



Connect, Transfer and Exchange All Digital Assets Over the World

WORLD'S FIRST PRACTICAL BLOCKCHAIN 4.0 PROJECT  
NEXT GENERATION GLOBAL VALUE INTERNET  
INFRASTRUCTURE TO SUPPORT BUILDING INDUSTRY CHAINS  
SCALABLE DAPP DEVELOPMENT PLATFORM

## TECHNICAL WHITEPAPER

InterValue Team

March, 2018

**Specification**

This document is InterValue Technology White Paper version V4.5. It mainly introduces the background, positioning, technical characteristics and application scenarios of InterValue. In the future, we will continually upgrade this document to keep it consistent with new technology evolvement. For the latest and more information of InterValue, such as technical white papers, software releases, developer communities, and more, please visit the official site: <http://www.inve.one>.

**Contact us**

White Paper: [whitepaper@inve.one](mailto:whitepaper@inve.one)

Community Management: [community@inve.one](mailto:community@inve.one)

Foundation: [foundation@inve.one](mailto:foundation@inve.one)

Others: [support@inve.one](mailto:support@inve.one)

**Copyright declaration**

Copyright of this document belongs to the InterValue team, all rights reserved.

**Disclaimer**

As Blockchain technology progresses, the InterValue team will improve and refine existing technology solutions as needed, and continue to improve the technical white paper.

# Contents

|  |           |
|--|-----------|
| <b>Abstract</b>  | <b>1</b>  |
| <b>1 Background</b>  | <b>3</b>  |
| 1.1 Blockchain Development Overview . . . . .  | 3         |
| 1.2 Key Technologies of Blockchain . . . . .   | 5         |
| 1.3 Current Problems of Blockchains . . . . .  | 6         |
| <b>2 Motivation</b>  | <b>9</b>  |
| 2.1 Name . . . . .   | 9         |
| 2.2 Vision . . . . .   | 9         |
| 2.3 Goal . . . . .   | 10        |
| 2.4 Ecological System . . . . .  | 10        |
| 2.5 Key Features . . . . .   | 13        |
| 2.6 Advantages . . . . .   | 14        |
| <b>3 P2P-based Anonymous Communication</b>   | <b>17</b> |
| <b>4 Data Structure</b>  | <b>20</b> |
| 4.1 Data Structure of the Basic DAG . . . . .  | 20        |
| 4.2 HashNet—a New DAG Data Structure . . . . .   | 22        |
| <b>5 Consensus</b>   | <b>27</b> |
| 5.1 DAG Consensus . . . . .  | 27        |
| 5.1.1 The Main Chain . . . . .   | 27        |
| 5.1.2 Double Spending . . . . .  | 27        |
| 5.1.3 Finality . . . . .   | 28        |
| 5.2 HashNet Consensus . . . . .  | 28        |
| 5.2.1 HashNet Overview . . . . .   | 28        |
| 5.2.2 Node Type . . . . .  | 30        |
| 5.2.3 Node Maintenance . . . . .   | 30        |
| 5.2.4 Sharding . . . . .   | 32        |
| 5.3 The Byzantine Agreement Consensus Based on Verifiable Random<br>Function . . . . . | 34        |
| 5.3.1 Consensus Status . . . . .   | 34        |
| 5.3.2 Selecting Full Nodes . . . . .   | 35        |
| 5.3.3 Byzantine Agreement . . . . .  | 35        |
| <b>6 Hash Algorithm and Signature Algorithm Against Quantum Attacks</b>                | <b>37</b> |

|           |  |           |
|-----------|--|-----------|
| 6.1       | Hash Algorithm Against Quantum Attacks . . . . .         | 37        |
| 6.2       | Signature Algorithm Against Quantum Attacks . . . . .    | 38        |
| <b>7</b>  | <b>Anonymous Transactions</b>                            | <b>41</b> |
| 7.1       | The One-Time Secret Key . . . . .                        | 41        |
| 7.2       | The Ring Signatures . . . . .                            | 41        |
| 7.3       | The Zero-Knowledge Proof . . . . .                       | 42        |
| 7.4       | The Confidential Transactions . . . . .                  | 42        |
| <b>8</b>  | <b>Smart Contract</b>                                    | <b>43</b> |
| 8.1       | Declarative Turing-incomplete Smart Contract . . . . .   | 44        |
| 8.2       | Advanced Turing-complete Smart Contract . . . . .        | 45        |
| 8.3       | Moses Virtual Machine (MVM) . . . . .                    | 46        |
| 8.4       | Smart Contract Accounts and Transactions . . . . .       | 47        |
| <b>9</b>  | <b>Applications and Scenes</b>                           | <b>49</b> |
| 9.1       | Applications . . . . .                                   | 49        |
| 9.1.1     | Distributed Social Network Applications . . . . .        | 49        |
| 9.1.2     | Divergent Contract Trading Applications . . . . .        | 49        |
| 9.1.3     | File Storage Grid Applications . . . . .                 | 50        |
| 9.2       | Scenes . . . . .   | 51        |
| 9.2.1     | Outline of Scenes . . . . .                              | 51        |
| 9.2.2     | Physical Asset Transaction Authentic Right . . . . .     | 51        |
| 9.2.3     | Decentralized Travel Service Platform . . . . .          | 52        |
| 9.2.4     | Asset Dividend Trading Block Chain . . . . .             | 55        |
| <b>10</b> | <b>Cross-chain Communication and Multi-chain Merging</b> | <b>57</b> |
| 10.1      | Introduction of Cross-chain Technology . . . . .         | 57        |
| 10.2      | Full-node Adapter Multi-chain Merging . . . . .          | 58        |
| 10.3      | Cross-chain Communication . . . . .                      | 60        |
| 10.4      | Cross-chain Asset Exchange . . . . .                     | 61        |
| 10.5      | Cross-chain Asset Transfer . . . . .                     | 62        |
| <b>11</b> | <b>Team and Planning</b>                                 | <b>63</b> |
| 11.1      | Foundation . . . . .                                     | 63        |
| 11.2      | Team Member . . . . .                                    | 64        |
| 11.3      | Project Consultant . . . . .                             | 68        |
| 11.4      | Consultant Institution . . . . .                         | 72        |
| 11.5      | Roadmap . . . . .  | 73        |
| <b>12</b> | <b>Token</b>   | <b>74</b> |
| 12.1      | Token Utility . . . . .                                  | 74        |
| 12.2      | Token Issuance . . . . .                                 | 75        |
| <b>13</b> | <b>Business Status Quo</b>                               | <b>79</b> |
| 13.1      | Technical Competition . . . . .                          | 79        |
| 13.2      | Company Competition . . . . .                            | 80        |

---

|                   |           |
|-------------------|-----------|
| <b>14 Risk</b>    | <b>82</b> |
| <b>References</b> | <b>85</b> |

# Abstract

Blockchain technology is considered to be the fifth most likely technology which will lead to disruptive revolution in productivity and production relations, following the steam engine, power, information technology and Internet. Since creation of Blockchain technology represented by Bitcoin in 2009, this technology has made great progress and received more and more attention. Especially in recent years, Blockchain technology has become global focus.

From core technologies to chain applications, comprehensive explorations have been carried out for Blockchain. However, as far as current Blockchain technology is concerned, there is a big gap between chain technology and various applications. Especially, there are many technical difficulties around Blockchain core technologies, which need breakthrough. At present, the infrastructure to support development of Blockchain applications is unstable, thus many applications are not effective. Therefore, it is urgent to make research and development on Blockchain infrastructure, thus providing reliable support for various Blockchain applications, as well as promoting implementation of Blockchain applications in all kinds of industries, which makes Blockchain serve human beings faster and better.

We propose a infrastructure for global value–internet, InterValue. It aims to solve the problems such as low applicability, transaction congestion, high commissions, long confirmation latency, weak resistance to quantum attacks, poor anonymity in communication and transaction, incapability in crossing and merging chains, large space for storage and etc. InterValue would optimize and improve Blockchain technology in all aspects including protocols and mechanisms, and become a genuine infrastructure of Blockchain 4.0. Also, InterValue would provide a platform for developing various DApps (distributed Apps), as well as feasible solutions to construct a global value–internet.

InterValue focuses on core technology of Blockchain infrastructure and platform. Our goal is to build an infrastructure conquering current key technical problems and supporting all domain applications in terms of ecological view. Main technological innovation of InterValue includes: **(1) Underlying P2P network**, combining the advantages of Tor–based anonymity and Blockchain–based distributed VPN, we design a novel anonymous P2P overlay network, including anonymous access method and encrypted communication protocol, which greatly enhances anonymity of nodes in the network and ensures that it's hard to trace node address and to crack communication protocol. **(2) Data structure**, a new data structure HashNet derived from DAG (directed acyclic graph) is proposed, which greatly reduces storage space required by nodes and improves efficiency and security of data storage. **(3) Consensus**, we design an efficient and secure double–layer consensus mechanism consisting of HashNet consensus and BA–VRF (Byzantine Agreement based on Verifiable Random Function) consensus, which supports high transaction concurrency, fast confirmation and building eco–systems for different

application scenarios. In version 1.0, due to the fact that HashNet consensus is much difficult to implement, we first implement a double-layer consensus mechanism combining DAG consensus with BA-VRF. **(4) Anti-quantum attack**, new anti-quantum algorithms are devised, which replaces existing SHA series algorithm with the Keccak-512 hash algorithm, and replaces ECDSA signature algorithm with an integer lattice-based NTRUsign signature algorithm. These algorithms reduce the threat coming from development of quantum computing and gradual popularization of quantum computer. **(5) Transaction anonymity**, based on anonymity characteristics of cryptocurrency such as Monero and ZCash, one-time key and ring signature are applied to transaction anonymity and privacy protection, which performs with high cost-effective ratio and excellent security. As a function of choice, zero-knowledge proofs are used to satisfy privacy requirements in different application scenarios. **(6) Smart contracts**, we design Moses virtual machine (MVM) which supports declarative non-Turing complete contract as well as advanced Turing complete contract programmed in Moses language. MVM is able to access off-Blockchain data conveniently and securely, and supports issuance of third-party assets, which can be integrated into applications in terms of public, permissioned (private) or consortium (hybrid) Blockchain. **(7) Crossing and merging chains**, we adopt chain-relaying technology to solve the problems in crossing chains transaction and transparent operations among multiple chains, which not only can maintain independence of crossing chains operation, but also reuses various functions of InterValue. **(8) Ecological motivation**, various token allocation methods are used, which support double-layer mining for incentives. **(9) Industrial application**, we design lots of industrial common interfaces in form of JSON-RPC, satisfying different scenarios such as circulation payment, data transmission, data search and contract invocation.

InterValue supports implementation for a variety of applications including anonymous communications, power sharing, storage sharing, bandwidth sharing, reputation sharing (credit guarantee), and it provides open interfaces for third-party DApp development. By connecting with various application scenarios, InterValue can cooperate with kinds of service providers and application providers to support commercial organizations or government agencies to build public, consortium or permissioned chain application systems according to business characteristics and requirements.

InterValue will reform existing operational mode in Internet. It introduced Token distribution mechanism for incentive to inspire community to maintain InterValue public chain and to develop DApps. InterValue will stimulate more value and network spreading effects on public chain, and turn economic incentive system into a self-renewing system, and create a completely decentralized ecosystem of value-internet and value transfer.

# 1

## Background

### 1.1. Blockchain Development Overview

Blockchain can be used as a peer-to-peer (P2P) decentralized system to store the pseudonymous transaction records in a trustless environment. Blockchain is the core technology of Bitcoin which was first proposed in 2008 and was implemented in 2009. Blockchain is essentially a distributed ledger, in which all committed transactions are stored in a chain. This chain continuously grows when the new transactions have been confirmed.

Blockchain is one of the most popular topics nowadays. First of all, it is a kind of social thought, which indicates the coming of a new era of transformation and change of human society. Kelly in the book "Out Of Control" describes: the natural, social, and technological evolution of biological logic is from the edge to the center then to the edge, from out of control to being controlled then to out of control. The technology base of Blockchain is distributed network architecture, because of the maturity of distributed network technology, it is possible to establish the business structure effectively by going to center, weak center, sub center and sharing, consensus and shared organization structure.

Today's Blockchain technology has undergone several iterations: **(1) Blockchain 1.0: Cryptocurrency.** In early 2009, the Bitcoin network was officially launched. As a virtual currency system, the total amount of bitcoin is defined by network consensus protocol. No individual or institution can freely modify the supply and transaction records therein. The underlying technology of Bitcoin, the Blockchain, is actually an extremely ingenious distributed shared ledger and peer-to-peer value transfer technology that has the potential to affect as much as the invention of double entry bookkeeping. **(2) Blockchain 2.0: Smart contracts.** Around 2014, industry community began to recognize the importance of Blockchain technology, and create a common technology platform to provide developers with BaaS (Blockchain as a service), which greatly improve the transaction speed, reduce resource consumption and support multiple consensus algorithms such as PoW, PoS and DPoS, as well as making DApp development easier. **(3) Blockchain 3.0: Blockchain technology application.** After 2015, with the rise of Blockchain 3.0 technology based on DAG data structures, such as Byteball and IOTA, Blockchain systems are more efficient, scalable, highly interoperable, and offer a better user



experience than before. Applications of Blockchain gradually extend to healthcare, IP copyright, education, and IOT. Broader applications such as sharing economy, communications, social management, charity, culture and entertainment.

**(4) Blockchain 4.0: Blockchain ecosystem.** Recently, Blockchain 4.0 technology based on Hashgraph data structure has gradually attracted attention of industry community. The consensus algorithm based on Hashgraph can achieve a qualitative growth in transaction throughput and scalability. The Blockchain will become the infrastructure of industry and form a consolidate ecosystem, which also changes people's lifestyle extensively and profoundly.

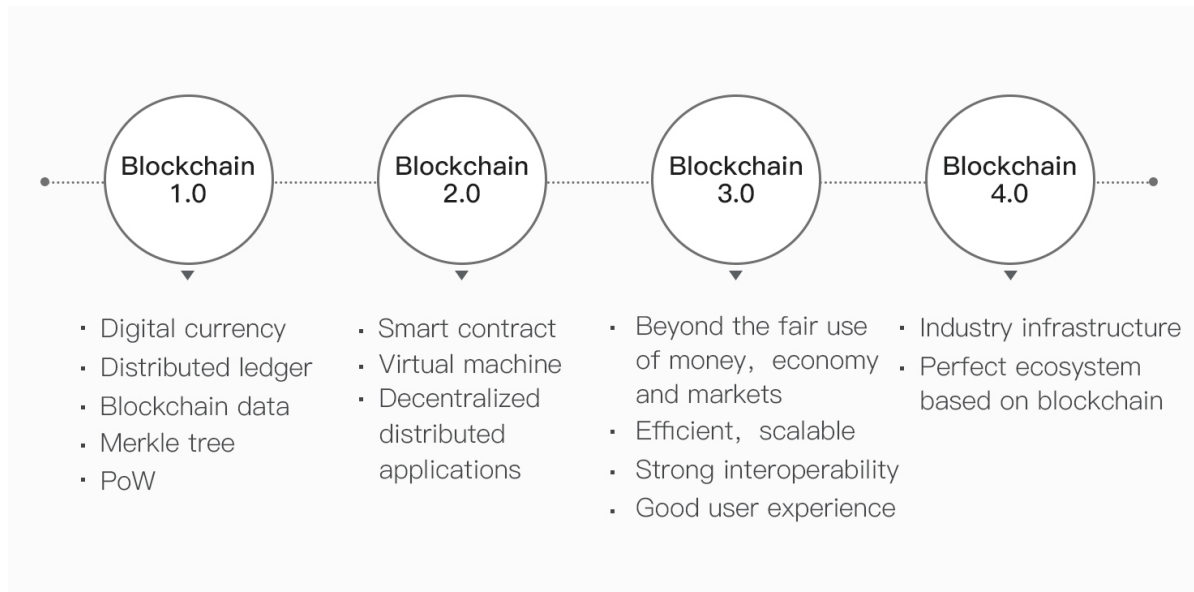


Figure 1-1: Blockchain Evolution Path

In recent two years, although some countries are conservative about use and development of cryptocurrencies, underlying technologies and applications of Blockchains are paid much attention by all of the world. With the deepening of recognition of Blockchain technology and application domain, people show great enthusiasm in development and implementation of Blockchain core technologies and chain applications.

The research and exploration on Blockchain technology mainly focus on three aspects: (1) Underlying technology and infrastructure layer: it mainly contains the basic protocol and related hardware. (2) General application and technology extension layer: it provides services, interfaces and related technical exports, including smart contract, quick calculation, mining service, information security, data service, BaaS, solution, traceable anti-counterfeiting and etc, for vertical industries. (3) Vertical industrial application layer: Blockchain is implemented in vertical areas such as finance, digital currency, entertainment, supply chain, healthcare, law, energy, public welfare, social, Internet of Things and agriculture. At present, people invest a great deal of enthusiasm in development and application of Blockchain technology. Among the teams engaged in Blockchain research and development, proportion of teams engaged in underlying technology research is about 20%, and proportion of teams using chains for application sce-

narios and vertical industries is 80%. Compared with application layer, underlying technologies can create token market value. In addition, it changes the traditional Internet-centric mode, i.e., data are centralized at application layer. Under Blockchain system, application layer becomes a complete service provider, it no longer owns user traffic and data value. These personal data are distributed to users, and underlying technologies is more valuable than application layer.

## 1.2. Key Technologies of Blockchain

**Underlying data structure.** Blockchain is originally a unique way of storing data in cryptocurrencies such as Bitcoin. It is a self-referential data structure for storing large amounts of transactions. Blocks are orderly linked up, and ultimately can not be tampered. And it is easy to trace transactions. The data structure of traditional Blockchain is a bottleneck hindering enhancing Blockchain concurrency. Technical geeks are constantly looking for a more efficient form of block linking. Directed Acyclic Graph (DAG) is a great solution, and we use “DAG chain” in the rest of white paper. In DAG, there is no process for packing blocks, but users confirm each other, which can greatly reduce transaction confirmation duration.

**Hash algorithm.** The hash algorithm is usually used to achieve information digest and its collision probability is very low. It can hide original information. The type of function arguments is string, the size of output is fixed, and the hash function is computationally efficient. Common hash algorithms include the MD5 and SHA series of algorithms. However, the GROVER algorithm in quantum computer can reduce the complexity of the attack hash algorithm from  $O(2^n)$  to  $O(2^{n/2})$ . Thus traditional hash algorithm is threatened by quantum attacks.

**Encryption signature algorithm.** The signature algorithm encrypts the information by using the private key to ensure the non-repudiation of the information. Current Blockchains mainly use ECDSA digital signature algorithm based on elliptic curves. It firstly generates the public-private key pair:  $(sk, pk) := \text{generateKeys}(\text{keysize})$ . The user keeps  $sk$  and  $pk$  can be shared to other people. Secondly, user can sign a specific message with  $sk$ :  $\text{Sig} := \text{sign}(sk, \text{message})$ . This yields signature  $\text{sig}$ . Finally, the party owning  $pk$  can verify the signature:  $\text{isValid} := \text{verify}(pk, \text{message}, \text{sig})$ . However, the SHOR algorithm under the quantum computer can reduce the complexity of ECDSA algorithm from  $O(2^n)$  to  $O(n^2(\log n)(\log \log n))$ , thus ECDSA cannot resist quantum attack.

**Anonymous protection.** In public chains, each participant can get a complete data backup, and all transaction data are open and transparent. However, this is a fatal flaw for many Blockchain applications. Not only some common users would like to protect account privacy and transaction information, also most organizations want to protect account information and trade secrets. Bitcoin achieves anonymity by blocking association between transaction address and the holder's true identity. However, such protection is weak and correlation between account and transaction can still be tracked by observing and tracking information of Blockchain through the address and IP information. To satisfy requirement of privacy protection in Blockchain, there are several solutions, such as ring signature, homomorphic encryption and zero-knowledge proof.

**P2P communication.** The Blockchain system uses P2P network technology to

connect peers. Different from centralized network mode, each node in the P2P network has equal status, each node has the same network authority, and there is no centralized server. However, because there is no centralized server, node's information can be easily leaked.

**Consensus mechanism.** There are several major consensus mechanisms: PoW, PoS, DPoS, PBFT. PoW (Proof of work) is a consensus strategy used in Bitcoin network. It requires a complicated computational process in authentication. In PoW, each node in network is calculating a hash value of the constantly changing block header. POW is completely decentralized, free to access, but mining causes a lot of waste resources, so consensus needs a long period, which is not suitable for commercial applications. PoS (Proof of stake) is an energy-saving alternative to PoW. Instead of demanding users to find a nonce in an unlimited space, PoS requires users to prove the ownership of the amount of currency because it is believed that users with more currency would be less likely to attack the network, and PoS still needs mining. DPoS (Delegated proof of stake). Similar to PoS, miners get their priority to generate the blocks according to their stake. The major difference between PoS and DPoS is that PoS is a direct democratic while DPoS is representative democratic. And the whole consensus mechanism still depends on tokens, while many commercial applications do not need tokens. PBFT (Practical Byzantine Fault Tolerance) is a replication algorithm to tolerate Byzantine faults. Hyperledger utilizes the PBFT as its consensus algorithm since PBFT could handle up to 1/3 malicious byzantine replicas/nodes. PBFT needs to know the identity of each node to select an accountant for each block, and nodes cannot join or exit arbitrarily, so PBFT is always used in private or permissioned Blockchains. It's high efficiency, but nodes need to fully trust each other.

**Incentive mechanism.** In order to ensure normal operation of Blockchain system, a large number of honest nodes need to remain online. The incentive mechanism is used to reward the users who contribute more to the system. And it should make benefits of honest users outweigh that of malicious users.

**Smart contracts.** Smart contracts were first proposed in 1994 by the cryptographic scientist Nick Szabo. When a predefined condition is satisfied, the smart contracts perform the corresponding contract terms. Ethereum provides a Turing complete contract programming language, but development and deployment of smart contracts is tedious and vulnerable. Smart contract of Byteball is easy to deploy, but it is non-Turing complete, and not scalable for contract applications.

### 1.3. Current Problems of Blockchains

Currently, various Blockchains such as EOS, NEO, ArcBlock and other projects emerge continuously, but most of them are based on Ethereum. They are far from criteria of Blockchain 4.0. Most of project teams which implement Blockchain with application scenario are limited by performance, applicability and stability of underlying chain. And they are currently at an early stage. Although it is estimated that many industry applications may rise in 2018, with the underlying agreements are constantly changing, more than 98% of the projects will be eliminated by history. The current Blockchain technology mainly has the following problems.

**Poor performance.** Performance is one of main challenges for current Blockch-

ain technology. Bitcoin is designed to handle only seven transactions per second, and Ethereum can only handle a few more. As of December of 2017, a simple CryptoKitties application can slow down Ethereum and increase transaction fees dramatically. Today's consumer applications must be able to handle tens of millions of active users daily. In addition, some applications will only become valuable when certain throughput is reached. The platform itself must be able to handle a large number of concurrent users. A fine experience demands reliable feedback within only second-class delays. Long latency frustrates users and make applications built on Blockchains less competitive with existing non-Blockchain alternatives.

**Difficult to use.** Today's Blockchain applications are built for the few tech whizzes who know how to use them, rather than common users. Nearly all Blockchain applications require users to either run a Blockchain node or install a "light node". It takes a long time for users to adapt to application. For example, while the Ethereum-based game CryptoKitties is probably the most user-friendly decentralized App ever built, it still requires users to install the Metamask light wallet browser extension. Users also need to know how to buy Ethers securely and use them with Metamask. To attract large numbers of people, Blockchain applications need to be as simple as today's Internet and mobile apps. Blockchain technology should be completely transparent to the consumer.

**High cost.** The extremely high cost of using Blockchain technology is a major barrier to adoption. It also limits developers who need the flexibility to build free services. Just like today's Internet and mobile Apps, there is no need to pay every operation during Blockchain transaction. Similar to the Internet, Blockchain technology should be able to support free applications. Making Blockchain free to use is key to its widespread adoption. A free platform will also empower developers and businesses to create valuable new services they can monetize, rather than having users pay fees to use the Blockchain network.

**Platform lock-in.** Same as the early days of any computing technology, Blockchains have critical "platform lock-in" problems. Developers have to decide which Blockchain to develop, then implement platform-specific code, which makes it very difficult to switch an application to another Blockchain. Developers don't want to be locked into working with a certain Blockchain technology. They need freedom to evaluate, use, and switch between options. Some applications may even need to run on multiple platforms to provide best user experience.

**Low applicability.** People have high expectations for Blockchain, kinds of media paint a bright future for decentralized applications for the public, especially with the increasingly high prices of cryptocurrencies. In reality, however, Blockchain technology is still in its infant stage. Most Blockchain services lack rich features and don't have a mechanism to encourage the community to contribute to the feature stacks.

Therefore, there is an urgent need to study the underlying mechanism of Blockchain, and redesign or improve the various key technologies of Blockchain to solve the problems such as transaction congestion, high transaction fees, long confirmation latency, weak anti-quantum attack capability, low anonymity of communication and transaction, weak crossing and merging chain capability, large storage

space and etc. We aim to implement a real practical support mechanism for all levels of value transfer network, provide the infrastructure for all kinds of value transfer applications, and a underlying development platform for all kinds of DApps and practical and feasible solutions for constructing the global value transfer and value internet.

# 2

## Motivation

### 2.1. Name

InterValue.

INVE: InterValue Token.

### 2.2. Vision

It is well known that Internet enables the free dissemination and sharing of some information, whereas Blockchain makes possible movement and exchange of whole information and real assets of human beings freely, which derives the Internet of Value. The significance of Internet and Blockchain is to map the real society to virtual society, means that information mapping is realized in Internet and value mapping is realized in Blockchain. InterValue has a set of technical and fuctional features for value mapping, which will be built to be an practical infrastructure of the Internet of Value.

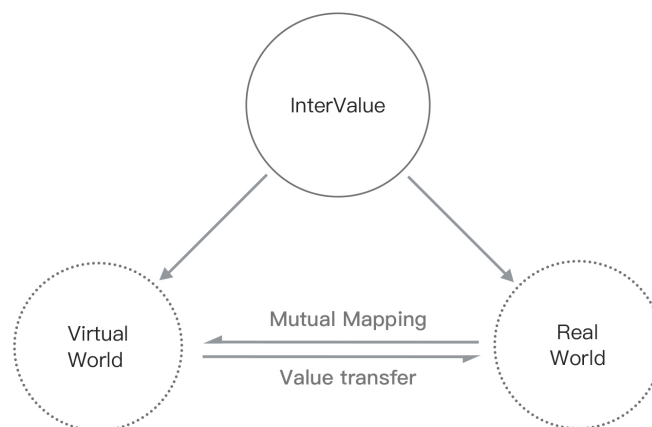


Figure 2–1: Mapping of Real World and Virtual World

Imagine a world within InterValue that all behaviors and activities of people involving pay, evaluation, retain, determine the legitimacy will be operated automatically. People can store their whole life's activities in digital media. In the

digital world, a virtual person can be built who has complete consciousness and completely autonomous intelligence, as the evolution of artificial intelligence. After the value of all kinds of assets be mapped to the chain, the virtual person will live in the virtual human society individually. It is a new world borned.

## 2.3. Goal

Our goal is to build InterValue to be an infrastructure of Blockchain 4.0 with features such as DAG enhanced, full functions supported, high-performance, easy to use, friendly user experience, scalability. And then we will produce the ecosystem of Blockchain 4.0 applications based on InterValue.

Key technologies in platform and features in Blockchain infrastructure are the topmost focus for InterValue. The features include the anonymous P2P protocols, a novel anti-quantum hash algorithm and a novel signature algorithm, a unique double-layer consensus and mining mechanism for transactional anonymous protection, a Turing complete smart contracts, etc. It uses fair distribution mechanism to support third-party asset distribution, cross-chain communications, multi-chain merging functions such as public chain, permissioned chain, consortium chain and other forms fall into the practical application of the Blockchain 4.0 infrastructure.

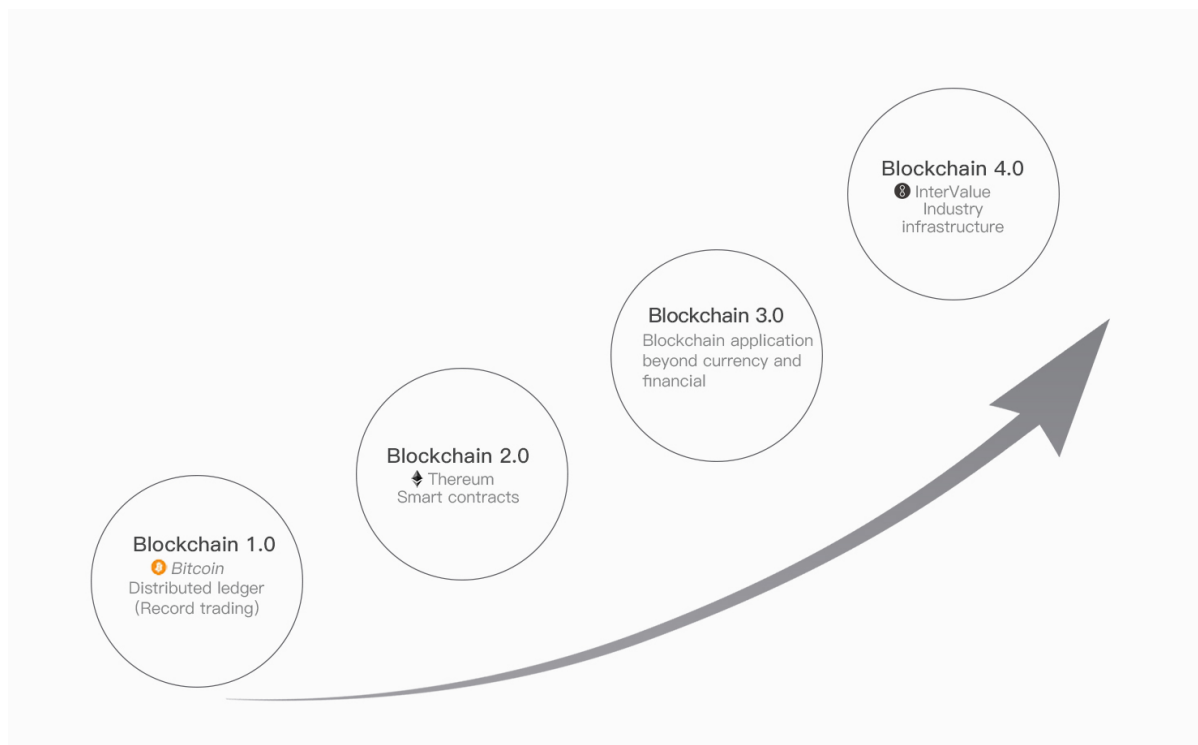


Figure 2-2: The Roadmap of Blockchain 4.0

## 2.4. Ecological System

InterValue takes advantage of the chains in Blockchain 1.0, 2.0 and 3.0, addresses their outstanding issues, break some key technologies, and can support more prosperous application ecosystem. As is shown in Figure 2-3, InterValue innovatively



designs the chain-down data mapping mechanism and a new enhanced data structure based on directed acyclic graph (DAG) and hash graph (HashNet), HashNet based consensus and BA-VRF based consensus mechanism, an advanced Turing complete intelligent contract with external triggers, Keccak512 and NTRDSign Based anti-quantum cryptanalysis algorithm, ring signature and zero-knowledge proof transaction anonymous protection mechanism. It has the functional characteristics of Blockchain 4.0 such as fast transaction confirmation, anti-quantum attack, anonymous node communication, anonymous protection of transaction, advanced smart contract, data link and so on. It also supports fair distribution mechanism to support third-party asset distribution and cross-link communication, Multi-chain Fusion and other functions.

Our vision for InterValue is to build the Internet of Value globally to provide the foundation network for Blockchain which supports a wide range of applications in the form of public Blockchain, permissioned Blockchain and private Blockchains. For a specific application, the data is operated by Hash and the value is stored on InterValue chain. All applications, such as the digital currency represented by Bitcoin in the context of Blockchain 1.0, the financial services combined of digital currency and smart contracts under the background of Blockchain 2.0 and 3.0, can be built based on InterValue. As a public chain of Blockchain 4.0, InterValue also supports more extensive applications, such as healthcare, IP copyright, education, Internet of Things, sharing economy, communication, social management, charity, cultural entertainment and so on.



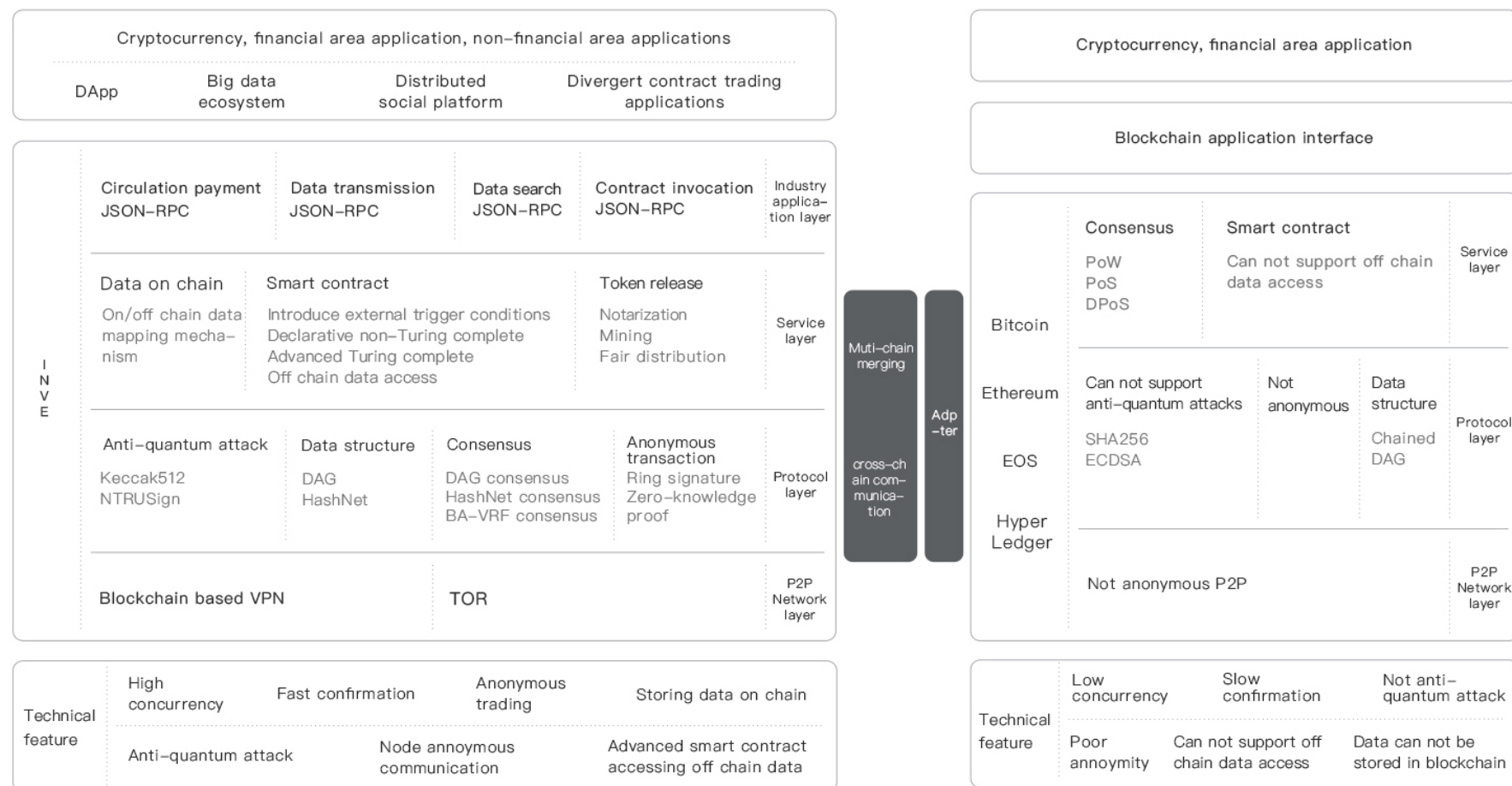


Figure 2-3: The Ecosystem Diagram of InterValue

InterValue will completely reshape the existing Internet operating model and transform the economic incentive system itself into a system that can circulate within the system to create a completely decentralized Internet value transmission ecosystem as well as a completely open community ecosystem that transcends National boundaries, so that each participant can get the corresponding value embodied.

## 2.5. Key Features

InterValue has made significant improvements in all aspects of the Blockchain infrastructure, with breakthrough innovations at some levels. Main technological innovation of InterValue includes: **(1) Underlying P2P network**, combining the advantages of Tor-based anonymity and Blockchain-based distributed VPN, we design a novel anonymous P2P overlay network, including anonymous access method and encrypted communication protocol, which greatly enhances anonymity of nodes in the network and ensures that it's hard to trace node address and to crack communication protocol. **(2) Data structure**, a new data structure Hash-Net derived from DAG (directed acyclic graph) is proposed, which greatly reduces storage space required by nodes and improves efficiency and security of data storage. **(3) Consensus**, we design an efficient and secure double-layer consensus mechanism consisting of HashNet consensus and BA-VRF (Byzantine Agreement based on Verifiable Random Function) consensus, which supports high transaction concurrency, fast confirmation and building eco-systems for different application scenarios. In version 1.0, due to the fact that HashNet consensus is much difficult to implement, we first implement a double-layer consensus mechanism combining DAG consensus with BA-VRF. **(4) Anti-quantum attack**, new anti-quantum algorithms are devised, which replaces existing SHA series algorithm with the Keccak-512 hash algorithm, and replaces ECDSA signature algorithm with an integer lattice-based NTRUsign signature algorithm. These algorithms reduce the threat coming from development of quantum computing and gradual popularization of quantum computer. **(5) Transaction anonymity**, based on anonymity characteristics of cryptocurrency such as Monero and ZCash, one-time key, ring signature, zero-knowledge proof are applied to transaction anonymity and privacy protection, which performs with high cost-effective ratio and excellent security to satisfy privacy requirements in different application scenarios. **(6) Smart contracts**, we design Moses virtual machine (MVM) which supports declarative non-Turing complete contract as well as advanced Turing complete contract programmed in Moses language. MVM is able to access off-Blockchain data conveniently and securely, and supports issuance of third-party assets, which can be integrated into applications in terms of public, permissioned (private) or consortium (hybrid) Blockchain. **(7) Crossing and merging chains**, we adopt chain-relaying technology to solve the problems in crossing chains transaction and transparent operations among multiple chains, which not only can maintain independence of crossing chains operation, but also reuses various functions of InterValue. **(8) Ecological motivation**, various token allocation methods are used, which support double-layer mining for incentives. **(9) Industrial application**, we design lots of industrial common interfaces in form of JSON-RPC, satisfying different scenarios such as circulation

payment, data transmission, data search and contract invocation.

The key features of InterValue are shown in Figure 2–4.

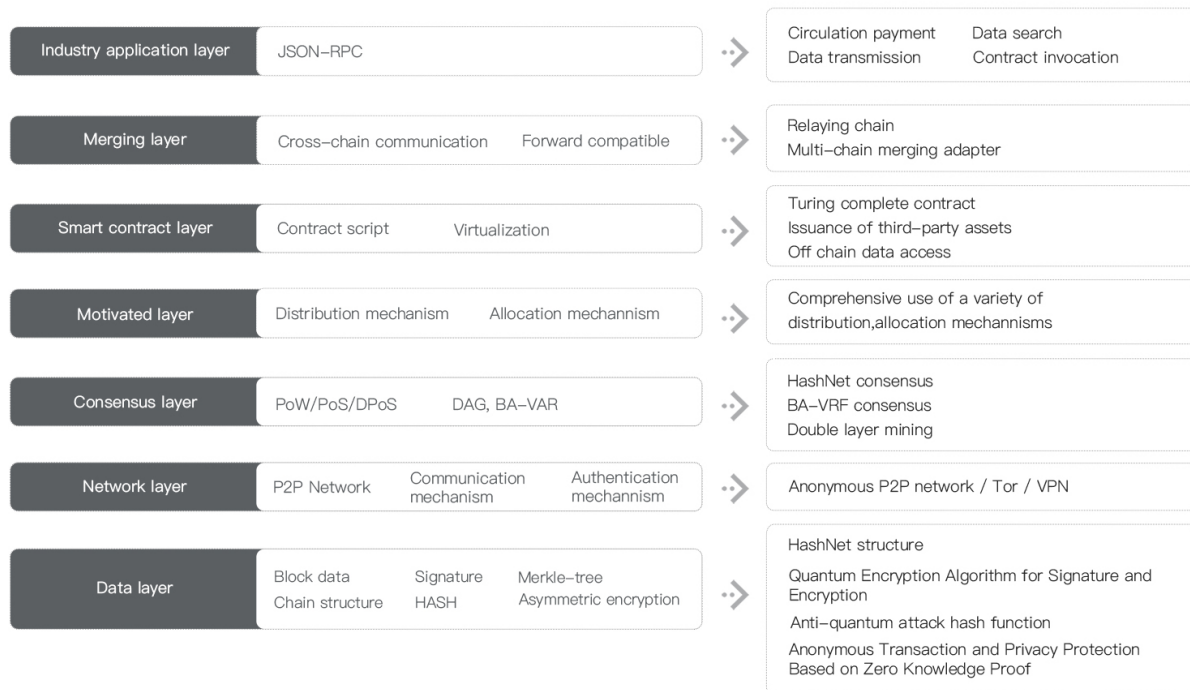


Figure 2–4: The Key Features of InterValue

Key features of InterValue are summarized:

- New data structure of DAG based on HashNet with small storage space requirement
- Multiple Consensus Mechanisms: HashNet, BA-VRF, and DAG Consensus
- Fully distributed anonymous P2P network communication
- Hash Algorithm and Signature Algorithm Against Quantum Attacks
- Transaction Anonymity and Privacy Protection Based on Zero Knowledge Proof and Ring Signature
- Support Turing complete advanced declarative smart contract
- Support high concurrent transactions, short transaction confirmation time

## 2.6. Advantages

The InterValue project incorporates the benefits of the existing Blockchain 3.0 project by highlighting the benefits of IOTA and Byteball. It designs and implements a new consensus mechanism based on improved HashNet by solving this problem of existing Blockchain infrastructure by adopting an innovative two-Layer consensus mechanism, designing and using a cryptographic algorithm with anti-quantum

attack characteristics, and build a more prosperous application ecosystem. Table 2–1 compares InterValue with the existing DAG program in the aspects of tokens, market capitalization, consensus mechanism, smart contracts, P2P networks, quantum security, privacy protection, reward mechanism, transaction speed, node classification and so on.

Table 2–1: Comparison with other DAG–Based Blockchain

|                       | IOTA                     | ByteBall                               | Hedera Hashgraph          | InterValue   |
|-----------------------|--------------------------|--|---------------------------|--|
| Token                 | IOTA                     | Byte                                   | Hashgraph                 | INVE   |
| Market capitalization | 14 billion               | 0.4 billion                            | -                         | -  |
| Consensus mechanism   | MCMC                     | 12 notaries                            | Hashgraph                 | Double consensus   |
| Smart contract        | Nonsupport               | Declarative contract                   | Turing complete contract  | Declarative contract and Turing complete contract                |
| P2P network           | No Anonymity             | No Anonymity                           | No Anonymity              | Anonymity  |
| Quantum security      | Partial resistance       | No                                     | No                        | Yes  |
| Privacy protection    | No                       | Yes                                    | No                        | Zero Knowledge Proof of Privacy Protection                       |
| Incentive mechanism   | No                       | Transaction citations and notarization | Transaction proxy service | Transaction reference, notary, mining                            |
| Transaction speed     | 1000 TPS                 | 100 TPS                                | -                         | >100000 TPS  |
| Node classification   | Full node and light node | Full node and light node               | Full node and light node  | Confirm node, Full node, Local full node, Light node, Micro node |

From InterValue current progress and follow-up development plan, InterValue mainly has the following advantages.

- Positioning as a practical Blockchain 4.0 infrastructure with advanced technical features is truly supported by the massive adoption of Blockchain 3.0 infrastructure.
- The InterValue team has reasonable matching and division of labor, strong technological research and development capabilities, strong market promotion ability and strong landing capability. It ensures that INVE can achieve various characteristics of design successfully.

- The application of chain based on InterValue is advancing rapidly. At present, InterValue based distributed social platform and InterValue based global distributed storage grid are currently being planned and developed. In addition, the team is still planning a killer chain application with a large user base.
- As a technology provider, InterValue team has been working with many companies that use blockchain technology to optimize and enhance the existing business processes. The InterValue infrastructure has been applied to many practical applications and scenarios, and is being developed and implemented.
- The InterValue team is actively building a coalition of partners to strive to apply InterValue to as many industry and physical scenarios as possible.
- The InterValue team is actively building a community of developers to ensure that more technical people are technically involved in the optimization of InterValue's infrastructure itself and in the development of DApps based on InterValue.
- InterValue team is actively building Blockchain technologies to popularize communities and promote popularization of Blockchain technology.

## P2P-based Anonymous Communication

The underlying network of InterValue adopts a P2P overlay architecture, which anonymity mechanism is built upon to ensure privacy preservation.

P2P is short for Peer-to-Peer, and is a kind of overlay network. IBM gives the following definition for P2P: "A P2P system consists of a number of interconnected computers and has at least one of the following characteristics: The system relies on the active cooperation of non-central server devices, and each member directly benefits from the participation of other members rather than from the server. Each member is not only a client, but also a server. Users are aware of existence of each other, and form a virtual or actual group."

In P2P system, each peer is an equal participant and assumes the role of consumer and provider. Ownership and control of resources are spread across the network. P2P makes communication easy, straightforward, and reduces reliance on servers to a minimum level. P2P technology has changed location of "content", making it from the "center" to "edge". This means it has changed the state of the Internet, which now centers around a centralized website. Resources are not stored on servers but stored on all users' PCs. P2P technology makes users' PCs no longer passive clients, but become server and client combined devices. Therefore, InterValue is featured by decentralization.

The anonymity mechanism for InterValue embedding in the P2P network is implemented by the following:

(1) InterValue runs a proxy server locally, periodically communicating with others to maintain a TLS link, which forms a virtual link in network. Specifically, each user runs its own proxy: getting directory, building link, and handling connection. These proxies accept the TCP data stream and reuse them on the same line.

(2) InterValue encrypts data in application layer, i.e., the transport between each relay node is encrypted using point-to-point key. The encryption encloses all user's packet between each pair of communication nodes, which ensures communication safety between the relay nodes. Specifically, each InterValue relay node maintains a long-term key and a short-term key. The long-term key verifies the key to sign a TLS certificate, signs the relay node descriptor, and signs the directory used by a directory server. The short-term key is used to decode the request sent by user, and then to establish a link while negotiating a temporary key. The

TLS protocol also uses short-term keys between the communicating relay nodes for periodically and independently change the impact of key leakage.

(3) Instead of taking a direct route from source to destination, data packets on the InterValue network take a random pathway through several relays that cover user's tracks so no observer at any single point can tell where the data came from or where it's going. To create a private network pathway, the user's client incrementally builds a circuit of encrypted connections through relays on the network. The circuit is extended one hop at a time, and each relay along the way knows only which relay gave it data and which relay it is giving data to. No individual relay ever knows the complete path that a data packet has taken. The client negotiates a separate set of encryption keys for each hop along the circuit to ensure that each hop can't trace these connections as they pass through.

The principle of anonymity communication for InterValue is shown in Fig. 3-1. Directory server is core of the network, which is responsible for collecting relay node information and distributing it to proxy in terms of snapshot and description. The relay nodes forms infrastructure of InterValue network, which collaboratively forward encrypted packets through anonymous links among multiple relay nodes. The proxy runs on the InterValue client, which is responsible for establishing anonymous links and relaying network traffic between the user's application and anonymous link. In Fig. 3-1, an anonymity link is formed by three relay nodes, which are labelled as entry, middle, and exit.

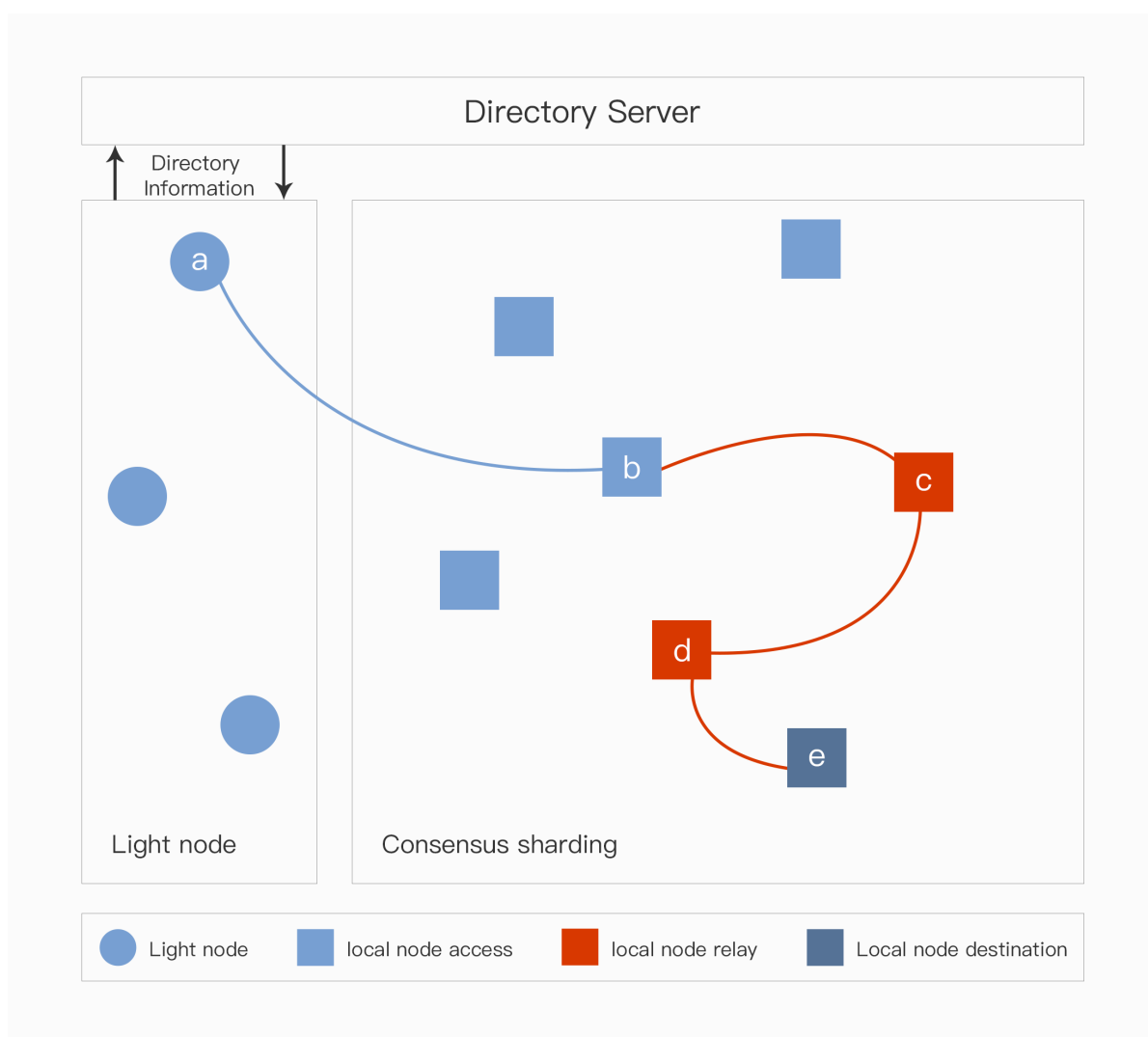


Figure 3–1: Principle of Anonymity Communication for InterValue



# 4

## Data Structure

### 4.1. Data Structure of the Basic DAG

InterValue uses the basic DAG data structure to store transaction data in its first development phase. The basic DAG data structure has been adopted in several projects (e.g. IOTA and Byteball) to support the long-term stable operation of public blockchains, which proves the advance and performance of DAG chain technology. In InterValue, transaction messages are encapsulated into units (Units), and a DAG graph is constructed by linking these units. A unit must confirm the units before linking them. Therefore, the cost of computing and time for consensus is reducing. It is blockless, and there is no data synchronization. As a result, it tremendously increases the transaction throughput and minimizes the confirmation time.

The DAG data structure of InterValue is shown in Figure 4-1. The directed edges between units indicate the reference relationship between them. There is a directed edge from unit B to A, indicating that unit B refers to A (or B confirms A), and A is a parent of B, B is a child of A. At the same time, we call unit C indirectly refers to A, A is C's ancestor unit. Unit G does not have any parent, and it is called the Genesis unit and it is unique. Units X and Y do not have any children, and such units are called top units.

The unit consists of two parts: the unit header and the unit message. The unit header mainly contains the following fields:

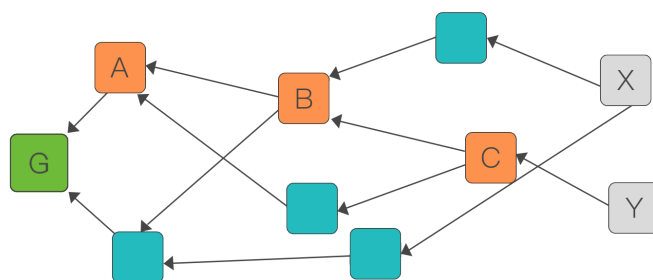


Figure 4-1: The DAG of InterValue

- Unit version;
- Token version;
- Unit creators' signature: single signature or multiple signatures;
- Parent units' hash: the hash of the referenced single or multiple parent-units;
- Witnesses list: Hash of another unit (usually its parent or ancestor) which has the same witnesses.

The unit message is used to store transaction information, InterValue has multiple types of transactions, including payment, data storage, voting, etc. The detailed description of the data structure is shown in Table 4-1.

Table 4-1: Detailed Description of the DAG Data Structure

|                   |  |
|-------------------|--|
| version           | The protocol version.  |
| alt               | An identifier of alternative currency.   |
| message           | <p>An array of one or more messages that contain actual data.</p> <ul style="list-style-type: none"> <li>• app: the type of message, e.g. 'payment' for payments, 'text' for arbitrary text messages, etc.</li> <li>• payload_location: where to find the message payload. It can be 'inline' if the payload is included in the message, 'uri' if the payload is available at an Internet address, 'none' if the payload is not published at all.</li> <li>• payload_hash: hash of the payload in base64 encoding</li> <li>• payload: the actual payload (since it is 'inline' in this example) .<br/>The payload structure is app-specific. <ul style="list-style-type: none"> <li>— inputs: an array of input coins consumed by the payment. All owners of the input tokens must be among the signers (authors) of the unit. <ul style="list-style-type: none"> <li>◊ unit: hash of the unit where the coin was produced. To be spendable, the unit must be included in last_ball_unit.</li> <li>◊ message_index: an index into the messages array of the input unit. It indicates the message where the token was produced.</li> <li>◊ output_index: an index into the outputs array of the message_index'th message of the input unit. It indicates the output where the token was produced.</li> </ul> </li> <li>— outputs: an array of outputs that indicates who receives the tokens. <ul style="list-style-type: none"> <li>◊ address: the address of the receiver.</li> <li>◊ amount: the amount the tokens.</li> </ul> </li> </ul> </li> </ul> |
| authors           | An array of the authors who created and signed this unit.  |
| parent_units      | An array of hashes of parent units.  |
| witness_list_unit | Hash of the unit where one can find the witness list.  |

Similar to the blockchain that each new block needs confirm all the previous ones, each new unit in the DAG needs to confirm its parents and ancestors. If you try to modify a unit in the DAG, you need to coordinate with a large and growing number of other users, most of whom are anonymous strangers. Therefore, the irreversibility in DAG is based on the complexities of coordinating with such a large number of strangers. These people have difficulty reaching an agreement, and anyone can break the cooperation unilaterally. After the unit is issued, the confirmation process immediately starts. A new unit that is issued by anyone can confirm it. Users help each other by issuing a new unit and referring it to other units.

## 4.2. HashNet-a New DAG Data Structure

As shown in Figure 4–2, HashNet is a directed acyclic graph (DAG) consisting of an infinite number of vertices and directed edges.

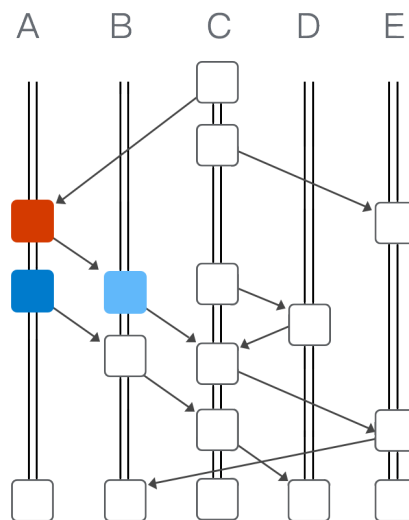


Figure 4–2: HashNet Data Structure

This figure records the communication history of the nodes in the entire network, including who sends information to whom in what order and time. Every node has such a copy of HashNet in memory. There are five nodes A, B, C, D, and E in the figure above. Each node has a column with some vertexes (also called events). The most recent vertex will be placed at the top of the column, so HashNet grows upwards with time.

- HashNet Features

1. Vertex. Also called event, including: construction timestamps, 0 or more transactions, signature of created, and hash value of self-parent & other-parent.
2. Edge. HashNet has 2 kinds of edge, vertical edge and bevel edge.

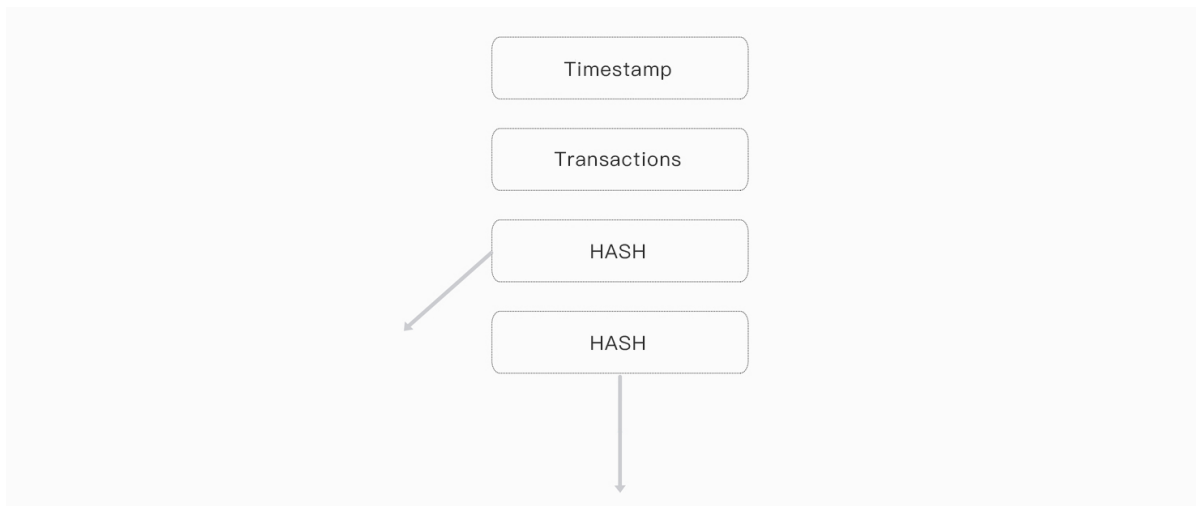


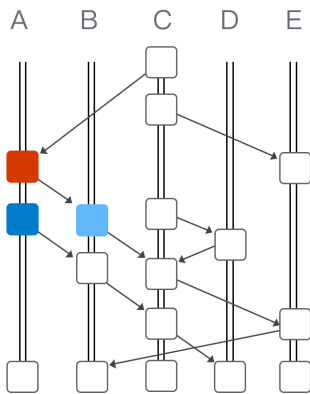
Figure 4–3: HashNet Vertex Inside

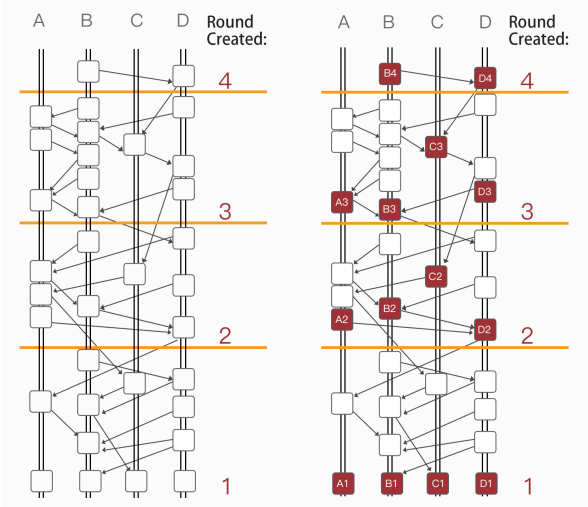
- The bevel edge connecting 2 vertexes, a source vertex and a destination vertex, represents a sync, where one node A sends a sync to another B. The data sent by A is the whole tree where the root is the source vertex.
  - The vertical edge looks like a chain, where events are placed in the order in which they were created. Events on the same vertical edge are created by the same node.
3. Every node has such a HashNet in memory. One vertex has only 2 downwards edges: one vertical edge another is bevel edge. The red event discovers a fact that B used to send a sync to A (light blue event is the source vertex)
  4. Each vertex has one or more upward bevel edges which mean syncs are sent from the itself. For example, there is one upward bevel edge from A (source vertex is the red event) to C. It means the data A sends to C is all the events on a tree where the root is the red event.
  5. A and C will negotiate before sending the whole tree. In fact, A only sends the part that C does not have of the tree to minimize network overhead.
  6. With more and more nodes sending syncs to each other, all the events happened will saturate the HashNet on each node. Occasionally, the top of HashNet on each node may have a little bit difference, it will soon be eliminated by new coming syncs.
  7. If the HashNets on node A and B both contain the event x, then the 2 HashNets contain all the ancestors of x. A and B will run Byzantine agreement algorithm locally to reach the consensus on the event x and all its ancestors.
  8. Every node sends the whole event tree (actually only sends part of the tree that the receiver does not have for optimization) he has to other nodes. The part of HashNet that a node does not have will soon be feed by lots of syncs on the network.

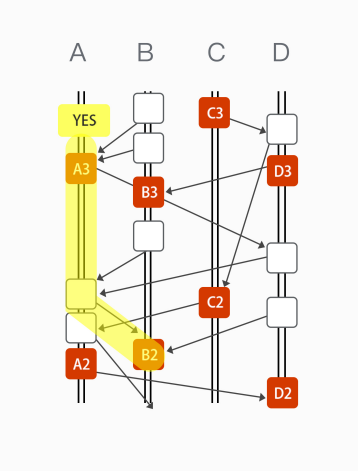
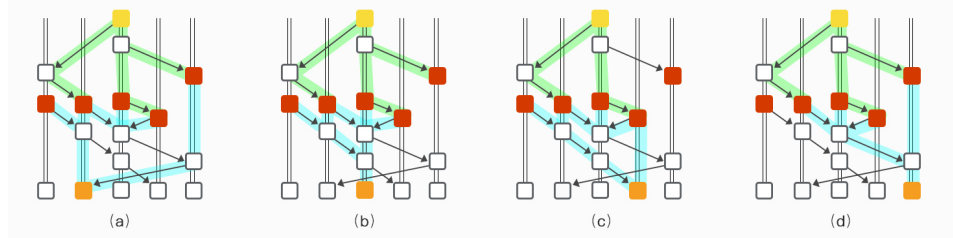
9. Because of #6, #7, #8, we can assume the HashNets on every node are almost the same.

- HashNet terminologies

Table 4-2: HashNet terminologies

| Terminology               | Description   |
|---------------------------|---|
| Transactions              | Any node can create a signed transaction at any time. All nodes get a copy of it, and the community reaches a Byzantine agreement on the order of those transactions  |
| Event (vertex of HashNet) | HashNet contains many events, which are containers of 0 or more transactions. An event can be regarded as a block in Bitcoin.   |
| Sync (edge of HashNet)    | Upward bevel edge. Representing a network communication from one node to another.   |
| HashNet                   | <p>HashNet is a kind of a directed acyclic graph (DAG) , consisted of many vertexes and edges. The graph displays the history of the nodes' communication. In DAG below, there are 5 nodes: A,B,C,D,E (Alice, Bob, Carol, Dave, Ed) . The most recent event that happened will be put on the top of graph, so the HashNet grows upwards with time.</p>  |
| World state (ws)          | The world state means a whole ledger. The world state in Bitcoin is a chain, however it is a HashNet (a kind of DAG) in InterValue  |
| Self-parent event         | The first event reached by the downward vertical edge is the self-parent event( the dark blue event is the self-parent of the red event).   |
| Self-ancestors event      | The Self-parent event and its Self-parent of the dark blue event are all Self-ancestor events of the red event  |

|                             |  |
|-----------------------------|--|
| Round created & Round index |  <p>In HashNet, all events are scoped into round by time.<br/> A child never has a round index before its parents. So as time goes by, the round index can only stay the same or increase.<br/> The round has an index started from 1.<br/> In round <math>r</math>, once there is an event that can strongly see more than supermajority witnesses, the event round index is <math>r+1</math></p>   |
| Witness                     | The first event that each node creates in each round is the witness. Each round has $n$ witnesses ( $n$ is the number of nodes).   |
| Famous witness              | The community could put a list of $n$ transactions into order by running separate Byzantine agreement protocols on $O(n \log n)$ different yes/no questions of the form “did event $x$ come before event $y$ ?” A much faster approach is to pick just a few events (vertices in the HashNet), to be called witnesses, and define a witness to be famous if the HashNet shows that most members received it fairly soon after it was created. Then it’s sufficient to run the Byzantine agreement protocol only for witnesses, deciding for each witness the single question “is this witness famous?” Once Byzantine agreement is reached on the exact set of famous witnesses, it is easy to derive from the HashNet a fair total order for all events |
| Election                    | The process for a decision on a node of whether a witness is famous  |
| Vote                        | In an election process, if witness A in round $r+1$ can see witness B in round $r$ , A will vote for B   |
| Round received              | Event $x$ has a received round of $r$ if that is the first round in which all the unique famous witnesses were descendants of it, and the fame of every witness is decided for rounds less than or equal to $r$ .  |
| Received time               | Suppose event $x$ has a received round of $r$ , and Alice created a unique famous witness $y$ in round $r$ . The algorithm finds $z$ , the earliest self-ancestors of $y$ that had learned of $x$ . Let $t$ be the timestamp that Alice put inside $z$ when she created $z$ . Then $t$ can be considered the time at which Alice claims to have first learned of $x$ . The received time for $x$ is the median of all such timestamps, for all the creators of the unique famous witnesses in round $r$ .  |

|                     |  |
|---------------------|--|
| Other-parent event  | The first event reached by the downward bevel edge of the red event is the Other-parent event of the red event   |
| Gossip              | Each node sends all the information it knows to another randomly selected node. Then the node that received the message continues to do the same thing.  |
| Gossip about gossip | The HashNet is spread through the gossip protocol. The information being gossiped is the history of the gossip itself, so it is “gossip about gossip”.   |
| Virtual voting      | Each node has a HashNet copy, so relying on traditional Byzantine protocols, Alice can figure out what votes Bob should send to her. So Bob doesn't need to send a real vote on the network. Each node has the same data (HashNet), then the same result can be calculated using the same algorithm (BFT) without network communication. Therefore, the network bandwidth consumption for the HashNet consensus algorithm is very low.   |
| Supermajority       | If $m > 2n/3$ ( $n$ is the number of node in network), $m$ is the Supermajority  |
| See                 | <p>If event <math>x</math> is able to directly or indirectly reach event <math>y</math> by a downward path:</p> <ul style="list-style-type: none"> <li>• <math>x</math> can see <math>y</math></li> <li>• <math>y</math> is other-ancestors of <math>x</math></li> <li>• <math>x</math> is descendent of <math>y</math></li> </ul>  <p>A3 is <math>x</math>, B2 is <math>y</math> in above graph</p> |
| Strongly seeing     | <p>If <math>x</math> can see <math>y</math> by more than supermajority downward paths, we can say <math>x</math> strongly sees <math>y</math>:</p>  <p>In graph (d), the top yellow event <math>w</math> can strongly see the orange event <math>x</math>, as <math>w</math> can reach <math>x</math> by 4 downward paths and each of them crosses a different red event.</p>                        |

# 5

## Consensus

In the v1.0, InterValue uses a two-layer consensus mechanism that combines the basic DAG consensus with the BA-VRF consensus. From v2.0, the basic DAG consensus of InterValue will be replaced by HashNet. Thus, the consensus mechanism of InterValue will be the combination of HashNet and the BA-VRF.

### 5.1. DAG Consensus

#### 5.1.1. The Main Chain

The main chain is a single chain built along the child-parent link, and it connects all units. The main chain is able to be built from any unit. If we select two main chains from two different units with the same rule, both main chains will completely coincide after they intersect with each other. The coincident part is called the stable main chain. In the worst case, they intersect in the Genesis unit. All units are either in this stable main chain or reachable in a number of steps from an unit of the stable main chain. Thus, the stable main chain is able to establish a total order between two conflicting unordered units. Firstly, index the units directly on the stable main chain. The index of Genesis unit is set to 0, the index of the Genesis unit's child is set to 1, and so on. Secondly, if an unit is not on the stable main chain, we use the index of the first unit which is on the stable main chain and directly or indirectly refers to this unit. Thus, each unit is assigned a Main Chain Index (MCI) . Units with smaller MCIs are generated earlier. If two units have exactly the same MCI, the unit with the smaller hash value is valid.

The process of building the main chain is recursive calling the best parent unit selection algorithm. We can find the best parent of a given unit by comparing the number of witness units in the alternative path. Witnesses may be non-anonymous people of long-term involvement in the community, or good reputation, or maintaining the development of the network. Since we expect but not trust witnesses are honest, multiple witnesses are selected simultaneously.

#### 5.1.2. Double Spending

Double spending transactions: Any out-of-order transactions issued with the same address are treated as dual payment transactions, even if they do not use the same



output. The double spending transactions are also called conflicting transactions or contradictory transactions.

When a user issues a new unit, this unit should directly or indirectly confirm all the units issued by the same address. That is, all units with the same address are connected.

When all the units with the same address are connected, the earlier one of the double spending transactions appears on the path is the valid one. If an attacker intentionally creates a double spending transaction, it can be resolved by the MCI: the transaction with a smaller MCI is the valid one. Suppose the attacker creates a shadow chain and issues a double spending transaction on it. When the shadow chain links into the real DAG, the number of witnesses on the shadow chain is small based on the best parent selection strategy. Thus, the shadow chain will not be part of the main chain, and the double spending problem in this scenario is solved. Note that, if most witnesses colluded with the attackers and issue units on their shadow chain, the attacker would attack successfully.

### 5.1.3. Finality

As new units arrive, each user keeps track of his current MC which is built as if he were going to issue a new unit based on all current childless units. The current MC may be different at different nodes because they may see different sets of childless units. The current MC will constantly change as new units arrive. However, old part of the current MC will stay invariant.

In future, all MCs collide with each other at one stable unit. The Genesis unit is a natural stable unit. Suppose that we have build a current MC based on unstable units, and there are a number of stable units on this MC. If we can find a method to push the stable unit far away from the Genesis unit, the existence of the stable unit is able to be proved by complete induction. The units referred by the stable unit get confirmed MCI. Besides, the messages in these units are confirmed.

## 5.2. HashNet Consensus

### 5.2.1. HashNet Overview

The existing HashGraph consensus algorithm achieves the consensus of transaction sequence through gossip network and virtual voting strategy. The prerequisite of this consensus requires that the network node's voting ability exceeding  $2n/3$  has unanimous voting results for the famous witness event, where  $n$  is the total number of votes, and it is commonly represented by the number of tokens. Because of local voting strategies, HashGraph achieves quick transaction confirmation speed. However, this method has the following problems:

(1) In a wide area network environment, the node has strong volatility, and the fluctuation of the voting ability  $n$  of the entire network also increases. This may lead to the system unable to find an event that meets the  $2n/3$  voting consensus for a long time, and thus cannot reach a consensus.

(2) Due to factors such as node stability, processing power, and bandwidth, the ability of different nodes to handle events varies greatly. If there are a large number of weak nodes participating in the voting in the system, the consensus

may be not achieved for a long time.

(3) In a wide area network environment, frequent node fluctuations may cause the global network to be split into multiple subnets. According to the gossip neighbor exchange protocol, the node periodically eliminates neighbors that have not been updated for a long time. When the neighbor list is stable, the node reaches a consensus within the subnet. If the subnet size is small, it is easy for the malicious node to generate two famous witness events in the same round, resulting in a double spend transaction.

(4) As the system scale increases, each node has to handle a large number of gossip packages. Thus, the throughput rate of the system will decrease as the number of nodes increases.

To this end, we propose HashNet consensus. As shown in Figure 5–1, HashNet adopts a two-layer gossip topology based HashGraph consensus. At the high layer, each node is called full node, and these full nodes are responsible for the transactional consistency. In order to maintain network stability, all full nodes are elected through DPOS. Each full node receives two types of data from the underlying network: transaction data and cross-subnet transaction data. At the lower layer, each node is called local full nodes and responsible for maintaining the intra-subnet transactional consistency. Different from the full node, the local full node election considers the factors such as the number of tokens, processing capacity, bandwidth, and online duration. The local full node achieves the consensus of subnet transactions through HashNet.

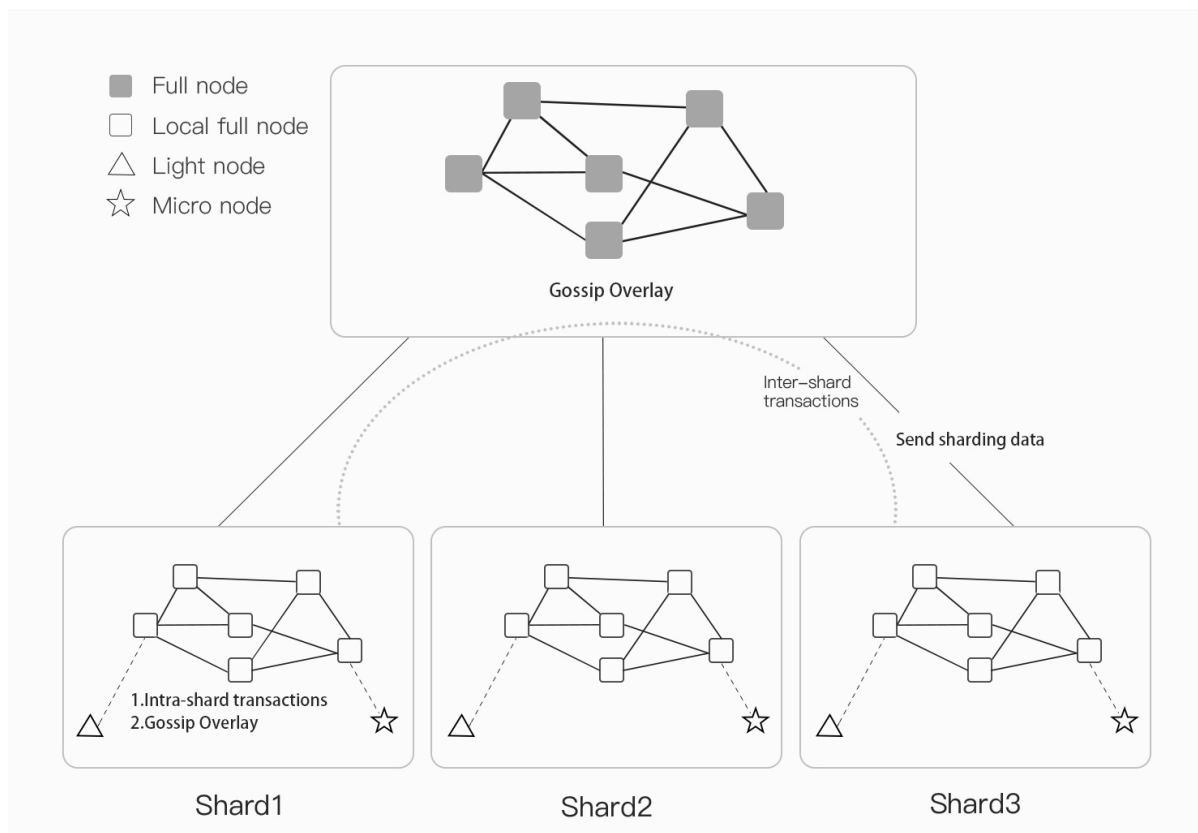


Figure 5–1: HashNet Overview Based on Two-layer Gossip Topology

The main advantages of the HashNet lie in two aspects:

(1) The full node and the local full node have strong stability and processing capability, so that they can avoid the problem that HashGraph can not reach a consensus for a long time. Meanwhile, these full nodes can also avoid the problem that the whole network is split into multiple subnets.

(2) Since we use a two-layer gossip topology to partition the nodes, full nodes do not engage in transaction consensus and verification, which ensures the system is able to extend to large scale.

### 5.2.2. Node Type

HashNet nodes are divided into four categories: full nodes, local full nodes, light nodes, and micro nodes.

- Full nodes: (1) It is responsible for maintaining the entire network topology, including full node joining/leaving, local full node joining/leaving. (2) It is responsible for updating shards, including calculating the number of shards, and partitioning local full nodes into different shards.
- Local full node: (1) As a proxy, it helps light nodes and micro nodes to send transactions. (2) Through HashNet, it engages in the process of transaction consensus, verification and storage. (3) To realize consistent database, each local full node synchronizes its HashNet with local full nodes of other shards.
- Light node: Commonly, it is a lightweight client wallet. It request or send data through a local full node.
- Micro node: It is usually an intelligent Internet of Things (IoT) device. Similar to light node, it request or send data through a local full node.

### 5.2.3. Node Maintenance

In HashNet, the transaction confirmation speed is affected by the stability, bandwidth, processing capacity of full nodes and local full nodes. On the other hand, full nodes and local full nodes have to be shuffled and updated to avoid collusion of Byzantine nodes. To this end, we designed a number of trusted and motivated mechanism to make nodes to join and update.

#### (1) Full Node Maintenance

However, there are two potential security risks if the full node are fixed. One is the full nodes may conspire and attack HashNet consensus. The other is that abnormal behaviors of full nodes are inevitable, such as software bugs, network congestion, or malicious attacks. Thus, it is vital to ensure the randomness of full nodes.

Suppose there are  $N$  full nodes. The lasted joined full node is called leader full node. We periodically run POW and HashNet consensus algorithms to update full nodes. The details are shown as follows:

- a) An applicant requests the full node list from a hub node. Next, it selects a full node and requests to do PoW. When the full node receives the request, it return the hash problem to the applicant.
- b) The applicant computes the hash result of PoW, which is signed by its private key. Next, the applicant sends its metadata of /public key, signature, hash result to a full node.
- c) When a full node receives the metadata of an applicant, it checks whether the candidate of the applicant has been confirmed. If yes, the full node ignores the applicant. Otherwise, the full node validate the signature and hash result of the applicant. When the validation is accepted, the full node launches the HashNet consensus at the top layer. The consensus content is the updated full node list, where the oldest full node is replaced by the new applicant.
- d) When the consensus is achieved, the updated full node list is sent to Hub node.

## (2) Local Full Node Maintenance

Compare to the full node, there are a large number of local full nodes, and they should be reviewed periodically. To this end, we use PoS+PoW+PoB+PoO to automatically determine the applicant's reputation, processing capabilities, bandwidth capabilities, and stability. Specifically, PoS is the proof of stakes, i.e., the applicant submits the proof of the number of tokens to a full node. PoW is proof of the work, i.e., the applicant randomly receives a hashing problem with a specific difficulty from the full node. The full node records its calculation time to evaluate the processing capacity. PoB is the proof of bandwidth, where the full node sends back-to-back data packets to measure the applicant's bandwidth. PoO is the proof of online duration, where the applicant submits its longest online duration to the full node. Finally, the applicant's composite score is:

$$\text{Score} = \alpha_1 \text{PoS} + \alpha_2 \text{PoW} + \alpha_3 \text{PoB} + \alpha_4 \text{PoO} \dots$$

where  $\alpha_i$  is the corresponding weight. According to the score ranking, the applicants with top-N score are selected as the local full nodes.

The local full node periodically updates its comprehensive score to the full node. When a new round of applications begins, the existing local full node and the new applicant jointly compete for the next round of local full nodes. After that, the full node partitions local full nodes into multiple subnets through sharding. The details of updating local full nodes are shown as follows:

- a) The applicant submits its proof to a full node.
- b) The full node computes the reputation score of the applicant. If the score is over a specific threshold, the full node launches the consensus at the top layer.

- c) When the apply window is closed, the leader full node selects the top-N applicants as the local full node candidates of next round. The leader full node splits all candidates into multiple shards, each of which has the same number of nodes.
- d) The leader full node launches a consensus of replacing the candidate shards with the existing shards. When the consensus is achieved, the candidates will substitute the existing local full nodes in next round.

#### 5.2.4. Sharding

After the full node has passed all local applicants for the next round, it is necessary to partition these applicants into multiple shards to ensure the scalability of the system.

##### (1) Number of Shards

The number of shards is a variable that needs to be carefully weighed. If that number is very small, the system's transaction confirmation throughput rate cannot be effectively improved. If that number is large enough, the possibility that the subnet is attacked by 1/3 malicious nodes greatly increases, and the full nodes have to handle a large number of cross-subnet transactions. To this end, we set the minimum number of nodes in each subnet to be 1000. In extreme cases, the number of shards is 1, if the total number of local nodes is less than 1000.

##### (2) Shading Details

To partition local full nodes into multiple shards, HashNet select a responsible full node through BA-VRF consensus protocol. The responsible full node determines the number of shards based on the minimum sharding size, and randomly divides all local full nodes into each subnet. Each subnet has a unique identifier `subnet_id`, and the corresponding node ID in the subnet is prefixed with its subnet `subnet_id`. Assume that there are four subnets in the network, and their subnet ids are 00, 01, 10, and 11 respectively. If there are four local full nodes in the 00 subnet, the corresponding node id is 0000,0001,0010,0011. Through prefix routing, each node is able to obtain the other node's subnet id. After that, the responsible full node allocates initial neighbor list to each local full node. Thus, the local full nodes automatically constructs the subnets based on their neighbor lists. Details are shown as follows:

- a) The responsible full node determines the number of shards based on the minimum sharding size, and randomly divides all local full nodes into each shard.
- b) The leader full node launches a consensus of the sharding at the top layer.
- c) When the consensus is achieved, the latest local full node list is sent to Hub node.

##### (3) Transaction Confirmation

Each local full node maintains all HashNets from every shard. The transaction confirmation contains four concurrent phases. The first is transaction consensus in shard, which means that each transaction consensus is completed in a single shard. The second is ledger synchronization among shards, which means the transaction data have to share among shards, such that each local full node maintain the global ledger. The third is event total order, which means that all consensus events have to be ordered totally to ensure the consistency of the global ledger. The fourth is event storage, which means to save events in database to help crash recovery.

Transactions are divided into following four cases:

Case 1: input (1)  $\rightarrow$  output (1), the input and output both belong to shard 1;

Case 2: input (1)  $\rightarrow$  output (2) + output (3), the input belongs to sharding 1, and two outputs belong to shard 2 and 3 respectively.

Case 3: input (1) + input (2)  $\rightarrow$  output(3), two inputs belong to shard 1 and 2 respectively, and the output belongs to shard 3.

Case 4: input (1) + input (2)  $\rightarrow$  output(3) +output(4), two inputs belong to shard 1 and 2 respectively, and two outputs belong to shard 3 and 4 respectively.

In case 1, since the input and output both belong to the same shard. For example, Alice in shard 1 sends 5 INVEs to Bob in shard 2. The detailed description is shown as follows: (1) Alice sends the transaction to a local full node L in shard 1. (2) After L ensures the transaction is legal, L packs the transaction into a new event and launches the HashNet consensus. (3) During the HashNet consensus, local full nodes of shard 1 send this event to local full nodes of other shards to realize the ledge synchronization. Note that, each local full node maintains multiple HashNet views, such that each received event is able to be verified. (4) For each local full node, the consensus events of different shards are totally ordered by their consensus timestamps.

In case 2, the input and output belong to different shards. Note that, we handle this case like the case 1. That is, we do not distinguish transactions in shard and among shards. The advantage is that it is able to avoid extra traffic overhead among shards and greatly reduce the consensus latency

The inputs in case 3 and 4 come from different shards, so we need to get confirmation of multiple shards to continue the transaction. We introduce “lock” and “release” operations to guarantee the atomicity of the transaction. For example, Alice in shard 1 and Bob in shard 2 jointly pay 5 INVEs to Lily in shard 3, where Alice pays 2 INVEs and Bob pays 3 INVEs. Assume that the transaction information is generated by shard 1. Step 1, the transaction information reached a consensus in shard 1 through HashNet, and two INVEs in the Alice account are locked. A validity certificate signed by Alice is generated, and sent to shard 2. Step 2, If there are enough balances in Bob’s account, 3 INVEs are locked through HashNet. Similarly, a validity certificate signed by Bob is generated and sent to shard 1. Step 3, Through HashNet of shard 1, the transaction is confirmed. Step 4, the transaction is distributed, confirmed and saved in other shards. To guarantee the atomicity of the transaction, the locked INVEs will be released if an abnormal case happens.



## 5.3. The Byzantine Agreement Consensus Based on Verifiable Random Function

During sharding, BA-VRF is used to select the responsible full node. BA-VRF is a consensus mechanism based on Verifiable Random Function (VRF) and Byzantine Agreement (BA) algorithm, it randomly selects a small number of full nodes as the attester nodes, and determines the priority of the attester nodes.

BA-VRF is executed every one minute. Every time when a consensus is reached, a number of full nodes will be selected as attester nodes in random. attester nodes have the authority to send attester units that must comply with DAG consensus' Parent-Child inter-reference rule. Once the attester unit sent by the attester node stabilizes on the MC, the attester node will get the attestation reward. When transactions are active and new units are generated continuously, attester nodes will receive their attestation rewards timely. Suppose that the transactions are less active or there is no new units generated in the last one-minute time window. In these cases, attester node will receive its attestation reward after the attester unit becomes stabilized MC unit. Meanwhile, those nodes who have not sent attester unit will not get the attestation reward.

### 5.3.1. Consensus Status

BA-VRF has two types of consensus status: final consensus and tentative consensus.

When a full node reaches final consensus, it means that any other full nodes also reach final consensus, or full nodes in the same round must agree on the same consensus result (tentative consensus), regardless of the strong synchronization assumption. Tentative consensus means that some full nodes may have reached a tentative consensus on other attester units, and no full node has reached the final consensus. All attester units must directly or indirectly reference the attester units that were generated before, which ensures the security of BA-VRF.

There are 2 cases where BA-VRF will eventually reach tentative consensus.

Case 1, suppose the network is strongly synchronized. With a small probability, An attacker may let BA-VRF reach tentative consensus. Thus, BA-VRF will not reach final consensus, and will not confirm that the network has strong synchronization. But after a few rounds, it is highly probable that the final consensus will be reached.

Case 2, suppose that the network is weakly synchronized. The attacker compromises the entire network, BA-VRF can reach tentative consensus and elects different sets of attester nodes, multiple consensus forks are formed. This will prevent BA-VRF from reaching final consensus, because the full nodes are divided into different groups, and the groups do not agree with each other. To regain activity, BA-VRF will be executed periodically until the disagreement is resolved. Once the network returns to strong synchronization status, final consensus will be reached in a short time.

### 5.3.2. Selecting Full Nodes

The lottery algorithm is constructed on the basis of a Verifiable Random Function (VRF) that selects a random subset of these Nodes based on the weightings of each full node participating in the BA-VRF consensus. The probability of a full node being selected is approximately the same as the ratio of its own weighting to total weighting. The randomness of the lottery comes from the VRF and a publicly verifiable random seed. Each full node can verify whether it is selected using the random seed.

Definition of VRF: Given an arbitrary string, the VRF outputs the hash value and the result of the proof.

$$(hash, \pi) \leftarrow \text{VRF}_{sk}(seed \parallel role)$$

The hash value *hash* is uniquely determined by the private key *sk* and the given string (*seed*||*role*), *hash* is not distinguishable from a random number without knowing the *sk*. The result of the proof  $\pi$  enables those Nodes who know the public key corresponding to the *sk* can verify whether hash is associated with *seed* or not. *seed* is randomly selected and publicly available, the *seed* of each round is generated from the *seed* of previous round. The lottery algorithm supports role assignment, such as selecting participants at a certain point during the consensus process.

All full nodes execute the lottery algorithm to determine whether they are authorized attestors. The selected full nodes broadcast their lottery results to other full nodes through the P2P network. Note in order to defend against a Sybil attack, the probability of selecting a full node by lottery is directly proportional to the full node's own weighting. A full node with a high weighting may be selected multiple times, for which the lottery algorithm will report the number of the full node been selected. If a full node is selected multiple times, it will be treated as multiple different full nodes.

### 5.3.3. Byzantine Agreement

Byzantine negotiation (BA) can determine the notarization priority for each selected full node and provide proof of notarization priority. The BA algorithm is executed multiple times to achieving the Byzantine consensus.

In BA algorithm, each negotiation begins with a lottery. Each full node checks whether it is selected as current BA participant. A participant broadcasts a message containing the priority of selecting a notary. After receiving the message, each full node initializes the BA algorithm. The above process repeats until there are enough full nodes to reach a consensus at certain round of negotiation. Note that the BA algorithm is not synchronized among different full nodes. When a full node finds the previous steps have finished, it should immediately check the results of new participant elections. A full node is allowed to participate the next negotiation until all full node vote and reach a consensus.

An important feature of the BA algorithm is that participants only need to store private keys, rather than maintaining private states. So each participant can be replaced after each step to reduce attacks on participants. When the network is strongly synchronized, the BA algorithm guarantees that the final consensus can be



reached within few interaction steps if all the honest full nodes are initialized with the same content. In this case, all the honest full nodes will reach final consensus in the limited interactive steps even if there are a small number of attackers.

# Hash Algorithm and Signature Algorithm Against Quantum Attacks

## 6.1. Hash Algorithm Against Quantum Attacks

Hash algorithm in cryptography, also known as hash function or hash function, plays an important role in modern cryptography. The hash algorithm is a public function  $H$  that maps any long message  $M$  to a shorter, fixed-length value  $h$ .  $h$  is called a message digest, also known as a hash, hash, or hash value. The structure of the hash algorithm is shown in Figure 6–1.

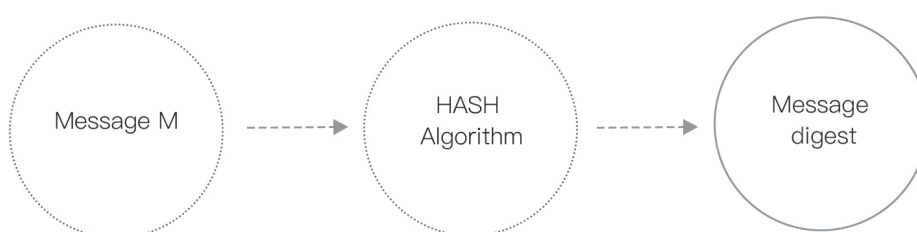


Figure 6–1: Hash Algorithm Schematic

In order to ensure that the data will not be altered, the Blockchain will save its hash function values in addition to the original data or transaction records. The transaction data on the Blockchain usually gets the final Merkle hash value after many hashes. The address data on the blockchain is usually obtained by computing a Hash value and then converting the Hash value into a string composed of numbers and letters through a specific coding (such as the Base58 code used in the Bitcoin blockchain).

At present, the most effective quantum algorithm for attacking hash algorithms is the GROVER's algorithm, which reduces the attack complexity of Hash algorithm from  $O(2^n)$  to  $O(2^{\sqrt{n}})$ . At present, the hash algorithm PIREMD160 used in the bitcoin system is insecure under quantum attack because the output length is

only 160 bits. An effective measure to resist the quantum attack is to increase the output length of the hash algorithm. At present, it is generally accepted that the hash algorithm can effectively resist the quantum attack as long as the output length of the hash algorithm is no less than 256 bits. In addition to quantum attack threats, a series of Hash functions which are widely used in practice (MD4, MD5, SHA-1, and HAVAL) are attacked by traditional methods such as differential analysis, modular differential analysis, and message modification analysis, so the hash algorithm in Blockchain also need to consider is the traditional attack resistance.

Earlier Blockchain projects such as bitcoin, Litecoin, and Ethereum used SHA series algorithms with design flaws (but not fatal ones), and the recent Blockchain projects all use the US National Institute of Standards and Technology SHA-3 plan series algorithms. InterValue uses Keccak512 which is the winner algorithms of the SHA-3. Keccak512 contains many new concepts and ideas of hash function and cryptographic algorithm design, and the design is simple and very easy to implement on hardware. The algorithm was submitted by Guido Bertoni, Joan Daemen, Michael Peters, and Gilles Van Assche in October 2008. Keccak512 uses a standard sponge structure that maps input bits of any length into fixed-length output bits. The algorithm is very fast, with an average speed of 12.5 cycles per byte under the Intel Core 2 Duo processor.

As shown in Figure 6-2, during the absorption phase of the sponge structure in the algorithm, each message packet is XOR'ed with the  $r$  bits inside the state and then packed into 1600-bit data along with the fixed  $c$  bits followed by the wheel function  $f$  and then into the extrusion process. During the squeeze phase, a hash value of  $n$ -bit fixed output length can be generated by iterating through 24 iterations, with only the last round of rounding constant different for each iteration, but this round of constants is often neglected in collision attacks. The algorithm has been shown to have very good differential properties, so far the third-party cryptanalysis does not show that Keccak512 has security weaknesses. The first type of preimage attack complexity under Quantum Computer for Keccak512 algorithm is  $2^{256}$ . Therefore, InterValue using Keccak512 algorithm can resist quantum attack.

## 6.2. Signature Algorithm Against Quantum Attacks

Hash algorithm can ensure that the transaction data is not modified, but there is no guarantee of simultaneous substitution attacks on data and digest, nor does it guarantee the non-repudiation of transaction data. Digital signature algorithm involves public key, private key and wallet and other tools. It has two functions: one is confirming that this message is signed and sent by the sender, which guarantees the non-repudiation, and the two is to confirm the integrity of the message. The technology of digital signature is to encrypt the summary information with the private key of the sender and transmit it to the recipient with the original message. The receiver can decrypt the encrypted digest information only with the sender's public key, and then use hash algorithm generates a digest of the received message and compares it with the decrypted digest. If they are the same, the received message is complete and has not been modified during the transmission, otherwise the message is modified. Therefore, the digital signature can verify the integrity

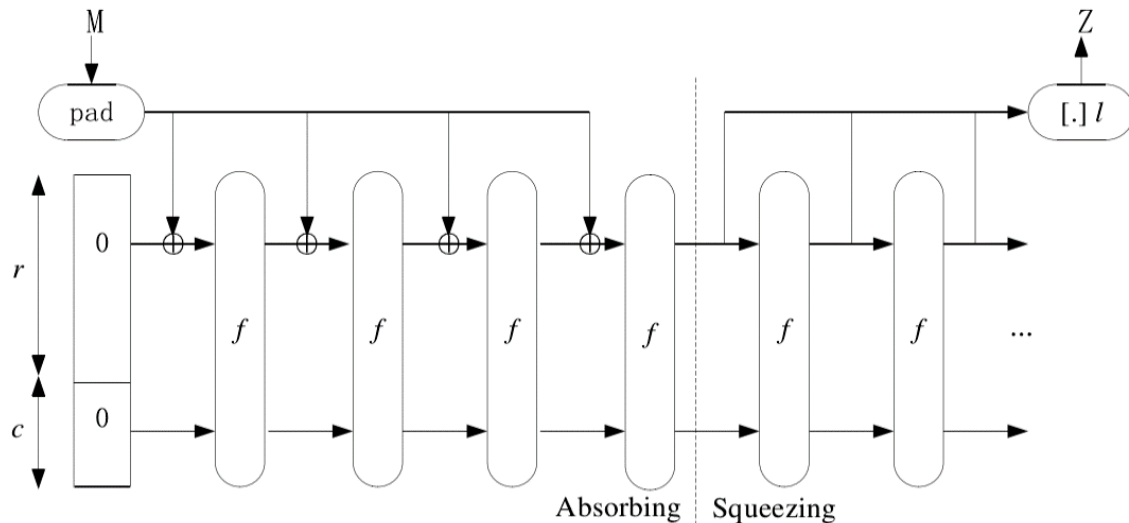


Figure 6-2: The Flowchart of Keccak512 Algorithm Implementation

of the message and ensure the non-repudiation of the message.

Existing Blockchain systems mostly use ECDSA, an elliptic curve digital signature scheme which is based on DSA signature algorithm. As the standard of ANSI, IEEE, NIST and ISO, ECDSA has the advantages of small system parameters, fast processing, small key size, strong anti-attack and low bandwidth requirements. For example, 160 bit ECC has the same security strength as 1024 bit RSA and DSA, while 224 bit ECC has the same security strength as 2048 bit RSA and DSS. For quantum computer there has a very efficient SHOR attack algorithm, SHOR's algorithm is suitable for solving large integer decomposition, discrete logarithm inversion and other difficult mathematical problems. At present, the public-key cryptosystems against quantum attacks mainly include the public-key cryptosystems based on lattice theory, the error-correcting code based public-key cryptosystems represented by McEliece, and Multivariable polynomials based public-key cryptosystems represented by MQ. The security of McEliece is based on error-correcting code, which is safe but low in computational efficiency. MQ cryptosystem is based on two variable polynomial equations in finite field. However, its security shortcomings are obvious. In contrast, the public key cryptosystem based on lattice theory has the advantages of conciseness, fast computing speed and small storage space. InterValue uses lattice theory based signature algorithm NTRUSign-251, the algorithm concrete realization process is as follows:

1. **Key Generation:** Select two polynomials  $f$  and  $g$  on ring  $R$  such that the numbers of 1 in the coefficients of  $f$  and  $g$  are  $d_f$  and  $d_g$  respectively, compute the public key  $h$ :  $h = F_q * g(\text{mod } q)$ .

Solve the polynomial  $(F, G)$  so that it satisfies the equation  $f * G - F * g = q$ .

And  $\|F\| \approx \|f\| \sqrt{N/12}$ ,  $\|G\| \approx \|g\| \sqrt{N/12}$ .

2. **Signature process:**

- 1) The HASH transformation of message  $M$  is transformed into a polynomial  $(m_1, m_2)$ , in which the polynomials  $m_1$  and  $m_2$  are a polynomial on the ring  $R_q$ .

- 2) The polynomials  $A, B, a, b$  on the ring are computed to satisfy:

$$G * m_1 - F * m_2 = A + q * B$$

$$-g * m_1 - f * m_2 = a + q * b$$

And the coefficients of each item of  $A$  and  $a$  are required to meet the conditions greater than  $-q/2$  and less than  $q/2$ .

- 3) The polynomial  $s$  is calculated as follows:

$$s = f * B + F * b(\text{mod } q)$$

$s$  is the signature computed by plaintext  $M$  using public key  $h$ .

3. **Verification process:**

Hash transformation of message  $M$  into polynomials  $(m_1, m_2)$ .

Calculated from the verifying signature  $s$  and the public key polynomial  $H$

$$t = g * B + G * b(\text{mod } q)$$

Calculating the distance between polynomials  $(s, t)$  and  $(m_1, m_2)$ :  $\|m_1 - s\| + \|m_2 - t\|$ , If the distance is greater than NormBound then the verification fails, otherwise the signature is validated.

It has been shown that the security of the NTRUSign-251 signature algorithm is ultimately equivalent to finding the shortest vector problem in a 502-dimensional integer lattice. The shortest vector problem in the lattice is invalid under the SHOR's algorithm, the best heuristic algorithm is exponential at the moment, the time complexity of attack NTRUSign-251 signature algorithm is about  $2^{168}$ , so InterValue using NTRUSign-251 algorithm can resist the SHOR's algorithm attack under quantum compute.

# Anonymous Transactions

Anonymous transactions and privacy protection are essentially properties of the electronic currency. However, the existing digital cryptocurrencies suffer from the insufficiency of anonymous and private transactions. InterValue is designed to be a cryptocurrency with unlinkability and untraceability transactions.

Blockchain 4.0 gives new definitions of unlinkability and untraceability. Unlinkability means for any two transactions, it should be impossible to prove that they were sent to the same person. Untraceability means given a transaction input, the real output being redeemed in it should be anonymous among a set of other outputs. In order to guarantee unlinkability and untraceability, InterValue introduces the *one – timesecretkey* and the cryptographic primitive called *ringsignatures*. InterValue by design employs strict *zero – knowledgeproof* to guarantee the confidential transactions.

## 7.1. The One-Time Secret Key

When using the one-time secret key scheme, a unique key pair is used for every transaction. A sender generates a temporary one-time public key based on the recipient's address and some randomness. With the temporary public key, a transactions key is generated, which is the transaction address. So, transactions destined to the same recipient are in fact sent to different one-time public keys. At the same time, only the recipient can recover the one-time private keys to redeem the funds. The unlinkability can be maintained because the randomness is different in every transaction.

## 7.2. The Ring Signatures

The Ring signature is a digital signature that specifies a group of possible signers such that the verifier can't tell which member actually produced the signature. It is derived from multi-user signature. However, the rings are geometric regions with uniform periphery and no center. So the ring signature has several advantages such as no the group administrator, with strong untraceability, etc. The principle of ring signature scheme is shown in Fig. 7-1.

When using ring signature, a message is signed by a group user, and the verifier

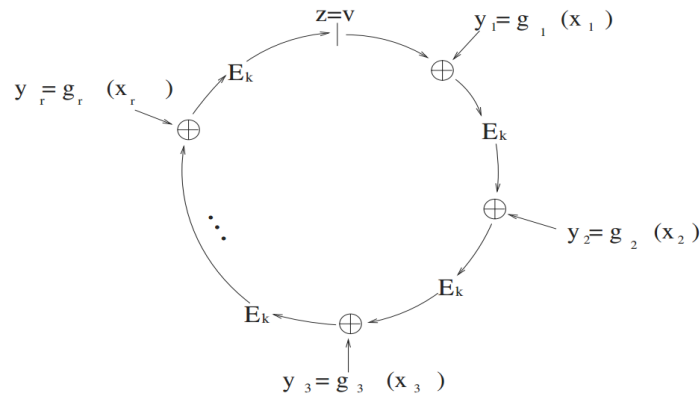


Figure 7-1: The Ring Signature

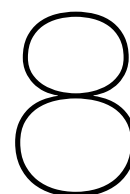
cannot know who is the target user. For this reason, transactions with ring signature in cryptocurrency is natural untraceability and privacy resistant. On the other hand, transactions with ring signature also suffers from double spending problem as the target signer is hidden from a group user. The linkable ring signature scheme can be used to avoid the double spending.

### 7.3. The Zero-Knowledge Proof

The zero-knowledge proof scheme was originally proposed by Goldwasser, S.Micali and C.Rackoff in 1985 by requiring that for every malicious efficient verifier  $V$ , there exists an efficient simulator  $S$  that can reconstruct the view of  $V$  in a true interaction with the prover, in a way that is indistinguishable to every polynomial-time distinguisher. Essentially, the zero-knowledge proof is derived from traditional mathematic proof system by introducing randomness and interactive variable. For an application with zero-knowledge proof, malicious verifier problem, which require the verifier cannot achieve new knowledge in the process of verification, is the main factor to be avoid. The ZCash is the first cryptocurrency using zero-knowledge proof to guarantee the confidentiality of transactions.

### 7.4. The Confidential Transactions

InterValue by design to be anonymous and privacy for confidential transaction. Inspired by Monero, InterValue 1.0 to 3.0 implements the one-time secret key and ring signature to satisfy the require of anonymous and privacy. InterValue 4.0 will implement the strong non-interactive zero-knowledge proof to achieve full confidential transactions.



## Smart Contract

Blockchain technology brings us a system with decentralization, no trust, no falsification, and high reliability. In this environment, the smart contracts are of great potential. Smart contracts are self-executing contracts with the terms of the agreement between buyer and seller being directly written into lines of code. The code and the agreements contained therein exist across a distributed, decentralized Blockchain network. Smart contracts permit trusted transactions and agreements to be carried out among disparate, anonymous parties without the need for a central authority, legal system, or external enforcement mechanism. They render transactions traceable, transparent, and irreversible.

Smart contract needs to find a subtle balance between the safety and usability. Existing blockchains are mostly of a monotonous design, seeking for the balance between safety and usability under the restriction of a given type of smart contract, and usually cannot guarantee rich user experience and satisfy various trading demands. The transaction script of the Bitcoin blockchain is an early prototype of the smart contract. It is Turing-incomplete, with low complexity and light weighted. For the past ten years of the Bitcoin, its transaction script has never experience any safety compromise. However, the Bitcoin transaction script has a highly limited function, and can only be used for payment verification. The Ethereum blockchain supports a Turing-complete smart contract which is programmed in Solidity. It enriches the functionality of the smart contract and largely extends the application scenarios for the blockchain. Unfortunately, an Ethereum smart contract suffers from potential safety hazards. The DAO incident is a famous example that the safety problem in the Ethereum smart contract leads to the split of the community.

Built upon the smart contract and the Moses Virtual Machine (MVM), InterValue takes a similar idea as the hierarchical design of the computer storage system and supports both the Declarative Turing-incomplete smart contract and the Advanced Turing-complete smart contract. The users choose between the two kinds of smart contracts based on their experience and trade demands, hence achieve the balance between the safety, functionality, complexity and cost. The declarative contract is easy to deploy, with a high level of safety and close to legal contract statements. The advanced contract is more difficult to deploy, and mostly used for



developing the DApp with a logic of higher complexity. The two smart contracts have different charging schemes. The declarative contract charges according to the number of bytes being taken, while the advanced contract charges according to the number of INVE tokens being consumed.

## 8.1. Declarative Turing-incomplete Smart Contract

The Declarative Turing-incomplete smart contract is light weighted, easy to program, and with low complexity and high level of safety. It consists of statements and boolean expressions, hence is close to the traditional language of legal contract. It supports boolean and mathematical operations, as well as data storage. InterValue provides a lot of predefined templates for the user to use or modify, thus reduced the difficulty of deployment and the level of error rate. Furthermore, in contrast to the Turing-complete smart contract, it has a higher level of safety. It uses the same scheme of charging as the common trade transactions, which is by the bytes.

It usually requires a specific level of knowledge about programming to make a smart contract. For the ease of use of common users, InterValue supports a various types of Declarative Turing-incomplete smart contract templates (Contract Template). All the user needs to do is to choose a preferred template and fill in the related parameters. The templates can be reused, or be referred in other ones. The following is an example of such smart contracts.

```
[ "contract template", [
  "hash of unit where the template was defined",
  {param1: "value1", param2: "value2"}
]]
```

Despite of its low complexity, the Declarative Turing-incomplete smart contract is still capable of advanced functionalities such as obtaining external data or inter-blockchain communication.

The following is an example of obtaining external data. If the data submitted by Alice, Bob or Cara is higher than the expected value, the condition is true. Other than "=", the contract also supports operations like "!=" , ">" , ">=" , and "<=" . Complex conditional control can be achieved by specifying the data source.

```
[ "in data feed", [[
  "Alice", "Bob", "Cara" ... ] ,
  "data feed name",
  "=",
  "expected value"
]]
```

The following shows an example of the interblockchain communication. Bob trades for BTC with Alice through INVE, and the transaction time is assigned at 2018-02-15. Before that time, if Alice transfers 10 BTC to Bob, the BTC oracle will have a corresponding record and the contract will trigger. Then Alice will receive the INVE which Bob has deposited into the contract beforehand. The exact number of INVE is based on the negotiation about the transferring rate by

Alice and Bob. If Alice does not transfer 10 BTC before the negotiated time point, Bob will get back his deposit.

```
[ "or", [[
  "and", [[ "address", "Alice"],
    ["in data feed", ["BTC oracle"],
      "BTC from Alice to Bob",
      "=",
      "10"]]]
  ],
  ["and", [[ "address", "Bob"],
    ["in data feed", ["TIMESTAMPER ADDRESS"],
      "datetime",
      "<",
      "2018-02-15 00:00:00"]]]
  ]]
```

## 8.2. Advanced Turing-complete Smart Contract

The Turing-complete smart contract supports the logics of goto and loop, thus can enable much richer functionality than the Turing-incomplete smart contract. However, it also requires more knowledge to program and easier to have safety issues. As a result, it requires professionals to build and test the Turing-complete smart contract. To protect the network performance from the logic bombs, and provide an anti-fraud mechanism, the Turing-complete smart contracts no longer charge according to the bytes being taken but adopt a mechanism similar to Gas which is used in the Ethereum smart contract. When the users call a smart contract, they have to deposit a certain amount of Gas beforehand. As the smart contract being carried out, Gas will be consumed as the instructions in the contract are executed. After the smart contract is finished, the remaining Gas will be returned to the publisher. If all the deposited Gas are consumed before the contract is finished, the status of the contract will be rolled back to the initial state, and the consumed Gas will not be returned.

InterValue uses a newly proposed advanced programming language, which is called Moses, to program the Advanced Turing-complete smart contract. Moses is object-oriented and has a programming style similar to JavaScript, thus gives ease to the huge amount of Web developers to migrate to InterValue. With Moses, the functionalities of the Declarative Turing-incomplete smart contract can also be realized. The unique feature of InterValue Advanced Turing-complete smart contract is that it supports access to data off the blockchain. As the application scenarios of blockchain rapidly expanding, the need of accessing data off the blockchain is also increasing quickly. The Ethereum smart contract which only supports on-blockchain data access is becoming limited. Here, the off-blockchain data does not generally refer to all the data that is not on the InterValue blockchain, but specifically to the data on distributed storage systems which are based on the blockchain technique. This kind of data usually have a high quality, but involves the

problem of profit distribution, which requires the use of smart contract to achieve authentication and granting of data access.

- Safe off-blockchain data access: Moses will have specifically designed built-in protocols for off-blockchain data access. For example, the built-in IPFS protocol is specifically designed for accessing data on the IPFS distributed storage system. By having the built-in protocol, the data access can be constrained, and the risk of accessing malicious data/program is lowered. At the time, InterValue will also build its own distributed storage system, and build in the data access protocol. The users who store data in the system will pay per the size, hence ensures the data quality.
- Safe off-blockchain data usage: Moses allows read/write operations to the off-blockchain data, but not the execute operation. By reading the off-blockchain data, Moses supports configurable business logic. The complexity of the Advanced Turing-complete smart contract lies not only in its program logic, but also the business logic. For example, when composing a smart contract related to legislations, support from legal professionals is needed, which cannot be provided by professional developers. InterValue provides rule-based configuration format which can support to store the knowledge in a specific profession in the forms of rules off the blockchain. By reading these docs, the smart contract realizes the business logic in the given professional area. The configuration doc in a specific professional area is reusable, thus opens the possibility of a data exchange market. In general, the data provided by the users is confirmed to be safe beforehand.

### 8.3. Moses Virtual Machine (MVM)

Both the Declarative Turing-incomplete smart contract and the Advanced Turing-complete smart contract are validated and executed in the Moses virtual machine. The Moses virtual machine adopts a stack-based structure. It not only can simplify the implementation of instructions and compilers, but also can provide outstanding portability. The data structure of a running MVM is shown below.

- Instruction counter: Stores the bytecode address of the next instruction.
- Virtual machine stack: Each time the Advanced Turing-complete smart contract is executed, MVM will create a virtual machine stack in the instruction dispatching area. The virtual machine stack consists of different stack frames, and each execution and completion of a smart contract correspond to a stack and pop process, respectively.
- Native method stack: Privately owned by the instruction dispatcher. It has a similar functionality as the virtual machine stack and is used to store the method related information.
- Heap: All the objects of the smart contract is allocated a storage space here.
- Method area: Used by the MVM to load the class, constants and static variables.

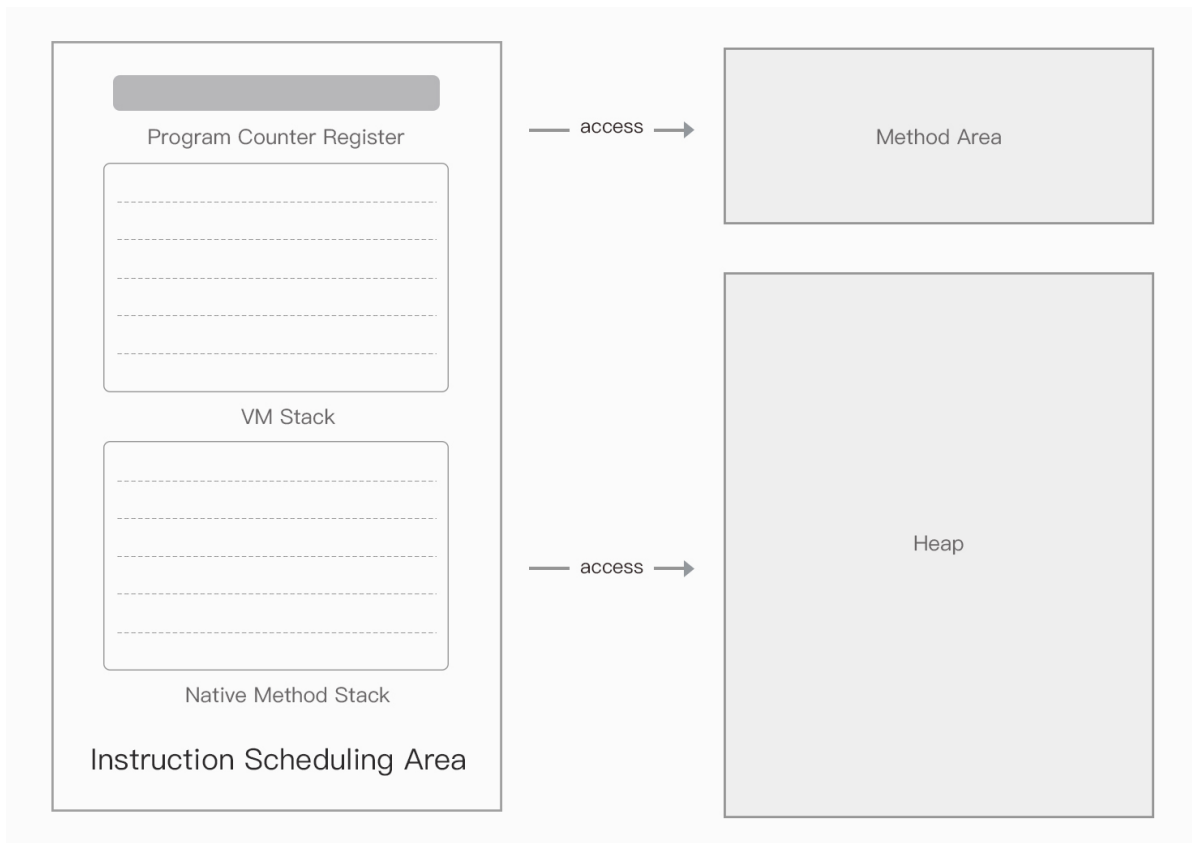


Figure 8–1: MVM Runtime Area

The Advanced Turing-complete smart contract is already compiled into byte-codes before deployed on InterValue, and MVM can directly load and run it. In contrast, the Declarative Turing-incomplete smart contract is embedded into the transaction data in JSON, which cannot be directly loaded and run by MVM. In the InterValue client, there will be a compiler for the Declarative Turing-incomplete smart contract, which will compile the contract into a default contract object byte-code. The bytecode is then loaded into MVM and run.

Take into consideration the system-level protection of smart contract from malicious attacks, MVM is designed to be a sandbox with strict access control policies. Based on the implementation of the process-level isolation execution environment for bytecode-oriented, a white list implemented according to the principle of least privileges is used in the security sandbox of MVM. Each method invoked by smart contract codes is checked strictly to restrict the access rights to satisfy its operational functions being designed. And the data in the stack and Heap is stored with strict access control policies for trusted use.

## 8.4. Smart Contract Accounts and Transactions

Similar to the account in Ethereum, there are external accounts and contract accounts in InterValue. The external contracts are controlled by the user, which are used for initiating a transaction. The contract accounts are controlled by the external accounts, which by taking calls from external accounts and other contract

accounts to initiate the execution of the smart contract.

The Declarative Turing-incomplete smart contract is embedded into the data of transactions initiated by external accounts. It is used for providing constraint conditions for the transaction and has no concept of accounts. The smart contract account specially refers to the account returned after the Advanced Turing-complete smart contract is deployed. The external accounts and contract accounts have states. For example, the INVE token balance and number of initiated transactions are both states of the accounts. To remove the difference between the external account and the contract account, the account state includes the hash of its MVM code, which is unchangeable after the Advanced Turing-complete smart contract is deployed. Besides, to access the user's data stored off the blockchain, the account states also includes the repository information of off blockchain data.

In InterValue, there are two types of transaction fees. The common transactions initiated by external accounts charge by bytes. The transactions calling a smart contract charge by number of executed instructions. To remove the difference between the two kinds charges, two fields similar to the Gas cap and Gas price in Ethereum are included in the transaction data structure to unify the charge schemes. For the charges by code bytes, the number of bytes of the transaction is given (i.e., the charge is known ahead), then we can fix the Gas cap and automatically compute the Gas price to charge the account. When the user sends a transaction of an Advanced Turing-complete smart contract, in the transaction data structure there will be a field specifying the MVM code.

# 9

## Applications and Scenes

### 9.1. Applications

#### 9.1.1. Distributed Social Network Applications

Distributed social network application is based on block chain technology and distributed P2P technology, in order to achieve decentralization, free access to any social network world, which is not affected by any organization. Different from traditional social networks, distributed social networks have no concept of server. All social data are stored in the distributed computers. Anyone needs only a pair of asymmetric keys to publish contents.

Everyone can find the publisher's computer in the P2P network through the publisher's private key, and download the site's data. After more and more people visiting, a number of computers will save the publisher's contents. The computers that have visited your home page will start to seed your site. Like the BT seeds we know, the contents of your site are alive in countless computers.

As long as there is a computer network connected with your site's seed, your contents will not disappear. Moreover, when the P2P network is big enough, your contents are not be completely deleted, and they will be immortal with the Internet world.

The distributed social network has become very ordinary because of its P2P's non-central host features. You do not need rent the host to register the URLs. All you need is to generate a random site address according to the HTML code, and publish it to other computer.

#### 9.1.2. Divergent Contract Trading Applications

The definition of Divergent contract trading applications is that a disagreed trading market. For example, the traditional "Beijing single field lottery" is a disagreed trading market, where the user is disagreed on the team's victory or defeat.

The Divergent contract trading applications based on InterValue can achieve a win-win ecosystem from five fields.

- Technology providers: providing all technologies of the entire platform,
- Platform operators: transforming the front-end interface, and providing multi-lingual operations,

- Divergent designers: finding divergences, designing divergent contracts,
- Contract market makers: providing liquidity,
- Divergent traders: buying and selling divergent contracts, balancing risk, and earning profit.

### 9.1.3. File Storage Grid Applications

File storage grid is a commercial public chain platform, which first provides basic services for individual data storage. Individuals can publish their data on the chain. Based on massive individual data, the platform realizes the decentralized data collection, sharing and governance, by developing various kinds of professional DApp. The platform creates an ecological system for decentralized data storage, convergence, sharing, governance, et al.

- Distributed data storage platform based on file storage grid,
- A secure, extensible commercial public chain infrastructure,
- A credit system.

The goal of the big data ecological chain is to realize distributed storage and large-scale decentralized applications. Moreover, the big data ecological chain has the following characteristics over the traditional public chain.

- Programmability,
- Extensibility,
- Upgradability,
- Transaction manageability,
- Visibility,
- Affordability,
- Safety,
- Speed / performance,
- High reliability,
- Ductility.

## 9.2. Scenes

### 9.2.1. Outline of Scenes

The main scenes of InterValue are as follows: (1) Digital currency; (2) Extensive financial application; (3) Non-financial applications. applications.

- Digital currencies

The main application scenes of digital currencies are as follows: ① Third party asset issuance; ② Crowdfunding.

- Extensive financial application

The main application scenes of digital currencies are as follows: ① Cross-border payment, Supply chain finance, Digital bill; ② Asset Securitization, Bank reference, Insurance.

- Non-financial applications
  - ◊ Medical care: Electronic health (EHR) , DNA wallet, Drug Counterfeit-proof.
  - ◊ Internet of things: Supply chain management, Sharing economy, Energy management.
  - ◊ IP copyright & Cultural entertainment: Copyright, Authentication and tracing of image, Intellectual property registration, Decentralization of digital rights management.
  - ◊ Public service & Education: Public audit, Land right, Public welfare project, Educational information registration.

The specific applications on a chain are as follows:

- ◊ Virtual assets: Game equipment, Live broadcast reward,
- ◊ Conditional payment: Pay for knowledge, API call, Centralization insurance, etc.,
- ◊ Privacy deals: Betting, Gambling, etc.,
- ◊ Ex-pit transaction: Currency exchange,
- ◊ Social transactions: Group of red packets, Group receipts,
- ◊ Sharing economy: Content distribution (CDN) incentive, Advertising flow division.

### 9.2.2. Physical Asset Transaction Authentic Right

- Joint signature

The asset owner and the right institution jointly sign the asset information to ensure that the authority approves the true information on the block chain. The asset owner registers the assets on the block chain, and the confirmation authority makes joint signature on the right information after the investigation and determination of the assets.



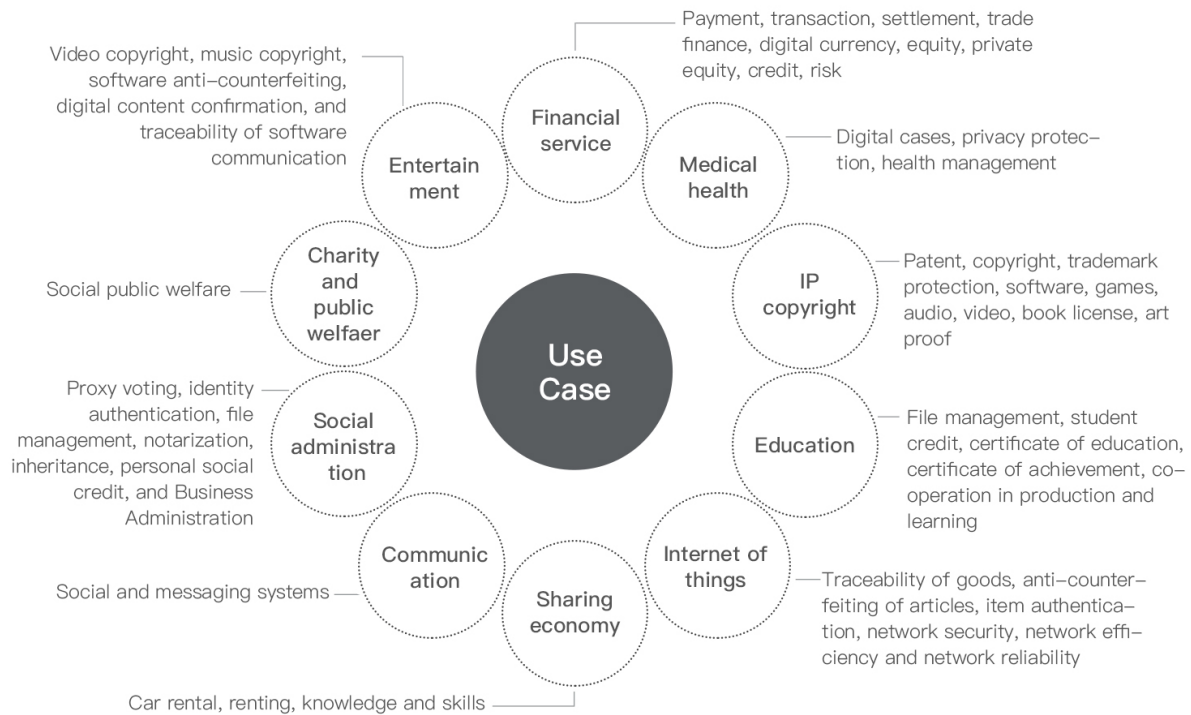


Figure 9-1: The Scene of Chain

- Block chain plus digital certificate

At present, digital certificates are mainly applied to industries related to asset exchange, such as finance, e-commerce, securities, insurance, and payment and so on. These industries provide a real estate based on strong identity authentication, an online operation anti repudiation and anti-counterfeiting based on the electronic signature.

In the physical assets transaction authentic right, we can apply for the certificate of ECC at the CA agency. The address on a block chain corresponds to a public key. This public key corresponds to the corresponding digital certificate. The authority approves this digital certificate. Digital identity could be authenticated as long as the digital certificate is published on the block chain. Then we carry out the asset information registration on the block chain, including assets category, name, total amount, owner, permissions and other information, and confirm the entity assets approved by the authorized authority.

### 9.2.3. Decentralized Travel Service Platform

The bottlenecks of the current travel service platform are:

**(1) Trust system:** The current travel market is centralized data storage, for example, platforms like TripAdvisor, Dianping, and Priceline. They all control centralized data for the purpose of business and advertising, and cannot guarantee the user experience. Feedback comes from disparate and subjective places and in many cases is fake or bought – this is a particular problem where positive reviews

can be bought for next to nothing. In order to maintain greater benefits, these platforms charge a large number of intermediate costs rather than creating better travel services for the resource providers and consumers.

**(2) Custom travel:** Finding trusted and relevant lifestyle services & experiences on your travels requires trawling through a glut of irrelevant, often outdated and sometimes fake information on multiple touch-points. It is time consuming and painful. How do you find information that is relevant to people like you and people who travel like you? This is not just inconvenience – studies show 56% of travelers want more personalised & relevant information and a massive 96% of travellers in general feel stressed with overwhelming information, while 74% feel crippled by indecision – wasting hours on research. Existing methods are skewed, noisy & subjective – search and reviews model is broken.

**(3) Block chain performance:** The traditional block chain technology is to solve most of the monetary system; its performance usually cannot meet the actual application scenarios. Technology represented by bitcoin usually supports only seven transactions per second. The technology represented by the ETH is only about 25 transactions per second. Traditional block chain technology cannot support such a huge global travel market.

In view of the above features, the main innovation scheme of the decentralized travel service platform based on InterValue public chain is as follows:

**(1) Trust system:** Based on block chain technology, we skip the platform intermediary difference to directly connect travel consumers and travel resources suppliers. From travel planners, airlines, hotel accommodation and reservations, we build a future travel service ecology based on trust, incentive and zero Commission. Based on smart contracts technology, travel planners, airline tickets, hotel accommodation, etc. are booked with INVE. Travel resources suppliers do not have to pay any commission to reduce their operating costs. Users will use lower prices to get better services.

**(2) Custom travel:** InterValue matches users to the best-personalized local experiences & services powered by proprietary AI & Data Science and driven by crypto. It is frictionless – InterValue cuts out the noise, enabling our users to discover & book immediate high-quality local services & experiences matched to their preferences, users can book or reserve directly through the platform. Additionally InterValue does not rely on long and subjective reviews, instead creating & curating meta-scoring and true representations of experiences through transactions using smart technology. InterValue focuses heavily on personalization and finding peers who have interests and tastes similar to make information & matches as relevant as possible. InterValue uses multiple layers of data including contexts, environment, behaviors and multiple other data points to create a complete picture of the “match”. As the ecosystem grows InterValue will open this out more for user cohorts publicly called “Travel Squads” to selectively recommend and enjoy experiences with as well as engage and help build the InterValue ecosystem and community.

**(3) Block chain performance:** InterValue public chain travel is based on block chain 3 technologies and uses the DAG consensus algorithm to make transactions faster and adapt to the huge travel market in the world. InterValue public chain

travel uses a non-Turing complete declarative smart contracts system. Smart contracts are made up declarative and complete Boolean statements, so it is closer to the traditional legal contract language, supporting Boolean operations, mathematical operations, data storage and so on.

InterValue is creating a robust business model that incentivizes providers and industry leaders with existing customer bases, to join the InterValue network and drive traffic to the network. InterValue can built a network of over lots of providers who will join the platform. These providers include everything the traveler will want locally when they are on their travels from dining, private drivers, nightlife, experiences and beyond. Providers are able to offer their goods and services across the InterValue loyalty network, in turn earning INVE. InterValue creates a unique solution for travel markets based on the INVE – revolutionizing the way people book experiences and use loyalty. InterValue will allow users to exchange their loyalty across the platform for discounts, real goods and experiences as well as exchanging loyalty with other users. We are allowing the user to take more control of their loyalty while giving providers and brands the opportunity to engage users on every part of their journey.

InterValue uses “genuine rating”, which means only those, who did transacted with providers or engaged in loyalty with them are able to provide feedback. This enables us to base reviews and feedback on real successful transactions – not assumptions, marketing information or paid reviews. Feedback is also taken in a contextual manner around the user, provider and conditions. This feedback builds up on the immutable Blockchain, and is later governed by AI to understand the complete data picture. This means that reviews are a lot less likely to be faked, and that the platform increases in its credibility and maintains solid authenticated data, unlike many platforms that currently exist. InterValue creates a quantified reputation system to aggregate reputation data and report trust scores for providers. InterValue will be able to employ AI on the chain to collect sentiment and metadata to accurately indicate the relevant feedback to the relevant party. For providers – funds are released per fulfilment of a smart contract written by InterValue, and the credentials tied to an ID stored on the Blockchain. Both executing a transaction and potentially in the future connections to the smart contract will release payment triggers. This means release of payments to providers is much quicker and more efficient than they would be otherwise providing greater satisfaction to vendors and providers.

Ultimately, InterValue is becoming a “full-stack” cryptocurrency-enabled travel destination marketplace. We are able to easily manage and automate a large part of availability between all the markets we operate in with a large database that is updated live with all its availability. The decentralization of our loyalty allows for scale and the ability to give ownership and loyalty earning ability back to users while creating new ways for brands, providers and companies can engage customer’s loyalty.

The power behind InterValue is the INVE digital token. All activity in the network revolves around INVE, from serving as the primary form for fees and collaterals, serving as the main currency used for purchasing experiences, goods & services, predicting & rewarding loyalty. INVE is the driver of a sustainable economy where

demand grows as more users and providers join the ecosystem.

### 9.2.4. Asset Dividend Trading Block Chain

Based on the block chain technology, we are going to realize the block chain ecosystem of asset dividend trading. We provide a safe and convenient trading platform for assets to enable asset owners to raise funds through assets. Buying assets to gain or adding value to the assets obtain a bonus.

The system operators provide the due diligence to the assets value, legitimacy and profitability of the whole system, and it realize the transaction of the rights of dividends through the packaging, listing and up chains of high-quality assets. We use block chain to issue digital currency for asset trading. Transactions can be carried out between asset owners and asset investors, or between investors.

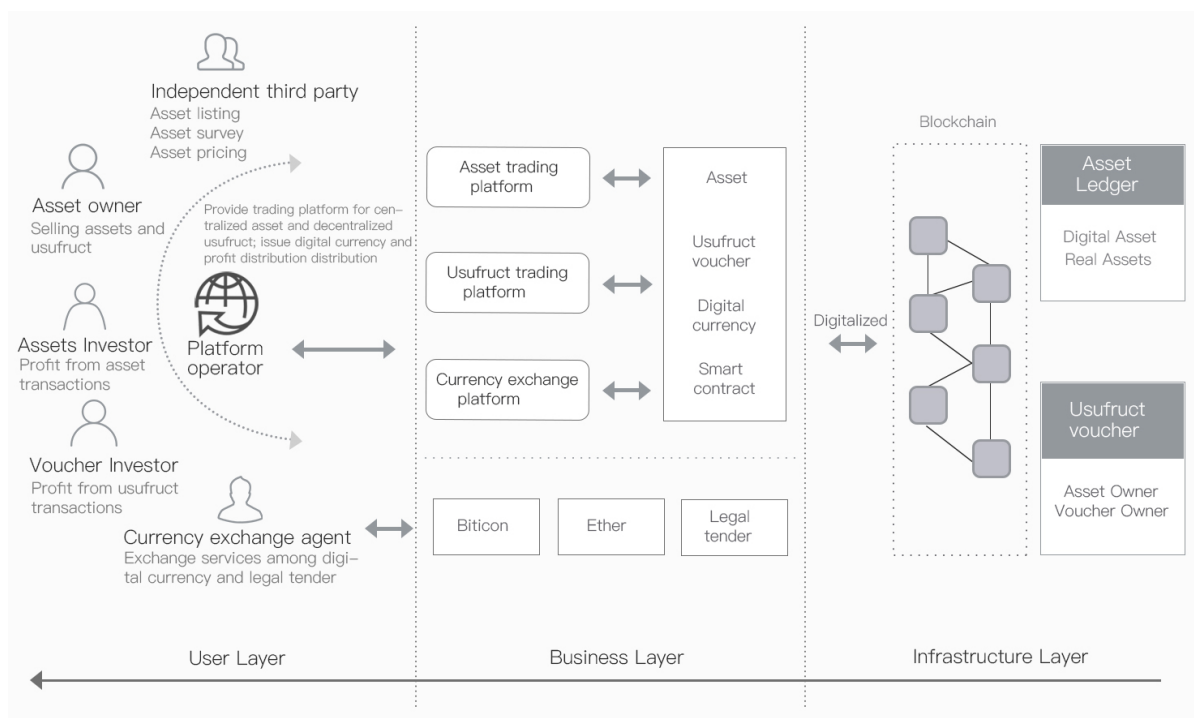


Figure 9-2: The Ecological of Asset Transactions

- Role division

- ◊ The asset owner: listing assets and selling assets to raise funds. After the assets are listed, the corresponding bonus rules will be announced. Once assets are sold, it is equivalent to signing smart contracts by the two sides according to the rules, and promoting automatic execution when conditions are triggered.
- ◊ Listing agencies: equivalent to the market maker, the assets of the owners should be listed on the chain of assets to perform the due diligence, to release the profit and appreciation of assets. They have a lower extraction of asset transactions to support the due diligence.

- ◊ Assets block chain: the information on the block chain can not be manipulated. The smart contracts are implemented to give asset dividends and asset trading.
  - ◊ Asset investors: they use idle capital to invest in assets to gain dividends, or to profit by asset appreciation.
  - ◊ Miners: they provide the computing and storage resources for digital currency incentives.
  - ◊ Digital currencies investors: they profit by hoarding and trading digital currencies.
  - ◊ Digital currency trading platform: they offer intermediaries for digital currency transactions to realize digital currencies.
- Smart contracts

We use a Turing complete high-level language as an implementation of the smart contract, which facilitates the implementation and verification of the contract's content by both parties. We quickly define and test smart contracts in the development environment of advanced languages. The bytecode compiled by a high-level language can also be encrypted to a certain extent for smart contracts. The execution of the contract requires the environment of the advanced language. Only using the block chain storage and smart verification of a contract, the contract is executed by block chain contracts in the proxy server to the proxy server, after verification of the contract as a node block chain for smart agents and provide contract execution environment. the contract is only the code to achieve. The proxy server receives external data and transmits the data to the dynamic loading contract code, or runs the contract code according to the time node provided by the contract itself, and the contract can access the external public data during the operation.

In the asset trading system, smart contract also provides for the asset investments before trading and the asset owners signing smart contracts. The investment shall have the right to opt out of the assets sold to property owners.

- Asset trading process

The asset transaction solution based on block chain can store user data and transaction data in the asset trading market, to solve the problems of no center, transparent transactions, and trust and so on.

- Share out bonus process

The block chain adopts the smart contract to solve the problem of automatic dividends. When the asset parameters conform to the dividend conditions, the part of the assets in the asset owner's account is allocated to the account of the asset investor as dividends.

# 10

## Cross-chain Communication and Multi-chain Merging

### 10.1. Introduction of Cross-chain Technology

Existing Blockchain projects cannot effectively serve commercial applications. One reason is that the capacity of Blockchain is limited and the speed of transaction confirmation is very slow, and the other important reason is that a single Blockchain project is an isolated value network. The problem of network isolation extremely restricts the potential of block chain technology, as the interoperability between existing block chain projects is hard to implemented. As a Blockchain project aiming at the interconnection of value, InterValue realizes not only the interconnection of value between its users but also the interconnection of value between existing block chain projects. The goal of InterValue is to change the status that each Blockchain project is independent and realize the ubiquitous interconnection of value eventually.

Cross-chain communication is becoming a hot topic in the research of Blockchain. There exist three cross-chain technologies: Notary schemes, sidechain/relays and hash-locking. In Notary schemes, a group of credible nodes act as notaries to verify whether a specific event has happened on Blockchain Y and prove it to the nodes of Blockchain X. Interledger proposed by Ripple Lab is a representative of Notary scheme. If Blockchain X enables to verify the data coming from Blockchain Y, Blockchain X is called a sidechain. Sidechains are usually based on tokens anchored on a certain blockchain, while other Blockchains can exist independently. Existing sidechain projects are unable to construct cross-chain smart contract and support all kinds of financial functions, which is the reason that these Blockchain projects fail to make progress in the realms of stock, bond and financial derivatives markets. The famous bitcoin-sidechains include BTC Relay (proposed by ConsenSys), Rootstock and ElementChain (Proposed by BlockStream), and the other sidechains, not for Bitcoin, include Lisk and Asch. Relay chain technology temporarily locks a number of tokens of an original Blockchain by transferring them to a multi-signature address of the original Blockchain, and these signers vote to determine whether the transactions happen on the relay chain are valid or not. Polkadot and COSMOS are representative relay chain technologies. Hash-locking

is a mechanism to carry out payment by locking some time to guess the plaintext of a hash value, which derives from Lightning Networks. However, hash-locking supports a limited number of functions. Although it supports cross-chain asset exchange and cross-chain asset encumbrance in most scenarios, it is not usable for cross-chain asset portability and cross-chain smart contract. The comparison of these three cross-chain technologies is shown in Table 10–1.

Table 10–1: The comparison of cross-chain technologies

| Cross-chain technique                    | Notary schemes                                      | Sidechain/Relays   | Hash-locking                             |
|--|---|--|--|
| Interoperability types                   | ALL   | ALL (If relays exist on both chains; otherwise one-way causality only) | Cross-dependency only                    |
| Trust model                              | Majority of notaries honest                         | Chains do not fail or get "51% attacked"                               | Chains do not fail or get "51% attacked" |
| Usable for cross-chain exchange          | YES   | YES  | YES                                      |
| Usable for cross-chain asset portability | YES (but requires universal long-term notary trust) | YES  | NO                                       |
| Usable for cross-chain oracles           | YES   | YES  | Not directly                             |
| Usable for cross-chain asset encumbrance | YES (but requires long-term notary trust)           | YES  | In many cases, but with difficulty       |

## 10.2. Full-node Adapter Multi-chain Merging

Existing projects focus on how to improve trading throughput and speed, but ignore the platform lock-in problem. For example, Alice and Bob have installed the bitcoin client application, and they can only transfer bitcoins in the bitcoin Blockchain. If they want to transfer eth, the eth client application needs to be installed for both Alice and Bob. This platform lock-in problem causes inconvenient switching among different chains, which impacts user experience. Besides, to use multiple public chains simultaneously, users need to equip servers with high memory and storage, which cost much money.

InterValue adopts Full-node adapter multi-chain merging technique to connect different Blockchains. Specifically, as the unified entrance, InterValue uses the full node merging adaptor to trigger the transactions on the external subnet (BTC, ETH) . The local full node network is composed of an external subnet and an internal subnet. The external subnet mainly includes other chain networks, such as BTC, ETH and so on. The internal subnet mainly includes the piecewise network of InterValue. The top-level network is mainly composed of higher nodes of all nodes.



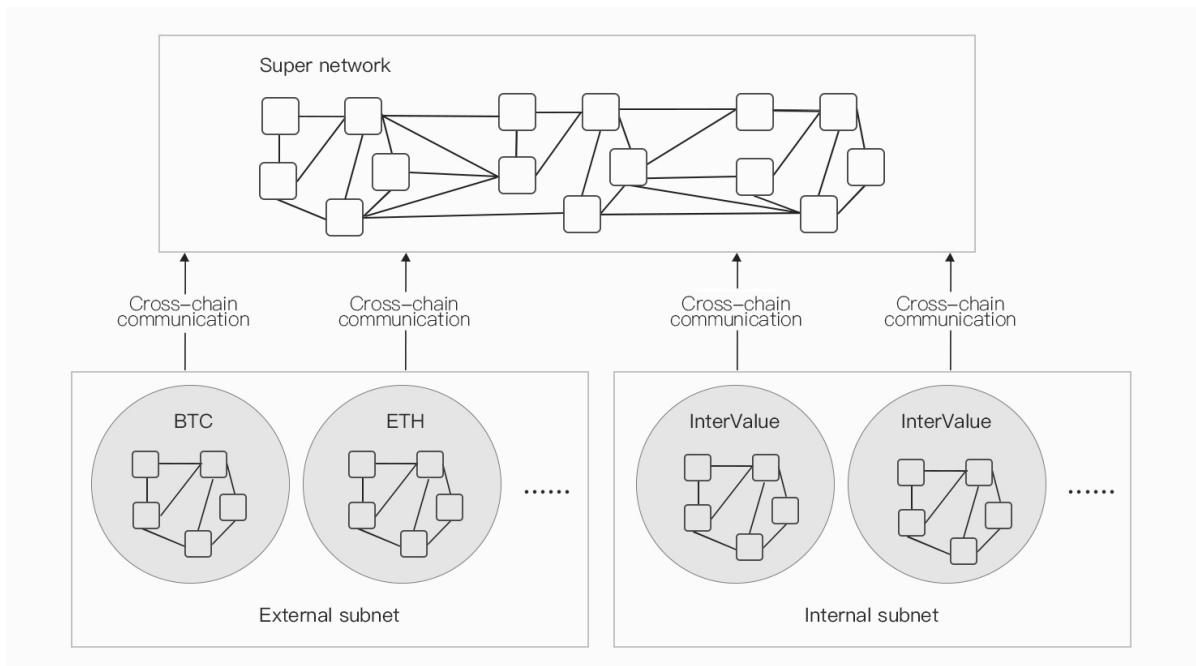


Figure 10-1: Full-node Adapter Multi-chain Merging

We deploy the multi-chain merging module to the full node, which acts as the transaction proxy on the external subnet (BTC, ETH). In the early stage, InterValue will support the proxy transaction among Bitcoin and Ethereum. Take Bitcoin proxy transaction as an example, the transaction information is shown as follows:

```
[ "cross chain transaction", [
  [ "InterValue", [ "Alice", "Bob" ] ],
  "targetchain": "BITCOIN",
  "txproxy": {
    "txid": "TRANSACTION HASH IDNEX",
    "version": 1,
    "locktime": 0,
    "vin": [
      { "txid": "UTXO HSAH INDEX",
        "vout": 0,
        "scriptSig": { "asm": "ASM STRING VALUE",
                      "hex": "HEX STRING VALUE":
                      },
        "sequence": SEQUENCE VALUE,
      }
    ],
    "vout": [
      { "value": 0.5,
        "n": 0,
        "scriptPubKey": { "asm": "SCRIPT CODE",
                          "hex": "HEX STRING VALUE",
                          "reqSigs": 1,

```



```

        "type": "pubkeyhash",
        addresses: [ "Bob" ]
    },
    ....
]
]]

```

If we want to support the proxy transaction of Ethereum, the only thing need to do is to change the domain of txproxy.

Note that, to implement the multi-chain merging, users of InterValue have to register accounts on the other public chains. When a user wants to trade in the other chains, he/she selects the target chain, inputs the transaction value, and launches the proxy transaction. After the proxy transaction is confirmed in InterValue, the full node obtain this transaction, extracts the information from the txproxy domain, broadcasts the transaction in the target chain. Thus, InterValue completes the proxy transaction and achieves multi-chain merging.

### 10.3. Cross-chain Communication

InterValue is not only a self-contained Blockchain network but also a bridge to support cross-chain communication functions, such as cross-chain asset exchange and cross-chain asset portability. By using InterValue platform, anyone can develop financial applications in accordance with the requirements of application scenarios. The basic idea of the InterValue cross-chain technology is adopting relay chain thoughts and implementing the cross-chain communication module as a full node overlay layer over the basic chain of InterValue. In this technology roadmap, we not only keep the independence of cross-chain interoperability but also reuse all kinds of functions offered by the basic chain of InterValue.

The cross-chain communication module of InterValue includes three types of nodes: verification nodes, block-aware nodes and merging nodes. Their respective functions are listed as below:

- The verification nodes are the notary nodes in the basic chain of InterValue. They verify the validity of data coming from some original Blockchain and construct new blocks in InterValue. The verification nodes have to mortgage enough asset to guarantee that they will do their jobs loyally.
- The block-aware nodes help the verification nodes to gather valid cross-chain communication block. These nodes, similar to the miners in PoW, run a full client of some original Blockchain, construct new blocks and execute transactions. After receiving cross-chain transaction request blocks, the block-aware nodes pack these request blocks and send them to the verification nodes.
- The merging nodes act like the gateway between InterValue and other original Blockchains. Each merging node has two queues which respectively handle incoming transactions and outgoing transactions. In addition, the merging

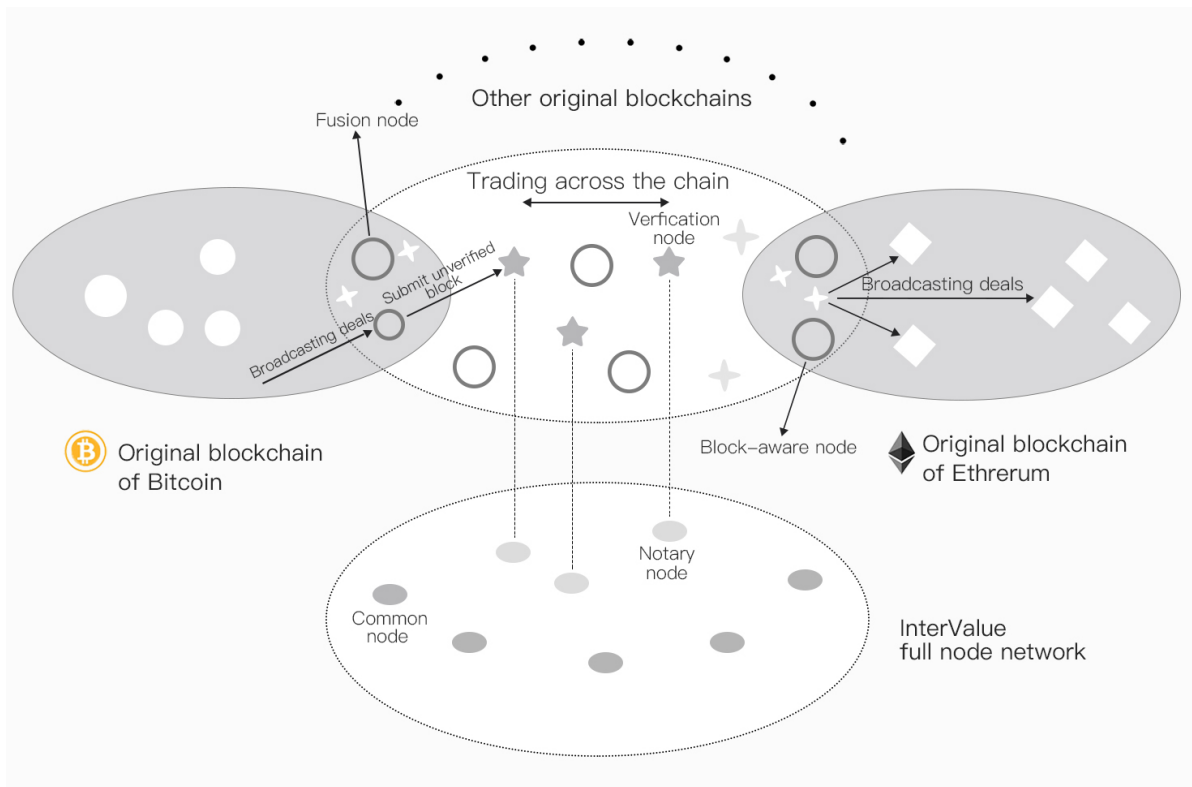


Figure 10-2: InterValue Cross-chain Technology

nodes should have some tokens of original Blockchains and support cross-chain oracle.

## 10.4. Cross-chain Asset Exchange

To clearly explain the process of cross-chain asset exchange, we take the exchange of Bitcoin and Ethereum as examples. Suppose that Alice wants to convert 1 BTC to 10 ETH. Meanwhile, Bob wants to convert 10 ETH into 1 BTC. The asset exchange between Alice and Bob is shown as follows:

- (1) Alice sends her 1 BTC to a multisig account of the relay chain of InterValue.
- (2) The block-aware node of bitcoin chain is responsible for monitoring the cross-chain communication. After the block-aware node captures the block containing the transaction of Alice, it packs the block header to a new unverified block, and sends the new block to a verification node.
- (3) After the verification node receives the new block, it verifies whether the block has been committed by the bitcoin chain. If yes, the verification node generates a new contract and write it to the relay chain of InterValue.
- (4) Bob sends his 10 ETH to a multisig account of the relay chain of InterValue.
- (5) The block aware node of Ethereum chain captures the block containing the transaction of Bob. Then it packs the block header to a new unverified block, and sends the new block to a verification node.
- (6) After the verification node receives the new block, it verifies whether the block has been committed by the bitcoin chain. If yes, the verification node gen-

erates a new contract and write it to the relay chain of InterValue. Meanwhile, the verification node checks whether there is a matching request with Bob, and it finds Alice's request.

(7) The verification node generates two new contracts. One is "sending 1 BTC to Bob's BCT account. The other is "sending 10 ETH to Alice's eth account". The two contracts are sent to the queue of the merging node of the bitcoin chain and Ethereum chain, respectively.

(8) The merging node of the bitcoin chain and the Ethereum chain read their corresponding queue, and send 1 BTC and 10 ETH to Bob and Alice, respectively. Thus, the cross-chain asset exchange completes.

## 10.5. Cross-chain Asset Transfer

To clearly explain the process of cross-chain asset transfer, we take the transfer from bitcoin to Ethereum for an example. Suppose that Alice wants to transfer 1 BTC to Bob's eth account. The asset transfer from Alice to Bob is shown as follows:

- (1) Alice sends 1 BTC to the merging node of the relay chain of InterValue.
- (2) The block-aware node of bitcoin chain captures the block containing the transaction of Alice, it packs the block header to a new unverified block, and sends the new block to a verification node.
- (3) After the verification node receives the new block, it verifies the block containing the transaction of Alice has been committed by the bitcoin chain.
- (4) Based on the cross-chain oracle, the merging node of bitcoin chain exchanges 1 BTC to the corresponding INVE. Then the merging node of bitcoin chain sends the INVE to the merging node of Ethereum chain by the backbone of InterValue.
- (5) The verification node of InterValue verifies the transaction between the merging node of bitcoin chain and the merging node of Ethereum chain.
- (6) Based on the cross-chain oracle, the merging node of Ethereum chain exchanges the received INVE token to the corresponding ETH token and sends the ETH token to Bob.

## Team and Planning

### 11.1. Foundation

InterValue Foundation is a non-profit organization. Through the establishment of related departments, the Foundation is committed to the development of InterValue and manages the open source, community construction and deliberations of InterValue improvement. Moreover, to make the project run better, the Foundation is also committed to the finance, team building and external relations.

The organization structure of InterValue Foundation is shown in Figure 11–1.

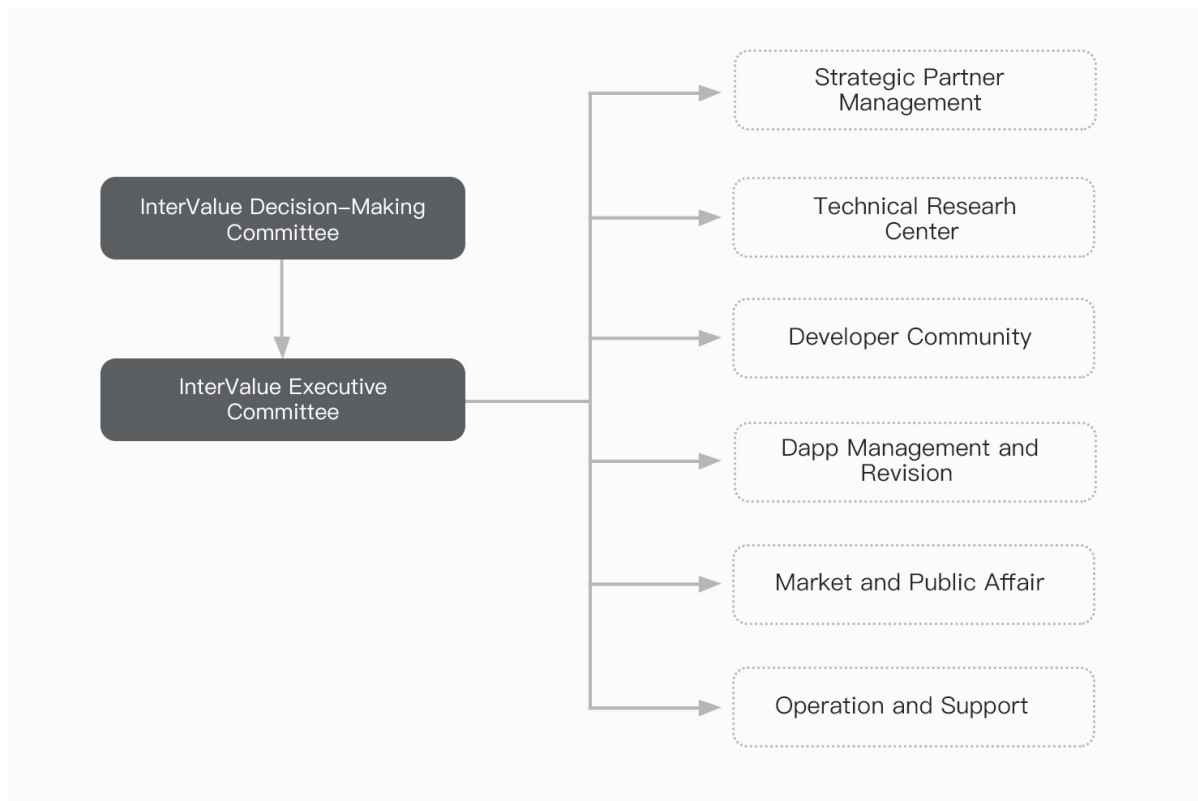


Figure 11–1: The Organization Structure of InterValue Foundation

- **InterValue Decision-Making Committee:** It is responsible for the management and decision-making of major issues, including the development of important strategic directions of InterValue, the appointment and dismissal of executive committee members, the election of the Executive Committee leader and the heads of the departments. Members of this committee are appointed for a term of three years and can be re-elected, and the committee has a chairman. The first members of the decision-making committee will be voted by the InterValue founding team and committee representatives, which takes annual rotation.
- **InterValue Executive Committee:** It is responsible for managing the work of each department, such as building open platform of consuming-serving network, defining rules of supervision, decomposing the objective of the decision-making committee, executing and supervising the work of each department. The detail responsibility of InterValue executive committee is show as follows:
  - ◊ **Strategic Partner Management:** Managing strategic partners and co-ordinating partner resources.
  - ◊ **Technical Research Center:** Responsible for the development of underlying technology protocols, blockchain system design and development, testing, iteration, standards development, etc.
  - ◊ **Developer Community:** Providing developers with education, training, technical support and other services. At the same time, it runs the community to provide a platform for development and communication.
  - ◊ **DApp Management and Audit:** Responsible for auditing all DApps that have joined InterValue to ensure DApp compliance on the InterValue platform, which is conducive to platform ecosystem health.
  - ◊ **Market and Public Affairs:** Including market development, user nurturing and management of public affairs.
  - ◊ **Operation and Support:** Including management of four more departments, such as finance, legal, personnel and administrative departments. The financial department is responsible for finance use and review, legal affairs is responsible for the foundation's compliance, as well as the preparation and review of various documents, to prevent possible various types of legal risks, and administrative and personnel departments are responsible for personnel, salary and daily administrative work.

## 11.2. Team Member

If new team members join us later, we will update this list below.



Barton Chao

CEO, deputy director of Xidian University blockchain application and test laboratory, distinguished researcher of Zhejiang University blockchain research center. Blockchain industry practitioner, Ph.D., Senior expert of P2P, cryptography, network security and Blockchain.

He is a pioneering developer of Blockchain since 2009. His main work contains researching underlying technologies of Blockchain, combining block chain with industry, and applying Blockchain technology in actual application scene. Since he has planned and developed a number of Blockchain related projects, he has profound understanding and rich practical experience of the technical principle of the blockchain, the underlying technology, the middle-layer protocol, applications on the chain, application scenes, development trends and etc.



Leo Cheung

CTO, Ph.D., Visiting scholar of Hong Kong University Science & Technology. His main research areas are P2P computing, efficient management of big data, intelligent analysis, deep learning and etc. He has published over 30 high-level papers, 4 monographs and has led and participated 10 high-level scientific research projects. He has been engaged in structure design of P2P system and has deep understanding of the double layer structure of P2P topology.



Xinwen Jiang

The Scientist of InterValue, Professor at the Computer Science Department of the National University of Defence Technology (China) and at the Computer Engineering Department of Xiangtan University (China). His research mainly focuses on computational complexity and cryptographic algorithms. He has presided China's National Sciences Foundation as well as five other national-level organizations and participated in over 10 major national-level scientific projects. He won one first-prize, two second-prizes, and one third-prize at China's Ministry of Science and Technology Awards, published two books, one thesis and more than 40 research papers in scientific journals. His work on the most fundamental and complex problem in cryptography, "P versus NP", brought some progress and received a lot of attention.

His long-term lectures include, among others, "Computational Complexity", "Applied Cryptography", "Mathematical Logic", "Algorithm Design and Analysis". In parallel of teaching, he explored the practice of discipline-building and the theory of education principles, obtaining awards for his achievements at national-level. He has published nearly 10 research papers about teaching in journals such as Computer Education. He received the Military Talent award twice.

|  |   |
|--|---|
|  <p>Roger Max</p>     | <p>Chief architect, Ph.D., is dedicated to distributed computing, cloud computing, and machine learning. He has published over 20 high level papers at home and abroad. In the area distributed computing, he has a deep understanding to the scalability, reliability and elasticity of distributed systems. In the area of blockchain, he has a deep understanding and practical experience to the blockchain principle and technology.</p>   |
|  <p>Jason Loong</p>   | <p>CSO, Ph.D. in Computer Science and Technology, Senior expert of Blockchain, Machine Learning and Network Security. He has a deep understanding of smart contracts, active learning and deep learning. He hosted and participated in more than 10 scientific research projects including the National Natural Science Foundation and Provincial &amp; Ministerial Level research. Besides, he published more than 30 academic papers indexed by SCI and EI.</p>   |
|  <p>Andy Tang</p>    | <p>InterValue Eco Construction Leader, Ph.D., main research direction for machine learning, intelligent information processing, information systems, has published more than 10 papers. It has long been engaged in large-scale information systems and distributed application development, and has rich experience in product and complex system design. Since 2015, he has been engaging with BlockChain technology and BlockChain related application, and has a deep understanding of the blockchain ecosystem.</p>                  |
|  <p>Storm Zhang</p> | <p>Master of engineering, senior programmer, Blockchain tech expert. He has worked in IBM's System Technology Department and Sina's Big Data Department for many years, and has extensive Hadoop and Map Reduce development experience. he was exposed to Bitcoin since 2013, and he is familiar with the principle of cryptocurrency and the store docking program for the Exchange Wallet. He is the Go technical director of Renrenbao. Currently, he is focusing on the direction of smart contracts and Blockchain applications.</p> |





Scott Guo

CMO, He worked for VIEDA, Red Net, Alibaba and Tencent as Marketing Director. 14 years experience in Internet product and service operations. Over the past ten years, has been committed to the Internet and big data and intelligence in the field of research and applications. In the past 10 years, he has been in charge of and participated in large-scale system development projects such as government and large enterprises. He has strong government and large enterprise service and cooperation experience.

He is responsible for the company's overall brand planning and marketing department organization. He is skilled in grasping market opportunities, maintaining market sensitivity, rationally deploying internal and external relationships. He is responsible for formulating, controlling, adjusting and amending strategies. Basing on the company's brand positioning and industry characteristics, He proposes an innovative cooperation method that is different from the traditional model and ultimately implements it in a rational and effective manner.



Isda Chen


Investor Relations Leader, Master Degree. Worked for AVIC International Holding and Youe Data as company's representative both oversea and domestic. Build connection with local governments and develop market. Develop and implement several government's projects. Recently, dedicate himself to Big Data and Blockchain industry. With an international vision and profound experience in government cooperation.



## 11.3. Project Consultant

Project Consultant List will be continuously updated.

|   |   |
|---|---|
|  <p>Allen Wu</p>       | <p>Mr. Wu has accumulated rich experience in software product development, technology research and development, and team management. He has served as one of the main leaders of the Product Technology Committee of Alibaba Group and Chief Architect of Yahoo China. Prior to this, he was involved in leading a number of system software, e-commerce, and mobile Internet projects at IBM, Silicon Valley, and Beijing Internet Corporation. At the same time, he is also a senior expert in artificial intelligence algorithms, NPL, and distributed databases.</p>  |
|  <p>Daxue Li</p>      | <p>Mr. Li has the unique grasp and fruitful experiences of the technology and operation of the Internet. Experts at technical architecture design and technical team management. He joined JingDong's technical research and development system in 2008 and let JingDong's business achieved 10,000 times growth times according to development of technology. In 2015, he founded Magcloud Digital Technology, let the company became a technology finance company with a core of blockchain, and became an industry leader quickly.</p> <p>In 2005, he was rewarded as "National Model Worker" by State Council; In 2012, he honored as "Zhongguancun Leading Figures"; In 2014, he honored as "2014 the Most Famous CTO"; In 2016 he was selected "Leading China Big Data Industry Process 100"; and honored "Most Technical Leader" by China Internet Weekly in 2017.</p> |
|  <p>Zongbin Wang</p> | <p>Principal Consultant in the Blockchain Industry, former Associate Professor of the Renmin University of China. He studied at the Berkeley University Business School in California from 1995–1998. He Cooperates with local governments all the year round to build a public service platform for nine industrial clusters such as aviation, automobile, rail transportation, petroleum equipment, titanium and machine tools. Moreover, he builds a public service platform for about 20 industrial parts.</p>  |

|   |   |
|---|---|
|  <p>Zhiqi Han</p>  | <p>Mr. Han is the Member of the Beijing Youth Entrepreneurs Association, UCSI MBA. He founded Stanley Ventures in 2007 and has served many domestic large-scale Internet companies, such as Sohu, Sina, and Fenzong. He helped complete multiple mergers and acquisitions. As one of the earliest FA organizations in China, He successively served the financing of a number of Internet companies, such as Tuniu Tourism, Jiamei Dental, Lvchuang Environmental Protection, etc., and the total amount exceeded 100 million U.S. dollars. From 2013, Mr. Han started to invest in digital currency, and had engaged in more than 50 Token projects, such as EOS, Kyber Network, Raiden Network, SmartMesh, MeshBox, Status, Bluzelle, Tezos, Nebulas, Tenx, 0x and so on.</p>   |
|  <p>Leo Li</p>     | <p>Founding Partner of Whales Capital. Leo received his Ph.D. degree in microelectronics from Chinese Academy of Sciences and a bachelor's degree in Biomedical engineering from Beihang University. He previously worked for China Development Bank Venture Capital, Tsinghua Holdings Capital, Prometheus Capital and Delong Capital. Leo accumulated extensive experiences in the past ten years in private equity investment. He is mainly focusing on TMT and Blockchain.</p>  |
|  <p>Bill Dai</p> | <p>Partner of Beijing DeTai JiuFang Assets Management Center and Assistant to President of Jide Holding Co., Ltd. Director of Zhongguancun Private Equity Association. He was the executive director of Wuxi Aerospace High-Energy Internet Equity Investment Fund, the vice president of Beijing Junyuan Capital Management Co., Ltd. and the chief investment officer of Datang Huayin Electricity Co., Ltd. He has more than 10 years of investment and management experience and is proficient in private equity investment and industrial investment. He is familiar with securities investment and corporate finance, understands investments in real estate, futures and financial derivatives, and is familiar with strategic management of companies and the management of listed companies and small enterprises.</p> |
|  <p>Wenli Su</p> | <p>He worked in a big investment bank in North America with merger and reorganization of enterprises over ten years. He has rich experience in acquisition of listed companies, hostile takeover, asset acquisition, corporate debt restructuring, and value assessment of company and asset. He personally dominated and participated in a number of ten billions of merger cases. As a supporter of block chain, Mr. V has involved in a number of block chain projects.</p>  |



Yugui Wang

He is a current supervisor of Minsheng Bank and has been a non-executive director since Minsheng Bank's establishment. He was the general manager of the China Shipowners Mutual Assurance Association and led the company to become the world's largest company and a founding shareholder of Minsheng Bank. He used to serve as executive director of China Maritime Law Association, China Service Trade Association, director of Minsheng Securities Co., Ltd., supervisor of Haitong Securities Co., Ltd., and arbitrator of China International Trade Promotion Committee Maritime Arbitration Commission. Mr. Wang was a director and supervisor of China Everbright Bank and a part-time lawyer of Beijing Jingwei Law Firm.



Weiye Hu

Managing director of China Merchants Securities Investment Bank.



Lizhi Ran

Founder of Roots Capital, 2015 Zhongguancun outstanding angel investor, member of Zhenghe Island. He has been involved in venture capital and private equity investment for more than 10 years. He served as executive vice president of Qingke Group and managing director of Qingke Capital which is the investment banking department of Qingke Group. Qingke Group is a Chinese famous integrated service provider in VC/PE area. He has participated in nearly 20 investment and financing transactions for internet companies (e.g., Baihe Network, Ganji Network and Siku Luxury, etc.) and established several companies, such as Amovo magic kiss chocolate brand and Business State. After building Qiyuan Captital, He led the investment of tens of companies, such as Xiaoneng Technology, SENSORO Yunzi, Redu Medium and Yami, etc. He is also the director of many famous Pre-IPO internet companies (e.g., Siku Luxury ).

|  |  |
|--|--|
|  <p>Junmin Zhou</p> | <p>Co-founder of Deya Village Manangment Consulting (Beijing) Co., Ltd., Deputy secretary-general of Science and Technology Chamber of Commerce in Shanghai Federation of Industry and Commerce and chief of Blockchain special committee, 985 Shanghai Alumni Association co-founder. He has more than ten years of IT product development and management experience and eight years of financial investment experience in the fields of finance, communications and internet. He is a senior product manager and has worked in such well-known domestic IT companies as Beida Fangzheng and Baoxin Software and high-end think tanks such as the National Strategy Research Institute.</p> |
|  <p>Jun Sun</p>     | <p>Yalian Advisory Group President, senior consulting expert of financial management/senior lecturer of China Banking Regulatory Commission Training Center. He has worked for major domestic financial institutions and international famous standardization organizations and has led his team to successfully provide advisory and training services to regulators and nearly one hundred financial institutions. He has also participated as lecturer in many training sessions of process banks and new capital conventions held by China Banking Regulatory Commission. He is one of the main drafters of multiple regulatory guidelines of China Banking Regulatory Commission.</p>   |
|  <p>Hui Wang</p>  | <p>Zhong Yu Capital co-founding partner, chief risk control officer. He is an independent director of Huajing Securities, an expert member of the Economic Responsibility Auditing Professional Committee of the Beijing Institute of Certified Public Accountants, and a member of the Beijing Institute of Certified Public Accountants. He used to be a partner of Reanda Certified Public Accountants, financial controller of NASDAQ listed company, and director of China Huajing Electronics Group.</p>   |
|  <p>Bruce Lee</p> | <p>Founding partner and CEO of BenRui Capital. He has many years of experience in investment and management. He has a strong understanding of private equity investment and secondary market securities. He has been involved in the financing of many major Internet companies. He has known Bitcoin since 2010 and has helped fund several blockchain and mining projects since 2016.</p>  |

## 11.4. Consultant Institution

Strategic Partners List will be continuously updated.

- **Roots Cap:** China's leading angel investment fund which focuses on emerging technology industries such as big data, finance, consumer upgrades, enterprise services, intelligent hardware (VR / AR), big creative writing and big health. It has successfully invested in dozens of early VC projects, involving big data, e-commerce, intelligent hardware, online travel, consumption upgrade and cultural entertainment, etc., of which 80% of the projects receives a new round of investment.
- **BenRui Capital:** Initiated and established by blockchain industry technical experts, professional investors, and VC/PE practitioners, focusing on technology-driven investment in the blockchain field.
- **Whales Capital:** A professional Venture Capital fund which mainly focuses on Blockchain. Seeking companies or projects with big market, leading technology and talented team. Believe in value investment and empowerment investment.
- **Genesis Capital:** Focusing on the block chain industry and committed to mining the best projects in early stage. It is one of the TOP 5 crypto currency funds in China. It has already invested around 50 blockchain-related projects.
- **Obsidian Capital:** European famous venture capital institution.

Other strategic partners include: Crypto Laboratory, OK Crypto, Bitcoin Capital, EYU Capital, Reflexion Capital, Hello Capital, Starwin Capital, Skyline Capital, Cloud Chain Capital and so on.

## 11.5. Roadmap

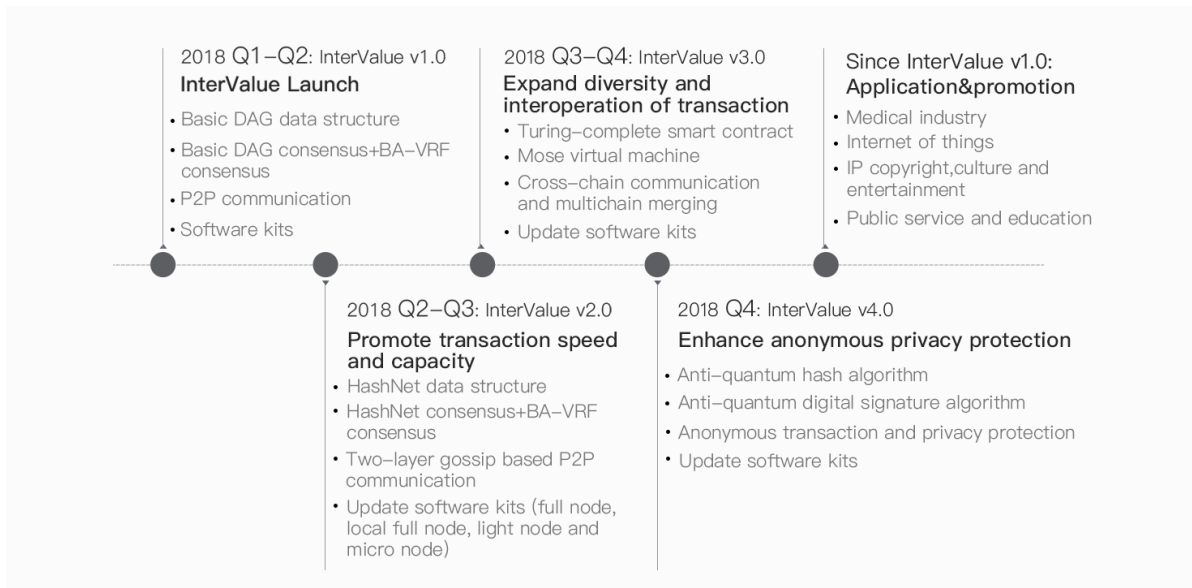


Figure 11–2: Roadmap

The roadmap of InterValue consists of two phases: development phase and pro-duction phase. After four times of iterative upgrade in the development phase, InterValue will be shaped in accordance with our vision and enters into the pro-duction phase.

2018 Q1–Q2: We will release InterValue 1.0 and its software kits. This ver-sion supports DAG mining, double consensus, anonymous P2P communication and smart contract.

2018 Q2–Q3: We will release InterValue 2.0 by changing the DAG graph of previous versions into HashNet, which will promote the capacity of InterValue and increase the transaction speed to hundreds of thousand TPS.

2018 Q3–Q4: We will release InterValue 3.0 which develop Turing’s complete smart contracts, implement cross-chain communication and multi-chain conver-gence on the basis of version 2.0.

2018 Q4: We will release InterValue 4.0 and its software kits. This version is highlighted by quantum-attack resistance by replacing the signature algorithm and hash algorithm in the previous version, it also supports anonymous privacy protection based on zero-knowledge proof and ring signature.

From the releas of InterValue 1.0 in 2018, we will apply InterValue platform in some application scenes, such as medical industry, internet of things, IP copyright, culture and entertainment, public service, education and so on. We will explore the application of InterValue with the community and expand its application areas.

# 12

## Token

### 12.1. Token Utility

InterValue aims to build a comprehensive and full-featured Blockchain 4.0 underlying technology platform, which supports commercial organizations and governmental agencies to construct public Blockchain, consortium Blockchain and private Blockchain to satisfy their respectively business features and requirements. In order to support public Blockchain, InterValue introduces token policy in the incentive layer to realize flexible consensus schemes. The built-in token named INVE stimulates the community to maintain the public Blockchain of InterValue and develop DApps, and then it increases the value of the public Blockchain of InterValue and promotes InterValue's network effect. In the public Blockchain of InterValue, the utilities of INVE tokens are listed as below:

- Stimulating the majority of users to trade their asset in InterValue network to earn transaction fees and notarization fees, which improves the security of InterValue network; Supporting mining by rewarding transaction nodes and notary nodes;
- Used as equity measurement to realize the double consensus architecture proposed in InterValue: Basic DAG consensus and BA-VRF consensus in the early development phase; HashNet consensus and BA-VRF consensus at a later stage;
- Supporting the ecosystem of InterValue to realize advanced smart contract, which supplies anti-fraud schemes to prevent “logic bomb” from influencing network effect;
- Playing the role of base currency in the ecosystem of InterValue, which endows the tokens of DApps with corresponding features and lays foundation of asset liquidity;
- Acting as escrow fees to manage DApp of the public Blockchain of InterValue and improve the popularity of DApps;
- Used to develop additional network functions and improve the scalability of the platform.



## 12.2. Token Issuance

INVE is the abbreviation for the base token of InterValue, and it is equal to  $10^{18}$  Atom, that is,  $1 \text{ INVE} = 10^{18} \text{ Atoms}$ . Atom is the smallest unit of INVE token, and it will be used as the transaction fee for advanced smart contract and smart contract based cross-chain transaction.

The total amount of INVE token is 10 billion, of which 6 billion is issued as mining reward through DAG mining and the rest is reserved for foundation, project development, project promotion and team building. Of 2.6 billion that were used to create foundations, 2 billion were ecological construction funds, which is used for InterValue's eco-investment; the remaining 600 million were INVE funds, which aims to ensure the normal operation of the Foundation's work. The project fund-raising is planned to launch on Ethereum in Q1 2018, and the issued ERC20 tokens can be converted into INVE tokens at ratio 1:1 when the main chain of InterValue is officially launched. The arrangement of INVE overall distribution and reserve INVE Token distribution are shown in Figure 12-1.

INVE overall distribution

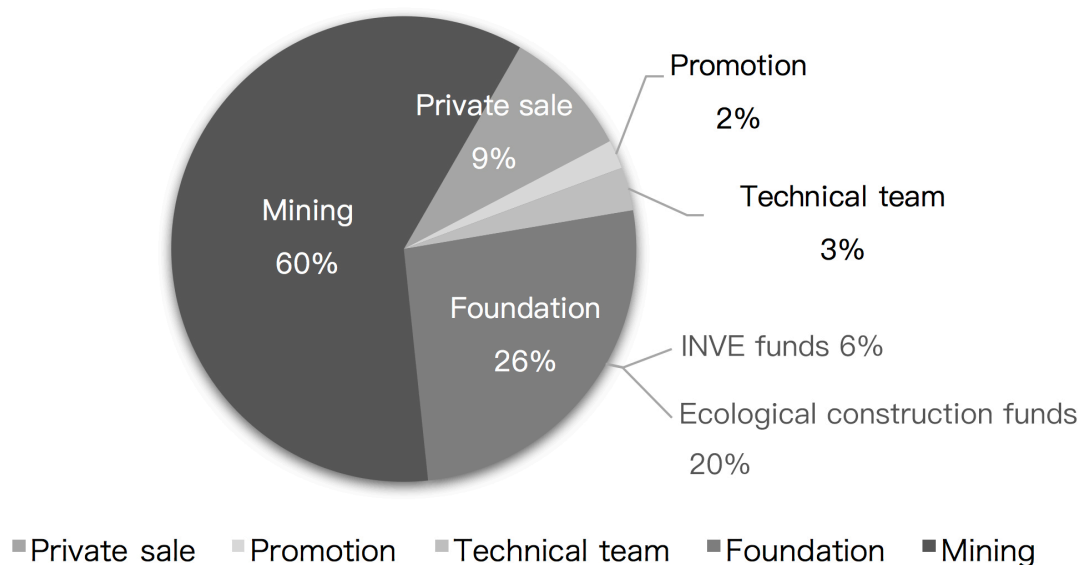


Figure 12-1: INVE Overall Distribution

Ordinary users need to send transactions through local full nodes. In order to prevent malicious users from having malicious DDoS attacks, an ordinary user has to perform a low-level POW calculation before initiating a transaction. After that, it submits the transaction to the local full node for processing. The local full node participating in the transaction confirmation verifies whether the hash of the transaction satisfies the mining difficulty. Once the transaction is verified and stabilized, the local full node which sends an event containing the transaction can obtain the corresponding number of INVEs as rewards. In order to reward the contribution of full nodes and local full nodes to the consensus of the entire network, 6 billion INVEs are generated by mining in a rewarding way. Meanwhile,



every time a normal user initiates a transaction, a certain fee will be incurred for the transaction. The beneficiary of the fee is the local full node that is responsible for the confirmation of the transaction. The upper limit of the fee is proportional to the size of the transaction, and the specific transaction fee is dynamically adjusted by the corresponding local full node.

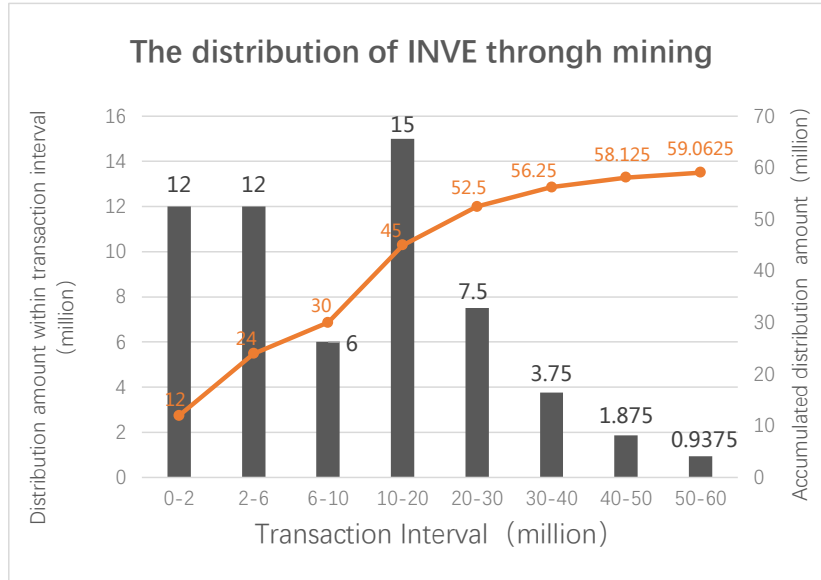


Figure 12-2: The Distribution of INVE through Mining Reward for the First 6 Billion Transactions

The 6 billion INVEs issued through the mining as reward is distributed to local full nodes and full nodes, and the reward decreases with increases of the batch number of transactions. The mining reward of a transaction is 6 INVEs when the transaction is included in the first batch (including the first 200 million transactions with total issuance volume  $S_1 = 1.2$  billion), 3 INVE tokens when the transaction falls into the second batch (the range is from the 200<sup>th</sup> million transaction to the 600<sup>th</sup> million transaction and the total issuance volume  $S_2 = 1.2$  billion) and 1.5 INVE tokens when the transaction falls into the third bath (the range is from the 600<sup>th</sup> million transaction to the 1<sup>st</sup> billion transaction and the total issuance volume  $S_3 = 0.6$  billion). The fourth batch and the subsequent batches are divided by every 1 billion transactions. The mining reward is 1.5 INVEs/transaction as in the fourth batch, and it decreases successively by a half in each of the subsequent batches. The distribution of INVE through mining (taking the first 6 billion transactions as an example) is shown in Figure 12-2.

$$\begin{aligned}
 \text{Total mining reward} &= S_1 + S_2 + S_3 + \lim_{n \rightarrow \infty} \sum_{i=4}^{i=n} S_i \\
 &= 3 \text{ Billion} + S_4 / (1 - q) \\
 &= 6 \text{ Billion} (S_4 = 1.5 \text{ Billion}, q = 0.5)
 \end{aligned}$$

The distribution of mining reward to local full nodes and full nodes takes the duty cycle of a responsible full node as a settlement cycle, which begins after the last event in the settlement cycle reaches the consensus confirmation. The initial allocation of mining rewards is based on the 80/20 Rule, which is written into the system contract as a parameter. The responsible full node collects all the information of transactions which are sent in its duty cycle, calculates the total mining rewards according to the distribution principle of mining reward mentioned above, and initiates consensus process in the full node network. 80

The setting of mining reward distribution cycle (divided by transaction number) comprehensively considers the advantage of the DAG chain data structure used by InterValue project in transaction confirmation speed and the project's post-development advantage (i.e., the acceptance of project concepts and community maturity).

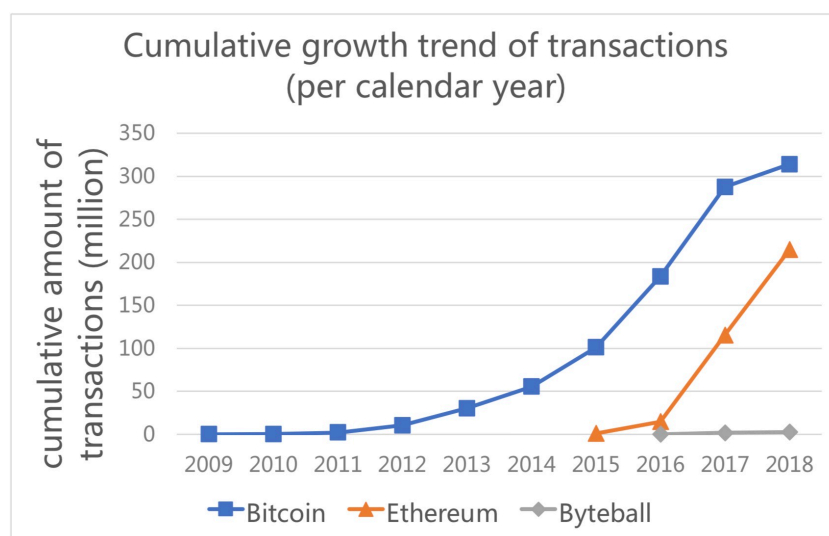


Figure 12–3: Cumulative growth trend of transactions (Bitcoin, Ethereum and Byteball)

- The advantage of transaction confirmation speed:** Without considering the advantage of post-development, the volume of transactions that the project can complete in a unit of time is mainly affected by the transaction confirmation speed. Bitcoin and Byteball are pioneering projects of single-stranded blockchain data structure and DAG chain data structure, respectively, and they have no post-development advantage in their respective blockchain technology categories. As shown in Figure 12–3, the cumulative growth of Bitcoin and Byteball transactions grew very slowly during the first three years after project launching, but the amount of transactions done by the Byteball project in the first full year was significantly higher than Bitcoin (As shown in Figure 12–4), which shows that using DAG chain data structure to improve the speed of transaction confirmation is conducive to improving the transaction volume of the project. Therefore, our InterValue project has an inherent advantage in increasing transaction volume.
- The advantage of post-development:** The post-development advantage of the project has a significant role in increasing transaction volume. As shown

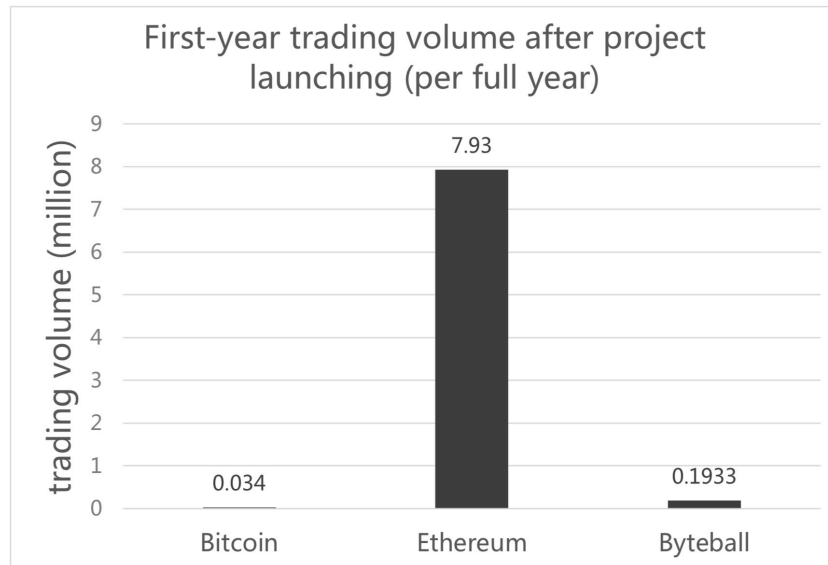


Figure 12-4: First-year trading volume after project launching (Bitcoin, Ethereum and Byteball)

in Figure 12-3, Ethereum, as the successor of Bitcoin, took advantage of the project's post-development advantage to achieve a growth rate comparable to Bitcoin in the first three years after project launching. In addition, in the first full year after project launching, the volume of transactions completed by Ethereum was far more than two orders of magnitude higher than the transaction volume of Bitcoin. Therefore, the post-development advantage of using DAG chain data structure leads InterValue having great potential for increasing transaction volume.

Taking into account the advantages of the above two aspects, with reference to the fact that Ethereum completed more than 200 million transactions in less than three years after project launching, we predict that our InterValue project is very likely to complete one billion transactions within one year after project launching.

# 13

## Business Status Quo

### 13.1. Technical Competition

- Bitcoin is the representative project of Blockchain 1.0. Its infrastructure, called Blockchain, is a distributed sharing account book to implement value communication in a peer-to-peer manner. The potential impact of Blockchain on finance and other industries may even be as good as the invention of double-entry bookkeeping.
- Ethereum is the representative project of Blockchain 2.0. It is an open-source fundamental system of Blockchain carried with smart contract. Hundreds of Dapps have been deployed on the Ethereum. However, the project like Cryptokitties shows the disadvantage of the transaction throughput and confirm speed of Ethereum.
- EOS is the benchmark product of Ethereum. Its ultimate goal is to become a blockchain operating system. It provides developers many basic functions, such as database, account privilege setting, execution schedule, authentication, network communication, and etc.
- IOTA is a cryptocurrency of IOT. To improve the transaction throughput of Blockchain, it designs DAG based distributed account book, called Tangle. Its goal is to achieve a global micropayment in the IoT industry.
- ByteBall is a decentralized system, and allows tamper-proofing storage for any data. The storage units of ByteBall connect with each other. Each of them contains one or more hash value of earlier storage units, which is used to confirm the earlier storage unit and build partial order among storage units. All the storage units form a DAG.

Table 13–1: Technical Advantage of InterValue

|                          | BTC                      | ETH                      | EOS                      | IOTA                    | ByteBall                             | InterValue  |
|--------------------------|--------------------------|--------------------------|--------------------------|-------------------------|--------------------------------------|---|
| Node Type                | Global Node, Light Node  | Global Node, Light Node  | Global Node, Light Node  | Global Node, Light Node | Global Node, Light Node              | Confirm Node, Full Node, Local Full Node, Light Node, Tiny Node |
| Anonymity of P2P Network | No                       | No                       | No                       | No                      | No                                   | Yes   |
| Consensus                | POW                      | Dagger POW               | DPOS                     | Weighted POW            | 12 Notary                            | HashNet BA-VRF  |
| Anti-quantum Attack      | No                       | No                       | No                       | Partial                 | No                                   | Yes   |
| Privacy Protection       | No                       | No                       | No                       | No                      | No                                   | Zero Knowledge Proof of Privacy Protection                      |
| Smart Contract           | No                       | Turing Complete          | Turing Complete          | No                      | Declarative Contract                 | Declarative Contract and Advanced Turing Complete               |
| Transaction Speed        | 7TPS                     | 30TPS                    | 3300TPS                  | 1000TPS                 | 100TPS                               | 1000000 TPS   |
| Price Scheme             | Transaction Fee & Mining | Transaction Fee & Mining | Transaction Fee & Mining | No Transaction Fee      | Transaction Reference & Notarization | Transaction Reference & Notarization & Mining                   |
| Application              | Few                      | Hundreds                 | Exploit                  | Exploit                 | Exploit                              | Massive applications in future                                  |

## 13.2. Company Competition

- **JingTong Technology:** It is a company of China in the research of the fundamental technology of the Blockchain. Its core team is composed of Blockchain engineers in silicon valley and China. In 2014, the company releases its fundamental platform for business applications. Until now, the company have developed a number of DApps in various fields, such as finance, travelling, smart city, logistics, medicine, and etc.
- **Ripple:** Ripple was founded in 2013. It provides the solution of global financial balance. The solution allows the balance between banks in a peer-to-peer manner, rather than through proxy banks, which makes the transfer fast, and greatly reduce the cost of balance. Ripple coin once was the second most valuable digital coin in the global, and it is the first model of deeply combining

digital coin and business application.

- Circle: Circle was founded in 2013. Its products contains bitcoin payment and social payment. The company has a complete and distinguish team. The founder has successful experience in the area of building platform-like company, software, media, and communication.

Table 13-2: Company Advantage of InterValue

|             | JingTong Technology                              | Ripple                                | Circle   | Hedera Hashgraph                      | InterValue  |
|-------------|--|---------------------------------------|--|---------------------------------------|---|
| Roadmap     | Blockchain commercial platform in various fields | Bank balance                          | Digital coin payment                               | Blockchain platform in various fields | Public chain、Blockchain browser、Blockchain Wallet、Commercial platform in various fields |
| Application | Business &Non-business                           | Finance                               | Digital coin                                       | Business &Non-business                | Digital coin& Business &Non-business  |
| Advantage   | Professional team, Intervene in various fields   | Professional team, High entry barrier | Professional team, Rich Experience, Abundant funds | Professional team, High creativity    | Professional team, Rich Experience, High creativity                                     |
| Vision      | Trust ecological builder                         | Global uniform payment standard       | Rebuild global payment network                     | Build the trust layer of the Internet | Build global value network  |

# 14

## Risk

Investing in Crypto-assets has many large risks. Investors need to fully understand these risks and take their own risk tolerance into account.

- Incomplete information disclosure

Until the day of publishing this whitepaper, INVE is still under development. Its core technologies such as the cryptographic algorithm, the communication network, consensus, may be frequently updated. This whitepaper contains a basic overview of INVE, but it is not absolutely complete. The foundation may update and improve the project from time to time based on changes in technology or for specific purposes. The Foundation cannot and does not have the obligation to inform the investors in real time of all the details of the INVE development process. Incomplete information disclosure is unavoidable and reasonable.

- Supervision

Crypto-assets have been supervised by many national regulatory agencies due to the high risks. The foundation may receive enquiries, notices, warnings, orders or rulings from regulators during the sale, and may even be ordered to terminate the sale. The supervision may greatly impact the development, marketing, advertising of INVE. Since the supervision rules may change at any time, the supervision allowance of INVE in any country may be temporal. Besides, INVE may be defined as a virtual commodity, digital asset, or securities currency. Thus, INVE may be forbidden to trade or hold in some countries.

- Project Failure

INVE is still under development. INVE may fail or stop for any reason. The main reasons include: forced termination by regulators, insufficient funds, and insuperable technical challenges. The INVE token may not be delivered to investors due to the project failure.

- Funds been stolen

Someone may attempt to steal the ICO funds of the foundation, and it will greatly impact the development of INVE. Although the foundation will adapt the most secure solution to protect the ICO funds. However, some network thefts are still difficult to completely prevent.

- Source code vulnerabilities

Although the foundation will invite the top security team to test the source code of INVE, no one can ensure that the source code is perfect. Maybe there are some bugs, defects or vulnerabilities, which make users not able to use some functions. Furthermore, these vulnerabilities endanger the availability, stability, or safety and negatively affects the value of INVE. The foundation will cooperate with INVE community to optimize and improve the security of the source code.

- Upgrade of source code

Since the source code of INVE is open source and continuously upgraded, nobody can predict or ensure the accurate result during an upgrade. Thus, the upgrade of the source code may incur unpredictable or non-anticipatory result, which may greatly impact the running and the value of INVE.

- DDoS

INVE may suffers the attack of DDoS, which makes the INVE system out-of-service. Besides, the transaction may be written into the INVE HashNet with delay or even cannot be executed.

- Insufficient capability of nodes

After the INVE system is online, the transactions will increase greatly. If the processing requirement is higher than the workload of INVE system, it may cause the failure of INVE. In the worst case, anyone may lose their INVE Token. Furthermore, the rollback or hard fork of INVE may be triggered, which endangers the availability, stability, or safety of INVE.

- INVE Token claimed without authorization

The attacker may decrypts or attacks the investor's account. Thus he/she is able to claim the victim's INVE tokens. That is, the INVE tokens bought by the victim may be sent to the attacker. Each investor has to protect his/her account. There are some tips: (1) Install anti-virus software, (2) Use high secure password, (3) Do not open or reply any juggling email, and (4) Store your account information and private key in a safe place.

- Lost of the private key

Each investor has to keep the private key of INVE wallet safely. If the investor loses or destroys the private key, the foundation cannot help the investor to find the INVE token.



- System fork

INVE is an open source project supported by the community. Although the foundation has some influence in the INVE community, the foundation cannot fully control the development and the market of INVE. Anyone is able to develop and upgrade INVE without any other people's authority. Once a part of users accept the pitch or upgrade of INVE, it will cause a hard fork. Further more, according to the roadmap, the foundation will make a hard fork. Theoretically, INVE Hashnet can fork many times. In the worst case, these forks may destroy the sustainability of INVE system.

- Lack of attention

The value of INVE depends on the popularity of the INVE Blockchain. The foundation does not ensure that INVE will be popular in a short time. In the worst case, INVE only attracts a few users, which leads to fluctuant token price and affects the development of INVE. Besides, the foundation is not responsible of stabling or influence the market price of INVE.

- Insufficient circulation

INVE is neither belonged to any people, entity, bank, country, organization, superstate or parastate, nor supported by any asset or credit. The trade of INVE is only based on the consensus among the investors. Nobody can ensure the circulation or market price of INVE. If a holder wants to sell his/her INVE, he/she needs to find the matched buyers. Besides, It is possible that there is no exchange or other markets to trade INVE.

- Fluctuant token price

In open market, the price of the crypto-token fluctuates greatly. The fluctuant is caused by the change of market, regulatory policy, technology, profit of exchange, and etc. The foundation is not responsible for the INVE trading in the secondary market. The risk of trading INVE is taken by the dealers.

- Competition

The fundamental protocol of INVE is based on open source protocol. Nobody owns the copyright or other rights of the source code. Therefore, everyone can copy, design, modify, and upgrade the source code to develop a more competitive protocol, system or virtual platform. In this case, the future competitive product may surpass or even replace INVE, and this can not be controlled by the foundation. Besides, a number of existing platforms like IOTA and ByteBall have already become the competitors of INVE. Maybe there are more and more competitors in the future. The foundation can not eliminate the appearance of the competitors.

# References

- [1] Bitcoin Computation Waste, <http://gizmodo.com/the-worlds-most-powerful-computer-network-is-being-was-50403276>. 2013.
- [2] Bitcoinwiki. Proof of Stake. <http://www.Blockchaintechnologies.com/Blockchain-applications>. Aug 2017.
- [3] Coindesk.com. Bitcoin: A Peer-to-Peer Electronic Cash System.
- [4] <http://www.coindesk.com/ibm-reveals-proof-concept-Blockchain-powered-internet-things/> Nov 2017.
- [5] Ethereum. Ethereum. <https://github.com/ethereum/>. Nov 2017.
- [6] IOTA. <https://github.com/iotaledger/>. As of 10 Nov 2017.
- [7] Byteball. Byteball. <https://github.com/byteball/>. Sep 2017.
- [8] Bernstein, Daniel J, et al. High-speed high-security signatures. *Journal of Cryptographic Engineering* 2.2(2012), 77–89.
- [9] M. Castro and B. Liskov. Practical Byzantine Fault Tolerance. *Proceedings of the Third Symposium on Operating Systems Design and Implementation*, New Orleans, Louisiana, USA, 1999, pp. 173–186.
- [10] Biryukov, Alex, and D. Khovratovich. Equihash: Asymmetric Proof-of-Work Based on the Generalized Birthday Problem. *Network and Distributed System Security Symposium* 2016.
- [11] Gilad Y, Hemo R, Micali S, et al. Algorand: Scaling Byzantine Agreements for Cryptocurrencies. *The Symposium* 2017, 51–68.
- [12] C. Decker and R. Wattenhofer. Information Propagation in the Bitcoin Network. *13-th IEEE Conference on Peer-to-Peer Computing*, 2013.
- [13] D. Dolev and H.R. Strong. Authenticated algorithms for Byzantine agreement. *SIAM Journal on Computing* 12 (4), 656–666.
- [14] A. Kiayias, A. Russel, B. David, and R. Oliynycov.. Ouroburos: A provably secure proof-of-stake protocol. *Cryptology ePrint Archive*, Report 2016/889, 2016. <http://eprint.iacr.org /2016/889>.
- [15] S. King and S. Nadal. PPCoin: Peer-to-Peer Crypto-Currency with Proof-of-Stake, 2012.
- [16] S. Micali, M. Rabin and S. Vadhan. Verifiable Random Functions. *40th Foundations of Computer Science (FOCS)*, New York, Oct 1999.
- [17] Directed acyclic graph: [https://en.wikipedia.org/wiki/Directed\\_acyclic\\_graph](https://en.wikipedia.org/wiki/Directed_acyclic_graph)