PENTA

THE UNIVERSAL BLOCKCHAIN CONNECTOR

Technology Whitepaper

Penta Network

V1.2.0 | 2018

Abstract

The excitement surrounding blockchain technologies has inspired in a profusion of different platforms and projects. With so many different platforms, however, the problem of interoperability has emerged as a significant challenge. A lack of interoperability between blockchain platforms is, in fact, a symptom of the larger problem that blockchains in the “on-chain world” lack compatibility with the “off-chain world”, creating a lack of connectivity between blockchain technology and the real economy. Next generation blockchain technology is focused on solving the challenges or interoperability and scalability, so that distributed ledger technology can be applicable in the real world.

This whitepaper discusses the core architecture of the Penta Network, a next generation blockchain network. The following sections will elaborate on Penta’s five dimensions of connectivity, which connect the digital world to the real world - Identity, Credibility, Value, Transferability and Economy – and will discuss how the Penta Network intends to use blockchain technology to build a better economy.

Table of Contents

1. Penta Overview

Penta, (also referred to as “ Penta Network ” or “ PNT ”) is a next generation platform for both public and private blockchain projects, designed to be a premier platform for transferring value and operating high-performance decentralized applications. Penta will remove roadblocks and reshape the blockchain landscape with an emphasis on impacting the real economy. With its unique consensus algorithm (DSC) and a truly distributed network architecture, Penta is building the world’s most inclusive, equitable, and decentralized blockchain community.

The Penta Network will be able to connect to a wide range of blockchain networks with existing digital networks and off-chain systems, providing a comprehensive solution to the interoperability problem. At the core of the Penta Network is a robust public blockchain infrastructure that supports a high-performance application platform. In the same way you can download apps from the App Store onto your smart phone, you will be able to access decentralized applications (DApps) that run on the Penta blockchain. Distributed applications launched on Penta will be able to traverse digital networks as productive tools for the digital economy.

Through its unique and innovative technology and its commitment to building an inclusive and decentralized community, Penta will be able to fulfill its goal of being a “Universal Blockchain Connector,” connecting blockchain technology to the real world.

Core team members of the Penta Network come from leading technical and financial organizations across the world, including NASA, Google, Morgan Stanley, ABN AMRO and Deutsche Bank. Penta’s experienced team possesses world-class experience in the technical, business, and economic aspects related to blockchain development.

At the center of Penta's mission is using blockchain technology to increase economic inclusion. We will achieve this by lowering barriers to entry and increasing opportunities for Penta stakeholders to share in the wealth generation of the Penta Network through incentive allocations. Penta has pioneered innovative technology and social governance mechanisms that will allow the Penta Network to thrive in the emerging Smart Economy.

Penta Network is shaping a connected future!

2. Five Dimensions of Connectivity

One of Penta's core tenets is a philosophy of universal connection, embodied by the Five Dimensions of Connectivity: Identity, Credibility, Value, Transferability and Economy. By interconnecting these five dimensions and integrating them into Penta's blockchain network, Penta will be able to bridge the gap between the digital world and the physical world. In acknowledgement of these five dimensions, Penta has adopted a five-pointed star as its logo.

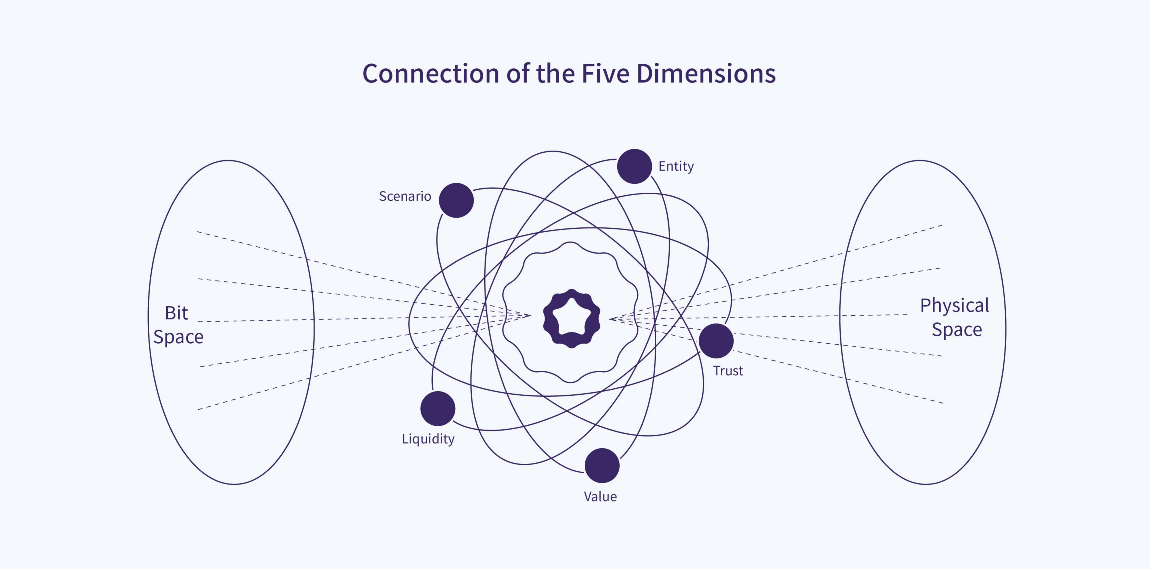


Figure 2 Connection of the Five Dimensions in the Penta Network

2.1. Identity

All participants, including any person, organization, system, will be assigned a standard form of digital identity in the Penta Network. The Penta Network will manage transactions and requests based on the authorization of a digital identity. This framework for digital identity allows for individuals to manage multiple identities.

The Identity dimension includes creation, use, verification, and storage. All these are managed in a decentralized manner to protect the privacy and security of transactions.

- Creation: Each identity is generated by using a PKI encryption mechanism, a form of asymmetric encryption; public address information is also generated. The owner of an identity possesses the public address and private key information. In addition, a certificate issued by the digital certification center for identity verification may also be supported.
- Use: An authorized 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 and verifies each transaction through a consensus mechanism, as described elsewhere in this white paper.
- Storage: Public information corresponding to an identity is saved in the distributed ledger of the Penta Network as public information.

In addition, Identity supports Smart Contract extensions and thus a wider range of forms for identity management that can meet diverse identity requirements in a variety of business areas. For instance, asset transactions in the financial sector are subject to KYC demands of the governing jurisdiction for a certain business. In such cases, Smart Contracts may be used to manage KYC across multiple jurisdictions.

2.2. Credibility

One of the important reasons for the boom in blockchain development is that blockchain technology has created trust through decentralization, increased transparency, and a community-oriented consensus mechanism that obviates the need for third parties to play a role as intermediaries in transactions. The Penta Network contains a distributed trust-generating mechanism that includes 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. Public information is recorded and saved in the distributed ledger. Some entities may manage their affairs by using a certified certificate.
- Trusted Network

  Transactions are confirmed and recorded in the Penta Network by using the Penta DSC consensus algorithm. Once confirmed, a transaction cannot be revoked or tampered with, in any form.
- Trusted Interaction

  Cross-chain transactions with other blockchain platforms or centralized systems are possible only after verifying authorization. The Penta Network supports cross-chain transactions via Smart Contract and requires consensus within the Penta Network, alongside any consensus as required by another blockchain in the transaction. This ensures data integrity and maintains an accurate record.

2.3. Value

The main function of blockchain is to support digital value transfer. All digital assets on the Penta Network can participate in transactions between participating entities, resulting in a transfer of value. The Penta Network offers a secure way for individuals, businesses, and communities to participate in the transfer of goods and services in a digital peer-to-peer network. Due to Penta's interoperability solution, such exchange of goods and services can take place across digital networks and involve real world assets, all powered and secured by the Penta Network.

Because Penta is a public blockchain, it contains a consensus mechanism that is used to validate Penta Network transactions. The unique consensus algorithm used in the Penta Network is called Dynamic Stake Consensus (DSC). Community members who contribute to the validation process receive a financial incentive in the form of Penta Network Tokens (PNT) as a reward for their participation. The hallmark of DSC is that it achieves scalability without sacrificing inclusion and fairness, fulfilling the goal of Penta to be an inclusive blockchain platform.

The Penta Network uses a Soft eXchange Adaptor to support trade and exchange of value with other blockchains, and uses Smart Contracts to confirm transactions and manage affairs.

2.4. Transferability

Envisioning itself as a blockchain platform for the future digital economy, or Smart Economy, the Penta Network not only supports new types of business scenarios but also addresses conventional business concerns. The Penta Network has been designed with business application in mind, and will connect business to one another and to other networks.

To assist businesses and entrepreneurs to activate their businesses on the blockchain, Penta offers DApp application development tools and SDKs to streamline the development process. Such DApps can be written in any coding language and do not require blockchain expertise, as once they are anchored on Penta, the Penta blockchain will provide the blockchain technology needed to run those applications. The Penta Network will offer the Chain Store to provide a platform for the use and promotion of DApps available on the Penta Network.

2.5. Economy

The Penta Network contains interoperability protocols to connect to other blockchains and digital networks in order to facilitate real world business application of blockchain technology. The Economy dimension reflects Penta's application-oriented approach to blockchain technology, which will empower DApps across industries to deploy successful solutions to any business scenario. Recognizing that to be successful in real world application there are a host of other technologies that play a role in workflow and transaction settlement, the Penta Network is designed to integrate cloud computing, big data, and artificial intelligence applications. See the network application chapter for more details.

3. Penta Technologies

Blockchain has gained wide attention from an increasing number of different industries with its attractive properties of: decentralization, immutability, and secure transfer of value. However, before it can fulfill its potential there are new, challenging obstacles for blockchain technology to surmount. The Penta Network seeks to address these, including:

1. Performance – Most existing blockchain platforms are weighed down by sluggish ‘transactions per second’ (TPS) throughput rates. While some advertise support for smart contracts, these show measurable performance gains only while executing simple contract code. Most of their associated DApps are slow running otherwise. Failing to meet user expectations, what is needed is a high performance blockchain platform to support real-world use cases.

2. Business Use Case Support - Another set of tests to commercial deployment of blockchain technology is capacity to support sophisticated business use cases. These vary greatly in their respective business logic, and thus require flexible application solutions. Practically every existing blockchain network does not support such as yet.

3. Risks from Centralization – A core feature of blockchain is providing computational efficiency without sacrificing the ‘democratization of authority’. But, any ‘proof of work’ (POW) consensus algorithm, firstly introduced with the bitcoin network, has eventually led to mining pool monopolies, while non-POW mechanisms such as ‘dynamic proof of stake’ (DPOS) and others, with a concentrated focus on efficiency-scalability issues, result in super-node centralization. A new and innovation-led approach is needed, incorporating the appropriate consensus mechanisms to deal with these issues.

4. Interoperability of Blockchain Platforms – Paradoxically the rapid progress of blockchain technology has been to a great degree due to development teams working independently and in isolation. The reasons for this may stem from how minimal attention to date has been given to discussion towards agreement on data standards and protocols, leaving developers free to quickly generate libraries of semi-functioning 'spaghetti code'. With the advantages of hindsight, these systems should have been planned to interoperate and function 'off-chain,' and now fail to effectively support any real business economy. Generating a suite of end-to-end blockchain technologies for seamless transfer of value between platforms, or between, blockchain platforms and existing cloud computing networks, or on-chain to off-chain is a central design requirement of the Penta Network.

As the 'universal blockchain connector' the Penta Network aims to serve real-world business needs and be the leading driver for commercial distributed applications (DApps).

3.1. Penta Network – Organization and Technical Structure

The framework of the Penta Network is composed of self-contained component. Like Lego bricks, developers build blockchain or sub-chain applications using these components that are designed for rapid prototyping, easy assembly and testing.

Storage and communication components are the main two for the blockchain platform. The Penta Network data messaging ranges from peer-to-peer (P2P) interactions, to distributed private communication networks and the Soft eXchange Adaptor. Besides blockchain archiving, data storage components offers file, database and key-value stores, which could be further extended to other storage components to meet user data volume demands and concurrency requirements.

The application components provide the basic utilities for creating Smart Contract, digital assets, incentive mechanisms, and tools for member and authority management.

Distinct from Ethereum's anonymity requirements, or Hyperledger’s certificate model, authentication of users is optional in the Penta Network and an identity might be displayed only when engaging with a specific type of DApps.

To promote a high level of security and efficiency, the framework is modular in design. Each operates as an independent service agent providing its set of functionality without impacting on the overall security of the solution architecture. For example, the consensus components support POW, POS, dPOS, PBFT, while the encryption algorithms modules supports RSA, and SM2, among others. Developers have freedom to extend the underlying component classes.

Functionally the Penta Network organizes itself into four divisions: Penta DLOS, Penta Blockchain, high performance DApp platform and Penta connector.

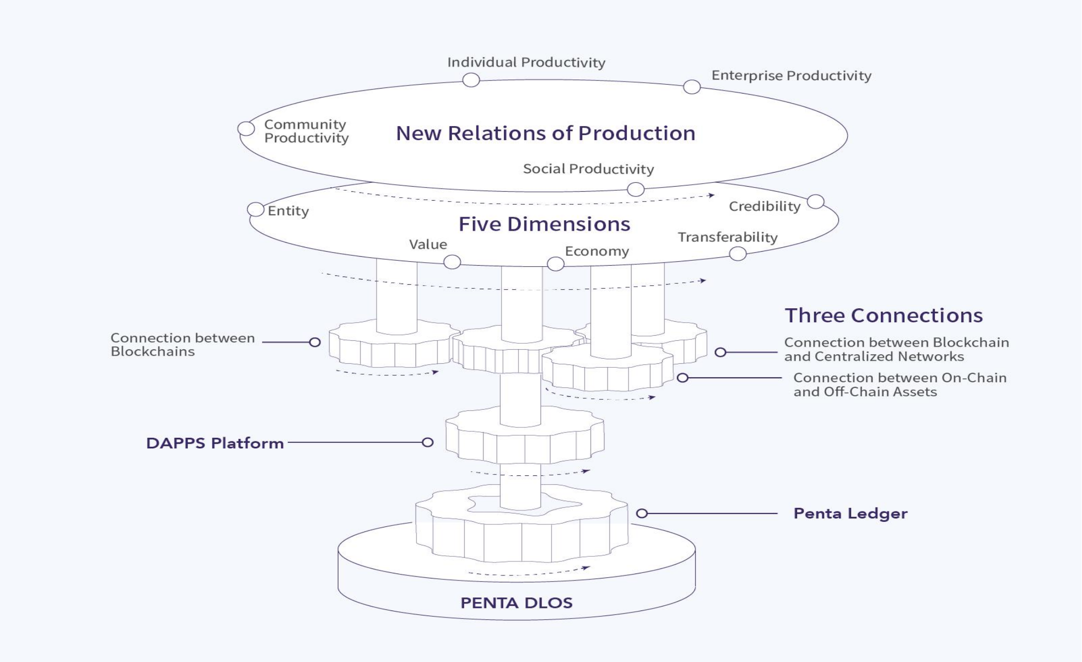


Figure 3.1-1 – Overview of the Penta Network Technical Structure

1. Penta DLOS - delivers a 'kernel' for building a blockchain platform, including: data storage, networking, and enterprise application and UI components.
2. Penta Blockchain - deploys the unique Dynamic Stake Consensus ('DSC') mechanism and Random Sorting Algorithm ('RSA') safeguarding a fair and democratic consensus mechanism that is consistent, efficient, scalable, and secure.
3. DApp Platform - delivers high-performance infrastructure to streamline use case application development. The DApp SDK includes tools and components for: information management, native file system access, application store, development testing and tools for DApp optimization.
4. Interoperability Layer - enables robust and secure exchanges of value between blockchain platforms, between blockchain and centralized cloud computing services, or from on-chain to off-chain systems.

Maintained by the Penta Global Foundation and its extended developer community, the Penta Network is a multi-chain system that hosts the 'Penta Blockchain' as its 'main chain'.

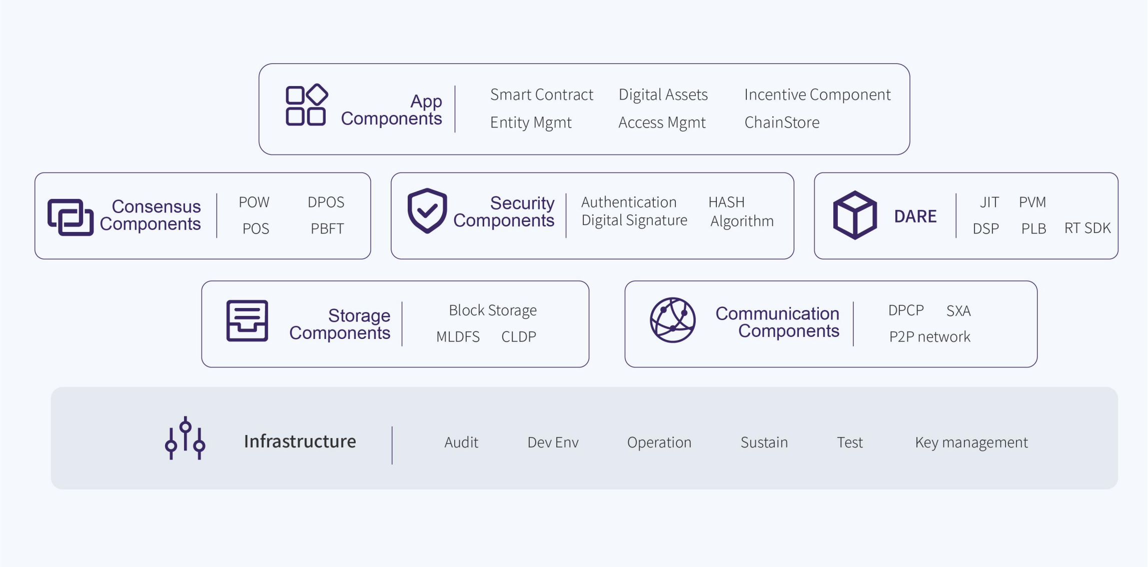


Figure 3.1-2 Penta Network Technical Framework Diagram

3.2. Penta Network – Ledger System Overview

The multi-chain Penta Network platform and Penta Blockchain kernel form the Penta Ledger system divided into the main-chain, side- and application chains, DApp state data, file and key-value stores. Together these support the essential application and interoperability functions for the Penta Network.

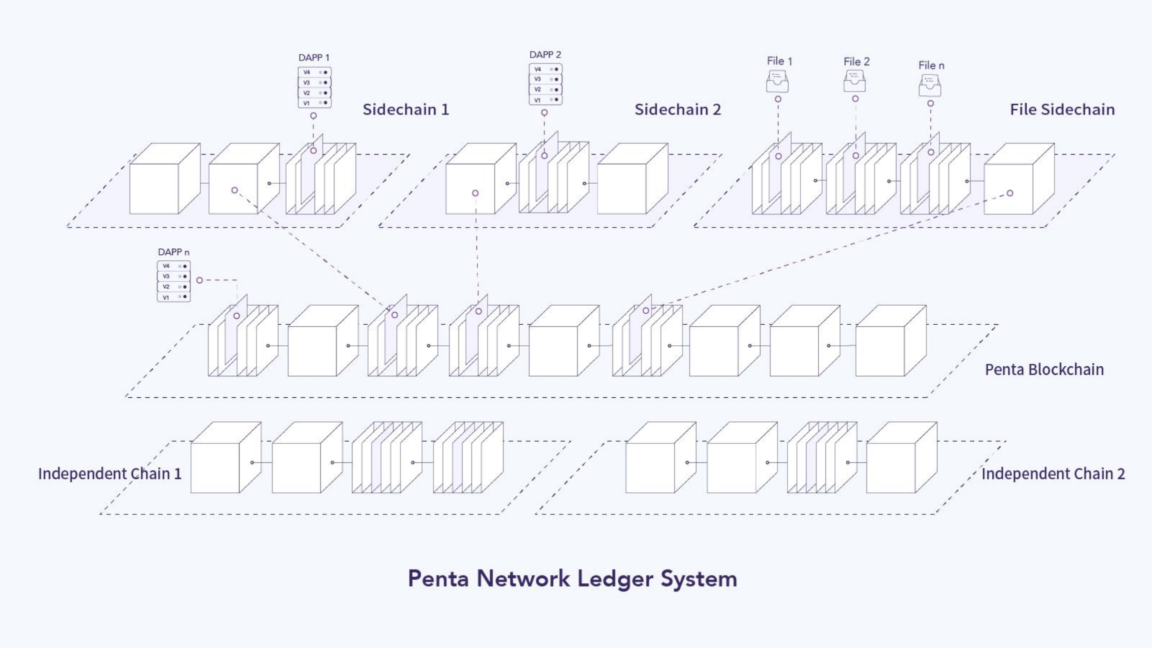


Figure 3.2 Overview of the Penta Network Ledger System

Business use-cases can host DApps directly on the Penta main-chain. Or, if DApps have extended use-case requirements outliers (user role-based authorization, storage and/or network hooks), custom side-chains or independent off-chain cloud computing can be utilized.

3.3. Penta Blockchain – Universal Connector Consensus Mechanisms

Any distributed ledger or blockchain builds a permanent and immutable record of information ‘truths’, like the cryptocurrency token balance for every address in a value transfer exchange. Key and critical to fault-tolerant operations in a distributed environment is the mechanism by which the network collectively agrees on the contents of the blockchain (the ledger).

3.3.1. Dynamic Stake Consensus (DSC) Algorithm

Blockchain design involves tradeoffs between interrelated questions of robustness, trust, and performance. These three issues can be visualized respectfully as a triangle connecting the blockchain properties of: ‘decentralization’, ‘security’ and ‘scale’.

More formally, a distributed ledger, or blockchain ‘system’ is any set of components following precise operating ‘rules’ to provide services to the users of the system. These services shape its ‘intended behavior’, and can be characterized in terms of a decentralization, consensus and scale ‘triangle’.

Before the Penta Network the available blockchain systems could deliver two, but not all three properties simultaneously. The Penta Blockchain deploys a breakthrough ‘dynamic stake consensus’ (DSC) algorithm developed specifically to get around the limitations suggested by the decentralization, consensus and scale triangle. Its intended behavior: for reasonable governance structure, self-sustainability, and node sharding delivers, concurrently, the robustness, security, and high performance of the Penta Network.

To further support real-world business applications, besides DSC the Penta Network will provision a wide range of consensus mechanisms as plug-in components. A side- or independent chain can adopt and make use of these for greater flexibility in validating DApp transactions to become part of their respective chain.

The end result is that developers can ‘dial-in’ where their application will sit in the space of decentralization, consensus, and scale.

3.3.1.1. Penta Blockchain DSC

In terms of consensus algorithms a ‘fork’ happens when a blockchain diverges into two potential paths forward. A fork can be either with regard to a network's transaction history or a new rule in deciding the validity of a transaction, and the blockchain needs a process to choose one ‘branch’ over another.

DSC is a consensus mechanism designed to avoid forks. Instead of optimizing solely for scale, and centralizing on an authoritative ‘super node’, Dynamic Stake Consensus takes a more balanced approach. With DSC, while taking scalability requirements into consideration, participating nodes have equal opportunity to partake in the consensus process.

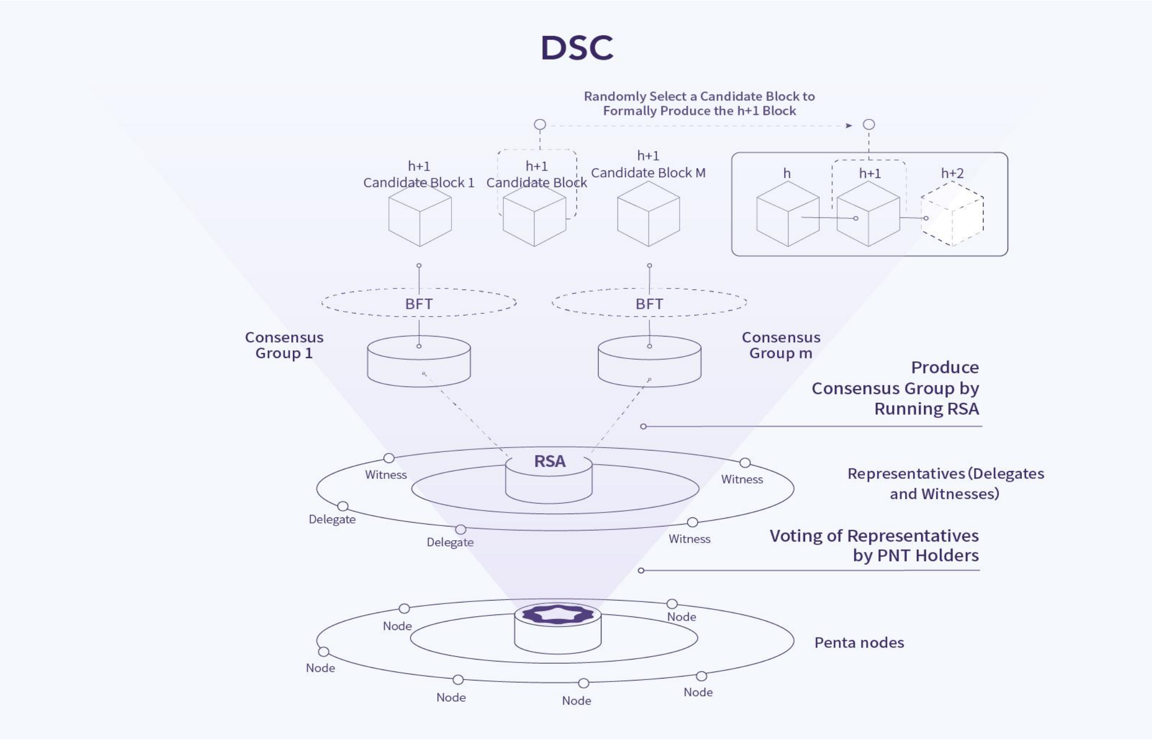

DSC
Randomly Select a Candidate Block to Formally Produce the h+1 Block
h+1 Candidate Block 1
h+1 Candidate Block
h+1 Candidate Block M
h
h+1
h+2
BFT
BFT
Consensus Group 1
Consensus Group m
Produce Consensus Group by Running RSA
RSA
Witness
Witness
Delegate
Delegate
Witness
Representatives (Delegates and Witnesses)
Voting of Representatives by PNT Holders
Node
Node
Node
Node
Node
Node
Penta nodes

Figure 3.3.1.1 The DSC Consensus Mechanism Diagram

Broadly, reaching consensus proceeds through a number of discrete steps:

1. A pool of active ‘delegates’ and moderating ‘witnesses’ are designated among the available network nodes. Whether a functioning node becomes a delegate or witness depends on the amount of Penta Network Tokens (PNT) they hold and/or ‘stake’ (pledge): delegates are required a larger number of pledged tokens, while witnesses less.

2. By mixing together delegates and witnesses employing a ‘random sorting algorithm’ (RSA) ‘consensus committees’ are formed. The number of committees is dynamic and adjusted depending on current conditions of the entire network. For each, the proportion of delegates to witness will be no less than one-third. Then, committees run a Byzantine fault-tolerant (BFT) consensus engine to elect a ‘proposer’ from among their delegates. The proposer will recommend a new block; with all the other members of the committee voting to validate it. Upon super-majority approval, a candidate block will be generated for insertion into the chain.

3. From the pool of candidate blocks, a single one is picked by RSA, and added to the blockchain.

4. If consensus is not reached within a specified timeout period, a ‘RESET’ mechanism is triggered and all delegates will run BFT to produce a ‘RESET’ block that reinitializes the DSC process for continued operations of the Penta Network.

The Random Sorting Algorithm (RSA) is designed for the consensus process to be secure and fair; and that consensus can be reached in a short timeframes, with small computational loads. Compared to the algorithms relying on many centralized ‘bookkeeping’ nodes, DSC is more resistant against Sybil attacks.

3.3.1.2. **DApp Consensus Mechanisms**

The DApp consensus will be determined by developers and it will be register in the metadata descriptions of the DApp. The consensus algorithm can be any consensus that the DApp framework provide, such as DSC, POS, dPOS, PBFT, POA, Notary and so on. Furthermore, the businesses have the possibility to create and use their own consensus mechanism to satisfy their 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 consensus results and register such results in a block.

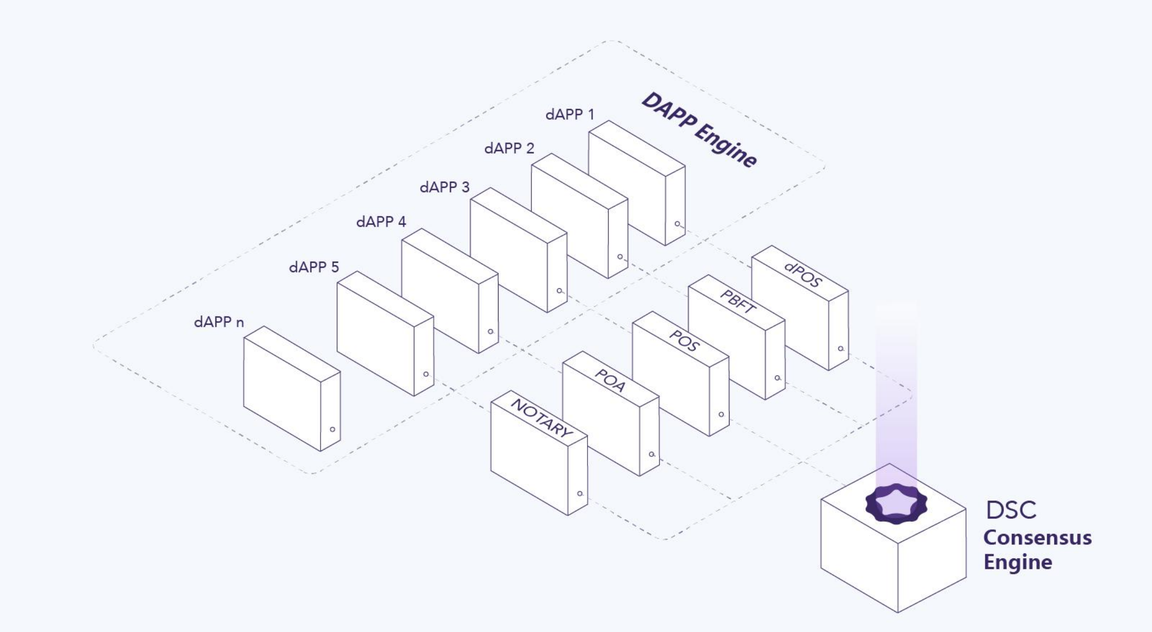


Figure 3.3.1.2 DApp and Consensus Engines

3.3.2. **Governance Structure**

The Penta Blockchain uses a role-based approach for DSC, defined as follows:

1. Delegate - nodes voluntarily apply to be designated a delegate, with other nodes voting to accept them as such. To become a delegate, any node is required to receive a specified number of votes while pledging a stipulated amount of PNT. Delegates have equal opportunity to participate in the consensus process.

2. Witness - nodes may voluntarily apply to be designated a witness, with other nodes voting on whether to accept them as such. Compared with delegates, witness nodes are required a smaller number of votes and smaller pledged amount of PNT.
3. Proposer- For the BFT process, a proposer-elect from the voting delegates is responsible for generating a ‘candidate’ block for eventual insertion into the blockchain.

The number of delegates for a consensus committee dynamically changes, with the initial number and the minimum amount of pledged PNT required depending on the number of nodes participating in the process and overall amount of held PNT. Adjustments are made during subsequent operations based on the total numbers of delegates and witnesses, with no cap on the number of witnesses.

The following diagrams the details participation in the consensus process:

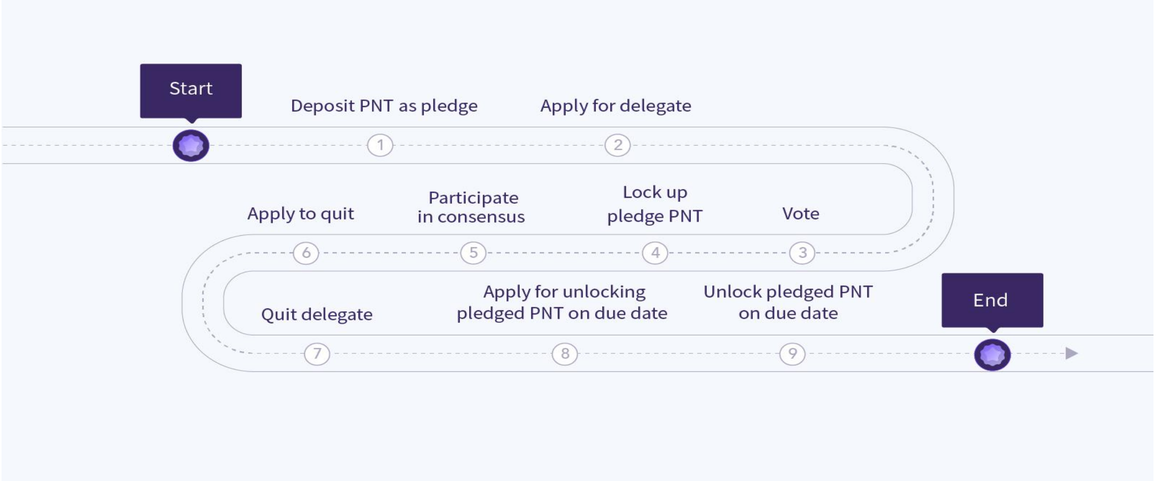


Figure 3.3.2 Participation and Quit Process for Bookkeeping

A consensus committee or ‘group’ will be formed by randomly selecting delegates and witnesses with RSA. Each group will have n delegate and witness where the number of delegates, n1, is bounded as:

$$\frac{n}{3} \leq n \leq \frac{2n}{3}$$

while the number of witnesses, n2 is $n2 = \ n - n1$

Consensus participating nodes must ‘stake’ (make available as a ‘bond’, or ‘pledge’) a specified amount of PNT. In the event of any malicious attempt to sabotage the network, staked tokens are forfeited as penalty. If a proposer node fraudulently attempts insertion of multiple blocks during the BFT process, other nodes may signal the deception and that node will be subject to penalties in the amount of multiples of the offered participation incentives.

Nodes exiting from the consensus process have their PNT stake released and returned within seven days.

Penta Blockchain will adopt a super-majority voting mechanism for any changes to the protocol, including: adjustment of parameters in relation to the cap on delegates, cap on the number of nodes in a consensus group, cap on transaction fees, and the minimum amount of staked PNT. All delegates are required to vote on protocol changes and the result will be determined by running BFT. Only with a super-majority of at least two-thirds, plus one, of the delegates will a new protocol be adopted. In this way the probability of forks are minimized or zeroed.

3.3.3. **Incentive Mechanism**

Upon reaching committee consensus, and production of a candidate block, every member of the committee producing a candidate will be rewarded PNT as incentive for participation. In this way, as part of sustainable operation of the overall Penta Blockchain, nodes are rewarded to participate in the consensus process. PNT incentives originate from two sources: a 50% reserve from the total token fund, and from an individual transaction fee.

3.3.4. **Sharding**

In a blockchain network, transactions are stored in an immutable data structure consisting of a list of blocks where each contains a hash ‘signature’ of the previous block data. Given the time required to produce a block and the intrinsic messaging speed of a peer-to-peer network, block size is usually limited to a smallish fixed value, introducing constraints on the throughput of the entire network. Typically the number of transactions grows non-linearly with network size, and scalability becomes bottlenecked, preventing blockchain technology from realistic, large-scale application use.

Consequently, capability to process transaction data asynchronously, in parallel has become a sought-for solution path. Among other possibilities, like ‘state channels’ or side-chains, developers are being drawn to ‘sharding’ as a viable option to overcome scalability bottlenecks.

Sharding is usually described in one of a couple ways: advancements in parallel, asynchronously processing of transactions, and enhancements to storage capacities.

In addition to designing the Dynamic Stake Consensus algorithm designed for scalability, the Penta Blockchain will use parallel transaction processing schemes, or ‘sharding’ to maximize throughput and prevent future scalability issues due to increasing transaction volume. For which, the Penta Network will implement the Penta Sharding Graph (PSG) on the Penta, with consistency of cross-shard transactions guaranteed by ‘Sync-Point’ technology.

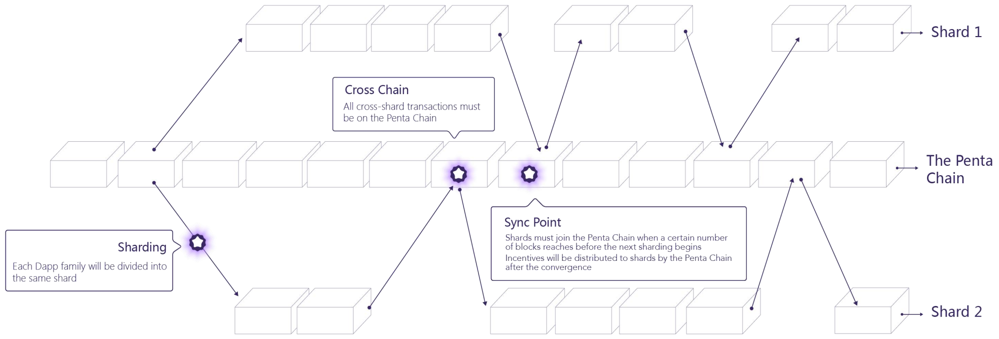

Shard 1
Cross Chain
All cross-shard transactions must be on the Penta Chain
The Penta Chain
Sharding
Each Dapp family will be divided into the same shard
Sync Point
Shards must join the Penta Chain when a certain number of blocks reaches before the next sharding begins
Incentives will be distributed to shards by the Penta Chain after the convergence
Shard 2

Figure 3.3.4 Penta Chain PSG Diagram

3.4. Penta DLOS

Distributed Ledger OS (DLOS) is the infrastructure underpinning the Penta Network for a scalable, micro-service based, distributed framework. Compute nodes connect to the multi-chain network Penta Network through DLOS. The Penta Blockchain sits at the center of the network with direct links to multiple side- and independent chains. To support the various data/network structures, ledgers and algorithms, DLOS separates out computation, storage, network, consensus and other resources, with an abstracted interface layer for each. DApps or other applications concentrate on their specific use-case requirements, interacting with the network through the micro-service interfaces.

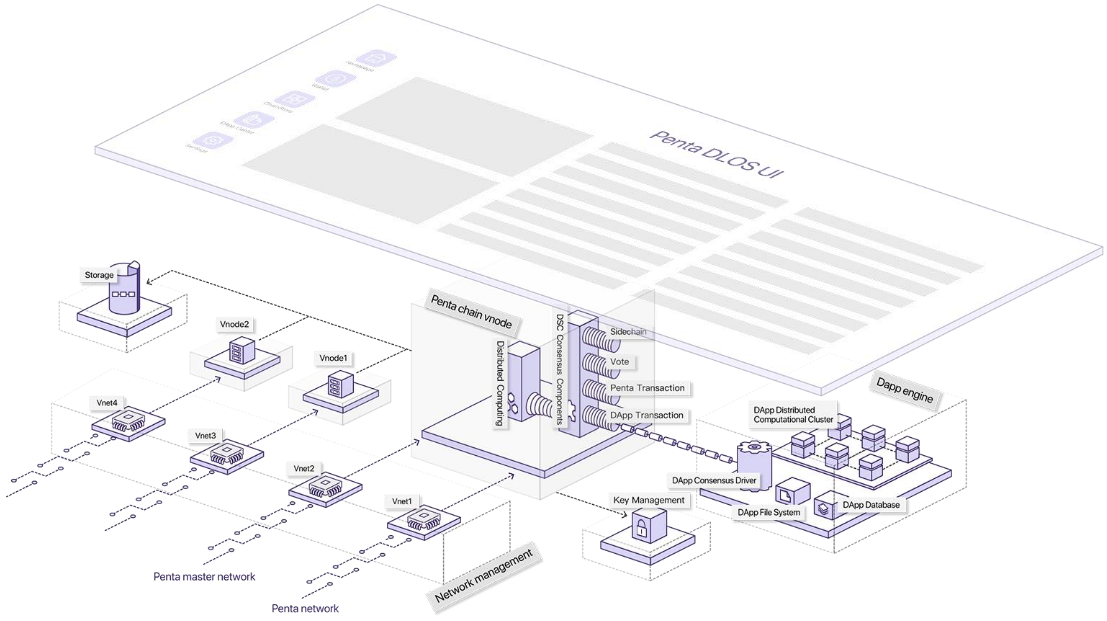


Figure 3.4 DLOS Logic and Data Structure(s) Diagram

Side-chains, Directed Acyclic Graphs (DAG) and other types of distributed ledgers will all co-exist in the Penta Network supporting the various kinds of (blockchain) applications deployed.

3.4.1. **Distributed Computational Framework**

A distributed computational framework (‘Constellation‘) is the core of DLOS, handling all service and messaging events of all nodes for a unified, integrated system. For enterprise applications, DLOS components can be run as part of a ‘cluster’ environment, providing both scalability and a high-availability environment for them.

3.4.2. **Storage**

DLOS will abstract the data storage layer and realize a common ledger storage component for use within any block data structure setting. The common ledger storage component does not preclude utilizing a different one for special ‘edge cases’.

Given the different storage requirements for fork-vulnerable chain and fork-proof chains, a set of storage engines will be designed around multiple data structure types to accommodate. For example, a Merkle Patricia Tree (MPT) data storage engine handling a fork-vulnerable chain while a different data engine deployed for fork-proof ones.

3.4.3. **Penta Network Management**

The Penta Network is a multi-chain platform where each node is able to concurrently ‘message’ (transfer data) to several chains. The network component of DLOS will manage several ‘virtual’ peer-to-peer (P2P) networks at a low-level layer. To meet specific DApp design and business requirements virtual networks could be reallocated to specific sub-networks for better performance and security. A first step of DLOS is to enable distributed hash tables (DHT) starting with Kademlia and the original four DHT protocols: CAN, Tapestry, Chord and Pastry for P2P network communication. DApp developers can supply their own P2P components to the network as well.

3.4.4. **DLOS UI**

The UI/UX view layer, or Penta DLOS UI, provides an intuitive, easy to use and consistent user experience for developers to develop applications with. It also offers an integrated DApp UI development framework and web components.
The MVVM model based DApp UI encapsulates a collection of standardized UI components and APIs for DApp development and for DLOS service layer interaction. For example, the DApp UI access service layer API, handles user account access and the security of client nodes.

3.4.5. **Merkle Patricia Trie (MPT)**

Merkle Patricia Tries are widely used for transaction validation, data storage and other process in the Penta Network.

Merkle 'Tries', pronounced and also known as 'trees', are fundamental to blockchain. They make possible blockchain nodes that run on desktop, laptop and small devices (mobile phones) too. Using a Merkle trie provides a mechanism for efficient verification, or 'Merkle proof' of the hashed data stored on a blockchain. They are well suited for authenticating information in 'list' format and are commonly implemented as Merkle binary trees.

Patricia (Practical Algorithm To Retrieve Information Coded In Alphanumeric) Trees are better in situations involving dynamic data. In other words, storing of application state data. Blockchain address account balances are a good example for use of a Patricia Tree.

The Merkle Patricia Tree (MPT) is an improvement on both, combining the technical strengths of the Merkle and Patricia Tries. 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, the same key will map to the same result with the same root hash;
2. Efficiency - When data is modified, a new root will be computed immediately without no need to re-compute of the entire tree, making it highly efficient for data insertion, search and deletion;

Security – A limited tree depth resists denial of service (DOS) attacks initiated by a malicious agent seeking to compromise a network through launch of an overwhelming number of transactions to increase the depth of a tree to an unmanageable size.

3.4.6. **Enterprise Application Components**

A participant in the Penta Network can be an individual or enterprise. However, the application requirements of individuals and those for enterprises are usually quite different. Individual Penta participants generally focus more on user-facing DApp features such as the application interface, while enterprises tend to have strict system requirements to be met. This is especially true for the stringent prerequisites for DApps servicing financial institutions.

The Enterprise version of DLOS will comply with COBIT (Control Objectives for Information and related Technology) standards, as a response to making it easier for enterprises to meet their IT auditing requirements. DLOS will also organize a security center with 'key' administrator, member administrator, authorization administrator, operation and maintenance, auditing assistance and so on towards making it as easy and accessible as possible for enterprises to develop blockchain applications on the Penta Network.

3.5. DApp Platform

A distributed blockchain application (DApp) is a key element of the application services in the Penta Network. Technically it includes code for user-facing view layers, business logic, data, network and messaging layers.

The data layer is comprised of the state/status data generated by a DApp and stored in the Penta ledger, as well as the information stored by each Penta node in file or database format. Penta clients normally only synchronize to block data, which contains a DApp version number and ‘signature’ fingerprint of status data rather than the DApp status data itself. Only when a user has downloaded a DApp from the Penta ChainStore will client status be synchronized to the local device from other nodes.

The DApp Business Logic layer climbs for a simple Smart Contract to complete complex system modules. Interfaces to the business function layer are of three classes: control (initialization, metadata, etc.), query search, and data updating.

Closest to end-users the DApp View Layer runs locally on the Penta as the UI. Completely compatible with the Penta View Layer development specifications and framework requirements it utilizes a MVVM pattern to improve code maintainability by separating the UI layout and front-end logic.

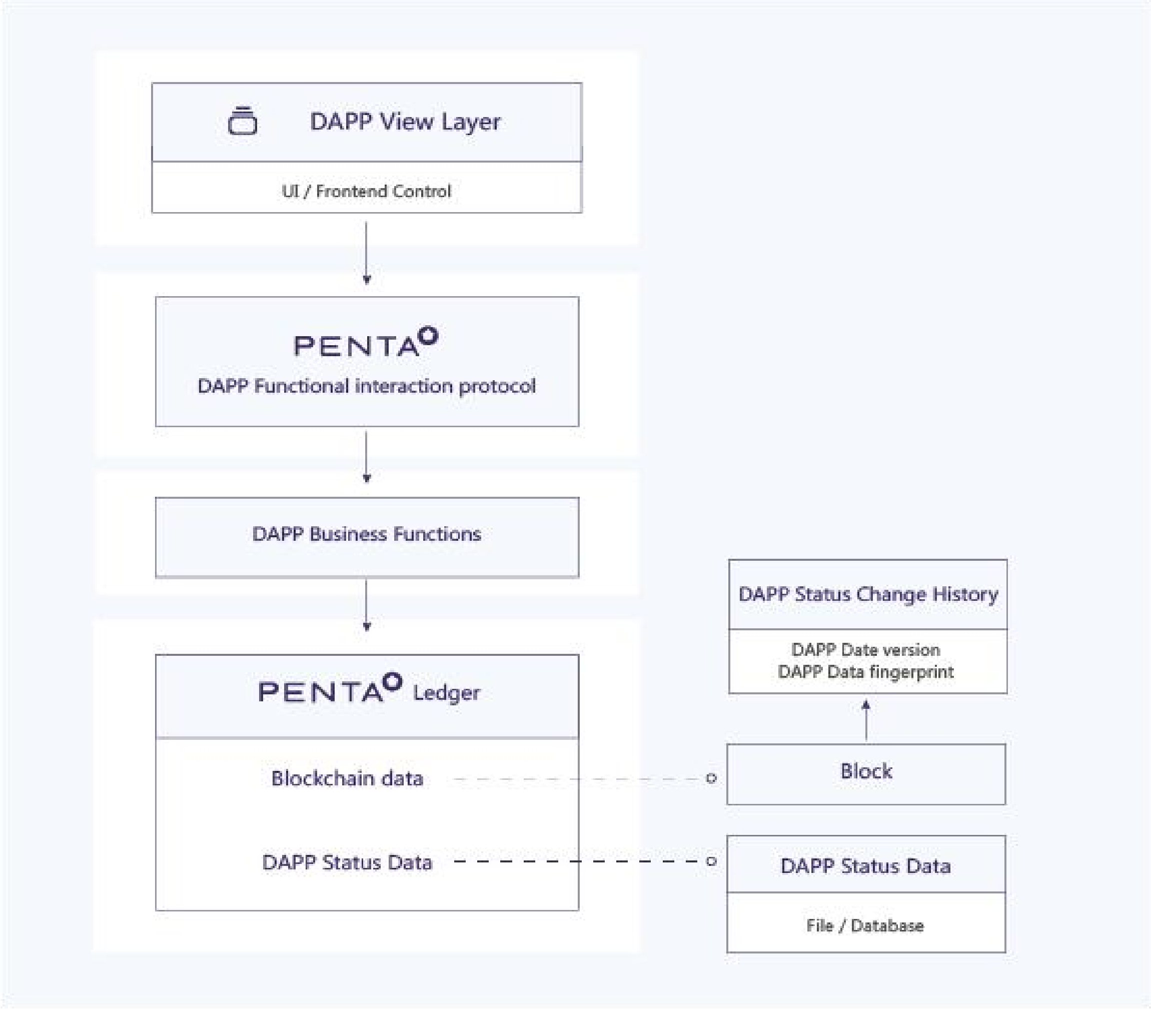


Figure 3.5 DApp Logical Structure and Framework Diagram

3.5.1 **DApp Operating Environment**

The Penta Dock World (PDW) provides a complete, independent virtual operating space for smart contracts and blockchain applications. The PDW will provide necessary resources to run a blockchain application including independent computational resources, database, and file storage. Blockchain application authorization to access resources is restricted to its individual PDW only. No application is allowed to cross PDW boundaries for other application resources.

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. State 'signature' fingerprints will be generated at the end of an operation and recorded in a block.

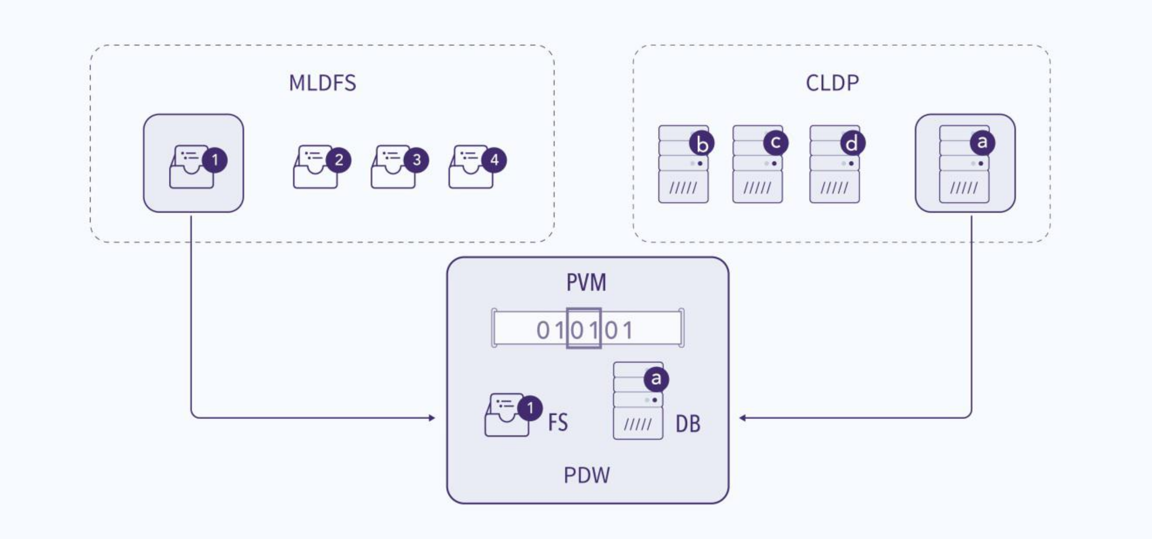


Figure 3.5.1 PDW Diagram

3.5.2. Penta DApp Database

The Container-level database protocol (CLDP) is a distributed database storage engine specially developed for the Penta Network. It is a set-oriented storage engine, a hybrid sitting between relational and noSQL databases performing with the strengths of both. It provides a SQL engine to simplify complicated blockchain application development. It also provides a virtualization mechanism for efficient synchronization and separation of smart contract data, transaction log caches. With the objective to supply a high performance, easy to integrate and accessible data storage, the CLDP responds well to the needs of individuals for lightweight application development, and satisfies strict enterprise performance requirements.

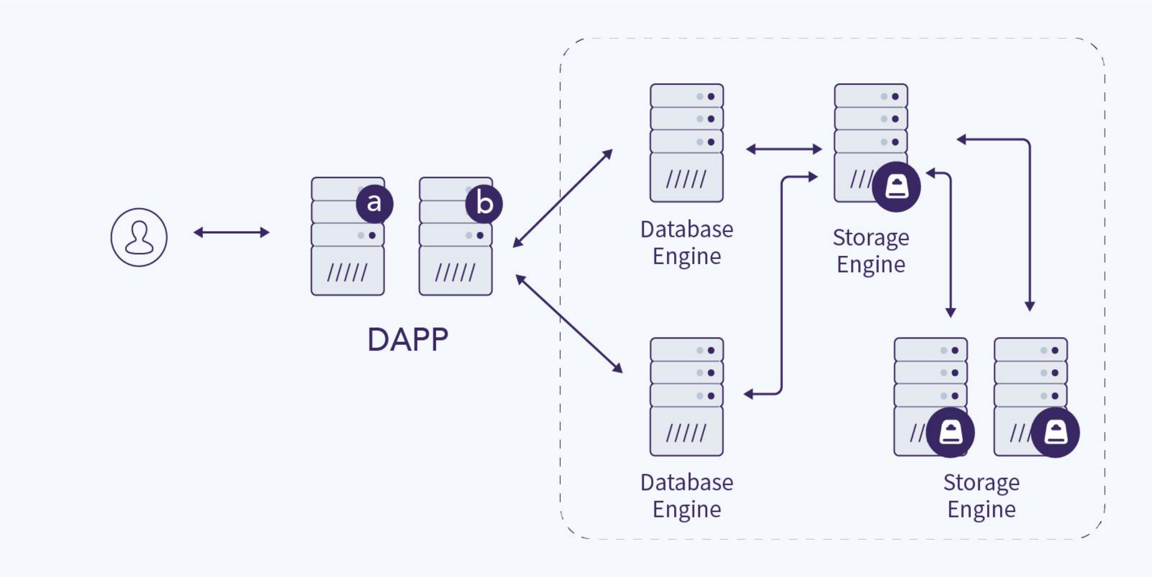


Figure 3.5.2 CLDP Protocol Diagram

3.5.3. DApp Multi-Layer Distributed File System

The Multi-Layer Distributed File System (MLDFS) is a distributed file system storage protocol. It consists of namespaces and data spaces. Namespaces manage file names, with file data stored separately in the data spaces. Data blocks can be stored by MLDFS or a distributed storage file system.

File version management is one function of MLDFS. For each consensus transaction, MLDFS creates a unique version number, in part containing a hashed value of transaction data (used to verify the data). Change history data will be recorded with each version, and the complete version number will be registered in the block to be used by nodes for file synchronization and to verify the integrity of the data. Nodes may incrementally update, synchronizing only a previous version 'delta' to lower network traffic and improving the entire blockchain network performance.

DARE is the Distributed Computing Engine of Penta Network and has a built-in parallel virtual machine (PVM), load balancing, QoS, and runtime SDK. PVM is a universal virtual machine similar to a Java Virtual Machine (JVM) to compile Smart Contracts.

DARE is responsible for the initialization and mounting of virtual machine environment, MLDFS and CLDP, and the operation of the distributed computing coordinator when running a blockchain application.

MLDFS supports distributed transaction management. All nodes participating in the consensus process validate results of a blockchain application, and sign the hashed data. A blockchain application can locally modify files, but relevant data will not be written to the file system until a consensus transaction commits and then a new file version is generated.

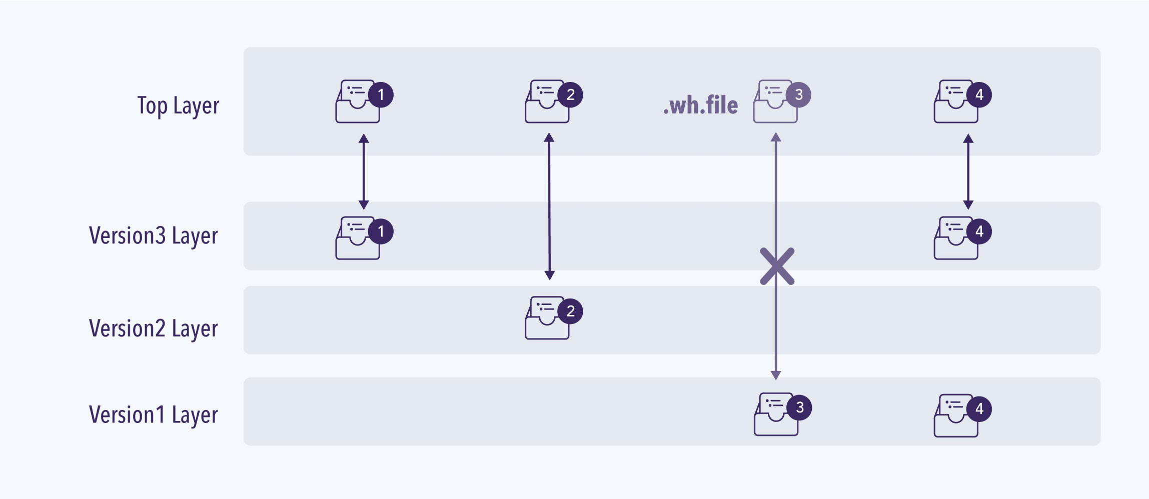


Figure 3.5.3 Multi-Layer Distributed File System

3.5.4. The DApp Store – Penta ChainStore

ChainStore is the digital distribution platform for the Penta Network, where side- and blockchain services, smart contracts and DApps are registered. Users download and install DApps from ChainStore with the Penta Network Client. The client automatically downloads available DApp information registered in the ChainStore to update its view layer with. The ChainStore automatically synchronizes DApp state data with a user's local device(s).

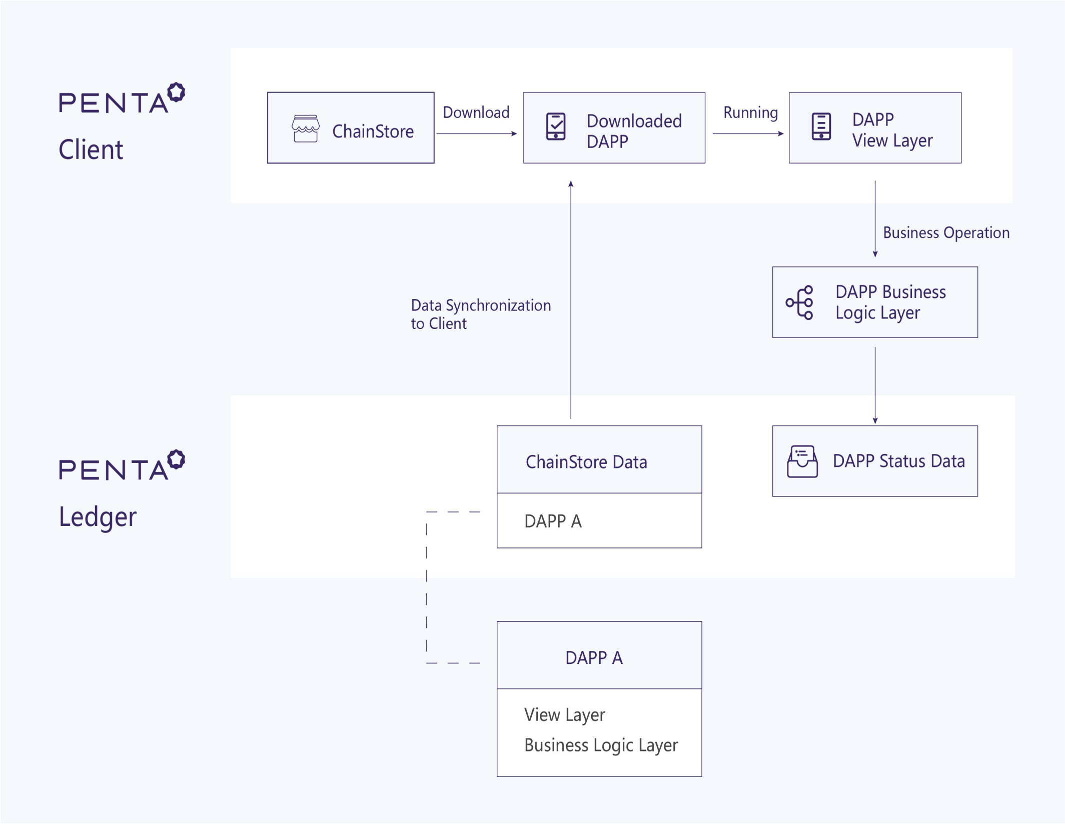


Figure 3.5.4 ChainStore Diagram

3.5.5. **DApp IDE**

Testing and debugging DApps is more complicated than for traditional systems. In anticipation, the Penta Network will provide a development environment that integrates coding, analysis, compilation, testing, release and other tools to facilitate end-to-end progress.

3.5.6. **DApp SDK**

The Penta DApp running environment provides different SDKs to simplify DApp development tasks. The DApp SDKs minimize ‘reinventing’ basic components with APIs including ones for data storage, signature verification, account management, identity, data connector, and digital assets.

3.6. Interoperability Layer

The Penta team presupposes blockchain distributed ledgers are not the best solution for every real-world use case. Operating under trusted central authorities was the norm until recently, and may be a preferred approach over blockchain, which is designed for 'trustless', working environments. Therefore, the Penta team is planning for a future where centralized networks, consortium chains and public chains co-operate to provide user services, and aims to build an interoperability infrastructure based on the robust, efficient, and secure Penta Blockchain.

The Interoperability Layer 'connector' is dedicated to the transfer of value between blockchains, between blockchains and centralized networks, or on-chain to off-chain. It is structured in four sub-layers: communication links, credibility, value, and application layers:

1. The low-level Communication Link Layer enables information exchanges with other blockchain or centralized networks, resolving communication transmission and data format issues.
2. The Credibility Layer provides a mechanism to build trust among entities and eliminates the needs for a central authority to hold and transfer measures of trustworthiness among different. Credibility data can take many forms including identity validation, guarantees, insurance records, timestamps, public comments and credit ratings.
3. The Value Layer has safekeeping responsibilities during the transfer of value on- and off-chain, potentially including escrow of a single entity or a consortium, contract accounting, bookkeeper tasks, and notary public.
4. The top-level Application Layer coordinates value transfer exchanges and serves business use-cases by selection of proper protocol combinations according to their specific requirements.

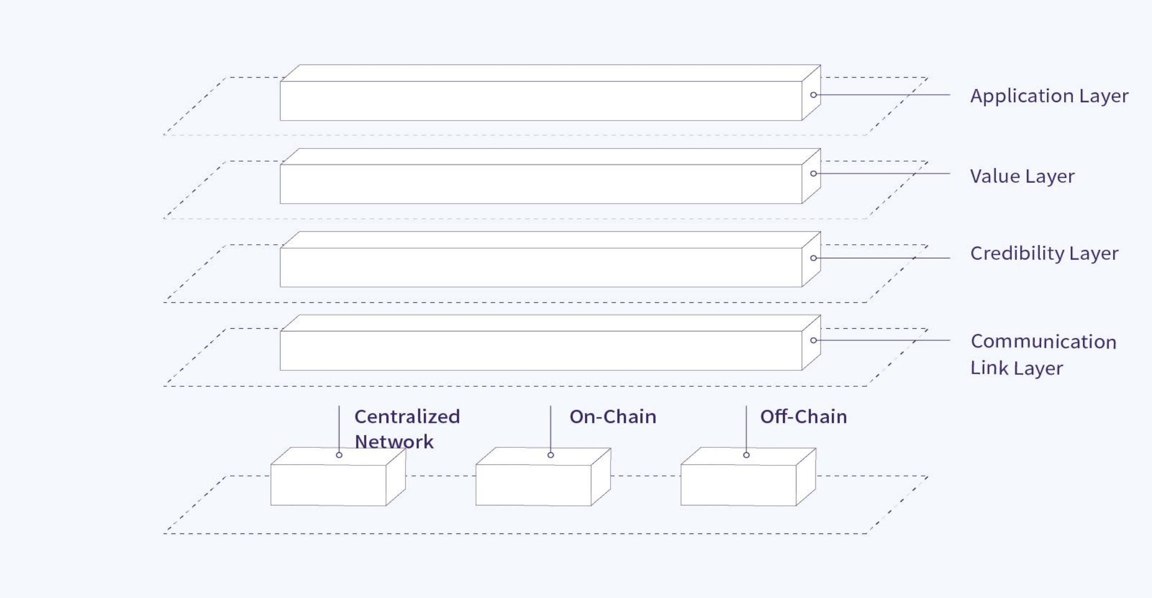


Figure 3.6-1 Structure of the Interoperability Layer

The Interoperability Layer protocols supports the Soft eXchange Adaptor for providing applications greater transaction control. The DApp SDK provides standard API calls for external major blockchain including BTC, ETH, Ripple, Stellar, NEO, Dash, and Hyperledger. These APIs enable developers to transact with other blockchains and traditional centralized systems. A functional component delivers services between different chains or between a blockchain and a centralized systems, including: unified identify validation, chain service registration, chain service discovery and chain service quality.

To provide a consistent user experience the Penta Network will provide an integrated client that is compatible with existing major clients of BTC, ETH, Ripple, Stellar, NEO, Dash, Hyperledger and more. The integrated Penta client has similar APIs so that other blockchains can easily interact with any blockchain on or off the Penta Network.

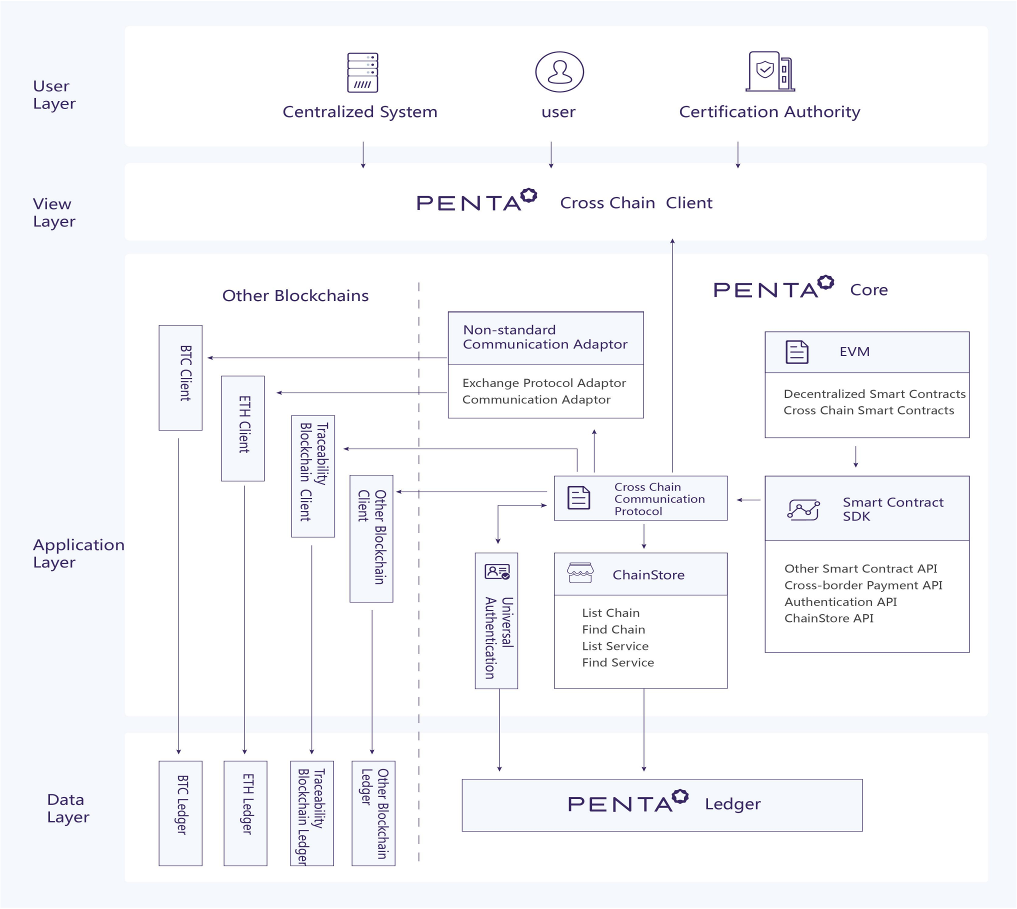


Figure 3.6-2 Cross-Blockchain Communication Structure

3.6.1 Soft eXchange Adaptor

Blockchain as a decentralized, distributed system technology is fast evolving, as complementary to, but never completely replacing the traditional centralized systems model that will continue to operate into the future. Coexistence between them will be necessary and requires tools for interaction and co-operation. The Penta Network presents the Soft eXchange Adaptor (SXA) as such, to effectively and efficiently co-exist with centralized systems. The SXA is divided into three layers: communications, protocol, and business layers, all of which act together to ensure a secure and trusted link to traditional centralized systems.

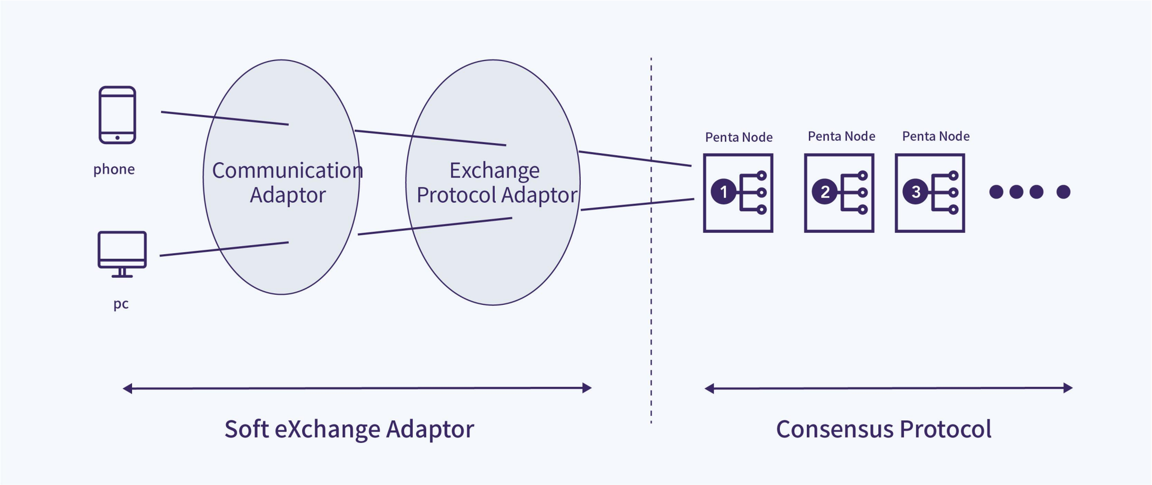


Figure 3.6.1 Soft eXchange Adaptor

3.6.2 Distributed Private Communication Protocol

By default, a blockchain utilizes a public peer-to-peer (P2P) network as a communications backbone, which exposes and broadcasts data between peers on it. Information published on a blockchain network is nominally readable by all peers. But, in practice transaction owners may be reluctant to disclose data to outside parties, which is the rationale for the Penta Communications Network (PCN). It supplies special communication network (DPCP) channels for Penta Network nodes. Node pairs seeking to transmit private information can initialize encrypted communication channels with the DPCP, and only these two parties may access the transmitted data. The Penta communication network also provides routing, channel establishment, traffic control, exchanges of certificate, key and encrypted data, channel destruction and other data communication tools.

Figure 3.6.2 Distributed Private Communication Protocol

3.7. Technical Roadmap

The mission of the Penta Network is to become the universal blockchain connector. Strategically, the Penta Network plans to first release the Penta Main Chain, and then will deploy the: DLOS infrastructure, a DApp development platform to support decentralized applications, and the Interoperability Layer tools. The Penta Network will incorporate a continuous integration and deployment methodology to improve its technologies in a concerted effort for advancement of the Penta Network as a whole.

The Penta Developer team is responsible for the Penta Blockchain, including DSC algorithm, voting center, Penta PC wallet and blockchain explorer, and will support PNT transactions with its first release. Core components for the first version of DLOS will align with the technical requirements of the Penta Blockchain enabling proprietary blockchain development based on DLOS and multiple blockchain interaction.

The Penta DApp platform is a key module to provide distributed application solutions for complex business use-cases. As with the Penta Main Chain the DApp platform will gradually roll-out a series of technical upgrades such as DApp VM environment, DApp dedicated database, DApp file system, DApp UI framework, and support of DApp development and maintenance.

The Interoperability Layer has a central role in the Penta Network that enables transfer of values between block chains, between a blockchain and a centralized network, or from on-chain to off-chain. It is hoped that the broader Penta community will collaborate on the enhancement and application of interoperability technologies so as to realize the Penta Network mission 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 a variety of underlying encryption algorithms such as ECC. It looks to introducing encryption algorithms (such as Lattice-based cryptography) that are able to resist the expected breaking of current encryption algorithms by emergent quantum computing projects.

The ECC encryption algorithm utilized is a mainstream (public key) asymmetric encryption algorithm. These types of algorithms are always based on 'extremely difficult to solve' (trapdoor) 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 back into p and q. This is one instance of a 'trapdoor function' that is easy to compute in one direction, but extremely hard to perform the inverse operation on.

The ECC algorithm is based on the following:
Consider the equation: $K = kG$ [where K, G are points on Ep (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 named the 'public key'.

To describe a process of using elliptic curve functions for encrypted communications, between two parties, 'Alice' and 'Bob' (A and B):

1. A selects an elliptic curve Ep (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 Ep (a, b) and point K, G to user B.
4. After B receives the message, it encodes the plaintext to be transmitted to Ep (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 C1 = M + rK; C2 = rG.

6. B passes C1, C2 to user A

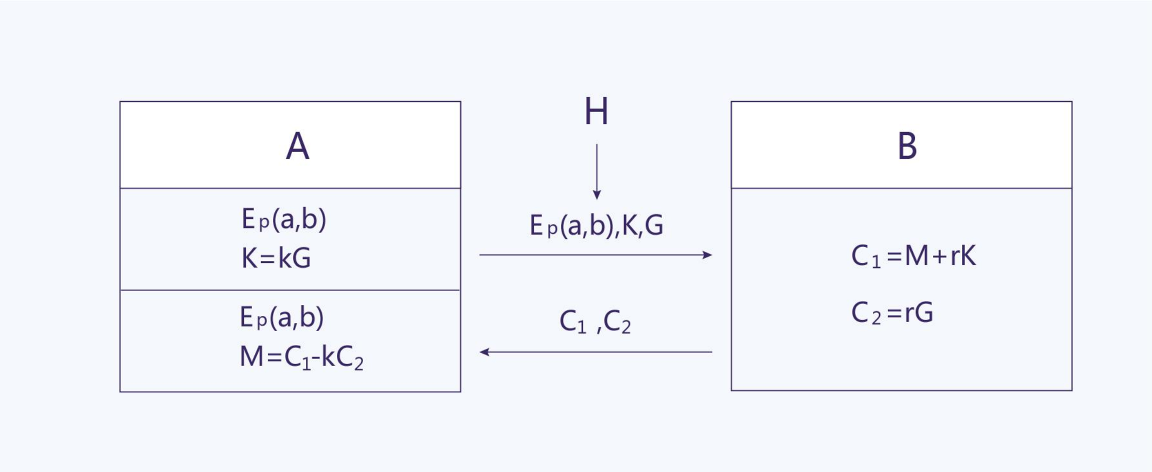
7. A receives the information, calculates C1-kC2, and the result is point M. The plaintext can be obtained by decoding the point M since C1-kC2 = M + rK-k (rG) = M + rK-r (kG) = M.

In this encrypted communication, ‘attackers’ can only see Ep (a, b), K, G, C1, C2 and would find it difficult to get k by K, G or obtain r by C2, G. Therefore, it is impossible for H to get to the plaintext message sent between A and B.

In cryptography, describing an elliptic curve on Fp, uses six parameters:

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 impacts 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. $4a3+27b2 \neq 0 \pmod{p}$
5. n is a prime number
6. $h \leq 4$

To minimize and limit possible abuse of Penta Network resources in the form of excessive ‘spam’ transactions generations and to enhance platform security, the Penta Network will ask for an operations and storage cost fee payment from transaction and execution of Smart Contracts. Extension of these fees to include security and encryption services will be decided via consultation with the wider community of PNT holders.

4. Applications of the Penta Network

In the past two years, the Penta team has been collaborating with partners in numerous industries to design and implement blockchain solutions. In the future, Penta is committed to penetrating more industries by developing a robust blockchain infrastructure that will enable and empower business solutions that improve efficiencies and significant cost savings.

The Penta Network encompasses an interconnected multi-chain ecosystem that offers diverse solutions to projects, businesses, communities, and individuals. Those solutions include private, permission, public, and hybrid blockchain technologies, which will be powered by and connected through the Penta Network's underlying DLOS. Only by offering specific and customizable solutions can we meet the complex and nuanced needs of the real world economy. Additionally, the Penta Network is designed to integrate and interact with other emerging technologies, such as artificial intelligence, big data, VR/AR, robotics, Internet of Things (IOT), and cloud services. These integrated technologies will be used for applications in healthcare, transportation, Intellectual Property licensing and protection, smart cars and automotive, agriculture, energy, fashion, food, e-commerce, finance, gaming, and other industries.

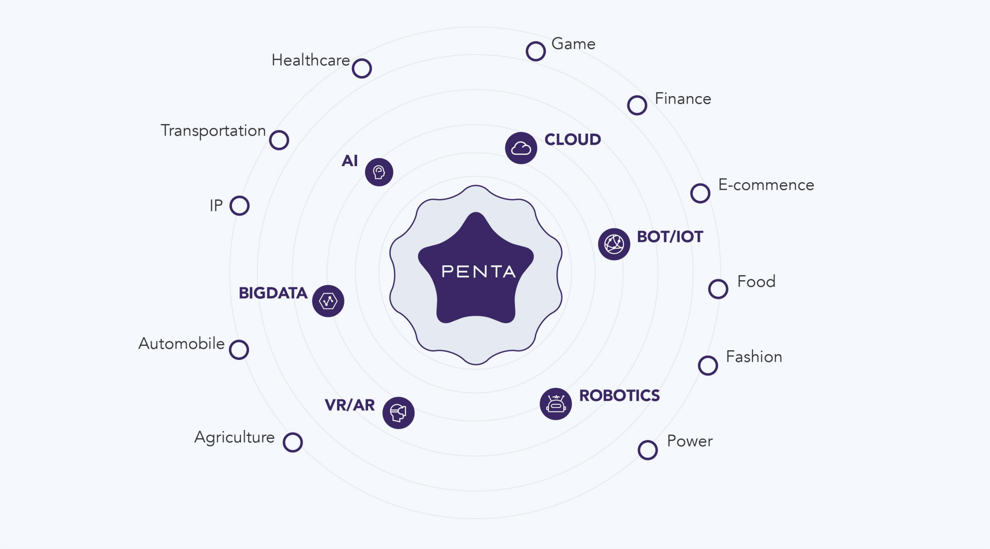


Figure 4 Applications of the Penta Network

4.1. Social Applications

4.1.1 Healthcare

The healthcare industry is undergoing a significant transformation: digitization of patient history, medicine, devices, services, and business models. Among the results of this transformation will be more secure, accurate, and real-time medical data, which will necessitate a more decentralized and less localized healthcare industry. Most countries have promulgated policies that aim to digitize national healthcare systems, which include widespread programs to digitize medical and hospital records, as well as information from other healthcare-related facilities and treatment centers.

Ensuring personal medical data is secure and limiting access to third parties are critical factors driving innovation in the healthcare industry. The healthcare sector has struggled to strike a balance between risks and returns when it comes to the handling of patient information, and many healthcare systems have been slow to digitize patient records. Blockchain technology can provide meaningful solutions to the healthcare sector in the following aspects:

1) Data Security

   Unlike existing security systems, blockchain runs on distributed networks that use encrypted security mechanisms which are highly resilient to intrusion. This offers obvious solutions to the healthcare field, where patient data, medical devices, medicines, and valuable patents all require enhanced digital security. Healthcare providers can leverage blockchain technology to monitor medical devices through IOT technologies, administer medications, and optimize treatment protocols.

2) Exchange of Healthcare Data

   Sharing healthcare data is about more than the exchange of information. It requires mechanisms to ensure trust between parties and healthcare systems that are party to the exchange of such sensitive information, and it requires technological solutions to maintain and continually update the integrity of the data and to secure data custody. The Penta Network provides a suite of blockchain solutions that allow for secure and controlled data exchange between numerous parties. Blockchain can be highly useful in addressing complex workflow systems that require access to sensitive information and ensuring the integrity of the system.

3) Medicine Security

A distributed healthcare system based on blockchain can improve security in pharmaceutical production and distribution by authenticating medicines based on their origin, and by securing supply chain data. Blockchain will also be able to make pharmaceutical pricing more transparent. Pharmaceutical companies are under increasing pressure to justify the value of their drugs. Based on industry estimates, approximately $300 billion of drugs are wasted each year due to failure to achieve desirable results. Meanwhile, countless patients suffer from the side effects of drugs. As a result, the pharmaceutical industry will increasingly move to a patient-centered drug development model, with increased accountability and transparency.

4) Precision Medical Treatment

The healthcare industry is expanding new areas of medical research, including research fields related to immunology, microbiome, genomics, customized nutrition, etc. Precision medical treatment will require integrated technologies, such as IOT and big data, so that treatments can be tailored to individual patient needs. This will radically change the service delivery model of the healthcare sector, and require blockchain technology solutions. The pharmaceutical industry will also play an important role in precision medicine, favoring individually tailored dosages and drug regimens based on patient data. Once again, blockchain can help mitigate costs, increase transparency and accountability, and optimize data collection and exchange.

5) Medical Research

Medical research suffers from tremendous inefficiencies caused by competing interests, patent disputes, and pride of authorship. Often times, research institutions like hospitals and universities, are encouraged to jealously guard research and clinical results rather than share them with the medical community, thus protecting the intellectual property and market value that such research may bring with it. Blockchain offers a solution to this problem, where intellectual property can be protected and managed, even while it is shared with the medical community. Greater sharing of research with a more distributed pool of medical and cross-disciplinary talent will likely reduce the timeline for medical research and allow the medical community to respond faster and more efficiently to health crises, like outbreaks of infectious diseases, when they arise.

6) Clinical Trials

Verifying the accuracy of clinical results, complying with legal standards for submissions of clinical research, and proving data custody are all problems to which blockchain offers innovative and valuable solutions.

With its reliable security infrastructure, blockchain technology enables seamless exchanges of health data and enables new potential for medical research and innovation. The Penta Network provides the digital infrastructure required by tomorrow's healthcare industry, a smart-and-secure healthcare system that is credible, traceable, transparent and safe.

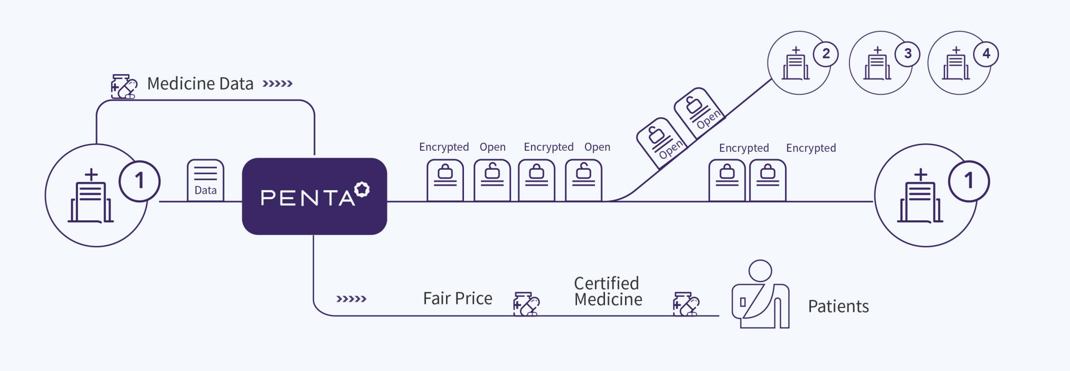


Figure 4.1.1 Penta Network-Based Medicine Traceability Application

4.1.2 Application in the Energy Sector

The growing shortage of conventional energy resources and the environmental pollution generated by fossil fuels are major worldwide problems. At the same time, technologies related to renewable energy (such as wind and solar) are gradually becoming more mature, but have not yet been widely adopted. According to industry statistics, wind accounts for a mere 4% of worldwide power, while solar contributes only 1%. One of the key problems facing mass adoption of renewable energy is lack of infrastructure to distribute power effectively. Compounding this problem are difficulties in power scheduling and transmission controls as a result of centralized power grids (i.e. State Grid, China Southern Power Grid, etc.). Thus, large-scale application of distributed energy faces technical obstacles as well conflicting commercial interests. The answer to these problems is building an infrastructure and a marketplace for distributed energy. This will enable energy to be transferred more efficiently to where it is needed, and will empower energy consumers to also be energy producers.

With the rapid development of Internet communication and processing technologies, the American scholar, Jeremy Rifkin, proposed the concept of "Energy Internet" in his book *Third Industrial Revolution*. The concept quickly gained popularity. In 2016, the State Grid released a "White Paper on Urban Energy Internet Development (2016)," which articulates a vision for an Urban Energy Internet (UEI), an autonomous entity that manages efficient, clean, and intelligent allocation of energy in urban areas.

Building on these ideas, many municipal governments and energy firms are experimenting with distributed miniature power grids. Mini power grids offer a promising alternative to the expensive and time-consuming process of overhauling traditional large-scale power grids. Linking them together technically and creating an energy marketplace on the mini power grids can form a Community Energy Internet (CEI) or UEI that “encourages multiple connection, interaction, access, transaction and response among various energies” within a certain geographic area. Such CEIs and UEIs will also be able to interface with existing power grid systems to form a more efficient energy ecosystem.

This requires development in the field of IOT, and also innovation in energy related information platforms and business models. Establishing a decentralized SPX (Smart Power Exchange) that facilitates autonomous, transparent transaction, and information sharing among electricity providers and consumers provides a win-win reward mechanism. An SPX will yield significant efficiency gains in energy transmission and utilization. It will also enable energy consumers to be producers and participate in the generation, transmission, and exchange of energy resources.

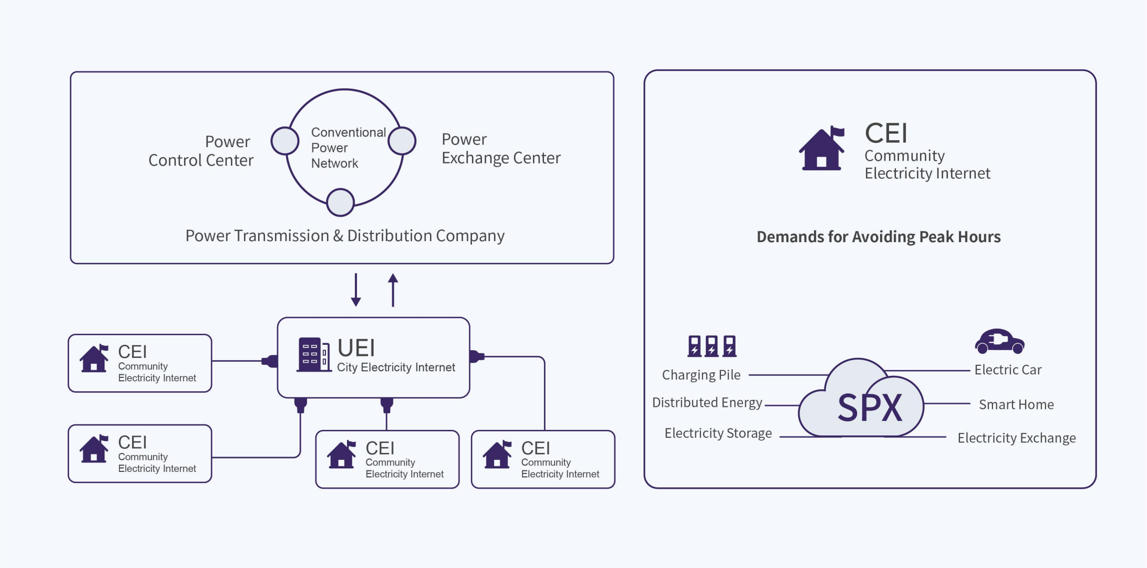

Power Control Center
Conventional Power Network
Power Exchange Center
Power Transmission & Distribution Company
CEI Community Electricity Internet
UEI City Electricity Internet
CEI Community Electricity Internet
CEI Community Electricity Internet
CEI Community Electricity Internet
CEI Community Electricity Internet
Demands for Avoiding Peak Hours
Charging Pile
Distributed Energy
Electricity Storage
SPX
Electric Car
Smart Home
Electricity Exchange

Figure 4.1.2 SPX Empowered CEI

The Penta Network aims to establish a decentralized SPX (Smart Power Exchange), the type of digital infrastructure needed to underpin emerging distributed energy markets. This SPX is essentially an internet and marketplace for energy, which includes a variety of functions such as uploading real-time information on available resources, linking energy production and consumption to a peer-to-peer network, smart matching to deliver resources to a consumer, order execution, smart meter and measurement data transmission, e-wallet, and payment settlement. The future energy industry will be a much more distributed multi-party system, with people and communities involved in more efficient resource allocation.

4.1.3 Internet of Things (“IOT”)

IOT technology, intelligent hardware, and IOT-driven consumer industries will inevitably lead to an era of the Blockchain of Things (“BOT”). The Penta Network has designed its network infrastructure to support BOT. Penta’s blockchain can interact with autonomous IOT and facilitate secure value transfer. In addition to enabling IOT technologies, the Penta Network will integrate artificial intelligence and robotics technologies, which will be important technological tools in optimizing IOT-related industries.

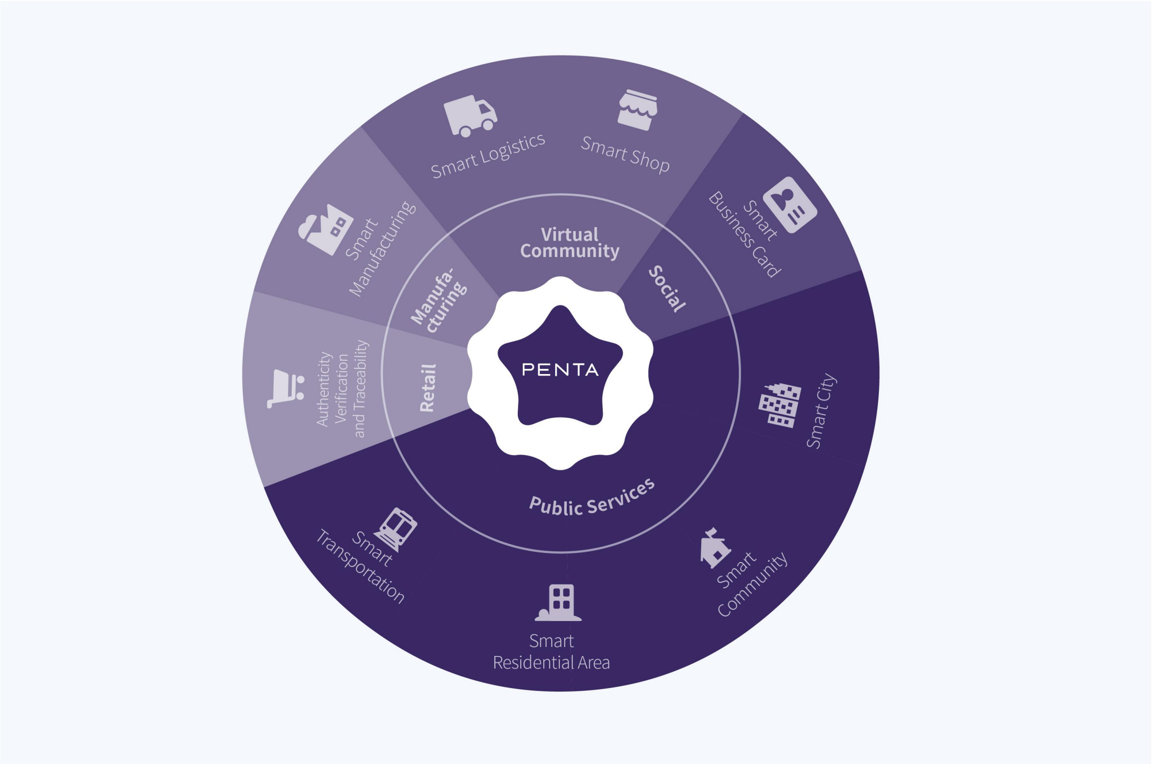


Figure 4.1.3-1 Penta-Based BOT Ecosystem

Charging stations for electric automobiles present a compelling example for BOT application. Governments across the world are instituting policy reforms that encourage the adoption of low-carbon vehicles. Germany, for instance, plans to halt production of gasoline and diesel vehicles by 2030, while Britain plans to ban gasoline vehicles by 2040. Currently, widespread usage of electric vehicles is impeded by poor access to charging stations. Large expanses of road are devoid of any charging stations, particularly in non-urban areas.

Within urban areas, other problems persist. A recent survey conducted by a media reporter found that out of 340 charging points in one city only 61 were functional, 35 were damaged or malfunctioning, and 92 were occupied and unable to be used by a vehicle in need of a charge. In this instance, electric cars in the city suffered from excessive dependence on a limited number of charging points. Moreover, a large number of the charging facilities were privately owned (by storeowners, private parking lots, etc.) and encountered difficulties getting sufficient electricity from power providers, which owned other charging stations and thus were competitors. The city surveyed by the reporter, therefore, lacked both a sufficient number of functioning charging stations accessible by the public, and an effective way to monitor the electrical supply and demand of individual charging facilities, and settlement measures.

To serve the rapidly growing amount of electrical vehicles on the road, a distributed network of charging facilities powered by blockchain technology is needed. The Penta Network can approach this scenario with a similar SPX platform as used by the UEI systems of smart grid cities. Through the SPX platform, the Penta Network can process data from smart metering devices and smart charging devices and correlate with car location data so that users may quickly find accessible charging facilities. Payment can then be accomplished through a DApp (decentralized application). Overall, applying BOT to the challenges of powering smart electric cars will dramatically improve access and efficiency to charging stations, and will allow for many stakeholders to participate in a marketplace of charging points.

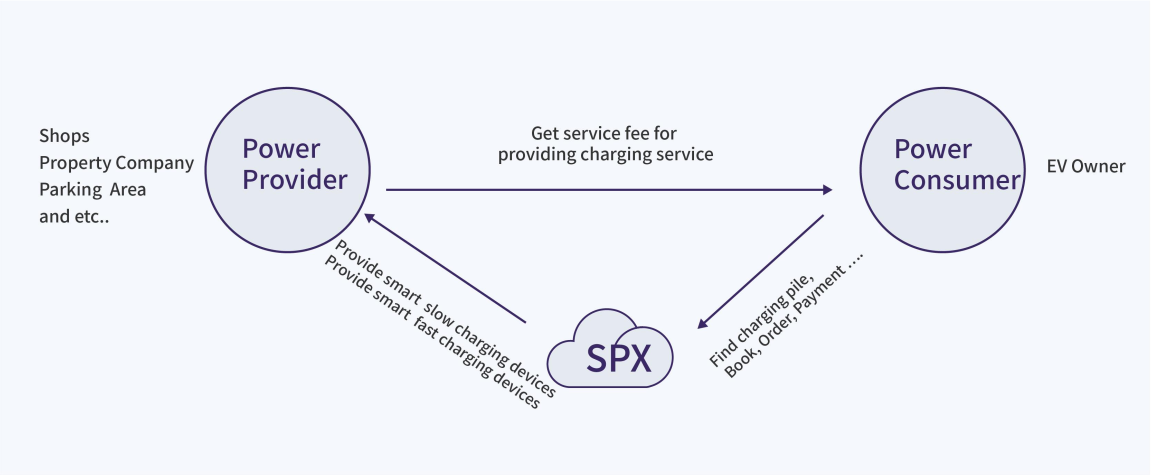

Shops
Property Company
Parking Area
and etc..
Power Provider
Get service fee for providing charging service
Power Consumer
EV Owner
Provide smart slow charging devices
Provide smart fast charging devices
SPX
Find charging pile,
Book, Order, Payment ....

Figure 4.1.3-2 Shared Charging Services Empowered by SPX

Demand Response:

Demand Response (DR) signifies inducing users to change a pattern of behavior related to electricity usage with a form of financial incentive. The purpose of DR is to reduce demand on the electrical grid at certain periods in order to better allocate energy resources and improve the stability of the power system. Even in many industrialized countries, certain areas may suffer from blackouts or brownouts more often than other areas, requiring a new approach to optimizing energy distribution.

Under the current system, DR is managed by centralized power grid operators that are largely unaccountable to the public. Organizations and individuals participating in demand response within this system are required to submit applications in advance of any potential DR implementation. The application process can be slow and subject to stringent requirements, thus making it difficult for retail users to participate, and rendering large-scale application impossible.

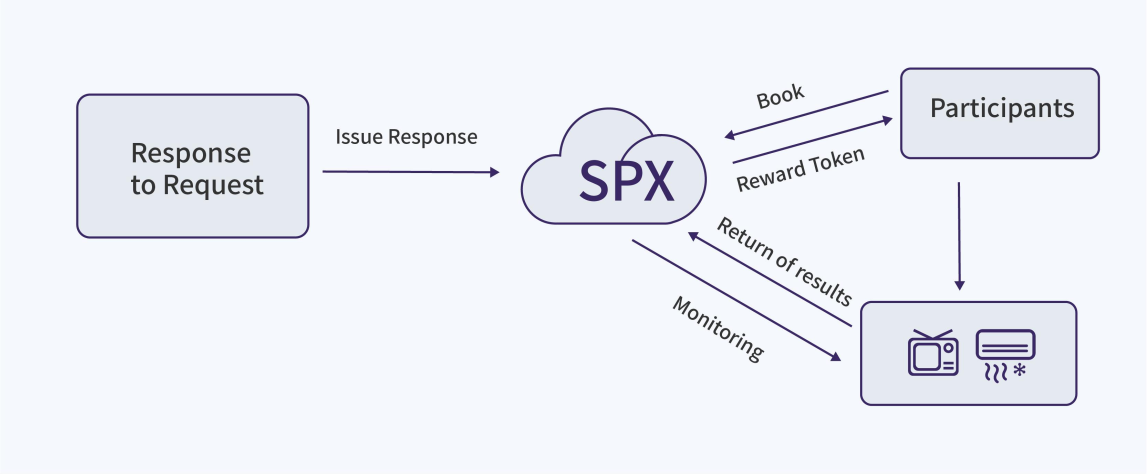


Figure 4.1.3-3 Demand Response Empowered by SPX

The Penta Network's SPX solution offers a way to streamline the DR application process. It can also use Smart Contracts in SPX that enable order placement and implementation by any entity within a CEI or UEI. During this process, SPX will obtain the total amount of DR workload and payment from grid companies and divide individual tasks to be executed by fragmented entities so that more retail participants may participate, thus achieving a long tail effect. In addition, a tolerance function can be set in the Smart Contract to prevent the accuracy of an overall demand response from being affected by a small number of defaults. During the execution of DR, SPX monitors the demand response through a terminal provided free of charge. SPX will receive financial incentives based on successful DR implementation from grid companies, and pass those incentives on to participants in real time in the form of a token.

4.2. Financial Application

The financial sector usually lags behind other industries in adopting new technologies. Nevertheless, financial institutions have been quick to adapt blockchain solutions, seeing the natural bond between blockchain and finance. This space is evolving rapidly, with various sub-sets of the financial services industry pursuing specialized solutions, including the following:

- Peer-to-peer asset transactions for stocks, bonds, derivatives, commercial paper, asset-backed securities, and other financial products.
- Payment Settlement: interbank settlements, cross-border payment, point rewards.
- Credit and Lending: compiling and verifying credit reference, loan issuance, mortgage lending, peer-to-peer lending, merchant loans, crowdfunding, etc.

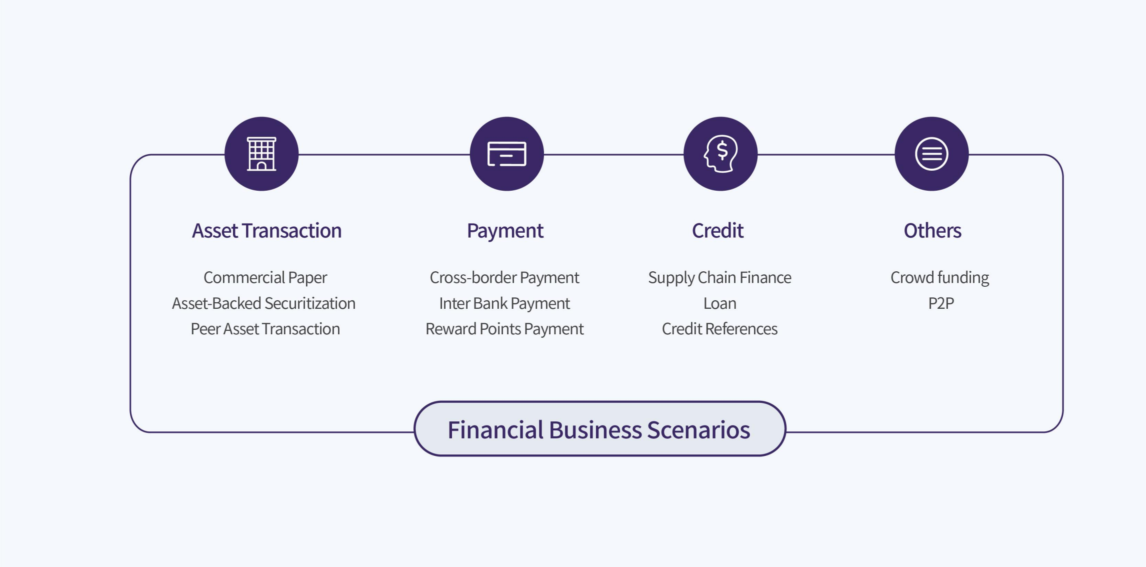


Figure 4.2 Financial Business Scenarios

The Penta team has particular experience in providing software solutions and blockchain solutions to financial institutions. Penta has already developed and launched unique blockchain projects related to compiling accurate credit reference and loan issuance for small merchants, point rewards programs, asset-backed securities, and supply chain finance.

4.2.1 Credit Reference

Recent years have seen exponential growth in credit markets and in the amount of people applying for credit. China, in particular, has seen a market increase in the amount of credit applications and credit circulation. However, there are many problems besetting the Chinese credit markets, especially for small merchants and individuals lacking credit history. Solving the problems of Chinese credit markets holds valuable insights for how to approach similar problems in other countries.

Critical challenges facing the Chinese credit market:

1) Credit history and related information are available to large banks, but smaller banks and credit reference agencies do not have access to this information, due to high credit reference threshold as set forth by the People's Bank of China. This creates problems for small businesses, which often apply for loans at local banks or non-commercial lenders.
2) Lack of data sharing between large banks and credit reference agencies creates a serious gap in information between credit reference agencies and smaller lenders.
3) Limited channels for collecting formal market data leads to bottlenecks and protracted turf battles over data resources.
4) Serious issues in data privacy protection exist in the Chinese credit market. Existing technologies often fail to meet new regulatory and government requirements.

Blockchain's decentralized and trustless peer-to-peer architecture has innovative ways to address the problems noted above. Digital time stamping and asymmetrical encryption, in combination with Smart Contracts, can verify credit reference information while concurrently protecting data privacy. To resolve problems in the current credit reference industry, the Penta Network designed a credit reference service platform powered by blockchain. The platform minimizes risks and costs for participants, expedites the submission and request process, and streamlines settlement.

Penta's credit reference service platform involves a variety of nodes, distributed to various participants involved in the workflow process. Nodes in this platform include credit reference institutions, small lending institutions, banks, insurance companies, government departments, and users. The platform enables data sharing between lending institutions and credit reference agencies.

To prevent abuse of credit information, the Penta Network uses Smart Contracts to set up credit reference verification and authorization mechanisms to control which parties have access to sensitive credit information. Because all of this occurs on a blockchain platform, the interactions are traceable, further contributing the efficiency and security of the platform. Since data on the blockchain cannot be modified, credit agencies are not able to abuse their use of credit references, a problem persistent in the industry as it is presently. In addition, sensitive client data are encrypted and may be accessed only by authorized users.

This credit reference blockchain platform has been launched in China and some small-loan lenders are already active on the platform, representing a successful Penta Network use case. The platform provides credit data, collateral data, data on blacklists, and data submitted or queried by a regulator or other third parties. In addition, the team also designed a point rewards and consumption incentive to encourage all connected participants to share more data.

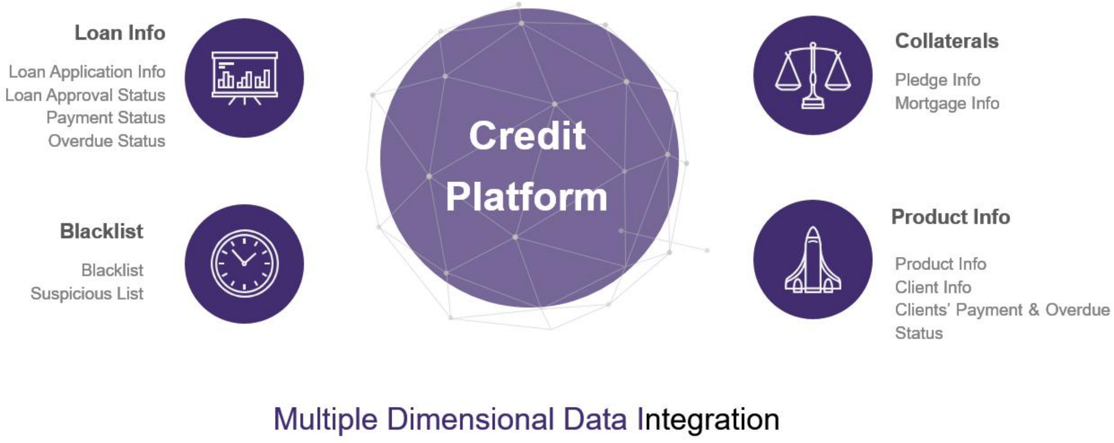


Figure 4.2.1-1 Penta-Based Credit Platform

The credit platform has operated smoothly since its launch, and has enjoyed consistent increases in usage by institutions and other nodes. The following is monitoring information taken from the trading blocks of the credit platform.

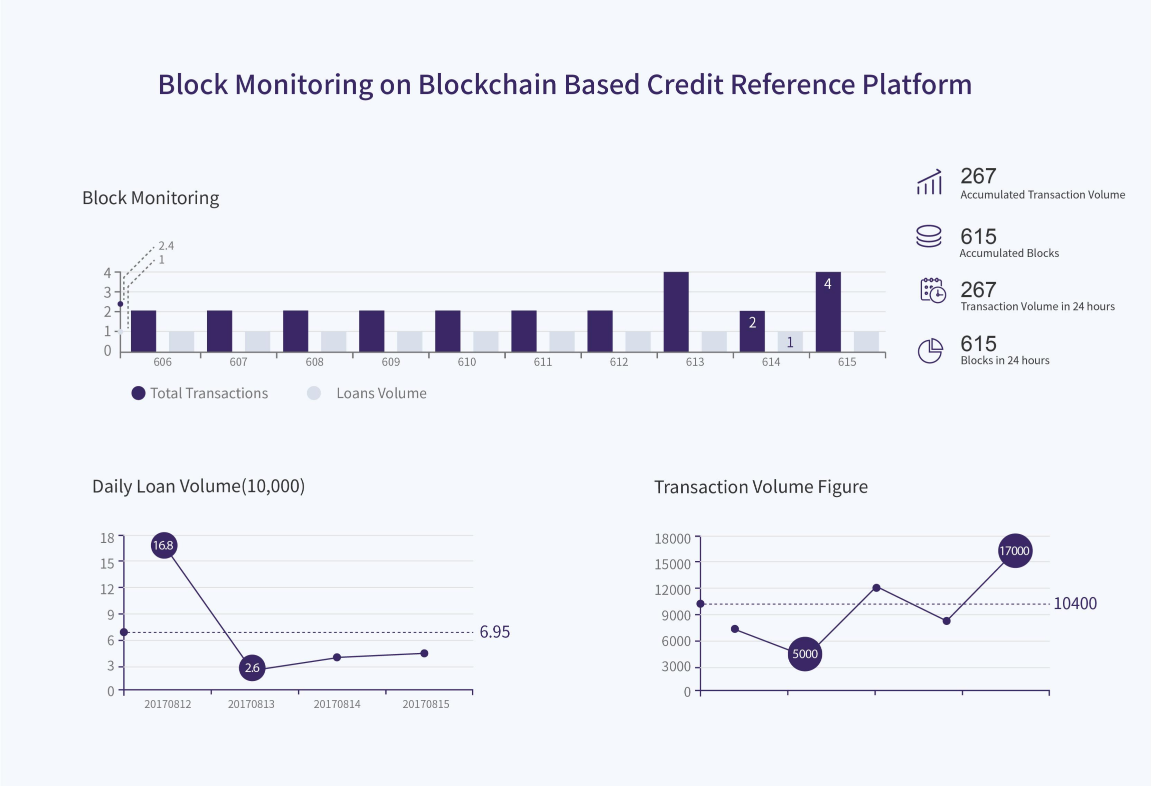


Figure 4.2.1-2 Block Monitoring in Credit Platform

4.2.2 Supply Chain Finance

As the world becomes increasingly globalized, supply chains become more complex and more in demand. Using receivables as collateral for bank loans offers huge growth potential to companies seeking supply chain finance.

An experienced provider of Fintech solutions to banks and financial institutions, the Penta Network has gained an in-depth understanding of the complexity of supply chain finance. Verification of multi-party contracts and transaction supporting documents are burdensome and inefficient. This is primarily due to a lack of trust, resulting in poor information exchange among the various parties involved in a supply chain finance process: buyer, seller, buyer's bank, seller's bank, logistics companies, supervisory agencies, customs authorities (cross-border order financing) and others.

In addition to being multi-party and multi-contract, supply chain finance also includes many different categories of financial products, such as purchase order financing, cash flow loans, and fund settlement. Applying for supply chain financing is constrained by a complicated workflow process, from provision of application documentation to formulation of suitable financial products, to closing the deal.

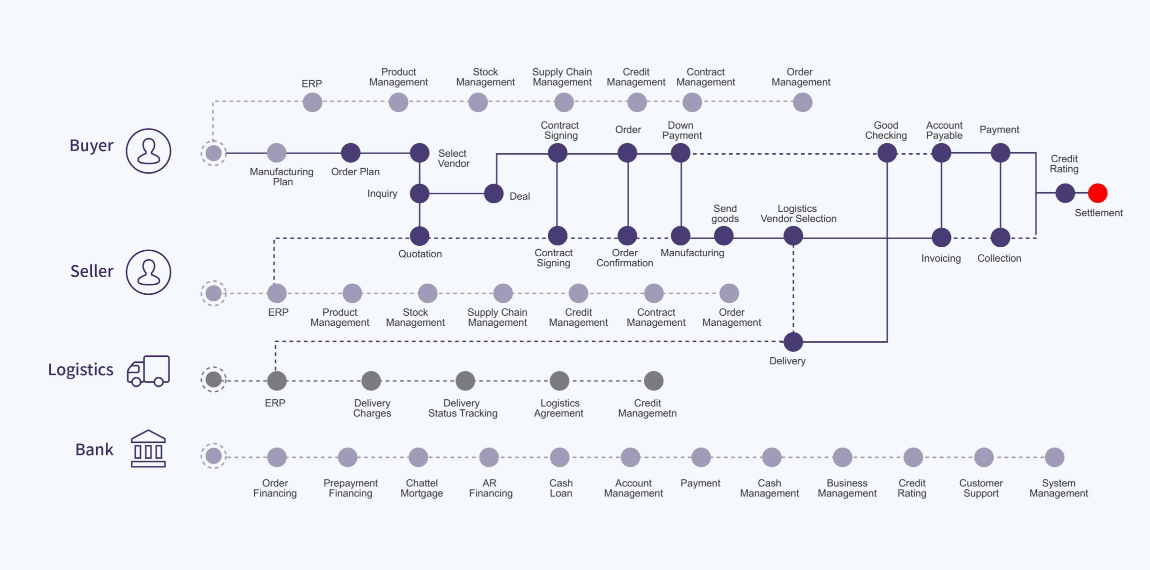


Figure 4.2.2-1 Supply Chain Finance

Blockchain technology is highly applicable to supply chain finance. It enables authentication and verification (anti-manipulation) by blockchain, and Smart Contract solutions. Digitized solutions for supply chain finance as provided by blockchain will increase transparency, lead to risk mitigation, and reduce man-hours spent on paperwork.

The figure below shows a particular scenario in which the Penta Network designed a blockchain solution for a financial institution for supply chain finance.

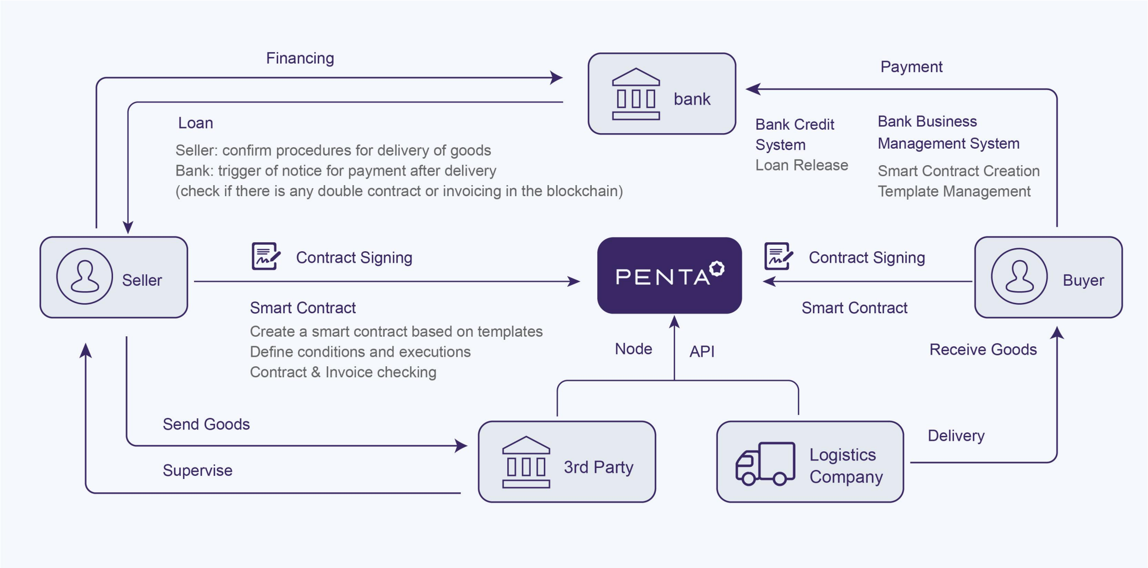

Financing
bank
Payment
Loan
Seller: confirm procedures for delivery of goods
Bank: trigger of notice for payment after delivery
(check if there is any double contract or invoicing in the blockchain)
Bank Credit System
Loan Release
Bank Business Management System
Smart Contract Creation
Template Management
Seller
Contract Signing
Smart Contract
Create a smart contract based on templates
Define conditions and executions
Contract & Invoice checking
PENTA
Contract Signing
Smart Contract
Buyer
Node
API
Receive Goods
Send Goods
Supervise
3rd Party
Logistics Company
Delivery

Figure 4.2.2-2 Purchase Order Financing

The workflow process depicted in the diagram above is as follows:

1) Terms and conditions for the contracts are coded into a Smart Contract;
2) The financial institution issues a loan based on the status of contract execution and shipment of goods.
3) Settlement by the buyer proceeds seamlessly in accordance with the payment terms as coded into the Smart Contract,
4) During the process, logistics and supervising companies contribute the business status and relevant data to blockchain, which information is available to interested parties.

4.2.3 Asset-Backed Securities

Asset-backed securities (ABS) involve multi-party transactions and complicated workflow processes. Often, transacting parties use complex corporate structures, such as establishing SPVs (special purpose vehicles) to mitigate risks. The following is the structure of a typical ABS transaction:

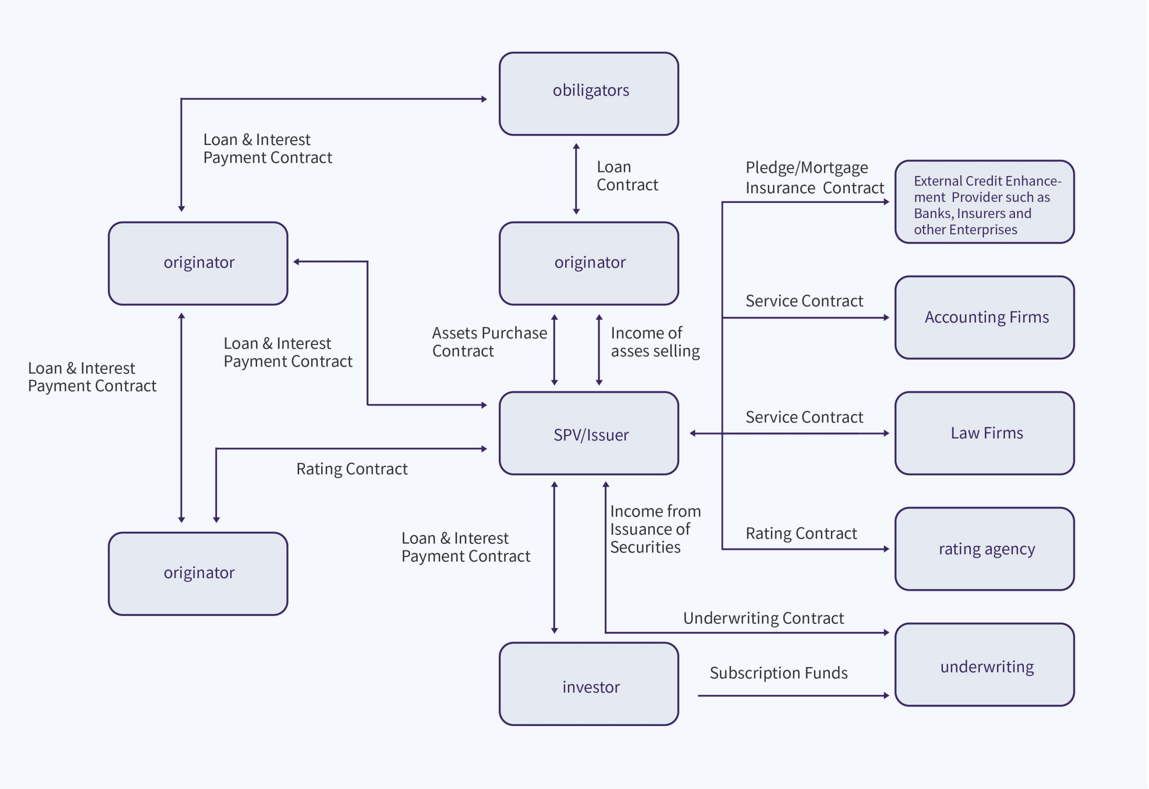

obiligators
Loan & Interest Payment Contract
Loan Contract
Pledge/Mortgage Insurance Contract
External Credit Enhance-ment Provider such as Banks, Insurers and other Enterprises
originator
originator
Service Contract
Accounting Firms
Loan & Interest Payment Contract
Assets Purchase Contract
Income of asses selling
Loan & Interest Payment Contract
SPV/Issuer
Service Contract
Law Firms
Rating Contract
Income from Issuance of Securities
Loan & Interest Payment Contract
Rating Contract
rating agency
originator
Underwriting Contract
underwriting
investor
Subscription Funds

Figure 4.2.3-1 Basic Transaction Structure

As shown by the diagram, there can be large numbers of transacting parties involved in a single deal. Information sharing among the transacting SPV, sponsors, debtors, investors, trustees, service providers, accounting firms, law firms, credit rating agencies, and securities underwriters is costly and verification of information is time-consuming. Blockchain offers viable solutions to information sharing and verification in this type of transaction. Using blockchain, multi-party asset distributions are traceable, and ratings by third-party agencies are more transparent. More reliable information due to blockchain creates significant time and cost savings. Enhanced transparency can help investors to make better-informed decisions on investment risk.

The Penta Network has created a smart ABS platform based on blockchain technology to register underlying assets, asset appraisal, auditing and transaction data. Greater transparency in asset allocation will promote healthy developments in the ABS markets and reduce regulatory costs.

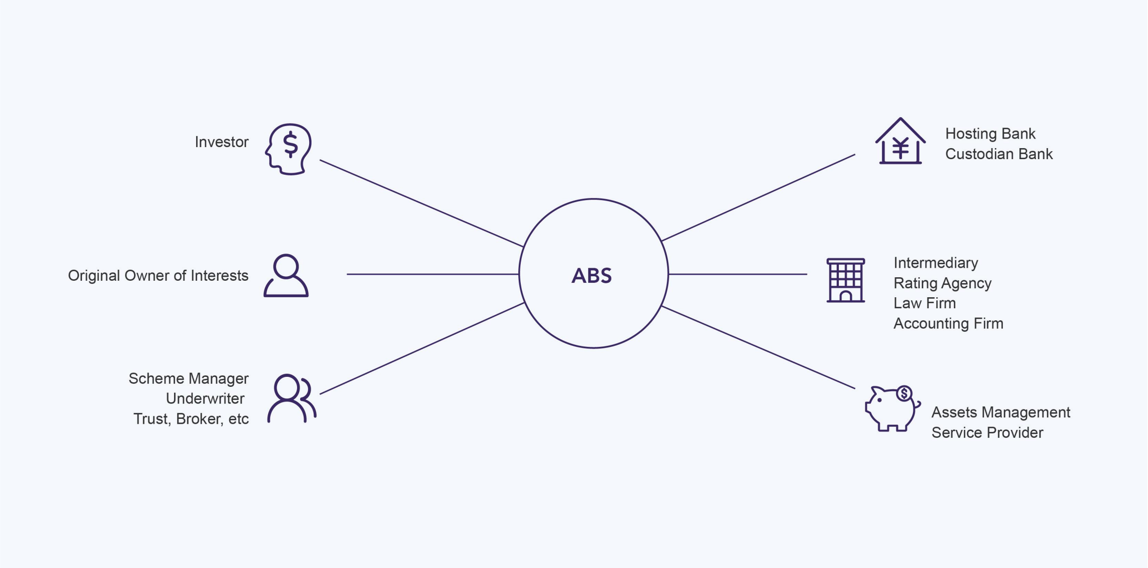


Figure 4.2.3-2 Penta-Based Asset-Backed Securitization Platform

As shown above, the blockchain ABS platform supports asset management and information sharing for each party involved in the 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, you 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 the capacity to retain assets on the ledger.

State Recognised Algorithms

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. Ohrimenko, 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