DAEX: A Distributed Digital Asset Clearing Ecosystem
Technical White Paper

contactus@daex.io

Introduction

The many benefits of digital assets are often overshadowed by credibility and security concerns. In its current state, the digital asset market has many problems, including its susceptibility to market volatility and price fluctuations as well as its lack of security and transparency. The DAEX project aims to solve these problems by creating a distributed digital asset clearing ecosystem based on blockchain technology—a secure, trusted and open network in which everyone can witness value.

1. Ecosystem Overview

1.1 Background

(1) Frequent Security Incidents

In the current blockchain-based digital asset market, there is a lack of clear boundaries, transparency and security. This leaves participants vulnerable to malicious attacks and theft. Security incidents are commonplace. These include hacks perpetrated both against individual investors and digital asset exchanges. The recent hack of the Coincheck exchange, for example, caused a market-wide decline in digital asset values. The continued frequency of these incidents only serves to further highlight the security and credibility issues faced by the market.

(2) Imperfect Clearing Solutions

At present, the digital asset market does not have any purpose-built clearing ecosystems. Although some product solutions have added clearing functionality, they are not built specifically around the clearing business process. In order to create a purpose-built Blockchain 3.0 clearing ecosystem that is both secure and efficient, it is therefore necessary to re-engineer and optimize many of the underlying blockchain protocols.

(3) A Lack of Secure and Trustworthy Infrastructure

The development of conventional digital asset clearing mechanisms is at a standstill, with current solutions failing to produce a standardized clearing mechanism for digital assets across multiple digital asset exchanges. In order to solve these problems, the market needs a new clearing solution which provides safe and credible services for all types of digital asset activities, including the ability to use said assets across multiple platforms. In order to achieve this, the necessary clearing solution should also include a reliable digital asset wallet based on blockchain technology. This wallet should not only solve market pain points, but also provide additional functionality when it comes to digital asset trading, thus becoming a truly trustworthy, useful tool for managing digital assets.

1.2 Ecosystem Design

DAEX aims to build a distributed digital asset clearing ecosystem using a multi-asset blockchain-based clearing and settlement protocol. The ecosystem will decouple assets and transactions, enable token-based authentication and restructure the transaction process. This will allow for safer and more efficient distributed registration, clearing and settlement of digital assets. Using this as a foundation, DAEX will serve the entire digital asset market, from digital asset exchanges comprising of multiple interconnected nodes to individual digital asset users.

1.2.1 Value Chain

The DAEX ecosystem optimizes and improves both the upstream and downstream architecture of digital asset transactions. It encompasses the entire value chain, from identity authentication and asset registration to asset clearing and settlement.

Figure 1: Clearing Ecosystem Value Chain

Formulated using the combined knowledge of the DAEX team's Internet technology experts and computer scientists, the DAEX solution separates transactions, clearing and custody. By connecting centralized exchanges with decentralized clearing and settlement services, DAEX will create a network in which all participants can witness value.

1.2.2 Ecosystem Components

In the DAEX ecosystem, DAEX's distributed multi-asset wallet (hereinafter referred to as the DAEX Wallet) acts as a connector, linking the Distributed ID Center, the Asset Clearing Center and the Asset Registration & Settlement Center. The Asset Clearing Center component of the DAEX Wallet uses a decentralized chain called the Clearing Chain. This increases the trustworthiness of digital asset transactions by relying on blockchain's inherent security and credibility mechanisms, while also promoting an open clearing ecosystem thanks to standardized clearing and settlement protocols.

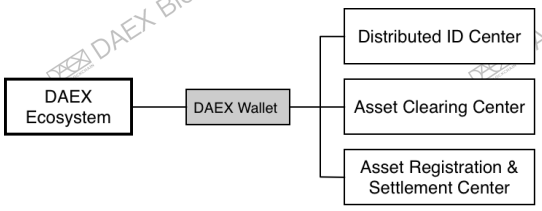


Figure 2: Clearing Ecosystem Components

The DAEX Clearing Chain possesses many of the technical characteristics of traditional public chains while specifically optimizing and upgrading key components, such as the consensus mechanism, transaction encryption and privacy protection. The system also provides various services related to digital assets such as identity authentication, the registration and mapping of assets, the exchange and payment of assets, as well as wealth management services. These services are all based on the clearing models found in traditional financial markets. Together with the Distributed ID Center and the Asset Registration & Settlement Center, the system not only provides infrastructure that is fully compatible with existing trading models, but also a Clearing-as-a-Service (hereinafter CaaS) solution that will support the development of both current and future digital asset exchanges. DAEX also aims to create a better trading environment by providing the traditional financial sector with clearing services based on smart contracts, which are both stable and auditable. With the addition of decentralized smart assets, digital asset options and futures, as well as other financial derivatives to its Clearing Chain layer, the system will have the ability to evolve on its own.

Connected to the Clearing Chain, the DAEX Wallet allows users to self-clear transactions, providing a better trading and payment user experience. Incorporating threshold signatures, global identity certificates and a trusted computing environment as well as other technologies and governance mechanisms, the wallet provides comprehensive digital asset management services for a wide range of users. For enterprise-level services, such as those used by digital asset exchanges, the focus is on separation of permissions and risk management. For individual wallet users, the focus is on asset diversity and the security of their private keys.

1.3 Capability Model

The open architecture of the DAEX ecosystem facilitates the collaboration of multiple entities when it comes to processing information and transactions. At each layer of the system, DAEX will provide the necessary basic functionality. This includes digital asset mapping and CaaS, as well as the multi-segment key and identity authentication components of the DAEX Wallet. DAEX will also provide certificate lifecycle management for the Distributed ID Center.

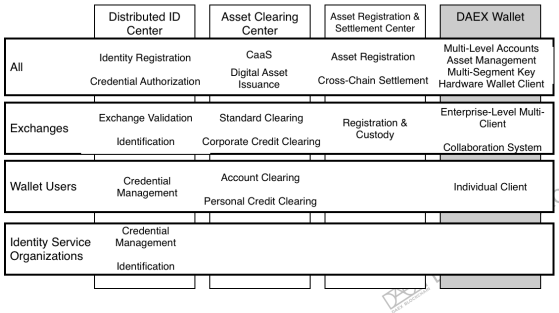


Figure 3: Clearing Ecosystem Capability Model

2. Ecosystem Solution

2.1 Ecosystem Architecture

The Clearing Chain is the basic core chain of DAEX's clearing ecosystem. Its application layer supports a complex cross-chain architecture that allows it to connect multiple chains, including the Identity Chain and the Settlement Chain. At the same time, by virtue of different levels of side-chains on exchanges, the system is able to meet high concurrent demand. The DAEX Wallet is the vehicle through which the digital asset management and decentralized clearing services are implemented. Based on the infrastructure of the Clearing Chain, the physically separated and logically independent Distributed ID Center and Asset Registration & Settlement Center are established simultaneously, thereby establishing a complete clearing and settlement value chain as well as an ecosystem governance protocol.

This "multi-center" hierarchical ecosystem solves many of the inherent limitations of the blockchain protocol, ensuring that the distributed network can interact with external data safely and reliably. As part of this process, the Distributed ID Center and the Asset Registration & Settlement Center connect to the Identity Chain and the Settlement Chain respectively. In order to improve the security of assets and transactions, multi-level authentication technology is used in order to reduce the degree of unilateral trust of each center as far as possible. The use of distributed ledger technology and a trustless consensus mechanism further ensures the integrity of the ecosystem.

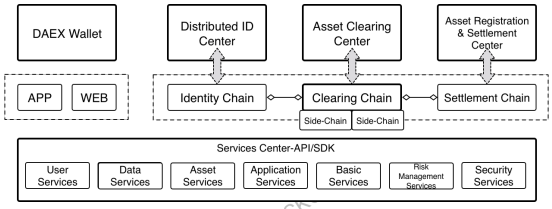


Figure 4: Clearing Ecosystem Architecture

2.2 Account System

The account system establishes the relationship between assets and their owners. For each participant, creating their own clearing account is the first step to enjoying distributed clearing services. These account owners form the core of the account system, which records the number of asset types and transaction logs in each account. Each account is an authenticated and trusted identity. Digital assets in these accounts are hosted in a controlled and secure environment, with users having full sovereignty over their assets. The account system also allows users to attach a non-disclosed real name identity to their digital assets in order to prove ownership and aid in asset recovery.

In the DAEX ecosystem, accounts are divided into Personal Accounts and Organizational Accounts, depending on the type of user. Organizational Accounts are further subdivided into General Organizational Accounts and Exchange Accounts, which are special types of Organizational Accounts used by digital asset exchanges. Generally speaking, Organizational Accounts are enterprise-level accounts that are suitable for high-frequency trading or multi-level licensing by users such as market makers and funds. Personal Accounts, on the other hand, are more suitable for individual payments and trading.

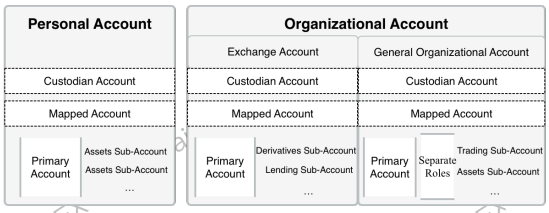


Figure 5: Clearing Ecosystem Account System

Each account has a corresponding Custodian Account and Mapped account. The Custodian

Account shows the custodial status of the account's registered assets while publicly supervising transactions and preventing abnormal behavior. The Mapped Account is the actual record of effective assets in the account after they have been registered on the Clearing Chain. The Custodian Account is updated and settled at regular intervals, while the Mapped Account can be split into various types of sub-accounts according to usage scenarios and business requirements.

The allocation of assets among these sub-accounts can be used to implement various business strategies, such as the separation of asset accounts and trading accounts. General Organizational Mapped Accounts are embedded with an authorization approval mechanism which relies on hierarchical roles. In addition, individual users are able to create sub-accounts associated with various exchanges, allowing them to make transactions on multiple exchanges under the same identity. Exchange Mapped Accounts support the clearing of transactions made by their users' sub-accounts, while also performing risk management for financial product sub-accounts.
All accounts include the following: a global identity, an account name, an account type, an account status, a clearing address, an asset list and an exchange ID. The asset list is a multidimensional array of key elements including digital asset type, custodian address and balance.

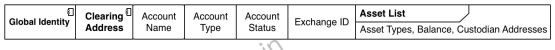


Figure 6: Clearing Account Structure

A transaction made by an account includes the following information: the transferrer, the transferee, asset type, amount, event time, event type, transaction channel, transaction hash, and block height.

Figure 7: Transaction Clearing Event Structure

2.3 Business Model

Since its inception, the digital asset market has become a globalized financial world of its own, connecting a variety of financial products. Currently, digital asset owners use a wide array of wallets and/or exchanges to manage and register their assets. These platforms all have different processes for completing clearing and settlement, which all require some form of decentralized nodes on public chains or a centralized entity to ensure the transparency of information and asset security. At the same time, the clearing and settlement process for cross-platform digital assets is limited by the business models of the various trading platforms as well as technical bottlenecks. DAEX solves the problem of credibility in centralized transactions by implementing a distributed clearing and settlement solution, thus combining the advantages of centralized and decentralized solutions. This is coupled with a complete set of security systems and digital asset vaults for both digital asset exchanges and individual investors, all of which are fair, efficient and compliant with standard regulations.

The traditional financial market is a mature ecosystem consisting of banks, registered clearing companies, exchanges, securities firms and funds. Naturally, the digital asset market will follow the same model, evolving into multiple professional organizations. The difference is that these organizations can be decentralized or distributed. This will create trust and reduce both financial and moral risk for the following reasons:

(1) Reliable and authentic data

The distributed clearing and settlement of digital assets prevents data modification and falsification. Only the owner of an asset has permission to modify said asset's data.

(2) Real-time asset registration

After a digital asset transaction is completed, the DAEX clearing and settlement process will ensure that the changes in data are synchronized between all nodes in a timely manner, achieving simultaneous registration of cross-platform assets.

(3) Personal Privacy Protection

Thanks to a built-in, smart-contract-based privacy protection protocol which uses chain identification codes, the system offers increased

protection of both personal and private exchange data.

The essence of the DAEX clearing ecosystem is to achieve a layered system of trading data and digital assets. Due to the system's hierarchical architecture and the fragmentation of data on said system, exchanges are able to realize their potential as professional trading services organizations. All digital assets are registered with a custodian organization while the decentralized Clearing Chain ensures the credibility of any clearing and settlement performed. The process for custody and clearing is shown in Figure 8:

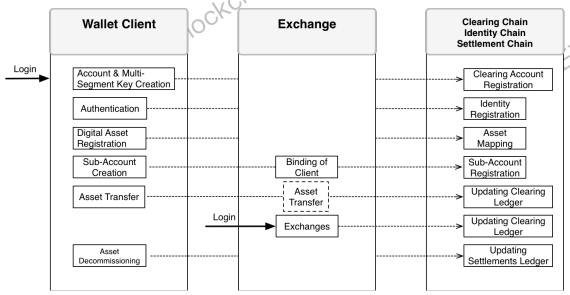


Figure 8: Custody and Clearing Business Process

In order to ensure business continuity of the exchange, the distributed clearing process can be divided into transaction-oriented custody and clearing as well as service-oriented credit clearing. While validation of the clearing process will initially be carried out by the exchanges themselves, this will gradually develop into a situation where all members of the DAEX ecosystem participate in clearing validation. The above components are laid out as follows:

- Custody and clearing is the primary accounting method for distributed clearing.
- Credit clearing will be an important clearing method for payments and trading once the ecosystem is more mature.
- Credit clearing is not limited to the asset registration process. It places certain requirements on the transaction process when it comes to risk management, credit rating and the exchange deposit.
- Every user in the DAEX ecosystem can participate in and validate the consensus process of digital asset clearing through multiple channels. By doing so, participants have the opportunity to obtain tangible rewards.

2.4 Ecosystem Protocol

A standardized business protocol is essential for CaaS. The protocol needs to be adaptable to different scenarios while allowing for the sharing of data between exchanges. Therefore, the ecosystem should record data in a way that is sufficiently versatile, standardized and easily constructible. At the same time, it should be able to effectively represent a variety of structured data, while its customizable open protocol should also be able to satisfy cross-platform and cross-chain requirements as the scope of services expands.

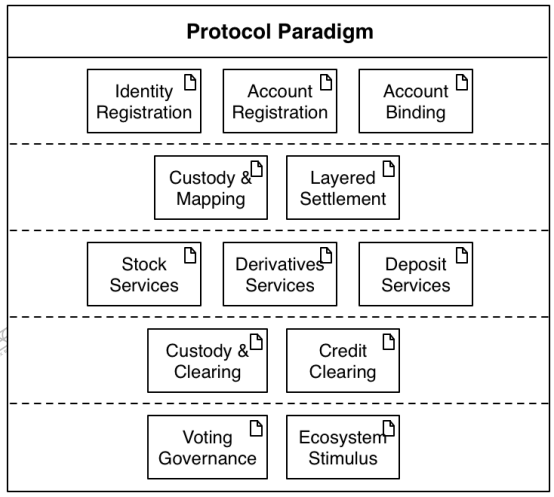


Figure 9: Clearing Ecosystem Base Protocols

The ecosystem's protocols regulate the domain and format of all information stored in the settlements ledger. They also regulate all processes on the Clearing Chain, the triggers and conditions for updating the status of these processes as well as any new information to be used in said processes.

During the clearing process, both participants sign an agreement based on smart contracts with an account linked to their identity. The process is objectively verified by the blockchain system and the agreement is implemented on each node, thus effectively being recognized by both business entities. In this way, the process is accurately recorded and the final result cannot be tampered with. This in turn means that the

final result of the aforementioned process is undeniable.

3. Ecosystem Structure

Blockchain technology provides basic solutions for the accumulation and distribution of value in the DAEX ecosystem. However, in order to achieve a truly autonomous distributed ecosystem, said ecosystem should also perform well enough to match current and future throughput. In addition, the ecosystem should also provide excellent interoperability through the use of a distributed file system to improve data storage performance and the optimization of the settlement model through optimized consensus protocols. Combining the secure, easy-to-use digital asset tools provided by the DAEX Wallet with service interfaces that enable rapid, accessible solutions, the DAEX clearing ecosystem has the following advantages:

(1) More Robust

The DAEX ecosystem prevents users from privately keeping and transmitting a complete key. By putting the user at the center of the process and using a consensus mechanism, it also makes accounting on the distributed ledger more efficient.

(2) A Richer User Experience

The DAEX solution also increases the scalability of the blockchain, allowing rapid transactions of multiple assets. At the same time, the basic high-level services of the Clearing Chain can retain the same transaction depth while providing an abundant business ecosystem for derivatives and smart assets.

(3) More Reliable

The multi-segment key mechanism used in the DAEX Wallet combined with a secure computing environment means assets are more secure. At the same time, a consensus mechanism based on a Clearing Value Factor (CVF) ensures a fair distribution of rewards and penalties for desired behavior and malicious conduct, respectively.

3.1 The Clearing Chain

The Clearing Chain provides an interface for digital asset exchanges, allowing both individual and organizational customers to use their DAEX Wallets to perform payments and conduct trades. Customers are also able to complete smart-contract-based asset clearing operations. Combined with the decoupled and flexibly configurable components of the ecosystem, the Clearing Chain's smart contract engine means the system is able to adapt to various scenarios, thus facilitating the various activities of the digital asset market.

When it comes to the clearing and settlement process, the most vital aspect of the DAEX Clearing Chain is that it allows smart-contract-less chains to perform atomic transactions. Through an agreement between the two parties, a clear settlement contract is achieved, ensuring the atomic settlement of the assets in question. The Clearing Chain bi-directionally anchors the assets under "custodian" and "mapped" assets, with only users able to confirm the movement of said assets. At the same time, the coalition of multiple exchanges using the DAEX clearing ecosystem, which are connected through shared use of the ecosystem's services, promotes trustworthy behavior from all participants. "Miners" on the ecosystem's shared Clearing Chain act as witnesses for the clearing process, effectively checking and monitoring the status of the digital assets currently on the chain. When they receive a transaction request, a synchronized clearing agreement is executed to ensure that the results are valid. The more trustworthy miners participate on the Clearing Chain, the higher the overall security of the system.

3.1.1 Design Principles

- Smart contracts are used as the primary method of storing value in the clearing ecosystem.
- The Clearing Value Factor acts as an incentive for node validation.
- An upgraded Proof of Stake mechanism boosts transaction performance and mathematical randomness.
- The system provides a directional encryption scheme for digital asset

transactions. Some scenarios only support viewing and transaction verification for clearing affiliates.

- The ecosystem meets regulatory support and audit implementation requirements.
- In order to ensure the consistency of data on the Clearing Chain, an effective governance mechanism prevents forking in the event of an emergency.

3.1.2 Product Architecture

The Clearing Chain's basic functions include key management, smart contracts and ledger data management. It also provides monitoring of node and block information. It is divided into three layers as shown in Figure 10.

(1) Underlying protocol and system support layer

The standards and protocols of the Clearing Chain's underlying infrastructure are clearly defined, including its block architecture, storage type, account model and operating instructions. They are also compatible with cloud service technology systems, with the ability to use container technology for rapid deployment and configuration management.

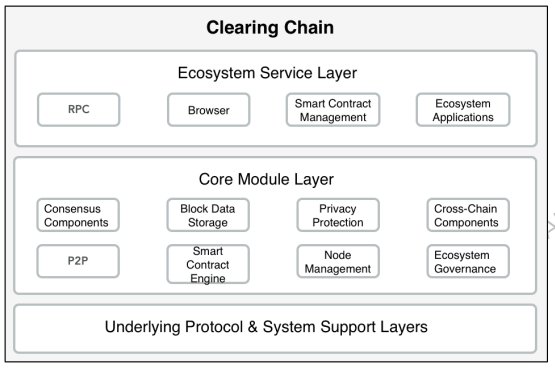


Figure 10: Clearing Chain Architecture

(2) Core Module Layer

The interaction of data in the core module layer is facilitated by an internal data exchange protocol. The components in this layer are independent and decoupled. At the same time, the data and logic are separated, making each module component pluggable and extensible.

Consensus Component:
The consensus component is primarily responsible for completing the broadcasting, sequencing, execution and consensus of transactions. Situated above the Proof of Stake deposit mechanism, it integrates the Clearing Value Factor incentive system with a verifiable random function (hereinafter VRF).

Ledger and Storage Component:
This component ensures the consistency of the ledger through the use of a mature NoSQL database. KV data formatting provides a simple and fast storage paradigm while protecting against data modification.

P2P Communication Component:
This component establishes P2P communication between blockchain nodes. When dynamically added nodes are discovered, block information is automatically synchronized.

Smart Contract Engine:
This is a Turing-complete execution engine based on a virtual machine that encapsulates and is compatible with smart contracts. Each node must achieve consensus on the status of process executions and results of said executions. Programmability of the Clearing Chain is achieved by coding smart contract logic that applies to different business scenarios.

Privacy Protection Component:
The privacy protection component supports transaction-level encryption that only transaction-related parties can see. Non-participants that have nothing to do with the transaction can only obtain and validate the encrypted hash value of the original transaction.

Node Management Component:
This component supports the dynamic configuration and verification of node permissions. Nodes are divided into validator nodes and regular nodes, with the former participating in the consensus process.

Ecosystem Governance Component:
This component provides a technical solution to improving the ecosystem governance mechanism, preventing damage to the ecosystem caused by unknown errors due to as of yet unresolved problems with blockchain technology. The DAEX clearing ecosystem is both stable and sustainable. Combining special

role functions, a distributed governance architecture and the ability of the Clearing Chain to handle emergencies using off-chain consensus, the ecosystem is able to guard against malicious attacks, software bugs, hard forks and other emergencies. This enables O&M to be performed autonomously. Through its parametric design, the ecosystem is thus capable of self-correction.

Cross-Chain Component:
This component supports the exchange of information between the ledgers of multiple chains as well as side-chains, including the Identity Chain, the Settlement Chain and the sub-chains of the Clearing Chain. During this process, data and business logic are separated.

(3) Ecosystem Service Layer

The ecosystem service layer is based on the underlying protocols and core modules of blockchain technology. It provides a complete toolkit including an API and SDK.

RPC Component:
The RPC component processes remote procedure call requests sent to nodes, acting as an entry point for node data interaction. The component uses a set of rules to filter invalid messages in order to reduce consensus load. At the same time, by utilizing flexibly configurable RPC services, load balancing can be achieved. Various transmission protocol specifications and scenario interfaces can also be customized to meet the requirements of different types of clearing services.

Browser Component:
This component forms the foundation of the Clearing Chain browser. It provides block information, transaction information, node status, network status and various other types of statistics.

Contract Management Component:
This component provides modularized management of smart contracts, including contract creation, testing, deployment, upgrades and template editing.

Ecosystem Application Component:
The Ecosystem Application component facilitates the implementation of application functions such as authentication, clearing, settlement, asset mapping and distribution.

3.2 The DAEX Wallet

The multi-asset DAEX Wallet is designed to meet the digital asset needs of both businesses and individual users. The wallet also acts as proof of identity. By using its identity authentication mechanism, users can access every exchange in the DAEX ecosystem seamlessly.

Users of current digital asset wallets frequently lose their assets due to uninstalling or re-installing applications, changes to app store product regulations, users forgetting mnemonics, losing keystore files and so on. The multi-layer security defense system provided by the DAEX Wallet protects the security of digital assets from multiple angles. These include mobile security defense mechanisms, secure key management, multi-factor authentication and protecting against malicious user behavior. Meanwhile, the wallet's segmented key mechanism can be used to recover assets if a user loses their key.

The DAEX Wallet is easy to use. Different features are provided according to the user's account type, making it a suitable asset manager both for organizations and individuals. By "mapping" users' assets on public chains into a separate Mapped Account on the Clearing Chain, the wallet provides an efficient channel for the management, sending and receiving of digital assets. At the same time, thanks to the wallet identity authentication mechanism embedded in DAEX-partnered exchanges, transaction costs are reduced and confirmation time for asset transfers is shortened. In addition, the DAEX Wallet will also provide hardware wallet access. Combined with the wallet's software keys, this will create an end-to-end security system that establishes a more trustworthy environment for the management and trading of digital assets.

3.2.1 Design Principles

- The DAEX Wallet supports multiple major digital assets.
- With its single-identity account asset management system, the wallet is able to overcome the challenges presented by the differences in account systems and

technical architecture between different exchanges and blockchains.

- A multi-segment key protects user assets, while providing total control of assets. If another organization holds a segment of the key, they cannot independently recover the whole key or initiate asset transactions.

- With enterprise-level functionality, such as multiple levels of authorization and collaboration features for multiple users of the same wallet, the DAEX Wallet is also an excellent digital asset manager for organizational users.

- As a one-stop digital asset management tool that is able to meet storage, payment, trading user requirements while also supporting third-party services, the DAEX Wallet expands on the value-added capabilities of digital assets.

3.2.2 Product Architecture

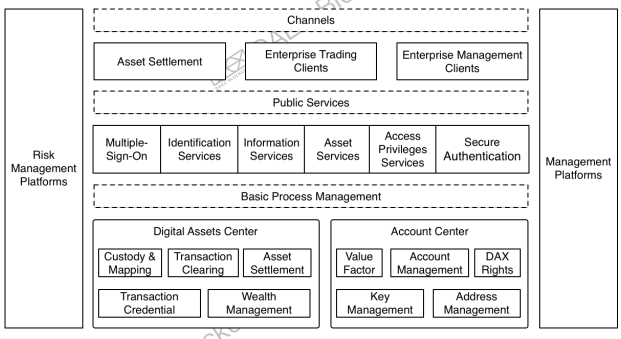


Figure 11: DAEX Wallet Architecture

(1) Basic Functionality

Asset addresses in the DAEX Wallet are randomly generated, with users able to customize and manage their various mapped assets. Asset transfers within the ecosystem are completed through the Clearing Chain's mapped assets credit ledger. Asset transfers based on user-defined IDs are also supported. During the settlement process, a combination of cross-validations is performed, including dynamic passwords, biological information and physical information. Each time a checksum is verified, a two-way checking of the balance is performed according to the flow of clearing and settlement in order to ensure the consistency of both the Clearing Chain's data and the wallet's asset account. A risk management platform provides pre-event and mid-event risk management, protecting users' assets from multiple angles by performing identity and device identification, risk monitoring and assisting in supervision of the entire transaction process.

Both personal and organizational wallets are specifically designed to meet the needs of their respective users. At the same time, the creation of different levels of sub-accounts allows for rapid cross-platform and cross-business asset management. The aim of the DAEX Wallet is to create a one-stop digital asset market, including derivatives services, high-quality financial management, digital asset search capabilities as well as financing and other financial instruments. In addition, the wallet will also provide various digital asset tools such as market information apps, third-party decentralized apps and more.

The wallet also enables DAEX token holders to fully participate in the development of the settlement ecosystem, including taking part in the voting process and obtaining rewards for clearing validation.

(2) Multi-Segment Private Key

The user's clearing and settlement account uses a three-stage key mechanism (user, server and custodian) in order to control the security of digital assets. The private key is stored in segments in ciphertext and the key fragments are stored in multiple locations. Relying on a trusted computing environment, the key mechanism covers the entire process including key creation, private key segmentation, private key segment encrypted storage, secure key transmission as well as key signing and recovery. Combined with a permissions management system, it provides increased security for digital assets.

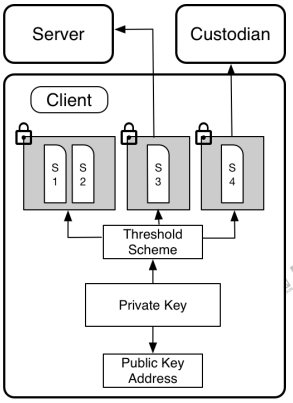


Figure 12: Multi-Segment Key Mechanism

3.3 The Identity Chain

The Identity Chain essentially connects the following DAEX partners together as links on the same chain: third-party identity service organizations, digital asset exchanges and the Distributed ID Center. The Distributed ID Center is a complete, compliant and trustworthy global identity management system. It handles the registration, management and authentication of user identities on the Clearing Chain, providing increased security and anonymity. In this way, it forms the basis for the circulation of value across exchanges and between users in the ecosystem.

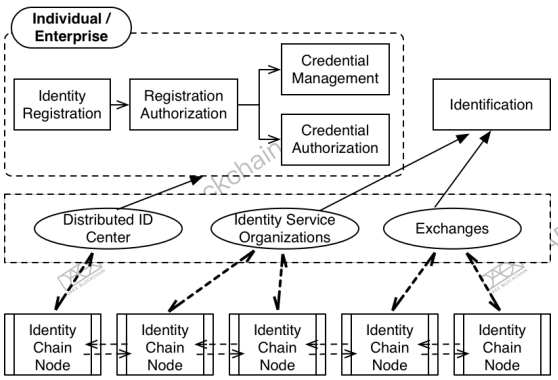


Figure 13: Identity Chain Structure

3.3.1 Design Principles

- Supports multiple participants and authentication methods
- Supports both strong and weak authentication
- Provides a trusted environment for identity authentication that can withstand security threats such as identity credential discovery, credential tampering, and account deletion
- Effectively creates a worldwide identity alliance consisting of digital asset exchanges, DApps and third-party identity agencies

3.3.2 Main Functions

The Distributed ID Center is responsible for the registration, management and authentication of user identities on the Clearing Chain. It operates within a trusted environment, allowing users to provide their credentials without this information being stolen. The identity authentication process faces various security threats. These include: password-guessing, service provider impersonation attacks, eavesdropping, replay attacks, session hijacking, man-in-the-middle attacks, denial-of-service attacks and malicious code injections. The system is designed specifically to guard against these threats.

Different levels of authentication credentials are given according to the authentication strength of each link in the identity authentication process. A user who just registered will have a relatively low-level authentication credential. However, after completing certain verification processes and becoming more trusted on the network, they may obtain higher levels of authentication credentials. The higher their level, the more digital asset services they will be able to enjoy. The identity management process consists of the following five components:

(1) Identity Registration

During the global identity registration process, users are required to fill in the necessary identification information and provide the relevant credentials. In order to simplify the process, the use of third-party identity service agencies is supported.

(2) Registration Authentication

Registration authentication is the confirmation of the newly registered identity. During this process, the identity data is encrypted and fragmented. After the identity is confirmed, the

Identity Chain registers only the encrypted identity information i.e. the identity fingerprint.

(3) Credential Management

After registration authentication has been completed, the identity's credentials are mapped immediately. This process involves the synchronization and binding of the identity's credentials to an address on the Clearing Chain. In addition, this section also provides identity life cycle management services, including the adding, updating, and canceling of credentials.

(4) Credential Authorization

With identities authenticated on the Identity Chain, users can enjoy cross-chain and cross-application services, both inside and outside of the ecosystem.

(5) Identification

After authorization has been completed, exchanges and third-party identity service organizations can use the Distributed ID Center's identification service to complete cross-validation and authentication of user identities.

3.4 Settlement Chain

The Settlement Chain connects the DAEX Wallet to public chains outside of the ecosystem. When a user wishes to bring their digital assets from outside public chains into the DAEX ecosystem, the DAEX Wallet's Asset Registration & Settlement Center facilitates the registration of these assets in the user's Custodian Account. These assets are subsequently "locked" into the DAEX ecosystem, with the custody of said assets transferred over to the Custodian Account. Users are able to "lock" and "unlock" their digital assets into and out of DAEX's custody as they please. In addition, the Asset Registration & Settlement Center also facilitates the mapping of assets into their Mapped Accounts on the Clearing Chain. Users can use these mapped assets for transactions in the DAEX ecosystem. At the same time, the Asset Registration & Settlement Center verifies the authenticity of those registering assets in the DAEX Wallet through multiple authentication methods. Finally, the center's distributed architecture and the dynamic nature of the accounts means that asset "freezes" caused by a single a point of failure are prevented.

Digital assets held in the Asset Registration & Settlement Center's Custodian Accounts are all stored in cold wallets located in offline safe houses. The system makes use of isolated networks on heterogeneous servers in order to monitor the digital assets independently. The data stored on the chain is synchronized at multiple points to ensure timeliness and accuracy. It is also checked in real time using a third-party block browser. The Asset Registration & Settlement Center's main responsibilities include:

- Dynamic creation and distribution of custodian keys
- Encrypted storage of private key fragments
- Asset receipt verification
- Asset registration and mapping
- Cross-chain exchanges of assets

Situated above the blockchain protocol layer, the DAEX clearing ecosystem facilitates cross-chain transfers of value. To some extent, it can be understood as a side-chain solution. Specifically, digital assets can be transferred from one blockchain to another blockchain, and at a later point in time, safely return from the second blockchain to the first blockchain. In this example, the first blockchain could be Bitcoin, Ethereum or another such chain while the second blockchain would be DAEX's Clearing Chain (which, in this scenario, acts like a "side-chain" of sorts). This clearing ecosystem also enables various types of digital assets to conduct asset transaction clearing and settlements that are more in line with business scenarios outside the main network.

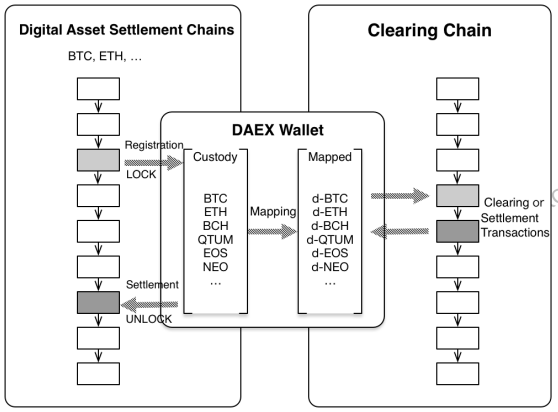


Figure 14: Registration and Settlement Diagram

4. Ecosystem Consensus

A consensus mechanism is a tool for reaching credible conclusions in an untrusted environment. Consensus mechanisms currently used by public chains have various problems. That is why DAEX has developed ASPoS (Accumulative Signatures for Proof of Stake): an efficient and secure consensus solution that uses minimal power. Blocks in ASPoS accumulate signatures from each validator node during the broadcast process. When enough signatures have been accumulated or a certain number of confirmations is achieved, the blocks will be accepted by the chain. The use of a VRF lottery in the algorithm guarantees the randomness of the nodes which can create blocks, while a deposit system resolves the nothing-at-stake problem. As an algorithm, ASPoS, which operates based on self-perspective, offers a high degree of availability on an asynchronous public network.

4.1 Basic Consensus

As the first implementation of blockchain technology, Bitcoin uses a mechanism known as the Proof of Work consensus. The core idea of this consensus is to maintain the integrity of the distributed ledger by using both economic incentives and node computing power competition. The result is that the block with the greatest workload wins the aforementioned consensus process. The node which has done the most work on this block receives an economic reward. The security of such a system depends on specially designed economic incentives that also achieve extremely high availability in an open network environment. At the same time, the complexity of the open network can lead to temporary bifurcation of the blockchain. These temporary bifurcations in turn lead to a decrease in system security and a lengthening of the consensus process. In order to balance availability and security, Bitcoin chose a longer period of time (10 minutes), which leads to a low efficiency (only 7 transactions per second). The high energy consumption of this process is one of the primary reasons for criticism levelled against the technology.

In order to solve this energy consumption problem, the Proof of Stake consensus system was released, which includes Proof of Stake 3.0, Delegated Proof of Stake, Casper and other components. In Proof of Stake, the probability that a node is granted the right to mine a block is based on its "stake" – a combination of a various factors including the amount of currency belonging to the node, the age of said currency as well as the size of the node's security deposit. There are two primary problems which seriously threaten the security of the Proof of Stake system: "nothing-at-stake" and long-range attacks. Casper solves the nothing-at-stake problem by instituting a mandatory security deposit system as well as the Slasher protocol, which punishes malicious behavior from validators. In addition, Slasher mitigates long-range attacks by using a checkpoint weak subjective judgement system. However, another problem arises when one considers that in the Casper algorithm, would-be attackers can predict which nodes will generate the next block in the chain. This leaves said nodes vulnerable to DDoS attacks. The Algorand algorithm solves this problem by selecting at random which node generates a new block in the chain.

During the convergence process, Casper's Consensus-by-Bet mechanism means that any given node's betting is based on the betting of other nodes. The convergence process therefore is heavily reliant on global betting information, increasing the difficulty of implementation and limiting availability. On the other hand, the selection of blocks by a node in the Proof of Work system is based solely on the information known by the individual block itself. This block selection mechanism reduces the difficulty of implementation and increases availability.

Taking the strengths and weaknesses of the aforementioned systems into account, DAEX has created the ASPoS consensus mechanism.

This is a combination of Casper's security deposit system, Algorand's lottery system and the Proof of Work self-perspective selection mechanism.

4.2 ASPoS Consensus

As a variant of the PoS algorithm, ASPoS achieves fork convergence during the block propagation process by selecting the block containing the smallest smaller lottery selection value and the greatest accumulative signature weight. The corresponding income distribution and penalty rules built into the protocol ensure the normal operation of the system.

4.2.1 Composition of Stake

When it comes to calculating stake, every PoS mechanism is different. Existing PoS algorithms use currency amount, currency age, deposit amount and various other statistics to calculate stake. ASPoS's stake system uses a combination of deposit amount, node activity and the Clearing Value Factor (CVF).

A validator node's CVF is calculated based on its past clearing performance and trustworthiness. A node's CVF affects the final reward it obtains. Therefore, ASPoS can also be called CVF-POS, in that it promotes the health of the ecosystem by encouraging each user to maintain a positive CVF.

$$S = C\sum_{i=1}^{n} F(e_i)$$

S represents the validator node's stake or weight. C represents the validator node's deposit amount. The *F* function calculates the node's trust value. e_i represents the i^{th} user's Clearing Value Factor. *n* represents the total number of trustworthy users.

4.2.2 New Block Creation

There are four types of nodes in the block system: regular nodes, validator nodes, quasi-creator nodes and creator nodes. A regular node becomes a validator node by paying and locking in a deposit. During the block creation process, the most active validator nodes are selected to become quasi-creator nodes. Quasi-creator nodes then go through a lottery process, during which one quasi-creator node is selected at random to become a creator node. The quasi-creator nodes not selected become validator nodes once again. The creator node then creates a new block and broadcasts it. The validator nodes (the creator node also acts as a validator node) then validate the new block. If the validation is successful, then the block is broadcast after being signed. Otherwise the block is discarded. Regular nodes have the same functions as validator nodes except that they cannot sign blocks.

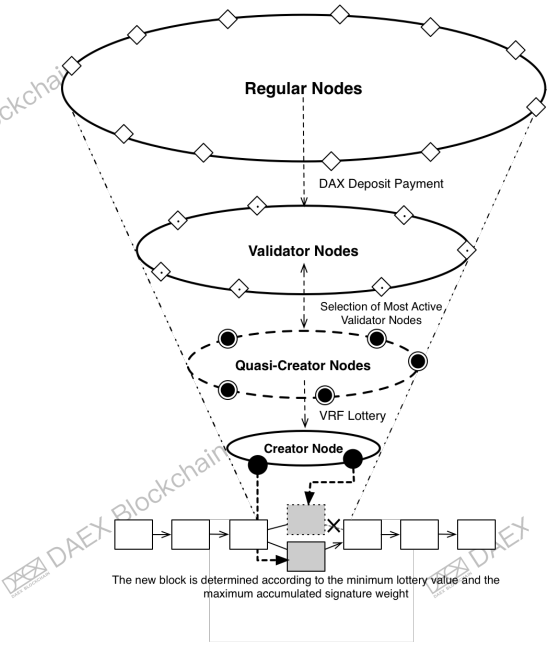


Figure 15: New Block Creation Using ASPoS

A validator smart contract located on a specific address is used to keep track of validator nodes. Regular nodes can become validator nodes by sending a deposit to this contract. The validator node can also apply to withdraw its validator node status by sending a message to the contract. After the withdrawal request is approved, the original deposit is returned to the specified address after a period of thawing.

The transactions in the N highest blocks on the chain are counted, with the total number of all transactions submitted by each node being added up. This total is then used to rank each node by their activity levels. The top K nodes are then selected to become quasi-creator nodes.

ASPoS uses the VRF lottery function to select the creator node for the next block. The randomness of the lottery prevents node bribery,

DDoS attacks and other problems. The lottery function is constructed using the hash of the previous block, the height of the current block, the lottery round number and the node stake. Each quasi-creator node submits its own private key to the VRF function in order to calculate its selection value. If the selection value of the quasi-creator node is smaller than the current selection value threshold, then the quasi-creator node becomes the creator node. Due to the random nature of VRFs, there may be multiple or no quasi-block nodes that satisfy the selection value threshold. In the case of multiple quasi-creator nodes satisfying the selection value threshold, each quasi-creator node will generate a block with its VRF function value included in said block. It will then sign the block and broadcast it. After the other nodes receive these blocks, the block with the smallest selection value will be selected for validation. If no quasi-creator node satisfies the selection value threshold, the next round of lottery is performed at the same block height and the selection value threshold is modified.

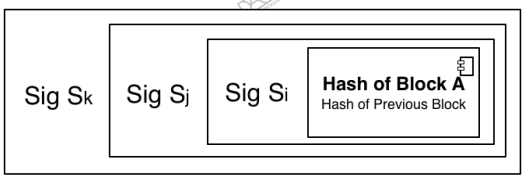
VRF(Hash(Block(R)),H,N, S, SK) < P

Please see above for an example of the VRF lottery function. H represents the current block height. N is the lottery round number. S is the stake of the node in question. R represents the local physical random factor added to the created block by the previous block creator node. Block(R) is the previous block.
SK represents the node's private key. P is the selection value threshold.

There is a higher probability that validator nodes with higher stakes will be selected in the lottery. In order to increase the randomness of the lottery process, each creator node adds the locally obtained random factors S and SK when creating a new block. In the case of multiple nodes being chosen to act as creator nodes, the block created by the creator node with the smallest selection value will be selected for propagation, with all nodes finally reaching consensus. In order to ensure the smoothness of block creation and propagation, the system will adaptively adjust the selection value threshold P at regular intervals.

4.2.3 The Consensus Process

Each validator node adds its signature to the hash of the block it receives with the smallest selection value. The block is then broadcast. If the node in question is a regular node, it only performs the block selection process and broadcasts said block. Validator nodes, on the other hand, broadcast both the block and the accumulated signature sequence on the hash of said block. These are broadcast separately. Because the size of each signature is relatively small, the accumulated signatures do not put excessive communications strain on the system. If a node receives different accumulated signature sequences of the same block and the accumulated signature weight of the new sequence is greater than the local one, the new sequence overlaps the local sequence. Otherwise, the new sequence is discarded. The schematic diagram of accumulative signatures is shown in Figure 16:



The accumulated signatures of Block A consist of the signatures from three validator nodes: Si, Sj and Sk. The accumulated signature stake of Block A is the sum of the stakes of the above three nodes.

Figure 16: Accumulated Signatures in ASPOS

When the cumulative weight of the new block reaches a certain proportion or when the time since the creation of the latest block reaches T, the activity ranking and lottery processes run again, creating a new block at the next height. A list of validator nodes that have signed the previous block is added to the newly created block (in the same sequence in which they signed it). This information will be used as proof by the signing nodes to obtain their rewards.

A creator node that signs and creates multiple blocks at any given height is called a dunkle node. Blocks created by dunkle nodes are called dunkles. If the current block with the lowest selection value is a dunkle, it is replaced by another block created at that height. Proof that the block is a dunkle is sent to a validation smart contract. After the validation smart contract validates the proof, the contract uses this as evidence to punish the dunkle node. This is collected on a certificate of penalization. The certificate of penalization is then recorded on the new block at the next height.

Each node completely ignores blocks whose timestamps differ from the local time by more

than a certain amount. They also ignore new blocks whose creation time differs to that of the block at the previous height by more than the system cycle.

4.2.4 Dealing with Forking

As was previously mentioned, when nodes encounter multiple blocks at the same height, the block with the smaller selection value is chosen. However, when a node encounters a block with the same selection value, the block with the highest accumulative signature weight is chosen, and the others are discarded. The selection values are compared between blocks at the same height with the same lottery round number. If a node encounters a legitimate new block at the same height as the locally cached block but with a greater lottery round number, the dunkle data set of the new block is checked. If the dunkle data set includes the node which created the locally cached block, the locally cached block is replaced by the new block. The node then signs the block (if it is a validator node) and broadcasts it.

4.2.5 Rewards and Penalties

There are 5 types of rewards given to nodes: rewards for creating blocks, rewards for adding proof of penalization, rewards for adding proof of revenue, rewards for adding proof of idleness as well as rewards for participating in block validation. When a block has been confirmed N times, the reward in said block's reward certificate can be used by its corresponding validator nodes and creator node. When a validator node exits the validator node set, the validator node's rewards and penalties are also settled.

Both nodes that record proof of penalization and nodes which record proof of revenue on new blocks receive a reward proportionate to the block's accumulative signature weight. In order to encourage validator nodes to perform timely validation signatures on the blocks they receive, their rewards are reduced exponentially the further behind the validation sequence they are. In order to prevent validator nodes from going offline or ignoring the propagation process, when the number of confirmations a certain level but the accumulative signature weight has not reached a minimum threshold, the validator nodes that have not signed the block are punished. This proof of penalization is then recorded on a certificate of idleness.

Every time a certain number of blocks have been propagated, the system will half the rewards. The total mining volume of DAX tokens is 1.39 billion.

4.3 Cheating Analysis

4.3.1 Double-Spend Attack

A node that wants to perform a double-spend attack needs to be selected as a creator node and then create multiple new blocks at the same time. But in the DAEX system, if multiple new blocks from the same node are detected during the propagation process, said node will be reported as a dunkle node and lose its whole deposit.

4.3.2 51% Attack

Due to the pseudo-randomness of the VRF lottery function and the randomness of the role of the previous block's input in said function, even if 51% of all nodes are controlled by one party, if one of these nodes is not selected as a creator node it is difficult to launch an attack. If all these nodes refuse to sign the new block, it will result in their deposits being forfeited.

4.3.3 Long-Range Attacks

There is a limited period of time between blocks. Blocks created outside of this timeframe will be treated as invalid blocks that cannot be propagated through the system. This prevents long-range forks being accepted by the system, making it impossible to carry out long-range attacks. At the same time, the block with the smallest selection value is chosen to be propagated. Therefore, a user who has just entered the system can determine which branch is the valid one simply by knowing the genesis block.

4.3.4 Isolation Attack

According to the rules of the lottery system, if some nodes are isolated from the system for a long period of time, this group of nodes will form an independent branch. When the number of confirmations reaches a certain amount, validator nodes whose accumulated signatures have not reached a certain proportion (p%) of

the confirmation number are penalized. Therefore, if someone wants to carry out an isolation attack, they must combine the validator nodes that account for at least p% of the total validator stake, while at the same time separately validating the blocks on both the isolated branch and the main branch. Only then can isolated propagation be achieved. Apart from the aforementioned scenario, it is inevitable that in the process of carrying out an isolation attack, the nodes responsible will be penalized for a lack of signatures, and the attack will therefore be discovered by the system.

5. Ecosystem Governance

The three essential components for a successful blockchain project are its proposed technical solution, the structure of its ecosystem and its governance model. The recommended ecosystem governance model combines a governance protocol on the chain with a collaborative consensus mechanism under the chain.

The purpose of the chain governance protocol is to empower all users of the ecosystem to participate in the issues they care about and to make decisions by voting. However, the current voting systems based on tokens or token holders are imperfect, sometimes even leading to the collapse of the entire ecosystem. This is due to a lack of knowledge on the part of the voters or simply indifference towards the voting process itself. Similarly, the voting process should avoid the emergence of one powerful entity which decides all, whether that entity be a users with a lot of tokens, the founding team or simply a miner—conflicts of interest are bound to arise. Therefore, DAEX aims enhance the flexibility and fairness of the system from three angles: token time value, value sequence management and dynamic seat management.

Collaborative consensus is a model of governance that has achieved off-line saturation. It not only includes technical components such as network monitoring, risk tracking and code review, but also collaborative mechanisms such as ecosystem fuses and risk funds. In the DAEX ecosystem, clearing validators maintain a constant value in the system by validating the legitimacy of transactions. There is also no management overlap between applications. If there is a problem with one application, its offline management mechanism can be repaired in time without affecting the normal operation of other applications in the ecosystem.

Another key aspect of the DAEX governance model is its compliance. It can therefore avoid regulatory uncertainty while also allowing mainstream organizations to legally participate in the world of digital assets. The blueprint of the DAEX ecosystem is based on a hierarchical structure of data and assets, creating a regulatory space for the separation of transactions and clearing.

Although the robustness of the blockchain has been tested, holistic security of a digital assets ecosystem requires much more. In order for an ecosystem to be secure, it requires an effective set of mechanisms as well as the focus and attention of the ecosystem's builders, users and regulators. Some users, however, prefer to not have such strict security requirements. Therefore, the DAEX clearing ecosystem aims to both reduce the frequency of governance interventions and improve the resilience of the ecosystem through the optimization of the following:

- Algorithmic Security:
  Multiple cryptographic algorithms in the ecosystem have been optimized, including threshold signatures, the pseudo-random number generator algorithm, VRF and more.

- Protocol Security:
  ASPoS consensus offers greater security and effectiveness. Its clearing and settlement protocols are safer, more efficient and less expensive than other cross-chain technologies.

- Implementation Security:
  The ecosystem supports multi-party audits of smart contracts, formalized validation and comprehensive testing.

- Management Security:
  The ecosystem's blockchain-based risk management system is custom developed, with off-chain data saving by physical isolation and hierarchical permissions management for organizational wallets.

6. Roadmap

Q2 2018:
Overall design of the clearing ecosystem, including the ASPoS consensus mechanism

Q3 2018:
Clearing Value Factor (CVF) and wallet solution based on a trusted computing environment

Q4 2018:
DAEX Fund report, token plan (clearing-as-mining), node deployment and governance model