DAEX: 분산형 디지털 자산의 청산 생태계 기술 백서

contactus@daex.io

개요

디지털 자산으로 묘사된 밝은 곡선은 신용 및 보안 앞에서 종종 빛을 잃는다. 현재 디지털 자산 산업에는 많은 결함이 있으며 시장의 유동성, 자산의 가치, 생태계 질서와 같은 내생적 요구가 진화해야 할 필요성이 있다. 본 눈문에서는 DAEX 청산 생태계의 분업 구조 및 청산 체인, 다중 자산 지갑 및 ID 체인 내 상품의 해결 방안을 소개하고 비동기식 개방형 네트워크에서의 ASPOS 가치 인식 메커니즘을 정의하여 투명하고 안전한 관리 메커니즘의 구축을 기대한다. 또한 미래의 디지털 자산 거래에 기반한 새로운 청산 네트워크를 창안하여 안전하고 신뢰할 수 있는 개방적 생태계계 비전을 달성하여 각 사람의 가치 증진을 촉진한다.

1 생태계 개론

1.1 배경

（1）빈번한 디지털 자산 보안 사고

디지털 자산의 발전으로 투자자 또는 거래소는 해커 공격에 노출되어 왔다. 특히 최근 디지털 거래소 Coincheck 는 해킹으로 큰 어려움을 직면했으며, 이로 인해 디지털 자산의 가치가 크게 하락했다. 이러한 사건으로 부각된 디지털 자산 시장이 직면한 보안 및 신뢰의 문제는 이미 매우 심각한 상황이다.

（2） 불완전한 산업 청산 설비

블록체인 3.0 시대에 필요한 것은 비즈니스 시나리오를 기반으로 구동되는 블록 체인 기반의 프로토콜을 재구성하여 특정 영역에 간판급 제품을 만드는 것이다. 블록 체인 기술을 기반으로 한 현재의 디지털 자산 산업에서는 명확한 책임의 경계, 충분한 투명성 및 보안의 부족으로 악의적인 조작 및 뜻밖의 도난에 취약하다.

（ 3 ） 안전하고 신뢰할 수 있는 인프라의 부족

디지털 자산 생태계 인프라의 핵심은 청산 메커니즘의 쇄신이다. 기존의 디지털 자산 청산 메커니즘은 확장성이 부족할 뿐 아니라 다양한 파생 상품과 스마트 자산 시장에 대한 조정 능력이 부족하여

꼭 필요한 생태계 청산 시스템은 디지털 자산의 다양한 유형의 활동에 안전하고 신뢰할 수 있는 서비스를 제공할 것이다. 동시에 우수한 디지털 자산 지

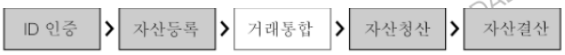
갑은 블록 체인 기술을 기반으로 안전성을 입증하고 시장의 문제점을 해결할 수 있을 뿐 아니라 디지털 자산의 거래 관계를 발전시켜 진정으로 안심할 수 있는 자산 보안 관리자가 될 수 있다.

1.2 생태계 설계

DAEX 가 구축한 분산형 디지털 자산 청산 생태계는 다중 자산 청산 및 결제 프로토콜에서 출발하여 자산 및 거래의 디커플링, 토큰과 권한의 부여, 디지털 자산 거래를 위한 인프라 재구축을 통해 여러 측면에서 청산 생태계 보안성 및 유연성을 보장한다. 이를 통해 DAEX 는 디지털 자산 상호 연결 노드 거래 플랫폼과 일반 디지털 자산 사용자를 포함하여 전반적인 디지털 자산 생태계 서비스를 제공함으로써 더욱 안전하고 효율적인 분산형 자산 등록, 청산 및 결제 산업 모델로 발돋움 하는 것을 가능케 한다.

1.2.1 가치 체인

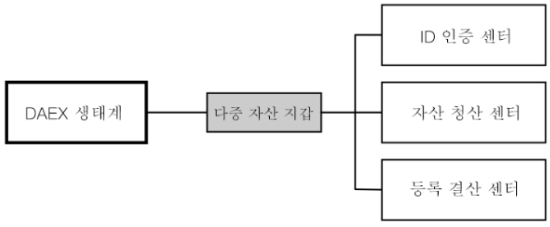
DAEX 생태계는 디지털 자산 거래의 업다운 스트림 산업 구조를 최적화하고 개선하는 것을 목표로 ID 인증, 자산 등록에서 자산의 청산 및 결산의 전체적인 가치 서비스 프로세스를 포괄한다.



거래, 청산, 위탁 관리의 분업은 DAEX 팀이 인터넷 기술 전문가 및 컴퓨터 과학자의 종합적인 지식을 수집하여 수년간 디지털 자산 산업에서 이뤄낸 최고의 솔루션이다. 중앙 집중화라는 아집을 버린 후, 분산형 거래 플랫폼과 분산된 청산을 결합한 실천을 통해 사람들이 증명할 수 있는 가치 기반의 인터넷 네트워크를 창출했다.

1.2.2 생태계 구성 요소

DAEX 생태계는 다중 자산 지갑을 링커로 사용하여 ID 인증 센터, 자산 청산 센터 및 등록 결산 센터를 연결한다. 청산 센터는 분산된 청산 체인을 사용하여 블록체인의 보안 및 신뢰성 메커니즘을 통해 디지털 자산 가치 이전 프로세스의 신용도를 높이고 표준화된 청산 및 결제 협약을 기반으로 열린 청산 생태계를 지원한다.



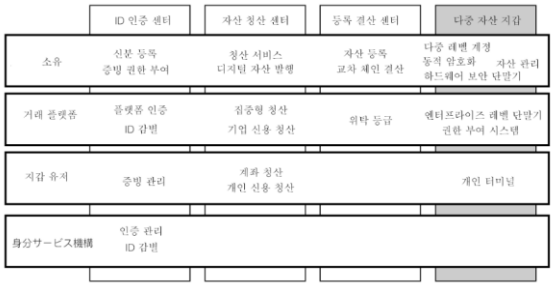
청산 체인은 전통적인 공유 체인의 모든 기술적 특성을 갖추며 합의합의 메커니즘, 트랜잭션 암호화 및 개인 정보 보호와 같은 핵심 기술의 최적화 및 업그레이드를 목표로 한다. 동시에 청산 시장을 기반으로 디지털 자산 영역의 ID 인증, 등록 매핑, 교환 지불 및 자산 관리 등의 구체적 요구를 세분화했으며 신원 확인 센터 및 등록 결산 센터와 함께 기존 거래 모델과 완벽하게 호환되는 인프라를 제공하여 향후 비즈니스 개발을 위한 청산 서비스(Clearing-as-a-Service) 솔루션을 지지한다. 또한, DAEX 는 건전한 거래를 위하여 안정적이고 검토 가능한 스마트 계약을 통해 금융 결제 시나리오를 확대할 것이며 지분 통합 지능형 디지털 자산과 디지털 자산 옵션, 선물 및 기타 금융 파생 상품을 추가함으로써 명확한 청산 및 결제 시스템에 무한한 자체 진화 공간을 마련했다.

청산 체인에서 파생된 분산형 디지털 자산 지갑은 사용자가 자체 청산에 참여하고 자산 관리를 실현하여 교환 지불 시나리오를 풍부하게 하는 도구이다. 임계 서명, 글로벌 ID 인증서, 신뢰가능한 컴퓨팅 환경 기술과 거버넌스 메커니즘을 기반으로 거래 플랫폼의 기업용 서비스 제품과 같은 다양한 유형의 사용자를 위한 포괄적인 디지털 자산 관리 서비스를 제공하고 권한 분리와 위험위험 통제, 사용자 자산 서비스 상품에 집중하여 자산의 다양성 및 개인 키 보안에 중점을 둔다.

1.3 역량 모델

개방형 생태계 구조는 여러 유형의 개체를 충족시켜 공동 작업을 통해 정보 처리와 가치 전달을 달성한다. 각 레벨의 개체에 대하여 DAEX 는 청산 체인을 기반으로 한 디지털 자산 매핑 및 청산 서비스와 같이

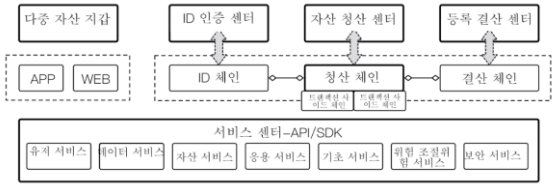
필요한 기본 역량을 활용해 다중 자산 지갑의 분할 키와 신뢰할 수 있는 인증 메커니즘 및 ID 인증 센터의 수명 주기 관리에 의탁한다.



2 생태계 방안

2.1 생태계 구조

청산 체인은 청산 생태계의 핵심 기반 체인으로 응용 프로그램의 계층은 복잡하게 교차 체인 비즈니스 구조를 지원하며 ID 체인과 결산 체인을 비롯한 여러 기능의 체인을 연결할 수 있다. 동시에 거래 플랫폼의 사이드 체인 분급으로 기술적 지표를 충족시킨다. DAEX 의 다중 자산 지갑은 분산형 자산 관리와 분산된 청산 서비스를 구현하여 표준화된 청산 서비스를 실현한다. 청산 체인의 인프라를 기반으로 물리적으로 분리되고 논리적으로 독립된 ID 인증 센터와 자산 등록 및 결산 센터가 동시에 구축되어, 완전하고 명확한 결제 가치 체인과 생태계 거버넌스 시스템을 구축한다. "다중 센터" 계층적 생태계 구조는 블록 체인 프로토콜 자체의 한계를 해결하고 분산 네트워크와 외부 정보가 안전하고 신뢰성 있게 상호 작용할 수 있도록 보장한다. 그 중 ID 인증 센터와 자산 등록 센터는 각각 신원 확인 체인과 결산 체인과 일치한다. 동시에 자산 및 운영의 보안 수준을 높이기 위해서 다단계 인증 기술을 채택하고 독립 센터의 일방적인 신뢰도를 가능한 한 낮춰, 분산형 장부와 생태계 인식의 중립적인 기술을 기반으로 생태계 신용 보증을 실현한다.



2.2 계정 시스템

청산 생태계 계정 시스템은 자산과 소유주 간의 관계를 수립하며 분산형 장부의 핵심 고리이기도 하다. 각 참가자의 경우 자신의 청산 계정을 만드는 것이 분산형 청산 서비스를 향유하는 첫번째 단계이다. DAEX 생태계에서는 계정 시스템의 소유자를 핵심으로 삼아 계정 및 트랜젝션 이벤트에 다양한 자산 유형을 기록하고 확장 가능한 계정의 구조는 유연한 비즈니스 모델을 지원한다. 동시에 각 계정은 인증되고 신뢰할 수 있는 ID 이기 때문에 디지털 자산이 통제되고 안전한 환경에서 호스팅될 수 있게 만들며, 사용자는 디지털 자산에 대한 주권을 갖는다. 이는 청산 생태계 계정 시스템이 존재하는 이유로 디지털 자산이 개인 정보 보호를 통해 비공개된 실명 ID 를 갖도록 허용하여 자산 권리의 확립과 복구를 지원한다.

청산 생태계에서는 이용자의 유형에 따라 개인 계좌와 기관 계좌로 나눌 수 있는데 기관 계좌에는 일반 기관 계좌와 거래 플랫폼 계좌가 포함된다. 일반적으로 기관 계좌는 시장 주체 및 기금 기관과 같은 고빈도 거래 또는 다중 레벨 권한 부여에 적합한 기업형 계좌이며, 개인 계좌는 현금 지급에 있어서 선호되는 방식이다. 거래 플랫폼 계좌는 특수한 기관 계좌로서 신용 청산 실현을 위한 중요한 부분이다.

디지털 자산의 상태에 따라 각 계정은 해당 에스크로우 계정 및 매핑 계정에서 파생될 수 있다. 에스크로우 계정은 등록된 자산의 신용 상태를 보여주며 비정상적인 도용을 공개적으로 감독하고 방지한다. 매핑 계정은 자산 등록 후에 청산 체인에 기록된 실제적으로 유효한 자산이다. 에스크로우 계정은 빈도에 따라 업데이트 및 정산이 진행되고 매핑 계정은 사용 배경 및 산업 요구 사항에 따라 다양한 유형의 하위 계정으로 나눌 수 있으며 하위 계정 간의 자산 배분을 통해 자산 계정 및 거래 계좌 분리 통제와 같은 다양한 비즈니스 전략을 구현할 수 있다. 일반 기관의 매핑 계정은 등급을 나눠 승인 메커니즘에 내장되며 개인 사용자는 거래소에 연결된 하위 계정을 만들어 동일한 ID 로 다중 거래 플랫폼의 분할 작업을 해낸다. 거래 플랫폼의 매핑 계정은 플랫폼 내의 사용자 하위 계정의 트랜잭션 결제를 지원할 수 있으며 금융 상품 하위 계정을 기반으로 위험위험을 차단한다.

청산 생태계에서 계좌의 일반적인 구조는 글로벌 ID 식별, 명칭 자체 정의, 계정의 유형, 계정의 상태, 청산 지역 및 자산 목록이 포함된다. 그 중에서 자산 목록은 디지털 자산의 유형, 에스크로우 주소 및 잔액과 같은 주요 요소의 다차원 배열이다.

글로벌 ID 식별	청산 주소	계정 명칭	계정 유형	계정 상태	거래 플랫폼 식별	자산 리스트 (자산 유형, 잔고, *에스크로 주소)

계정의 트랜잭션 이벤트에는 양도인, 양수인, 자산 유형, 발생 금액, 이벤트 시간, 이벤트 유형, 트랜잭션 채널, 트랜잭션 해시 및 블록 높이와 같은 플로우 정보가 포함된다.

전출 주소	전입 주소	자산 유형	발생 금액	사건 시간	사건 유형	경로	*거래 해시	*블록 높이

2.3 산업 모델

디지털 자산 산업은 설립 초기부터 다양한 지역 금융 상품을 연결하는 세계화된 금융 세계였다. 현재 사용자의 디지털 자산은 다양한 유형 및 기능적 특성을 지닌 디지털 자산 지갑 또는 거래 플랫폼에 의해 관리되며 각 도구는 자산의 청산 및 결제 프로세스를 완성한다. 정보의 투명성 및 자산 보안은 분산된 체인 노드 혹은 중앙집중식 운영 주체가 책임지고 있으며 교차 플랫폼의 디지털 자산 청산 및 결제는 동시에 산업 모델 및 기술적인 병목 현상으로 인해 제한을 받는다. DAEX 는 분산형 청산 솔루션을 통해 집중식 거래에서 자산 신뢰 문제를 해결하고 디지털 자산 산업에 적합한 보안 시스템 및 자산 보관소를 갖춘 완벽한 디지털 자산 거래 플랫폼과 투자자 집합을 위하여 중앙집중화 되고 분산화 된 트랜잭션의 장점을 결합함으로써 공정성, 컴플라이언스 및 효율성을 동시에 고려한다.

현재의 전통적인 금융 시장은 은행, 등록 결산 회사, 증권 거래소, 증권 회사 및 펀드 회사에 의해 형성된 성숙한 상업 생태계이다. 디지털 자산 시장의 구조적 발전 과정 역시 이와 비슷하며 다양한 전문가 조직으로 더욱 변모할 것이다. 이러한 조직은 탈중심화 혹은 분산화 된 지역 사회의 형태로서 기술을 통해 신뢰를

창출하고 재정 및 도덕적 위험을 감소시키거나 분리하여 다음과 같이 실현될 수 있다.

(1) 데이터 진실성

데이터를 신뢰할 수 있는 디지털 자산의 분산형 청산 및 결산은 데이터 위조의 위험을를 차단하며, 데이터의 자산 소유자만이 데이터의 "변경" 작업에 대한 권한을 갖는다.

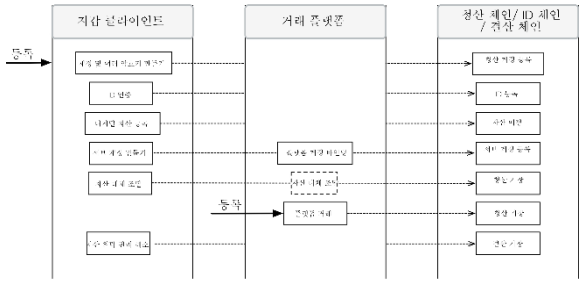
(2) 자산 실시간 등록

자산을 실시간으로 등록할 수 있는 디지털 자산의 거래가 전송된 후 데이터 정리 프로세스를 통해 데이터의 변경 사항이 모든 노드에 적시에 동기화되고 도메인 간 자산의 통합 등록이 가능하다.

(3) 개인정보 보호

시스템 내부의 개인 프라이버시 보호와 스마트 협약에 개인 정보 보호 전략이 추가되며 자산 관련 당사자의 명백한 요인과 신원 식별 코드를 토대로 개인 및 거래 플랫폼의 개인 정보 보호 데이터를 보호할 수 있다.

DAEX 청산 생태계의 본질은 거래 데이터와 디지털 자산을 분리한 후 계층화 된 시스템을 실현하는 것에 있다. 계층화 된 아키텍처와 데이터 단편화를 통해 거래 플랫폼은 전문 거래 서비스 기관이 되고 모든 디지털 자산이 관리 기관에 등록되어 거래의 내역이 탈중앙화 된 청산 체인에 의해 보장된다. 위탁 청산의 기본적인 비즈니스 프로세스는 그림 8과 같다 .

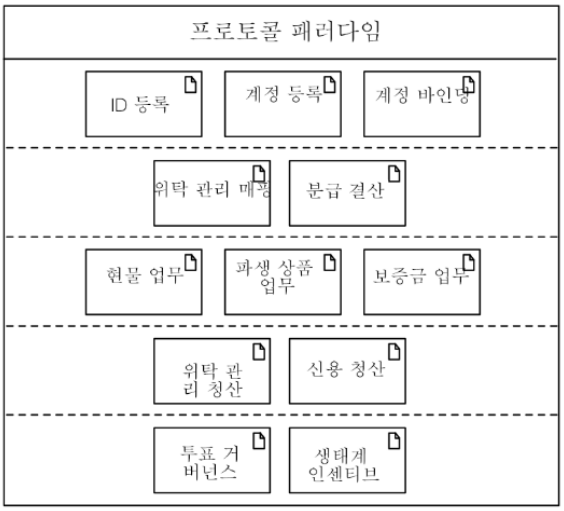


거래 플랫폼의 비즈니스 연속성을 보장하기 위해서 분산형 청산 프로세스를 트랜젝션 중심의 위탁 청산 및 서비스 지향적인 신용 청산으로 나눌 수 있으며 점차 모든 사람들이 사용할 수 있는 청산 프로그램으로 업그레이드 할 수 있다. 그 중 위탁 청산은 분산형 청산의 주요 회계 처리 방법이다. 신용 청산은 미래의 외환 결제를 위한 중요한 청산 방식인데 이는 자산 등록 절차에 국한되지 않고 프로세스의 위험 관리, 신용 등급 및 플랫폼 마진에 대한 특정 요구 사항을 포함한다. 모든 사람들이 사용할 수 있는 청산 시스템으로 인해 DAEX 생태계의 모든 사용자는 여러 채널을 통해 디지털 자산 청산의 동기화 프로세스에 참여하고 청산에 대한 보상을 받을 수 있다.

2.4 생태계 프로토콜

통합 서비스 협약은 청산 서비스와 같은 서비스 패러다임을 실현하기 위한 기초이며 다양한 배경에 적용할 필요가 있을 뿐 아니라 풍부한 추상 비즈니스 모델을 통해 플랫폼 간 데이터 공유를 충족시킬 수 있다. 따라서 청산 생태계의 기록 방식은 표준적이며 쉽게 구성되어 있어야 한다. 동시에 구조화된 다양한 정보를 효율적으로 나타낼 수 있으며 비즈니스의 범위가 확장될 때 필요한 교차 플랫폼 및 교차 체인

요구 사항을 충족할 수 있도록 사용자가 정의 가능한 개방형 프로토콜을 제공한다.



생태계 프로토콜은 청산 및 결산 장부에 저장된 비즈니스 정보의 도메인 및 형식, 비즈니스 과정 중에 생성된 비즈니스 상태, 서비스 상태 변경을 위한 트리거 방법 및 조건과 관련된 업데이트 정보 등을 규정한다. 각 참가자는 신원 계정을 통해 스마트 계약을 기반으로 한 비즈니스 협약에 서명했으므로 구현 프로세스가 각 노드에서 균일하게 구현되는 프로토콜을 포함하여 블록 체인 시스템에 의해 객관적으로 승인되었다. 즉, 비즈니스 개체로부터 인식되고 협약의 실행 프로세스가 정확하게 기록되어 최종 결과를 위조할 수 없이 비즈니스가 구현된다는 사실을 부정할 수 없다.

3 생태계 구조

블록 체인 기술이 보유하고 있는 탈중개화와 수정이 불가능한 유전자는 DAEX 생태계의 가치 축적과 유통을 위한 기본적 솔루션을 제공하지만 분산형 자치 커뮤니티 생태계를 달성하기 위해서는 기본적인 플랫폼이 갖고 있는 서비스와 관련한 요구 사항을 처리할 수 있는 우수한 성능 뿐 아니라 전반적인 생태계 인프라가 데이터 저장 성능을 향상시키기 위한 분산형 파일 시스템의 사용과 합의 프로토콜의 최적화를 통한 청산 및 결제 모델의 뛰어난 상호 운용성을 통해 전반적인 "합의"를 달성해야만 한다. 또한 신속한 접근과 같은 솔루션을 지원하는 서비스 지향적인 인터페이스를 제공할 뿐 아니라 디지털 자산 도구의 보안 및 사용 용이성을 향상시키는 다중 자산 지갑을 기반으로 하는 청산 환경 시스템은 다음과 같은 이점을 제공한다:

(1) 더욱 견고함

사용자가 사적으로 전체 키를 보관하여 전송의 가능성을 피하고 사용자를 핵심으로 삼아 체인의 여러 합의에 따라 분산형 장부에 대한 효율적인 기장을 완성한다.

(2) 더욱 다양함

신속한 다중 자산 거래를 지원하기 위해 블록 체인의 확장성을 연장한다. 동시에 청산 체인 상위층의 기본 서비스는 최초 거래의 깊이를 유지하고 파생 상품 및 스마트 자산의 풍부한 비즈니스 생태계계를 제공할 수 있다.

(3) 더욱 안정적임

다중 자산 지갑은 분할된 키 메커니즘과 신뢰할 수 있는 컴퓨팅 환경을 사용하여 자산의 보안성을 향상시키는 동시에 청산 가치 요소에 기반한 합의 메커니즘은 공평한 가치 보상과 사기 행위에 대한 페널티를 보장한다.

3.1 청산 체인

청산 체인은 디지털 자산 거래 플랫폼을 위한 인터페이스를 지원함으로써 개인 고객 및 기관 고객이 디지털 자산 지갑의 신원 확인 정보를 사용하여 지불 교환 작업을 수행하고 핵심적 스마트 협약의 자산 정리 프로세스를 완성할 수 있게 한다. 또한 분리 및 유연한 설치가 가능한 기능적 구성 요소와 청산 체인의 스마트 협약 엔진을 다양한 시나리오에 적용할 수 있을 뿐 아니라 디지털 스마트 자산의 다양한 활동 역시 충족시킬 수 있다. 청산 및 결산 업무에 있어서 청산 체인의 필요성은 스마트 협약이 없는 원래의 사슬의 원자성에 부여하는 것에 있다. 양 당사자 간의 합의 결과를 바탕으로 정보에 오류가 있을 경우 취소가 가능한 청산 및 결제 협약을 실현하여 자산 결제의 원자성을 보장한다. 청산 체인은 자산을 양방향으로 매핑하여 사용자만이 디지털 자산의 흐름을 확인할 수 있으며, 이와 동시에 청산 생태계 건설을 위한 거래 플랫폼 연합은 모든 참가자의 정직성을 유지하고 향상시킨다. 청산 체인의 "채굴자"는 증인으로서 청산 체인의 현재 디지털 자산 상태를 점검하고 모니터링한다.

트랜젝션 요청을 받으면 결과가 실제로 일치하는지 확인하기 위해서 청산 및 결산 협약이 실행된다. 정직한 채굴자의 청산 체인에 대한 참여도가 높을수록 전반적인 보안 수준은 향상된다.

3.1.1 설계 원칙

• 스마트 협약은 청산 생태계의 주요 가치 보유 방법이다.

• 청산 가치 인자는 노트 검증 인센티브의 중요한 요소이다.

• POS 합의 메커니즘을 업그레이드하고, 트랜젝션 성능과 수학적 임의성을 향상시킨다.

• 디지털 자산 거래를 위한 방향 암호화 스키마를 제공하고 일부 시나리오에서만 관련 당사자 청산을 위한 보기 및 거래 확인을 지원한다.

• 모니터링 지원 및 감사 구현에 대한 요구 사항을 충족한다.

• 청산 체인의 데이터 일관성이 핵심적 요구 사항이며, 비상 사태 시 효과적인 통제 메커니즘을 통해 포크를 방지할 수 있다.

3.1.2 상품 구조

청산 체인에 의해 구현된 블록 체인의 기본 기능에는 키 관리, 스마트 협약 및 장부 데이터 등이 포함되며 노드 및 블록 정보를 모니터링 할 수 있다. 구체적으로 그림 10 과 같이 세 개의 레이어로 분류된다.

（1）기본 프로토콜 및 시스템 지지층

청산 체인의 기본 인프라로서 블록 체인의 블록 구조, 스토리지 유형, 계정 모델 및 운영 지침의 기준과 프로토콜 뿐만 아니라 클라우드 서비스 기술 시스템과도 호환되며 신속한 배포 및 관리를 위해 컨테이너 기술을 사용할 수 있다.

（2）핵심 모듈 계층

핵심 모듈 계층의 데이터 상호 작용은 내부 데이터의 교혼 프로토콜을 통해 구현되며 구성 요소는 독립적으로 분리된다. 동시에 데이터와 논리가 분리되어 모듈 구성 요소의 확장과 분리를 실현한다.

합의 구성 요소 : 합의 구성 요소는 주로 방송, 순서, 실행 및 합의 등으로 완성되며 POS 마진 메커니즘 위에 청산 가치 인자 인센티브와 입증 가능한 랜덤 함수를 융합한다.

계정 및 저장소 구성 요소 : 장부 정보의 지속성은 성숙한 NoSQL 데이터베이스 구현을 기반으로 하며 KV 데이터 형식은 간결하고 빠른 저장 패러다임을 제공하지만, 저장 정보의 수정이 불가능하다.

P2P 통신 구성 요소 : 블록 체인 노드 간에 P2P 통신이 설정되며 동적으로 추가된 노드를 검색하고 블록 정보를 동기화 할 수 있다.

스마트 계약 엔진(Smart Contract Engine) : 가상 시스템을 기반으로 하는 튜링이 완비된 실행 엔진은 스마트 계약의 캡슐화 및 호환을 가능하게 한다. 각 노드는 실행 상태 및 결과에 대한 합의를 보장해야 한다. 청산 체인의 프로그램화 가능성은 다양한 비즈니스 시나리오에 적용되는 계약 논리를 편집함으로써 실현된다.

프라이버시 보호 구성 요소 : 트랜젝션 관련 당사자만 볼 수 있는 트랜젝션의 암호화를 지원하며 트랜젝션과 관련이 없는 비 참가자는 원래 트랜젝션 내용의 암호화된 해시 값을 통해 확인할 수 있다.

노드 관리 구성 요소 : 노드 권한의 동적 구성 및 검증을 지원한다. 노드는 검증 노드와 공통 노드로 분류되며 전자는 합의 프로세스에 참여한다.

생태계 거버넌스 구성 요소 : 생태계 거버넌스 메커니즘을 개선하기 위한 기술 솔루션으로서 블록 체인 기술의 초기 단계에서 발생할 수 있는 알 수 없는 오류로 인한 생태계적 피해를 방지한다. 청산 생태계는 장기적이고 안정적으로 지속 가능한 생태계로 생태계 커뮤니티에 기반한 몇 가지 특수 역할 기능을 설정하고 분산형 거버넌스 구조를 결합하여 체인 외부 협상이 일치하는 상황에서 청산 체인에 응급 사태 처리 능력을 갖추게 함으로써 악의적 손상 및 소프트웨어 버그, 하드 포크 등과 같은 돌발 상황을 해결할 수 있다. 이는 블록 체인 생태계와 커뮤니티 자치 프로세스에서 유지 및 보수를 수행할 수 있게 한다. 즉, 생태계가 파생 모델을 통해 자체적인 치유 능력을 갖게 되는 것이다.

교차 체인 구성 요소 : 다중 체인 및 사이드 체인 장부 사이의 정보 교환을 지원하고 트랜젝션 청산 하위 체인, ID 체인 및 결산 체인 등을 포함하여 데이터 및 비즈니스 논리를 분리한다.

（3）생태계 서비스 계층

생태계 서비스 계층은 블록 체인 프로토콜 및 코어 모듈의 구체적인 구현과 시나리오의 인터페이스를

기반으로 API 및 SDK 와 같은 완벽한 도구 세트를 제공한다.

RPC 구성 요소 : 노드로 전송된 RPC 요청은 노드 데이터 상호 작용의 진입점이다. 규칙 확인에 의해 유효하지 않은 메시지 필터링을 통해 합의 로드를 감소시킨다. 동시에 RPC 서비스의 유연한 구성을 통해 로드의 균형적인 조정을 달성할 수 있으며 다양한 프로토콜 사양 및 시나리오 인터페이스를 정의하여 다양한 유형의 청산 및 파생 서비스를 충족시킬 수 있다.

브라우저 구성 요소 : 청산 체인 브라우저 구현을 위한 기초. 블록 정보, 트랜젝션 정보, 노드 상태, 네트워크 상태 등 정보 및 다양한 통계 결과를 제공한다.

계약 관리 구성 요소 : 계약 생성, 테스트, 배치, 업그레이드 및 템플릿 편집을 포함한 스마트 계약의 모듈 관리를 제공한다.

생태계 응용 프로그램 구성 요소 : 청산 체인은 비즈니스 프로세스를 지향하는 블록 체인 상품으로 생태계 응용 프로그램 구성 요소를 통해 신원, 청산 및 결산, 자산 매핑과 발행 등과 같은 효율적인 응용 프로그램 기능을 구현한다.

3.2 다중 자산 지갑

청산 생태계의 다중 자산 지갑(DAEX 지갑)은 기업 및 개인 사용자를 위한 디지털 자산 관리에 대한 요구 사항을 충족한다. 동시에 이 지갑은 디지털 자산의 ID 인증이기도 하며 ID 권한 부여를 통해 DAEX 생태계 내부의 각 거래 플랫폼에 접근할 수 있다.

현재의 디지털 자산 지갑은 사용자의 앱 삭제 및 재설치와 앱스토어 상품의 조례(규정) 변경으로 인해 사용자가 연상 기호를(mnemonic) 잊거나 키 저장 문서 등을 잃어버려 사용자의 자산이 분실되는 사건이 늘 발생한다. DAEX 지갑지갑이 제공하는 다 계층 보안 방어 시스템은 사용자 행위 보안, 모바일 보안 방어, 주요 보안 관리 및 다중 요소 인증을 비롯한 여러 차원에서 디지털 자산의 보안을 보호하고 자산의 도용을 방지한다. 동시에 키 손실로 인한 자산 손실의 문제는 분할 키 메커니즘을 통해 조건적으로 해결된다.

편의성은 DAEX 지갑의 핵심인데 이는 고객 계층화에 우선적으로 반영되어 기관 및 개인 사용자 용으로 제작된 제품의 기능 및 클라이언트로 다양한 역할에 대한 자산 관리자로 활용된다. 또한 청산 체인의 고급 자산 체인을 기반으로 하여 디지털 자산의 관리 및 송수신을 위한 신속한 채널을 제공한다. 동시에 지갑을 통해 ID 의 방식에 거래 플랫폼을 내장시키면 트랜젝션 비용을 줄이고 자산 이전의 확인 시간을 단축할 수 있다. 또한 DAEX 지갑은 하드웨어 지갑 항목을 제공할 것이며 소프트웨어 키로부터 파생된 종단 간 보안 기초를 완비하여 서명 부인 방지를 통해 디지털 세계에 대한 높은 수준의 신뢰도를 구축할 수 있다.

3.2.1 설계 원칙

• 여러 자산 관리자를 대상으로 다양한 주류 디지털 자산을 지원한다.

• 통합 ID 지표를 통해 계정 자산 관리를 정상화하고

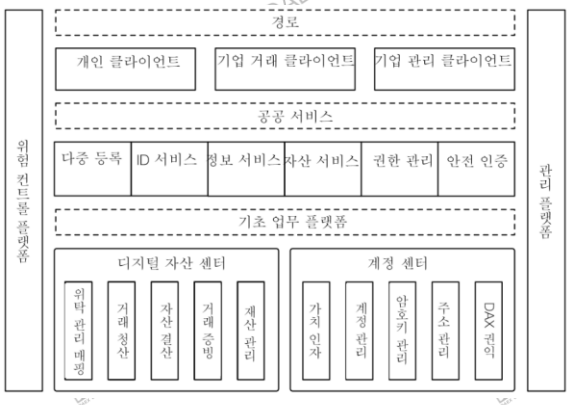
다양한 블록 체인에서 서로 다른 계정 체인 및 기술 아키텍처를 통합하는 문제를 해결한다.

•다단계 키 배포는 사용자 자산을 보호하며, 사용자가 절대적인 거래 권한을 갖는다. 기타 주요 부분 에스크로우 기구는 독립적으로 키를 복구하거나 자산 거래를 시작할 수 없다.

• 거래 플랫폼에 적합한 전문적이고 독립적인 자산 관리자 플랫폼은 다단계 인증 및 비즈니스 협업과 같은 기업 레벨의 기능적 속성을 갖는다.

•원스톱 디지털 자산 관리 도구. 스토리지, 지불, 교환 및 타사 서비스 등과 같은 시나리오의 요구 사항을 충족하는 동시에 디지털 자산의 부가 가치 기능을 확장한다.

3.2.2 상품 구조



（1）기본 기능

지갑 속 자산의 주소는 무작위로 생성되며 사용자는 다양한 매핑 자산을 정의하고 관리할 수 있다. 생태계 내 자산 이전 프로세스는 청산 체인의 매핑 자산 시용 기장을 통해 완성되며 사용자가 정의한 ID 를 기반으로 자산 전송을 지원한다. 분할 세션의 결산 프로세스는 위험 수준 적용에 해당하는 계층적 전략을 기반으로 하며 동적 암호, 생물 정보 및 물리적 정보와 같은 여러 조합의 유효성 검사를 지원한다. 결산 검증은 잔액에 대한 양방향 확인이 분명한 청산 및 결제 흐름에 의해 수행되며 청산 체인 데이터와 지갑 자산 계정의 일관성을 보장한다. 위험 관리 플랫폼은 디지털 자산의 사전 및 사중 위험 제어 시스템을 제공하며 신원 및 장치 식별, 위험 모니터링, 동적 전략 등과 같은 여러 차원에서 사용자의 자산을 보호하고 프로세스 모니터링을 지원한다.

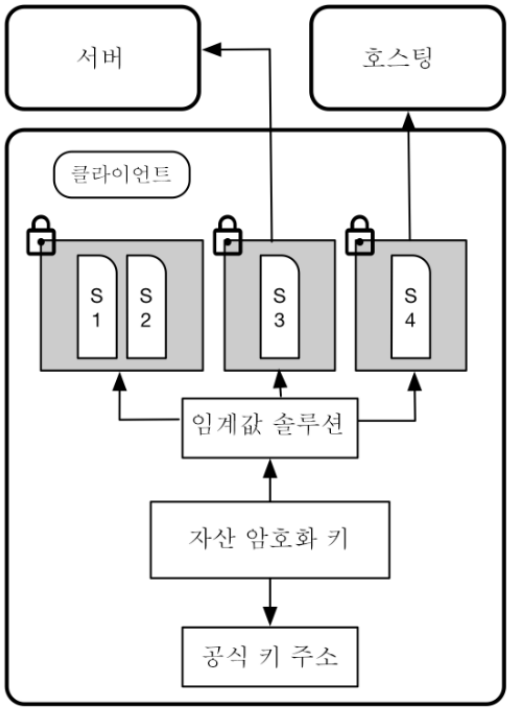
독립적 개인 및 기업용 지갑은 편리한 개인 작업 및 프로세스 통제의 다중 운영 요구 사항을 충족시킬 수 있다. 동시에 서로 다른 수준의 하위 계정을 만들어 신속한 교차 플랫폼 간 자산 재무의 관리를 수행한다. DAEX 지갑은 파생 상품 서비스, 고품질 재무 관리, 디지털 자산 검색, 융자 코인 등 금융 도구를 포함한 원스톱 디지털 자산 시장 구축에 전념하고 있으며 지갑은 시장 정보, 타사 DAPP 등의 서비스를 포함한 풍부한 디지털 자산 응용 생태계를 제공할 수 있다.

이 지갑은 DAX 패스의 다양한 권리와 이익을 통합하여 DAX 를 보유한 사용자가 신탁 투표 및 청산 인증 인센티브 획득을 포함한 생태계 환경 조성에 완전히 참여할 수 있게 해준다.

（2）분할 키

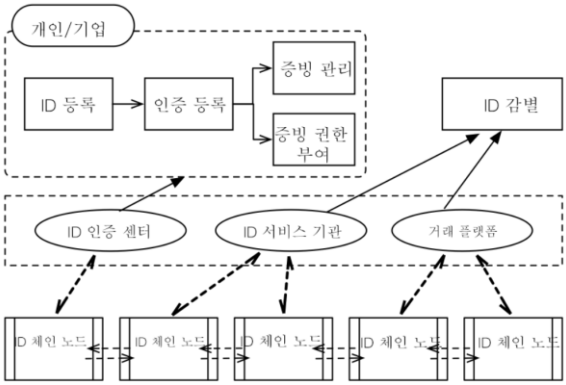
사용자의 청산 및 결산 계좌는 3 단계 키 메커니즘(클라이언트, 서버, 호스팅)을 채택하여 디지털 자산의 보안 통제를 구현하는데 그 중 개인 분할 키는 암호 텍스트로 저장되고 분할된 키 조각은 여러 매개체에 저장된다. 신뢰할 수 있는 컴퓨팅 및 통신

환경을 기반으로 한 키 메커니즘은 키 생성, 개인 키 분할, 개인 키 세그먼트 암호화 저장, 키 보안 전송, 키 로컬 복구 및 서명을 포함한 전반적인 프로세스를 포괄한다. 따라서 권한 관리 전략과 함께 다양한 시나리오의 보안과 관련한 요구 사항을 실현할 수 있다.



3.3 ID 체인

디지털 자산을 처리하는 과정 중에 완전하고 호환되며 신뢰할 수 있는 ID 서비스를 제공하기 위해서 ID 라이센스 체인을 기반으로 하는 분산형 ID 인증 센터는 ID 등록, 인증 등록, ID 자격 증명 관리, ID 식별 및 권한 등 내부 협약과 규범을 포함한 ID 관리의 글로벌 뷰를 구현한다. DIDC 가 각 사용자를 위해 생성한 청산 체인의 ID 식별은 ID 정보 등을 통해 체인이 유통될 때 신뢰할 수 있는 익명성을 실현하는데 이는 플랫폼 간 가치 순환을 위한 ID 기반이다.



3.3.1 설계 원칙

• 다중 참여자, 다중 인증 방법, 다중 정보 수집 채널

• 강약 인증 내부의 분급 인증 등급 지원

•신뢰할 수 있는 ID 인증 환경을 제공하여 신원 확인, 업데이트 및 해약 등과 같은 보안에 대한 위협을 감소시킴

•디지털 자산 거래소, DAPP 및 타사 ID 기관과 완벽한 네트워크 동맹 구축

3.3.2 주요 기능

ID 인증 센터는 ID 관리 프로세스를 완성하기 위해 ID 체인을 지원한다. 이는 신뢰할 수 있는 환경에서 작동하며 사용자가 자격 증명 정보를 안전하고 정확하게 제공할 수 있도록 지원함으로써 타인이 자산을 악의적으로 취득하는 것을 방지한다. 동시에 ID 인증 프로세스는 공격자의 다양한 공격 방법으로 인한 보안과 관련한 위협에 직면하여 인증 통신 중 온라인 추측, 서비스 공급자 롤 플레이 공격, 도청 공격, 리플레이 공격, 세션 도용, 중간자 공격, Dos 공격 및 악성 코드 삽입 공격을 방지하기 위해 필요한 보안 기술을 배포해야 한다.

ID 인증 과정에서 각 링크의 인증 강도에 따라 서로

다른 수준의 ID 인증 신뢰 수준이 등급이 정의된다. 즉, 사용자가 등록할 때 서로 다른 등록 자격 등급이 적용되고. 관련 사용자의 ID 인증에 대응한 후 다른 자격 보증 등급을 얻을 수 있다. 신뢰 등급이 높을수록 향유할 수 있는 디지털 자산 서비스가 더욱 다양해진다. ID 관리 프로세스는 주로 다음의 5 가지 부분을 포함한다.

（1）ID 등록

전 세계적으로 공유되는 ID 등록 서비스를 이용하기 위해서 사용자는 필요한 ID 식별 정보를 입력하는 동시에 관련 증명 자료를 제공해야 한다. 프로세스를 단순화하기 위하여 타사 ID 서비스 기관의 접근 권한 등록을 지원한다.

（2）인증 등록

인증 등록은 등록된 ID 에 대한 검증이며 ID 데이터의 암호화 및 단편화를 완성한다. 인증이 통과된 후, ID 체인은 암호화된 ID 정보인 ID 지문만을 등록한다.

（3）증빙 관리

ID 인증 등록을 완료한 즉시 ID 증빙의 매핑이 집행된다. 즉 청산 체인 주소 및 ID 증빙의 동시 바인딩이 완료되는 것이다. 또한 이 부분에서는 증빙 추가, 업데이트, 해약 등과 같은 ID 수명 주기 관리 서비스를 제공한다.

（4）증빙 권한 부여

신뢰할 수 있는 ID 체인을 기반으로 생태계 전반에 걸쳐 교차 체인 교차 앱(Cross app)의 ID 공유 서비스를 구현한다.

（5）ID 식별

거래 플랫폼과 ID 서비스 기관이 권한을 부여 받은 후 ID 식별 서비스를 사용하여 사용자 ID 인증 정보의 교차 검증 및 인증 피드백을 완성한다.

3.4 결산 체인

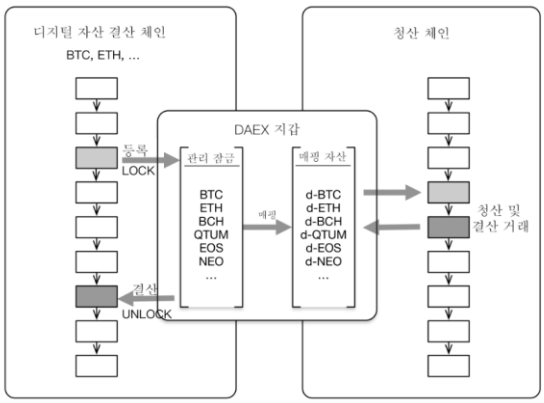
디지털 자산 등록 센터(Digital Assets Registration Center)는 결제 체인의 디지털 자산 등록과 에스크로우 및 청산 체인에 대한 자산 매핑을 구현한다. 자산 매핑은 교차 체인 바인딩을 통해 다양한 디지털 자산의 자유로운 발행 및 유통을 지원한다. 동시에 다양한 인증 기술과 전략을 통해 "등록인"의 신뢰성을 검증하고 분산형 아키텍처와 동적 계정을 통해 가치 관리의 안전성을 향상시키고 단일 지점의 장애로 인한 자산의 "동결"을 방지한다.

자산 등록 센터의 디지털 자산 호스팅 지갑은 모두 콜드 지갑으로 오프라인 세이프 하우스에 있다. 다양한 유형의 디지털 자산은 해당 기종 서버에서 독립된 네트워크를 사용하여 독립적으로 실행되거나 모니터링한다. 체인의 데이터가 여러 시점과 동기화될 때 적시성과 정확성을 보장하며 제 3 자 블록 브라우저를 통해 실시간으로 대조 확인할 수 있다. DARC 의 주요 임무는 다음과 같다:

- 에스크로 키의 동적 생성 및 배포
- 시크릿 키(secret key) 단편 데이터 암호화 스토리지
- 자산 수수 검사
- 자산 등록 및 매핑
- 자산의 교차 체인 호환

DAEX 의 청산 생태계는 블록 체인 프로토콜 계층

위에서 교차 체인의 가치 이전을 구현하며 일정 부분 사이드 체인 솔루션으로 이해될 수 있다. 구체적으로 말하면 디지털 자산은 첫번째 블록 체인에서 두번째 블록 체인으로 이전될 수 있으며 그 후 시점에서 두번째 블록 체인에서 안전하게 첫번째 블록 체인으로 복귀할 수 있다. 여기에서 말하는 첫번째 블록 체인은 비트코인, 이더리움과 같은 청산 체인을 말하며 두번째 블록 체인은 청산 체인의 "사이드 체인"을 말한다. 바로 이러한 청산 생태계의 존재로 인해 다양한 디지털 자산이 주요 네트워크 외부의 비즈니스 시나리오 및 규정 준수와 더 일치하는 자산 거래 및 결제를 수행하게 된다.



4 생태계 합의

합의 메커니즘은 신뢰할 수 없는 환경에서 신뢰할 수 있는 결론에 도달하기 위한 메커니즘이다. 현재 공유 체인의 다양한 합의 메커니즘에는 여러 가지 문제가 존재한다. 우리가 제시하는 ASPOS（Accumulative Signature for POS) 메커니즘은 효율적이고 적은 에너지를 소비하는 안전한 합의 메커니즘이다. ASPOS 블록은 방송 과정에서 각 인증 노드 별로 축적되는데 서명이 일정 비율로 축적되거나 일정 수의 확인이 이루어질 때 수용된다. 알고리즘에서 VRF 추첨 함수를 사용하면 블록 노드 생성의 무작위성을 보장하는 동시에 보증금 제도를 사용하여 이익이 없는 관련 문제를 해결할 수 있다. ASPOS 는 자기 원근법을 기반으로 한 비동기 공용 네트워크에서 높은 수준의 가용성을 갖는 알고리즘이다.

4.1 기본 합의

블록 체인 기술의 선례로 비트코인은 POW 합의를 채택했다. 이 합의 메커니즘의 핵심 아이디어는 경제적 인센티브와 노드 컴퓨팅 경쟁을 통해 장부의 일관성을 유지하는 것이다. 합의 결과는 합의 프로세스에서 가장 큰 작업량을 가진 블록이 승리하고, 승리한 블록 체인의 노드가 경제적 인센티브를 획득한다. 이러한 합의 메커니즘의 안전성은 특별히 고안된 경제적 인센티브에 달려 있으며 개방형 네트워크 환경에서 매우 높은 가용성을 제공한다. 동시에 개방형 네트워크의 복잡성으로 인하여 체인 포크의 단축을 야기시키는데 이 일시적인 포크는 시스템의 안전을 저하시키고 합의 프로세스를 길어지게 만든다. 가용성과 보안의 균형을 맞추기 위해 비트코인은 더욱 긴 출력 블록 시간(10 분)을 선택하여 합의 효율의 저하(초 당 7 회의 트랜젝션만 처리할 수 있음)를 야기시켰다. 또한 비트코인 합의 프로세스의 높은 에너지 소비 또한 비판의 이유 중의 하나이다.

POW 의 에너지 문제를 해결하기 위해서 POS 시스템 합의(POS3.0、DPOS、Casper 등)가 제안되었다. POS 에서 노드가 블록 작성 권한을 획득하게 될 확률은 해당 블록이 보유한 권익(코인, 통화 연령, 보증금 등)의 비율에 따라 상이하다. POS 에서 발생하기 쉬운 아무것도

수행하지 않는 문제(Nothing at stake)와 장거리 공격(Long range attack)은 시스템의 보안을 심각하게 위협할 수 있다. Casper 는 보증금 및 슬래셔(slasher)를 통해 아무것도 수행하지 않는 문제를 해결했으며 약한 주관적 교정과 검사 포인트 시스템을 통해 원격 포크 문제를 처리한다. 하지만 Casper 알고리즘의 블록 노드는 예측할 수 있기 때문에 잠재적인 DDOS 공격을 유발하여 시스템의 보안을 저하시킬 수 있다. Algorand 알고리즘은 무작위 크림으로 새 블록의 생성 노드를 결정하는데 이러한 무작위성은 Casper 가 직면한 DDOS 공격의 문제를 해결하는데 사용될 수 있다.

Casper 의 베팅 기반 합의는 수렴 과정 속에서 다른 노드의 베팅에 기반한 자체 베팅을 결정한다. 이러한 수렴 프로세스는 글로벌 베팅 정보(즉, 하나님의 시각)에 대한 의존성이 강하므로 시스템 구현의 어려움을 증가시키고 가용성을 제한한다. POW 노드에 의한 블록의 선택은 실제로는 베팅의 종류이며 블록의 알려진 정보 (즉, 원근법)만을 기반으로 한다. 원근법에 기반한 이 블록 선택 메커니즘은 시스템 구현의 어려움을 줄이고 시스템의 가용성을 향상시킨다.

요약하자면 우리는 ASPOS 합의 메커니즘을 제안한다. 이는 Casper 의 보증금 제도, Algorand 의 추첨 제도 및 POW 의 원근법 선택 메커니즘이 조합된 합의이다.

4.2 ASPOS 합의

ASPOS 는 POS 알고리즘의 변형으로서 더 작은 로터리 선택 값과 더 많은 검증 서명 누적 가중치가 포함된 블록 체인을 선택하여 블록 체인의 방송 과정에서 포크의 수렴이 달성된다. 해당 소득 분배 및 페널티 규칙은 시스템의 정상적인 작동을 보장하기 위한 프로토콜에서 고안되었다.

4.2.1 권익 구성

서로 다른 POS 메커니즘에서 권익의 의미는 상이하다. 기존 POS 메커니즘은 통화 가치, 통화 연령 및 보증금 금액 등에 따라 다른 형태를 취한다. ASPOS 의 권익은 보증 금액, 노드 활동 및 청산 가치 요인과 유기적으로 결합된다.

노드 가치 요소는 검증 노드가 사용자의 청산 신뢰를 얻게 되는 수학적 통계로 종합적인 형평성은 트러스트 사용자의 청산 값 요소를 기반으로 하며 노드 값의 고저는 노드의 최종 이익에 영향을 준다. 따라서 ASPOS 는 CVF-POS 라고도 불리우는데 각 사용자의 긍정적인 청산 값 요소를 통해 전반적 생태계 시스템의 건전한 발전을 촉진할 수 있다.

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

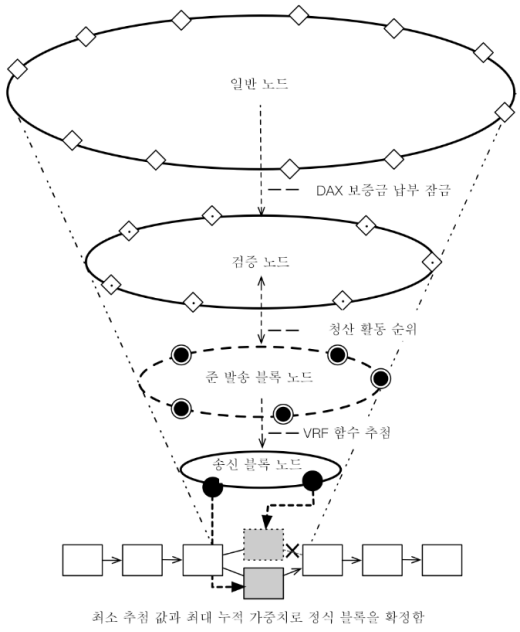
S 는 검증 노드의 형평 또는 가중치, C 는 검증 노드의 보증 가치, F 는 가치 신뢰 함수, ei 는 i 번째 사용자의 청산 값 요소, n 은 신뢰할 수 있는 사용자의 총 수 이다.

4.2.2 새로운 블록 생성

시스템에는 일반 노드, 인증 노드, 준 발송 블록 노드 및 송신 노드의 네 가지 유형의 노트가 포함된다. 일반

노드는 묶여 있는 보증금의 납부를 통해 인증 노드가 되고 활성도가 상위권에 위치하는 인증 노드는 준 발송 블록 노드가 된다. 준 발송 블록 노드는 추첨 함수의 추첨을 통해 송신 노드가 되고 추첨되지 않은 송신 노드는 인증 노드로 반환된다.

송신 노드가 생성한 새로운 블록은 방송되어 나간다. 인증 노드(송신 노드 또한 인증 노드임)는 수신된 새로운 블록을 검증할 수 있다. 만약 인증이 통과되면 서명 후의 블록이 방송되는데 그렇지 않으면 그 블록은 삭제된다. 일반 노드는 블록에 서명을 할 수 없다는 점을 제외하면 다른 기능 및 인증 노드와 동일하다.



특정 주소에는 검증 세트 계약이 있어 검증 프로그램의 변화를 추적하는데 사용된다. 일반 노드는 이 계약에 보증금을 발송하여 인증 노드가 될 수 있다. 인증 노드 역시 계약서에 정보를 발송함으로써 검증 자 세트를 철회할 수 있다. 철회 요청이 효력을 발생하면 일정 시간의 해동 기간을 거쳐 지정된 주소로 보증금이 반환된다.

체인의 가장 높은 곳에 있는 N 블록의 거래 통계가 진행되면 모든 거래의 제출 당사자가 제출한 거래의 총수가 통계로 잡히며, 총 거래 수는 각 거래 제출자의 활동도로 순위가 매겨진다. 활동도가 상위를 차지하는 K 노드는 준 발송 블록 노드가 된다.

ASPOS 는 VFT 추첨 함수를 사용하여 다음 높이 블록의 블록 노드를 선택한다. 추첨에 의한 무작위성은 노드 뇌물 수수와 DDOS 공격 등과 같은 문제를 방지한다. 추첨 함수는 이전 높이 블록의 해시, 현재 높이, 추첨 라운드 수 및 노드 권익을 사용하여 구성된다. 준 발송 블록 노드는 자체 키를 VRF 함수로 가져와 자체 선택한 값을 계산한다. 만약 준 발송 블록 노드에 의해 선택된 값이 현재 선택된 값의 임계값보다 작다면 준 발송 블록 노드는 발송 노드로 간주될 수 있다. 전체적인 관점에서는 VRF 의 무작위성 때문에 선택된 값을 만족시키는 것으로 간주되는 하나 이상의 블록 노드가 존재할 수도 있으며 존재하지 않을 수도 있다. 하나 이상의 블록 노드가 존재한다면 선택된 값의 조건을 만족하는 준 발송 블록 노드는 각각의 블록을 생성하고 자체적으로 생성한 블록 및 서명 블록에 VRF 함수를 포함하여 브로드캐스팅된다. 다른 노드가 여러 블록을 수신한 후, 가장 작은 값을 가진 블록을 선택하여 인증을 진행한다. 만약 준 발송 노드가 조건을 충족하지 않는다면 동일한 높이에 대한 다음 라운드 추첨이 진행되고 선택된 임계값이 수정된다.

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

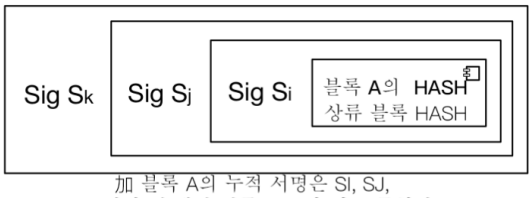
추첨 함수 VRF 의 예는 위와 같다. H 는 현재 고도, N 은 추첨 라운드 수, S 는 노드에 해당하는 형평성, R 은 이전

블록에서 만들어진 노드에 의해 생성된 블록에 추가된 로컬 물리적 임의 요소이다. Block (R)은 이전 높이의 블록, SK 는 노드 개인 키, P 는 선택된 임계값이다.

높은 공정성을 갖는 인증 노드가 추첨될 확률이 더욱 높은데 추첨 프로세스의 무작위성을 증가시키기 위해서 각 발송 노드는 새로운 블록을 형성할 때 노드로부터 획득된 랜덤 인자 S 와 SK 를 추가한다. 다수의 노드가 추첨되면 선택된 값이 가장 작은 발송 노드에 의해 생성된 블록이 후속 전파에서 선택되어 각 노드의 로컬 체인에 입력되고 마지막으로 모든 노드가 합의에 도달하게 된다. 시스템 출력 블록의 평활도를 보장하기 위해서 시스템은 규칙적인 간격으로 선택된 임계값 P 를 조정한다.

4.2.3 합의 과정 설명

각 인증 노드는 수신한 가장 작은 선택 값의 합법적 블록의 해시를 누적 서명하고 방송한다. 만약 일반 노드라면 블록 선택 및 브방송만을 수행한다. 인증 노드는 블록 해시 누적 서명을 블록과 별도로 방송한다. 서명의 크기가 비교적 작기 때문에 시스템은 누적된 서명의 존재로 인해 통신의 압력을 크게 증가시키지 않는다. 노드가 동일한 블록의 다른 누적 된 서명 시퀀스를 수신할 때, 새로운 시퀀스의 누적된 서명 가중치가 로컬보다 큰 경우 새로운 시퀀스는 로컬 시퀀스를 커버하는데 사용되고 그렇지 않으면 새로운 시퀀스는 폐기된다. 누적 서명의 도식 다이어그램은 그림 16 과 같다.



加 블록 A의 누적 서명은 SI, SJ,
SK이며 세 개의 검증 노드가 서로 중첩됨

새로운 블록 누적 가중치가 일정 비율에 도달하거나 현재 블록의 생성 시간이 T 에 이르면 활동도 순위 및 추첨이 다시 시작되어 다음 높이 블록을 만든다. 생성된 새로운 블록에 이전 블록에 설명한 인증 노드 목록(시퀀스 있음)을 추가하면 이러한 정보는 서명 노드의 수익 증거로 사용된다.

특정 높이에서 여러 블록을 발행한 발송 노드를 흑암 노드라고 한다. 흑암 노드에 의해 생성된 블록은 흑암 블록이다. 현재 선택된 가장 낮은 값을 가진 블록이 흑암 노드인 경우, 해당 노드의 블록이 다시 생성된다. 흑암 증거는 검증 세트 계약서에 전송된다. 검증 세트 계약이 흑암 증거를 검증한 후 합법적인 근거에 의해 흑암 노드에 대한 페널티가 적용된다. 흑암 근거는 페널티 자격 증명에 수집되고 페널티 자격 증명은 다음 높이의 새로운 블록에 기록된다.

각 노드는 타임스탬프와 로컬 타임의 차이가 일정한 주기의 블록을 초월하는 것을 직접적으로 간과하고 이전 높이 블록의 생성 시간의 차이가 시스템 주기를 초월하는 새로운 블록을 무시한다.

4.2.4 포크 처리

앞에서 동일한 높이의 다른 블록이 발생하면 더 작은 값을 가진 블록이 선택된다는 것을 언급했다. 어떤 노드가 동일한 값을 가진 블록을 만날 때 누적된 서명 가중치가 더 높은 블록이 선택되고 나머지는 버려진다.

선택한 값은 동일한 높이와 같은 라운드 수 사이에서 비교된다. 로컬 캐시 블록과 동일한 높이를 갖지만 라운드 수가 더욱 많은 합법적 새로운 블록이 발생할 때 새로운 블록에 그 높이의 어두운 데이터 세트가 로컬 블록의 생성 노드에 포함되면 로컬로 버퍼링 된 블록이 새 블록으로 교체되고 새로운 블록을 서명(검증 노드인 경우에) 방송한다.

4.2.5 인센티브와 페널티

노드의 수익은 블록 생성으로 획득한 수익, 페널티 자격 증명 추가에 대한 인센티브, 수익 자격 증명에 대한 인센티브, 지연 자격 증명 추가에 대한 인센티브 및 블록 인증 참여 인센티브의 5 가지를 포함한다. 블록이 N 번 확정되면 블록의 인센티브 자격 증명 속 인센티브는 상응하는 검증 노드와 발송 노드에 의해 사용될 수 있다. 검증 노드가 검증 노드 집합에서 나오면 검증 노드의 인센티브와 페널티도 결산 처리된다.

페널티 자격 증명이 기록된 노드에 인센티브가 주어지고 수익 자격 증명이 기록된 노드는 상응하는 누적 가중치 수익을 얻는다. 검증 노드가 수신한 블록에 적시에 검증 서명을 수행하도록 장려하기 위해서 인증 노드의 수익은 수익 자격 증명의 순서에 따라 그 수준이 약화된다. 인증 노드의 태업(오프라인 혹은 블록 전파)을 방지하기 위해서 확인 수치가 일정한 높이에 도달하나 누적 가중치가 최소 한도에 도달하지 않는 상황에서 서명되지 않은 검증 노드에 페널티를 부과하여 페널티 자격 증명이 나태한 자격 증명에 기록된다.

시스템에서는 특정 블록 수마다 수익을 반으로 줄인다. DAX 패스의 총 채굴량은 13 억 9000 만이다.

4.3 부정 행위 분석

4.3.1 더블 스펜드 공격 (Double spend attack)

노드가 더블 스펜드 공격을 수행하기 위해서는 우선 발송 노드로 선택되어 동시에 여러 개의 새로운 블록을 생성해야 한다. 그러나 블록 방송 과정에서 노드에 여러 개의 새로운 블록이 동시에 감지되면 흑암 노드로 보고되어 모든 보증금을 잃게 된다.

4.3.2 51% 공격

추첨 함수에 사용된 VRF 함수의 무작위성 및 함수 입력 구성 요소에는 이전 블록의 무작위성이 존재하기 때문에 51%의 노드가 집중되더라도 발송 노드로 선택되지 않으며 공격을 시작하기 어렵다. 만약 연합된 51%의 노드가 새로운 블록의 인증 서명을 거부하면 결과적으로 보증금의 몰수를 야기한다.

4.3.3 원격 포크 공격

각 블록 사이에는 제한된 시간 간격이 있다. 즉, 일정 기간을 넘어 만들어진 블록은 무효한 블록으로 처리되어 시스템에서 방송될 수 없는 것이다. 이렇게 원격 포크는 시스템에서 승인되지 않는다. 원격 포크는 만들어질 수 없는 동시에 가장 작은 선택 값의 블록을 선택하여 승인하기 때문에 새롭게 진입한 클라이언트는 생성된 블록을 알고 있다는 전제 하에 어떤 브랜치가 합법적인 브랜치인지를 판단할 수 있다.

4.3.4 격리 공격

만약 노드의 일부가 오랜 시간 시스템 밖에서 격리된 경우 추첨 규칙에 따라 이 일부 노드는 독립된 브랜치를 만들게 된다. 시스템은 확인 수에 대한 일정한 양에 도달하지만 누적 서명이 대응하는 수익 비율이 p%의 검증 노드에 도달하지 못하면 페널티를 부과하므로 격리 공격을 실현하기 위해서는 적어도 검증 수익이 p%를 차지하는 검증 노드를 결합하고 동시에 격리된 브랜치와 메인 브랜치의 블록을 별도로 검증함으로써 절연 전파를 실현할 수 있다. 그렇지 않으면 일부 인증 노드에 격리 공격에 의해 만들어진 서명의 결핍으로 페널티가 부과될 때, 이 격리 공격이 시스템의 의해 발견된다.

5 생태계 거버넌스

기술 솔루션, 생태계적 구조 및 거버넌스 모델은 블록체인 프로젝트의 성공을 위한 세 가지 핵심 요소이다. 합리적인 생태계 거버넌스 모델은 체인 거버넌스 협약과 체인 아래 협업 합의의 융합이다.

체인 거버넌스 협약의 목적은 생태계계의 모든 사용자가 관심을 갖는 생태계 문제에 참여하고 투표를 통해 의사 결정을 내리도록 하는 것에 있다. 그러나 토큰의 양 혹은 토큰의 소유자를 기준으로 한 현재의 투표는 순수한 민주주의 또는 투표에 대한 무관심으로 인해 전체 생태계의 붕괴를 야기할 수 있다. 마찬가지로 투표 과정은 유일한 결정권자의 출현을 피해야만 하며 토큰의 매수자, 창업 그룹 혹은 채굴자는 모두 이익에 대한 이해 상충이 있을 수 있다. 따라서 DAEX 는 토근의 시간 가치, 거버넌스 가치의 시서, 동적 커버넌스 위치라는 세 가지 측면에서 자율성의 유연함과 공정성을 향상시켜 거버넌스 협약의 방식으로 생태계적 합의를 도출한다.

체인 아래의 협업적인 합의는 체인 외부의 가치 매핑에 기반한 거버넌스 모델이다. 이러한 합의에는 네트워크 모니터링, 위험 추적, 코드 검토 등과 같은 기술적 조치 뿐 아니라 생태계적 퓨즈, 위험 기금 등과 같은 협업 메커니즘이 포함된다. DAEX 생태계계에는 거래 확인의 합법성을 검증함으로써 거래 확인자의 가치를 일정하게 유지하며 앱이 서로 중첩되지 않는다. 응용 프로그램에 문제가 있는 경우 오프라인 관리 메커니즘이 적시에 복구되어 다른 생태계계 응용의 정상적인 작동에 영향을 미치 않는다.

거버넌스 모델의 또 다른 중요한 점은 컴플라이언스이다. 법규의 준수는 규제 불확실성을 피할 수 있어야 하고 기본 설계 분야의 합법적 참여를 위해 주류 기구를 지원하는 기술 구조를 충족해야 한다. DAEX 생태계의 청사진은 데이터 및 자산의 구조적 계층화를 기반으로 거래 및 청산 분리의 규제 공간을 만든다.

블록 체인 자체의 견고성에 대한 테스트는 이미 수행되었지만 안전은 전체인 동시에 유효한 메커니즘이기 때문에 생태계 빌더, 사용자 및 감독자의 주의가 필요하다. 하지만 사용자에게 있어서 보안의 임계값이 종종 너무 높아 많은 수의 공격을 야기하기 쉽다. 따라서 청산 생태계는 다음과 같은 보안의 관점에서 거버넌스 개입의 빈도를 줄이고 생태계의

위험 탄력성을 향상시킨다.

• 알고리즘 보안 : 임계 서명, 랜덤 생성 알고리즘, VRF 등을 포함한 여러 가지 암호화 알고리즘을 최적화한다.

• 프로토콜 보안 : ASPOS 는 보다 안전하고 효과적인 합의 메커니즘으로 청산 및 결산 협약은 상대적으로 일반적인 교차 체인 기술보다 더욱 안전하고 효율적이며 비용이 적게 든다.

• 보안 실현 : 스마트 협약 다자간 감사, 공식 검증 및 포괄적 테스트

• 관리 보안 : 블록 체인 모델의 위험 통제 체계, 오프 체인 데이터의 물리적 격리 혹은 조각난 스토리지, 기업 지갑 권한의 급별 관리를 기반으로 맞춤 개발한다.

6 공개 계획

2018.Q2 청산 생태계의 전반적인 설계 및 합의 메커니즘

2018.Q3 청산 가치 인자 및 토큰 계획

2018.Q4 생태계 배치 및 노드 거버넌스, 하드웨어 지갑 솔루션

7 핵심 멤버

Gu Yanxi : 최고 전략 책임자, 기금회 주석. 중국 및 미국의 유명 금융 회사, 엔터프라이즈 소프트웨어 회사 및 인터넷 금융 회사의 풍부한 전문성과 관리 경험을 보유하고 있다.

그는 화태연합증권정보기술의 부 총감과 여러 금융 서비스 회사의 COO 를 역임했으며 미국의 옵션 거래소에서 근무할 때 미국 옵션 거래 시장의 유일한 청산 시스템인 ENCORE 개발과 운영에 직접적으로 참여했다. 미국 텍사스 대학에서 MBA 를 취득했으며 노트르담 대학교와 중국 과기대에서 석사 학위를, 산동 대학교에서는 학사 학위를 취득했다.

Tang Ruicong : 공동 창업자이자 수석 건축가. 금융 기술 제품의 설계 및 운용 연구에 중점을 두고 블록 체인, 인공 지능 분야의 제품이 있다. 국내 상업은행의 첫번째 블록 체인 프로젝트와 블록 체인 기술을 기반으로 하는 업계 최초의 매출 채권 플랫폼을 담당했으며 두 개의 블록 체인 특허를 보유하고 있다. 절강 대학교에서 소프트웨어 공학 석사 학위를 취득했다.

Zhang Hua : 공동 창업자. 다수의 디지털 자산 거래 플랫폼 투자자이자 IDEL 국제 디지털 경제 연맹의 창설 구성원. 세계 유수 금융 기관에서 근무하며 오랫동안 세계 500 대 기업의 업무 분석 및 전략 컨설팅 분야에 종사했다. 2014 년 이래로 블록 체인과 디지털 자산 분야의 비즈니스를 시작했으며 블록 체인의 지불, 지갑 등 영역에서 힘쓰고 있다. 블록 체인 업계의 오피니언 리더, 2016 년도 금융 과학기술·핀테크 어워드 여성 CIO, Qtum、Vechain 등 여러 개의 블록 체인 프로젝트의 초기 투자자로 상해 교통 대학교를 졸업했다.

Zhou Yan : 지갑 아키텍처 과학자. 10 년 이상의 인터넷 프로젝트 관리 및 개발 경험을 갖고 있는 스택 엔지니어로 모든 종류의 데이터베이스 클러스트 구축에 정통하다. 모든 주요 블록 체인 및 디지털 자산 지갑의 아키텍처에 정통하다.

Shen Bingliu : 브랜드 시장 파트너로 다년간의 인터넷

금융 및 기업 서비스 경험이 있다. 텐센트의 선임 비즈니스 관리자이자 우수한 직원으로서 위챗 지불과 금융 과학 기술 및 O2O 산업의 전략적 협력을 담당하여 많은 고객이 APP Store 상위 10 개 순위에 진입할 수 있도록 지원했다. 화동정법 대학교에서 경제법을 전공했다.