DAEX：分布式数字资产清算生态
技术白皮书

contactus@daex.io

摘要

数字资产所描绘出的亮丽曲线，在信用和安全面前却常黯然失色。当下的数字资产行业存在着诸多缺陷，市场流动性、资产价值、生态秩序等内生诉求有待进化。本文介绍了DAEX清算生态的分层架构，以及清算链、多资产钱包、身份链在内的产品解决方案，定义了异步公开网络下的ASPOS价值共识机制，并期望建立一套透明安全的治理机制，以打造未来数字资产交易基础的全新清算网络，实现安全、可信、开放的生态愿景，促成人人见证价值。

1 生态概述

1.1 背景

（1）数字资产安全事件频发

数字资产发展至今，投资者或交易所遭受黑客攻击的事件屡见不鲜，尤其是近期数字交易所 Coincheck 遭受黑客攻击，使得主流数字资产价值均出现不同幅度的下跌。这些风险事件凸显出的数字资产市场所面临的安全与信任问题已经迫在眉睫。

（2）行业清算设施不完善

区块链 3.0 时代，需要的是基于业务场景驱动的区块链底层协议重构，从而实现具体领域的重量级产品。当下基于区块链技术记账的数字资产行业，缺乏清晰的责任边界和足够的透明与安全度，易遭受恶意操作和意外失窃。

（3）安全可信基础设施匮乏

数字资产生态的基础设施中，改变清算机制是关键。常规的数字资产清算机制缺乏拓展性，对于多市场及丰富的衍生品与智能资产市场缺失穿透和统筹能力，必要的生态清算设施将为数字资产的各类活动提供安全可信的服务。同时，优质的数字资产钱包需要基于区块链技术展现其背后的可靠性，既能解决市场痛点，又可以进化数字资产的交易关系，成为一个真正令人放心的资产安全管家。

1.2 生态设计

DAEX 所立志建设的分布式数字资产清算生态，从构建一个基于区块链的多资产清结算底层协议出发，通过资产与交易的解耦、通证与权限的赋能，重铸数字资产交易的基础架构，多方面保证清算生态的安全性和灵活性。这使得 DAEX 能为整个数字资产生态服务，包括承担数字资产联通节点的交易平台和普通的数字资产用户，让更安全、更高效的分布式资产登记和清结算业务模式成为可能。

1.2.1 价值链条

DAEX 生态，以优化并完善数字资产交易的上下游产业结构为方向，覆盖了从身份认证、资产登记到资产清算与结算的全链路价值服务过程。

图 1：清算生态价值链

将交易、清算、托管进行分层，是 DAEX 团队在数字资产行业实战多年，汇聚互联网技术专家、计算机科学家的聚合知识后共同得出的最佳解决方案。在抛去极致追求中心化的偏执后，通过将分布式交易平台和去中心化清算结合的实践，创造人人可以见证的价值互联网络。

1.2.2 生态组件

DAEX 生态以多资产钱包为链接器，链接起身份认证中心、资产清算中心和登记结算中心。清算中心由去中心化的清算链通过区块链的安全可信机制提升数字资产价值转移过程的信用度，又基于标准化的清结算协议支撑开放的清算生态。

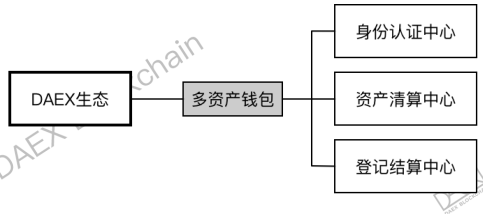

图 2：清算生态组件

清算链具备传统公有链的各项技术特性，并针对性地对共识机制、交易加密、隐私保护等关键技术进行优化升级。同时基于清算市场，细分了数字资产领域身份认证、登记映射、兑换支付和财富管理等的具体需求，与身份认证中心和登记结算中心一同提供充分兼容现有交易模式的基础架构，并可支撑未来业务发展的清算即服务（Clearing-as-a-Service）解决方案。此外，为了肩负健康交易生态的建设，DAEX 还将通过稳定可审查的智能合约拓展金融清算场景，在清算链层加入去中心化的智能数字资产和数字资产期权期货等金融衍生品，使开放的清结算体系蕴藏无限的自进化空间。

基于清算链衍生出的分布式数字资产钱包是用户参与自清算的工具，实现资产管理并丰富了兑换支付场景。基于门限签名、全局身份证书、可信计算环境等技术与治理机制，为不同类型用户提供功能完善的数字资产管理服务，例如交易平台的企业级服务产品，注重权限分离和风险控制；用户资产服务产品，注重资产多样性和私钥的安全性。

1.3 能力模型

开放式的生态结构可以满足多类实体通过协作完成信息处理与价值转移。而面向每一层级的对象，DAEX 将提供所需的基础能力，如基于清算链的数字资产映射和清算即服务、依托多资产钱包的分段密钥与可信授权机制以及身份认证中心的凭证生命周期管理。

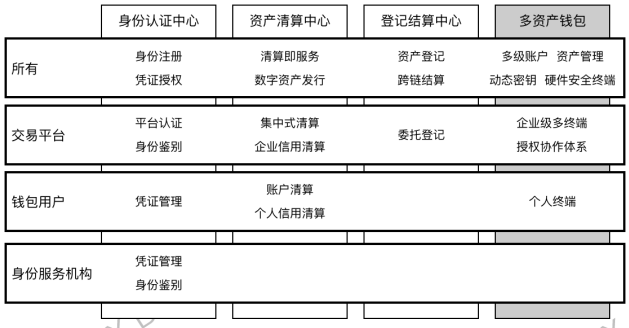

图 3：清算生态能力模型

2 生态方案

2.1 生态架构

清算链是清算生态的核心基础链，其应用层支持复合式的跨链业务结构，可连接身份链和结算链在内的多个功能链。同时，借助于交易平台的分级侧链，满足高并发需求的技术指标。DAEX 多资产钱包是分布式资产管理和去中心化清结算服务的实现载体，实现标准化的清算即服务。而基于清算链的基础设施，将同步建设物理隔离且逻辑独立的身份认证中心和资产登记结算中心，从而构建完善的清结算价值链和生态治理体系。“多中心”分级分层的生态架构是为了解决区块链协议自身存在的局限，并保障分布式网络能够安全可信地与外部信息进行交互。其中，身份认证中心和资产登记中心分别匹配于身份链和结算链。与此同时，为提高资产和操作的安全等级，还将采用多级多样的认证技术并尽量降低独立中心的单方信任程度，转而由基于分布式账本和生态共识的中立技术实现生态的信用背书。

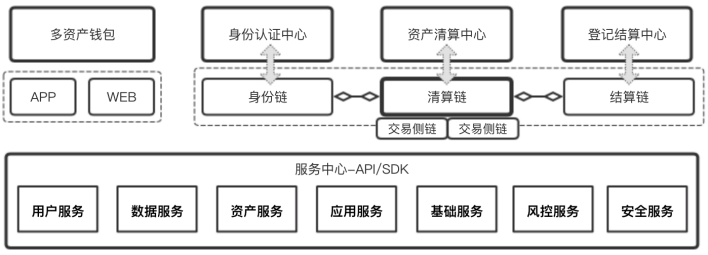

图 4：清算生态架构

2.2 账户体系

清算生态的账户体系将建立起资产与所有者之间的关系，也是分布式账本的核心环节。对于每一位参与者来说，创建属于自己的清算账户是享受分布式清结算服务的第一步。DAEX 生态中，账户体系以所有者为核心，记录账户的各类资产数量与交易事件，而可扩展的账户结构将支持灵活的业务模式。同时，每一个账户都是经认证的可信身份，数字资产托管于可控的安全环境，用户拥有数字资产主权。也正是该账户体系的存在，使得数字资产可以通过隐私保护策略有了非公开的实名身份，为资产确权和找回提供支持。

在清算生态里，按照使用者类型来分，账户可细分为个人账户和机构账户，其中机构账户包含普通机构账户和交易平台账户。一般来说，机构账户是适合高频交易或多级授权的企业型账户，如做市商和基金机构，而个人账户是支付兑换的首选方式。交易平台账户作为特殊的机构账户，是实现信用清算的重要部分。

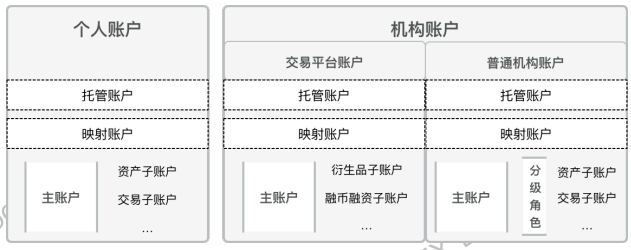

图 5：清算生态账户体系

从数字资产状态来分，每个账户又可衍生出相应的托管账户和映射账户。托管账户展示登记资产的托管状态，公开监督。映射账户是资产登记后清算链记载的实际有效资产。托管账户依频次更新与结算，而映射账户可根据使用场景与业务需求拆分为各类子账户，

通过子账户间资产调配实现不同业务策略，如资产账户和交易账户间的隔离管控。普通机构映射账户通过分级角色嵌入授权审批机制；个人用户通过创建关联于交易所的子账户，实现同一身份下的多交易平台分户操作；交易平台映射账户可支持平台内部用户子账户的交易清算归集上链，并基于金融产品子账户实现风险阻断。

清算生态中，账户的一般结构包含全局身份标识、自定义名称、账户类型、账户状态、清算地址及资产列表，其中资产列表是数字资产品种、托管地址、余额等关键要素的多维数组。

全局身份标识	清算地址	账户名称	账户类型	账户状态	交易平台标识	资产列表 资产种类、余额、*托管地址

图 6：清算账户结构

账户的交易事件则包含转出方、转入方、资产类型、发生额、事件时间、事件类型、交易渠道、交易哈希、区块高度等流水信息。

转出地址	转入地址	资产类型	发生额	事件时间	事件类型	渠道	*交易哈希	*区块高度

图 7：清算交易事件结构

2.3 业务模型

数字资产行业自诞生起便是全球化的金融世界，链接各种区域化的金融产品。当前，用户的数字资产由不同类型和功能特性的数字资产钱包或交易平台管理并记账，每个工具各自完成对资产的清结算过程，信息透明度和资产安全的权责由去中心化的公链节点或中心化的运营主体承担，跨平台的数字资产清结算同时受限于业务模型和技术瓶颈。DAEX 通过分布式清算解决集中化交易的资产信任问题，结合中心化和去中心化交易各自的优势，为数字资产交易平台和投资者提供一整套适用于数字资产行业的安全系统和资产保险箱，兼顾公平、合规与效率。

当下的传统金融市场，是由银行、登记结算公司、交易所、券商、基金公司等共同组成的成熟商业生态，而数字资产市场的结构性发展历程也会相似，进一步转变为多个专职的组织，只不过这些组织可以是去中心化或者分布式的社区形态，由技术创造信任，并降低与隔离财务和道德风险，实现：

（1）数据真实可信

数字资产分布式清结算阻断数据篡改造假的风险，只有数据背后资产的所有者才能有权发起数据“变更”操作。

（2）资产实时登记

数字资产交易转让后通过标准清结算过程保证数据变更能够及时同步到所有节点，实现跨域资产的统一登记。

（3）个人隐私保护

在系统内部与智能合约中加入隐私保护策略，基于资产关联方的显性因子及链上身份的代号化，可加固个人和交易平台隐私数据的保护。

DAEX 清算生态的本质是实现交易数据与数字资产分离后的分层体系，通过架构分层与数据分片，使交易平台成为专业的交易服务机构，而所有的数字资产由托管机构完成登记，交易清结算由去中心化的清算链保障。托管清算的基本业务流程如图 8 所示。

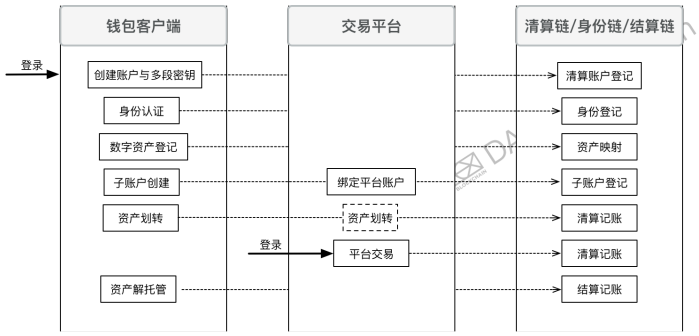

图 8：托管清算基本业务流程

为了保证交易平台的业务连续性，分布式清算过程可分为面向交易的托管清算和面向服务的信用清算，并逐步升级为人人清算。其中：

- 托管清算是分布式清算的主要记账方式。
- 信用清算是未来支付兑换的重要清算业态。
- 信用清算不受限于资产登记过程，对交易的过程风控、信用等级和平台保证金有一定要求。
- 人人清算使得 DAEX 生态的每一位用户可通过多种途径参与并验证数字资产清算的共识同步过程，并有机会获得清算奖励。

2.4 生态协议

统一的业务协议是实现清算即服务等业务范式的基础，需要适应多样化的场景需求，通过丰富的抽象业务模型，满足跨平台的链上数据共享。因此，清算生态对数据的记录方式要足够的通用、标准且易于构建。同时能够有效表示各种结构化信息，并具备可定制的开放协议，从而实现随着业务范围拓展所需的跨平台与跨链要求。

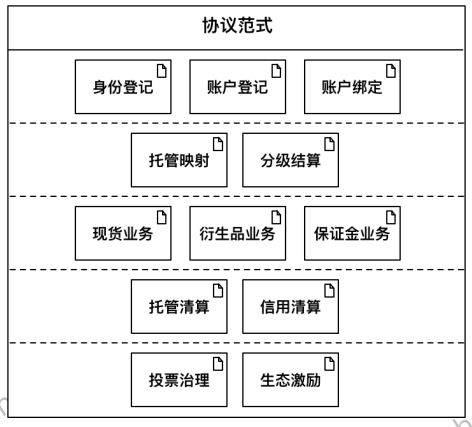

图 9：清算生态基本协议

生态协议规范了清结算账本中保存的业务信息域与格式、业务过程中产生的业务状态、业务状态变更的触发方式与条件以及所涉及的更新信息等。由于各参与者凭借身份账户签署基于智能合约实现的业务协议，所以其执行过程得到了区块链系统客观的技术背书，包括协议在每个节点上被一致执行，即得到业务主体认可；协议的执行过程被准确记录、最终结果无法篡改，即被执行的业务事实不可抵赖。

3 生态结构

区块链技术所具有的去中介化、不可篡改基因，为 DAEX 生态的价值积累与流通提供了基础的解决方案，但要实现一个分布式自治的社区生态，除了基础平台应具备良好的性能，即可以实现匹配业务需求的吞吐量，还需要全生态基础设施通过优异的互操作性达成整体“共识”，包括利用分布式文件系统改善数据存储性能、通过共识协议的优化适配清结算模型、基于多资产钱包提升数字资产工具的安全性和易用性、以及提供业务导向的服务化接口支持快速接入等解决方案，这

使得清算生态的产品组合具备了以下优势：

（1）更健壮

避免了用户私下保管、传输完整密钥的可能性，并以用户为核心，基于链上的多方共识，在分布式账本上完成高效记账。

（2）更丰富

延伸区块链的可扩展性，支持多资产的快速交易；同时，清算链的上层基础服务，能够保留原有的交易深度，并提供衍生品和智能资产的丰富业务生态。

（3）更可靠

多资产钱包采用的分段密钥机制与可信计算环境提升资产安全性；同时基于清算价值因子的共识机制保证了公平共享的价值激励与对欺诈行为的惩罚权威。

3.1 清算链

清算链为数字资产交易平台等提供接口支持，使得个人客户、机构客户可以延用数字资产钱包中的身份认证信息进行支付兑换操作，并完成核心智能合约的资产清结算过程。此外，可解耦与灵活配置的功能组件、与清算链的智能合约引擎一起能够适应多种场景需求，满足数字智能资产的各种行为活动。

就清结算业务而言，清算链的必要性在于它赋予那些不带智能合约的原生链于原子性。通过双方的协议结果，实现带冲正能力的清结算合约，保证资产交割结算的原子性。清算链双向锚定托管资产和映射资产，仅由用户确认数字资产的流动，同时清算生态共建的交易平台联盟维护且提升了各参与方的诚实度。清算链“矿工”作为清算见证人，对清算链当前的数字资产状态进行检验和监控。当它们收到交易请求时，会同步执行清结算协议以确保对结果达成真实的一致性。诚实矿工在清算链中的参与程度越高，系统的整体安全性也就越高。

3.1.1 设计原则

- 智能合约是清算生态的主要价值承载方式。
- 清算价值因子是节点验证激励的重要元素。
- 升级 POS 共识机制，提升交易性能与数理随机性。
- 提供数字资产交易的定向加密方案，部分场景仅支持清算关联方的查看和交易验证。
- 满足监管支持和审计实现的要求。
- 清算链的数据一致性是核心诉求，能在紧急情况下通过有效的治理机制避免分叉。

3.1.2 产品结构

清算链所实现的区块链基本功能，包括密钥管理、智能合约、账本数据等，并提供对节点、区块信息的监控。具体分为如图 10 所示的三层结构。

（1）底层协议与系统支撑层

作为清算链的底层基础设施，不仅定义了区块链的区块结构、存储类型、账本模型、操作指令等标准与协议，同时兼容云服务技术体系，且可利用容器技术实现快速部署和

配置管理。

图 10：清算链结构

（2）核心模块层

核心模块层的数据交互通过内部数据交换协议实现，各组件功能独立且解耦，同时数据与逻辑分离，从而实现模块组件的可插拔性与可扩展性。

共识组件：共识组件主要完成交易的广播、排序、执行和共识等环节。在 POS 保证金机制之上，融入清算价值因子激励和可验证随机函数。

账本与存储组件：账本信息的持久化基于成熟的 NoSQL 数据库实现，而 KV 数据格式提供了简洁快速的存储范式，存储信息具备不可篡改性。

P2P 通讯组件：区块链节点间建立 P2P 通讯，可发现动态新增节点并同步区块信息。

智能合约引擎：基于虚拟机的图灵完备的执行引擎，能够对智能合约进行封装与兼容。各节点需要保证执行状态和结果的共识。通过编写适用于不同业务场景的合约逻辑，实现清算链的可编程性。

隐私保护组件：支持仅交易相关参与方可见的交易级加密，与交易无关的非参与方仅能获取、验证原有交易内容加密后的哈希值。

节点管理组件：支持节点权限的动态配置与验证。节点分验证节点和普通节点，前者参与共识过程。

生态治理组件：作为完善生态治理机制的技术解决方案，避免因区块链技术处于早期阶段由未知错误带来的生态破坏。清算生态是一个长期稳定的可持续生态，基于生态社区设定一些特殊角色功能，结合分布式治理结构，在链外协商一致的情况下使清算链具备应急处理能力，解决恶意破坏、软件 BUG、硬分叉等突发情况。这使得可运维性在区块链生态与社区自治过程中得以表现，即通过参数化设计使生态具备自愈能力。

跨链组件：支持多链及侧链账本的信息交互，数据与业务逻辑隔离，包括交易清算子链、身份链及结算链。

（3）生态服务层

生态服务层是基于区块链底层协议和核心模块的具体实现与场景对接，提供 API、SDK 等完整工具集。

RPC 组件：处理发送至节点的 RPC 请求，是节点数据交互的入口。可通过规则校验过滤无效消息，减轻共识负荷。同时，通过灵活配置 RPC 服务，可以实现负载均衡，并可定制各种传输协议规范与场景接口，以满足各类清算及衍生服务。

浏览器组件：实现清算链区块浏览器的

基础。提供区块信息、交易信息、节点状态、网络状态等信息及各类统计结果的直查询。

合约管理组件：提供智能合约的模块化管理，包括合约创建、测试、部署、升级和模板编辑。

生态应用组件：清算链是面向业务过程的区块链产品，通过生态应用组件实现高效的身份、清结算、资产映射与发行等应用功能。

3.2 多资产钱包

清算生态的多资产钱包（DAEX 钱包），将分别满足企业与个人用户管理数字资产的要求。同时，该钱包也是数字资产的身份凭证，通过身份授权，可逐一接入 DAEX 生态内的各交易平台。

当下的数字资产钱包，因用户卸载或重装 APP、应用商店产品条例变更、用户忘记助记词、丢失 keystore 文件等情况导致的用户资产丢失事件时有发生。DAEX 钱包提供的多层安全防御体系，从用户行为安全、手机安全防御、密钥安全管理、多因子验证等多个维度保障数字资产的安全，防止资产被盗。同时，通过分段密钥机制有条件的解决了因密钥遗失导致的资产丢失问题。

易用性是 DAEX 钱包的一大亮点，这个亮点首先体现在客户分层上，为机构与个人用户分别打造的产品功能和客户端，使其成为适应不同角色的资产管家。而基于先进的清算链资产映射，它又为数字资产的管理和收发提供了快捷通道。同时，通过钱包即身份的方式嵌入交易平台，有助于降低交易成本、缩短资产转移的确认时间。此外，DAEX 钱包将会提供硬件钱包入口，由其派生的软件密钥具备端到端的安全基础，通过防抵赖签名可建立数字世界的高强度信任。

3.2.1 设计原则

- 定位于多资产管家，支持各种主流派系数字资产。
- 通过统一身份标识归一化管理账户资产，解决不同区块链有各自的账户体系和技术架构的集成难题。
- 多段密钥分散保护用户资产，用户拥有资产的绝对交易权。其它密钥片段托管机构均不能独立恢复密钥或发起资产交易。
- 具有独立且适用于交易平台的专业资产管家平台，嵌入企业级功能属性，如多级授权和业务协作。
- 一站式的数字资产管理工具。满足存储、支付、兑换、第三方服务等场景化需求，同时拓展数字资产增值功能。

3.2.2 产品结构

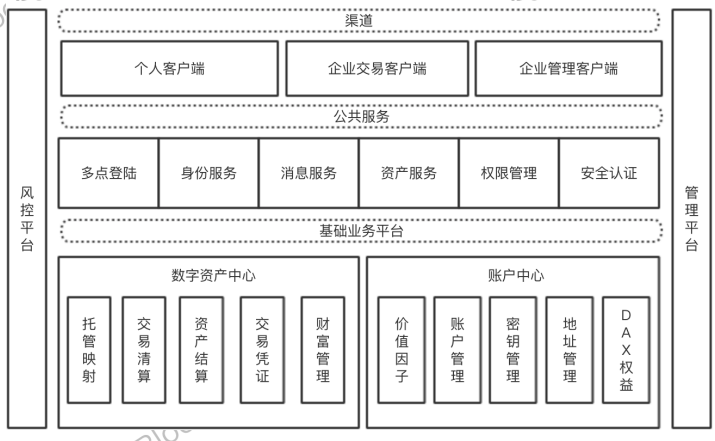

图 11：多资产钱包产品结构

（1）基本功能

钱包资产地址随机生成，用户可自定义管理各种映射资产。生态内的资产转移过程通过清算链的映射资产信用记账完成，且支持基于用户自定义 ID 的资产转移。分场次的结算过程依据风险等级适配相应的分层策略，支持动态口令、生物信息、物理信息在内的多组合交叉验证。每次结算校验时，根据清结算流水进行余额双向核对，确保清算链数据和钱包资产账户的一致性。风控平台提供数字资产事前、事中风控体系，从身份与设备识别、风险监控、动态策略等多个维度保障用户资产，辅助过程性监管。

独立的个人与企业级钱包，能够满足便捷的单人操作和流程化控制的多方操作需求。同时，通过创建不同等级的子账户，实现快捷的跨平台跨业务资产财务管理。DAEX 钱包致力于打造一站式的数字资产财富市场，包括衍生品服务、优质理财、数字资产投顾、融资融币等金融工具。此外，钱包还可提供丰富的数字资产应用生态，如行情资讯、第三方 DAPP 等服务。

该钱包也集成了 DAX 通证的各种权益，使持有 DAX 的用户可以充分参与清算生态的建设，包含信任投票与获取清算见证奖励。

（2）分段密钥

用户清结算账户采用三段密钥机制（用户端、服务端、托管端）实现数字资产的安全控制，其中私钥分段密文存储，密钥片段多方多介质存储。依托于可信计算和通讯环境，密钥机制涵盖了密钥创建、私钥切分、私钥片段加密存储、密钥安全传输、密钥本地恢复与签名在内的全流程。因此，结合权限管理策略，可实现不同场景的安全需求。

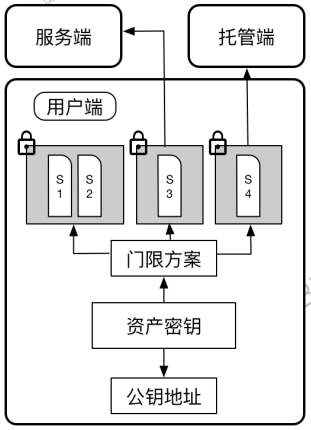

图 12：分段密钥机制

3.3 身份链

为了在数字资产交易流转过程中提供完整、合规、可信的身份服务，基于身份许可链的分布式身份认证中心（Distributed ID Center）实现了全局视角的身份管理，包括身份注册、认证登记、身份凭证管理、身份鉴别与授权等在内的协议和规范。DIDC 为每位用户创建的清算链身份标识，通过身份信息符号化，实现链上流通时的可信匿名，是跨交易平台价值流通的身份基础。

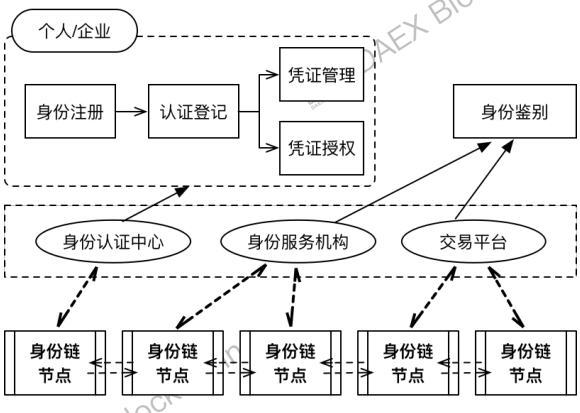

图 13：身份链总体结构

3.3.1 设计原则

- 多参与主体、多认证方式、多信息采集渠道。
- 支持强弱认证在内的分级确信认证等级。
- 提供身份认证的可信环境，能够抵御身份凭证发现、更新、注销等环节的安全威胁。
- 与数字资产交易所、DAPP 及第三方身份机构共建全网身份联盟。

3.3.2 主要功能

身份认证中心将协助身份链完成身份管理过程。其在可信环境运行，能够支持用户安全准确地提供身份凭证信息，避免被他人恶意获取。同时，身份认证过程中会面临着攻击者不同攻击手段造成的安全威胁，需部署必要的安全技术来防范认证通讯过程中的在线猜测、服务提供方扮演攻击、窃听攻击、重放攻击、会话劫持、中间人攻击、拒绝服务攻击和恶意代码注入攻击。

根据身份认证过程中各个环节的认证强度，定义不同级别的身份认证确信等级，即用户注册时申请不同的注册确信等级，对应关联的用户身份凭证后，可获得不同的凭证确信等级。越高的确信等级，可享受的数字资产服务更丰富。身份管理过程主要包含以下五个环节：

（1）身份注册

全局共享的身份注册服务，使用者需填写必要的身份证明信息，同时提供相关的凭证材料。为了简化流程，支持第三方身份服务机构的接入注册。

（2）认证登记

认证登记是对注册身份的校验，并完成身份数据的加密与分片持久化。认证通过后，身份链仅登记加密后的身份信息，即身份指纹。

（3）凭证管理

完成身份认证登记后，身份凭证的映射是立即执行的,即完成清算链地址与身份凭证的同步绑定。该环节提供了凭证添加、更新、注销等身份生命周期的管理服务。

（4）凭证授权

基于身份链的可信认证，实现生态内外的跨链跨应用的身份共享服务。

（5）身份鉴别

交易平台和身份服务机构经授权后可使用身份鉴别服务，完成对用户身份认证信息的交叉验证及认证反馈。

3.4 结算链

数字资产登记中心（Digital Assets Registration Center）实现结算链数字资产的登记托管与清算链上的资产映射。资产映射通过跨链锁定，支持各种数字资产的自由发行与流通。同时，通过多种认证技术与策略核实“登记人”真实性，以分布式架构和动态账户提升价值管理的安全性，避免单点故障导致的资产“冻结”。

资产登记中心的数字资产托管钱包均为冷钱包，位于离线安全屋。各类数字资产采用

隔离网络在异构服务器独立运行与监控。链上数据通过多点同步保证时效性和准确性，并实时与第三方区块浏览器双向核对。DARC 的主要职责包括：

- 托管密钥的动态创建与分配
- 密钥碎片加密存储
- 资产接收核验
- 资产登记与映射
- 资产跨链互换

DAEX 清算生态在区块链协议层之上，实现了跨链的价值转移，在某种程度上可以理解为一种侧链解决方案。具体来说，就是数字资产可从第一个区块链转移到第二个区块链，并在之后的某一时刻从第二个区块链安全返回到第一个区块链，这里的第一个区块链就是比特币、以太坊等结算主链，第二个区块链就是清算链这个“侧链”。也正是清算生态的存在，使得各类数字资产能够在主网外进行更符合商业场景与合规监管的资产交易与清结算。

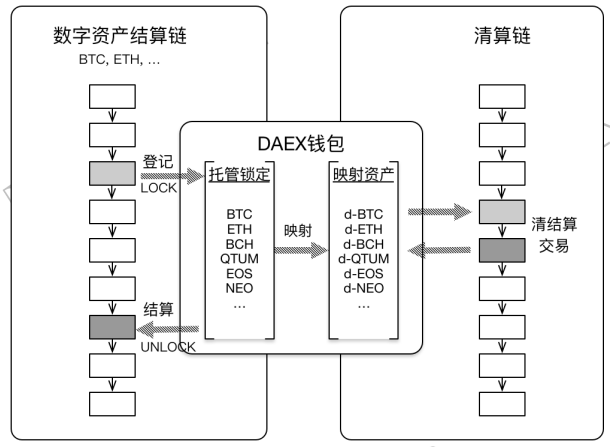

图 14：登记结算示意图

4 生态共识

共识机制是用于在不可信环境中达成可信结论的机制。目前公链上的各种共识机制存在着不同的问题。我们提出的 ASPOS（Accumulative Signature for POS）机制是一种高效、低能耗、安全的共识机制。ASPOS 中区块在广播过程中被各个验证节点依次累积签名，当签名累积到一定比重或有一定的确认数后被接受上链。算法中使用 VRF 抽签函数保证了创建区块节点的随机性，同时使用了保证金制度来解决无利害关系问题。ASPOS 是一个基于自视角的在异步公开网络上具有高可用度的算法。

4.1 基本共识

作为区块链技术先河，比特币中使用了工作量证明（POW）共识，该共识机制的核心思想是通过经济激励和节点算力竞争来维护账本的一致性。共识的结果是附加了最大工作量的区块在共识过程中胜出，胜出区块的创造节点获得经济奖励。这类共识机制的安全性依赖于特别设计的经济激励，并在开放式网络环境中有极高的可用度。同时开放式网络的复杂性会导致链的短暂分叉，这种暂时的分叉会导致系统安全性的降低和共识过程的拉长。为了平衡可用度和安全性，比特币选择了较长的出块时间（10 分钟），从而导致了共识效率的低下（每秒仅能处理 7 笔交易）。另外，比特币共识过程中的能源消耗大也一直成为其被诟病的原因之一。

为解决 POW 的能源消耗问题，POS 系共识

被提了出来（POS3.0、DPOS、Casper 等）。POS 中节点获得区块创建权的概率取决于其持有的权益（币数、币龄、保证金等）比例。POS 中容易出现无利害关系（Nothing at stake）和远程分叉攻击（Long range attack），会严重威胁系统的安全性。Casper 中通过保证金和 slasher 解决了无利害关系问题，并通过弱主观性纠正和检查点制度来处理远程分叉问题。但 Casper 算法中出块节点可以被预知，这会导致潜在的 DDOS 攻击，降低系统的安全性。Algorand 算法通过随机抽签来确定新区块的产生节点，这种随机性可用于解决 Casper 面临的 DDOS 攻击问题。

Casper 中基于投注的共识在收敛过程中依据其他节点的投注情况来决定自身的投注。这种收敛过程对全局投注信息（即上帝视角）有着强依赖，增加了系统实现难度，限制了可用度。POW 中节点对区块的选择实际也是一种投注，是完全基于本区块的已知信息（即自视角）。这种基于自视角的区块选择机制减轻了系统的实现难度，提高了系统的可用度。

综上，我们提出 ASPOS 共识机制。这是一种融合了 Casper 的保证金制度、Algorand 的抽签制度和 POW 自视角选择机制的共识。

4.2 ASPOS 共识

ASPOS 作为 POS 算法的变种，通过选择包含更小抽签选出值和更多验证签名累积权重的区块在传播区块的过程中实现了分叉的收敛。协议中设计相应的收益分配和处罚规则来保证系统的正常运行。

4.2.1 权益构成

不同的 POS 机制中权益的内涵有所不同，现有的 POS 机制有基于币值、币龄、保证金数额等的不同形式。ASPOS 的权益有机结合了保证金额、节点活跃度及清算价值因子。

节点价值因子是验证节点获得用户清算信任的数理统计，综合权益基于信任用户的清算价值因子，其高低会影响节点的最终收益。因此，ASPOS 也称为 CVF-POS，可通过每位用户正向的清算价值因子促进整个生态系统的良性发展。

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

S 为验证节点的权益或权重，C 为验证节点的保证金额度，F 是价值信任函数，e_i为第 i 个用户的清算价值因子，n 为信任用户的总数。

4.2.2 新区块的创建

系统中包含 4 种类型的节点：普通节点、验证节点、准发块节点、发块节点。普通节点通过缴纳锁定保证金成为验证节点；活跃度排名前几位的验证节点成为准发块节点；准发块节点通过抽签函数抽签成为发块节点，没被抽中的准发块节点退回为验证节点。

发块节点创建新的区块，并广播出去。验证节点（发块节点也是验证节点）可以对收到的新区块进行验证。如果验证通过则签名后广播该区块，否则抛弃该区块。普通节点除了无法对区块签名外其他功能和验证节点相同。

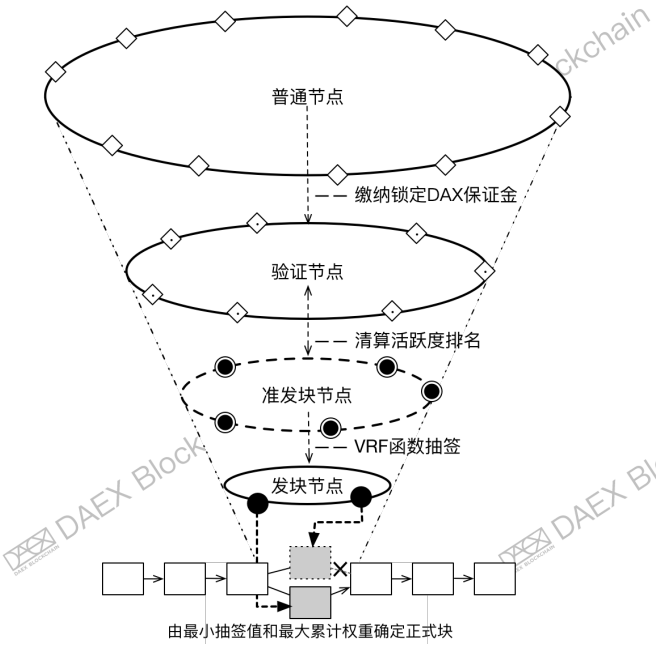

图 15：ASPOS 的区块创建过程

在特定地址存在验证集合约，用于追踪验证者集合的变化。普通节点可以通过向该合约发送保证金来成为验证节点。验证节点也可以通过发送消息到该合约来申请退出验证者集，退出申请生效后需要经过一段时间的解冻期间保证金才能退回到指定地址。

对链上高度最高的 N 个区块中交易进行统计，统计所有交易的提交方提交的交易总数，对交易总数进行排名，作为各个交易提交方的活跃度排名。活跃度排名前 K 的节点成为准发块节点。

ASPOS 采用了 VRF 抽签函数来选择下一高度区块的发块节点。抽签带来的随机性可以避免节点贿赂、DDOS 攻击等问题。抽签函数通过使用前一高度块的 hash、当前高度、抽签轮数和节点权益进行构建，准发块节点将自己的密钥带入 VRF 函数中计算出自己的选出值。如果准发块节点的选出值小于当前的选出值阈值，那么该准发块节点可自认为是发块节点。从总体视角来看，由于 VRF 的随机性，自认为满足选出值的准出块节点可能存在多个，亦可能不存在。若存在多个时，各个满足选出值条件的准发块节点都各自产生区块，并且将 VRF 函数值包含在自己产生的区块中，签名区块并广播。其它节点接收到多个区块之后，选择选出值最小的区块进行验证。若没有准发块节点满足条件是，则重新对同一高度进行下一轮抽签，并修改选出阈值。

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

抽签函数 VRF 的示例如上，H 为当前高度，N 为抽签轮数，S 为节点对应的权益，R 为前一区块创建节点在创建的区块中添加的本地物理随机因子，Block(R) 为前一高度的区块，SK 为节点私钥，P 为选出阈值。

拥有越高权益的验证节点会有越大的概率被抽中。为了增加抽签过程的随机数，每个发块节点在创建新区块时会添加从节点本地获得的随机因子 S 和 SK。当有多个节点被抽中时，拥有最小选出值的发块节点创建的块将在后面的传播中被选中记入各个节点的本地链中，最终所有节点达成共识。为保证系统出块的平滑度，每隔一段固定时间，系统会自适应地调整选出阈值 P。

4.2.3 共识过程描述

每个验证节点对自己收到的拥有最小选出值的合法区块的 hash 进行累积签名并广播，如果是普通节点则只进行区块的选择和广播。验证节点将区块哈希累积签名和区块分开传播。因为签名的尺寸比较小，所以系统并不会

因为累积签名的存在而增加太多的通信压力。当节点收到相同区块的不同累积签名序列时，如果新序列的累积签名权重大于本地，则用新序列覆盖本地序列，否则抛弃新序列。累积签名的示意如图 16：

图 16：ASPOS 累计签名

当新区块累积权重达到一定比例或者距离现在最新块的创建时间达到 T 时，就再次运行活跃度排名和抽签创建下一高度的区块。在创建的新块中加入对前一区块签名的验证节点列表（有先后顺序），这些信息将作为签名节点的收益凭据。

一个在某个高度签发了多个区块的发块节点被称为黑暗节点。黑暗节点创建的区块为黑暗区块。如果当前选出值最小的区块为黑暗区块，则重新创建该高度的区块。黑暗凭据会被发到验证集合约。验证集合约验证黑暗凭据后会依据合法的凭据对黑暗节点进行处罚。黑暗凭据会被收集到处罚凭据，处罚凭据会被记入到下一高度的新区块中。

每个节点直接忽略时间戳与本地时间相差超过一定周期的区块，并忽略和前一高度区块创建时间相差超过系统周期的新区块。

4.2.4 分叉处理

前文提到当遇到同一高度的不同区块时选择选出值较小的那个区块。当某个节点遇到选出值相同的区块时，累积签名权重较大的区块将被选中，其他的将被抛弃。选出值在同一高度同一轮数之间进行比较。如果遇到和本地缓存区块高度相同但轮数更多的合法新区块时，如果新区块中该高度的黑暗数据集中包含本地区块的创建节点，则本地缓存的区块将被新区块替换，并签名（如果是验证节点）广播新区块。

4.2.5 奖励与处罚

节点的收益包括 5 种：创建区块获得的收益、添加处罚凭据的奖励、添加收益凭据的奖励、添加懒惰凭据的奖励、参加区块验证的收益。当某区块获得 N 次确认后，该区块收益凭据中的收益可以被相应的验证节点、发块节点使用。在验证节点退出验证节点集时也会对验证节点的奖罚进行结算。

把处罚凭据记入区块的节点将获得奖励，把收益凭据记入区块的节点获得相应累积权重比例的收益。为了鼓励验证节点对收到的区块进行及时的验证签名，验证节点的收益会根据收益凭证中的顺序进行幂级衰减。为防止验证节点怠工（离线或无视块的传播），在确认数达到一定高度，但验证累计权重未达到最低限度的情况，对尚未进行签名的验证节点进行惩罚，惩罚的凭据被记入到懒惰凭据中。

系统每隔一定数量的区块会对收益进行对半衰减。DAX 通证的总挖矿量为 13.9 亿。

4.3 作弊分析

4.3.1 双花攻击

一个节点想要进行双花攻击需要先被选

为发块节点，然后同时创建多个新区块。但在区块传播的过程中，如果该节点的多个新区块被同时检测到，它就会被举报为黑暗节点，失去所有的保证金。

4.3.2 51%攻击

由于抽签函数中使用的 VRF 函数的伪随机性以及该函数输入分量中有上一个区块的随机性，即使集中了 51%的节点，如果没被选为发块节点，也很难发动攻击。如果联合 51%的节点拒绝对新区块认证签名，最终会导致保证金被罚没。

4.3.3 远程分叉攻击

每个区块之间有时效期限制，即超过一定期限创建的区块将被视为无效区块，从而无法在系统中传播。这样将阻止远程分叉被系统接受。远程分叉无法创建，同时拥有最小选出值的区块被选择接受，所以新进入系统的客户端在仅需知道创世块的前提下就可以判断出哪个分支是合法分支。

4.3.4 隔离攻击

如果一部分节点被长期隔离到系统之外，根据抽签规则，这部分节点会创建独立的分支。由于系统会对确认数达到一定量但累积签名对应的权益比例达不到 p%的验证节点进行处罚，所以如果想实现隔离攻击就必须联合至少占总验证权益 p%的验证节点，同时对被隔离的分支与主分支上的块分别验证，隔离传播才能实现。否则，在一部分验证节点因为隔离攻击造成签名缺失而被惩罚时，这个隔离攻击就会被系统发现。

5 生态治理

技术方案、生态结构、治理模式是一个区块链项目能否成功的三个关键维度。一种合理的生态治理模式是链上治理协议与链下协作共识的融合。

链上治理协议的目的是让生态的所有用户都有权参与他们所关心的生态事宜，通过投票表述决策。但是，当前以通证量或者通证持有者为标准的投票，可能会因为纯粹民主或投票冷漠导致整个生态的崩溃。同样，投票过程应当避免唯一决定方的出现，无论是通证多头、创始团队还是矿工，都可能出现已方偏袒的利益冲突。所以 DAEX 会从通证时间价值、治理价值时序和动态治理席位三个方面提升自治的灵活和公正性，以治理合约的方式达成生态共识。

链下协作共识是链外世界基于价值映射的治理模式。这样的共识不仅包括了网络监控、风险跟踪、代码审查等技术手段，还有生态熔断、风险基金等协同机制。DAEX 生态里，清算验证者通过验证交易的合法性维护价值恒定，应用程序间的管理不存在重叠。如果某个应用程序存在问题，线下管理机制可以及时修复，而不会影响其它生态应用的正常运作。

治理模式的另一关键维度，是合规化。合规要能够避免在监管上的一些不确定性，并在底层设计上满足支持未来主流机构合法参与该领域的技术架构。DAEX 生态的蓝图便是基于数据和资产的结构分层，创造交易和清算分离的监管空间。

虽然区块链本身的健壮性已经接受过考验，但是安全是一个整体，同时也是一套套行之有效的机制，需要生态建设者、使用者和监管者共同注意。但对使用者来说，有时安全的门槛太高，却会更容易滋生大量的攻击事件。因此，清算生态通过以下安全视角的优化来降低治理介入的频率、提升生态的风险抵御能力。

- **算法安全性**：优化多种密码算法，包括门限签名、伪随机生成算法、VRF 等。
- **协议安全性**：ASPOS 是更安全有效的共识机制，清结算协议相对一般跨链技术更安全、高效、低成本。
- **实现安全性**：智能合约多方审核、形式化验证与全面测试。
- **管理安全性**：定制化开发基于区块链模型的风控体系，链外数据物理隔离或分片存储，企业钱包权限分级管理。

6 披露计划

2018.Q2 清算生态的总体设计与共识机制

2018.Q3 清算价值因子与基于安全计算环境的钱包解决方案

2018.Q4 生态基金、通证计划（清算即挖矿）、节点部署及治理模型