for users to issue and other operations like transaction and checking balance. The produced Token can be built-in protocol like ERC20 [36], and can natively support for the issuing method of token based on Bancor protocol [37] and the issued token with the storage of reserve fund, which means that a certain number of bonded INB can be used to issue the Token.

- INB Blockchain will provide smart contracts related to data's producing,

processing, analyzing and resulting, which can all be chosen for users to design a big smart contract containing multiple module smart contracts.

- INB recommends corresponding every function of DApp to smart contracts to ensure the credibility of procedures.

2.7.2 Smart Contracts Based on IVM

As well, INB Blockchain will provide Turing-complete smart contracts for un-common or more complex logic to call. INB Blockchain will support smart contracts through the wholly new Virtual Machine (the IVM, INB Virtual Machine) that will use WebAssembly (WASM) [38] scheme, which means that developers can use any familiar programming language to develop smart contracts with more superior performance.

2.7.3 Smart Contract Service Providers: Implementation of Big Data Algorithm

INB Blockchain will separate the ownership and the using right of smart contracts, and introduces smart contract service providers to impel service providers to provide smart contracts related to big data processing and analyzing. Therefore, the big data algorithm can be integrated for the payment of third-party.

2.8 Random Validation Mechanism Based on VRF

INB Blockchain's introducing verifiable random function, VRF, takes full advantage of the randomness and verifiability of VRF, and implements verifiable random logic, preventing from cheating. There are two places using VRF: the selection and block producing of validation nodes and the sharding logic of validation.

After producing block, the super node should verify the block firstly. At the same time, in order to prevent united cheating of super nodes, a random group of validation

nodes need to be chosen to verify blocks, while the random drawing mechanism of VRF for choosing validation nodes effectively prevent the united error of super nodes and validation nodes. Such random drawing will be conducted by other nodes to verify, so as to prevent cheating.

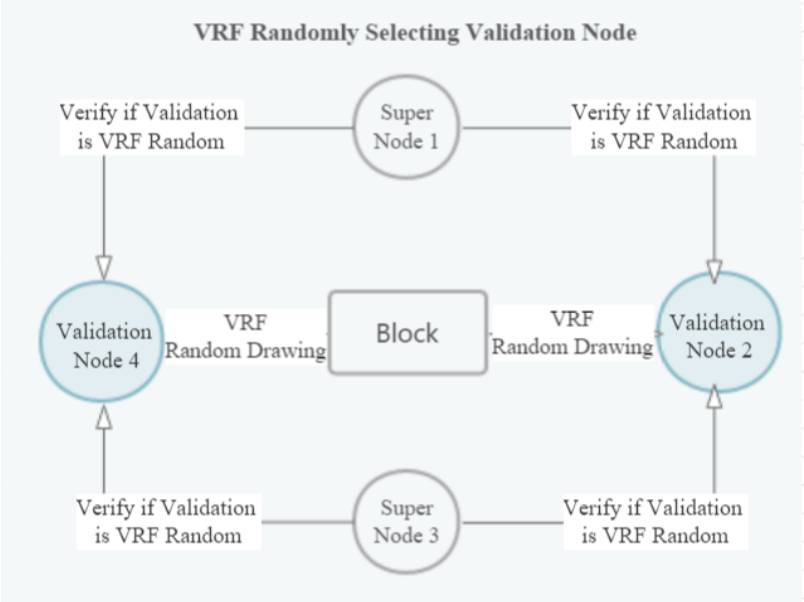
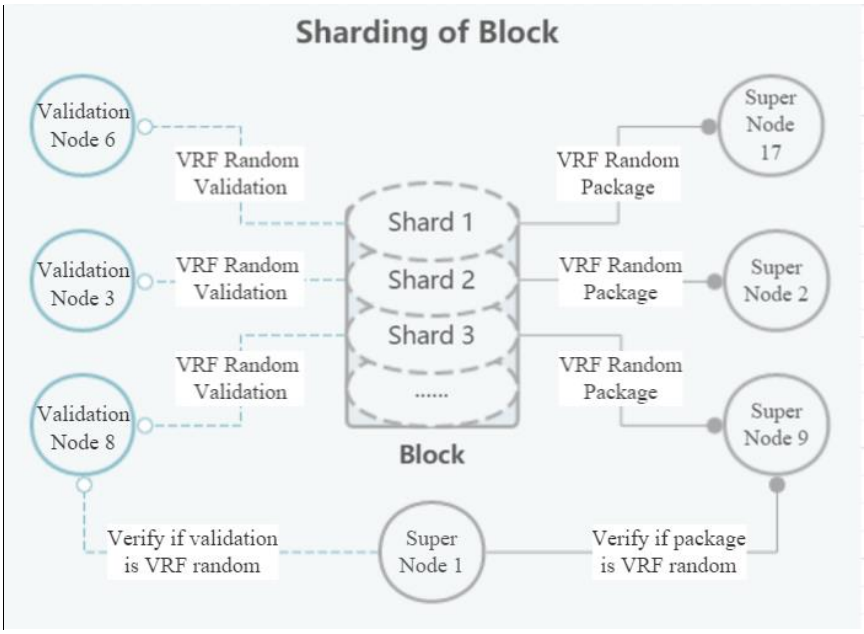


Diagram of Randomly Selecting Validation Node Based on VRF

INB Blockchain will use a kind of method for block package and validation sharding. If the data volume of each block is huge, the block package and validation are both time-consuming. INB Blockchain will conduct sharding towards each block with VRF random drawing mechanism and then give out to various nodes to package and validate, which can improve the utilization of nodes maximumly and reduce the processing time. At the same time, this kind of random drawing will be validated by other nodes to prevent cheating.



Sharding Diagram of Data Package and Validation

2.9 Storage on Blockchain Mechanism of Data

To support more applications put into use and realize data's structuration storing on blockchain, INB Blockchain divided stored data into several kinds: INB transaction data, Token transaction data and business data, the former two kinds of which can be collectively described as transaction data, similar as stored data on current public blockchain. The third is the storage on blockchain of business data, also called non-transaction data.

It is a great advantage of INB Blockchain to conduct structural storage of business data on blockchain, differing from traditional public blockchain projects' simply storing data content on blockchain instead of properties of data and storage process. As a result, it can truly guarantee data credibility. At the same time, data stored on blockchain are not structural, thus information like relevance between data, as well as relevance between data and property and so on cannot be expressed; while structural storage of data on blockchain is taken in INB Blockchain, the business data can be explained through the chain itself without calling for a third party application to explain

nonstructural data, so that data credibility can be realized and value transferring can be guaranteed.

The business logical diagram of the whole data being stored on blockchain is as follow:

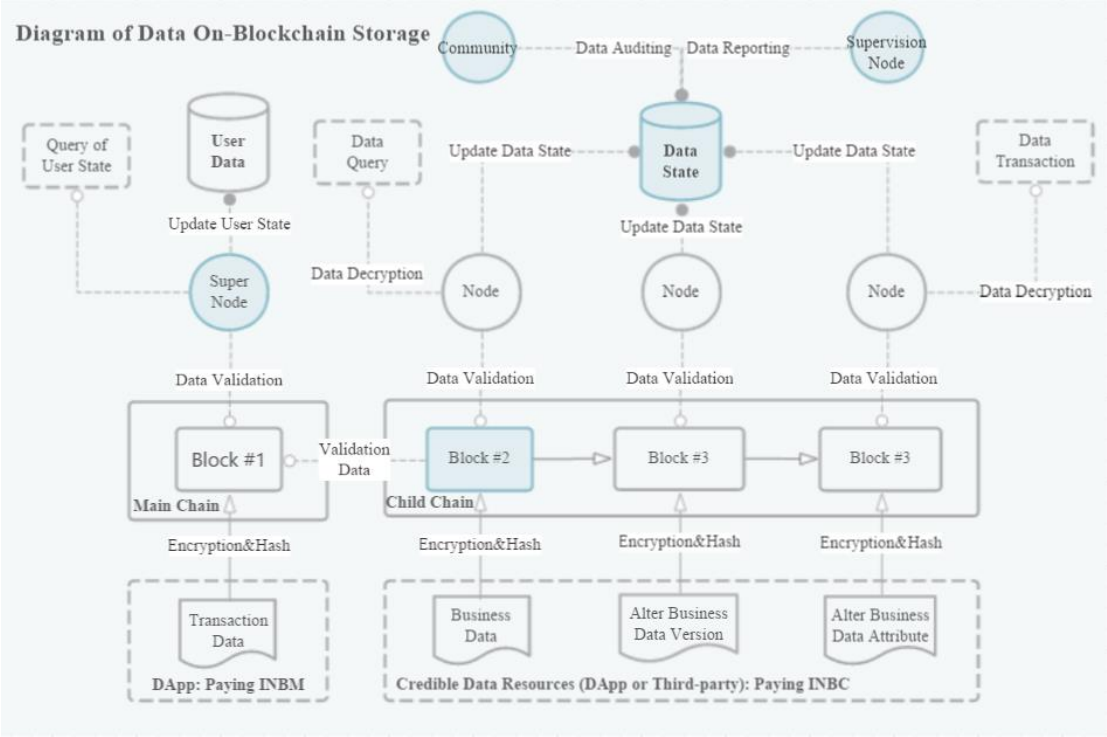
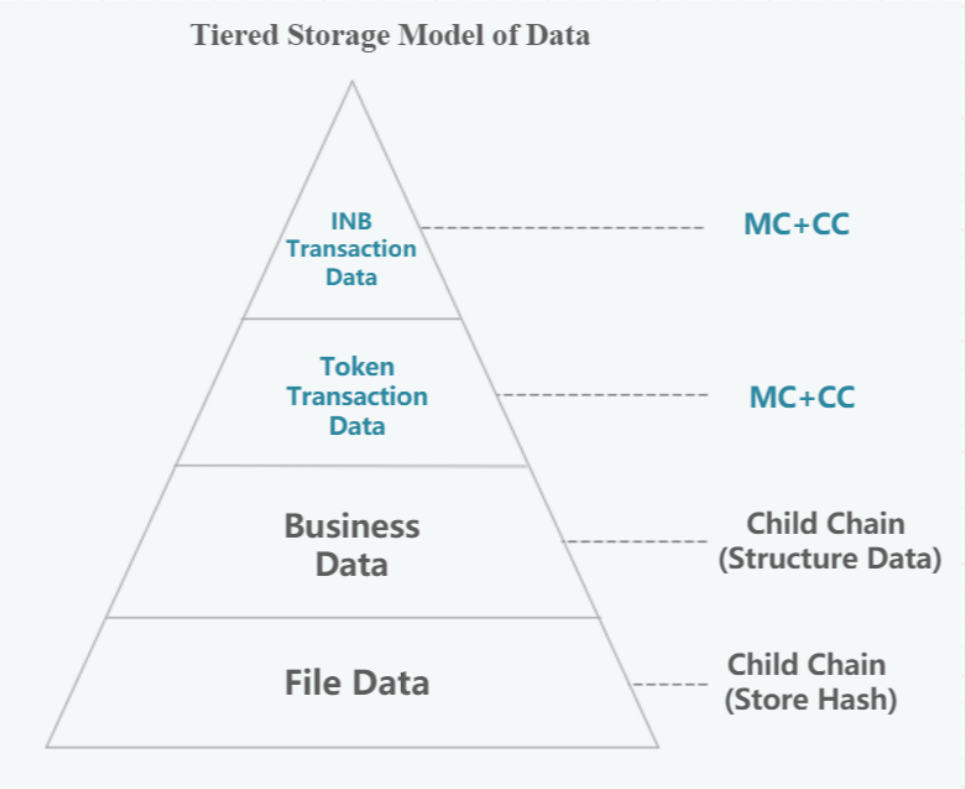


Diagram of Data On-Blockchain Storage

2.9.1 Tiered Storage Model of Data

INB Blockchain will store the data mentioned above hierarchically to satisfy the needs of multiple kinds of data. Transaction data of INB and Token will be stored on main chain to satisfy the demand of transaction data on high reliability and unchangeable attribute, while the business data are kept on child chain to meet the demand for high availability. In view of the demand of being stored on blockchain of business data with low value and oversize volume, it is suggested by INB Blockchain that the Hash value can be stored on blockchain while initial data can be stored off blockchain.



Tiered Storage Model of Data

2.9.2 Storage on Blockchain of Business Data

INB Blockchain defines two types of business data: main business data and relevant business data. The former is business data initially set, for example: original information of questionnaire. The latter is process business data related to main business data, generally corresponding to some certain operation of users, and sometimes it is also called operation data, for example: users' answers data for certain a questionnaire. Information of establishment and revision records of data, revision record of common properties of business data, business data operation record of accounts, business data transaction record, etc. are stored on INB Blockchain, and the process of completing storing business data on blockchain can fulfill requirements of tamper-resistance and traceability.

In many application scenarios, being stored on blockchain of business data, for example, the users' research data, the purchasing data of goods, evaluation data of brands, etc., is helpful to improve the credibility and traceability. And there is a very strong demand for the purchasing volume and evaluation value of data to be stored on blockchain, which cannot be supported by existing public blockchains. Seeing that, INB Blockchain designs the structural storage on blockchain mechanism for business data. Business data is the innovative structuralizing storage method of data in INB Blockchain, being stored various version, various attributes of data and the relevance relationship between data on blockchain structurally and conducting traceable upgrading and maintaining. The storing on blockchain of Business data features in three aspects:

- Data can be changed, reflected as data version in INB Blockchain. Every change of data will be stored in the form of version on the blockchain, and all the change history can be traced back to the data.

- The attributes of data are stored structurally. Data attribute can be divided into association attribute and general attribute. The former attribute itself cannot be changed directly, but another piece of data on the association blockchain can be changed automatically. Taking purchasing data as example, users' purchasing data stored on blockchain can be added automatically. The latter can be changed directly. For example, the price data of data is fixed by data owner, which has lower association with data on other blockchain. As well, all changes history of attributes will be stored.

- Relevance between data, as well as relevance relationship between data is the process of data generation or change and the base of data trustworthiness and credibility. INB Blockchain stores the relevance relationship and truly realizes credibility of data. For instance, the relevance between purchase data of users and purchase quantity of goods can be associated and updated automatically

through public blockchain.

- Encrypted validation, changes of data and attribute need to be encrypted with users' private key and can be stored and changed only after public validation.

2.9.3 Safety of Business Data

Before being stored on blockchain, sensitive data or data users want to use for transacting can be set to encrypted data. In this way, INB Blockchain will make use of users' private key to encrypt part of the data and independently store it to attributes: in encryption fields, other users can only view the encrypted data when browsing, which can ensure the safety of data. When users want to view or transacting data, their own private keys or authorized private keys are needed to decode. The encrypting and decrypting are finished by super nodes, showing fair and credible.

2.9.4 State of Business Data

In traditional public blockchains, the whole state of accounts is stored on the blockchain: information like account balance. Except for these, INB Blockchain stores the whole state of business data mentioned above, shown in the table below:

Data Hash	Unalterable
Original Data Hash	Unalterable
Data Version	Business Data Content
Related Data	Unalterable
Price	General property
Browsing number	Association property
Likes number	Association property
Dislikes number	Association property
Collection number	Association property
Purchasing number	Association property

Level	General property
Transaction or not	General property
Limitation	General property
Encrypted fields	General property
Examiner	Association property
Whistleblower	Association property
Any problem or not	General property
Classification	General property
Owner	Association property
Founder	Association property

INB Blockchain stores the whole state information of data, which is convenient for fast query and more application data being stored on blockchain, such as research data, commodity purchasing data, evaluation data and browsing information. It is not recommended to store multimedia files or oversize business data on blockchain. INB Blockchain will limit the size of stored data, and the for oversize data, it is recommended to store its Hash value. on blockchain while the initial data can be stored off blockchain.

2.9.5 Transaction of Business Data

INB Blockchain will provide transaction module of business data and original support of data transaction for data to be transacted. After encrypted data receiving users' transaction request and obtaining the agreements of all data users or authorized users, INB Blockchain will give new users data decryption as well as data viewing right, so that a new global data state can be formed and same encrypted fields will be stored after being encrypted with new user's private key. Data transaction is going to be taken on INB or INBC and charged according to the price in data attributes and INB Blockchain will charge a fee as mining fee.

2.10 Credible Data Resources Mechanism

At present, there are many platforms reserved a great number of users' data like shopping data on JD.COM, interest data on Weibo and voting data on WeLike, showing users' great demand to store existing data on blockchain and conduct transaction. In order to adapt to this kind of scenario, INB Blockchain provides a reliable data resource mechanism launched by community credible data application and voted by super nodes. Credible data through voting will be written on the blockchain and then users' produced data on credible resources can be saved on the blockchain for transacting or viewing. Similarly, DApps on INB Blockchain are original credible resources, and therefore, users' data produced in DApp can be stored on the blockchain.

2.11 Auditing and Reporting of Data

After business data's being stored on blockchain, because the owner and producing process of data need to depend on a third-party DApp, which cannot be complete credible, INB Blockchain provides functions of auditing and reporting towards initial data.

Data stored on blockchain can be audited by other users, processing of which can be stored on blockchain by public blockchain, including approved and not approved users. The following specific processing logic will be different according to different processing logic of DApp. For example, it can be thought that in a DApp, only a 100% auditing approval can show this data and conduct transaction while in other DApps only 60% is needed. Meanwhile, DApp can reward auditing users with INB.

Similarly, after being stored, data can be reported by other users. Data reported for too much times may be taken down on DApp, prohibiting viewing and transacting. The specific quantity requirement is also specified by DApp according to internal logic. At the same time, DApp can reward users who report data with INB.

2.12 Introducing in DApp Role

To adapt to the implementation of applied blockchains, the INB Blockchain introduces in the DApp role to distinguish the DApp role from the account, many DApps constituting the data ecosystem of INB Chain. DApp is composed of multiple accounts and smart contracts, multiple accounts of which are used for the circulation between the currency/Token owned by DApp and that of users and public blockchains while multiple smart contracts embody the transfer of DApp's functions into smart contracts.

Meanwhile, DApp will be associated with business data and operations on the INB Blockchain, and DApp generated by data will be stored for business data and operations saved on the blockchain.

2.12.1 Payment by Others of Using Public Blockchain Resource

At the same time, paying by others is supported in INB Blockchain. DApp will be able choose other users to pay for the use of public blockchain resources, separating common users from the storage and use of the underlying blockchain and avoiding too much understanding of users about the storage and payment logic of blockchains, as well, laying a foundation for the large-scale application and popularization of blockchain.

2.13 Using Rules of Resources on Blockchain

In response to different application scenarios, INB Blockchain will provide two kinds methods to use resources on blockchain: usage method of business data-related resources based on INBC and usage method of transaction data-related resources based on INBM.

2.13.1.1 Use of Business Data-Related Resources

Business data-related resource is kind of child chain related resource. As a result of the huge storage volume of business data, it is needed to pay independently for each data production and transaction. INB Blockchain will issue an internal token: INBC, which is issued based on Bancor protocol, using INB to exchange for the production, viewing and transaction of data. At the same time, users' residual INBC not used can return to the INB Blockchain smart contracts to cash for INB at current price.

2.13.1.2 Use of Transaction Data-Related Resources

Transaction-related resources includes resources of super node and network resources between super nodes. For transaction data, INB Blockchain will issue an internal token: INBM and a smart contract of mortgaging INB. The token can be produced once every day after the INB mortgage to smart contract, and can be used in scenarios related to transaction, such as creating smart contract, transacting and calling smart contracts. Users can redeem mortgaged INB if there is no need of INBM.

2.14 Cross Blockchain

As more and more blockchains appear, demand for cross blockchain [42] has been more intense. An outstanding characteristic of INB is to provide atomic-scale interaction between different coins and INB Blockchain coins. As well, the public blockchain and child chain of INB Blockchain need interactions. The next will be discussed from two aspects.

2.14.1 Cross Blockchain between INB Blockchain and Other Public Blockchains: State Channel Contract

INB Blockchain uses state channel to build cross blockchain with other public

blockchains, providing a series of native state channel smart contracts, each of which corresponds to one public blockchain and the mapping of corresponding currency on public blockchain.

For example, with regard to BTC, INB Blockchain will provide a BTC cross blockchain state channel smart contract, an account receiving BTC and IBTC tokens, in which the IBTC token is the 1:1 mapping of BTC on INB Blockchain. When users store BTC in this account receiving BTC, this smart contract will allocate same amount of IBTC to users automatically. The transaction of IBTC represents real BTC transaction. When users want to get their BTC back, they return IBTC to smart contract which will send BTC in account to certain appointed account automatically.

Such built-in cross blockchain mechanism increases the convenience to help scenarios like decentralized exchange with strong demand for cross blockchain.

2.14.2 Cross Blockchain within INB Blockchain: Execution by Mandate and Public Notary Person

INB Blockchain includes main chain and child chain, and therefore involves two cross blockchain modes: cross blockchain between main chain and child chain as well as between child chains.

The users' transaction on the main chain and the child chain at the same time, INB Blockchain provides two ways of cross blockchain for data transaction aiming at the cross blockchain problem between main chain and child chain:

- One kind is similar to the cross blockchain way between INB Blockchain and other public blockchains, to provide a smart contract to solve such problem, which is equivalent to make the child chain as one state channel of main chain;

- One way is entrusted to execute the cross blockchain. When users perform

transactions on the child chain, the transact will be transferred to the main chain and be returned back when finished, so as to insure correct transaction.

With regard to the cross blockchain between child chains, the main chain will be the public notary, supervising and locking the related data and asset in smart contract between two child chains. When the transaction or data operations of two child chains are finished, unlocking can be implemented to ensure the atomicity of the whole cross blockchain operation.

2.15 Encryption and Validation Mechanism Based on ECDSA Algorithm

The account system INB Blockchain will use is based on both public key and private key, in which requests initiated by each account to public blockchain like transaction, data storing and data transaction will be asymmetrically encrypted, that is, encrypted by Elliptic Curve Digital Signature (Elliptic Curve Digital Signature Algorithm, abbreviated as ECDSA [15]) Algorithm. Super nodes will verify whether the encrypted data should encrypt for the account to confirm the legitimacy of the request. Only legitimate requests can be implemented, and at the same time, the validation of block is also based on ECDSA Algorithm. Each request in the block will be verified to prevent counterfeiting and falsifying.

2.16 Data Structure Based on MPT

MPT is the abbreviation of Merkle Patricia Trie, derived from the Trie structure and respectively inherited the advantages of Patricia Trie [20] and Merkle Tree [23]. On account of the characteristics of internal data, MPT designs a new node system, inserting and loading mechanism. In the storage of transaction data, user state, business data and data state as well as the validation of data on child chain, INB Blockchain utilizes the MPT data structure, as well as quick query and validation based on MTP.

INB Blockchain will use RLP (Recursive Length Prefix) [40] encoding to serialize data which will be stored into LevelDB [41].

2.17 On-Blockchain Data Query

Aiming at the enormous quantity of business data, INB Blockchain will provide much faster on-blockchain data query ways utilizing caching mechanism, and therefore really meets the needs of million level internet applications.

3. Insight Chain Operating System

Based on the above technical architecture, INB Blockchain provides 9 systems to form a complete operating system for public blockchain users like DApp.

3.1 Smart Contract Management System

INB Blockchain provides smart contract management system, with which users can manage their own created Token and smart contracts.

Token management includes functions like creation, inquiry, transaction of Token.

Smart contract management includes creating smart contract, invoking smart contract, payment settings, charge query, and other functions.

3.2 Reliable Data Resource System

Reliable data resource system can be applied to manage the credible data resource in INB Blockchain, save the data produced by credible data resource into public blockchain, and conduct data transaction. Its functions include: to start a vote towards credible data, to report credible resources and to inquire credible data, etc.

3.3 Child Chain Management System

Child chain management system manages child chains on INB Blockchain, including starting child chain voting, reporting child chain, viewing child chain data, applying child chain servicers and so on.

3.4 Account Management System

INB Blockchain designs a tiered management model of accounts, including the affiliation between accounts, classification of account permission, account authorization and so on. The system functions include: to provide convenience for scenarios like company accounts' management from the account management, permission management, multi-account authorization, authorization management, multi-signature, payment by another one (INBC, INBM and INB can support the payment by another one), etc., and to fully ensure the safety of the account.

INB Blockchain will provide a unified account system, and DApp on blockchain can use public blockchain account to log in. After logging in, users can directly authorize the wallet function on third party and manage authorized DApp.

3.5 Data Transaction System

INB Blockchain provides built-in data transaction system, including: data hosting, purchasing, query and other functions. After hosting, other users can directly purchase data through committed trustees.

3.6 Voting System

INB chain provides voting system including: the super nodes' election voting, child chains' voting, voting of complaint nodes and data, and voting of credible data resources.

There are two kinds of voting: anonymous voting and real-name voting. Anonymous voting will use ring-signature mechanism for encryption, while real-name voting records users' every voting process on blockchain.

3.7 Resource Management System

The resource management system offered by INB Blockchain includes two important functions: management of INBC and management of INBM, of which INBC is exchanged from using INB and INBM is got automatically from mortgage INB. The management of the two tokens are completed automatically by smart contracts, respectively used to pay for using resources of child chain and main chain.

3.8 Task System

INB Blockchain system built in the task system, becoming an in-depth exploration of the business layer of INB Blockchain and regularizing procedures of tasks like launching, accepting, pricing and paying into smart contracts. As well, INB Blockchain provides mechanism to manage smart contracts uniformly for the using of scenarios such as survey and sub-package related to tasks.

3.9 RPC API system

All kinds of nodes in INB Blockchain will provide RPC API, so as to offer the using function of resource on blockchain and viewing function of data on blockchain to outsiders.

4. Insight Chain Ecosystem

As a public blockchain in blockchain 3.0, Insight Chain realizes, in addition to the high TPS, the implementation of Internet and traditional business scenarios is also

important. And we believe that 2019 is expected to see the implementation of application scenarios. With the joint exploration of the blockchain industry, Internet and business, there will be a large number of new different application scenarios, pushing the blockchain industry to a new level, which is the symbol of the entire blockchain industry entering the 2.0 stage. So, we propose two points as the core goals of Insight Chain: to improve scalability and to meet the requirements of more applications to store business data on-blockchain under the premise of decentralization and security.

In INB Blockchain, all participants constitute a complete ecological system to ensure the healthy operation and development of INB Blockchain, including: super nodes, validation nodes, supervision nodes, common nodes, child chain service providers, child chain nodes, smart contract service providers, INB community, INB committee and INB team.

4.1 Economic Model

During initial design of Insight Chain, the using scenarios for coins have been designed, the Insight Chain White Paper [1] content being quoted as follows:

• Raising: 30%, private raising for funding, only for institutional investors, will be locked for one year;

• Community: 30%, being used to reward partners in the public blockchain, such as DApps and nodes;

• Team: 20%, being used to reward teams, consultants and other participants as well as foundation operation. It will be locked for 3 years;

• Marketing: 20%, being used for marketing of products, fund raising and so on.

INB Blockchain will not modify INB allocation plan, just to prevent the abuse of INB and increasing issuance, ant then alter 67% of the currency to mining producing mechanism (in fact, there is no mining in INB Blockchain, but here we call a processing, in which a node catches the excitation of blockchain, mining), and specific strategies are as follows:

Raising: 30%, need to be reserved before mining because it should be given out before the lock period in a year;

Community: 30%, divided into three parts. One part equals 20% for mining, assigned to mining nodes and validation nodes; one part for 9%, gradually produced by mining, assigned to community; the remained 1%, should be set aside and assigned to participants of community in the early period.

Team: 20%, divided into two parts. One part is reserved to assigned to INB development and operation team (still abiding by the promised three-year deblocking period in the white paper); the remained 19% will gradually produce with mining.

Marketing: 20%, divided into two parts. One part of 1% reserved for marketing related to INB Blockchain while remained 19% will be produced with mining step by step.

From the total quantity, INB will reserve 33% for allocation of raising, marketing and team, while the remained 67% will produce with mining and release gradually, 20% of which are assigned to super nodes, validation nodes and supervision nodes as award, and 47% are assigned to teams, community and marketing, as details are shown in the table below.

Allocation	Total Quantity	Proportion	Statement	Reserved	Mining
Raising	30%	30%	Reserved for private participants, released in a year	30%	
Community	30%	20%	Mining fee, award to participant nodes		20%
		9%	Producing in equal proportion with mining, community incentives		9%
		1%	Early community incentives	1%	
Team	20%	1%	Reserved for the early team incentives, released in three years	1%	
		19%	Producing in equal proportion with mining		19%
Marketing	20%	1%	Reserved for early INB marketing	1%	
		19%	Producing in equal proportion with mining, used for late marketing		19%
Total	100%	100%		33%	67%

4.2 INB Blockchain Management

INB Blockchain governance can be divided into on-blockchain governance, mainly conducted by super nodes like the set-up of child chain, nodes with problems and dealing with business data, and out-of-blockchain governance, decided by INB policy committee which is elected annually by INB holders.

4.2.1 Selection of Super Nodes

Super nodes will be selected by INB holders, taking one coin for one vote, voting for participating entity, which can be held in real time. INB Blockchain will update super nodes according to real-time voting results at regular intervals (1 hour).

4.2.2 Proposal

INB Blockchain employs proposal system to collect suggestions of community

towards the development of INB Blockchain, being adopted by committee, suggestions will receive certain INB incentive award from the INB part of community.

4.2.3 Supervision Node

With the introduction of supervision nodes, INB monitors the operation situation of the public blockchain and submits problems to super nodes for voting processing. The problems include but not limited to: data quality problem, super node cheating, cheating of nodes on child chains, cheating of node verification, etc. If the super node, after a voting, gives rewards to supervision nodes, and imposes corresponding penalties on cheating behaviors, the penalties include but not limited to deduct mortgaged INB, appear in the blacklist, ban the data, etc.

The regulatory nodes in DApp are similar to the rule of operating and auditing, taking charge of the auditing after the storage on blockchain of data. The data with problems, if being voted to agreement by super nodes, will be banned and nodes will never deal with any other request of the data.

4.3 Service Provider Ecosystem

INB Blockchain will introduce child chain service provider and smart contract service provider. Child chain service provider takes charge of starting child chain and offer storage on blockchain service of DApp on blockchain, profiting with taking INBC. Smart contract service provider will write smart contract with high quality of big data processing and AI, and open this smart contract in the form of service to other DApp, charging INB fee.

4.4 Data Transaction Ecosystem

INB Blockchain will build in the support for transaction business data, that is, transaction data can be the primary data on the blockchain and also can be proved third-

party data.

4.5 Ecological Application Scenarios

There are two key application scenarios of INB Blockchain: application like research industries, e-commerce industry and communities, which needs to make business data stored on blockchain and decentralized exchanges.

4.6 The Application of INB Blockchain in the Research Industry

In present research industry, problems like research user fraud, research data fraud, the overlong data blockchain remain very serious. Insight Chain, the first company putting forward the concept of storing data on blockchain, records the research scenarios and data onto blockchain, removes data mediator and uses smart contracts on research logistic and data processing. Insight Chain helps research data to regain its value to individual and the point-to-point transaction of research data, really realizing the blockchain transformation in research industry.

5. Insight Chain Roadmap

At present, INB Blockchain is under developing and the roadmap is as follows:

2018 Q3-Q4: The development and operation of Insight DApp, the design of INB Blockchain;

2019 Q1: Write the technical white paper, feasibility validation and the development of the prototype;

2019 Q2: Launch the Testnet, implement DPoS + BFT consensus;

2019 Q3: Realize smart contract based on IVM and INB transaction engine;

2019 Q4: Launch the Mainnet, realize multi-child chain architecture, business data onto blockchain;

2020 Q1: Realize multi-main chain architecture, INB utilization model and the main chain's self-adaptive sharding mechanism;

2020 Q2: Realize the cross blockchain mechanism both among public blockchains and among main-chains and child-chains;

2020 Q3: Realize the random validation mechanism based on VRF and to completely implement VDPoS consensus algorithm;

2020 Q4: Realize business data trading on blockchain, the high-speed query mechanism of business data and transaction.

6. Reference

[1] Insight Chain Founding Team, Insight Chain White Paper V 1.0, https://github.com/insight-chain/documentation/blob/master/en_US/insight_chain_whitepaper_v1.0_en_US.pdf, 2018

[2] Nakamoto S. Bitcoin: A peer-to-peer electronic cash system[J]. 2008.

[3] Buterin V. A Next-Generation Smart Contract and Decentralized Application Platform[J]. white paper, 2014.

[4] EOS.IO Technical White Paper v2[EB/OL]. https://github.com/EOSIO/Documentation/blob/master/TechnicalWhitePaper.md, July, 3, 2018.

[5] The ZILLIQA Team, The ZILLIQA Technical Whitepaper, 8, 2017

[6] Joseph Poon, Vitalik Buterin, Plasma: Scalable Autonomous Smart Contracts, 11, 2017

[7] Wood T, Singh R, Venkataramani A, Shenoy P, Ceeehet E. ZZ and the art of practical BFT execution. In: Proc. of the 6th Conf. on Computer Systems. New York: ACM Press[J], 2011.

[8] Micali, Silvio; Rabin, Michael O.; Vadhan, Salil P. (1999). "Verifiable random functions". Proceedings of the 40th IEEE Symposium on Foundations of Computer Science[J]. pp. 120–130.

[9] Castro M, Liskov B. Practical Byzantine Fault Tolerance And Proactive Recovery. ACM Trans. on Computer Systems[J]. 2002.

[10] Serafini M, Nokor P, Dobre D, Majuntke M, Suri M. Scrooge: Reducing the Costs of Fast Byzantine Replication in Presence of Unresponsive Replicas. In: Proc. of the 2010 IEEE/IFIP Int'l Conf. on Dependable Systems and Networks[J]. 2010.

[11] Dmitry Khovratovich, Christian Rechberger & Alexandra Savelieva (2011). "Bicliques for Preimages: Attacks on Skein-512 and the SHA-2 family" (PDF). IACR Cryptology ePrint Archive. 2011:286.

[12] Mario Lamberger & Florian Mendel (2011). "Higher-Order Differential Attack on Reduced SHA-256" (PDF). IACR Cryptology ePrint Archive. 2011:37.

[13] Ji Li, Takanori Isobe and Kyoji Shibutani, Sony China Research Laboratory and Sony Corporation, Converting Meet-in-the-Middle Preimage Attack into Pseudo Collision Attack: Application to SHA-2

[14] Dodis, Yevgeniy; Yampolskiy, Aleksandr. (2005). "A Verifiable Random Function With Short Proofs and Keys". 8th International Workshop on Theory and Practice in Public Key Cryptography. pp. 416–431.

[15] Koblitz, N. (1987). "Elliptic curve cryptosystems". Mathematics of Computation. 48 (177): 203–209. doi:10.2307/2007884. JSTOR 2007884.

[16] Miller, V. (1985). Use of elliptic curves in cryptography. CRYPTO. Lecture Notes in Computer Science. 85. pp. 417–426. doi:10.1007/3-540-39799-X_31. ISBN 978-3-540-16463-0.

[17] Bernstein, Daniel J.; Lange, Tanja. "SafeCurves: choosing safe curves for elliptic-curve cryptography". Retrieved October 1, 2016.

[18] Perlroth, Nicole; Larson, Jeff; Shane, Scott (2013-09-05). "N.S.A. Able to Foil Basic Safeguards of Privacy on Web". New York Times. Retrieved 28 October 2018.

[19] Morin, Patrick. "Data Structures for Strings" (PDF). Retrieved 15 April 2012.

[20] Knizhnik, Konstantin. "Patricia Tries: A Better Index For Prefix Searches", Dr. Dobb's Journal, June, 2008.

[21] Morrison, Donald R. Practical Algorithm to Retrieve Information Coded in Alphanumeric

[22] Merkle, R. C. (1988). "A Digital Signature Based on a Conventional Encryption

Function". Advances in Cryptology — CRYPTO '87. Lecture Notes in Computer Science. 293. pp. 369–378. doi:10.1007/3-540-48184-2_32. ISBN 978-3-540-18796-7.

[23] Becker, Georg (2008-07-18). "Merkle Signature Schemes, Merkle Trees and Their Cryptanalysis" (PDF). Ruhr-Universität Bochum. p. 16. Retrieved 2013-11-20.

[24] Koblitz, N. (1987). "Elliptic curve cryptosystems". Mathematics of Computation. 48 (177): 203–209. doi:10.2307/2007884. JSTOR 2007884.

[25] Miller, V. (1985). Use of elliptic curves in cryptography. CRYPTO. Lecture Notes in Computer Science. 85. pp. 417–426. doi:10.1007/3-540-39799-X_31. ISBN 978-3-540-16463-0.

[26] Bernstein, Daniel J.; Lange, Tanja. "SafeCurves: choosing safe curves for elliptic-curve cryptography". Retrieved October 1, 2016.

[27] Perlroth, Nicole; Larson, Jeff; Shane, Scott (2013-09-05). "N.S.A. Able to Foil Basic Safeguards of Privacy on Web". New York Times. Retrieved 28 October 2018.

[28] Adamsky, Florian (2015). "P2P File-Sharing in Hell: Exploiting BitTorrent Vulnerabilities to Launch Distributed Reflective DoS Attacks".

[29] Denardo, E.V. (2003), Dynamic Programming: Models and Applications, Mineola, NY: Dover Publications, ISBN 978-0-486-42810-9

[30] Sniedovich, M. (2010), Dynamic Programming: Foundations and Principles, Taylor & Francis, ISBN 978-0-8247-4099-3

[31] Moshe Sniedovich (2002), "OR/MS Games: 2. The Towers of Hanoi Problem", INFORMS Transactions on Education, 3 (1): 34–51.

[32] Floyd, Robert W. (June 1962). "Algorithm 97: Shortest Path". Communications of the ACM. 5 (6): 345. doi:10.1145/367766.368168.

[33] Cormen, Thomas H.; Leiserson, Charles E.; Rivest, Ronald L. (1990). Introduction to Algorithms (1st ed.). MIT Press and McGraw-Hill. ISBN 0-262-03141-8. See in

particular Section 26.2, "The Floyd–Warshall algorithm", pp. 558–565 and Section 26.4, "A general framework for solving path problems in directed graphs", pp. 570–576.

[34] Johnson, D. S.; McGeoch, L. A. (1997). "The Traveling Salesman Problem: A Case Study in Local Optimization" (PDF). In Aarts, E. H. L.; Lenstra, J. K. Local Search in Combinatorial Optimisation. London: John Wiley and Sons Ltd. pp. 215–310.

[35] "'Travelling Salesman' movie considers the repercussions if P equals NP". Wired UK. April 26, 2012. Retrieved April 26, 2012.

[36] "ERC-20 Token Standard - The Ethereum Wiki". Theethereum.wiki. Retrieved 30 August 2017.

[37] Bancor Protocol - Bancor Network, https://www.bancor.network/

[38] "WebAssembly High-Level Goals". GitHub / WebAssembly / design. 11 December 2015.

[39] Bright, Peter. "The Web is getting its bytecode: WebAssembly". Ars Technica. Condé Nast. 6, 2018.

[40] Recursive Length Prefix, Web3j, https://docs.web3j.io/rlp.html

[41] "Google Open-Sources NoSQL Database Called LevelDB". ReadWriteWeb. July 30, 2011. Retrieved July 30, 2011.

[42] Joseph Poon and Tadge Dryja. Lightning Network. https://lightning.network/lightning-network-paper.pdf, Mar 2015.

[43] Kademlia: A Peer-to-peer information system based on the XOR Metric.