



THE UNIVERSAL BLOCKCHAIN CONNECTOR

Technology Whitepaper

Penta Network



V1.1.1 | 2018

Abstract

With the thriving arrival of blockchain technologies, there comes a diversified and intricate system of blockchain platforms. However, these platforms are not yet interconnected, and they lack interaction with off-chain scenarios, thus affecting effective interactions between the real world and the world of blockchain network. A goal the new generation of blockchain technology aims to achieve is how to build on the diversified blockchain ecosystem to smoothly connect the distributed and decentralized world of blockchain platforms to the existing centralized world – thereby bridging the gap between blockchain platforms.

This whitepaper elaborates on the core architecture of the Penta Network, on how the five dimensions, i.e. Entity, Credibility, Value, Transferability and Economy, are connected, and how the Penta Network would serve as a platform to help connect the world of blockchain and shape a more convenient future.

Table of Contents

Abstract.....	1
1. Penta Overview.....	4
2. Connection of the Five Dimensions.....	5
2.1. Entity.....	5
2.2. Credibility.....	6
2.3. Value.....	7
2.4. Transferability.....	7
2.5. Economy.....	8
3. Penta Technologies.....	9
3.1. Penta Network -- Technical Structure.....	11
3.2. Penta Network -- Ledger System.....	13
3.3. Penta Blockchain.....	14
3.3.1. Consensus Algorithm.....	14
3.3.2. Governance Structure.....	18
3.3.3. Incentive Mechanism.....	20
3.3.4. Sharding.....	20
3.4. Penta DLOS.....	21
3.4.1. Distributed Computational Framework.....	22
3.4.2. Storage.....	22
3.4.3. Network.....	23
3.4.4. DLOS UI.....	23
3.4.5. MPT Tree.....	23
3.4.6. Enterprise Application Components.....	24
3.5. DApp Platform.....	24
3.5.1 DApp Operating Environment.....	26
3.5.2. DApp Database.....	27
3.5.3. DApp File System.....	28
3.5.4. DAppStore.....	29
3.5.5. DApp IDE.....	30
3.5.6. DApp SDK.....	30

3.6. Interoperability Layer.....	31
3.6.1 Soft eXchange Adaptor.....	33
3.6.2 Distributed Private Communication Protocol.....	34
3.7. Technical Roadmap.....	35
3.8. Security Strategy.....	36
4. Application of Penta Network.....	40
4.1. Social Applications.....	40
4.1.1 Healthcare.....	40
4.1.2 Application in the Energy Sector.....	43
4.1.3 Internet of Things (nergy	45
4.2. Financial Application.....	48
4.2.1 Credit Reference.....	50
4.2.2 Supply Chain Finance.....	53
4.2.3 Asset-Backed Securitization.....	55
5. Definitions.....	58
6. References.....	61

1. Penta Overview

Penta, (also referred to as “Penta Network” or “PNT”) is a new-generation of underlying blockchain network. Penta originates from Pentacle, a symbol that represents the birth of “Five Times Interlacing”, explores the cause and effect underlying everything, and goes after the development history and results of intertwined networks with a view to pursue a desirable blockchain world in the future.

By building five dimensions, i.e. Entity, Credibility, Value, Transferability and Economy, the Penta Network connects to a wide range of blockchain networks and systems, integrates with fragmented centralized systems, and ensures unimpeded interactions between such networks and systems with a view to eventually connect the worlds in and off blockchain in an effective and convenient manner. This would make blockchain a universally-benefiting technology, make it easier to create and apply blockchain technologies and ultimately provide a platform that connects the world of blockchain in the future.

Core members of the Penta Network come from leading technical and financial organizations and institutions across the world, including NASA, WikiLeaks, Google, Morgan Stanley, ABN AMRO, Deutsche Bank and beyond. They have an in-depth understanding and insight as to technical, social and economic developments and life circles. As blockchain is gradually becoming the key to building the order for the world in the future, Penta Network is exploring the future world of blockchain from the very beginning.

Penta Network. Shaping a connected future!

2. Connection of the Five Dimensions

The core of Penta is the connection among the five dimensions, (Entity, Credibility, Value, Transferability and Economy), and Penta would become a platform that helps connect the world of blockchain and shape a more convenient future.

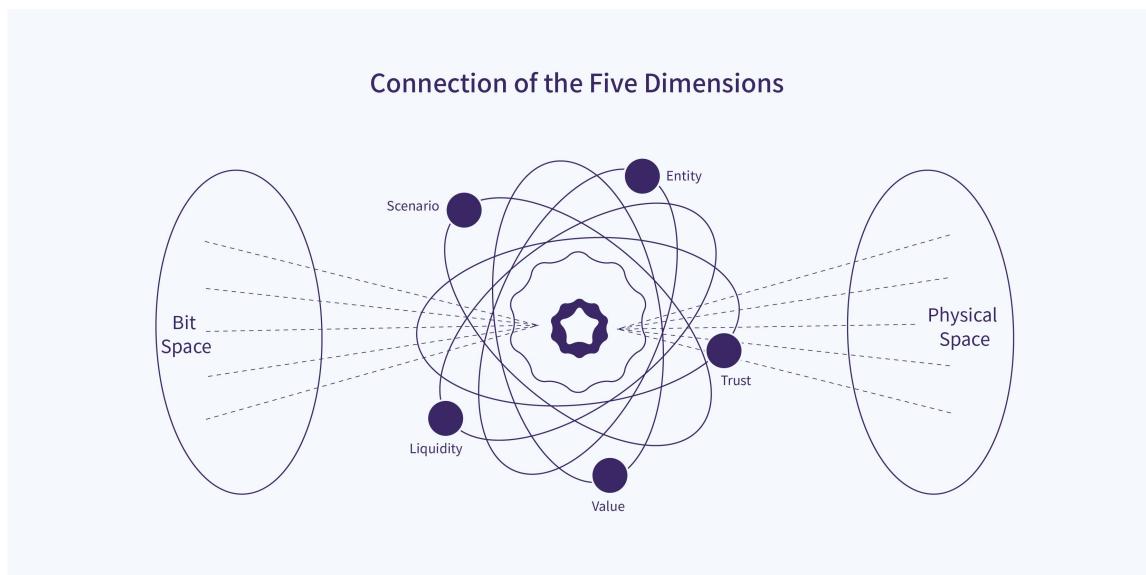


Figure 2 Connection of the Five Dimensions in the Penta Network

2.1. Entity

All participants, including any person, thing, organization, system, are assigned an identity in the Penta Network in a unified manner. The Penta Network manages interests and processes business based on the authority of an identity and is supportive of the management of multiple identities for the same entity.

Identities, including creation, use, verification and storage of identities, are managed in a decentralized manner to protect privacy and security of transactions.

- Creation: Each identity is generated by using PKI encryption mechanism, a form of asymmetric encryption, and public address information is

generated. The owner of an identity possesses the address and private key information. In addition, selection of a certificate issued by the digital certification center for identity purposes by a participating entity is partially supported.

- Use: The entity with an identity may use its private key information to trade all of its interests or digital assets in the Penta Network and may send requests to the Penta Network.
- Verification: The Penta Network examines all interests, verifies transactions and reaches a consensus across the network.
- Storage: Public information corresponding to an identity is saved in the distributed ledger in the Penta Network as public information.

In addition, identity supports Smart Contract extensions and thus a wider range of forms for identity management are made possible to meet diversified identity management requirements in varied business areas. For instance, asset transactions in the financial sector are subject to KYC demands of the jurisdiction governing a certain business, and in such cases extended Smart Contract may be used for setting and saving KYC contents.

2.2. Credibility

One of the more important reasons for the boom in blockchain development is that blockchain technology has implemented a decentralized trust mechanism that makes it a trusted machine. The Penta Network builds a distributed trust-generating mechanism through trusted entity, trusted network and trusted interaction.

- Trusted entity

Each participating entity has an identity in the Penta Network that is created by using the PKI mechanism and public information is recorded and saved in the distributed ledger. Some participating entity may manage their affairs by using a certified certificate.

- Trusted Network

Transactions are confirmed and recorded across the entire Penta Network by using a consensus algorithm. Once confirmed, a transaction cannot be revoked in any form.

- Trusted Interaction

Cross-blockchain transactions between other blockchain platforms or centralized systems are made possible by using key or certificate to give authorization. The Penta Network supports cross-blockchain transactions via Smart Contract and reaches a consensus within the Penta Network after consensus are reached by affiliated blockchain or system so as to make transactional control and ensure data integrity.

2.3. Value

The essence of the blockchain realizes the decentralization of digital asset value transfer. All assets recorded in the Penta Network exist in the form of a certain value, and participate in transactions between participating entities for a transfer of value. The Penta Network offers value management, including generation and exchange of values and cross-blockchain transactions.

In the Penta Network, value is generated when each consensus is reached and PNT is subsequently released to the nodes that have contributed to such consensus. In addition, the mapping of off-blockchain assets in the blockchain by a participating trusted entity is supported.

The resulting value assets are exchanged for value based on the Penta Network. The Penta Network adopts Soft eXchange Adaptor to support trade and exchanges of value with other blockchain and uses Smart Contract to lock transaction and manage affairs.

2.4. Transferability

Envisaging itself as a platform that helps connects the future blockchain world, the Penta Network not only supports new types of business scenario but also improve transferability into conventional business. In this way, the Penta Network connects all business and builds a foundation for trust and exchanges of value for business in the future to come.

For this purpose, the Penta Network offers DApp application development components and SDK, and streamlined the development of DApp. The combined toolkit does not require developers who are focused on business and scenarios familiar with the underlying technology of the blockchain. In addition, the Penta Network offers ChainStore to provide a platform for the use and promotion of DApp.

2.5. Economy

The Penta Network supports connection to each blockchain network, fragmented centralized system and participating entities and enables support for and connection to business scenario. As a hub for exchanges of values, the Penta Network combines cloud computing, big data, and artificial intelligence to provide perfect support for business scenario. See the network application chapter for more details on the application of the Penta Network in some business areas.

3. Penta Technologies

With properties such as decentralization, immutability and transfer of value, the blockchain technology has attracted attention from an increasing number of people in different industries. However, the blockchain technology exists some shortage, such as low performance, lack of capacity to support sophisticated business scenarios, arising centralization risks, growing block size, lack of interoperability, etc.

1. Low Performance

Existing blockchain platforms are plagued by low TPS and throughput. Although some of those do support smart contracts, only simple code can be run smoothly. When a DApp is written with complex code, the running of the DApp is becoming inefficient. Existing blockchain systems do not perform well enough to support running of any complicated DApp, thus failing to meet the real-world demands from users. A high performance blockchain platform is needed to support real-world business cases.

2. Lack of Capacity to Support Sophisticated Business Scenarios

Another challenge to commercial deployment of the blockchain technology is its lack of capacity to support sophisticated business scenarios. Business scenarios vary in their respective business logic and thus are in need of more flexible solutions. Existing blockchain networks are not flexible enough to fit various business scenarios.

3. Arising Centralization Risks

POW, the consensus firstly introduced with the bitcoin network, may lead to monopoly by chip makers while non-POW consensus such as DPOS, DBFT and others, focusing on efficiency would result in centralization by creating super-nodes. The core value that blockchain offers is not to seek efficiency at the expense of democracy. Instead, it is to build trust among nodes that

lack mutual trust and synergies by running neatly designed consensus mechanism.

4. Lack of Interoperability between Blockchain platforms

With rapid development of the blockchain technology comes various blockchain systems. However, these systems cannot talk to each other or truly go off-chain to serve business scenarios, thus failing to efficiently support the real economy. How to build on a wide variety of blockchain technologies to enable seamless transfer of values between blockchain platforms, or between blockchain platforms and existing centralized networks, or from on-chain to off-chain is a pain point that must be addressed by the new generation of blockchain network.

Penta Network aimed to serve real world businesses and to become a universal blockchain connector that provides a solid platform to support the wide deployment of distributed commercial applications in the future. Inspired by such vision, Penta Network will build Penta Blockchain, Penta DLOS, high performance DApp platform and Penta connector.

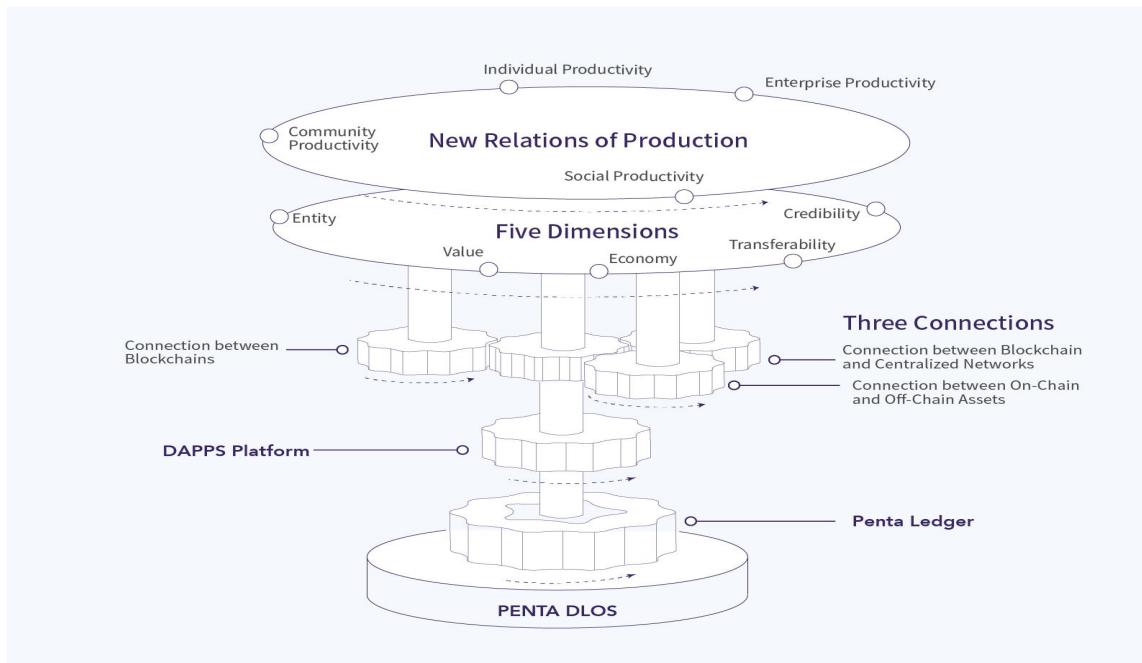


Figure 3 Penta Network's Technical Structure

Penta Blockchain: it uses Dynamic Stake Consensus ("DSC") that runs the Random Sorting Algorithm ("RSA") to ensure everyone are equal in the consensus process, thus forming a democratic consensus mechanism that is efficient, scalable, secure and consistent.

Penta DLOS: It provides fundamental technologies for building a blockchain platform, including but not limited to storage, networks, and enterprise application and UI components.

DApp platform: It aims to build a high performance DApp infrastructure that provides the environment, database, file system, application store, development SDK and other tools for the smooth running of a DApp for enhanced performance and streamlined development process.

Interoperability Layer: it aims to enable smooth transfer of value between blockchain platforms, or between a blockchain system to a centralized network, or from on-chain to off-chain.

Penta Network is a multi-chain network and Penta Blockchain is the main chain of the Penta Network that will be primarily maintained by the Penta Global Foundation and its developers' community. Penta DLOS will provide fundamental technology support, DApp platform will make it easier for businesses to solve real world problems, and the Interoperability Layer will ensure interoperability between blockchain platforms, or between blockchain platforms and centralized networks, or transfer of value from on-chain to off-chain, thus eventually fostering synergies among the five dimensions essential for wide deployment of blockchain platforms to resolve real world problems and reforming relations of production to make it better serve the needs of a new economy.

3.1. Penta Network -- Technical Structure

The framework of the Penta Network is composed by pluggable components. When users build a blockchain or sub-chain application, most of the components are designed in a manner that enables easy assembly like Lego bricks. Each component is pluggable. For instance, consensus components support POW, POS, dPOS, PBFT, etc. The encryption algorithm supports RSA, and SM2, among others, and is extensible by users.

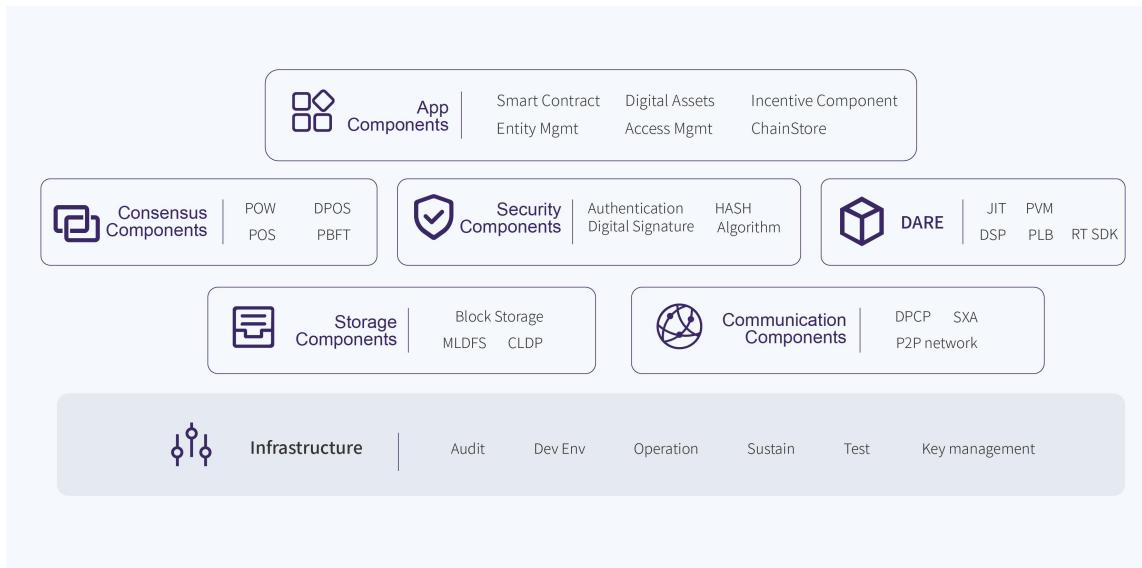


Figure 3.1 Penta Technical Framework Diagram

Storage components and communication components are the basic components of the blockchain platform; in terms of communication components, the Penta Network extend from P2P to distributed private communication network and Soft eXchange Adaptor; In terms of storage components, the Penta Network keeps commonplace block storage and extends to file storage and database storage, which could be further extended to other storage components to meet demanding volume and concurrency requirements by institutional users;

In terms of security components, unlike Ethereum's complete anonymity and Hyperledger's certificate authentication, identity authentication is optional in the Penta Network and users may need to display identity only when running a particular blockchain application;

In terms of application components, the Penta Network has provided the basic components for creating Smart Contract application and DApp such as Smart Contract, digital assets, incentive mechanisms, and member and authority management.

3.2. Penta Network -- Ledger System

Penta Network builds a multi-chain platform with the kernel of Penta Blockchain and forms a Penta Ledger system composed by Penta Blockchain, side-chain, other application chains, DApp State data, files and others so as to support applications and interoperability functions essentially for the Penta Network.

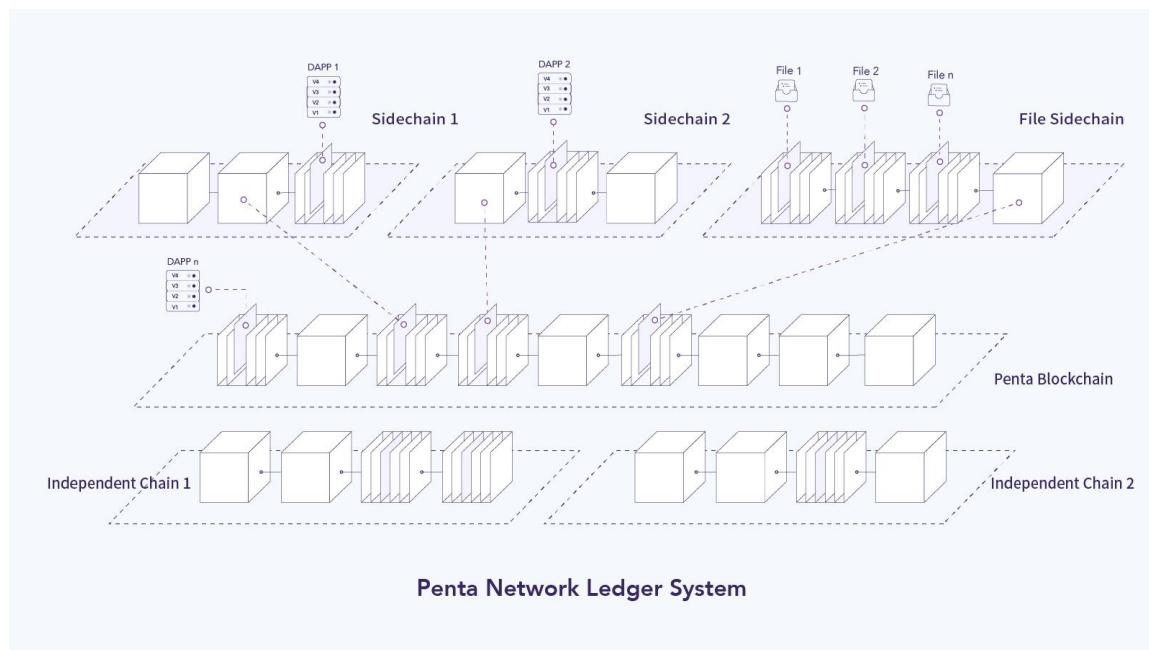


Figure 3.2 Penta Network Ledger System

Businesses may use the Penta blockchain, sidechain or independent chain to create DApp. Sidechain and independent chain could use pluggable consensus algorithms to provide customized support for various business scenarios. Based on the specific DApp that a user has downloaded, Penta Network will reduce burden on the user by syncing solely the data from the sidechain or independent chain on top of which the downloaded DApp runs.

3.3. Penta Blockchain

Penta Blockchain will apply a unique DSC consensus ingeniously developed by Penta. Reasonable governance structure, efficient incentives and underlying sharding technologies will be combined with DSC to significantly enhance the efficiency, security and consistency of the Penta platform. Application and interoperability functions essential will be available for the Penta Network so as to build a Penta Ledger system with the core of Penta Blockchain.

3.3.1. Consensus Algorithm

A consensus algorithm is the core of blockchain networks. Blockchain data is stored in each distributed network node and thus it is critical to have an algorithm to ensure these ledger data is consistent. Blockchain nowadays faces the trilemma of performance, security and equality. A blockchain network should develop efficient algorithm to achieve synergies in a multi-player game and create a secure, balanced, stable P2P network for value transfer.

To achieve this goal, Penta Blockchain designs a unique DSC consensus that balances democracy, efficiency and security by RSA algorithm. In addition, Penta Network will apply pluggable consensus components to support a wide range of consensus algorithms that any sidechain or independent chain in the Penta Network will adopt. In terms of design, the consensus algorithm used for bookkeeping on the Penta Blockchain is separated from that for DApp transactions and validation in a sidechain or independent chain, thereby decoupling the platform layer and the business layer, vastly enhancing operating efficiency of the Penta Network and enabling flexible solutions to real world business applications.

3.3.1.1. DSC by the Penta Blockchain

DSC is a consensus mechanism designed to avoid forks. Instead of trying to achieve extreme efficiency, DSC adopts RSA to ensure every node has an equal opportunity to participate in the consensus process and keeps taking efficiency into consideration.

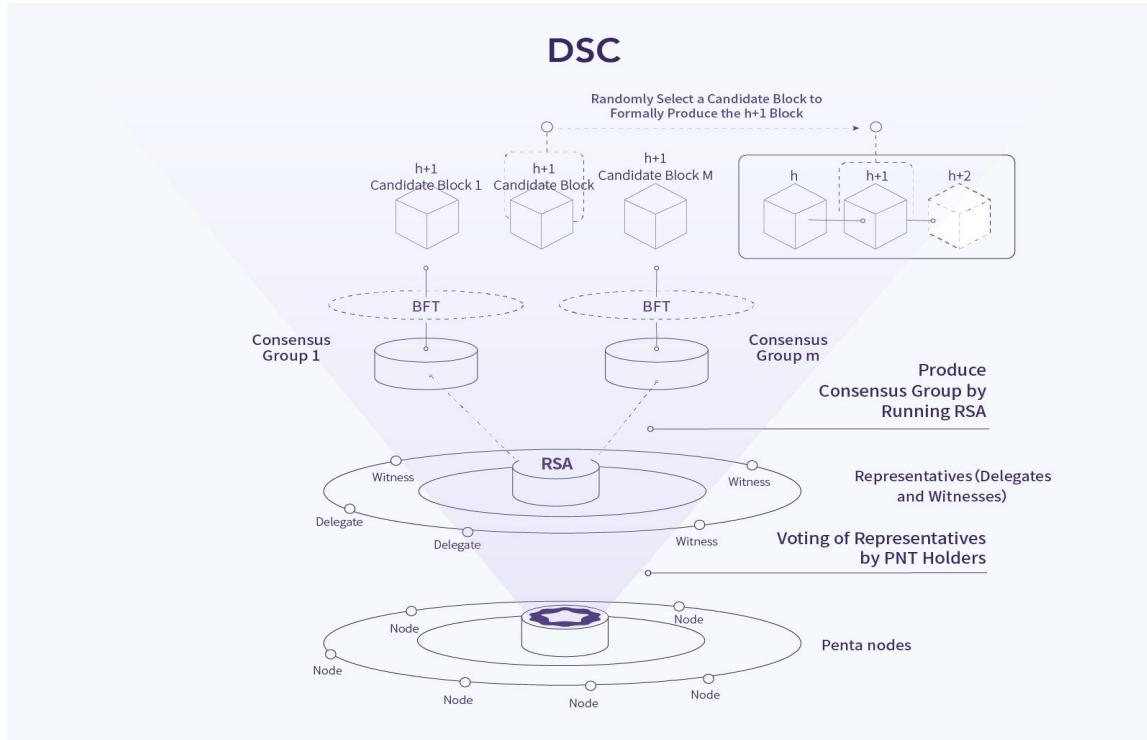


Figure 3.3.1.1 DSC Consensus

The following is a detailed description of the DSC process:

1. First, delegates and witnesses will be selected from all nodes in the network. Whether a node will become a delegate or witness depends on the number of PNT that they hold: delegate requires larger number of tokens while witness less.
2. Several consensus groups will be composed to select certain number of delegates and witnesses by running RSA. In each consensus group, the proportion of delegates against witness shall be no less than 1/3. Each group will run a BFT consensus to elect a proposer from participating

delegates. The proposer will propose a block while other delegates and witnesses will validate the block together. Upon approval of at least 2/3 nodes in a group, a candidate block will be produced. The number of consensus groups will be dynamically adjusted depending on condition of the entire network at that moment.

3. By selecting one of the candidate blocks via RSA, a block will be formally generated.

If a consensus cannot reach within a certain time frame, the RESET mechanism will be triggered and all the delegates will run BFT to produce a RESET block so that new members of consensus groups will be reselected to ensure normal operations of the entire network.

DSC adopts RSA to ensure that the consensus process is secure and fairness. A consensus can reach in a very short time frame with very little computational capacity. Because consensus groups are formed with Random Sorting Algorithm, unlike the algorithms relying on dozens of centralized bookkeeping nodes, DSC is more secure to resist attacks.

3.3.1.2. **DApp Consensus**

The DApp consensus will be determined by the issuer of a DApp by means of designating the consensus algorithm in the metadata descriptions. The consensus algorithm can be any consensus that the platform offers in default including DSC, POS, dPOS, PBFT, POA, Notary and so on. Also, it can be any consensus that an issuer specifically develops to satisfy its unique needs. Penta Network is responsible for coordinating the consensus process for a DApp. Penta Network will provide scheduling mechanisms to execute DApp transactions in parallel or serial, validate the authentication of consensus results of a DApp transaction and will then register such results in a block.

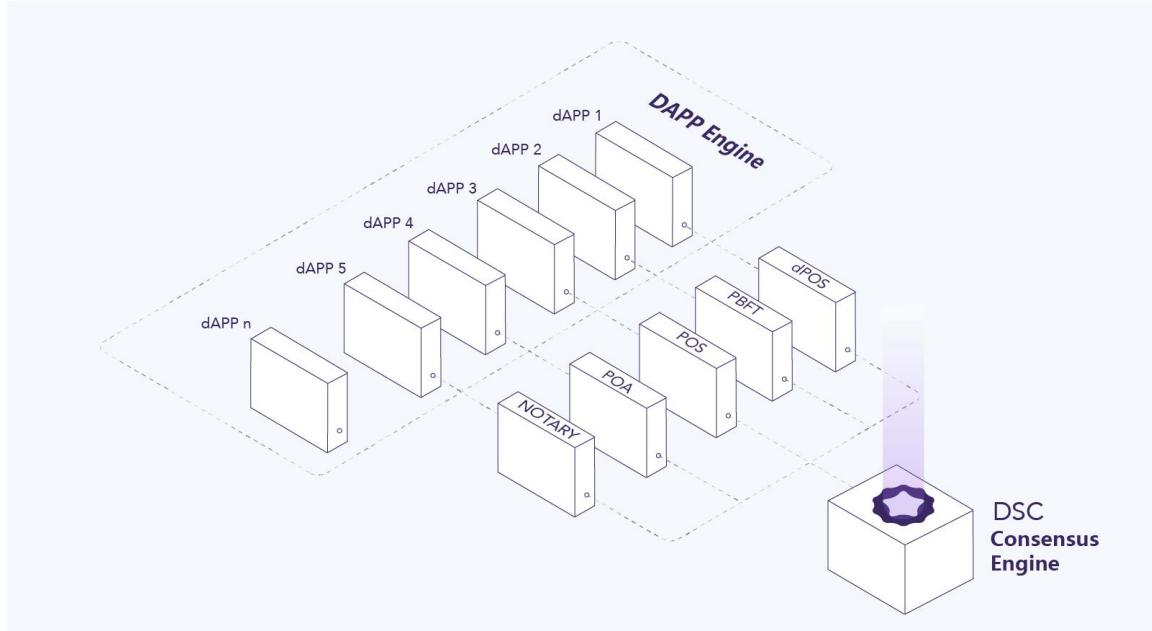


Figure 3.3.1.2 DApp and Consensus Engines

Penta Network innovatively adopts a consensus mechanism that allows co-existence of multiple consensus algorithms so that respective consensus may be independently used for execution and confirmation of smart contracts or block generation, thus reducing extra links during the block generation process so as to more reasonably use resources on and enhance the overall performance of the platform.

Penta Network is a multi-chain platform that provides pluggable components to support a wide range of consensus algorithms including DSC, POS, dPOS, PBFT, POA, Notary and so on.

- POS primarily means that the difficulty in a node's receipt of book-keeping rights is inversely proportional to the interests held by the node.
- dPOS node elects several agents who implement validation and book-keeping.
- PBFT is a consensus mechanism that uses a permissive and majority vote to elect leaders for book-recording purpose.
- POA allows users to create new nodes on a blockchain and to ensure that a blockchain is secure with a set of authorizations.

- Notary adopts a model that allows witnesses with multi-signature.

3.3.2. Governance Structure

Penta Blockchain defines following roles:

Delegate: a PNT holding node may voluntarily apply to be a delegate and other nodes will vote on whether to accept such nodes as a delegate. To become a delegate, a node is required to receive a certain number of votes and to pledge a designated amount of PNT. Each delegate has an equal opportunity to participate in the bookkeeping.

Witness: a PNT holding node may voluntarily apply to be a witness and other nodes will vote on whether to accept such nodes as a witness. To become a witness, a node is required to receive a smaller amount of votes and pledge a smaller amount of PNT. There will be a large number of witnesses from diversified origins.

Proposer: As a role of the BFT process, a proposer will be elected from delegates to be responsible for producing a proposed block.

The number of delegates will dynamically increase. The initial number of delegates and the minimum number of PNT required to be pledged will depend on the number of nodes participating in the process and the ranking by the possession of PNT . They will be dynamically adjusted during subsequent operations of the Penta Blockchain based on the total numbers of delegates and witnesses. There will be no cap on the number of witnesses who are required to pledge a small amount of PNT. The following are more details on how to participate in and exit from the bookkeeping process:

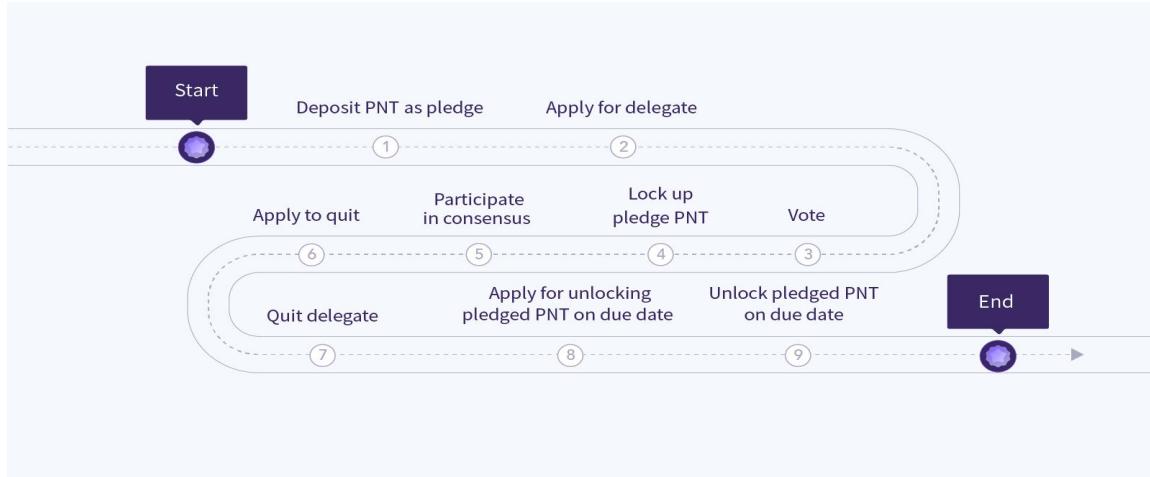


Figure 3.3.2 Participation and Quit Process for Bookkeeping

A consensus group will be formed by randomly selecting delegates and witnesses with RSA running. Each group will have n members including delegates and witnesses. The n as referred to in the foregoing is a dynamical value. In each group, the number of delegates is (n_1) : $n/3 < n_1 < 2n/3$ while the number of witnesses is $n_2 = n - n_1$.

Nodes participating in consensus are required to pledge a certain amount of PNT and in the event of any malicious attempt to sabotage the network, pledged PNT will be forfeited as penalty. If a proposer puts forwards two or more blocks during the BFT process, other nodes may blow the whistle and the proposer will be subject to penalties times of the benefits that the proposer will receive.

If a node exits from the consensus process, the pledged PNT will be unlocked in seven days.

Penta Blockchain will adopt corresponding mechanism for protocol upgrade, including adjustment of parameters in relation to the cap on delegates and witnesses, cap on number of nodes in a consensus group, cap on transaction fees, and the minimum amount of PNT to be pledged and otherwise. All delegates are required to vote on a protocol upgrade and the result will be

determined by running BFT. Only upon approval of at least $(2n+1)/3$ delegates will a new protocol be adopted at certain block height. In this way, the risks of fork are eliminated.

3.3.3. Incentive Mechanism

Upon each reach of the consensus and production of the block, the bookkeeping nodes (including every member in a consensus group that produces a candidate block) will receive certain amount of PNT as incentives. In this way, more nodes will participate in the bookkeeping process to maintain normal operation of the entire Penta Blockchain. PNT incentives come from two sources: first, Penta reserves 50% of the total tokens as bookkeeping incentives; second, a transaction fee will be charged for each transaction.

3.3.4. Sharding

In a blockchain network, transaction data is stored in a serial chain structure and each block will be generated within a fixed time frame. Given the time required to produce a block and the speed of broadcast in a P2P network, the block size is usually limited which restricts the throughput of the entire network. With the surge of transactions in a network, lack of scalability will become a bottleneck that prevents the blockchain from large-scale applications. Consequently, how to enhance the capacity to process transaction data in parallel has become an issue that must be considered by each blockchain network. As of now, some developers have made helpful attempts and discussions on how to resolve scalability issues, namely by using state channel, sidechain and sharding, among others.

Sharding usually has two solutions: one aims to enhance the capacity to process transactions in parallel while the other one focuses on the enhancement of storage capacities. In addition to an efficient consensus algorithm, Penta Network will apply parallel schemes to enhance the capacity of transaction processing that will prevent any scalability issue due to the volume of transactions increasing in the future. Penta Network will use transaction sharding

and adopt PSG (Penta Sharding Graph) with the Penta Chain as the core of ledger architecture to enhance the scalability and security of transaction. Consistency of cross-shard transactions will be guaranteed by the Sync Point technology. The capacity of transactions processing will be enhanced in parallel, i.e. dynamically classify different addresses or DApp transactions to enable parallel processing while automatically coordinating transactions processed in parallel or serial.

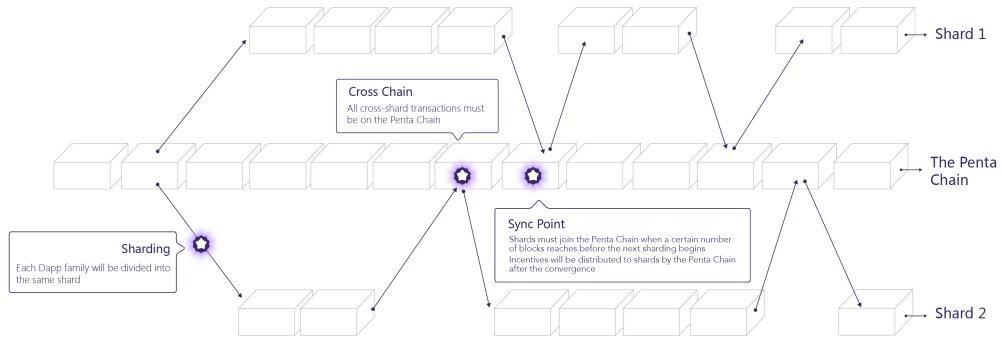


Figure 3.3.4 Penta Chain PSG Diagram

3.4. Penta DLOS

DLOS is the infrastructure of Penta Network that provides a scalable, micro-service, distributed framework. Nodes connect with Penta Network by using DLOS. Penta Blockchain is the core of Penta Network, which is a multi-chain network with other sidechains and independent chains. To support various network structures, ledgers and algorithms, DLOS separates computation, storage, network, consensus and other resources and provides abstract interface in each layer. It connects each service components through service administrator and event components. Base structure is decoupled from specific applications with DLOS implementation. DApp or other application chains only need to focus on their unique needs without paying too much attention to underlying technologies irrelevant to their specific business case.

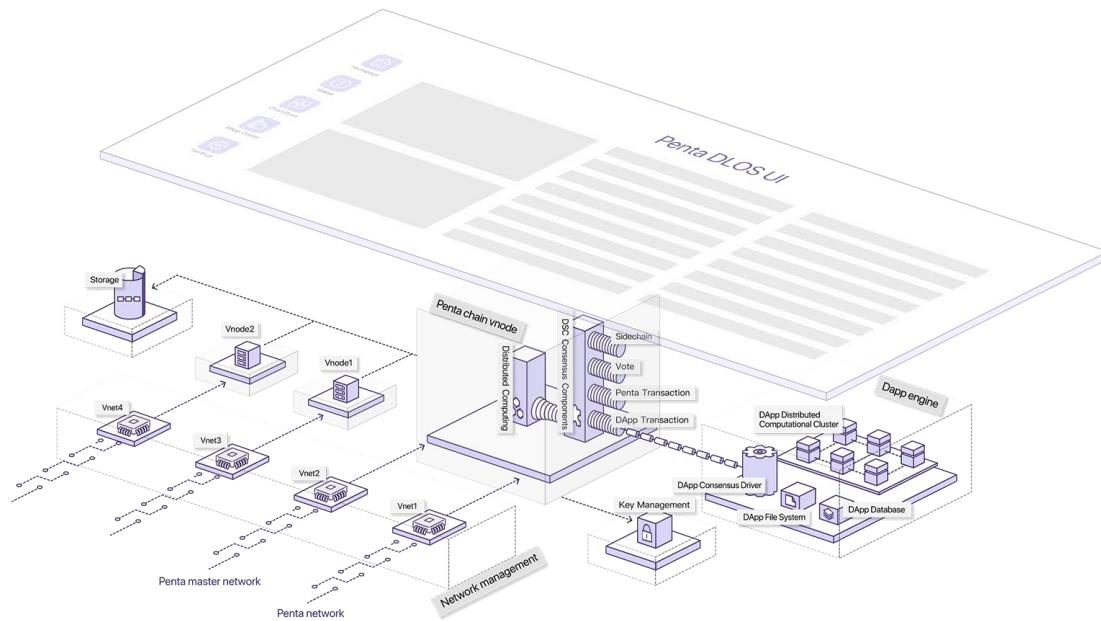


Figure 3.4 DLOS Logic and Structures

3.4.1. Distributed Computational Framework

Distributed computational framework is the core of DLOS. It handles all service and event administration for all nodes. It enables synergies among DLOS components, making them work as a whole.

For enterprise applications, DLOS components can be run in a cluster environment with various hosts, which will enhance the scalability of a single node and provide high availability environment for enterprises.

3.4.2. Storage

Multiple forms of ledgers exist in Penta Network such as sidechains, DAG, and so on to support various applications in the network. DLOS will abstract the storage layer and realize the common ledger storage components which can be easily used by block structures setting. Only in some special cases, new ledger storage components need to be added along with a ledger structure expansion.

Given different circumstances of fork-vulnerable chain and fork-invulnerable chain, various storage engines are achieved to support varied data structure of DApp State data. For example, MPT data storage engine is designed for fork-vulnerable chains while a specific data storage engine is designed for fork-invulnerable chains.

3.4.3. Network

Penta Network is a multichain platform on which each node is able to connect to several chains concurrently. The network administrator of DLOS will manage several virtual P2P networks at the network layer. On a specific chain, each virtual network will be allocated to a specific chain and assigned tasks of sending or receiving messages. Due to varied requirements on P2P network, the first step of DLOS is to enable Kademlia P2P network with new P2P technical components increasingly added. App developers can build their own new P2P technical components to the network as well.

3.4.4. DLOS UI

Penta DLOS UI is the UI framework running on the view layer. It provides friendly and consistent user experiences for users, which also offers developers a unified and easy-to-use DApp UI development framework and technical components. The MVVM model based DApp UI encapsulates standardized UI components and APIs used for DLOS service layer interaction, which controls DApp UI access service layer, especially API access related to accounts. The coordination with the service layer enhances the security of client nodes.

3.4.5. MPT Tree

Merkle Patricia Tree (MPT) is an improvement that combines technical strengths of both the Merkle tree and Trie. It maps key-value pairs and provides a

cryptographic, self-validating, tamper-proof data structure with certainty, efficiency and security.

1. Certainty: When searching for a data in the tree, the same key will map to the same result with the same root hash;
2. Efficiency: When a data is modified, a new root will be computed immediately without no need to re-compute the entire tree, thus making it highly efficient for data insertion, search and deletion;
3. Security: Limited depth of the tree will resist any DOS attack initiated by some attacker who maliciously creates an overwhelming amount of transactions with an attempt which can manipulate the depth of a tree.

MPT is widely used for transaction validation, data storage and other process in the Penta Network.

3.4.6. Enterprise Application Components

A participant in the Penta Network can be an individual or enterprise. However, needs of individuals and enterprises are quite different. Individuals focus on more features such as user-friendly, lightweight and so on while enterprises have strict requirements on each system indicators. This is especially stringent with financial institutions. Enterprise version of DLOS will comply with COBIT (Control Objectives for Information and related Technology) standards, making it easier for enterprises to meet IT auditing requirements.

DLOS will add security center, key administrator, member administrator, authorization administrator, operation and maintenance, auditing and other components to make it easier for enterprises to develop blockchain applications thereon.

3.5. DApp Platform

DApp (blockchain application) is the key part of application services in the Penta Network and technically includes view layer, business logic layer, and data layer.

Data layer is the status data generated by DApp stored in the Penta ledger, and the data is stored in each Penta node in file or database format. Penta client normally only syncs block data, which only contains DApp version number and fingerprint of status data other than DApp status data itself. Only when a user has downloaded DApp from ChainStore in Penta client, the status data will be synchronized to the local from other nodes.

The DApp business logic layer could be a simple Smart Contract or a complex system. The interfaces on business function layer have three classes: Control (initialization, metadata, etc.), Query (query only and will not modify data in the data layer), and Change (change in business logic may lead to data update in data layer and will take effect only when bookkeeping nodes reach consensus.)

The DApp view layer runs on the Penta client and interacts with end users. The view layer development must comply with Penta view layer development specifications and framework requirements to ensure well operations in the Penta client. The DApp view layer framework uses the MVVM pattern to effectively separate UI layout and front-end logic to improve the code maintainability of the view layer. DApp can provide services as interfaces only without view layer.

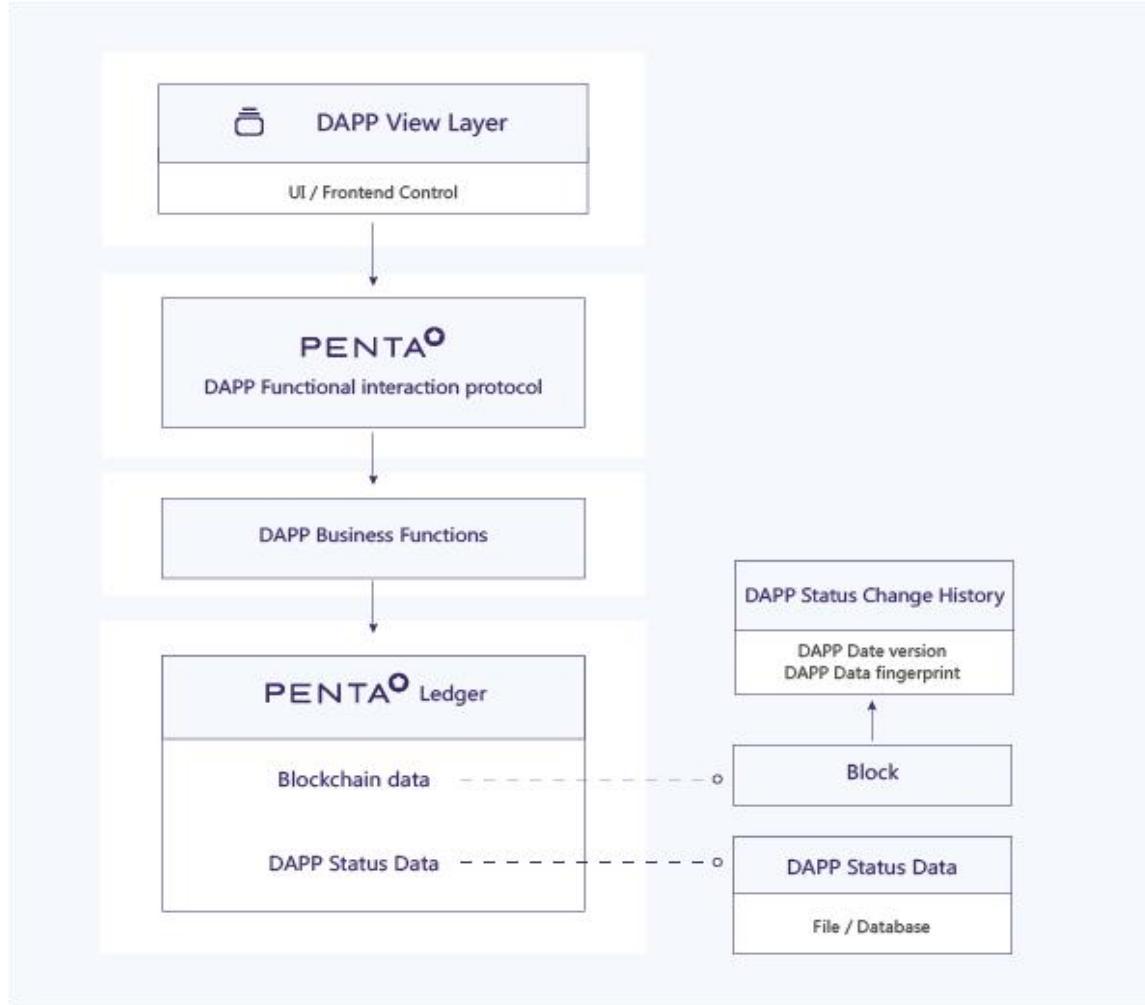


Figure 3.5 DApp Framework

3.5.1 DApp Operating Environment

PDW provides complete, independent virtual smart operating space for smart contracts and other blockchain applications. PDW will provide resources necessary for running a blockchain application including independent computational resources, database, file storage and others. Blockchain application's authorization to access resources is limited to PDW and no application is allowed to access data or file of another blockchain application across the boundary of PDW.

Computational resources, database and file storage in the PDW are respectively allocated by DARE, CLDP and MLDFS. Blockchain applications may use

dedicated APIs provided by MLDFS and CLDP to access resources. Fingerprints of state will be generated at the end of an operation and will be recorded in a block.

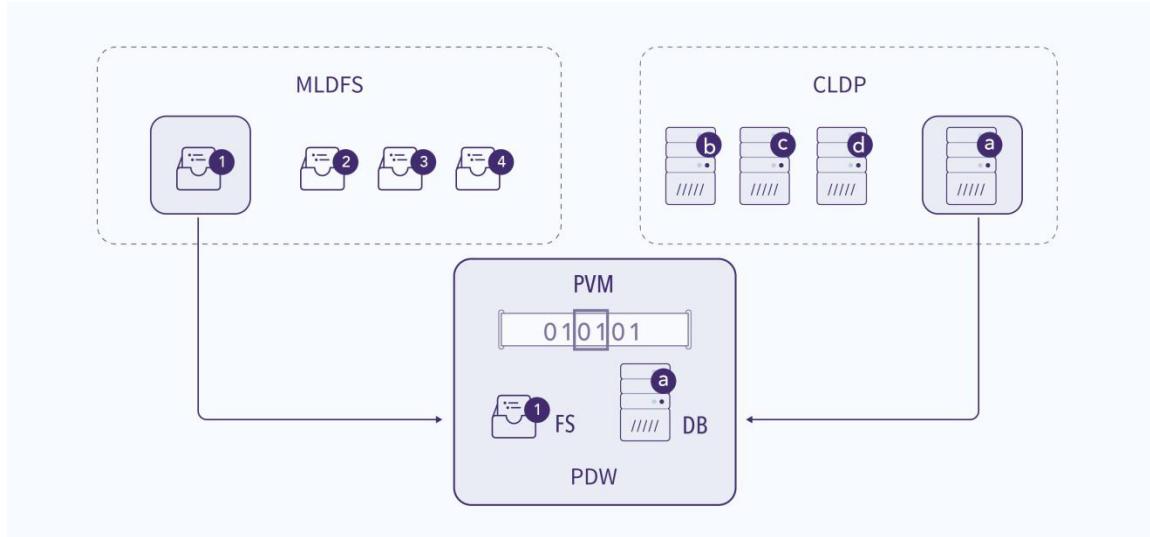


Figure 3.5.1 PDW Diagram

3.5.2. DApp Database

CLDP is a distributed database storage engine specially developed for Penta Network. It is a set-oriented storage engine. It is something between relational and non-relational databases but is equipped with strengths of both. It provides SQL engine to simplify complicated blockchain application development. It also provides virtualization mechanism to meet the need of a separation between smart contract data and transaction logs for efficient sync and duplicate of blockchain application data. With features of high performance, easy deployment, easily applicable and convenient data storage, it will not only meet the needs of individuals on lightweight applications, but also satisfy strict requirements of performance for enterprises.

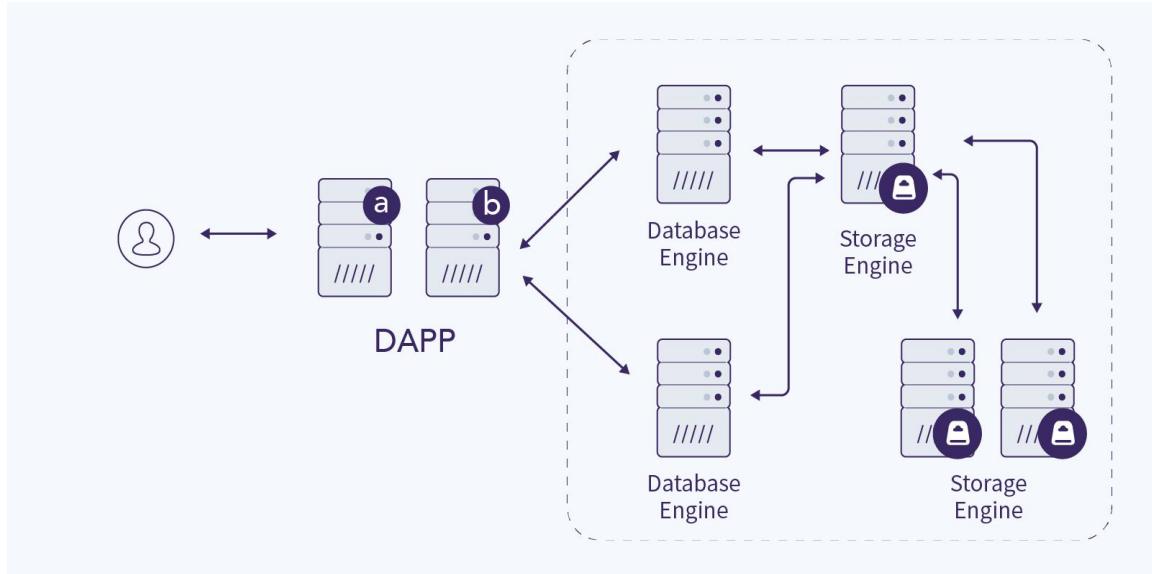


Figure 3.5.2 CLDP Protocol Diagram

3.5.3. DApp File System

MLDFS (Multi-Layer Distributed File System) is a distributed file system storage protocol that consists of namespaces and data spaces. Namespaces manage file names, data spaces store specific data, and data files are separated into a number of blocks to be stored in the data spaces. Data blocks can be stored by MLDFS or a traditional file system by means of distributed storage.

Version management is adopted for file storage in MLDFS. For each consensus transaction commit of a block chain application, MLDFS creates a unique version number. The version number uses a hashed value of this version to verify the version data. Modified data will be recorded by each version and the version number will be registered in the block, which will be used by other nodes for file synchronization of DApp status data and the version number is used to verify the integrity of the synchronized data. Other nodes may synchronize data incrementally (synchronize only the data differs from previous version) to cost a lower traffic and time expense effectively and improve the performance of the entire blockchain network.

MLDFS also uses virtualization technology. An independent file storage environment will be allocated by DARE when each blockchain application runs. Smart Contract or blockchain application manages all file modification records. The version change of stored files is dedicated to each blockchain application.

MLDFS supports distributed transaction management. All nodes participating in the consensus process run the blockchain application, validate the results, and sign. Files are modified when running a blockchain application, but relevant data will not be written in the file system until a consensus transaction commits. Then a new version of file will be generated. In this way, each version will eventually be arranged in a multi-layer form.

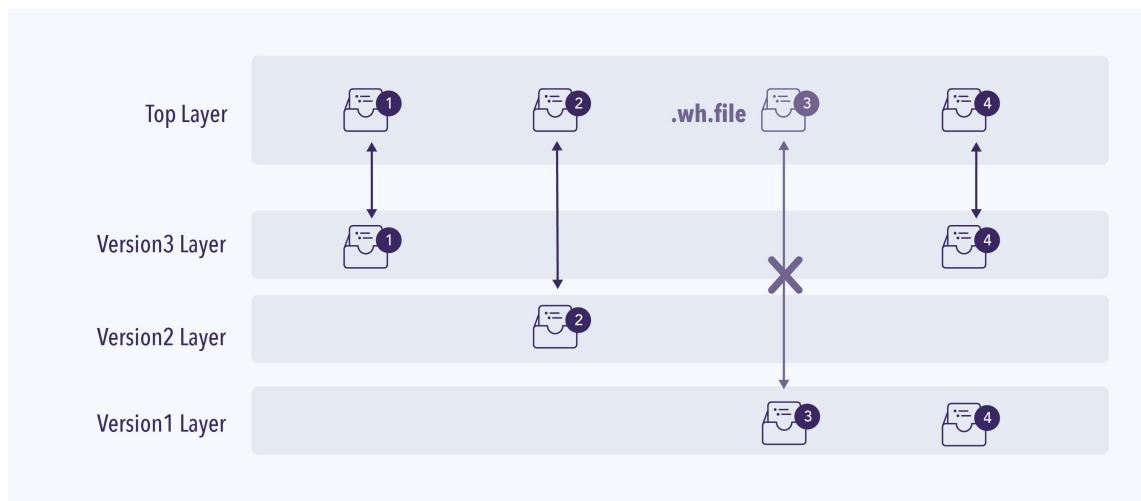


Figure 3.5.3 Multi-Layer Distributed File System

3.5.4. DAppStore

ChainStore is the information center in Penta Network where chain and chain services (smart contracts and other DApps) are registered. Data on ChainStore is partly stored in the distributed ledger of Penta Blockchain. Logic of ChainStore's view layer is provided by Penta Network client. Users may download DApp from ChainStore via Penta Network client. After the download of the ChainStore, the client will automatically download view layer programs based

on the DApp information registered in the ChainStore and will automatically sync state data of DApp to the local.

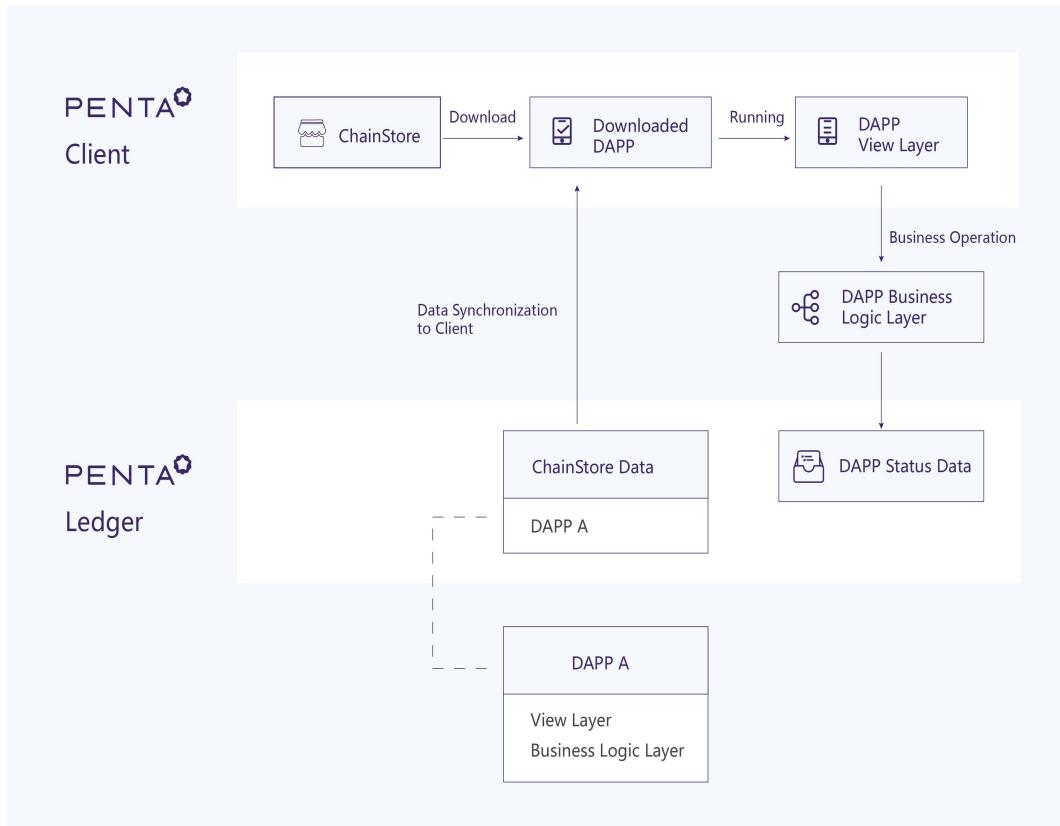


Figure 3.5.4 ChainStore Diagram

3.5.5. DApp IDE

Debugging and testing of DApp is much more complicated than those of traditional system. Penta Network will provide developers with development environment that integrates coding, analysis, compilation, testing, release and others tools to facilitate development. Also, Penta Network will provide a wide variety of tools and functions to help developers organize resources and reduce errors.

3.5.6. DApp SDK

Penta's DApp running environment provides various SDK according to the different layers, making it easier for developers to develop real-life applications.

SDK provides with APIs applied to storage, signature verification, account, identity, connector, digital assets and so on.

3.6. Interoperability Layer

Penta team believes that distributed ledger technology including blockchain cannot cover every real world scenario. The blockchain does its good job in scenarios lack of mutual trusts. In some other cases, people prefer to trust credible central systems, which have more authoritativeness. Therefore, Penta envisages a future where centralized networks, consortium chains and public chains work closely together to provide services to users, and thus aims to build an interoperability infrastructure based on the efficient, secure and consistent Penta Blockchain. The connector is dedicated to the transfer of value between blockchains, or between blockchains and centralized networks, or from on-chain to off-chain. It is structured in four layers: communication link layer, credibility layer, value layer and application layer.

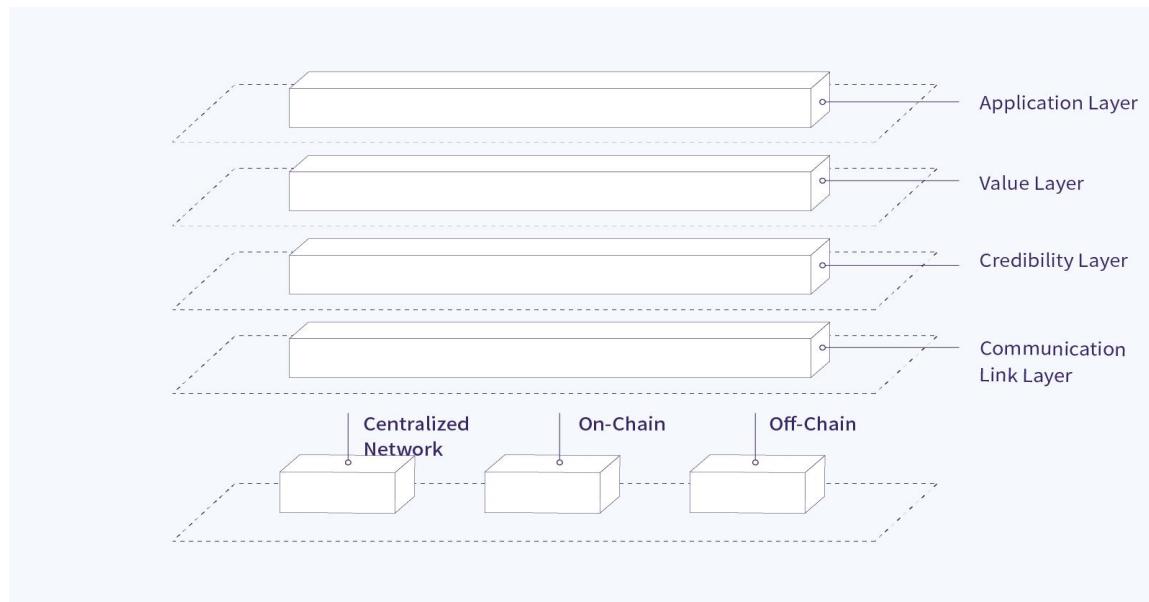


Figure 3.6-1 Structure of the Interoperability Layer

- Communication link layer realizes information exchanges with other blockchain or centralized networks by solving issues of communication transmission and data format.

- Credibility layer provides a mechanism to help build trust among entities and eliminates the needs for a middleman when transferring values among different platforms including measures of technology and entity credibility. Measures of technology will be applied such as HTLC, multiple signatures, distributed key control, smart contract and sidechain. Measures of entity credibility will be applied such as identity validation, information validation, guarantees, insurances, timestamps, comments by the public and credit ratings.
- Value layer is primarily responsible for value-laden during the transfer of value on and off a chain, potentially including escrow of a single entity or a consortium, contract account, bookkeeper, notary public and so on.
- Application layer will realize transferring values and serving business by selection of proper protocol combinations according to specific scenarios.

Interoperability protocols will support Soft eXchange Adaptor so as to help distributed applications control their transactions. DApp SDK, the primary running environment of Penta Network, provides standard API calls for other chains and existing major blockchains including BTC, ETH, Ripple, Stellar, NEO, Dash, Hyperledger and so on. By calling such APIs, developers will be able to interact with other blockchains and traditional centralized systems. Functional component layer provides a variety of functions, including unified identity validation, chain service registration, chain service discovery and chain service quality evaluation to ensure synergies services between different chains or between a blockchain and a centralized systems. Penta Network will provide an integrated client that is compatible with existing major clients of BTC, ETH, Ripple, Stellar, NEO, Dash, Hyperledger and more, so as to provide consistent user experience. Identical APIs will be introduced into the integrated client so that other blockchains may easily interact with any blockchain on or off Penta Network by these API calls.

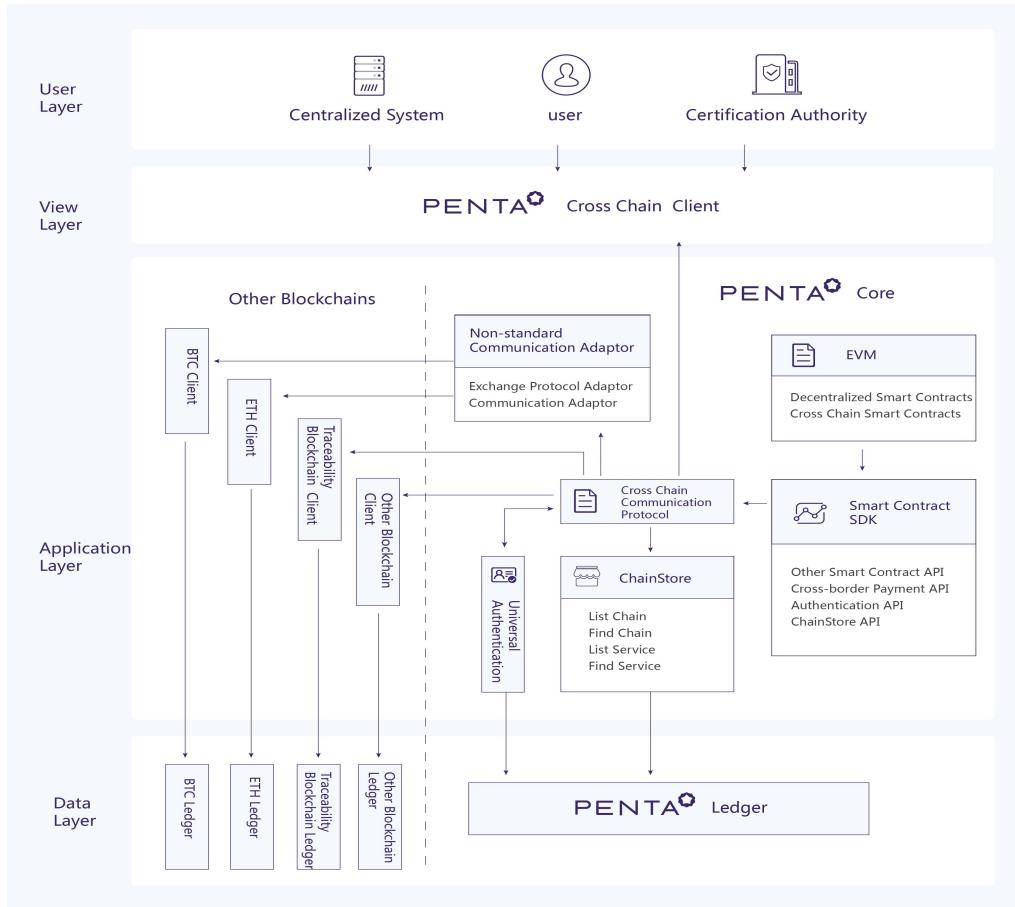


Figure 3.6-2 Cross-Blockchain Communication Structure

3.6.1 Soft eXchange Adaptor

Blockchain technology evolves very fast as a decentralized system. But the application of a blockchain system requires a specific business scenario. Traditional centralized system will exist for a long time. Application of a blockchain system to a wider range of areas inevitably requires interaction with existing centralized systems. The Penta Network introduces Soft eXchange Adaptor (SXA) to communicate with existing centralized systems swiftly, stably and efficiently. SXA is divided into three layers: communication layer, protocol layer, and business layer, all of which act together to ensure quick adaption to traditional centralized systems.

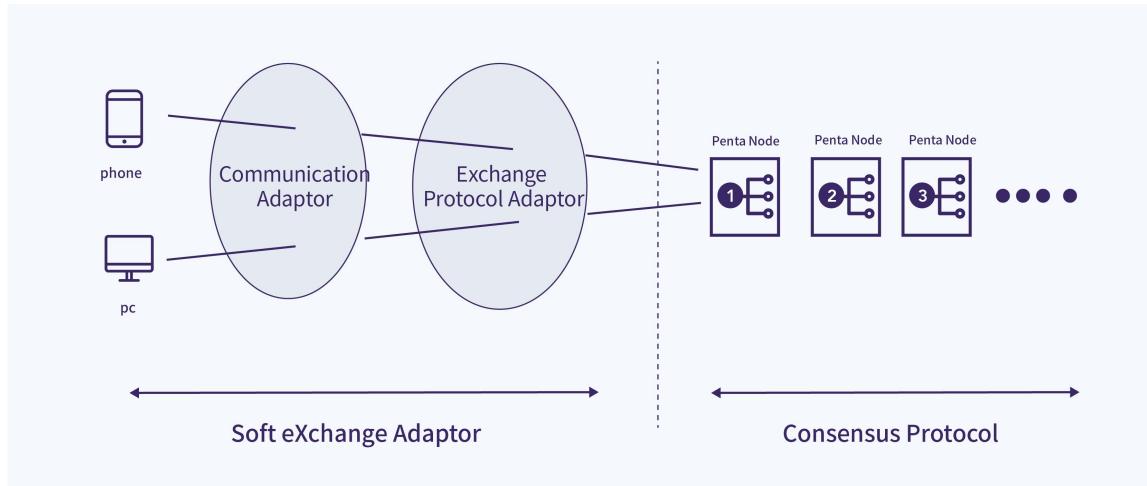


Figure 3.6.1 Soft eXchange Adaptor

3.6.2 Distributed Private Communication Protocol

A blockchain by default considers the public P2P network as a communication system that exposes information and broadcasts data. All participants will be able to look up the information that is published in a blockchain network. Nevertheless, in real practices, the transaction owners may be reluctant to disclose certain data to irrelevant parties and here comes the Penta communication network. The Penta communication network builds a special communication network (DPCP) through the existing network nodes. If two participating nodes need to transmit private information, the network will set up a special communication channel in the network. All data in the channel may be accessed only by these two involved parties, and no third party will be able to pry into. The Penta communication network provides routing, channel establishment, traffic control, exchanges of certificate, key and encrypted data, channel destruction and other mechanisms.



Figure 3.6.2 Distributed Private Communication Protocol

3.7. Technical Roadmap

Penta Network aims to become a universal blockchain connector. To achieve this goal, Penta Network will first make the Penta Blockchain available in the distributed credibility layer. Then Penta Network will gradually build the DLOS technical infrastructure, a DApp platform to support decentralized applications, and an interoperability layer. Penta Network will continuously improve technologies for each layer to enhance the performance of Penta Network as a whole.

Penta's developer community will first build the Penta Blockchain, including DSC algorithm, voting center, Penta PC wallet and blockchain explorer, and will release the first version to support PNT transactions.

Core parts for the first version of DLOS will be reorganized based on technical components of the Penta Blockchain. Users will find it easier to build their own chain based on DLOS. In this way, nodes in the Penta Network will be able to connect more chains.

DApp platform is a critical part that enables the Penta Network to provide distributed solutions applied to complex business scenarios. The platform will gradually realize series of technologies such as DApp running environment, DApp dedicated database, DApp file system, DApp UI framework, and support of DApp development and maintenance.

Interoperability layer is a key role in the Penta Network that enables transfer of values between blockchains, or between a blockchain and a centralized network, or from on-chain to off-chain. Core components of the interoperability layer include standards, protocols, norms and technical components, which will need to be advanced by the industry together. Fortunately, Penta community will consistently work on the enhancement and application of interoperability technologies so as to realize the vision of creating a universal blockchain connector.

3.8. Security Strategy

The Penta Network uses multiple security strategies to protect the safe operation of the platform, and provides a variety of underlying encryption algorithms such as ECC and otherwise, and introduces encryption algorithms (such as Lattice-based cryptography) that is able to resist the brute force of quantum computing as appropriate depending on the progress of projects.

The ECC encryption algorithm used in the Penta is a mainstream asymmetric encryption algorithm. Public key algorithms are always based on unsolved math problems.. For example, RSA is based on the following: Given two prime numbers p, q is easy to multiply to obtain n, whereas it is relatively difficult to factorize n. The ECC algorithm based on the following:

Consider the equation: $K = kG$ [where K, G are points on $E_p(a, b)$ and k is an integer less than n (n is the factorial of G)]; It is not hard to see that given k and

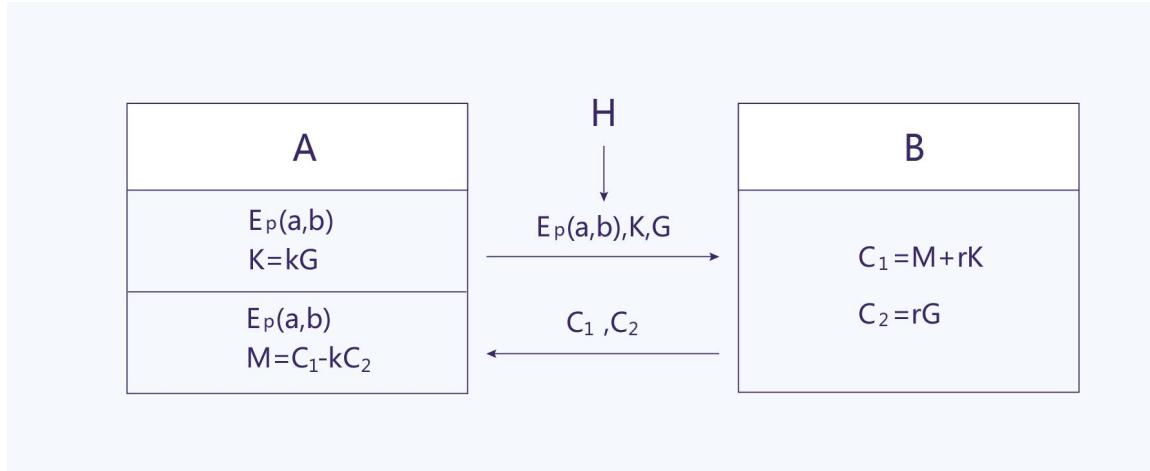
G , it is easy to calculate K ; but given K and G , it is relatively difficult to find k . This is the puzzle underpinning the elliptic curve encryption algorithms. We call the point G as the base point, k ($k < n$, n is the factorial of G) is called the private key, K is called the public key (public key).

Now we describe a process of using elliptic curve for encrypted communication:

1. A selects an elliptic curve $E_p(a, b)$ and takes a point on the elliptic curve as the base point G .
2. A chooses a private key k , and generates a public key $K = kG$.
3. A passes $E_p(a, b)$ and point K, G to user B.
4. After B receives the message, it encodes the plaintext to be transmitted to $E_p(a, b)$ at point M (a wide variety of coding methods may be used for this purpose and are not discussed in detail here) and generates a random integer r ($r < n$).
 5. B Calculation point $C_1 = M + rK; C_2 = rG$.
 6. B passes C_1, C_2 to user A
 7. A receives the information, calculates $C_1 - kC_2$, and the result is point M .

The plaintext can be obtained by decoding the point M since $C_1 - kC_2 = M + rK - k(rG) = M + rK - r(kG) = M$.

In this encrypted communication, a peeper can only see $E_p(a, b)$, K, G, C_1, C_2 and would find it difficult to get k by K, G or obtain r by C_2, G . Therefore, it is impossible for H to get the plaintext sent between A and B.



In cryptography, describing an elliptic curve on F_p , six parameters are commonly invoked:

$$T = (p, a, b, G, n, h)$$

(p , a , b used to determine an elliptic curve, G as the base point, n is the factorial of the point G , h is the integer results from division of the number of all points on the elliptic curve m by n); The value of these parameters directly impact the security of encryption. The parameter values generally require the following conditions:

1. The bigger the value of p , the more secure, but the slower the computing speed: it is sufficient to meet general safety requirements to have a value of around 200
2. $p \neq n \times h$
3. $pt \neq 1 \pmod n$, $1 \leq t < 20$
4. $4a^3 + 27b^2 \neq 0 \pmod p$
5. n is a prime number
6. $h \leq 4$

The Penta Network has set up an identity authentication system to make it easier to achieve synergies with consortium blockchains and centralized systems that

adopt stricter requirements on security, information sensitivity and qualification of participants. In the Penta Network, the identity authentication is performed by an authoritative traditional certification agent and then the user identity and authorization information would be desensitized before saving them in the Penta ledger for verification by other users.

In order to prevent abuse of resources in the Penta Network and generation of excessive spam transactions and to enhance platform security, the Penta Network deducts a certain amount of PNT as operation and storage cost from wire transfer and execution of Smart Contract by a user. PNT holders may vote to determine if PNT deduction system and quota are applicable to these actions above.

4. Application of Penta Network

In the past two years, our Penta team has been collaborating with numerous industries in the field of blockchain and has implemented several projects. In the future, our Penta team will be committed to penetrate into more industries by developing a robust blockchain infrastructure that help provide more business solutions to improve efficacies and save costs.

The Penta Network will build a universal-benefiting blockchain network that may contribute to social, economic and other areas. The Penta Network will combine new technologies such as artificial intelligence, big data, VR/AR, robotics, internet of things, and cloud services to promote applications in healthcare, transportation, IP, automobile, organic agriculture, power, fashion, food, e-commerce, finance, game and other industries.

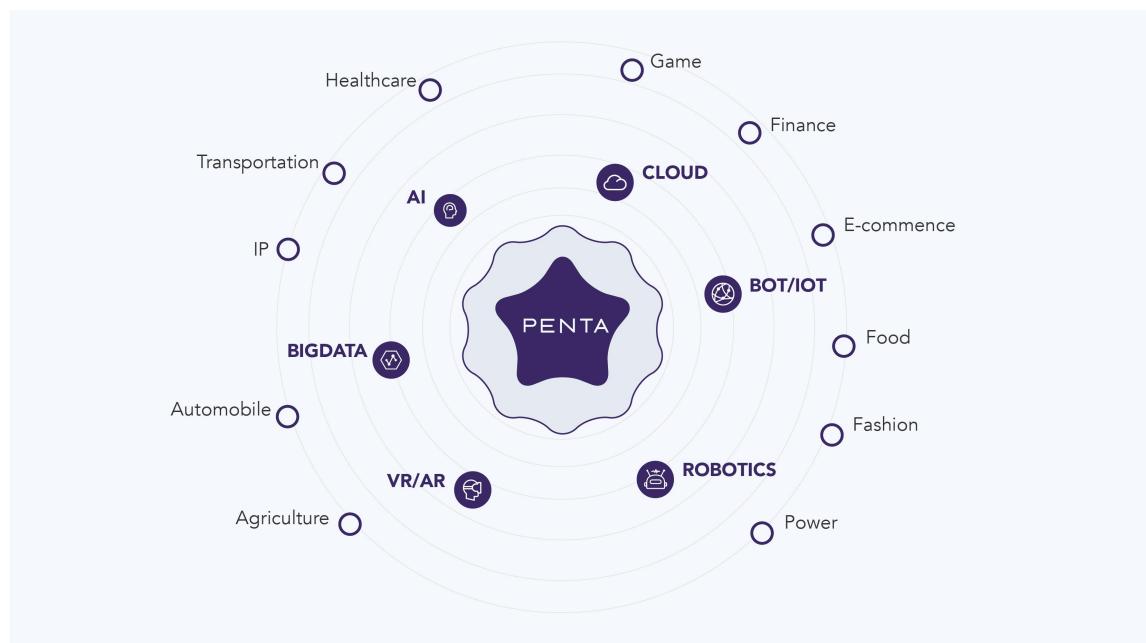


Figure 4 Application of Penta Network

4.1. Social Applications

4.1.1 Healthcare

The healthcare industry is undergoing a significant reform: the digitization of medicine, devices, services and business models. During the process, the health care system is becoming friendlier to the public and new values are generated. Most countries have promulgated policies that aim to digitalize the health care system and increase digital health records which include digitalization of health care and medical records as well as other healthcare systems or facilities.

Security, integrity and limits on authority and access to personalized healthcare data have now becoming the critical factors that would affect the success of innovation in the healthcare industry. The health care sector has been struggling to strike a balance between risks and returns and the blockchain technology boasts the potential to promptly meet the pressing needs by contributing to the healthcare sector in the following aspects:

- 1) Data Security

Unlike existing security systems, blockchain runs on distributed networks using a built-in encryption security system that is technically anti-manipulation. Players in the health care sector such as equipment manufacturers and medical technology companies may leverage the blockchain technology to enhance their capacity in identifying and managing devices and to provide selective access to a patient's health data.

- 2) Exchange of Healthcare Data

The sharing of health care data is more than information exchanges. It is the share of accountability and information based on mutual trusts between two or more systems or entities. The Penta Network may provide a trusted, anti-manipulation workflow by forming a "single source of data" for the exchanges of health data to ensure the integrity of the system and model.

- 3) Medicine Security

A distributed healthcare system based on blockchain may help verify whether medicines are authentic and make the medicine prices transparent.

4) Precise Medical Treatment

Pharmaceutical companies are under increasing pressure to prove the value of their drugs. Based on industry estimates, about \$300 billion of drugs were wasted each year due to failure in achieving desirable results while patients are suffering from the side effects of drugs. As a result, the pharmaceutical industry must move to a patient-centered drug development model that may enables targeted therapies in the future.

The concept of precise medical treatment changes service delivery model in the healthcare sector.

With its perfect security infrastructure, blockchain technology enables seamless exchanges of health data and promotes larger-scale genomics and scientific research, thus facilitating the development of precise medical treatment. With more players in the pharmaceutical industry increase their stakes in precise medical treatments, anti-manipulation records kept by a blockchain may help mitigate the burdens and costs on verification of clinical data and may facilitate the sharing of research achievements.

Commercialization and combination of the Penta Network with the healthcare industry in the future may effectively improve efficiency in the operation and management of the health care system by building a medical security system that is credible, traceable, transparent and safe.



Figure 4.1.1 Penta Network-Based Medicine Traceability Application

4.1.2 Application in the Energy Sector

The growing shortage of conventional energy resources and the environmental pollution goes with them have plagued the world. On the other hand, technologies related to renewable energies (such as wind and solar) are gradually becoming mature but have not yet been widely adopted. Pursuant to estimates on the industry, wind contributes merely 4% of powers while solar a meagre 1%. The underlying causes of such discrepancy are complicated transmission conditions, diversified equipment and difficulties in power scheduling and transmission channel controls as a result of centralized operations by traditional large power grid (State Grid, China Southern Power Grid, etc.). In this case, large-scale application of distributed energies is facing an array of technical obstacles and conflict of commercial interests.

With the rapid development of Internet communication and processing technologies, Jeremy Rifkin, an American scholar, proposed the concept of "Energy Internet" in his book named "Third Industrial Revolution" and the concept quickly gained popularity. In 2016, the State Grid released the "White Paper on Urban Energy Internet Development (2016)" in which the vision is first proposed

that an Urban Energy Internet UEI (Urban Energy Internet) should be built to make the city an autonomous entity featuring efficient, clean, electrified and intelligent allocation of energies in urban areas.

Given access, transaction and use of a distributed energy network is currently made possible, a solution to existing issues may be revisited from a new perspectives: building mini power grids that are independent from each other, rather than making an overhaul of the traditional large power grid. A Community Energy Internet (CEI) that “encourages multiple connection, interaction, access, transaction and response among various energies” within a certain area may be formed and combined to generate a UEI that eventually interfaces with traditional power grid and forms an energy internet ecosystem. This requires not only a breakthrough in the field of internet of things but also innovation and reform in information platform and business model. To make breakthroughs, it is critical to establish a decentralized SPX (Smart Power Exchange) that facilitates autonomous, transparent transaction and information sharing among electricity providers and consumers in a certain physical region and provides a win-win reward mechanism that helps enhance efficiency in energy transmission and utilization.

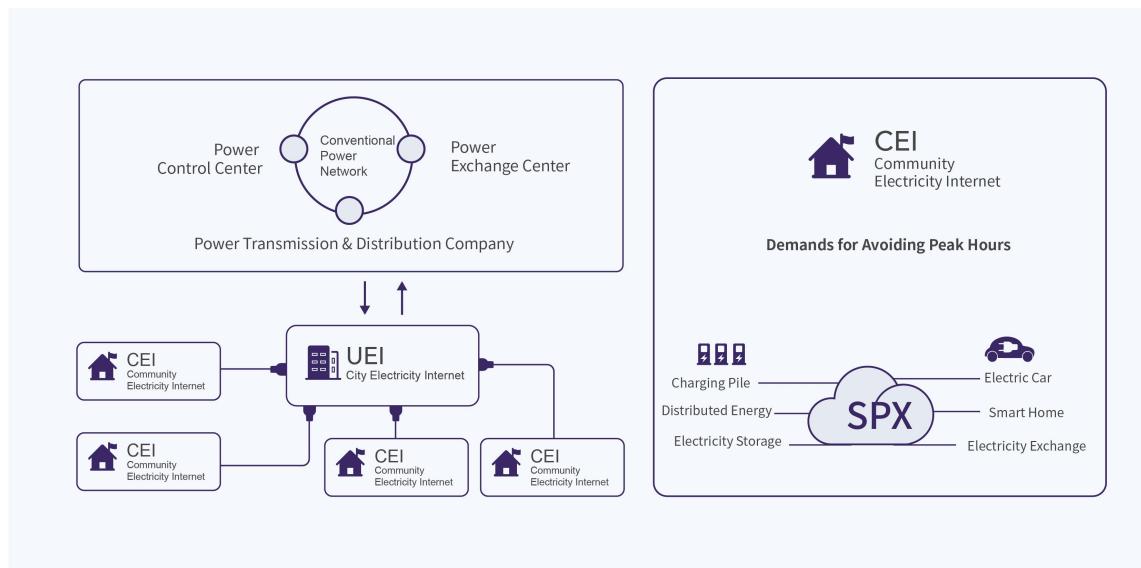


Figure 4.1.2 SPX Empowered CEI

A decentralized power-trading SPX (Smart Power Exchange) based on the Penta Network aims to establish an information platform and create a new business model that enables energy internet in a limited virtual community with an application structure including a variety of functions such as publishing available resources, finding energy and posting request, smart matching, order execution, smart meter and measurement data transmission, e-wallet, order settlement and otherwise.

4.1.3 Internet of Things ("IOT")

With the development of IOT technology, intelligent hardware and blockchain technology, IOT will inevitably lead to an era of the blockchain of things ("BOT").

The Penta Network is dedicated to eventually enable an era of BOT that combines technologies of things autonomy, value transfer, artificial intelligence and robotics.



Figure 4.1.3-1 Penta-Based BOT Ecosystem

Taking Distributed Charging Points (“DCP”) business, an application of BOT, for example, given the low-carbon feature of electric vehicles, and the initiatives to make vehicles oil-free as increasingly taken by governments across the world (it is reported that Germany plans to stop production of gasoline and diesel vehicles by 2030 and Britain plans to ban gasoline vehicles by 2040), the development of electric vehicles has become an irresistible historical trend. Nevertheless, the convenience of charging is a critical issue that impedes the widespread application of electric vehicles. As revealed in a survey conducted by a media reporter, among the total of 340 charging points in the 42 public charging stations in a city’s core six areas, 61 are charging, accounting for 17.9%, 35 are damaged or malfunctioned, accounting for 10.2%, and 92 are occupied, accounting for 27%”. Because these charging facilities are centrally invested, constructed and operated by power grid companies, electric car companies and charging point operators, there are multi shortcomings in terms of flexible operation, connectivity and sustainability, and thus are difficult to meet increasing demands for charging electric vehicles.

The main reason for the difficulties in charging is excessive dependence on the charging points (fast and slow charging points). In addition, a large number of privately-funded charging facilities are not shared and other potential power providers (such as community stores and parking lots) simply cannot provide charging services. All of these in essence are due to the lack of an effective form of electricity transactions, including lack of supply and demand matching, measurement, and settlement measures.

By building a SPX platform, the Penta Network is able to provide smart metering devices, and smart fast and slow charging devices to potential power providers such as private charging points, parking lots and community stores, thus making it possible for them to provide charging services while concurrently publishing available resources in SPX so that users may quickly find charging points and

complete transactions through a variety of channels including APP or SPX APP of electric car companies, thus dramatically improving efficiency in transmission and in utilization of electric energy.

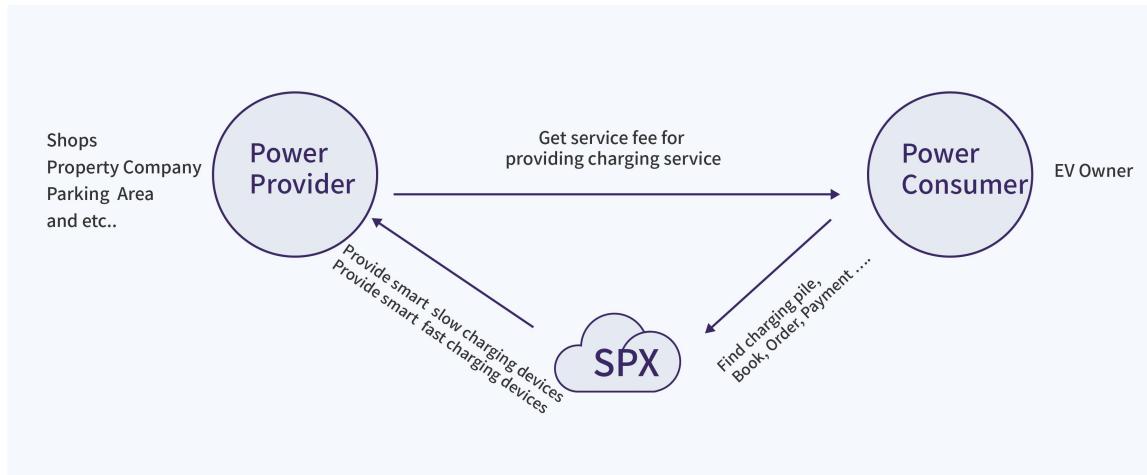


Figure 4.1.3-2 Shared Charging Services Empowered by SPX

Demand Response:

Demand Response (DR) means using capital rewards to induce users to change the original pattern of behavior in respect of the use of electricity for the purpose of reducing or delaying demands on electricity in a certain period of time to better allocate the power supply, thus ensuring the stability of the power system.

Under the current centralized system managed by power grids, demand response is managed in a centralized manner. Organizations and individuals participating in demand response need to submit applications in advance, electrical equipment should be renovated and monitored, and a contract should be executed, all of which are burdensome and subject to stringent requirements, thus making it difficult for retail users to participate and rendering large-scale application impossible, both of which in turn affects effects of demand response.

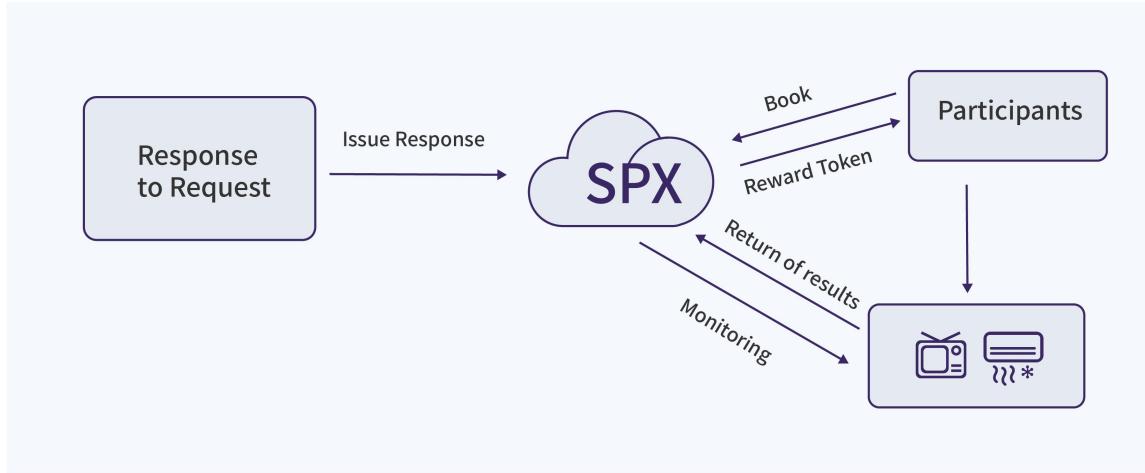


Figure 4.1.3-3 Demand Response Empowered by SPX

SPX may become an integrator in respect of demand response by receiving demand contracts and events from power grid companies and publishing them and setting Smart Contract in SPX that enable order placement or making of reservation by any entity in CEI. During this process, SPX will obtain the total amount of demand response from grid companies, and will break down the total amount to individual tasks to be executed by fragmented entities so that more retail participants may take part in the demand response process, thus achieving a long tail effect. In addition, the tolerance function is set in the Smart Contract to prevent the promptness and accuracy of the overall demand response from being affected by a small number of defaults. During the execution of demand response, SPX monitors the demand response through the intelligent terminal provided in advance free of charge. Or a proactively response may be rendered possible without any such intelligent terminal based on a trusted relationship and credit evaluation. As an integrator, SPX receives demand response rewards from the grid company, and pass such rewards to participants in real time in the form of token.

4.2. Financial Application

Blockchain is an emerging technology that develops fast. The financial sector usually lags behind other industries in the adoption of a new technology. Nevertheless, seen from the members in various blockchain organizations, financial institutions are the most active participants with the largest number of members comparing to those from other industries. This is because of the natural bond between blockchain and finances, which also enables the use of blockchain in various sub-divisions of the financial sector including the following:

- In terms of asset transaction, blockchain may be used for peer transaction, commercial paper, supply chain finance, asset-backed securitization and otherwise.
- In terms of payment settlement, blockchain may be used for interbank settlements, cross-border payment, point rewards and otherwise.
- In terms of credit, blockchain may be used for credit reference, pledge, mortgage, loans, supply chain finance and otherwise.
- Blockchain may be used for other financial services such as P2P lending crowd funding and otherwise.

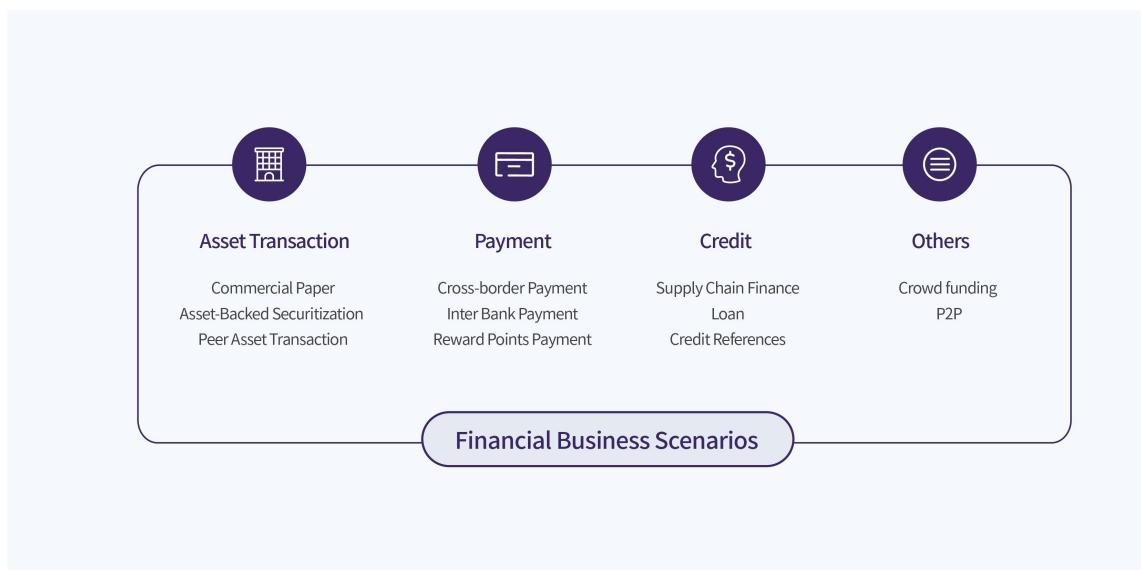


Figure 4.2 Financial Business Scenarios

The Penta Team has accumulated profound experience in combining blockchain with the financial sectors and has launched physical projects in respect of credit reference, point rewards, asset-backed securitization and supply chain finance.

4.2.1 Credit Reference

Recent years have seen exponential growth in the scale of credit and the population using credit. Continued growth in credit business leads to increasing demand for credit reference services at a time when technical improvements and recognition by the public have provided conditions conducive for fast development in China's credit reference sector.

Critical challenges facing the Chinese credit reference market are as follows:

- 1) Currently credit reference and information on banks and their clients are readily available but information on smaller companies such as smaller financial leasing entities are not due to high credit reference threshold as set forth by the People's Bank of China.
- 2) Lack of data sharing between credit reference agencies and serious gap in information between credit reference agencies and users.
- 3) Limited channels for collecting formal market data leads to wasteful fight over data sources.
- 4) Serious issues in data privacy protection and failure of traditional technical architecture in meeting new regulatory and government requirements.

Blockchain featuring decentralization, trustless, time stamping, asymmetrical encryption in combination with Smart Contract may help share and verify credit reference information in a limited and controlled manner with effective protection for data privacy. To resolve problems in the current credit reference industry, the Penta Network focuses on data sharing and builds a credit reference service

platform powered by blockchain so as to minimize risks and costs for participants and to expedite submission, query and settlement in respect of credit data.

The credit reference service platform offered in the Penta Network involves a variety of nodes including credit reference institutions, users and other institutions (such as small lending institutions, banks, insurance companies and government departments), and enables data sharing between lending institutions and credit reference agencies.

To prevent abuse of credit information, the Penta Network uses Smart Contract to set up credit reference verification and authorization mechanism and record such authority and queries by using the blockchain to make them traceable. Because a blockchain cannot be reversed, credit agencies will not be able to abuse its use of credit references. In addition, sensitive clients' data are encrypted and may be accessed only by authorized users.

This blockchain platform is currently launched in China and some small-loan lenders are already active on the platform. The platform provides credit data, collateral data, data on blacklists or data submitted or queried by a regulator or other third parties. In addition, the team also designed a point rewards and consumption mechanism to encourage all connected participants to share more data.



Figure 4.2.1-1 Penta-Based Credit Platform

This credit platform operates smoothly ever since its launch and has seen consistent increases in participating institutions and other nodes. The following is the monitoring information in respect of the trading blocks in the credit platform.

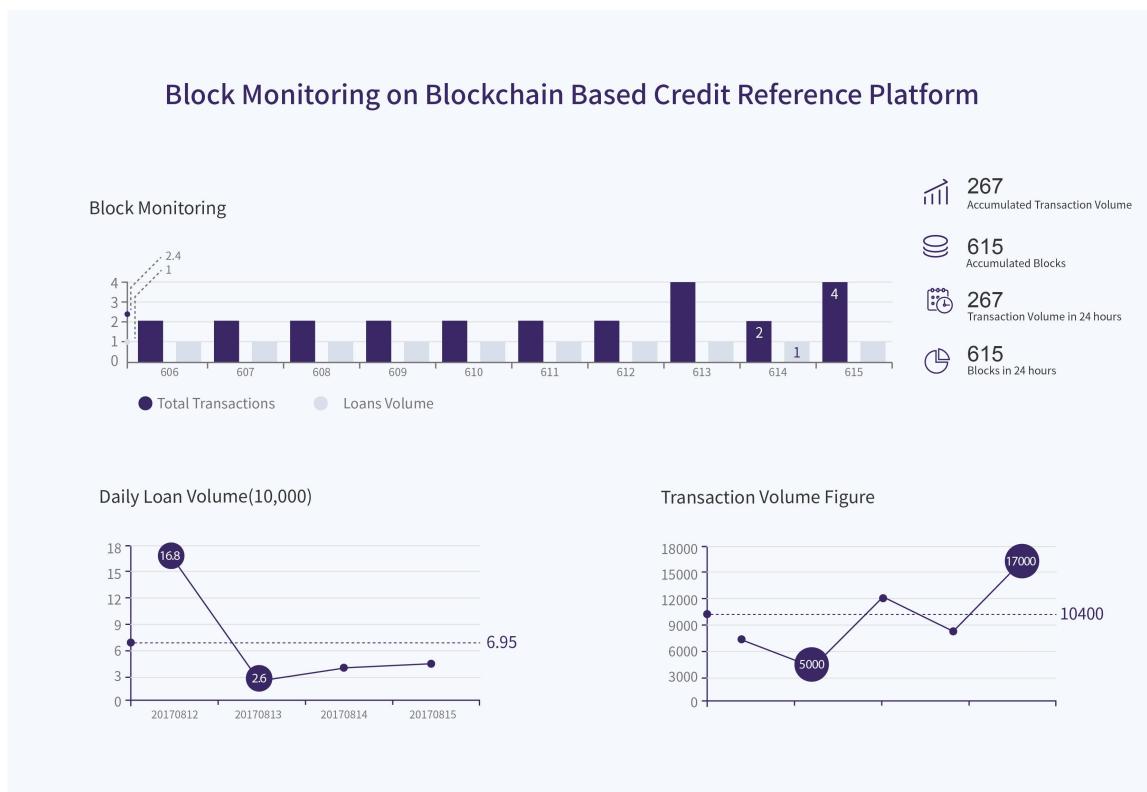


Figure 4.2.1-2 Block Monitoring in Credit Platform

4.2.2 Supply Chain Finance

With the development of economies and industries, accounts receivables in enterprises are growing. Fully using the receivables as potential collateral for bank loans spells huge potential in supply chain finances.

The Penta Network has provided solutions for a number of banks, financial companies and other financial institutions in the past few years. During the provision of such services, the Penta Network gained an in-depth understanding in the complexity of supply chain finances: verification of multi-party contracts and transaction supporting documents are burdensome, time-consuming and inefficient. This is primarily because of lack of trust and information exchanges among multi-players in supply chain finances. For instance, a typical order financing transaction would involve buyer, seller, buyer's bank, seller's bank, logistics companies, supervisory agencies, customs authorities (cross-border order financing) and others.

In addition, many categories of financial products are involved in supply chain finances throughout a specific transaction from the formulation of production plans, acceptance of goods to closing of funds. Furthermore, a wide range of products is supported including purchase order financing, cash flow loans and fund settlement.

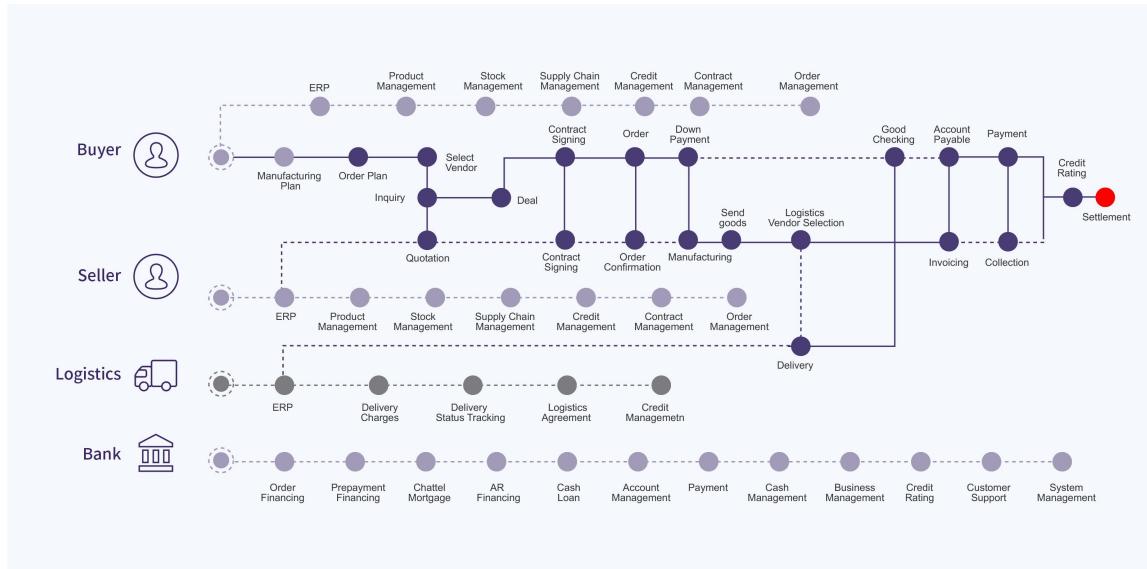


Figure 4.2.2-1 Supply Chain Finance

Combining blockchain with supply chain finance enables authentication and verification (anti-manipulation) by blockchain of the orders, L/C, bill of lading and documents related to trade procedures that are placed in the blockchain. Meanwhile, the digitalized solution as provided by using the blockchain may completely replace paperwork that is manpower-consuming and may bring in total transparency, enhanced efficiency and mitigate risks.

To elaborate on the services that the Penta Network has provided for a certain financial institution for an order financing transaction, the figure below shows the scenario and how the blockchain contributes to make it easier: .

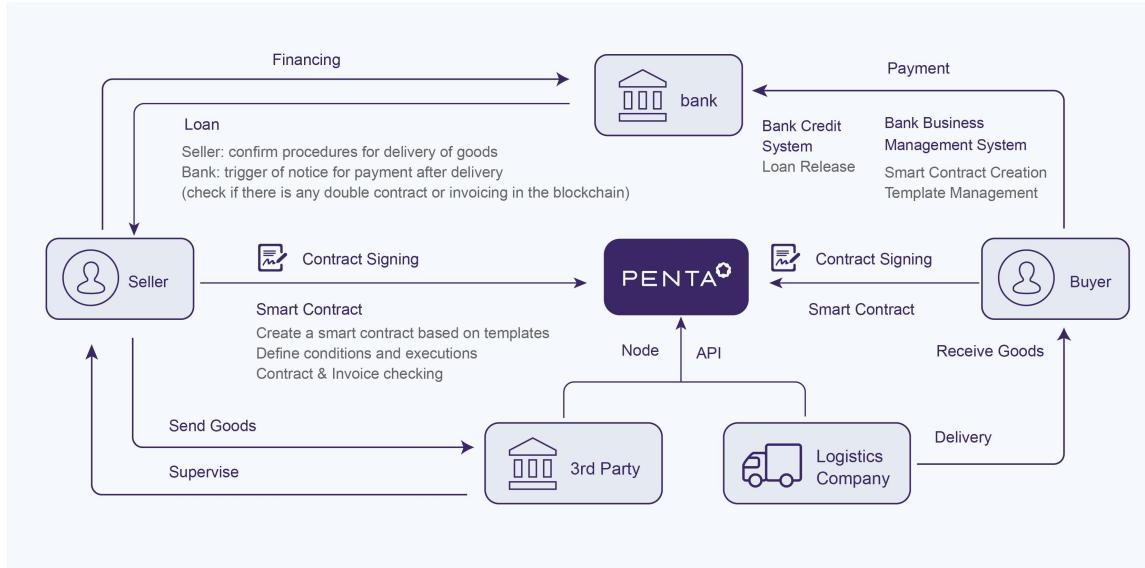


Figure 4.2.2-2 Purchase Order Financing

Parties to the foregoing transaction include buyer, seller, buyer's or seller's banks, logistic companies and third-party regulators and specific procedures are as follows:

- 1) Entry of terms and conditions of the contracts executed for the order financing transaction into the Smart Contract;
- 2) Grant of credits and loans by financial institutions based on the status of contract execution and shipment.
- 3) Financing by the buyer based on status of the underlying order and automatic implementation and payment by Smart Contract upon expiry,
- 4) During the process, logistics and supervising companies register the business status on blockchain.

4.2.3 Asset-Backed Securitization

Asset-backed securitization involve multi-parties and a burdensome process and requires the establishment of a dedicated SPV (special purpose vehicle for asset management) to insulate risks. The following is the structure of a typical asset-backed securitization transaction:

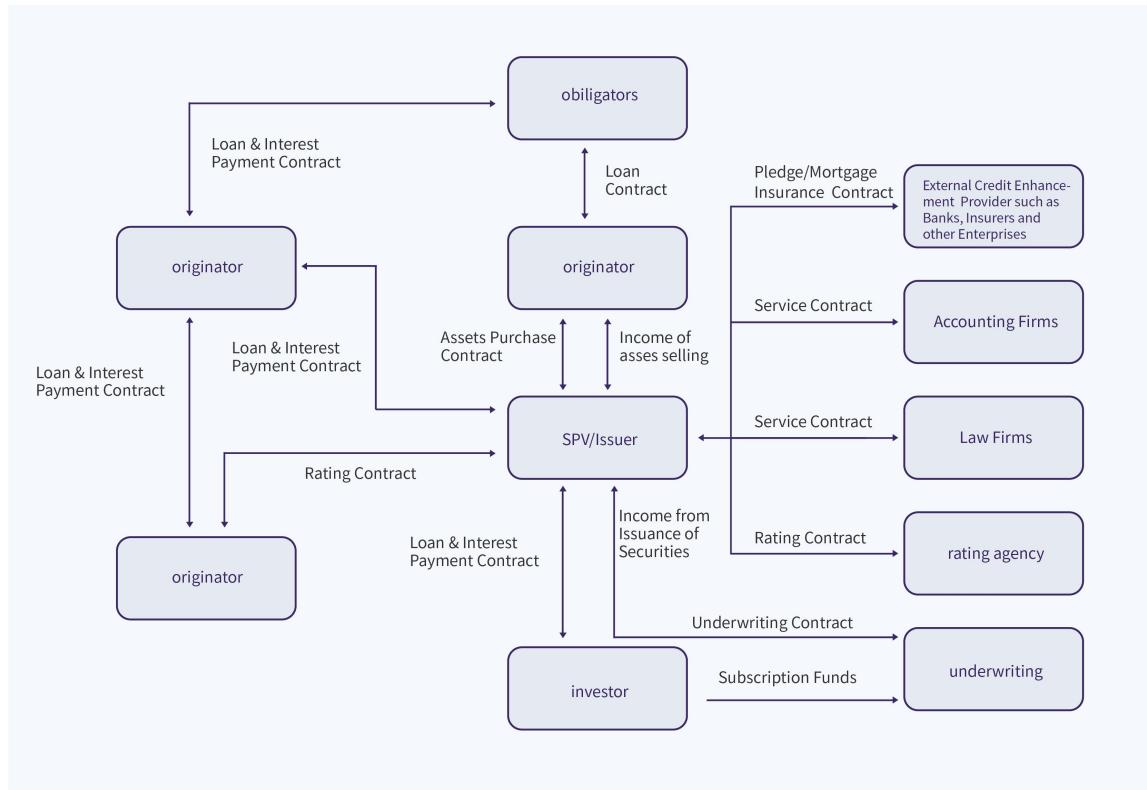


Figure 4.2.3-1 Basic Transaction Structure

Exchanges of information among SPV, sponsors, original debtors, investors, trustees, service providers, accounting firms, law firms, credit rating agencies, securities underwriters and others are costly and verification of information is time-consuming. After connecting all B institutions and C clients with a blockchain, data on secured assets are reliable, distributions of assets among participants are traceable, and ratings by third-party agencies are transparent. Reliable blockchain information effectively reduces costs on communication among and verification by institutions. Transparent information may help investors to make informed decisions on investment at risk on the basis of accurate information.

For this purpose, the Penta Network has created an intelligent asset securitization platform based on blockchain to register underlying asset and asset appraisal, audits and transaction information in the blockchain.

Transparency in assets may promote healthy developments in asset-backed securitization business and reduce regulatory costs.

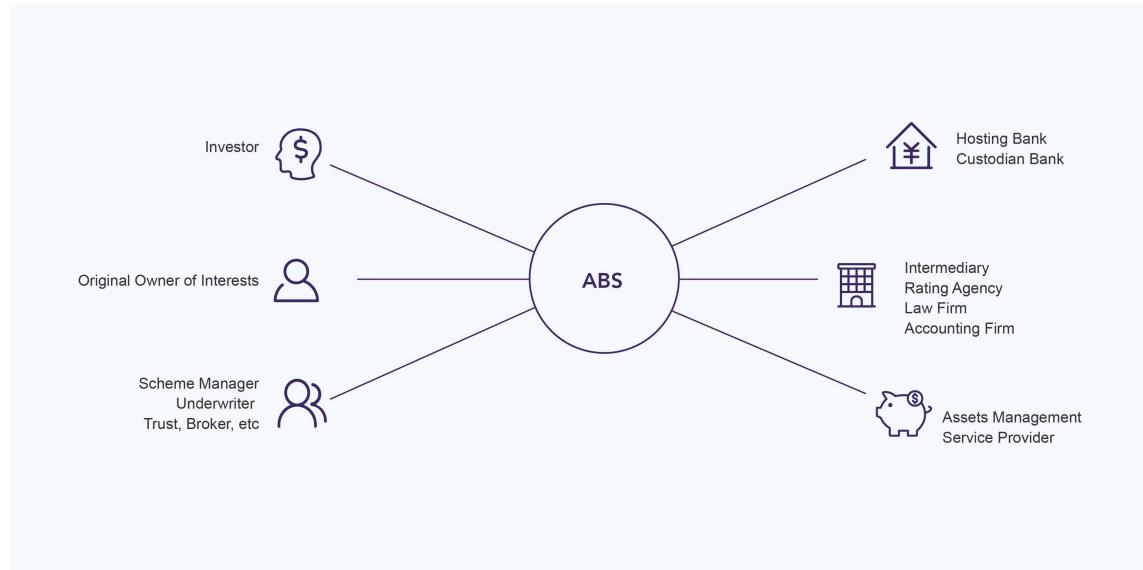


Figure 4.2.3-2 Penta-Based Asset-Backed Securitization Platform

The intellectual asset securitization platform based on blockchain supports asset management and operations by each party to an asset-backed securitization transaction. Each institution may create a node for recording its own data and thus make its data more reliable.

5. Definitions

Definition	Description
Bitcoin	A crypto-currency that was launched by a developer using the fake name of Satoshi Nakamoto in 2009 in the form of open-source software.
Consortium Blockchain	The blockchain that is restrictive in terms of openness and decentralization, in relation to Public Blockchain and in which participants have already reached consensus and mutual trust.
Ethereum	A public blockchain platform that offers smart contract functions.
Ethereum Virtual Machine	A virtual machine that runs on all nodes participating in the peer-to-peer network that may read and write executable codes and data in a blockchain. May verify digital signatures and may run codes by way of half-Turing completeness. Such machine executes codes only upon receipt of message verified with a digital signature and information storage in a blockchain may distinguish appropriate acts.
Hyperledger	The open-source community originated by IBM with a focus on consortium blockchain.
Load Balance	Built on the existing network structure. It made available a transparency, effective and cheap method to expand the bandwidth of network devices and servers, increase traffic, enhance the capacity for processing network data and improve flexibility and availability of a network.
P2P	Peer to Peer network. It is a distributed application structure that enables assignment of tasks and work load among peers and is a form of network or web generated in the application layer by using the peer-to-peer computer models. The English word of peer means 'counterparty, partner and opposing end'. Therefore, seen from the literal meaning of the word, P2P may be understood as peer-to-peer computing or networking.
PBFT	Practical Byzantine Fault Tolerance, an algorithm put forward by Miguel Castro and Barbara Liskov in 1999 to resolve the inefficiency in the original Byzantine Fault Tolerance by reducing the complexity of the algorithm from the exponential

	level to the polynomial level and thus making it possible to run the Byzantine Fault Tolerance in real system applications.
POS	Proof of Stake. A system that enables the distribution of interests based on the quantity of coins and the length of the time that a person holds the same. The term of Coin Age is introduced under the POS model. A coin may accumulate one Coin Age for each day for each coin. For instance, if you hold 100 coins for a total of 30 days, then your Coin Age will be 3,000, and if at that time you find a POS block, your Coin Age will be cleared to zero.
POW	Proof of Work. The number of coin depends on the effective work that a person has contributed to mining. Most coins including Bitcoin, Litecoin and otherwise are based on POW models: the greater the computing power and the longer the mining time, the larger number of coins that a person may receive.
Public Blockchain	A blockchain that enables anyone to send a transaction from anywhere to get the transaction effectively confirmed and that enables anyone to participate in the consensus process.
QOS	Quality of Service. The capacity how a network takes advantage of various basic technologies to provide better services to a designated network communication. It is a network security mechanism and a technology that may be used to resolve network latency and congestion.
RSA	An internationally accepted public key algorithm that was first published in 1978 by Rivest, Shamir and Adleman. The password system for public keys is different from that of traditional symmetric passwords that solely use one key. Algorithms are based on mathematical functions rather than replacement and substitution. Public key is encrypted in an asymmetric form and uses two independent keys. In other words, the key is divided into public and private ones, thus being called a two-key system. The public key in the two-key system may be made public and is thus called the public key algorithm.
Smart Contract	A program that is time-driven, in a certain status and is run in a reproduced, shared ledger that has

State Recognised Algorithms

the capacity to retain assets on the ledger.

The algorithms recognised by the State Cryptography Administration Office of Security Commercial Code Administration which primarily include SM1, SM2, SM3 and SM4 with key and grouping lengths both at 128 bits. SM1 is symmetric encryption system with encryption strengths the equivalent of AES. Its algorithm is not public and is called by using interface of encryption chips. SM2 is an asymmetric system based on ECC. Its algorithm is made public. Because its algorithm is based on ECC, the speed of signature and generation of private key is faster than RSA. ECC 256 Bits (SM2 uses a form of ECC 256 bits) is of security strengths stronger than RSA 2048, but enjoys a computing speed faster than RSA. SM3 message summary may be understood by comparing it with MD5. It's algorithm is made public and the verification result is of 256 bits; SM4 is the standard data grouping algorithm for Wireless LAN. Symmetric encryption and the lengths of private key and grouping are all 128 bits.

Token

Digital currencies other than Bitcoin

Turing Complete Language

A computer system that can resolve each Turing-computable function is considered a system with Turing completeness. If a language is deemed as a language with Turing completeness, it means that the language has the computing power equaling that of a Universal Turing Machine, (i.e., the greatest power that a modern computer programming language may possess.)

6. References

- [1] G. Ateniese, R. Burns, R. Curtmola, J. Herring, O. Khan, L. Kissner, Z. Peterson, and D. Song. Remote data checking using provable data possession. *ACM Trans. Info. & System Security*, 14(1), May 2011.
- [2] M. T. Goodrich, M. Mitzenmacher, O. Ohremenko, and R. Tamassia. Privacy-preserving group data access via stateless oblivious RAM simulation. In *SODA*, 2012.
- [3] H. Shacham and B. Waters. Compact proofs of retrievability. *Proc. Asiacrypt* 2008.
- [4] C. Huang, H. Simitci, Y. Xu, A. Ogus, B. Calder, P. Gopalan, J. Li, , and S. Yekhanin. Erasure coding in Windows Azure storage. In G. Heiser and W. Hsieh, editors, *Proceedings of USENIX ATC 2012*. USENIX, June 2012.
- [5] L. Rizzo. Effective erasure codes for reliable computer communication protocols. *ACM SIGCOMM Computer Communication Rev.*, 27(2):24 – 36, Apr. 1997.
- [6] M. Liskov, R. Rivest, and D. Wagner. Tweakable block ciphers. *J. Cryptology*, 24(3):588 – 613, July 2011.
- [7] V. Buterin. Ethereum , Apr. 2014.
- [8] V. T. Hoang, B. Morris, and P. Rogaway. An enciphering scheme based on a card shuffle. In R. Safavi-Naini, editor, *Proceedings of Crypto 2012*, LNCS. Springer-Verlag, Aug. 2012. To appear.
- [9] Nakamoto, S. 31 October 2008. "Bitcoin: A Peer-to-Peer Electronic Cash System". Also known as the Bitcoin whitepaper.
- [10] Kyle Randolph. "A Next-Generation Smart Contract and Decentralized Application Platform". Also known as the Ethereum whitepaper.
- [11] Christopher Ferris. "Hyperledger fabric Protocol Specification".

-
- [12] Miguel Castro, Barbara Liskov. "Practical Byzantine fault tolerance and proactive recovery".
 - [13] Hal, F. "Reusable proofs of work" <http://www.finney.org/~hal/rpow/>.
 - [14] Tushar Deepak Chandra, Vassos Hadzilacos, Sam Toueg. "The Weakest Failure Detector for Solving Consensus".
 - [15] Manos Kapritsos, Yang Wang, Vivien Quéma, Allen Clement, Lorenzo Alvisi, Mike Dahlin: All about Eve."Execute-Verify Replication for Multi-Core Servers"
 - [16] ZMWorm[CCG]. Introduction to ECC encryption algorithm
 - [17] Michael Rosing. Chapter 5, "Implementing Elliptic Curve Cryptography", Softbound, 1998