FAB
Fast Access Blockchain

WHITEPAPER
October 10, 2017

FAST ACCESS BLOCKCHAIN

A Highly Scalable Public Blockchain Network

FAB Foundation
215-7300 Warden Ave, Markham ON L3R9Z6
Canada

Website: http://www.fabcoin.org

CATALOG

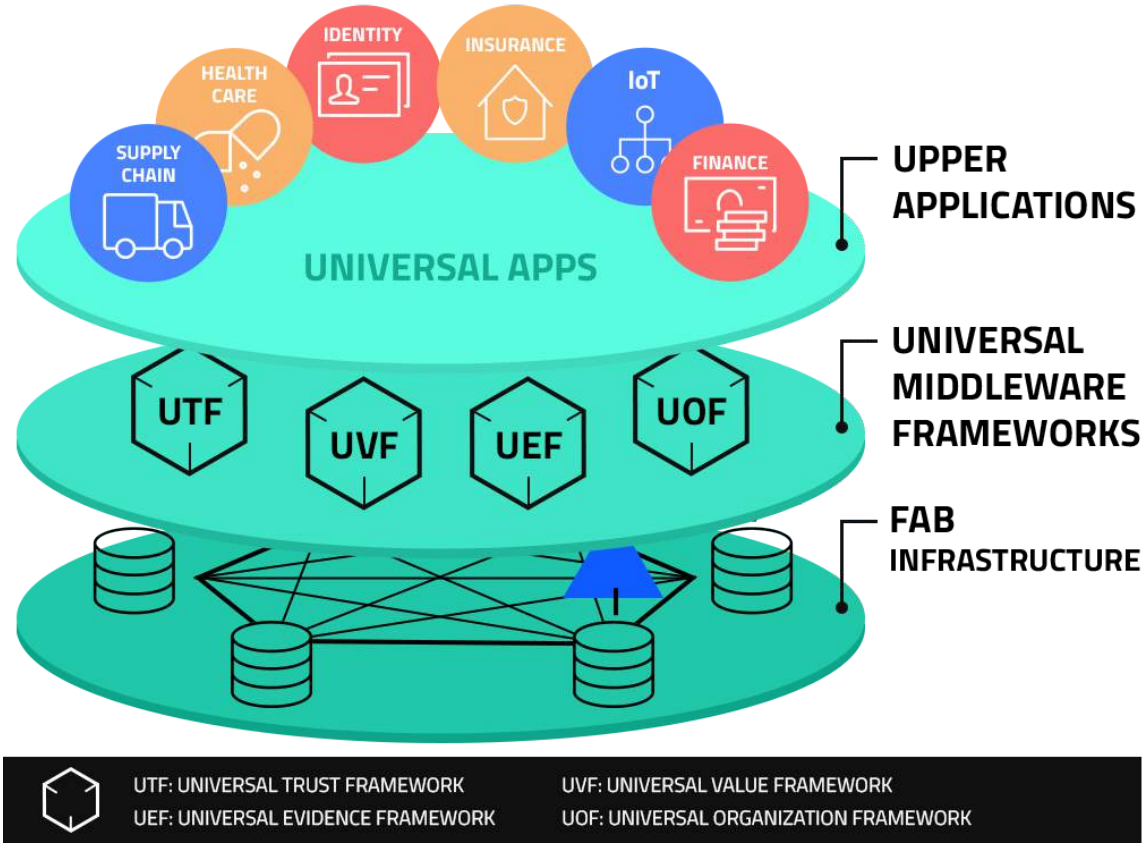
Abstract: The blockchain for high performance enterprise and ecommerce applications.

The use of blockchain in enterprise applications is significantly hindered by the limitations of the currently existing systems.

- The Bitcoin public blockchains do not have the levels of transaction processing performance required for enterprise applications.
- The complexity of developing applications for/on the Bitcoin blockchain cans make it difficult and time consuming for developers unfamiliar with the underlying technologies.

The Fast Access Blockchain(FAB) is capable of processing 1 million transactions per second while maintaining security, double spend protection, and decentralization.

The FAB Universal Framework Application Development layer shields developers from the underlying complexity of the blockchain and makes it easier and faster for them to deploy applications. This makes it possible to rapidly deploy blockchain applications and make them available for monetization in the FAB Application Marketplace.



1. SUMMARIES

Scalability is one of the major bottlenecks in public blockchain platforms. While the successful operation of Bitcoin, Ethereum and similar systems has inspired great enthusiasm for blockchain technologies, the transactional capacities are severely limited on most of the blockchain platforms that are available. The most popular platforms - Bitcoin and Ethereum are able to handle no more than seven to fifteen transactions per second.

This level of performance is unacceptable for enterprise level applications. Almost any business application will exceed the transactional capability of the existing blockchain platforms. Simple applications like ecommerce websites need more capability and more intensive systems and supply-chain automation or Internet of Thing platforms will never be able to perform at business level speeds with what is available today.

The very nature of public blockchain p2p networks are constrained by nodes whose functions and degree of participation may differ significantly. Most experts agree that that there is no simple way to break through this barrier by working with the base system and instead another solution must be pursued.

There seems to be an ever increasing demand in the enterprise sector to use Blockchains for the underlying processing of business applications. This makes the quest for a solution to the transactional performance issues critical, while still maintaining the benefits gained from using blockchain platforms.

This paper proposes the Fast Access Blockchain network (FAB). FAB is a complete solution for constructing a practical public blockchain ecosystem with high scalability, effective security, reliability, decentralization and the flexibility to develop multiple application types.

FAB is based upon a dedicated underlying protocolized framework design, middle layer smart contract enforcement, and an upper layer functional architecture implementation. It will allow blockchain technologies to succeed in real commercial use cases.

FAB foundational blockchain is composed of three key components:

The Foundation Blockchain

The Annex Blockchain and

The Open Storage Network

These three components are designed with a unified protocol and streamlined logic process. They integrate with each other to create a complete ecosystem with features of powerful scalability, strong reliability and true decentralization.

1.1 PRINCIPLES AND PHILOSOPHY OF THE PROJECT DESIGN

The strict design logic of the FAB network is based upon rigorous design principles and philosophies. The distinctive nature of blockchain platforms conflict with enterprise application requirements. In order for a blockchain to be used in applications like supply chain automation, the network must be able to perform to the demands of the full scope of the applications intended for their use.

1.1.1 Design Principles

Constructing Trust - One of the core missions of blockchain applications is to be able to build trust across a trustless system.

Decentralization - A primary feature of all blockchain systems is that by their very nature, they are decentralized and decentralization is the building block for building trust. You cannot have one without the other in a public blockchain system.

Open Source - Open source is critical to the idea of a public blockchain and makes the entire ecosystem examinable and more trustworthy for everyone involved.

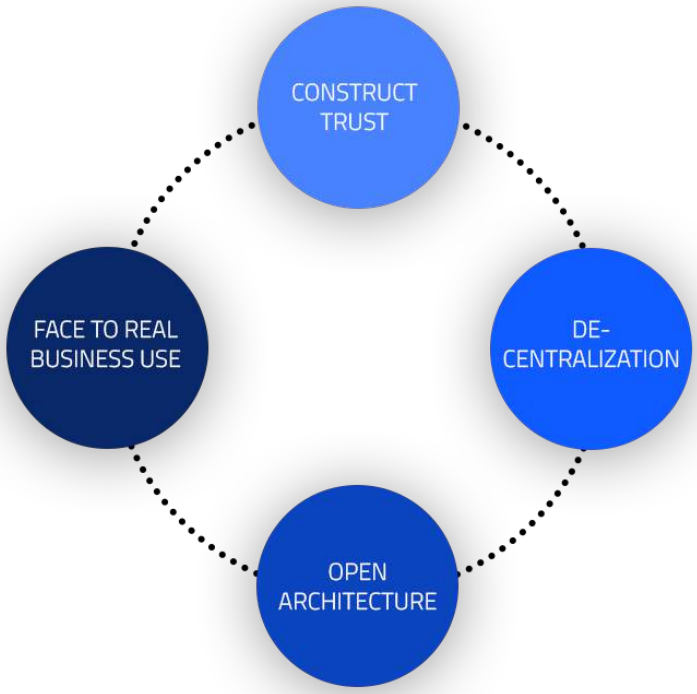


Diagram 2. Principles and targets relations in project design

1.1.2 Philosophy

Building a blockchain system according to the above design principles will be controversial. There will be claims that you cannot make the system decentralized, scalable, and reliable at the same time.

Currently, if a blockchain system is decentralized and scalable, it is unreliable. If it is scalable and reliable, it then becomes centralized. If it is decentralized and reliable, it is unable to scale up.

After much research, the following four declarations are stated in support of the philosophy that decentralization, scalability, and reliability can be realized simultaneously:

- Trust is built out of distrust - Blockchains secure trust between parties that do not trust each other by securing and recording transactions across the network.
- Scalability may be possible in non-scalable environment - a decentralized public blockchain is non-scalable while specific nodes may be scalable, because a specific node may be equipped with more powerful processing devices.

- Centralization is convertible to decentralization - it is possible to convert a centralized structure into a decentralized one without reshaping the entire system.
- Reliability can be created from an unreliable system - by disconnecting related elements in an unreliable system it is possible to convert it into a reliable system.

1.2 TECHNICAL FACTS

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

1.2.1 How to Overcome the Inherent Weaknesses in Current Blockchain Technologies

To overcome the hindrances to performance, we propose a theoretical resolution - constraints dislocation.

Our idea is to build a decentralized infrastructure using three primary components: The Foundation Blockchain, the Annex Blockchain and an Open Storage Network. Each of these infrastructure components has advantages and disadvantages, but when combined together each component's disadvantages can be addressed with another component's advantages. This allows us to connect one component to another as a closed loop, which in turn creates a complete platform that is decentralized yet scalable and reliable.

The design ideology:

Open Public Blockchain - The foundation blockchain is highly decentralized and very reliable but has poor scalability. Its purpose is to be the primary trust provider and final decision maker on the chain. It is expected to process a normal amount of data with ordinary calculation ability and to moderate network bandwidth. It is the basis of a decentralized ecosystem.

Adoption of Auxiliary Blockchain - The annex blockchain can be highly scalable for local implementation. It is a necessary component of the entire platform, but it is potentially centralized and untrustworthy.

Open Storage Network (OSN) - This is a decentralized data storage and consensus mechanism. An off-

chain data storage can be scalable but it is unreliable and untrustworthy and cannot constitute a completely decentralized system by itself.

Each of the three components has defects, but when joined together it will be shown they make up an ideal blockchain ecosystem.

1.2.2 Implementation Measures

Conceptually our solution makes sense, but just using the new concepts is not enough. Our solution requires additional technical components in order to make it successful and ensure the adherence to the design principles mentioned above.

There are three key technical components that make it possible for us to achieve our goals as stated above:

KanBan

Smart Contract Address Router (SCAR)

Sharding

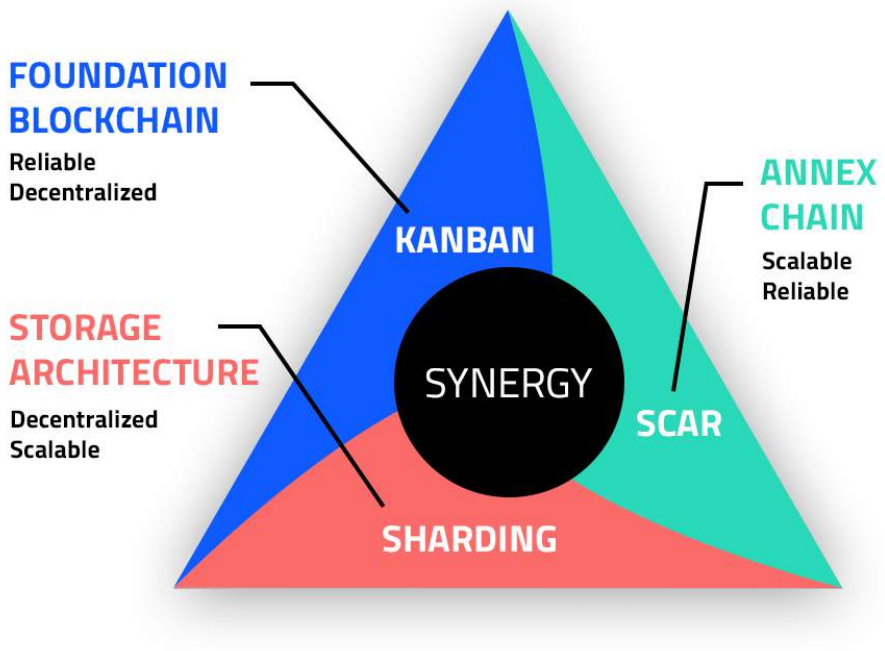


Diagram 3. Close loop of constraints dislocation

These three components work in conjunction with the Foundation Blockchain, Annex-chain and OSN. Sharding is taken from existing big data technology and is used for rapid data queries and consensus decision making throughout the ecosystem. KanBan and SCAR are two new concepts we are introducing to the blockchain system.

Sharding in the FAB system is different than in normal big data applications, it follows a rule for blockchain global searching, i.e., it's

compatible with the protocol defined by the foundation chain.

Foundation Blockchain + KanBan - Annex Chain + SCAR - Open Storage Network + MapReduce forms the complete solution.

In order to make the platform streamlined for easier implementation and wider adaptation, 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 across the entire platform, while CCSPV and CCTIP are needed to connect to third party blockchain systems, are omitted in this paper to be covered in another paper.

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

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

2. TECHNICAL SOLUTIONS

It is widely recognized, that the current bitcoin blockchain infrastructure is incapable of handling a large number of transactions per second due to the varied processing capabilities of nodes on the network and the constraints of the consensus mechanism. This limitation means that it is impossible for enterprise performance level applications to be built upon the existing bitcoin blockchain.

2.1 SYSTEM OVERALL ARCHITECTURE

The FAB network consists of three components: the Foundation Blockchain, the Annex Blockchain and the Open Storage Network, it is based on the contradictory dislocation mechanism and the core rules of the unified underlying protocol and consensus mechanism. Each is a component of the trustworthy eco-system. Each component has its own special role in the FAB ecosystem to create a platform with mutual collaboration and mutual verification in order to create a guarantee of trust and value while solving the decentralization, scalability, and security coexistence problem of the current Bitcoin blockchain.

Overall Architecture:

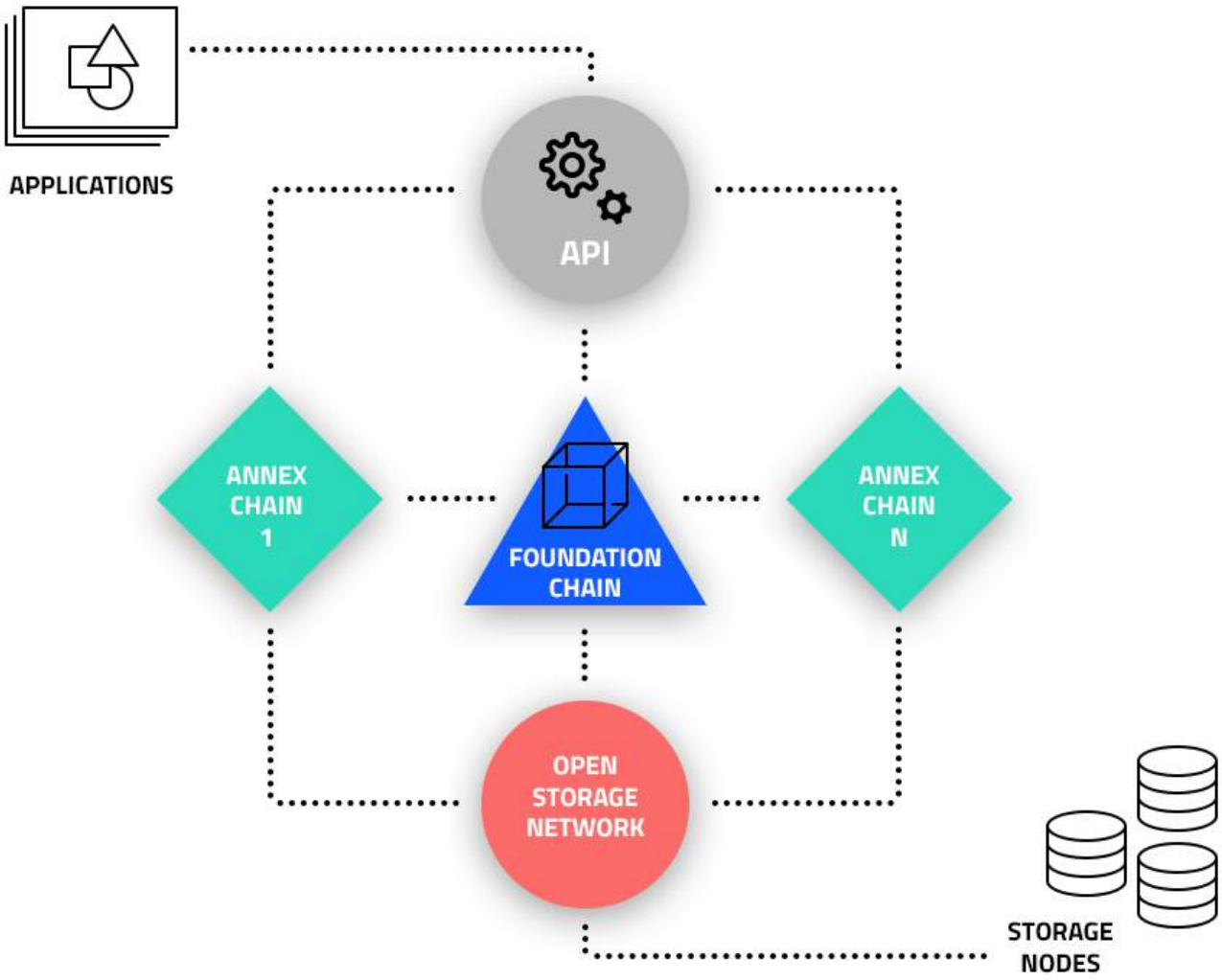


Diagram 4. The Overall Architecture

Unlike the current mainchain / sidechain design applied to Bitcoin or other blockchain platforms, FAB's Foundation Blockchain, Annex Blockchain, and Open Storage Network mechanism is designed from the ground up so that the data encryption/decryption algorithm and verification process are compatible with each other. It is a decentralized system with high efficiency and security assurance. It avoids the centralization problem and improves efficiency and makes the system safe, reliable and flexible for configuration. One can freely join the network as a node with powerful local transaction processing capability.

The design ideology of the FAB system is that the base blockchain uses the minimum data volume, calculation capability, and network bandwidth requirements to provide the core underlying protocol, the smart contract, the root ledger, and will have the final decision rights over all transactions. The Annex chain or the local node performs large-scale local off-chain transactions for its business needs. The Open Storage Network is to ensure

that the local data in the auxiliary chain can be stored in a decentralized way.

Three key technologies are introduced in the proposal: KanBan, SCAR and CCUA. These technologies enforce the states of local transactions on the annex-chain and can be updated and monitored globally in real-time across the entire blockchain network, in order to prevent double-spending and make the system meet the need for large scale transaction scenarios. This can include exchanges, IoT, ecommerce, supply-chain, medical services, etc.

In order to enforce decentralization for local transactions, the Open Storage Network will be introduced with economic incentives and mandatory rules. It is enforced by smart contracts and a consensus mechanism to force the auxiliary chain or localized nodes to support the use of decentralized storage.

The incentive mechanisms for the Foundation Blockchain are mining rewards and transaction fees. The incentive mechanisms for the Annex-chain are business profits, local transaction fees, and decision-making rewards in the consensus. The incentive mechanism of the Open Storage Network 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 focused upon minimum data volume, minimum calculation amount, and the minimum network bandwidth requirements. It contains the base protocol, the root ledger, the smart contract, and the value and trust system final decision rights. The Foundation Blockchain's legitimacy comes from all participating nodes.

The Foundation Blockchain will use a Proof-of-Production (PoP) consensus mechanism in conjunction with actual productivity. It is a specific type of Proof Of Stake(PoS), but a Proof of Work consensus mechanism similar to Bitcoin's will be used until sufficient scale of production can be achieved.

2.2.1 Partition function of Foundation Blockchain full node

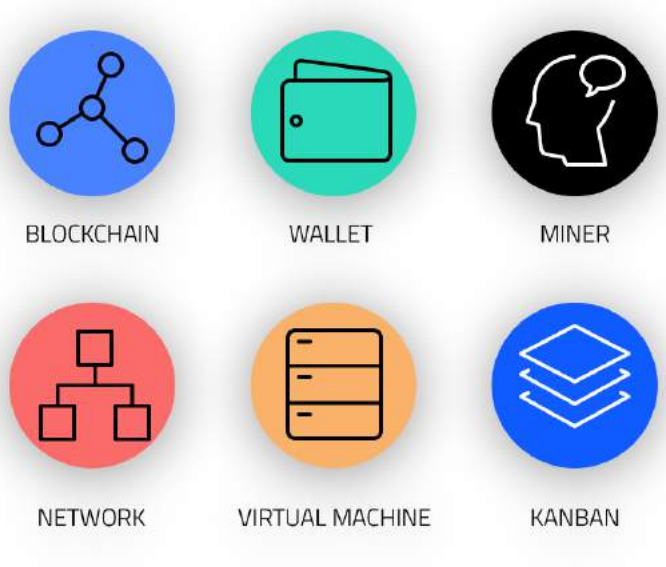


Diagram 5. Partition Function of Foundation Blockchain Full Node

In addition to the common blockchain, the wallet, miner, routing system, virtual machine and other functional modules, the Foundation Blockchain introduces a KanBan function.

KanBan means "watching board" in Chinese, which comes from the modern supply-chain / manufacturing-chain system where workers are engaged in fixed process work, but the KanBan system provides immediate information like a dashboard to keep track of warnings or changes.

2.2.2 KanBan

The KanBan is designed to provide real-time updates and querying capabilities for the 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.t

In the FAB network, KanBan runs in a GPU in the form of a memory data management program or an in-memory database within a node computer of the Foundation Blockchain. It can also run in a standalone computer that cooperates with the Foundation Blockchain providing state monitoring globally for the Annex-chain transaction. The KanBan is designed as a GPU-based in-memory database. The KanBan does not require the resources of an ordinary node. This helps to ensure that the Foundation Blockchain operates efficiently. GPU in-memory database processing is far more efficient than utilizing the computer's 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.t

The KanBan functionality facilitates decentralized transactions in the Annex-chain globally in real-time, thereby achieving the purpose of preventing double spending. However, since KanBan runs in the computer's GPU and takes up GPU memory, the miner software which also utilizes GPU features needs to be segregated and run on a different computer.t

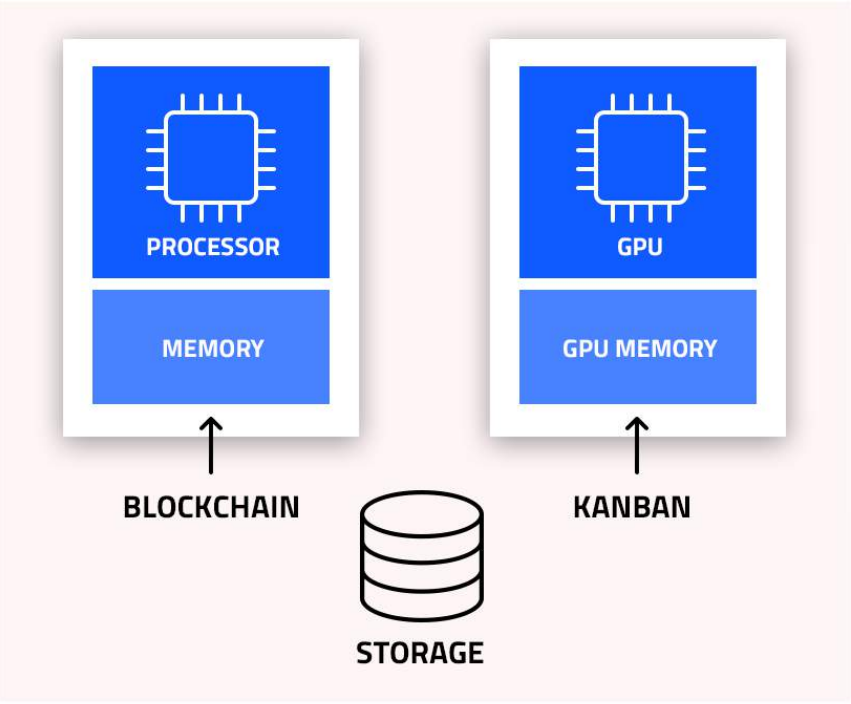


Diagram 6. Foundation Node KanBan Illustration

KanBan state maintenance and updates are controlled by smart contracts. This provides strict validation and verification relationships between KanBan, the Foundation Blockchain, the Annex Chain and the Open Storage Network to ensure that the KanBan data is accurate and legitimate.

KanBan's procedures:

1. **Receive the package from the Annex-chain**
2. **Verify the legitimacy of the package**
3. **Verify the legitimacy of the transaction**
4. **Update the KanBan state**
5. **Return the 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	ly8r5t4s...gte	9rc6ghd8fjcndu	goir7q3c9sk4ge8rd3afrb	400	20160508T223611
...	...	...			...
n					

Diagram 7. Annex Chains Table in KanBan

Address (Account) State

Address	Balance	Locked	Timestamp
0m5frtfgdesr.....	200000	F	20160312T100325
0msetvuehfe.....	16000000	T	20160520T081220
...	...		...

Diagram 8. Address (Account) Table in KanBan

Unlocked Transactions Table

Txid	Address	Input Address	Amount	Timestamp
1	4ds5kgce3...vd3	309ew98gweio	40000	20160223T021405
2	ly8r5gdt4s...gte	9rc6ghd8fjcndu	1200000	20160508T223611
...	...	...		...
n				

Diagram 9. Unlocked Transactions Table in KanBan

Upon receiving data from the Annex-chain, KanBan verifies the legitimacy of the package and the transactions within it. If the transactions are valid it updates the state of the relevant address and returns the signed receipt as proof to the Annex-chain and simultaneously notifies the Open Storage Network with the updated node balance and the contract signature. If the verification fails, it rejects and notifies the Annex-chain.

KanBan can supply the current state of each activity in real-time to prevent a double-spending attack. It also provides the signature stub for the last block for each Annex-chain to confirm the validity of the block and the transactions that are included.t

2.2.4 Verifying transaction validity

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

If conflicts occurs on an address or account it will set priority based on the timestamp and if the timestamps are identical will choose by hash priority.

If a transaction conflicts, KanBan will set a warning flag on the address of the transactional conflict.

When an address is flagged as suspicious in KanBan it will check for full validity through all transaction records on the Open Storage Network.

In order to strengthen KanBan's processing performance, it was designed as a dedicated GPU data processing

program, thus KanBan can take advantages of a 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 the Annex-chain address state, KanBan participates in the PoS consensus for the Annex-chain as well.

2.2.5 Constitution of KanBan in Foundation Blockchain Network

KanBan may be run in a node computer of the Foundation Blockchain network that is not used for mining or it may run on a separate computer associated with the Foundation Blockchain node. It can also alongside the Open Storage Network node computer or an independent computer that accesses the Foundation Blockchain and OSN through the network. Technically, a node can be a KanBan only node without the Foundation Blockchain, Annex-chain, or OSN function activated at all.

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

The system design does not require that all nodes in the Foundation Blockchain be equipped with KanBan, but nodes with KanBan have a special KanBan flag in the nodes list.

Nodes without KanBan functionality do not participate in the KanBan services and do not participate in any Annex-chain consensus mechanisms. Nodes that provide KanBan functionality can earn consensus rewards from the Annex-chains, which are derived from a transaction fee in the Annex-chain.

It is possible to run full node functionality on computers that have higher end capabilities including the Foundation Blockchain, KanBan, Annex Chains and Open Storage Network nodes.

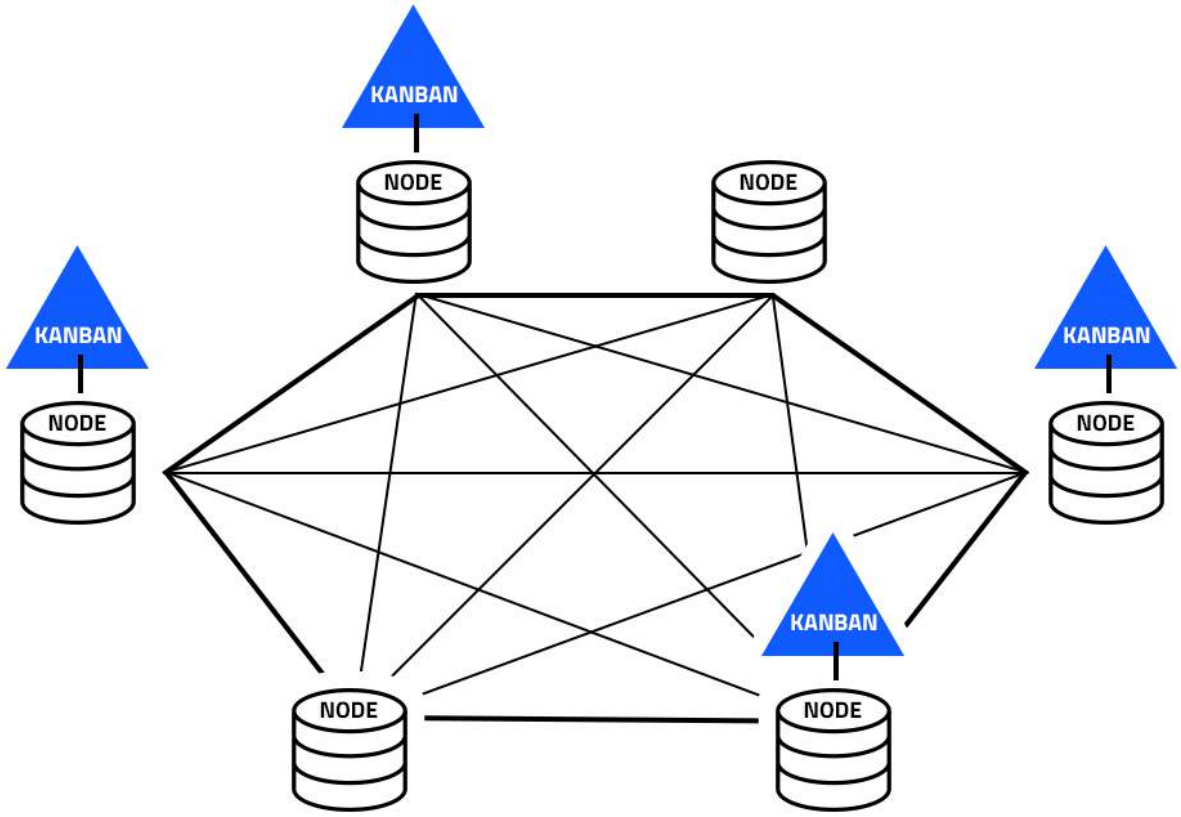


Diagram 10. Foundation Blockchain Network (Not all nodes are KanBan nodes)

2.2.6 KanBan Configuration Requirements

To activate KanBan functionality, a node computer is required to be equipped with a proper graphics accelerator(GPU) that can run the appropriate algorithm and with ample memory to handle the processing functions. The hardware requirement for the initial KanBan nodes is a GPU with no less than 16GB memory. This minimum requirement may change as the amount of data increases. Since no consensus issues will be affected there is no forking risk for upgrading GPU hardware after a KanBan node is running.

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 such as KB1 for 16GB and KB2 for 32GB, it should fit an Annex-chain's requirement at a minimum.

Assuming that 2GB of GPU memory is reserved for the computer's normal operations, then 2GB is reserved for Annex Chain related data, and the rest is used for the state table for all off-chain transactions.

An account state record will be no greater than 64 bytes allowing 12GB to contain about 200 million active account state records. If a 32GB graphics card is installed, it can provide about 500 million active account states.

The system is designed to support a KanBan grouping function which allows for a group of KanBan services for one or more Annex-chains.

2.2.7 Implementation of the Foundation Blockchain

The Foundation Blockchain is a refactored and improved version of the Bitcoin blockchain with key features added such as KanBan, SCAR and CCUA.

In addition, a virtual machine will be added to it for serving smart contracts.

The Foundation Blockchain will be equipped with functionalities to collaborate with the Annex-chain as well as the Open Storage Network.

Since the Foundation Blockchain is designed to serve as the root ledger, we have decreased the need for unnecessary data.

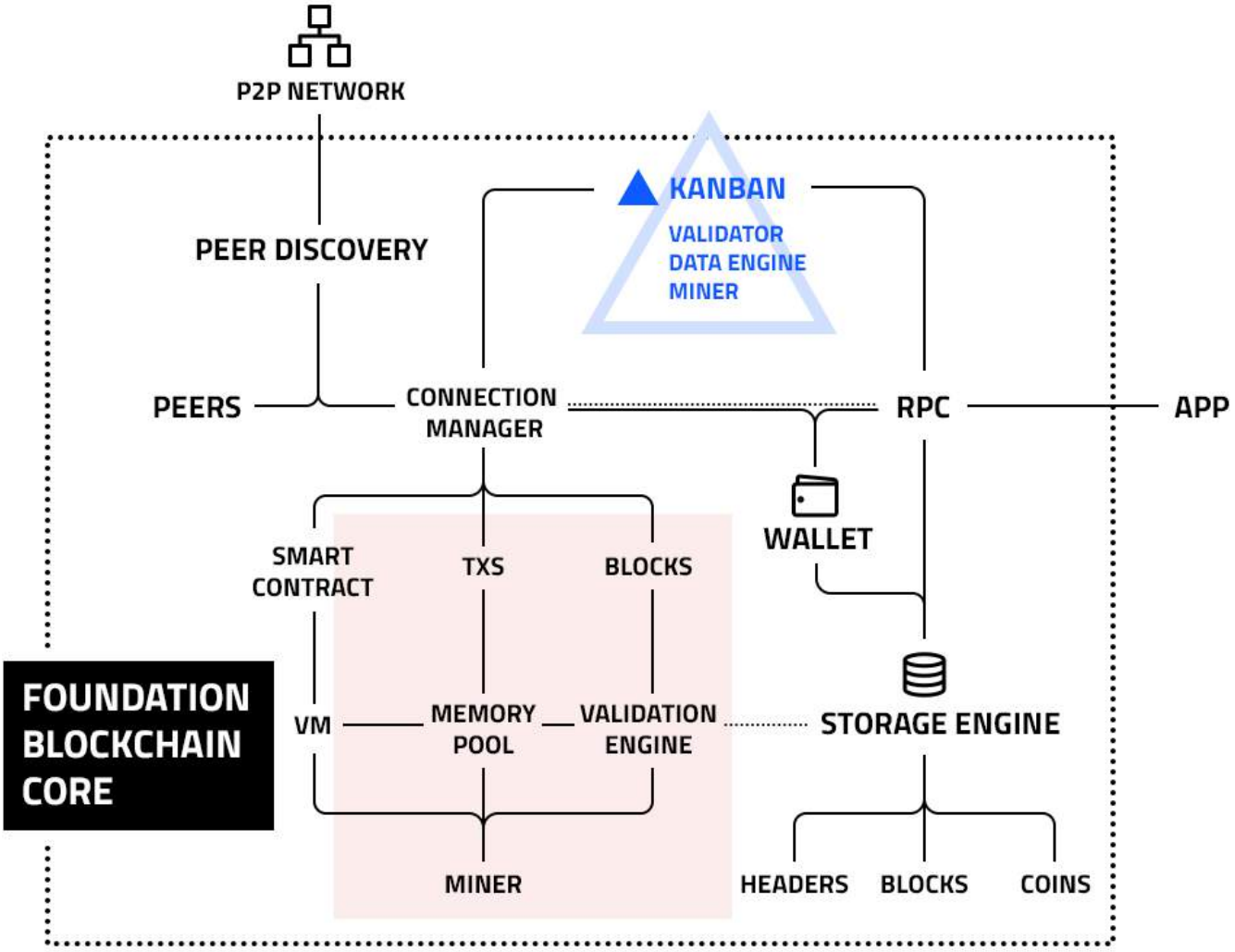


Diagram 11. Foundation Blockchain Core Architecture

Development of the Foundation blockchain will be governed by a streamlined architecture free of dependencies whenever possible. The goal is to 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 Network.

t

2.3 THE ANNEX BLOCKCHAIN

The Annex-chain is a critical component of the FAB system. Usually an Annex-chain node will carry a large number of transactions for a specific business use case, such as for an exchange, e-commerce transactions, supply-chain automation, an Internet-of-Things platform or a medical platform.

In a business point of sale scenario, an Annex-chain node may perform similarly to a how a typical centralized system may perform. It may carry a huge amount of transactions but according to the system design the final confirmation of value and state of the off-chain transactions are implemented in a decentralized way via KanBan. In accordance with having a decentralized data storage on the Open Storage Network, it is fundamentally guaranteed that local transactions on the Annex-chain with centralization and localization characteristics will have the features of decentralization, security and reliability.

According to the system design, even if an Annex-chain is deployed or designed for fraud it is unable to cause any loss to its customers, because account states are updated by the KanBan transaction data stored in the OSN and client applications. The central account of the annex chain SCAR is dominated by Foundation blockchain, but there is nothing dominated by the annex chain except calculation and communication for transaction processing.

2.3.1 Annex-chain technical structure

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

The design strategy is to dispose of the need for the primary network transmission and data processing as far as possible on the Annex blockchain and enforce the necessary transaction evidence and data submission through KanBan and OSN.

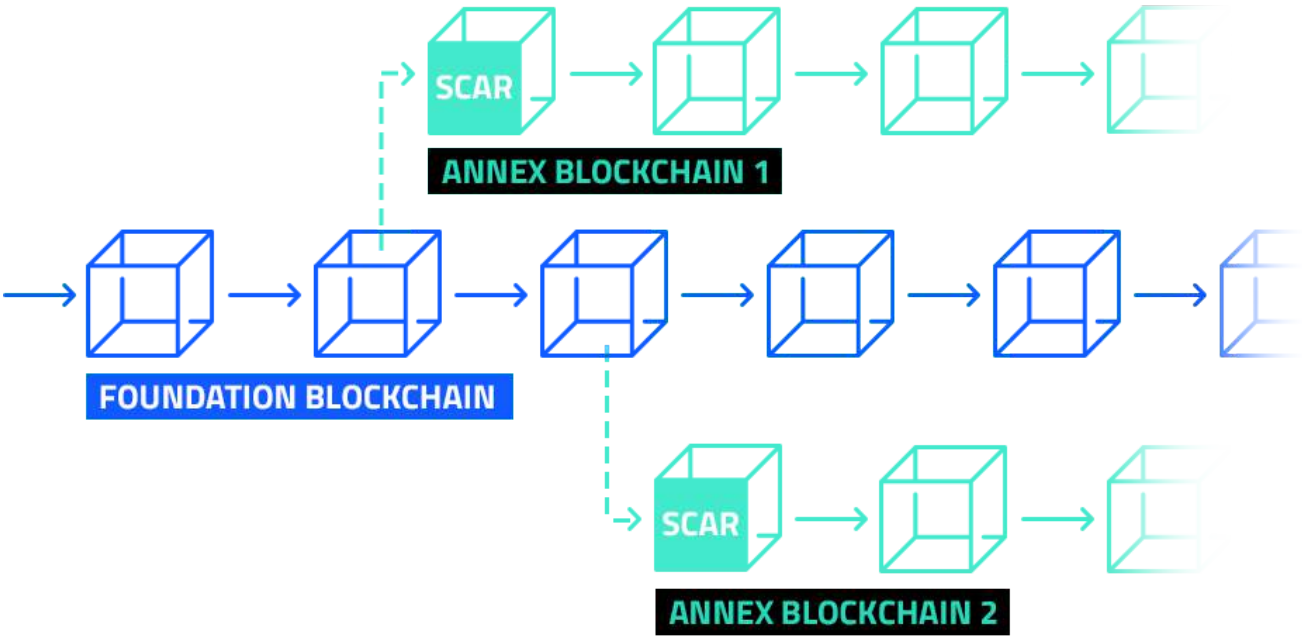


Diagram 12. Schematic Diagram of Annex Blockchain Structure

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 the sidechain is that the Annex-chain derives and uses the Foundation chain's currency directly while the sidechain always has its own currency no matter how newly created. The Annex chain is a part of the entire system while the sidechain is tied to the main blockchain.

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

The first block of the Annex-chain starts from a special block issued by the Foundation blockchain smart contract. It defines a special account for the Annex chain known as a Smart Contract Account Router (SCAR). SCAR 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 the value blockchain the other is the business affairs blockchain, used to serve the value maintenance of the Annex-chain and business affairs management respectively.

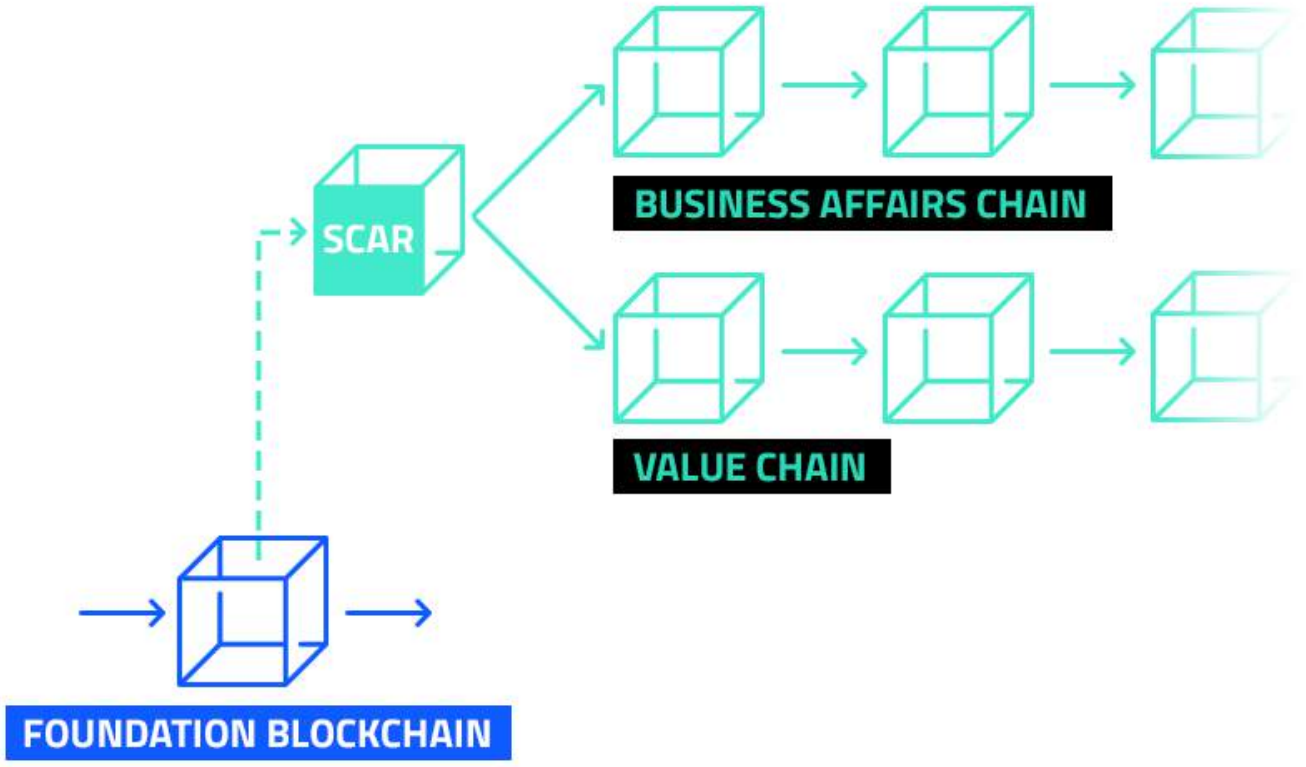


Diagram 13. Complete Double Chain Structure of Annex Chain

The Value chain records value transactions and The Business affairs chain records business logic and business data (Hash values).

This double-chain mechanism allows the system to build a 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 design documents.

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 a smart contract issued by the Foundation blockchain. The results and the final decisions are attributed to the Foundation blockchain.

The identity and attributes of the Annex chain are determined by the Foundation chain. The validity of its transactions are subject to the approval of the Foundation chain. The data storage on OSN 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 the Annex chain bear responsibility for communication and calculation as much as possible while the Foundation chain dominates validity and credibility.

The internal value maintenance of the Annex blockchain will be treated differently based on the situation:

When the Annex-chain value system is derived from the Foundation blockchain currency, which means it is implemented according to the Foundation blockchain's protocol and consensus mechanism. It is bound by the blockchain's smart contract, so it is subject to the blockchain's supervision and eventually accepts its decisions.

When the Annex chain is using its own independent currency its value is not derived from the Foundation blockchain and transactions related to the Annex chain are limited conditionally. Any transactions between the Annex and external systems can only be implemented as a 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 is submitted to the Foundation chain, this will result in the ID of the Annex chain, its private / public key pair, attributes, and smart contract being generated by Foundation blockchain. The data is stored in the first block along with timestamp and other data. The system supports KYC (Know Your Customer) function in an optional way, so as to confirm the 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 as well.

Each Annex chain will be generated with a unique account authenticated by the Foundation blockchain when it is initially created. Identified as a Smart Contract Agent Route (SCAR). This account plays a special role as the only

unique agent of the Annex chain, to execute transactions between the Annex and externals.

As a special account, SCAR is ruled and operated by a smart contract issued by the Foundation blockchain, No one can manipulate the account, not even the Annex chain 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 by implementing the Annex-chain's local transaction capabilities by updating internal address 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 as well.

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 created by the Foundation Chain. Its core structure and most of its functions are the same as the Foundation Blockchain. Some modules are shared between the two chains.

The Annex-chain has a separate consensus and miner and has more modules and options than the Foundation.

Since an Annex can customize and own its own currency and transactions, it can package, process, and submit data to the Open Storage Network features. The kernel of the Annex needs to contain the package process module, the KanBan communication capabilities, and the data exchange module along with the OSN data manipulating module, etc.

The core of the Annex-chain contains an important component - the SCAR process module. It plays the role of converting any 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 Network.

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 is shown as follows: (value component only)

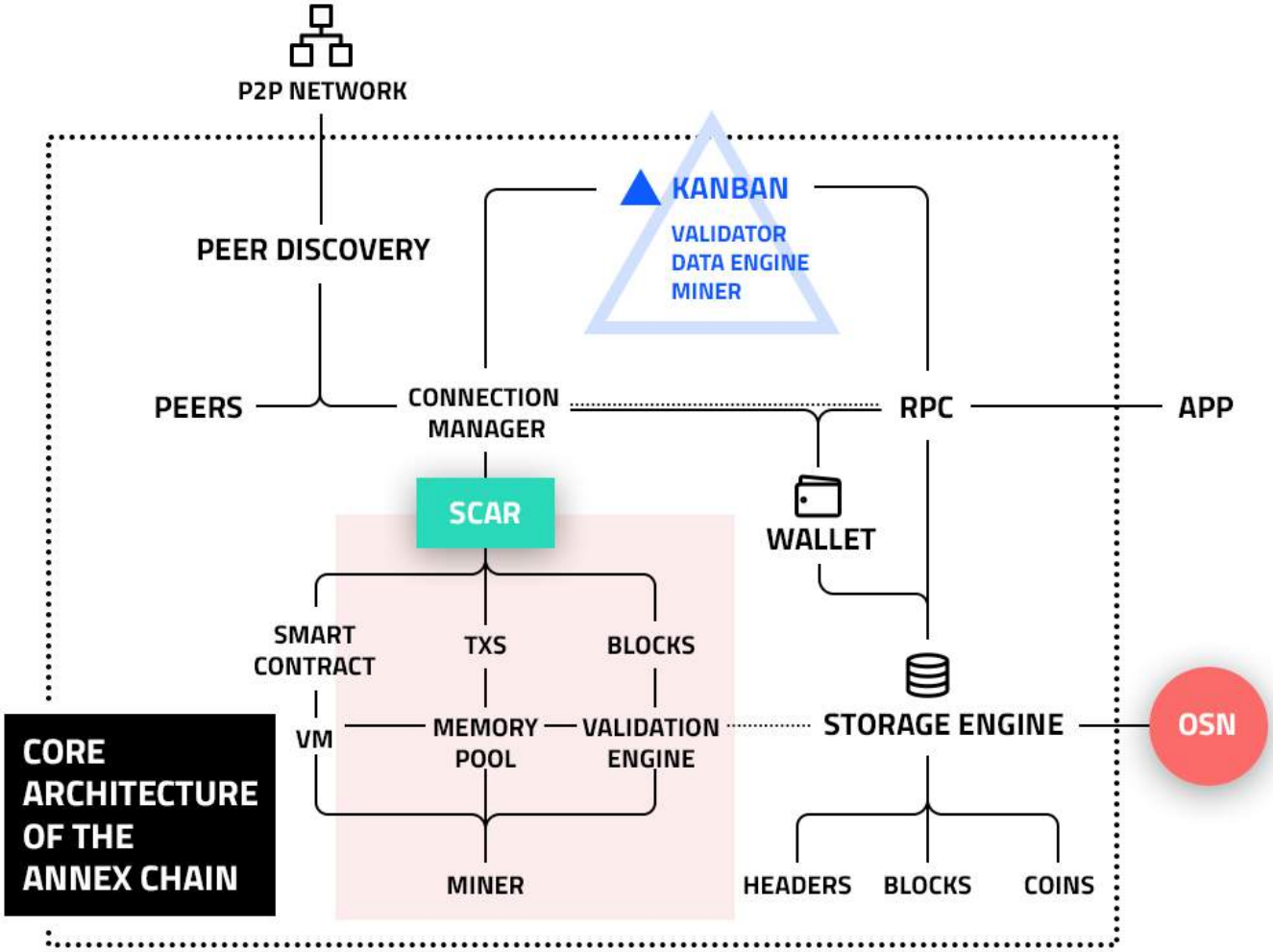


Diagram 14. Core architecture of the Annex Chain

The diagram shows the components structure of the Annex-chain within the system design. Since the Annex-chain supports the business data chain, there are more modules omitted. The following covers the value chain only.

2.3.5 Address Format

A set of special rules for address formats is designed within the system called the Cross Chain Unified Address (CCUA). These are address-specific rules with the same address-code segment belonging to the same owner and controlled by the same private key.

The specific rules for CCUA are as follows.

An address consists of four code segments, namely:

Address type code

Chain code

Address code

Verification code

The address type code is 2 bytes, currently 0m for the Foundation chain's PKH (Public Key Hash) address. 1a is for the Annex chain's PKH address.

The chain code takes 4 bytes, it stands for the unique id of the 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 use 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 are controlled by same private key, no matter from which blockchain it comes:

0m 0000 aaabbbccc123 y4sg

1a 0a4u aaabbbccc123 g8rj

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

Transactions between the Annex chain and the Foundation chain only allow for addresses belonging 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 with the same address-code as the Annex chain address.

An address in the Annex chain is a transaction state address. The address won't change after a transaction occurs, but it's state will be updated.

The Cross Chain Unified Address protocol provides a convenient means 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.

2.3.6 SCAR Account and Transaction

Each Annex chain has a special account called the Smart Contract Agent Route (SCAR). The authority 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. The smart contract relationship to the SCAR is established and controlled by the Foundation chain only.

SCAR is a special transaction hub in the Annex chain. Any transaction between two accounts in the Annex chain is converted into transactions between the SCAR and the participant accounts. All transactions between the Annex chain and the Foundation chain or other Annex chains are carried out through the SCAR account as well, so that all the transactions on the Annex chain are turned into a streamlined process. The reason for doing this is so that when an account in the Annex chain submits a clearance request to the Foundation blockchain, no consent is needed from related accounts. It is only one transaction between SCAR and the account and the SCAR is manipulated by the smart contract and will be executed automatically by miners. This reduces the amount of transaction data dramatically for the Foundation blockchain. In addition, SCAR plays an important role in preventing fraudulent transactions related to the Annex-chain.

The hub functionality of SCAR appears to be centralized because all transactions go through it, however the transaction is verified by the decentralized KanBan and data is stored on the decentralized OSN. The Annex chain itself does not have the right of adjudication, nor the exclusive rights to the data, therefore it is fully decentralized by its nature.

The private key of the SCAR is controlled by the 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 participant accounts.

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

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

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

For 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 the Annex chain's UTXO collection.

2.3.7 Transaction State of Annex Chain

The FAB system defines four states for valid transactions on the Annex chain. The states are executed, witnessed, confirmed, and completed and represent four different transaction states respectively.

When the Annex chain receives a transaction, the transaction is executed and generated and completed locally in a few milliseconds. This is an internal transaction on the Annex chain. If the Annex chain is one single full node, it equates to a centralized transaction. The trustworthiness of the transaction in this state is equivalent to the trustworthiness of the Annex chain as a whole.

When the Annex chain submits the transactions package to KanBan and receives the KanBan's confirmation, it is now in witnessed state. Typically this state can be achieved in several seconds to a few minutes from the time the transaction is initiated. Since it is submitted to the KanBan, the state of the transaction is maintained by the KanBan and its trustworthiness is enhanced. Since the submission to KanBan is the Annex chain's initial purpose, it is not manipulated by the Foundation blockchain. Therefore, the number of KanBan confirmations is taken as an important parameter to measure the trustworthiness of the transaction. The higher the number, the more reliable the transaction.

The block is generated on the Annex chain and is validated by the KanBan and stored on the Open Storage Network system. The state of the transaction is then confirmed. Typically it should complete in a few minutes from the time the transaction initiated. Once submitted to the OSN the data storage is decentralized and the transaction is trustworthy. Similar to the KanBan confirmations count, the higher the number of OSN nodes that are submitted, the higher the trustworthiness of the transaction.

When an account submits the settlement to the Foundation blockchain and completes, the transaction state is completed, it 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 transaction can be regarded as reliable, while a transaction in confirmed state means it has sufficient security to be guarantees. A large transaction can be recognized as assured.

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

2.3.8 Annex Chain Transaction Processing Flow

The Annex chain transaction needs to be verified by KanBan to prevent double-spending attacks and transactions are valid only through the KanBan's verification and receipt of KanBan confirmation.

Annex chain transaction processing flow shown as below:

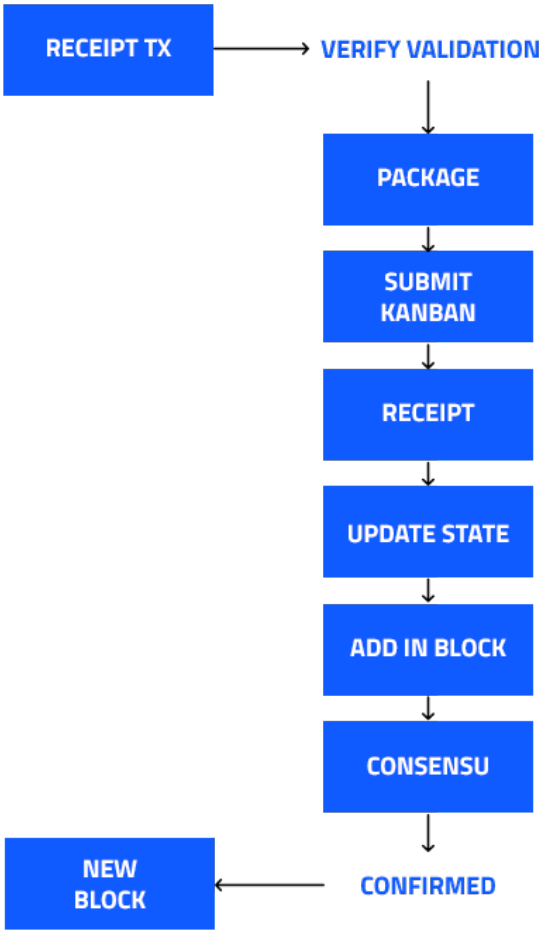


Diagram 15. Annex Chain Transaction Processing Flow

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

When an Annex chain receives a denied notification from the KanBan, it will remove the problem item and repackage it to be submitted.

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

A packet sent to the KanBan on the Foundation blockchain by the Annex-chain contains one or more transactions.

A transaction is validated globally after the Annex-chain receives verification from the KanBan. The more KanBan confirmations 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 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 by Annex chain nodes, KanBan and OSN 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 the KanBan and the block data is stored in the OSN nodes.

The transactions in the Annex chain are packed and sent to the KanBan nodes by Annex nodes and the KanBan nodes are no longer able 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. The data transmitted includes nonce, the last packet ID, and the merkle root. Nodes involved in the p2p network include all Annex chain full nodes, mining participating in the KanBan, and mining participating in the OSN nodes.

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

2.3.10 Double Spending Attack Prevention in Annex Chain

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

The Annex chain is invulnerable to double spending attacks and can not be implemented at all. The states of all the Annex chain's internal accounts are updated locally. Any node in the Annex chain can obtain the status easily in real-time.

If the Annex chain is deployed for fraud, the client application validates the transaction's validity through the KanBan and the Open Storage Network. The KanBan and Open Storage Network's validation mechanism will determine whether it is client fraud or Annex chain fraud. If it is client fraud, the transaction is invalid and the suspicious account in the transaction will be tagged with a warning flag in the KanBan. If the Annex chain is the source location of the fraud it will call the smart contract in the KanBan to invoke the investigation process. The review process will validate all unlocked transactions of the Annex chain and it's privileged SCAR account will be frozen until the completion of the investigation. If the Annex chain is determined to be fraud it will be suspended and can only be re-activated upon request and via a successful vote by the majority of all the participants KanBan nodes.

In case of a double-spending attack between the Annex chain and the Foundation chain the FAB system limits transactions between the Annex chain and the Foundation chain so that funds can only be transferred to related CCUA addresses. There is no possibility for double-spending attacks if vulnerability is eliminated in the Annex chain.

A cross Annex chain double-spending attack is when 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 and the attack was initiated by the client only:

   In this case, the transaction cannot be verified through the KanBan, the Open Storage Network, and the Annex chain nodes and the client can not obtain the state of the related account in time, so the transaction fails;

b) In the case where only part of the Annex chain nodes participating the attacks are dishonest:

   The client can verify the validity of the transaction through the KanBan and the Open Storage Network, but does not just go through the Annex chain nodes. If the transaction seems to be fraudulent, then the review process in the KanBan or OSN will be invoked to investigate the involved client and Annex chains;

c) In the case where all the Annex chains are involved in the double-spending attack are dishonest:

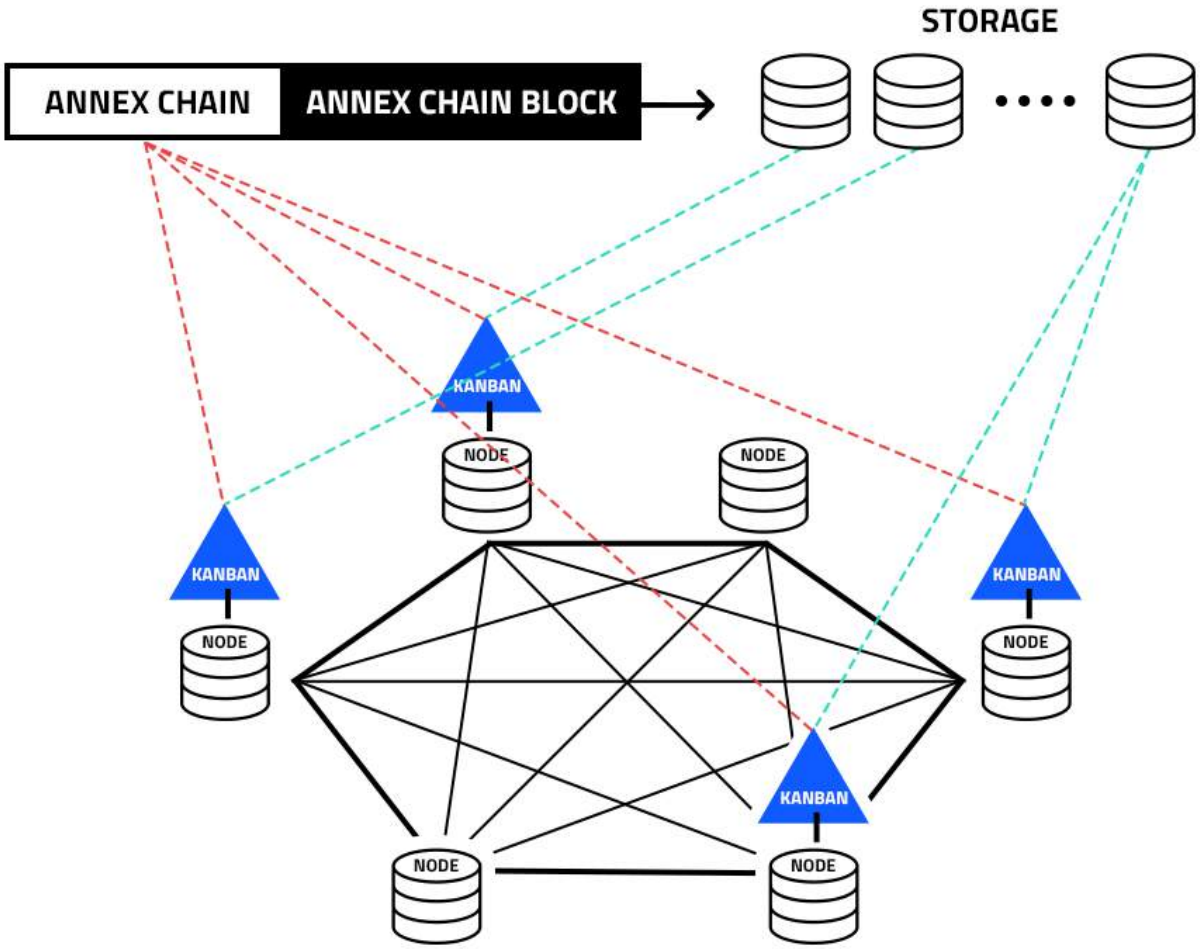
   Clients can be verified with the KanBan and the Open Storage Network. In fact, due to the establishment of the SCAR channels and CCUA, the more Annex chains involved in the cross-chain transaction, the higher difficulty for a successful attack because of more verifications of the attack process.

The KanBan and the Open Storage Network play critical roles in the process of preventing double-spending

attacks.

In addition, because the Annex chain's initiated time and its transaction amounts in history is stored in the Annex-chain table, in the KanBan and the OSN, it can be referenced as the Annex-chain's credit by clients.

Diagram 16. Verification Relation in the Whole System



2.3.11 Settlement of an Annex Chain Account

Transactions on the Annex chain are valid and effective globally. That is implemented and assured through the decentralized KanBan and the Open Storage Network.

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

When an Annex chain account submits a request to the Foundation blockchain for settlement, even if the Annex chain disappeared, crashed or hacked, or is otherwise not available, the settlement can be implemented successfully because the decentralized KanBan and Open Storage Network maintain the full state and detailed transaction records. Due to the establishment of the SCAR mechanism all Annex chain related transactions are converted into transactions between client accounts and the SCAR. While the SCAR is controlled by smart contracts on the 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 and the related records in the KanBan are deleted as well.

The Annex chain itself can request a settlement to a specific account or all accounts only through the SCAR account.

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

That is how the FAB system handles a large number of transactions while eliminating the need for the main Foundation blockchain to handle them.

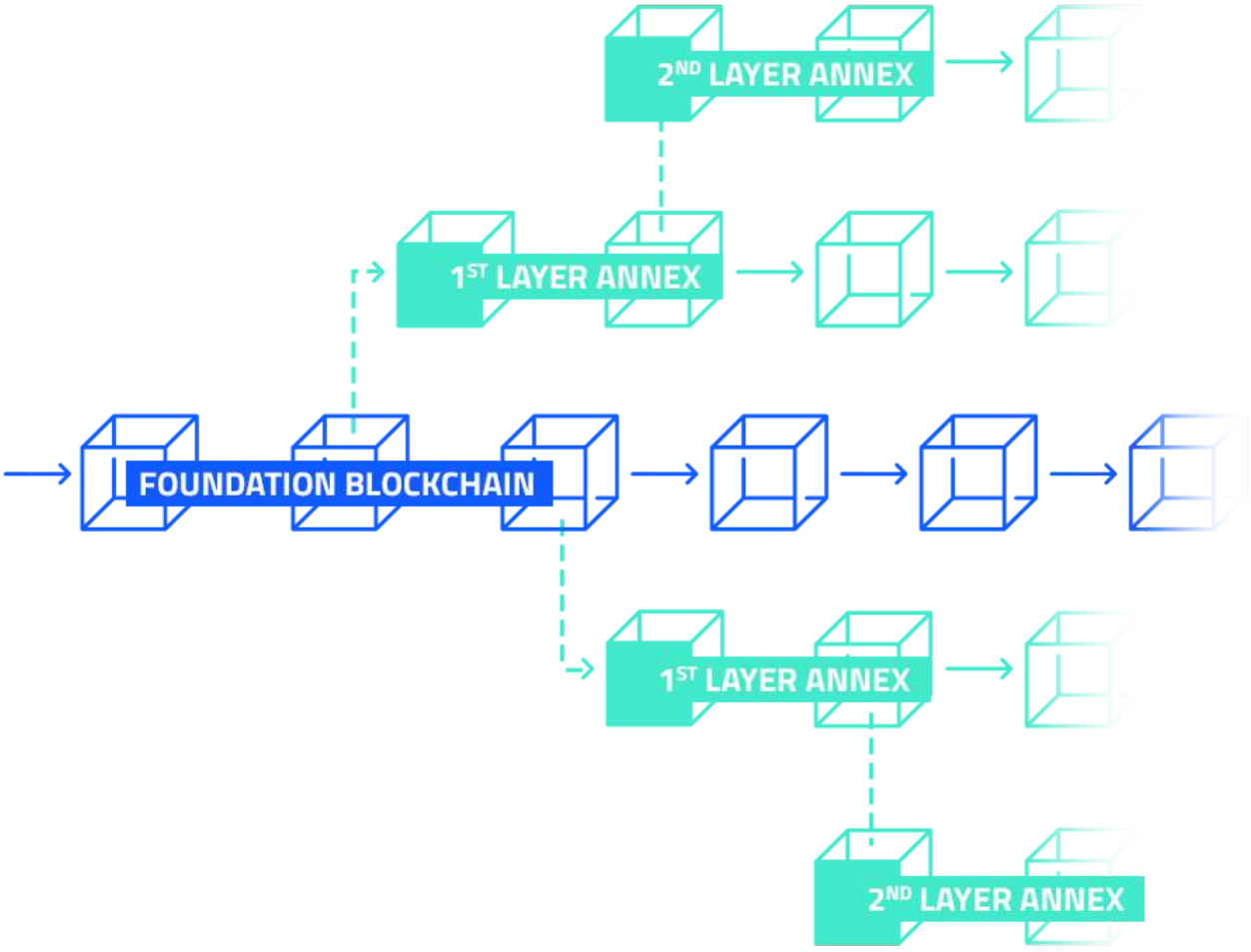
2.3.12 Hierarchical Annex Chain Architecture

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

Shown as below:

Diagram 17. Hierarchical Annex Chain Architecture

The Hierarchical multi-layer Annex chain architecture is a new Annex-chain that can be derived from an existing



Annex chain. The existing Annex-chain is called the parent chain, and the newly derived chain is called a child chain.

In the hierarchical Annex-chain system, the KanBan of the child chain is placed in and maintained by the parent chain nodes and the Annex chain core program contains the KanBan module. It can be configured and activated as 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 up to 256 layers of Annex-chains and each layer can have up to 16,777,216 Annex chains.

2.3.13 Value System and Consensus in the Annex Chain

The Annex-chain uses the same value system as the Foundation blockchain, because the Foundation chain's currency is circulating and trading in the Annex-chain directly. The only prerequisite 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 of this is to enhance the FAB ecosystem's flexibility and adaptability. For the sake of enterprise use cases, an Annex-chain can issue its own currency to maintain its own independent value system.

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

2.4 OPEN STORAGE NETWORK (OSN)

The Open Storage Network is one of the three major components of the FAB system, it is critical for building a decentralized ecosystem.

2.4.1 Design of the Open Storage Network

The Open Storage Network fully supports the value-chain transaction, the business affairs chain transaction, and the related business data. It utilizes the map/reduce function model with MapReduce technology to enable fast big data queries.

The Open Storage Network not only supports quick queries for blockchain-based data and transactions, but it also supports quick queries of content-based public information as it relates to the business affairs chains while still serving the FAB system. This allows FAB to serve as the building blocks for a next generation search engine in the blockchain era.

The FAB system is designed to stimulate the incentive mechanism to attract service providers to join in. There are three aspects to this strategic design. The first is to take a storage fee as 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 as is the basis for a 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 the Annex-chain as well for processing ultra-large numbers of transactions.

Overall Logic Architecture of OSN:

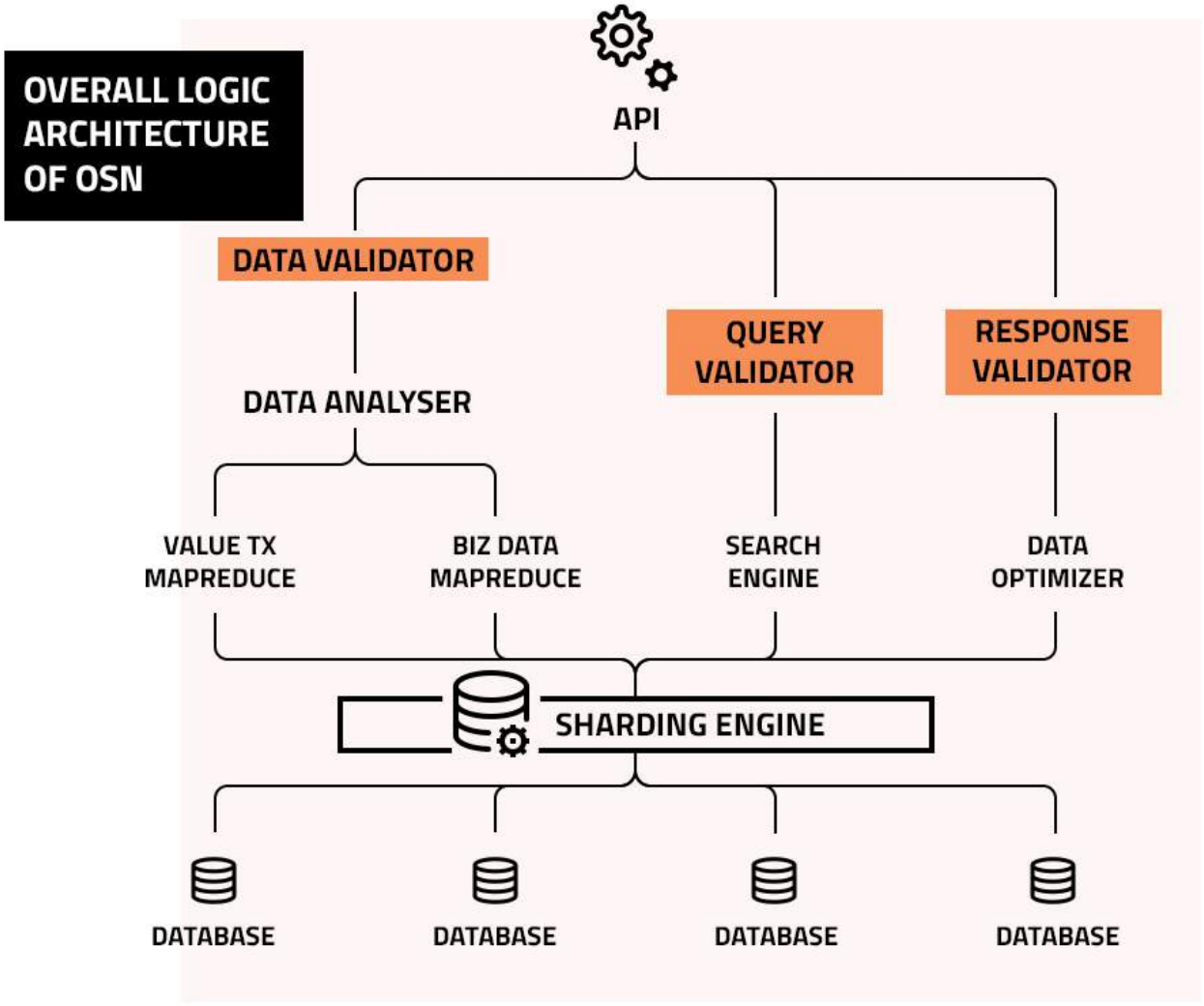


Diagram 18. Overall Logic Architecture of OSN

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 OSN

In addition to the data storage architecture, the Open Storage Network has a p2p protocol connection, connection management capabilities, and a communication interface that is compatible with the blockchain. This makes it easier for an OSN node to join the network.

The Open Storage Network node participates in the Annex-chain consensus mechanism through the p2p network as well.

An Open Storage Network node may be associated with multiple Annex chains and provide data storage services for them while participating in multiple Annex-chain consensus mechanisms.

Core Architecture of OSN:

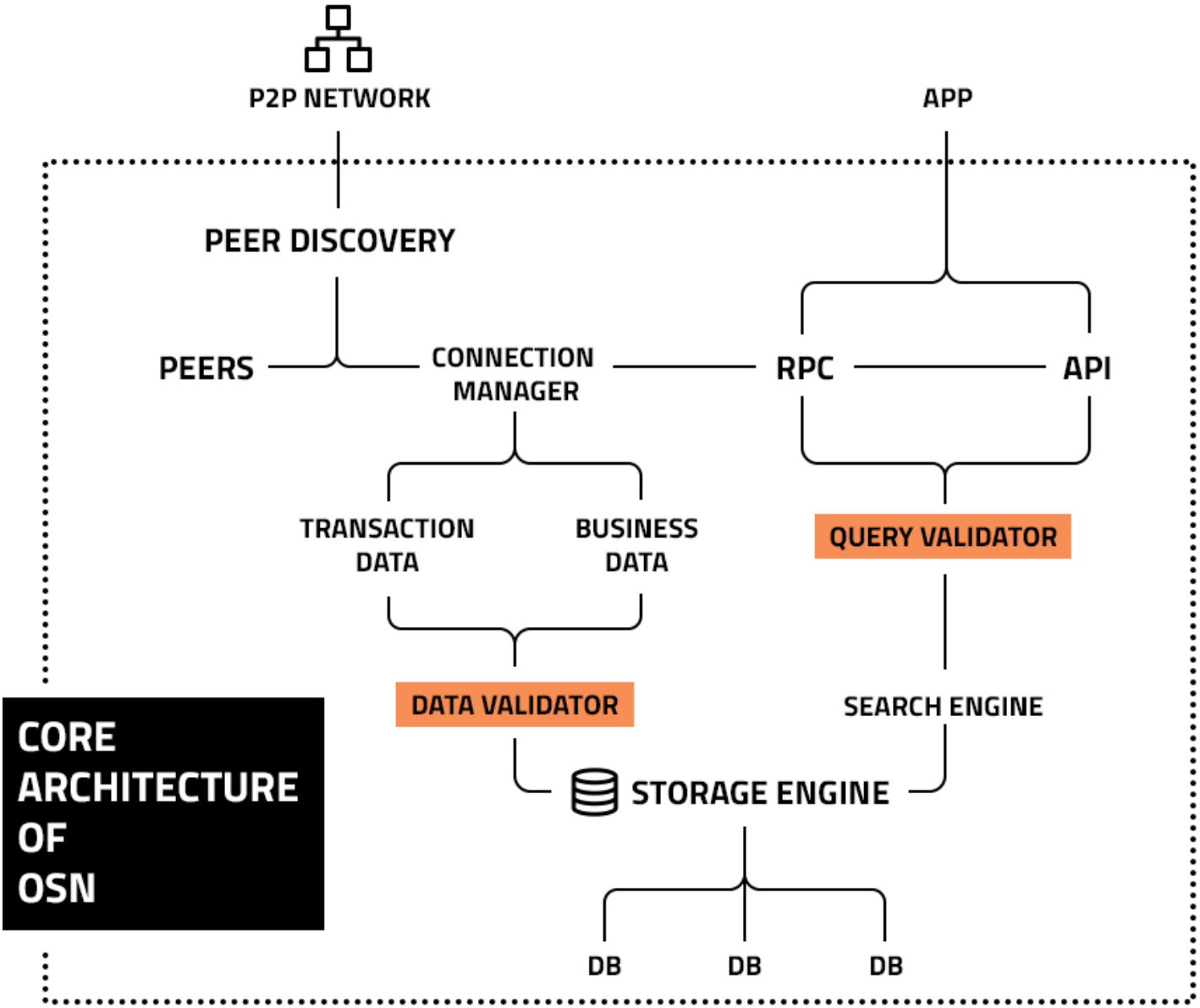


Diagram 19. Core Architecture of OSN

2.4.3 The Incentive Mechanism of the OSN

The incentive mechanism of the Open Storage Network is developed by smart contracts from 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 OSN node's immediate income includes storage fees and PoS decision-making rewards. Other potential income could be the data source which is the basis of the search engine capabilities discussed above.

3. VALUE SYSTEM

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

The project has a fixed total of 76 million coins, of which 8 million are reserved for development and marketing. 24 million are to be distributed through an ICO and the remaining 44 million are to be produced by mining. Initially the mining mechanism is similar to that of Bitcoin's.

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