FAST ACCESS BLOCKCHAIN (FAB) WHITE PAPER

A high scalable public blockchain network

OCTOBER 10, 2017

FA ENTERPRISE SYSTEM INC (CANADA)
665 Hood Road, Markham, ON L3R4E1 Canada
Tel: 1-800-734-9388 Email: paul@fa.biz Website: fa.biz

Catalog

A high feasible scalable public blockchain network

Fast Access Blockchain (FAB) White Paper

Paul Liu & Team

Canada FA Enterprise System Inc

Add: 665 Hood Road, Markham, ON L3R4E1, Canada

Tel: 1-800-734-9388, Email: paul@fa.biz, website: fa.biz

1. Summaries

Scalability is one of the major bottlenecks in blockchain developments, the successful operation of Bitcoin, Ethereum and similars inspired great enthusiasm on blockchain technologies widely, however, the transactional capacities are desperate on all of them – only a few transactions per second, such as Bitcoin and Ethereum is no more than seven for each.

It is unacceptable for today's actual business use, there are many existing production scenarios are far more than this scale even in its single application, such as ecom website, supply-chain system or IoT platform.

By the nature of public blockchain's p2p network, constrained by nodes that their functions and degree of participation may differ dramatically, it has been recognized that there is no way to breakthrough this barrier by working on the base blockchain itself only, should focus on something else.

Blockchain sectors are seeing a splendid future, it will be widely used in almost all industries, with an ever-accelerating adoption, it outlines an urgent need to conquer the obstacle on blockchain scalability.

This paper proposed a completed solution for constructing a practical public blockchain eco-system with high scalability, security, reliability, decentralization and application – the Fast Access Blockchain network (FAB for short).

Based on a dedicated underlaying protocolized framework design, middle layer smart contract enforcement as well as upper layer functional architecture implementation, FAB network is the most powerful blockchain infrastructure with feasibility so far, it will bring blockchain into real commercial use in business.

FAB network is composed of three key components: Foundation Blockchain, Annex Blockchain as well as Open Storage Architecture, these three parts are designed with unified protocol and stream-lined logic process, they federate each other theoretically and functionally, make them into a fine trinity of completed ecosystem with features of powerful scalability, strong reliability and real decentralization.

1.2 Principles and philosophy in project design

The strict design logic of FAB network is based on rigorous design principles and philosophies, the distinctive natures of blockchain platform conflict with application needs, technical means to achieve goals are contradictory with objective conditions, it is difficult to reconcile between them, however, any problem has a resolution, the network must be made coordinating and working properly in the whole infrastructure scope, it is essential for actual business and commercial application of the decentralized ecosystem.

1.1.1 Design principles

Constructing trust – it is blockchain's core target, the purpose of blockchain platform is to construct trust;

Decentralization – it is blockchain's principle feature and necessary condition for contrasting trust.

Open architecture – Open is prerequisites for decentralization, open means equal for everyone, open source and ordinary facilities;

For practical business applications – Open leads to equal participation or use for everyone, this requires it must be a solid trustworthy platform.

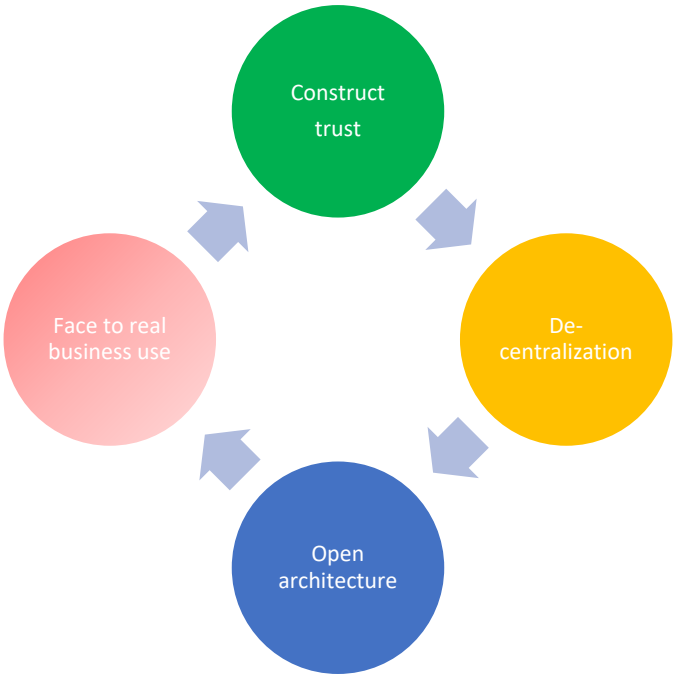

Figure 1. Principles and targets relations in project design

1.1.2 Philosophy

Building a blockchain system according to above design principles will face an uncoordinated controversial: unable to make decentralization, scalability, reliability coexist while they are the three must have key elements for a public blockchain platform.

For current blockchain system, if it is decentralized and scalable, it is unreliable; if it is scalable and reliable, it becomes centralized; if it is decentralized and reliable, it turns into non-scalable, this seems an inevitable plight.

To break this deadlock some breakthrough thinking and proper philosophy theories are needed, we outlined four clauses after deep research:

Trust is built out of distrust – to construct trust by participants who don't trust each other;

Scalable exists in non-scalable – a decentralized public blockchain is non-scalable while its nodes are scalable;

Centralization is convertible to decentralization – it is possible to convert a centralization structure into decentralization without reshaping.

Reliable may be consists of unreliable – by dislocating related elements in an unreliable system is always possible to change it into reliable.

1.2 Technical facts

In accordance with the principle of system design, focusing on the core characteristics of public blockchain along with practical business applications, we need to address the philosophical contradictions, which not only requires theoretical solutions, but also the need for viable technical methods.

1.2.1 Measures of eliminating contradictions

To challenge these objective controversial, we proposed a theoretical resolution – constraints dislocation.

Compose the decentralization infrastructure with three parts: Foundation Blockchain, Annex Blockchain and Open Storage Architecture, each has its advantages and disadvantages. Making each of them using its own advantages and replacing its disadvantage with other's advantage, one by one connect into close loop as a whole, so that to form a completed platform with full features of decentralization, scalability and reliability.

The design ideology:

Constructing an open public blockchain – Foundation Blockchain, which is highly decentralized and strong reliable but hardly scalable, aims to serve as highest trust provider and final decision maker, it is expected to process normal amount of data, with ordinary calculation ability and moderate network bandwidth, it is the basis of the decentralization ecosystem.

Framing auxiliary blockchain – Annex blockchain, which can be highly scalable for the local implementation, it is necessary for the whole platform though it is potentially centralized and untrustworthy.

Building Open Storage Architecture for decentralized data storage and consensus mechanism, the off-chain data storage can be strong scalable but is unreliable and untrustworthy, it can't constitute a complete decentralization system itself.

Each of the three parts has its defects, but to compose them together economically and logically will make up an ideal blockchain ecosystem.

1.2.2 Implementing measures

It is unable to build up an ideal blockchain ecosystem only by using Foundation Blockchain, Annex Chain and Open Storage Architecture, it needs additional technical measures.

We came up with three key technical proposals: KanBan, SCAR and MapReduce which works with the Foundation Blockchain, Annex-chain and OSA respectively. MapReduce is quoted from current existing big data technology, which is used for quick data query and consensus decision making in the ecosystem, while the KanBan and the SCAR are the two new concepts introduced to the blockchain system specially.

MapReduce in FAB system is different than in normal big data applications, it follows a rule for blockchain global searching, i.e., it's compatible with protocol defined by Foundation chain.

Foundation Blockchain + KanBan – Annex Chain + SCAR – Open Storage Architecture + MapReduce forms the completed solution, shown as the following diagram:

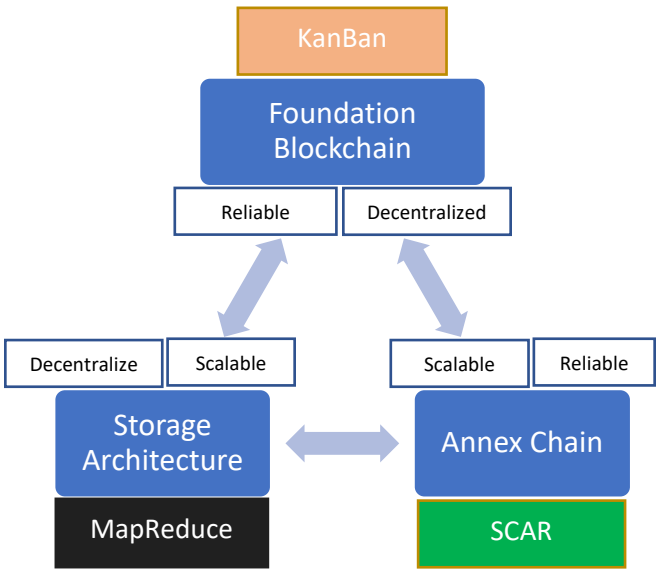

Figure 2. Close loop of constraints dislocation

In order to make the program as streamlined processes for easy implementing so that the system can be adapted easily and widely, we put forward three technology concepts:

CCUA – Cross Chain Unified Address;

CCSPV – Cross Chain Simple Payment Verification Protocol;

CCTIP – Cross Chain Transaction Interexchange Protocol;

CCUA is used in the whole platform, while CCSPV and CCTIP relates to third party blockchain, will be omitted in this paper to be covered in other paper.

By far the system is backed with completed solution theoretically and technologically along with compatibility proposal.

These measures provide not only comprehensive theoretical and technological support to build up typical and ideal public blockchain, but means for preventing double-spending attack on the Annex-chain, removing transaction partner account association as well as simplifying transaction verification procedure also. With the help of these measures, we broke through the bottleneck in blockchain scalability, enable us to construct a real decentralized, high scalable and strong reliable blockchain ecosystem.

The FAB platform is the first feasible public blockchain system that truly meets the needs of real business applications.

2. Technical solutions

As the communication conditions and procession capacity among all nodes vary dramatically and as the constraints of the consensus mechanism, it is publicly recognized fact that it is impossible to deal with a large number of transactions per second by the underlaying blockchain only, therefore, to break through the obstacle, innovation technology has to be taken into the overall system architecture.

2.1 System overall architecture

The Fast Access Blockchain system (FAB) aims to use profit incentive mechanism to construct a high scalable, low cost, efficient, safe and reliable decentralized public blockchain economic ecosystem that satisfies large-scale daily business needs in real economy environment.

The FAB network consists of three components: Foundation Blockchain, Annex Blockchain and Open Storage Architecture, it is based on the contradictory dislocation mechanism and the core rules of the unified underlying protocol and the consensus mechanism. They are consisting components of the trustworthy open economic ecology, each plays its special role and mutual collaboration, mutual verification overall, so that to constitute a complete guarantee of trust and value maintenance mechanism to resolve the plight of the decentralization, scalability, security unable to coexist.

The overall architecture figure:

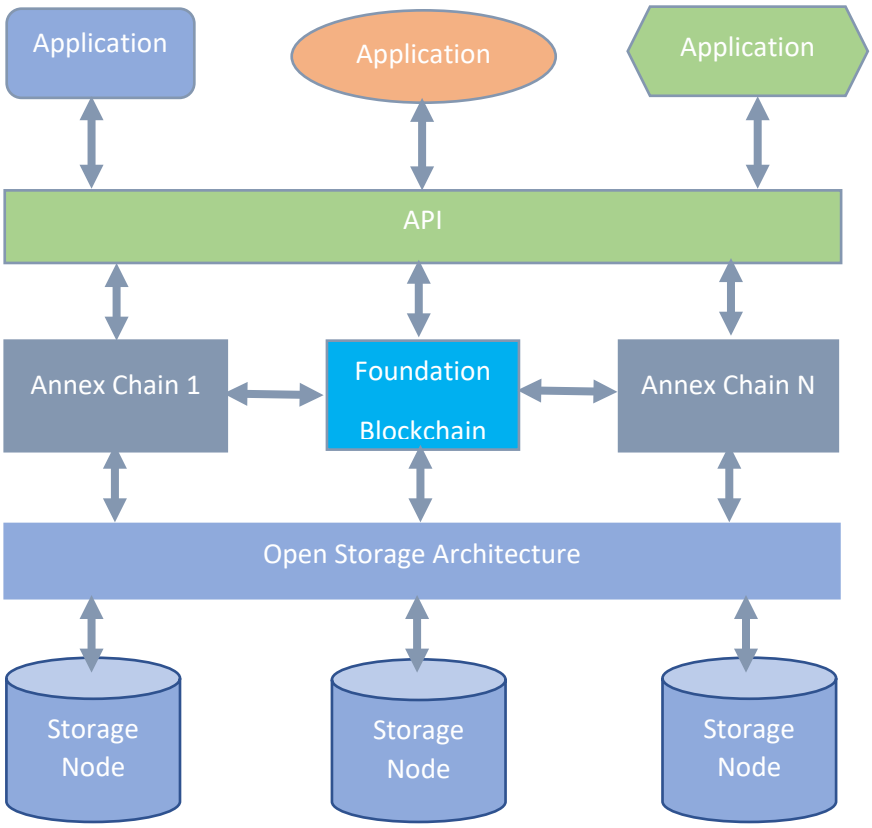

Figure 3. The overall architecture

Unlike the existing mainchain / sidechain design applied to Bitcoin or other blockchain, FAB's Foundation Blockchain – Annex Blockchain – Open Storage Architecture mechanism is a complete architecture designed as a whole from the underlying protocol ground up, their data encryption /decryption algorithm and verification process are compatible and collaborative with each other, it is an dedicated designed unify system with high efficient and security assurance, it avoids the centralization problem and improves efficiency greatly, makes the system safe, reliable and flexible for configuration, so that with it one can freely join the network as a node with powerful local transaction process ability easily, it is the first real public blockchain to meet massive transactions needs.

The design ideology of the FAB system is that the base blockchain aims at the minimum data volume, calculation amount and network bandwidth requirement, to provide the underlying protocol, the smart contract, the root ledger, the final decision right over all transactions; the auxiliary chain or the local node performs large-scale local off-chain transactions for its business needs; open storage architecture is to ensure that the local data in auxiliary chain to be stored in decentralized storage.

Three key technologies are introduced in the proposal: KanBan, SCAR and CCUA, aim to enforce states of local transactions on Annex-chain can be updated and monitored globally in real-time in the entire blockchain range, so that to prevent double-spending and make the system meets the need for large scale transaction scenarios, including exchange, IoT, e-commerce, supply-chain, medical service, etc.; in order to enforce decentralization features for local transactions, the Open Storage Architecture introduced with economic incentives and mandatory rules, it is enforced by smart contract and consensus mechanism to force the auxiliary chain or localized nodes to support the use of decentralized storage.

The incentive mechanism of the Foundation Blockchain is the mining rewards and transaction fee; The incentive mechanism of the Annex-chain is the business profit, the local transaction fee and the decision-making rewards in consensus; The incentive mechanism of the Open Storage Architecture is the data, the storage fee and the rewards of consensus.

2.2 Foundation Blockchain

The Foundation Blockchain is the root of the system, it is aimed at the minimum data volume, the minimum calculation amount and the minimum network bandwidth requirements. It mainly provides the base protocol, the root ledger, the smart contract, the value and trust system with the final decision right, its legitimacy comes from all participating nodes.

The Foundation Blockchain is planned to use a Proof-of-Production (PoP) consensus mechanism in conjunction with actual productivity, it's a specific type PoS, but a PoW consensus mechanism similar to Bitcoin is used before sufficient scale of actual production achieved.

2.2.1 Partition function of Foundation Blockchain full node

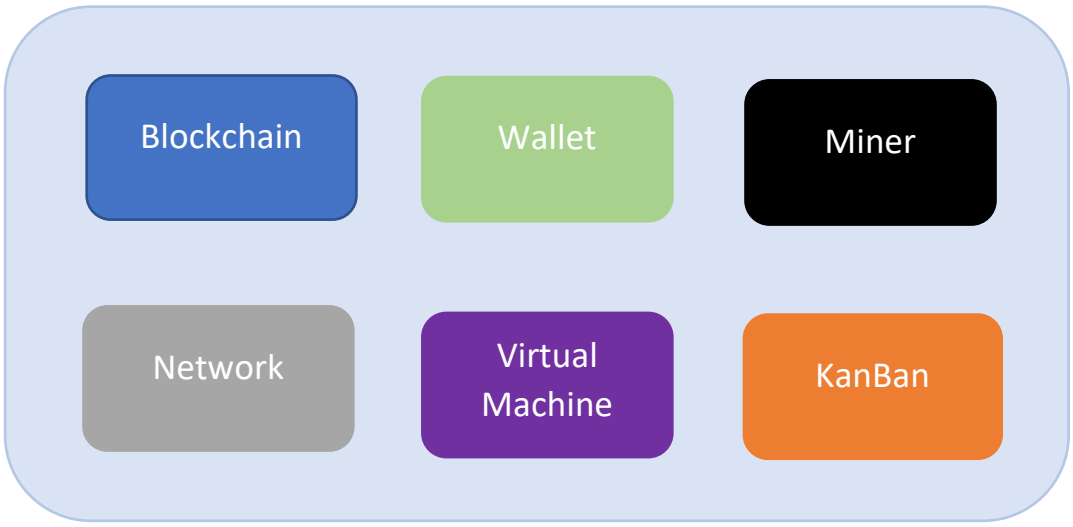

Figure 4. Partition Function of Foundation Blockchain full node

In addition to the common blockchain, wallet, miner, routing, virtual machine and other functional modules, the Foundation Blockchain introduces of KanBan function. KanBan is the meaning of “watching board” in Chinese language, which comes from the modern supply-chain / manufacturing-chain system where workers are engaged in fixed process work, but KanBan provides immediate information to remind of specialties, warnings or changes.

2.2.2 KanBan

KanBan is designed to provide real-time updates and query capabilities for Annex-chain transactions in a global context without significantly increasing the burden on the Foundation Blockchain. It is a special module designed to prevent double-spending attacks effectively.

In FAB network, KanBan runs in GPU in the form of a memory data management program or an in-memory database in a node computer of Foundation Blockchain or runs in a standalone computer that cooperates with the Foundation Blockchain presenting state monitoring globally for the Annex-chain transaction. KanBan is designed as a GPU in-memory database, on the one hand basically do not take the node’s ordinary resources to ensure that the Foundation Blockchain operation efficiency, on the other hand, GPU in-memory database data processing capabilities is far more than the computer main processor, it can greatly improve the KanBan’s operating efficiency, so that state updates and query operations for a small batch of records can be implemented in a few milliseconds.

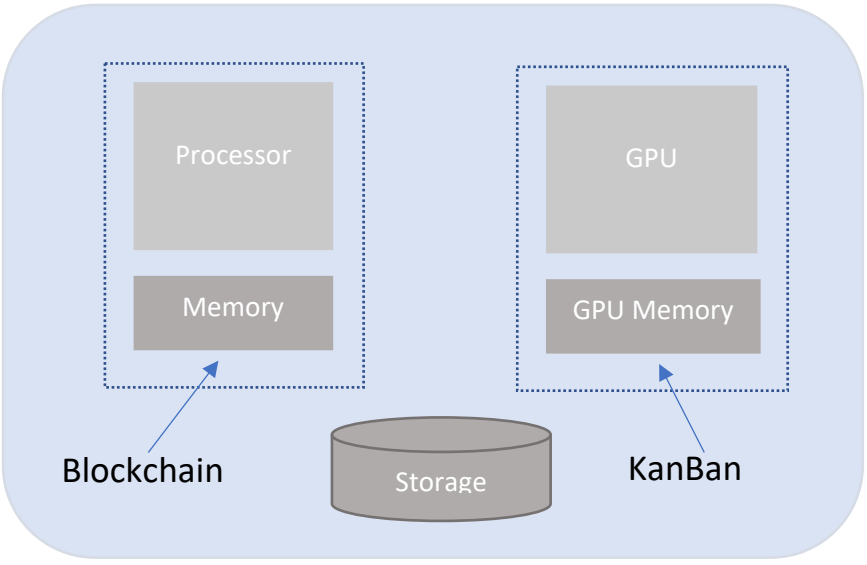

Figure 5. Foundation node KanBan illustration

As KanBan function facilitated, transactions in Annex-chain are presented in a decentralized way globally in real-time, achieving the purpose of preventing double spending effectively. However,

since KanBan runs in the computer's GPU and takes up GPU memory, the miner software which utilizes GPU features needs to be separated and run on a different computer.

KanBan state maintenance and update is controlled by smart contracts, the more, there are strict validation and verification relationships among KanBan, Foundation Blockchain, Annex Chain and Open Storage Architecture to ensure that KanBan data is accurate and legitimate.

KanBan's processing is: receive the package from the Annex-chain ---> verify the legitimacy of the package ---> verify the legitimacy of the transaction ---> update KanBan state ---> return receipt to the Annex-chain.

This allows KanBan to maintain the exact state of the address or account in the Annex-chain transaction and, if necessary, to further verify the Annex-chain's transaction details to the open storage node.

2.2.3 Data in KanBan

Annex-chains table

No.	Public Key	Last Hash	Unlocked tx Merkle Root	Bal	Timestamp
1	4ds5ke3…vd3	309ew98gweio	hgurs2ua6serhufdsfe423	2000	20160223T021405
2	Iy8r5t4s…gte	9rc6ghd8fjcndu	goir7q3c9sk4ge8rd3afrb	400	20160508T223611
…	…	…			…
n					

Figure 6. Annex Chains table in KanBan

Address (account) state

address	Balance	Locked	Timestamp
0m5frtfgdesr……	200000	F	20160312T100325
0msetvuehfe……	16000000	T	20160520T081220
…	…		…

Figure 7. Address (account) table in KanBan

Unlocked transactions table

Txid	Address	Input Address	Amount	Timestamp
1	4ds5kgce3…vd3	309ew98gweio	40000	20160223T021405
2	Iy8r5gdt4s…gte	9rc6ghd8fjcndu	1200000	20160508T223611
…	…	…		…
n				

Figure 8. Unlocked transactions table in KanBan

On receiving data from Annex-chain, KanBan verifies the legitimacy of the package and its inside transactions first, if valid, updates the state of the relevant address and returns the signed receipt as proof to the Annex-chain and in the same time notifies the Open Storage Architecture with the node balance and the contract signature. If failure on verification, rejects and notifies the Annex-chain.

KanBan can supply current state in real-time for each active address to prevent attack of double-spending, it also provides the signature stub for the last block for each Annex-chain to confirm the validity of the block and transactions inside.

2.2.4 Verify transaction validity

For new transactions on the Annex-chain, the system validates their validity first through the KanBan state and the underlying blockchain transaction state.

If conflict occurs on an address or account, take the early on according to the time priority, if timestamp is the same, take it by hash priority.

If a transaction conflicts, set a warning flag to the address of the conflicted transaction.

For an address is flagged as suspicious in KanBan, when new transaction occurs, check its full validity through all transaction records on the Open Storage Architecture.

Technically, in order to strengthen KanBan's processing performance, it was designed as a dedicated GPU data processing program, thus KanBan can take the advantages of node computer's GPU instead of its ordinary resources, so that the node computer can deal with Foundation Blockchain effectively.

In addition to the rapid processing of Annex-chain transactions and maintenance of Annex-chain address state, KanBan participants in the PoS consensus for the Annex -chain as well.

KanBan can also periodically mirror the data to the hard drive to prepare for fast recovery after power failure.

2.2.5 Constitution of KanBan in Foundation Blockchain network

KanBan may run in the node computer of Foundation Blockchain network, or it may run in a separate computer associated with the Foundation Blockchain node, it even can run on the Open Storage Architecture node computer or an independent computer that access Foundation Blockchain and OSA through network. Technically, a node can be a KanBan node only without Foundation Blockchain, Annex-chain or OSA function activated at all.

Since the KanBan is designed as a GPU database program, running in a computer GPU and occupying GPU memory, devices that without an appropriate graphics accelerator and enough GPU memory can not facilitate KanBan.

In the design scheme, the system does not require that all nodes in the Foundation Blockchain equip with KanBan, but nodes with KanBan function have a special KanBan flag in nodes list.

Nodes without KanBan function do not participate in KanBan services and do not participate in any Annex-chain's consensus mechanism; nodes that provide KanBan functionality can earn consensus rewards from Annex-chains, which are derived from transaction fee in Annex-chain.

In fact, for nodes with advanced facilities, all system functions, including full node Foundation Blockchain, KanBan, Annex Chains and Open Storage Architecture nodes can all be equipped.

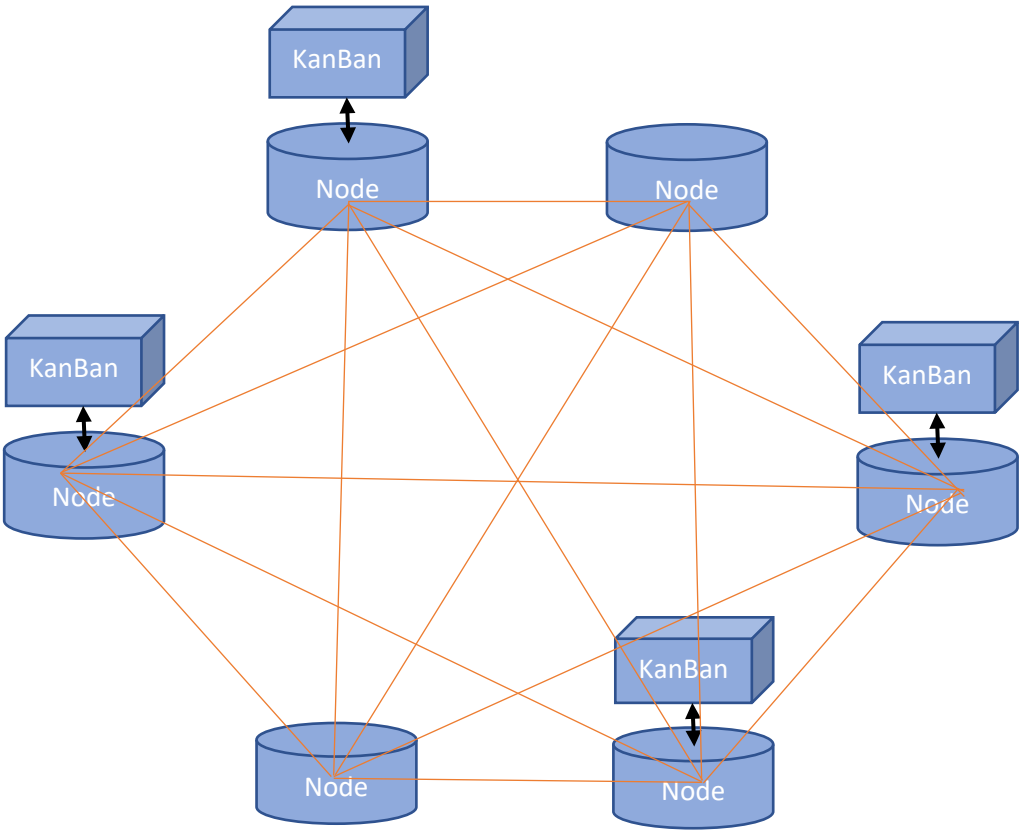

Figure 9. Foundation Blockchain network (not all nodes are KanBan nodes)

2.2.6 KanBan configuration requirements

To activate KanBan feature, a node computer is required to equip with a proper graphics accelerator card that runs the appropriate algorithm and with enough memory. The hardware requirement for the initial KanBan node is to install a graphics accelerator card with no less than 16GB memory, but change may apply as the amount of data increases, there is no consensus issues affected therefore no forking risk for upgrading GPU hardware.

Increasing GPU hardware requirements does not affect the consensus mechanism, but may affect operational efficiency. Because the KanBan nodes in the system are classified according to performance and are identified, such as KB1 for 16GB, KB2 for32GB, it should fit an Annex-chain's requirement to serve it needs.

Assuming that 2GB of GPU memory is reserved for other purposes as node computer's normal needs, 2GB is used as Annex Chain related data, and the rest is used for the most important data – the state table for all off-chain transactions.

An account state record is of no more than 64 bytes, then 12GB can fit about 200 million active account state records; if 32GB graphics card installed, it can provide about 500 million active account states.

By system design scheme, it supports KanBan grouping function, a group of KanBan services for one or more Annex-chains.

2.2.7 Implementation of the Foundation Blockchain

The Foundation Blockchain program is refactored and improved from Bitcoin system, in its core some key features will be increased, such as KanBan, SCAR and CCUA.

A virtual machine will be added to it for serving smart contract.

The Foundation Blockchain will be equipped with related features to collaborate with Annex-chain as well as Open Storage Architecture.

Since the Foundation Blockchain is designed to serve as root evidence and ledger, unnecessary data will be decreased.

Foundation Blockchain core architecture

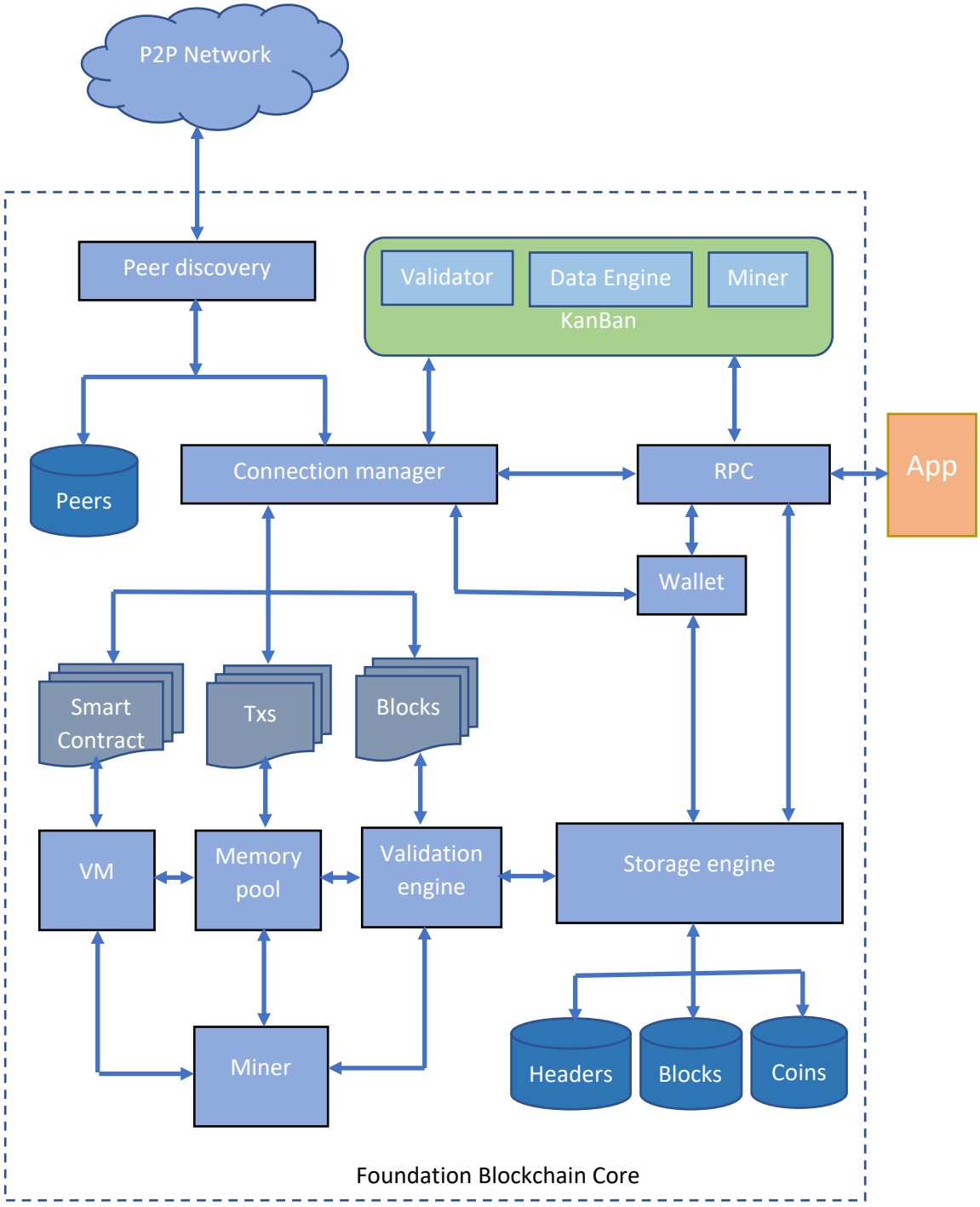

Figure 10. Foundation Blockchain core architecture

Streamlined and dependency independent structure will be adopted in all the development, it will make the system easy to configure, control and maintain. Many of the modules in the Foundation Blockchain core will also be used in the Annex-chain and Open Storage Architecture.

2.3 Annex Blockchain

Annex-chain is an important part of the FAB system, usually an Annex-chain node may carry a large number of transactions for specific business, such as exchange, e-commerce, supply-chain, Internet-of-Things platform or medical platform.

As a business point of sales, an Annex-chain node may perform as a typical centralization one, it may carry huge amount of transactions itself, however, according to the system design, the final confirmation of value and state of the off-chain transactions are implemented in a decentralized way through KanBan, accordance with data decentralized storage on Open Storage Architecture, it is fundamentally guaranteed that local transactions on Annex-chain with centralization and localization characteristics turn out to be with full features of decentralization, security and reliability.

According to the system design, even if an Annex-chain is deployed or designed for fraud in purpose, it is unable to cause any lose to its customers.

2.3.1 Annex-chain technical program

An Annex chain originates from the Foundation blockchain's authorization, which provided the original evidence and identity from the Foundation blockchain, Annex blockchain's properties and parameters are authorized through the smart contract issued by the Foundation blockchain. In transactional process all states will be validated though smart transaction authorized by the Foundation blockchain, KanBan and the Open Storage Architecture.

In design strategies, dispose the main network transmission and data processing as far as possible on the Annex blockchain, enforce the necessary evidence and data submit to KanBan and OSA only.

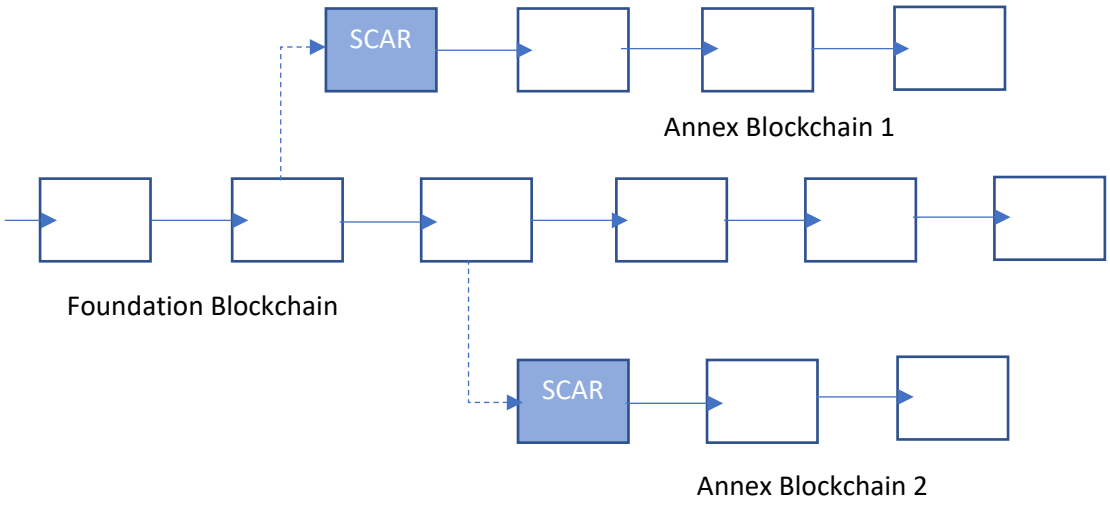

Figure 11. Schematic diagram of Annex blockchain structure

Note that the illustrated Annex chain is not forked from the Foundation blockchain, the dotted line only represents the dependency relationship.

The main difference between the Annex-chain and so-called sidechain is that the Annex-chain derives and uses Foundation Chain's currency directly while the sidechain always has its own currency no matter newly created or held and converted from main chain's currency, that is Annex is a part of the whole system while the sidechain is a help of a main blockchain.

An Annex blockchain contains the following key elements: initial block, smart contract address route (SCAR), cross-chain unified address (CCUA) protocol and KanBan proof, they guarantee the reliability, security and effectiveness of the Annex chain's transactions.

The first block of the Annex-chain starts from is a special block issued by the Foundation blockchain smart contract, it defines a special account for the Annex chain, known as Smart Contract Account Route (SCAR), which acts as the agent of the Annex chain to execute transactions between it and all external accounts.

In the overall design of the system, two independent Annex blockchains can derive from the same starting block one is value blockchain the other is business affairs blockchain, used to serve the value maintenance of the Annex-chain and business affairs management respectively.

As shown below:

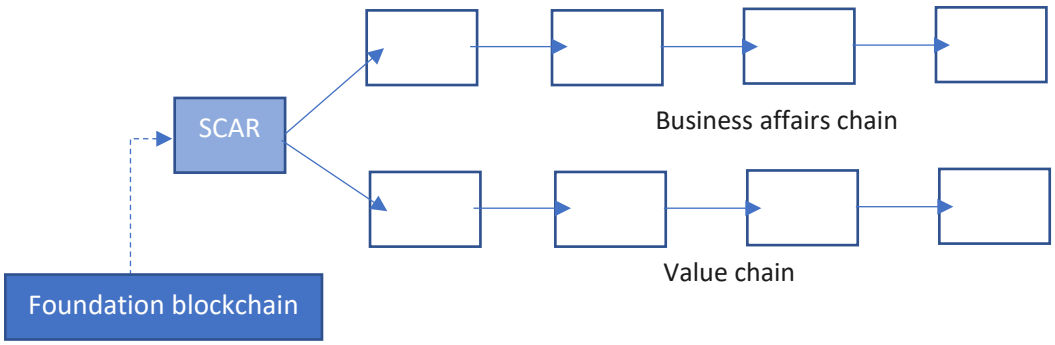

Figure12. Complete double chain structure of Annex chain

Value chain records value transactions, business affairs chain records business logic and business data. This double-chain mechanism allows the system to build an universal functional layer between the underlying blockchain platform and the upper layer business logic to support all kinds of specific business application requirements.

This scenario in this paper is limited to the introduction of the value chain only, the business affairs chain and the general functional layer will be covered by other papers.

In principle, the Annex chain adopts the Foundation blockchain value system, that is, in the Annex chain the Foundation chain currency is circulating and trading directly. But in order to make the platform more flexible to suit a variety of application scenarios, the system design supports custom Annex chain protocols and consensus mechanisms that allow users to issue their own currency.

2.3.2 The value and trust mechanism maintenance in Annex chain

The trust mechanism of the Annex chain is derived from the Foundation blockchain, which is restricted and ruled by smart contract issued by the Foundation blockchain. The result and the final decision are attributed to the Foundation blockchain as well.

In layman's terms, the identity and attributes of the Annex chain are determined by the Foundation chain, the validity of its transaction is subject to the approval of the Foundation chain, the data storage on OSA is required by the Foundation chain and the final settlement is determined by the Foundation chain. The design principle of the system is to let Annex chain to bear communication and calculation as much as possible upon meet these Foundation chain domination promise.

On the internal value maintenance of the Annex blockchain, according to the situation to be treated differently:

For the Annex-chain using the Foundation Blockchain’s currency, its value system is derived from the Foundation Blockchain directly, which means it is implemented according to the Foundation Blockchain’s protocol, normative and consensus mechanism. It is bound by the Foundation blockchain’s smart contract as well, so it subjects to the Foundation blockchain’s supervision and eventually accepts its decision.

For the use of its own independent currency of the Annex chain, its value is not derived from the Foundation blockchain, transactions relate the Annex chain are limited conditionally, any transaction between the Annex and external can only be implemented as local exchange, the Foundation chain does not verify its consensus mechanism, but the Foundation Blockchain still has the right of supervision and the final decision, the transaction verification rules are still based on the Foundation blockchain through smart contract.

2.3.3 The first block of an Annex chain

When an Annex chain is initialized, a request to authenticate submitted to the Foundation chain, this will result in the ID of the Annex chain, its private / public key pair and attribute and smart contract generated by Foundation blockchain. These data are stored in the first block along with timestamp and other data. The system supports NYC function in an optional way, so that to confirm owner’s identity (optional).

It should be noted that the Annex chain id is different from the node id, one node can run multiple Annex chains, each Annex chain has its own independent id and key pair, the same Annex chain can run on multiple nodes also.

Each Annex chain will be generated with an unique account authenticated by the Foundation blockchain when it is initially created, known as Smart Contract Agent Routing (short for SCAR), this account plays a special role as the only and unique agent of the Annex chain, to execute transactions between the Annex and externals. As a special account, SCAR ruled and operated by smart contract

issued by Foundation blockchain only, with particularity, no one can manipulate the account initiatively, even the Annex chain itself or its owner. The account can only be executed by the Foundation blockchain for transactions in related addresses between the Foundation Chain and the Annex-chain or implementing the Annex-chain's local transaction by updating internal addresses state of the Annex chain logically.

The Annex chain id, its public key and related attribute parameters are stored in the KanBan's Annex-chain list also.

The starting block of an Annex-chain is the authorization block issued by the Foundation blockchain, it contains the verifiable id of the Annex chain and the id is stored in the Foundation Chain and KanBan's Annex-chain list.

2.3.4 Core Architecture of Annex-chain

The Annex-chain is programmatically originated from the Foundation Chain, its core structure and most of its functions are the same as the Foundation Blockchain, many of its modules are shared between the two chains.

However, the Annex-chain has different consensus and miner, it has more modules and options than the Foundation actually.

Since an Annex can custom and own its own currency and with transactions package process and data submission to Open Storage Architecture features, the kernel of the Annex needs to contain package process module, KanBan communication and data exchange module as well as OSA data manipulating module, etc.

The core of the Annex-chain contains an important part – the SCAR process module also, it plays the role of converting any a transaction into transactions between it and the origin participants and maintaining related transactions state.

In addition, the Annex-chain needs to be expanded to support the manipulation of data storage on the Open Storage Architecture.

In the Annex-chain, the KanBan function is optional and is only required if there is a lower layer sub chain – its child chain.

The core structure of the Annex-chain shown as following: (value part only)

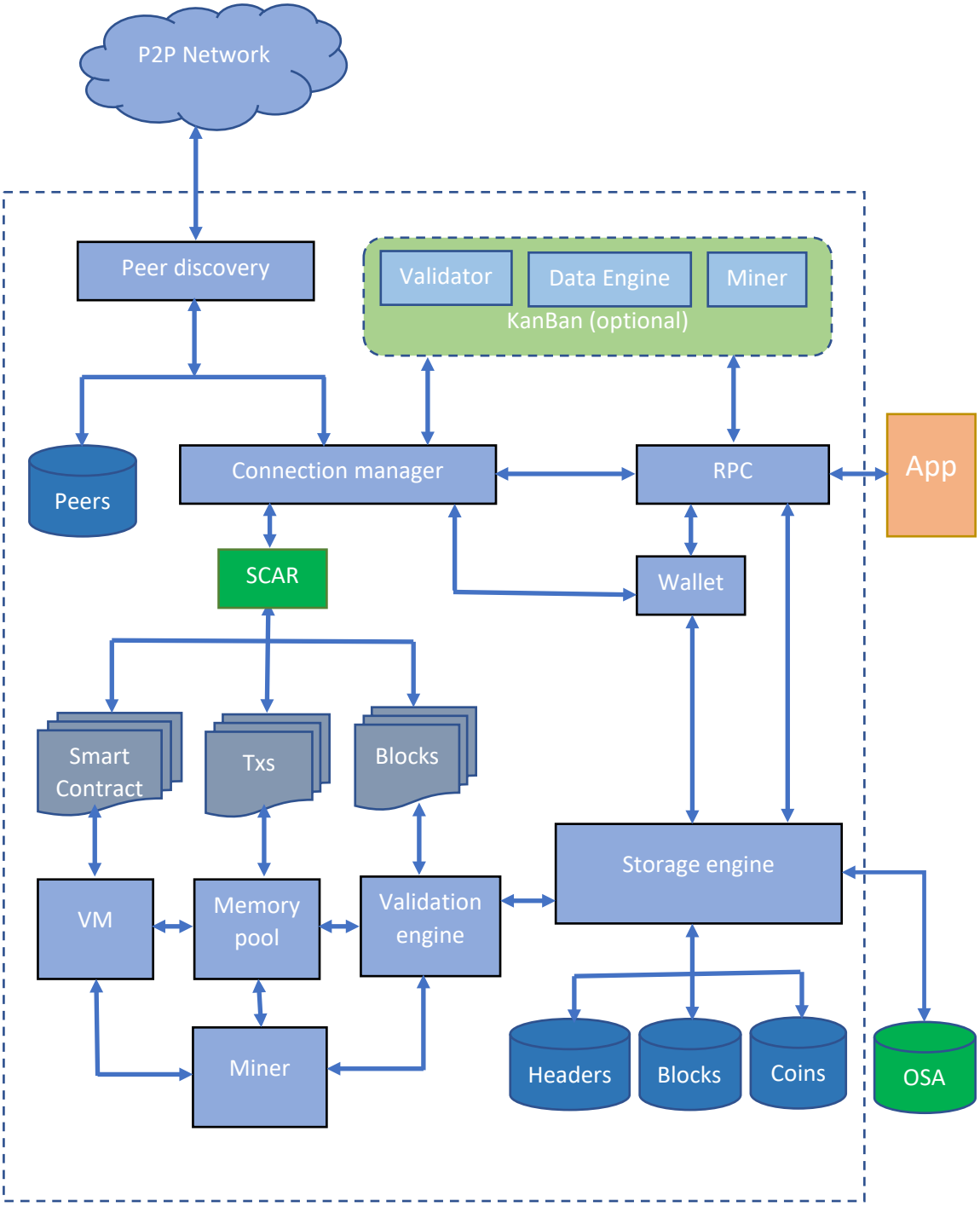

Figure 13. Core architecture of the Annex Chain

The figure shows value relevant components structure of the Annex-chain, in the system design, since the Annex-chain supports the business data chain also, there are more modules omitted, here covers the value chain only.

2.3.5 Address Format

A set of special rules for address format is designed in the system - the Cross Chain Unified Address (CCUA), that is, address-specific rules, addresses with the same address-code segment belong to the same owner and controlled by the same private key, the specific rules are as follow:

An address consists of four code segments, namely: **address type code** - **chain code** - **address code** - **verification code**;

Address type code is 2 bytes, currently 0m is for the Foundation chain's PKH address, 1a is for the Annex chain's PKH address;

The chain code takes 4 bytes, it stands for the unique id of related blockchain, the Foundation chain code is 0000;

At present, the address code is assumed to be PKH only, the Annex chain and the Foundation chain uses the same private key and public key, so their corresponding addresses are the same;

The verification code is taken from the first four bytes of double hashing value of the combined address string.

Any addresses with the same address-code belong to the same owner and controlled by same private key, no matter which blockchain it is from, such as:

0m 0000 aaabbbccc123 y4sg

1a 0a4u aaabbbccc123 g8rj

The two addresses with different address types and chain codes, one is for the Foundation blockchain, another is for the Annex chain with chain code 0a4u, because their address-codes are the same, the two addresses belong to the same owner.

The FAB system's specialty is, transactions between Annex chain and Foundation chain only allowed for addresses belong to the same owner with same address-code.

When an Annex chain account submits a settlement request to the Foundation blockchain, the coin must go to the corresponding address that with the same address-code as the Annex chain address.

An address in the Annex chain is a transaction state address, that is, the address won't change after a transaction happened, but only its state updated.

The Cross Chain Unified Address protocol CCUA provides a convenient mean for implementing transaction verification and simplifying the management of cross chain transactions. In fact, the CCUA is not limited to the FAB system only, it can be used as a universal cross-chain address protocol, adapted to any blockchains, for the implementation of generalized management for decentralized transactions in convenient means.

2.3.6 SCAR Account and Transaction

Each Annex chain has a special account, called Smart Contract Agent Route, shorts for SCAR. The dominance of the SCAR is limited to the smart contract authorized by the Foundation blockchain for the execution of transactions between it and the Annex chain counterpart, smart contract relates to the SCAR is established and controlled by Foundation chain only.

SCAR is a special transaction hub in Annex chain, any a transaction between two accounts in the Annex chain is to be converted into transactions between SCAR and the participants accounts. All transactions between the Annex chain and the Foundation chain or other Annex chains are carried out through the SCAR account too, so that all the transactions on the Annex chain are turned in to streamlined process – between SCAR and an account, the purpose to do so is when an account in the Annex chain submits a clearance request to the Foundation blockchain, no consent needed from related accounts, it is only one transaction between SCAR and the account and the SCAR is manipulated by smart contract will be executed automatically by miners, this reduces transaction data dramatically for the Foundation blockchain, in addition, SCAR plays an important role in preventing fraud transaction relates to Annex-chain.

The hub functional SCAR appears centralized features as all transactions deal with it, however the transaction is verified by the decentralized KanBan and data is stored on the decentralized OSA, the Annex chain itself does not have the right of adjudication, nor the exclusive rights to the data, it is fully decentralized by its natures.

The private key of the SCAR is controlled by smart contract manipulated by the Foundation blockchain.

Any transaction on the Annex chain is verified by a smart contract and SCAR for legality.

The transactions between any two accounts on the Annex chain are streamlined into transactions between the SCAR and the participants accounts.

To a transaction between account A and B on Annex chain: A->B => A->SCAR, SCAR->B;

To a transaction between A on Annex and X on Foundation: A->X => A->X1, X1-SCAR, SCAR->X;

To a transaction between X on Foundation and A on Annex: X->A => X->SCAR, SCAR->X1, X1->A;

To a transaction between AB on different chains: A->B => A->SCAR1, SCAR1->SCAR2, SCAR2->B.

KanBan will always keep the SCAR's overall state in an Annex chain, the state can be verified and confirmed by calculating Annex chain UTXO collection.

2.3.7 Transaction State of Annex Chain

The FAB system defined four states for valid transactions of the Annex chain, namely executed, witnessed, confirmed and completed, representing four different transaction states respectively.

On the Annex chain receives a transaction, the transaction is executed and generated locally, it is usually completed in a few milliseconds. This is an internal transaction only on the Annex chain. If the Annex chain is with only one single full node, it equals to a centralized transaction, the trustworthiness of the transaction in this state is equivalent to the trustworthiness of the Annex chain;

When the Annex chain submits the transactions package to KanBan and received KanBan's confirmation, it is in witnessed state. Usually this state can be achieved in several seconds to a few minutes since the transaction initiated. Since it is submitted to KanBan, the state of the transaction is maintained by KanBan and its trustworthiness is greatly enhanced. But since the submission to KanBan is the Annex chain's initiative purpose, it is not manipulated by the Foundation blockchain, therefore, number of KanBan's confirmation is taken as an important parameter to measure the trustworthy of the transaction, the higher the number, the more reliable;

The block is generated on Annex chain and is validated by KanBan and stored on the Open Storage Architecture system, the state of transaction is confirmed. Usually it should be completed in a few minutes since the transaction initiated. Submitted to the OSA indicates that the data storage is decentralized, the transaction is already very trustworthy, similar to KanBan confirmations count, the higher the number of OSA nodes that are submitted to, the higher the trustworthiness of the transaction is;

When an account submits the settlement to the Foundation blockchain and completed, the transaction state is completed, that depends on when the account to submit. In this case, the transaction associated with the account has been submitted to the Foundation blockchain, it has the highest level of trust.

Generally, a transaction in witnessed state is basically risk-free, a small amount transaction can be regarded as reliable; while a transaction in confirmed state means it is with sufficient security guarantee, a fairly big amount of transaction could be recognized as assured.

Since the credibility of the witnessed state is determined by confirmation number of KanBan, while the credibility of the confidence state is determined by the number of storage nodes submitted to, the FAB will supply a set of dedicated api to provide a simple means of judgment through smart contract for the client.

2.3.8 Annex chain transaction processing flow

The Annex chain transaction needs to be verified by KanBan, which is a necessary process for preventing double-spending attack and is valid only through KanBan's verification and receipt of KanBan's confirmation.

Annex chain transaction processing flow shown as below:

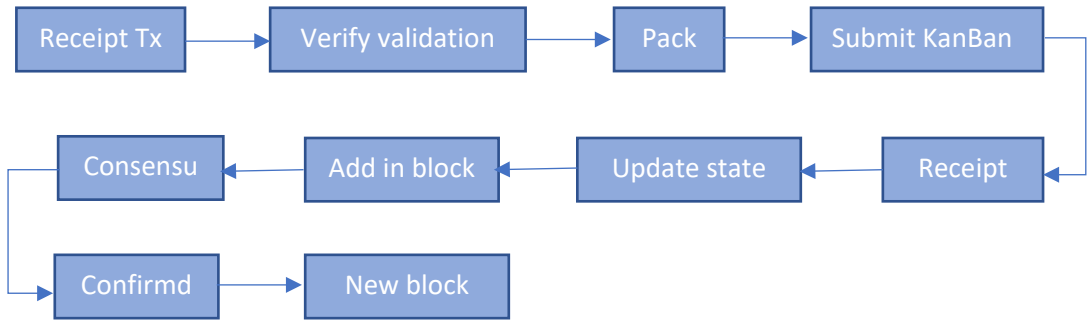

Figure 14. Annex chain transaction processing flow

After receiving the package submitted by the Annex chain, the Foundation chain verifies the package first and then verify the validity of the record in the packet, if has problem the packet will be rejected and notification will be sent to the Annex chain, and if passes validation, the transaction state in KanBan will be updated and place the transaction into the unsettled list, sign it and send the confirmation to the Annex chain.

When an Annex chain received denied notification from KanBan, it should remove the problem item and repack it to submit.

Package data and transaction records on both the Annex-chain and KanBan should be exactly in the same order and timestamp, and each sent packet contains the hash value of the previous packet, so that to minimize data transmission. When a node generates a block through PoS, only needs to notify the hash value of the last packet.

In general, a packet sent to KanBan on Foundation blockchain by Annex-chain contains one or more transactions;

A transaction is validated globally after Annex-chain received verification from the KanBan, the more the KanBan confirmation received by the Annex-chain, the higher the trustworthiness of the transaction.

The transactions in the Annex chain are packed and sent to KanBan by the Annex chain, the KanBan nodes do not automatically propagate it to other P2P nodes.

2.3.9 Block processing flow in Annex chain

In the Annex chain, the blocks are generated by the POS consensus mechanism that is involved by the Annex chain nodes, KanBan, OSA nodes, they can be verified by KanBan or the Open Storage framework.

A block's validation confirmation condition for the client application is that the block passes validation, the block or its downstream blocks are signed by KanBan and the block data is stored at the OSA nodes.

The transactions in the Annex chain are packed and sent to the KanBan nodes by Annex nodes initiatively, the KanBan nodes are no longer to propagate automatically.

When a block is mined by a node according to the Annex's consensus, it will be propagated between nodes of the Annex p2p network, data transmitted include nonce, the last packet id and merkle root, nodes involved in the p2p network include all Annex chain full nodes, mining participated KanBan and mining participated OSA nodes.

After a block is mined in the Annex chain, it will be broadcast to its participants OSA node.

2.3.10 Double Spending Attack Preventing in Annex-chain

The FAB system is designed with strong ability to prevent double-spending attach on Annex chain.

First of all, in the case of Annex chain is honesty, double-spending attack insides the Annex chain can not be implemented at all, states of all the Annex chain's internal accounts updated locally, any node in the Annex chain can obtain it easily in real-time, there is no double spending attack vulnerability;

In another case, if the Annex chain is deployed for fraud, the client application validates the transaction's validity through KanBan and the Open Storage Architecture. KanBan and the Open Storage Architecture's validation mechanism will determine whether the client fraud or the Annex chain fraud, if the client fraud, the transaction is invalid and the suspicious account in the transaction will be placed a warning flag in KanBan; if the Annex chain fraud, it will call smart contract in KanBan to invoke the investigation process, the review process will validate all unlocked transactions of the Annex chain, its privilege account SCAR will be frozen until the completion of the investigation, if the Annex chain reviewed as to be fraud, it will be suspended and can only be re-activated upon request and voted successful by the majority of all the participants KanBan nodes;

For the double-spending attack occurs between the Annex chain and the Foundation chain, since the FAB system limited transactions between Annex chain and Foundation chain only can be implemented between related CCUA addresses, there is no chance for double-spending attack if only vulnerability eliminated in the Annex chain.

To cross-Annex chain double-spending attack refers to an attack occurs between two or more Annex chains, there are several different cases that need to be considered:

a) All the Annex chains involved are honest, the attack was initiated by the client only: In this case, the transaction can not be verified through KanBan and the Open Storage Architecture, the Annex chain nodes and the client can obtain the state of the related account in time, the transaction fails;

b) In case of partial the Annex chain nodes participant in the attack are dishonest:
The client can verify the validity of the transaction through KanBan and the Open Storage Architecture, do not only through the Annex chain nodes. If the transaction is suspicious of fraud, the review process in KanBan or OSA will be invoked to investigate the involved client and Annex chains;

c) In case of all the Annex chains involved in the double-spending attack are dishonest:
Clients can be verified with KanBan and the Open Storage Architecture. In fact, due to the establishment of SCAR, SCAR channels and CCUA, the more Annex chains involve in the cross-chain transaction, the more difficult to success for the attack because of more loopholes on the attack process.

It is clear that, KanBan and the Open Storage Architecture play very important roles in the process of preventing double-spending attack.

In addition, the Annex chain's initiated time, its transactions amount in history is kept in the Annex-chain table in KanBan and OSA, it can be referred as the Annex-chain's credit by clients.

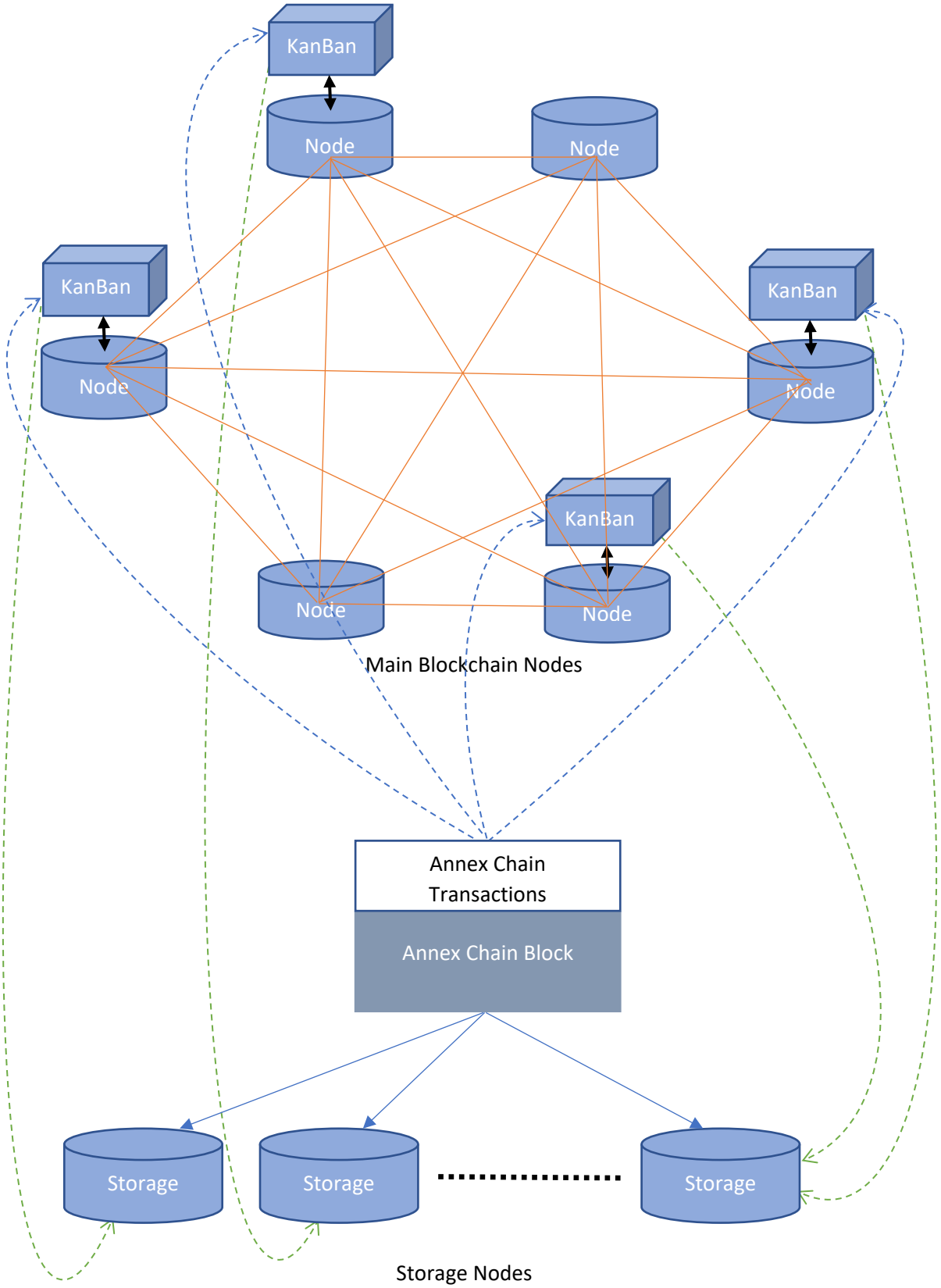

Figure 15. Verification relation in the whole system

2.3.11 Settlement of an Annex chain account

Transaction of the Annex chain is valid and effective globally, which is implemented and assured through the decentralized KanBan and the Open Storage Architecture.

That is, the account state of the Annex chain is always synchronized with related KanBan, and the blocks containing the detailed transaction records are submitted and stored to the Open Storage nodes required and enforced by KanBan.

When an Annex chain account submits a request to the Foundation blockchain for settlement, even if the Annex chain disappeared or cracked-down, the settlement can be implemented successful, because the decentralized KanBan and Open Storage Architecture maintains full state and detailed transaction records respectively, and since the establishment of SCAR mechanism, all Annex chain related transactions are converted into transactions between client accounts and the SCAR, while the SCAR is controlled by smart contract on Foundation blockchain, the settlement can be performed without the consent of the other parties.

After settlement, the related account on the Annex chain is cleared, related records in KanBan are deleted also.

In addition, the Annex chain itself can request a settlement to a specific account or all accounts, it is through SCAR account only.

In the most ambitious situation, a settlement requested by SCAR is only one transaction but contains hundreds even thousands or more of outputs and it may refer to millions of local transactions in the Annex-chain.

That is how the FAB system works to deal with huge amount of transactions while the main blockchain – the Foundation chain does not need to deal with large amount of transactions.

2.3.12 Hierarchical Annex-chain Architecture

Annex chain is not limited to only one layer, it can be hierarchical with multiple layers in the system design.

Shown as below:

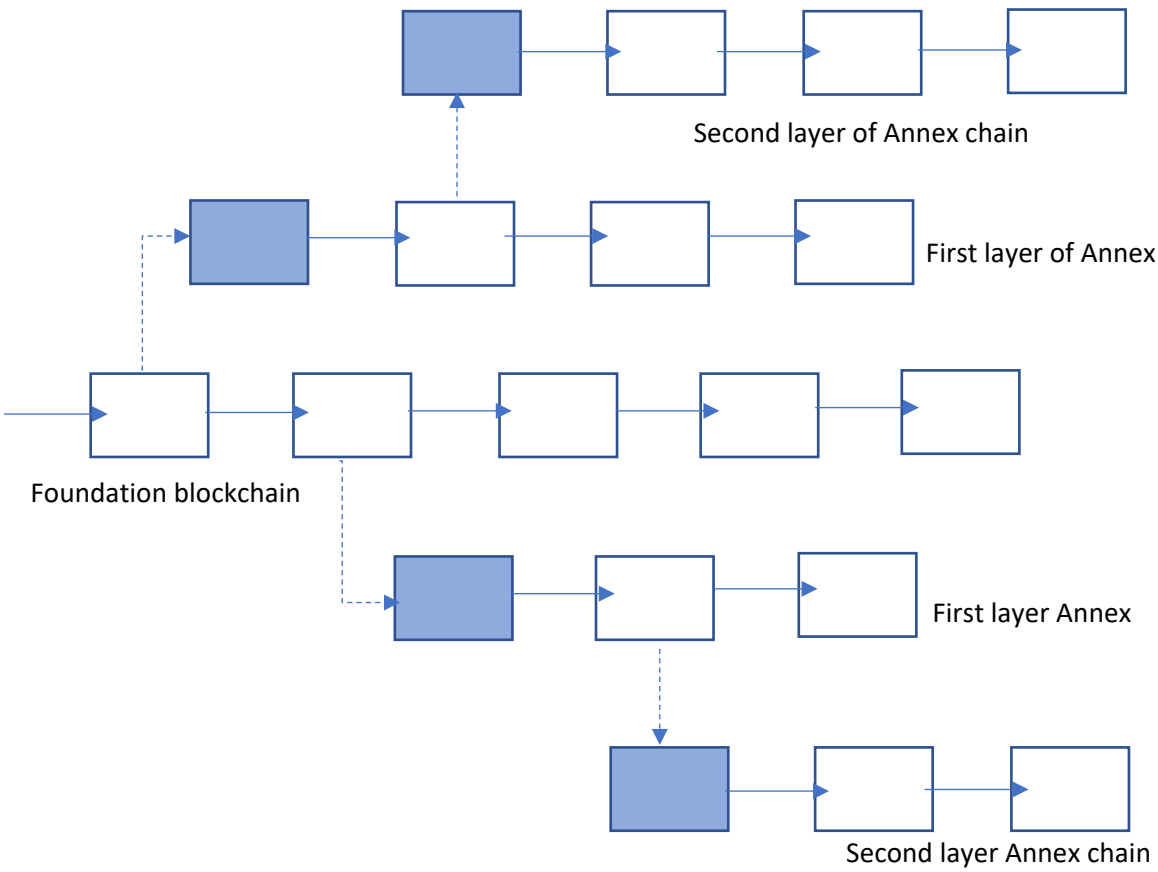

Figure 16. Hierarchical Annex-chain Architecture

Hierarchical multi-layer Annex chain architecture, that is, a new Annex-chain can be derived from an existing Annex chain, the existing Annex-chain is called parent chain, and the newly derived chain is called child chain.

In the hierarchical Annex-chain system, the KanBan of the child chain is placed in and maintained by the parent chain nodes, so the Annex chain core program contains the KanBan module, it can be configured and activated when needed.

Since the first byte of the four-byte chain-code segment in the CCUA address is used to express the depth and the remaining three bytes are used for the chain numbers, the entire system can be with up to 256 layers of Annex-chains, each layer can have up to 16,777,216 Annex chains in maximum.

2.3.13 Value System and Consensus in Annex-chain

In general, the Annex-chain uses the same value system as the Foundation blockchain, that is, the Foundation chain's currency circulating and trading in the Annex-chain directly, the prerequisites is that all its antecessors use the Foundation currency.

However, the FAB system supports the Annex-chain customizing its own value system and consensus mechanism, the purpose to do so is to enhance the FAB ecosystem's flexibility and adaptability. For sake of business needs, an Annex-chain can issue its own currency to maintain its own independent value system.

In the multi-layer architecture, parent chain KanBan maintains transaction and account state for its child chains, if the Annex-chain uses the same currency as its parent chain, transaction between them can be implemented freely, if the child chain uses its own currency which is different as its parent's, transactions between them are limited as in-layer conversion first.

2.4 Open Storage Architecture (OSA)

The Open Storage Architecture is one of the three major components of the FAB system, it is very important for building up the decentralized ecosystem.

2.4.1 Design of Open Storage Architecture

The Open Storage Architecture fully supports both the value-chain transaction and the business affairs chain transaction and business data, it constructs the map/reduce function model with MapReduce technology for big data quick query.

The Open Storage Architecture not only supports quick queries for blockchain based data and transactions, but also supports quick query of content-based public information relates to the business affairs chains, while serving the FAB system, it is building the resources repositories for next generation search engine in blockchain era.

The FAB system is design to stimulate the incentive mechanism to attract service providers to join in, there are three aspects: the first is to take storage fee as the income; the second is to support the use of MapReduce function to participate in the Annex chain's consensus and obtain profit by decision-making; the third is to take benefit from the public open business data, it is the basis of next generation search engine.

In order to support large volume communication and big data concurrency, the system architecture design scheme uses sharding technology in the database layer to support the horizontal expansion of the database, sharding technology can be used in Annex-chain as well for process ultra large volume of transactions.

Overall Logic Architecture of OSA:

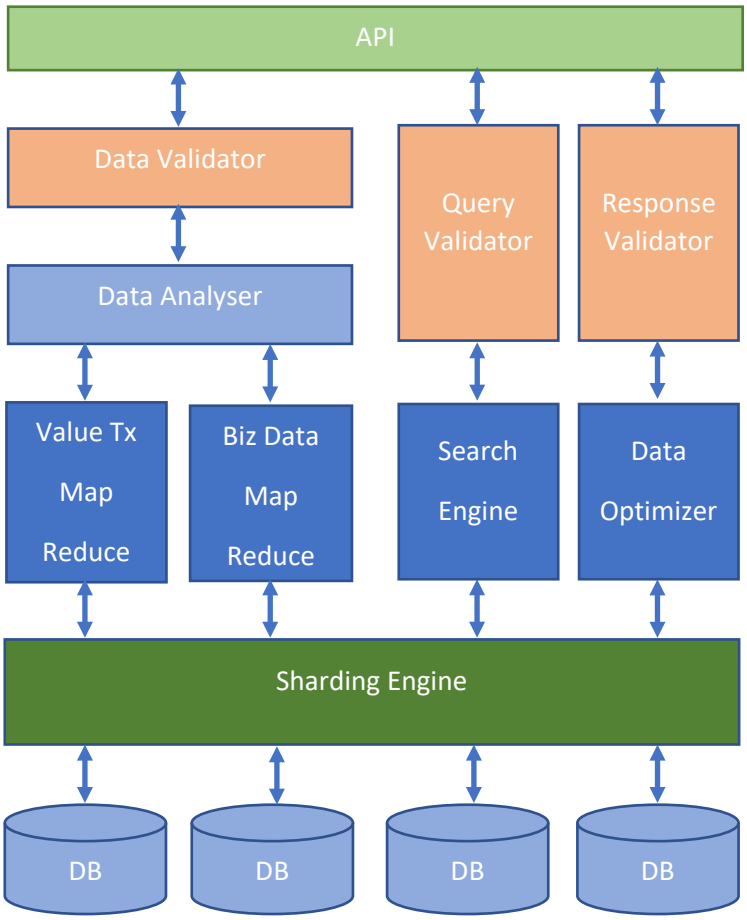

Figure 17. Overall Logic Architecture of OSA

The design of the entire storage system, like the public blockchain system, uses an open system architecture, where service providers and users are free to join in.

2.4.2 Core Architecture of OSA

In addition to the data storage architecture, the Open Storage Architecture is with p2p protocol, connection management and communication interface that compatible with the blockchain also, this will let an OSA node can join the network easily.

The Open Storage Architecture node participates in the Annex-chain consensus mechanism through the p2p network also.

An Open Storage Architecture node may be associated with multiple Annex chains, providing data storage services for multiple Annex chains and participating in multiple Anne-chain's consensus mechanisms

Core Architecture of OSA:

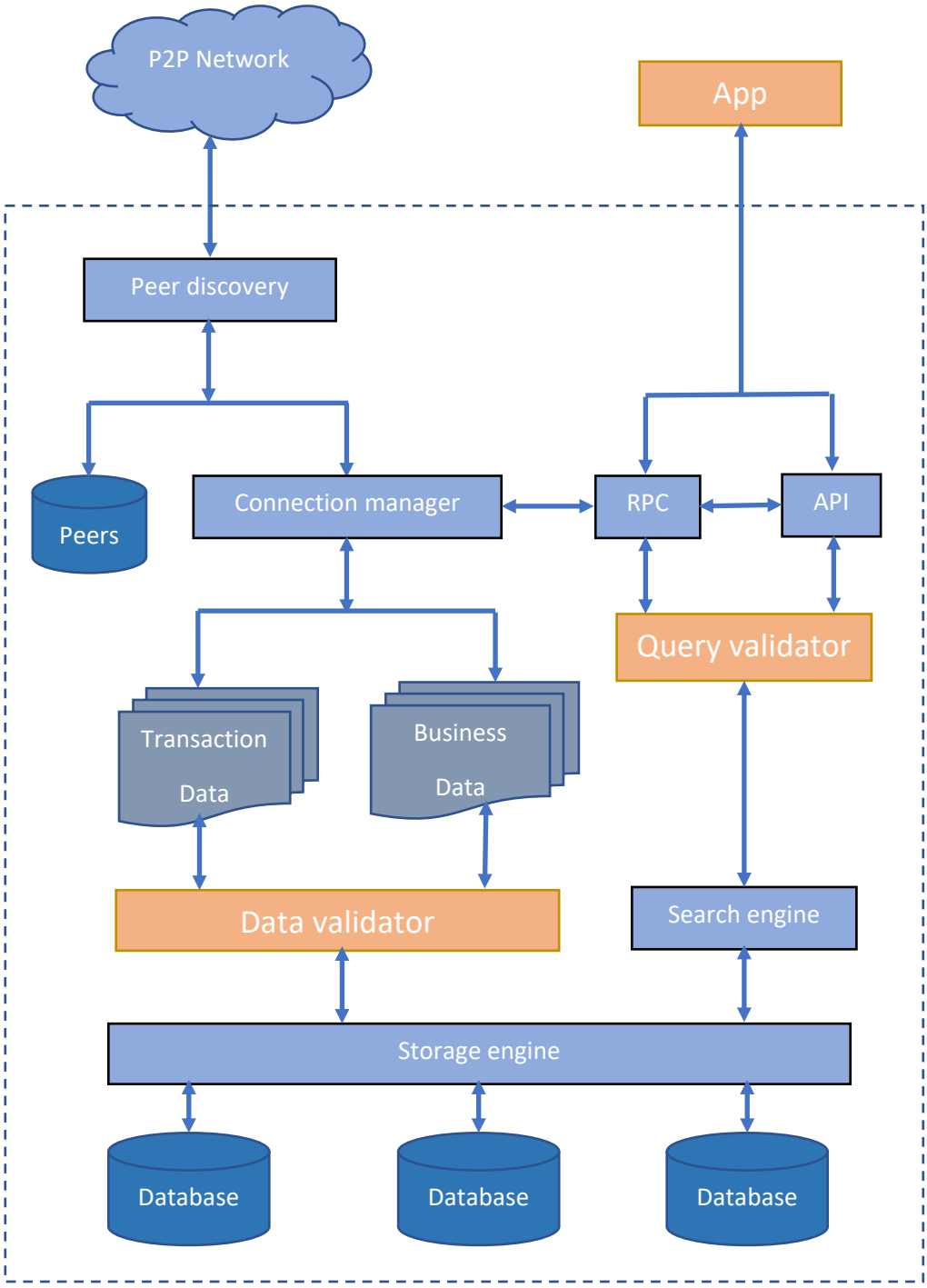

Figure 18. Core Architecture of OSA

2.4.3 The Incentive Mechanism of OSA

The incentive mechanism of the Open Storage Architecture is developed by smart contract of the Foundation blockchain. In principle, the storage node can freely formulate its storage rate, however the rate will be taken as a parameter to join the PoS consensus mechanism. The higher the rate, the lower the voting power. The formula for calculating the weight is:

$$W = V / R$$

Where: W – Voting weight;

V – Voting value;

R – Storage rate.

An OSA node immediate income include storage fee and PoS decision-making rewards; potential income is data source which is the basis of next generation search engine.

3. Value System

The FAB system uses a unified base currency system - FAB coin, which is the abbreviation of Fast Access Blockchain, it is the value basis of the whole ecosystem, is used in all the three major components as standard value unit for any fees, costs, rewards, spending and exchanging.

A total of fixed 200 million coins, of which 8 million are reserved for development and marketing, 24 million are to be distributed through ICO, and the remaining 166 million are to be produced by mining, the mining mechanism is similar to the bitcoin at the beginning.

References

1. A method of validating external data block by Bitcoin transaction to construct new blockchain, Paul Liu
2. Using Smart Contract Account Routing (SCAR) to Streamline Transactions, Paul Liu
3. A method of constructing scalable blockchain by using KanBan to update off-chain state, Paul Liu
4. Bitcoin: A Peer-to-Peer Electronic Cash System, Satoshi Nakamoto
5. The Business Blockchain–promise, practice and application of the next internet technology, William Mougayar
6. Omni Layer Specification, https://github.com/OmniLayer/spec
7. Enabling Blockchain Innovations with Pegged Sidechains, Adam Back et al
8. Blockchain – Blueprint for a new economy, Melanie Swan
9. Mastering Bitcoin, Andreas M. Antonopoulos, O'REILLAY, First Edition, December 2014