everiToken

기술 백서

버전 3.1

퍼블릭체인

추크, 스위스

everiToken

마지막 업데이트: 2019 년 3 월 26 일

면책 사항

- everiToken 기술 백서는 정보 제공을 목적으로 합니다.
- 백서는 어떠한 명시적 혹은 묵시적인 보증, 증명, 기대 등을 나타내지 않습니다.
- 백서에 기재된 기술 사양이나 기술 실현 방법은 시간에 따라 변경될 수 있습니다.
- 기술팀은 언제든지 해체되거나 재편성 될 수 있으며 핵심 기술자의 손실로 사업의 실패나 부분적 실현으로 이어질 수 있습니다.
- 이 백서는 어떠한 보증도 하지 않으며 프로젝트 팀이나 프로젝트 멤버 중 어느 누구도 백서 콘텐츠의 향후 사용으로 인한 어떠한 내용이나 결과도 책임지지 않습니다.
- 백서에 기재된 토큰은 실질적인 가치가 없고 가상 세계에서만 사용되며 유일한 목적은 토큰의 사용자 권한을 확인하는 것입니다.
- 기술 백서에 기재된 기술에 의해 운영되는 블록체인이나 그 파생상품 내의 어떠한 것도 프로그램 자동화에 의해 자동적으로 발생하며 결과에 책임지지 않습니다. 개인 또는 단체는 everiToken 블록체인을 사용할 때 내재된 결과에 대한 책임이 있습니다.
- 기술 백서에 포함된 모든 내용은 비상업적 사용을 전제로 사용할 수 있지만 기술 백서는 어떤 식으로도 수정하거나 변경해서는 안됩니다. 당사는 컨텐츠의 사용으로 인한 어떠한 결과도 책임지지 않습니다.

everiToken

목차

everiToken

Part I. 배경과 비전

토큰 이코노미의 탄생

블록체인 기술은 2019 년 2 월에 10 주년을 맞이했습니다. 이 기간 동안의 혁명에도 불구하고 여전히 한가지 중요한 질문이 남아있습니다. 블록체인 기술은 생산 혁명을 일으켜 세계 경제의 가치를 창출하고 있습니까?

자료를 살펴봅시다 - 현재 블록체인('온체인'이라고 함)에서 관리하는 자산은 기본적으로 다양한 코인/디지털 통화로 총 시장가치가 약 1500 억 달러입니다. 온체인 자산은 일반적으로 높은 변동성과 강한 투기를 특징으로 하며 세계 경제에 이익을 제공하지 못합니다. 사토시 나카모토의 출현 이후 사람들은 이러한 '코인'을 결제통화로 만들기를 원했지만 현재까지는 디지털 통화 기능을 하며 전통 통화 역할을 하지 않고 있습니다. 디지털 통화는 실제 통화라기 보다는 단순한 명칭에 가깝습니다.

통화 발행권은 정치적 의미이며 통화에 대한 권한은 국가에 속해야 합니다. 따라서 암호화폐가 법정화폐를 대체하는 것은 매우 어렵습니다. 국가의 승인과 지원이 없다면 이른바 '디지털 통화'는 이상주의적인 추구일 뿐입니다.

반면 대부분의 세계적인 주류자산(유형자산과 무형자산)은 블록체인('오프체인'이라고 함)에 있지 않으며 블록체인과 오프체인 자산 간의 거래가 제한적입니다.

그렇다면 토큰은 단지 또 다른 디지털 통화일까요? 그렇지 않습니다. 토큰의 기본 정의는 "심볼, 표시"이지만 디지털 통화보다는 인증서로 더 적절합니다. 이러한 인증서는 쇼핑 포인트, 쿠폰, 신분증, 졸업장, 부동산, 비밀번호, 이벤트 티켓을 포함한 여러가지 종류의 권익을 나타낼 수 있습니다. 과거로부터 권익의 증명은 인류 사회의 모든 문명의 필수적인 요소입니다. 계정, 소유권, 자격, 증명 등은 모두 권익을 대표합니다. Yuval Noah Harari 가 *Brief History of Humankind* 에서 "이러한 '허위적 사실'이 현명한 사람들이 두드러지고 인간 문명을 구축해야 하는 핵심적인 이유입니다" 라고 언급했습니다. 만약 이러한 권익의 증거들이 모두 디지털, 전자, 그리고 암호화된 방식으로 보호되어 진위성과 진실성을 입증한다면 인류 문명은 혁명을 일으킬 것입니다. 당사는 이러한 현상을 **토큰 이코노미**라고 부릅니다.

온체인 인증서를 실행하면 기존의 중앙화 인프라에서 제공하지 않는 신뢰성과 추적성을 제공합니다. 따라서 인증서가 토큰 이코노미의 프론트-엔드라면 블록체인은 토큰 이코노미의 백-엔드 기술입니다. 두가지는 통합적으로 연결되어 있고 상호 의존적입니다.

경쟁사 분석

토큰 이코노미를 위한 **퍼블릭 블록체인** everiToken 은 현재 이더리움과 EOS 라는 두개의 주요 경쟁사가 있습니다. 당사의 경쟁 우위는 시장 내 강점, 약점, 기회 및 위협을 분석을 통해 알 수 있습니다.

강점과 약점:

everiToken 은 토큰 이코노미를 위한 블록체인 기술이 다음 세가지 측면을 통해 권익의 증거를 효과적으로 관리해야한다고 믿습니다:

1. **디지털 권익의 증명**: 증명서(유형 혹은 무형)는 실물 가치가 뒷받침 하는 권익의 신뢰할 수 있는 디지털 형식이어야 합니다.
2. **보안, 암호화 및 권한 관리**: 증명서는 검증 가능, 변조 방지, 개인 정보 보호, 감독, 암호화에 의해 보호되어야하며 승인된 사람만 사용할 수 있어야 합니다.
3. **양도성:** 증명서는 편리하게 거래 및 교환이 가능해야합니다**.**

상기의 요건에 따라 토큰 이코노미의 기본 니즈에 부응하고, 토큰의 관리와 유통을 촉진하고, 토큰 이코노미의 기술적 기반을 구축하기 위한 솔루션을 제시했습니다. 구체적으로는 상기의 요건에 따라 이하의 3 개의 주요 특성을 실현했습니다.

- **빠르고 편리한 토큰 발행:** 사용자는 코드를 작성할 필요가 없으며 API (애플리케이션, 웹 페이지 또는 타사 애플리케이션)를 통해 자신의 토큰을 쉽게 발행할 수 있습니다.
- **효율적인 토큰 전송:** 수억 개의 토큰 거래량으로 몇 초 이내에 토큰을 전송할 수 있습니다.
- **유연한 권한 관리:** 권한 관리를 위한 단순하고 세련된 통합 모델로 추가 코딩 없이 다중 사용자 보관, 개인 키 복구, 다계층 권한, 합법성, 정부 감독 및 기타 복잡한 기능을 지원합니다.

이더리움 및 EOS 에 대해 살펴보겠습니다.

이더리움: ERC20/ERC721

이더리움을 통해 토큰 이코노미를 달성하는 주요 방법은 ERC20 및 ERC721 프로토콜을 기반으로 한 스마트 계약을 개발하는 것입니다. 이 중 ERC20은 대체가능 토큰(대체가능 토큰)를 지원하고 ERC721은 대체불가 토큰(대체불가 토큰)를 지원합니다. 그러나 다음과 같은 몇 가지 심각한 문제가 있습니다:

- **TPS**: 현재 이더리움은 초당 20 개 미만의 트랜잭션만 지원할 수 있으며 토큰 사용 및 유통에 필요한 모든 실질적인 요구를 충족할 수 없습니다.
- **비용**: 이더리움 스마트 계약 사용 시 각 단계마다 가스 요금이 요구됩니다. 복잡한 비즈니스(다중 사용자 보관, 감독, 합법성 등)에 경우, 비용이 높고 통제할 수 없을 수 있습니다.
- **대중화**: 이더리움을 통한 토큰 이코노미는 스마트 계약을 중점으로 두고 있으며, 복잡한 성격 때문에 타사 애플리케이션을 사용하지 않으면 개발자가 접근할 수 없습니다. 이로 인해 보안 및 규제 문제가 발생하며 대량 채택을 가로막습니다.
- **비표준화**: 서로 다른 스마트 계약에는 완전히 다른 개발이 필요할 수 있기 때문에 이런 가상 토큰의 메타데이터는 교환할 수 없으며 결과적으로 무용지물이됩니다. 이것은 토큰 이코노미의 생태학적 발전에 도움

이 되지 않습니다. 또한 사용자는 자신이 소유한 모든 종류의 토큰 자산을 조회하기 위해 통일된 방법을 사용할 수 없습니다.

EOS

EOS 는 2018 년 6 월 메인넷을 출시했습니다. EOS 의 주요 목표는 새로운 솔루션을 만들어 이더리움의 문제를 해결하는 것이었습니다. 그러나 이로 인해 새로운 문제가 발생했습니다.

- **보안성**: 토큰 트랜잭션은 매우 귀중하고 갱신할 수 없는 실체를 나타내므로 보안 문제가 발생하지 않는 것이 중요합니다. 하지만 계속해서 스마트 계약에 중점을 두고 있는 전체적인 개발은 개발자의 숙련도에 의해 결정되며 모든 유형의 토큰 개발자가 충분한 보안 의식을 가지고 있는지 확인하기 어렵습니다.

  EOS 의 스마트 계약는 상대적으로 새로운 **웹어셈블(WebAssembly)**를 기반으로 하며 아직 테스트(베타) 단계에 있습니다. 또한 EOS 의 스마트 계약 코드는 튜링 컴플리트(Turing complete)이며 과도한 권한을 가지므로 의도하지 않은 보안 허점에 취약합니다.

  대부분의 사람들은 안전한 스마트 계약을 쓸 수 없습니다. 토큰을 발급 및 전송하려면 사용자가 타사 애플리케이션에 의존해야 하며 해당 타사 코드의 품질을 신뢰해야 합니다. 따라서 자산의 통제는 이용자 자신의 것이 아니라 제 3 자에게 양도됩니다.

- **비표준화**: 이더리움과 같은 서로 다른 스마트 계약의 메타데이터는 상호 작용하거나 협력할 수 없습니다.

- **규제, 신뢰, 합법성:** 비표준화와 코드 판독에 필요한 기술적 전문성 때문에 정부가 규제하기 어렵습니다. 마찬가지로 비개발자들은 관련 프로그램을 신뢰할 수 있는지의 여부를 결정하는 데 어려움을 겪을 수 있으며, 이로 인해 블록체인이 일반인과 정부에 의해 사용되기 어려울 수 있습니다.
- **실행효율:** EOS 의 스마트 계약 기능은 복잡하고, 시스템 모듈이 많으며, 리소스 예약 및 배포가 어렵습니다. 이를 통해 시스템의 복잡함이 크게 증가하고 작업 속도가 감소합니다. 데이터 및 기능 간에 충돌이 발생할 수 있기 때문에 멀티스레딩을 사용하여 속도를 높이는 것은 쉽지 않으며 스케줄링 비용이 높습니다. 그러나 토큰 이코노미의 경우 이러한 복잡한 기능이 중요하므로 반드시 해결해야 합니다.
- **대중화:** 세계 경제의 비즈니스 니즈는 복잡하고, 변칙적이며, 일관성이 부족합니다. 하지만 스마트 계약는 개발과 테스트에 시간이 걸리기 때문에 다양한 시장의 요구를 단기간 내에 해결하기 어렵습니다. 이것은 토큰 이코노미 발전의 장애입니다.

everiToken 과 타사의 주된 차이점은 everiToken 은 "안전 계약(safe contract)"을 사용하는 반면 타사는 스마트 계약을 사용한다는 것입니다. 즉 everiToken 은 튜링 컴플리트가 아니며 언제나 everiToken 이 만족할 수 없는 복잡한 애플리케이션 시나리오도 있을 것입니다. 그러나 everiToken 은 토큰 이코노미 수요의 99%를 충족할 수 있으며 전 세계 모든 사람들에게 가장 안전하고 효율적인 비용을 제공하며 사용자 친화적인 퍼블릭체인입니다.

기회와 위협

당사는 기존의 강점과 더불어 NFC, 블루투스, QR 코드를 포함한 다양한 데이터 채널을 통해 지급인과 수취인을 연결하는 데 사용되는 EvtLink 표준을 만들었습니다. EvtLink 를 기반으로 하는 everiPay 는 핵심 인프라로 everiToken 퍼블릭 블록체인을 사용하며, 토큰 소유권 검증 프로토콜로 everiPass 를 사용하여 직접 토큰 소액결제를 가능하게 하는 결제 프로토콜입니다. everiPay/everiPass 는 **QR 코드** 생성의 표준과 통신 프로토콜을 의미합니다. 당사는 다음과 같은 혁신을 통해 특징 목록을 만들었습니다:

- **즉각 승인**: 트랜잭션은 곧 결제입니다.
- **탈중앙화**: P2P 지불이 가능하고, 중앙화 플랫폼이 없고, 아무도 온체인 데이터를 수정할 수 없으며 누구나 가격경쟁에 참여할 수 있습니다.
- **최고의 보안**: 사용자 재산의 보호 및 보안을 극대화하기 위해 블록체인 내의 데이터와 콘텐츠를 위조하거나 변조할 수 없습니다.
- **호환성**: everiPay/everiPass 는 항상 everiToken 이 지원하는 모든 토큰과 화폐, 포인트, 심지어 문을 여는 열쇠까지 지원합니다. 핸드폰만 있으면 어디에서든 사용할 수 있습니다.
- **최고의 편리함**: 인터넷에 연결할 수 없어도 트랜잭션을 완료할 수 있습니다.

상기의 5 가지 특징을 바탕으로 everiPay/everiPass 는 세계에서 가장 안전하고 편리하며 사용자 친화적인 서비스를 제공할 수 있습니다.

요약

아직도 몇 가지 위협 요소가 있습니다. 앞서 언급했듯이 이더리움과 EOS 는 토큰 이코노미 내에서 특정 요구에 대한 훌륭한 퍼블릭체인이 될 수 있습니다. 그러나 이더리움과 EOS 의 가장 큰 문제는 스마트 계약 때문에 생긴 사용자의 높은 진입 장벽입니다. 당사는 이 문제를 안전계약의 개발로 해결했고 이제 everiToken 은 전 세계 모든 사람들을 위한 토큰 이코노미를 지원할 준비가 되었습니다.

위의 분석을 바탕으로 대부분의 블록체인 애플리케이션에 완벽하게 적합하고 바람직한 새로운 개념을 설계하고 토큰 이코노미의 발전을 위해 새로운 퍼블릭체인 및 에코시스템인 **everiToken** 을 제안했습니다. 토큰을 발행하여 실제 세계의 자산, 인증서 및 증표를 **디지털화**할 수 있으며 전례 없는 보안, 속도 및 네트워크 호환성과 함께 쉽게 사용할 수 있습니다.

Part II. everiToken 의 기술

안전계약

스마트 계약은 이론상 중개인 없이도 탈중앙화된 상품이나 서비스의 거래를 용이하게 하는 효과적인 디지털 수단입니다. 그러나 실제로 스마트 계약은 부적절한 구현과 논리적 오류로 인해 발생하는 광범위한 보안 취약성으로 인해 락아웃, 접근 불편 및 부적절한 종료와 같은 결과가 초래됩니다. 따라서 스마트 계약은 종종 충분한 신뢰를 제공하지 못하며 전통 계약이나 거래소보다 신뢰성이 낮은 것으로 평가되고 있습니다.

everiToken 은 API 레어어를 통해 안전계약에 대한 새로운 아이디어를 소개합니다. 코드에 직접 의존하기보다는 안전계약을 통해 토큰의 발행 및 전송과 같은 과정을 용이하게 합니다. 안전계약은 사용 가능한 API 기능을 충분히 검토하고 검증하므로 핵심 요구사항에 맞게 기능을 간소화함으로써 모든 체인 트랜잭션을 빈틈없이 안전하게 보호합니다. 안전계약이 체결되지 않았더라도 API 를 통해 필요한 대부분의 기능을 달성할 수 있으며 오프체인 서비스를 위해 토큰 발행자에게 유연성을 제공합니다.

안전계약은 접근성과 TPS 를 증가시킨다는 추가적인 이점을 가지고 있습니다. API 를 사용하면 처음부터 체인 통합 코드를 작성할 필요 없이 기존 워크플로우에 쉽게 통합될 수 있으며, 다양한 변환 유형을 쉽게 구분할 수 있으며 독립적인 토큰 트랜잭션을 더 빠른 속도로 병렬 처리할 수 있습니

다(메인넷 10000 TPS 달성: 2018 년 12 월).

데이터베이스

EOS 는 롤백 작업을 지원하는 멀티인덱스 기반 메모리 데이터베이스(Chainbase)인 부스트를 활용합니다. 모든 계약 작업의 결과가 메모리 데이터베이스에 있습니다. 계약 코드가 비정상적일 때 브랜칭 및 복구 시 롤백을 지원하려면 모든 작업에서 롤백을 위한 추가 데이터를 기록해야 합니다. 또한 모든 데이터가 메모리 데이터베이스에 저장되고 처리됩니다. 사용자와 트랜잭션이 증가함에 따라 메모리에 대한 수요가 크게 증가할 것으로 예측됩니다. 이로 인해 블록 프로듀서에게 메모리 용량을 많이 요구하게 됩니다. 또한 프로그램이 충돌하거나 다시 시작되면 메모리 데이터가 손실됩니다. 데이터를 복원하려면 블록의 모든 작업을 반복해야 하므로 시작 시간이 오래 걸리고 비현실적입니다.

EOS 의 메모리 데이터베이스를 보존하면서 다음과 같은 몇 가지 이점을 가진 RocksDB 기반의 토큰 데이터베이스를 개발했습니다.

- RocksDB 는 페이스북의 핵심 클러스터에서 이미 검증되고 사용되는 매우 성숙한 산업용 키 밸류 데이터베이스입니다.
- RocksDB 는 LevelDB 를 기반으로 하지만 LevelDB 보다 뛰어난 성능과 풍부한 기능을 제공합니다. 또한 플래시 또는 SSD 와 같은 대기 시간이 짧은 스토리지 상황을 최적화할 수 있습니다.
- 필요한 경우 RocksDB 를 메모리 데이터베이스로 사용할 수 있습니다.
- RocksDB 기반 아키텍처는 버전 롤백과 지속성을 자연스럽게 지원하며 성능에 미치는 영향도 매우 낮습니다.

토큰 데이터베이스는 RocksDB 를 기본 스토리지 엔진으로 사용합니다. 성

능을 극대화하기 위해 토큰 관련 작업을 완벽하게 최적화했습니다. 이 기술을 사용하면 더 낮은 비용으로 롤백을 할 수 있습니다. 또한 토큰 데이터베이스는 초기 재시동(cold startup)과 같은 문제를 해결하기 위해 데이터 지속성, 정량적 백업 및 증분 백업과 같은 선택적 기능을 지원합니다.

everiToken 에서의 작업은 매우 구체적이기 때문에 코드는 고정되고 각 작업에 필요한 정보는 최소화됩니다. 따라서 데이터 중복성은 EOS 와 같은 일반 시스템에 비해 매우 낮아서 블록의 크기도 감소합니다.

토큰 모델

개요

토큰 이코노미를 위해 탄생한 everiToken 은 고유의 토큰 관리 방법으로 독특합니다. 토큰은 중앙 은행에서 발행하는 디지털 통화 및 암호화폐(비트코인 또는 이더리움)와 다릅니다.

토큰은 자산, 기간, 특정 장소 또는 특정 기업이 제공하는 서비스의 지분을 보유하고 있다는 증거입니다. 토큰은 두 가지 유형으로 나뉩니다. 대체가능 토큰(대체가능 토큰)과 대체불가 토큰(대체불가 토큰)입니다. 적용 시나리오와 구조에는 몇 가지 차이점이 있습니다. 당사의 분석에 따르면 대체불가 토큰이 토큰 이코노미에 더 광범위한 역할을 할 수 있습니다. 따라서 당사는 대체불가 토큰으로 분석을 시작할 것입니다.

대체불가 토큰(Non-Fungible Tokens)

대체불가 토큰을 이해하기 전에 해변에 있는 많은 돌멩이를 상상해보십시오. 실제 세계에서 해변의 모든 돌들은 다른 무게, 모양, 그리고 물질을 가지고 있습니다. 정확히 같은 돌은 없습니다. 또한 돌은 쉽게 함께 결합될 수 없습니다. 따라서 당사는 모든 돌은 '분리할 수 없다'고 말합니다.

블록체인의 예로는 한때 블록체인 세계에서 유행한 게임이었던 크립토키티가 있습니다. 각각의 고양이는 고유한 숫자와 속성을 가지고 있습니다. 대체불가 토큰은 개인, 돌 또는 블록체인 고양이와 유사합니다. 이렇게 현실에서 자연적으로 다르며 독특한 돌과 마찬가지로 대체불가 토큰은 당사 시스템에서 독특합니다.

일반적으로 대체불가 토큰은 다양한 값 유형에 따라 서로 다른 범주로 나뉩니다. 당사는 유사한 종류의 대체불가 토큰을 분류하여 도메인을 형성할 수 있습니다.

토큰으로 everiToken 의 높은 표준화 기능을 사용할 수 있습니다. 사용자가 발급한 모든 커스텀 토큰은 동일한 구조를 가집니다. 각 토큰에는 특정 **도메인**(토큰이 속한 분류)에 해당하는 하나의 **도메인 이름**이 있습니다. 또한 발행자는 도메인 내에서 고유한 **토큰 이름**을 지정합니다. 토큰 이름은 일반적으로 몇 가지 특별한 의미를 나타냅니다. 예를 들어, 제품의 바코드에는 원산지 및 제품 제조업체에 대한 정보가 포함된 네이밍 룰이 사용될 수 있습니다. 각 토큰의 고유성은 토큰 이름과 함께 도메인 이름에 따라 결정

됩니다. 또한 소유권에 대한 정보가 포함되며 각 토큰에는 하나 이상의 **소유자**가 있습니다.

위에서 언급한 바와 같이 토큰 **ID** 는 도메인 이름과 토큰 이름으로 고유하게 결정됩니다. 토큰의 기본 구조는 그림 1에 나와 있습니다. 토큰 ID 외에도 구조에는 토큰 소유자와 기타 필요한 정보가 표시됩니다.

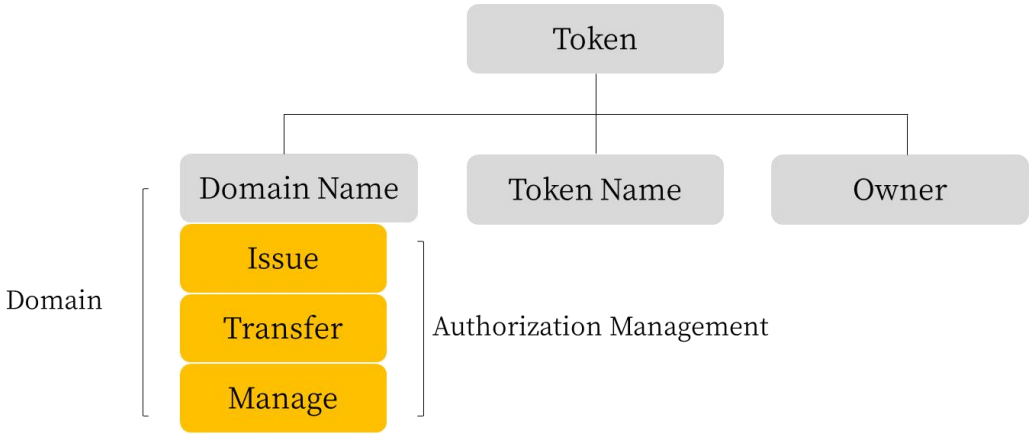


그림 1. everiToken 의 토큰 구조

도메인 이름을 통해 도메인 세부 정보를 문의할 수 있습니다. 각 도메인은 상대적인 권한 관리 정보도 표시합니다.

모든 사람은 자신의 토큰을 발행할 수 있는 권리가 있습니다. 토큰 자체는 가치가 없으며 유틸리티는 발행자의 실제 신용에 의해 보증됩니다. 새 토큰이 발급되면 트랜잭션을 통해 전송할 수 있습니다.

대체불가 토큰의 경우 토큰을 전송하는 것은 해당 토큰의 소유자를 변경하는 것을 의미합니다. 모든 토큰에는 **소유자 그룹**이 있습니다(하나 이상의 소유자가 있을 수 있음). 소유자 그룹을 변경해야 할 경우 토큰 변경의 구성원은 디지털 서명을 통해 작업을 확인할 수 있으며, 트랜잭션에서 사용권한 요구사항을 충족하고 다른 노드와 동기화되는지 확인한 후 토큰의 소유자 그룹이 변경됩니다.

권한 관리

everiToken 시스템에는 권한 관리에 대한 세 가지 권한(발행, 전송 및 관리)이 있습니다.

(1) **Issue** 는 도메인에서 토큰을 발급할 수 있는 권한입니다.

(2) **Transfer** 은 도메인의 토큰을 전송할 수 있는 권한입니다.

(3) **Manage** 는 권한 관리 및 기타 매개 변수를 포함하여 도메인을 수정할 수 있는 권한입니다.

각 특정 권한은 트리 구조를 따르므로 **권한 트리**라고 합니다. 각 사용 권한에는 임계값이 있으며 하나 이상의 actor 에 연결됩니다.

Actors

Actor 들은 계정, 정규 그룹, 소유자 그룹 세 그룹으로 분류될 수 있습니다.

계정은 개별 사용자이고, 그룹은 클러스터된 계정이며, 소유자 그룹은 특별한 형태의 정규 그룹입니다.

그룹은 클럽, 회사, 정부 부서, 재단 또는 개인일 수 있습니다. 그룹은 그룹의 공개 키와 각 구성원의 공개 키 및 가중치를 보유합니다. 작업을 승인하는 그룹의 모든 인증된 구성원의 총 가중치가 그룹의 필요한 임계값을 충족할 경우 작업이 승인됩니다.
그룹의 공개 키를 보유한 구성원은 그룹 구성원과 가중치에 대한 수정을 승인할 수 있습니다. 이 메커니즘은 **집단 자율성**이라고 불립니다.

그룹이 시작되면 시스템은 자동으로 그룹 ID 를 생성합니다. 발행자가 도메인에 대한 권한 관리를 설계할 때 기존 그룹 ID 를 사용 권한 시스템에 직접 참고하여 실행할 수 있습니다. 집단 자율성으로 각 그룹을 편리하게 재사용할 수 있습니다.

토큰 소유자는 토큰 소유자의 집합을 나타내는 고정된 이름 '.owner'를 가진 특수 그룹 이름을 가집니다. 항상 각 토큰의 실제 소유자를 지칭하기 때문에 특별하고 유연하며 그룹의 승인 조건은 그룹 내에서 모든 사람이 동의하는 것입니다(즉 그룹 내 각 사람의 가중치는 1 이고 그룹의 임계값은 그룹 내 구성원 수입니다).

관리

권한은 토큰 발행자에 의해 시작되며 각 권한은 하나 이상의 그룹에 의해 관리됩니다. 토큰이 발행되면 발행자는 각 권한에 따라 각 그룹의 정보와 상대적 가중치를 지정하고 토큰 임계값을 설정합니다. 특정 도메인에서 작업을 실행하기 전에 시스템은 먼저 운영 그룹의 가중치가 충분한지 확인하고 가중치가 임계값을 초과할 경우에만 작업을 승인합니다. 이러한 그룹화 설계는 실제 세계의 많은 상황에 적합하며 가중치와 임계값의 유연한 설정은 모든 종류의 복잡한 조건을 충족시킵니다. 예로 그림 2 를 참고하십시오.

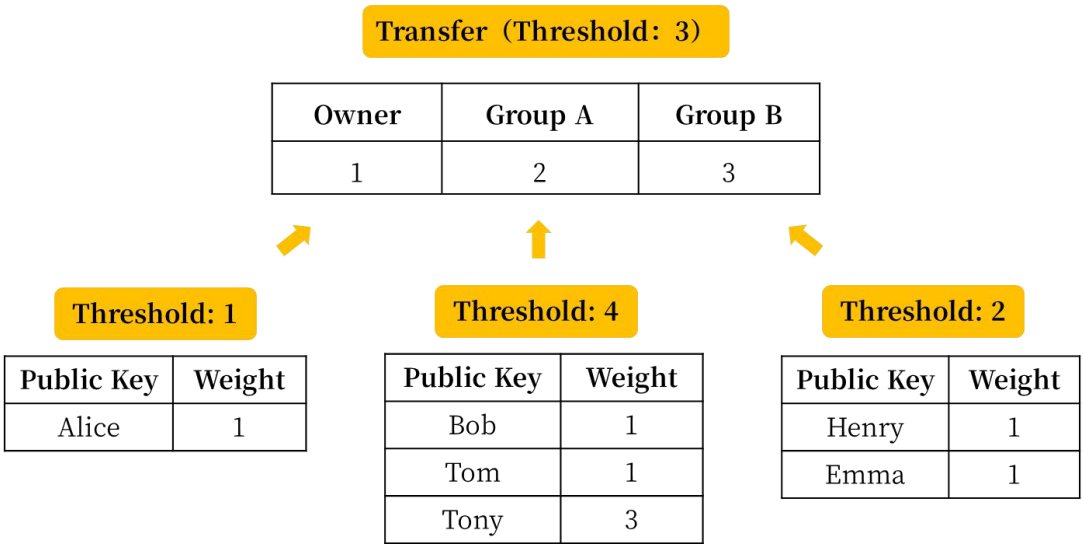


그림 2. 전송 권한

그림 2 는 도메인의 전송 권한을 설명합니다. 임계값은 3 이고, 소유자, 그룹 A, 그룹 B 등 3 개의 그룹이 있습니다. 각 그룹의 현재 가중치 집합을 기준으로 소유자와 그룹 A 가 함께 권한을 부여해야 하거나 그룹 B 가 전송 임계값을 충족하도록 단독으로 권한을 부여할 수 있습니다.

Owner 는 Alice 의 권한을 부여받습니다. 그룹 A 는 Bob/Tony 또는 Tom/Tony 의 권한으로 임계값(4)를 충족할 수 있습니다. 그룹 B 는 임계값(2)을 충족할 수 있도록 Henry 와 Emma 모두의 권한을 받아야 합니다.

모든 사용자는 토큰을 발행할 권한이 있지만 각 도메인의 토큰의 상황에 따라 시나리오는 다릅니다. 예를 들어 재산 이전은 엄격한 감독 하에 정부 관계 기관에 의해 검토되어야 합니다. 예를 들어, 체인의 회원 카드와 쿠폰은 그들을 승인하기 위해 회사의 브랜드를 필요로 하고 콘서트 티켓은 콘서트가 끝난 후에 쓸모없어집니다. 하지만 고정된 주차장의 주인은 시간에 따라 바뀔 수 있습니다.

토큰을 발행할 때 토큰의 발행자는 도메인에서 사용 권한을 설계하여 권한 관리를 구현할 수 있습니다. 다음의 시나리오는 권한 관리의 편리함을 보여줍니다.

그림 3 은 everiToken 의 권한 관리 메커니즘을 사용하여 복잡한 문제를 해결할 수 있는 방법을 보여줍니다.

한 회사가 새 사무실 건물을 지었고 건물의 재산권을 가진 1000 개의 토큰을 발행하기를 희망하고 있습니다. 본 업체는 이러한 토큰을 발행하고 유지하기 위해 특수 목적 회사(Special Purpose Vehicle)을 설립합니다. 실제 세계에서는 재산의 토큰 발급 및 양도를 검토하고 지역 재산 관리국의 승

인을 받아야 합니다. 현지 기준에 따라 발행해야 하며 토큰 상세 내역(총계, 발행인, 권한 관리 구조 등)을 공식 플랫폼에 표시해야합니다. 게다가 중앙 재산 관리국은 지방 재산 관리국과 소유자를 제한하고 관리하는 최고 권한을 가지고 있습니다.

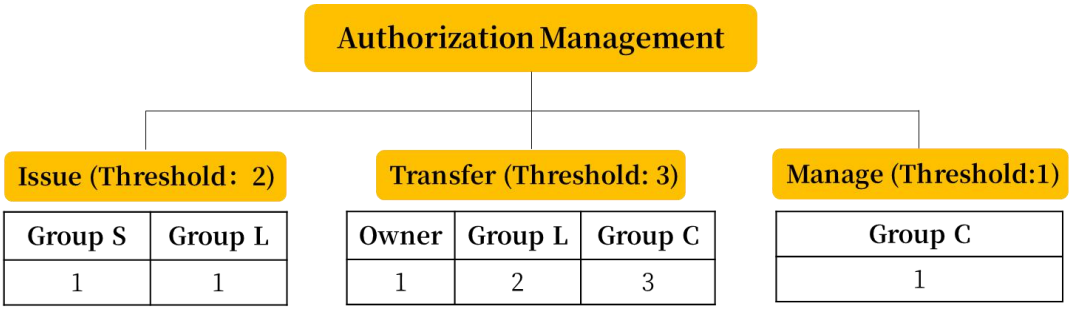


그림 3. 권한 관리 구조

Group S 는 도메인에 있는 토큰의 SPV(특수 목적 회사), 발행자 및 초기 소유자를 나타냅니다. **Group L** 은 지역 재산 관리국을 나타내고, **Group C** 는 중앙 재산 부서를 나타냅니다.

대부분의 경우 토큰을 양도하려면 소유자 및 지역 재산 관리국의 승인만 필요합니다(결합 가중치 3 이 임계값을 충족함). 이 과정에서 전송 방식은 지방 재산국의 감사를 받습니다. 토큰 소유자에게 개인키 분실, 사망 등의 사고가 발생한 경우 중앙 재산 관리부는 법원 또는 관련 부서의 판단이나 검토를 거쳐 토큰 소유권을 법정 상속인에게 양도할 수 있습니다.

SPV 및 다른 토큰 소유자가 새 토큰을 추가하기로 동의하는 경우, 발행 기관이 실제 요구를 충족하여 새 토큰을 추가할 수 있습니다. 또한 권한 관리 구조는 극단적인 경우를 처리하는 데에도 적합합니다. 예를 들어 중앙 재산 부서에서 이런 유형의 토큰 확산을 일시적으로 중지해야 하는 경우에는 보유하고 있는 관리 권한을 통해 전송 권한의 임계값을 변경하여 도메인에 있는 모든 토큰의 유통을 동결할 수 있습니다.

대체가능 토큰(Fungible Tokens)

발행

누구나 EVT 와 같은 고유 심볼로 등록 후 대체가능 토큰을 발행할 수 있습니다. 사용자는 이 심볼을 사용하여 총 토큰 수를 설정할 수 있습니다. 그런 다음 사용자는 즉시 발행하고자 하는 토큰 수를 결정할 수 있습니다.

전송

개인 키를 가진 사람은 누구나 토큰을 다른 사람에게 양도할 수 있습니다.

기타 세부사항

각 계정은 관련 심볼과 함께 보관되는 토큰 수를 기록합니다. 서로 다른 심볼이 있는 토큰의 기본 정보를 저장하는 독립적인 키값 기록이 있습니다. 또한 사용자는 다른 개인 키가 지정된 심볼을 사용하여 지정된 수의 토큰을 전송할 수 있는 권한을 갖도록 허용할 수도 있습니다. 이 기능을 **토큰 허용량**이라고 하며 토큰 거래소에서 사용할 수 있습니다.

토큰 기반 트랜잭션 모델

개요

everiToken 은 시스템 내의 모든 토큰과 관련하여 **토큰 기반 트랜잭션 모델**을 사용합니다.

토큰 기반 레저의 각 토큰에 대해 토큰 소유권의 전체 기록을 저장할 독립 데이터 공간을 생성합니다. 이렇게 하면 지정된 토큰의 데이터 공간이 다른 토큰과 관련이 없기 때문에 샤딩 및 멀티 코어 병렬 처리를 매우 쉽게 수행할 수 있습니다. 따라서 다양한 토큰의 작동이 충돌 없이 병렬로 쉽게 수행될 수 있습니다. 또한 CPU 코어를 쉽게 샤딩하거나 추가하여 TPS 를 지속적으로 개선하고 초고성능을 실현할 수 있습니다.
토큰 기반 트랜잭션 모델은 everiToken 의 여러 핵심 팀 구성원에 의해 개발되었으며 대체불가 토큰에 적합한 것으로 입증되었습니다.

everiToken 과 같이 토큰 기반 트랜잭션 모델을 사용하는 블록체인은 데이터베이스를 Token DB 와 Block DB 두 부분으로 나눌 수 있습니다. 토큰 기반 트랜잭션 모델이 모든 대체불가 토큰의 데이터 공간을 작동, 저장 및 관리하는 것입니다. 반면 Block DB 는 오리지널 블록을 저장합니다.

블록이 되돌아 갈 경우 빠르게 롤백하려면 Token DB 와 Block DB 모두 다중 버전 데이터베이스여야 합니다. 예를 들어 everiToken 은 Rocks DB 를 Token DB 의 기본 데이터베이스 시스템으로 사용합니다.

Token DB 및 Block DB 는 변경/추가 전용(append-only) 데이터베이스입니다. 따라서 다른 사용자가 기록를 업데이트할 때마다 향상된 버전의 새 값이 데이터베이스에 추가됩니다. 그러나 이전 버전이 포함된 기록은 제거되지 않습니다.

Token DB

Token DB 는 토큰 소유권 및 체인에 있는 대체가능 토큰의 계정 잔액과 같은 블록체인의 최신 상태를 신속하게 검색하고 변경할 수 있는 인덱스 데이터베이스입니다.

Token DB 는 키값 데이터베이스(key-value database)입니다. 키는 토큰의 ID 를 나타내고 값은 토큰의 현재 소유권을 나타냅니다. 데이터베이스가 변경/추가 전용(append-only)이기 때문에 각 키에 대해 많은 값이 존재하지만 최신 값만 토큰의 현재 소유 상태를 나타내며 다른 값은 이전 참조 및 롤백에만 사용됩니다. 각 토큰에는 별도의 체인처럼 모든 소유권 기록을 포함하는 독립 데이터 공간이 있습니다.

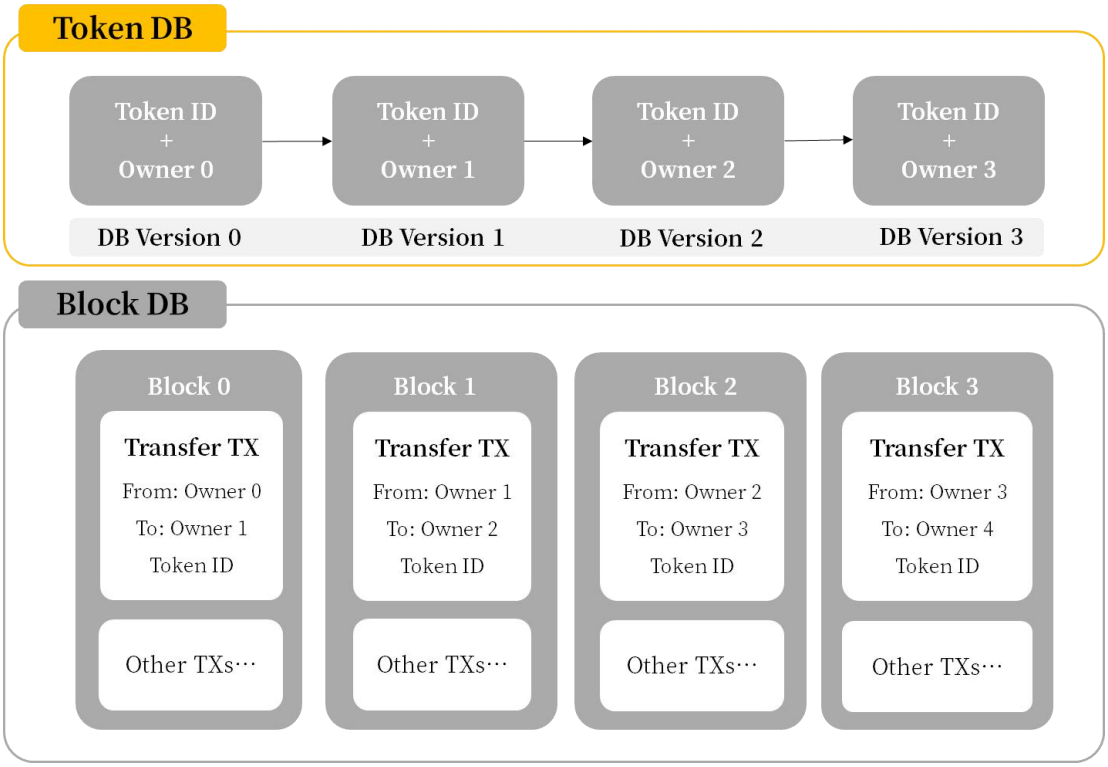
체인의 첫 번째 값은 초기 소유권입니다. 예를 들어 트랜잭션을 실행하면 데이터베이스에 새 소유권이 추가됩니다. 블록을 되돌려야 하고 최종적으로 가비지 콜렉션(garbage collection)이 되는 경우 이전 버전을 사용하여 값을 롤백할 수 있습니다.

각 토큰에는 독립적인 데이터 공간이 있기 때문에 샤딩이 매우 쉽습니다. 예를 들어, 한 노드에 컴퓨터가 두 대 있는 경우 각 컴퓨터에서 토큰의 절반을 처리할 수 있습니다. 토큰이 100 개라면 첫 번째 컴퓨터에서 토큰을 1 - 50 개, 두 번째 컴퓨터에서 토큰을 51 – 100 개 처리합니다. 토큰의 소유자를 변경하면 다른 토큰에는 영향을 주지 않으므로 두 시스템이 병렬로 처리될 수 있습니다.

Block DB

Block DB 는 체인의 되돌릴 수 없는 모든 오리지널 블록을 저장하는 역할을 합니다. 각 블록에는 이름, 실행된 작업의 매개 변수, 블록의 서명 등을 포함한 모든 상세 정보가 저장됩니다.

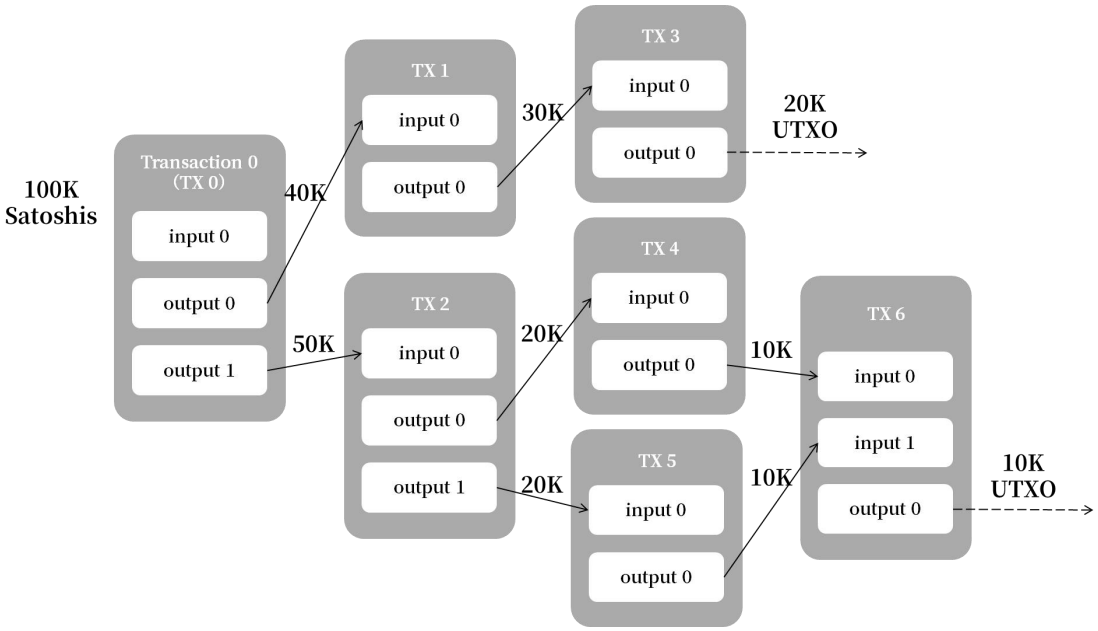
다음 그래프는 대체불가 토큰에 대해 두 가지 유형의 데이터베이스가 함께 작동하는 방식을 보여 줍니다:



트랜잭션 모델 비교

a) UTXO

UTXO 모델에서 각 토큰 소유자는 이전 트랜잭션의 해시 및 다음 소유자의 공용 키(주소)에 디지털 서명하여 자신이 소유한 코인을 다른 소유자에게 전송합니다. 이 메커니즘은 기본적으로 입력(input)과 출력(output)의 연속적인 활동이며 토큰 소유자가 실제로 토큰을 직접 소유하지 않고 특정 수의 토큰에 대한 출력을 소유하며, 이 출력은 새 출력을 제어하는 새 소유자에게는 입력의 역할을 합니다.



(출처: bitcoin.org)

UTXO 는 어떤 입력도 단 한 번만 사용할 수 있어서 이중 지출을 방지하는 데 유용하지만 다음과 같은 몇 가지 단점이 있습니다.

- BTC 는 대체불가 토큰이 아니라 대체가능 토큰입니다. 모든 UTXO 에 고유한 ID 를 유지하는 것은 쓸모가 없습니다(everiToken 은 대체불가 토큰과 대체가능 토큰를 모두 지원합니다).
- UTXO 는 일회성입니다. 엄청난 양의 UTXO 를 저장하는 것은 컴퓨팅 리소스와 디스크 용량의 낭비입니다.

b) 계정 기반

계정 기반 트랜잭션 모델은 은행이 하는 것과 같습니다. 은행에 계좌를 만든 다음 잔고를 변경하여 계좌에 돈을 저축합니다. 이것은 UTXO 의 작동 방식과는 완전히 다릅니다. 새 UTXO 를 생성하지 않고 데이터베이스의 잔액만 업데이트하면 되기 때문에 UTXO 보다 효율적입니다. 따라서 UTXO 모델은 대체불가 토큰에 적합하지 않습니다.

잔액 기반 모델은 다른 사람에게 전송할 때 두 가지 단계를 필요로 하기 때문에 샤딩에 능숙하지 않습니다. 첫째는 구 보유자의 계정을 수정하는 것이고, 둘째는 새 보유자의 계정을 수정하는 것입니다. 안전상의 이유로 한 번의 원자 단위 연산(atomic operation)으로 두 가지 단계를 수행해야 하지만 샤딩 환경에서는 그것이 어렵고 성능 수준이 열악합니다. 그러나 토큰 기반 트랜잭션 모델에는 토큰의 새 소유권을 추가하는 단 하나의 단계가 있습니다.

보안성

토큰의 기능에 초점을 맞추어 everiToken 은 불필요한 추상적 개념을 간소화하여 효율성을 크게 높일 뿐만 아니라 뛰어난 안전성을 제공합니다. 토큰의 유형은 이론적으로 제한이 없을 수 있지만 통합된 토큰 구조를 통해 시스템 또는 타사가 동일한 원칙에 따라 토큰을 감사할 수 있습니다. 시스템은 하나의 형태의 스마트 계약만 인식하므로 복잡한 감사와 보안의 영향을 피할 수 있습니다.

everiToken 코어 코드베이스

everiToken 은 2019 년 봄부터 Hacken Proof, Chaitin 등 4 개 퍼블릭체인 코어 코드 검토 조직을 도입했습니다. 정적 및 동적 분석이 모두 있습니다.

everiToken 은 *안전계약*을 사용하므로 당사의 코어 코드베이스가 안전하다는 것이 증명되면 everiToken 을 기반으로 한 모든 계약도 안전하다는 것이

증명됩니다.

스크립트 (everiSigner)

everiSigner 는 브라우저용 오프라인 서명 플러그인입니다. 이 추가 기능 내에서 전체 서명 과정이 수행되므로 개인 키가 노출되지 않습니다. 웹사이트는 보안을 보장하기 위해 새 채널을 만들어 everiSigner 를 사용합니다. 웹사이트는 서명할 자료를 채널에 전달합니다. 그런 다음 everiSigner 가 서명된 데이터를 반환합니다.

개인 키 분실

권한 관리를 사용하여 타사에서는 많은 서비스를 제공할 수 있습니다. 예를 들어 C 사는 암호 보호 서비스를 전문으로 하며 Alice 는 자신의 토큰의 개인 키를 잊어버렸거나 잃어버릴까봐 두려워합니다. Alice 는 도메인의 소유자 (1), 그룹 C (1)에 대한 전송 권한을 관리하고 임계값을 1 로 설정할 수 있습니다. 앨리스가 개인키를 잊어버려 스스로 허가를 받지 못했다면 그녀는 자신이 신분증이나 지문을 통해 C 사에 앨리스임을 증명하여 여전히 C 그룹을 통해 허가를 받을 수 있습니다. 이러한 방법으로 앨리스는 토큰을 확인 후 새 계정으로 전송하여 복구할 수 있습니다.

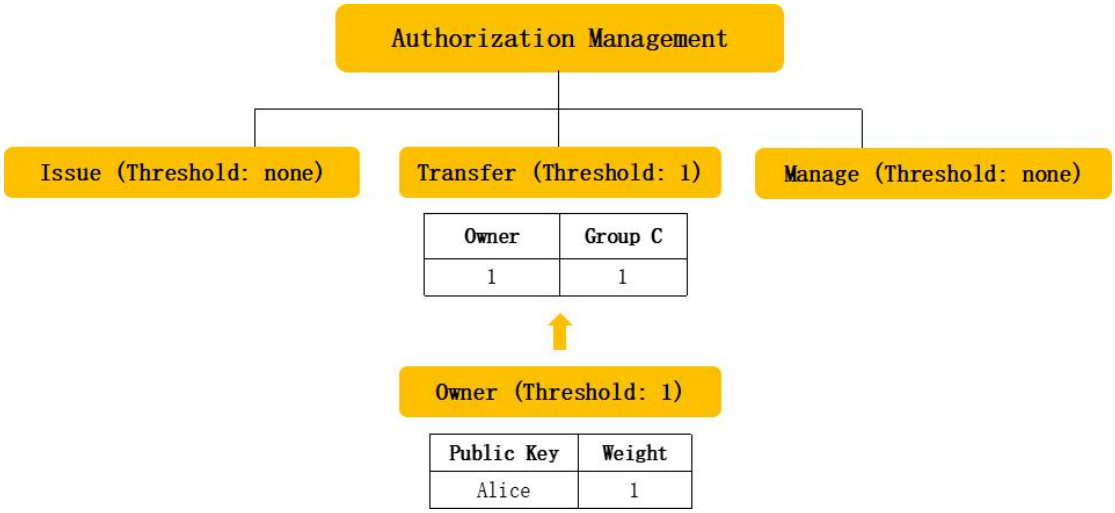


그림 4. C 사는 키를 되찾아주는 서비스를 제공합니다

물론 C 그룹은 앨리스의 토큰을 훔칠 수도 있지만 모든 과정은 체인에 기록될 것이고 이것은 C 그룹의 신용을 파괴할 것입니다.

컨센서스 알고리즘

everiToken 은 BFT-DPOS 를 합의 알고리즘으로 사용합니다. DPOS 는 온체인에 있는 애플리케이션의 성능 요구 사항을 충족할 수 있습니다. 이 알고리즘에 따르면 EVT 를 보유한 사람은 승인 투표 시스템을 통해 블록 프로듀서를 선택할 수 있습니다. 누구든지 블록 생성에 참여할 수 있으며 토큰 소유자에게 투표하도록 설득할 수 있다면 블록을 생성할 수 있는 기회가 주어집니다.

everiToken 은 0.5 초마다 블록을 생성할 수 있으며 단 한 명의 프로듀서가 블록을 생성할 수 있도록 승인됩니다. 예약된 시간에 블록이 생성되지 않으면 해당 시간 슬롯의 블록을 건너뜁니다. 하나 이상의 블록을 건너뛰면

블록체인에 0.5 초 이상의 간격이 생깁니다.

everiToken 퍼블릭체인의 블록 프로듀서 수는 유연합니다. 초년도에는 15 명의 프로듀서로 제한되어 있습니다. 그리고 그 숫자는 온체인 거버넌스 위원회가 결정할 것입니다. 편의상 백서에는 15 개를 사용합니다.

everiToken 에서는 블록이 180(각 12 개 블록에 15 개를 곱한 값)개로 생성됩니다. 각 라운드가 시작될 때 15 개의 고유 블록 프로듀서가 EVT 보유자에 의해 투표된 선호도에 의해 선택됩니다. 선정된 프로듀서는 11 명 이상의 프로듀서가 합의한 순서에 따라 일정을 잡습니다.

프로듀서가 블록을 놓치고 지난 24 시간 이내에 블록을 생성하지 않은 경우, 블록체인에 블록 생성을 다시 시작하겠다는 의사를 통지할 때까지 고려 대상에서 제외됩니다. 따라서 신뢰할 수 없는 것으로 입증된 프로듀서를 스케줄링하지 않음으로써 누락된 블록 수를 최소화하고 네트워크가 원활하게 작동하도록 보장합니다.

비잔틴 장애 허용(Byzantine fault tolerance)은 모든 프로듀서가 서명한 모든 확인을 요구함으로써 사용자에게 추가적인 보안과 안전을 제공하기 위해 사용됩니다. 어떠한 프로듀서라도 동일한 타임스탬프 또는 동일한 블록 높이의 두 블록에 서명할 수 없습니다. 11 명의 프로듀서가 블록에 서명하면 되돌릴 수 없습니다. 비잔틴 프로듀서가 동일한 타임스탬프나 블록 높

이로 두 블록에 서명을 하면 반역 행위에 해당하는 암호화 증거가 생성됩니다.

보너스 디자인

보너스는 2019 년 2 월 'everiToken 3.0'이 출시되면서 추가되었습니다. 강력하고 유연하며 편리한 요소로 기존 기능과 결합하였습니다. 정해진 규칙에 따라 이해관계자나 주주에게 이익을 분배하기 위해 고안되었습니다. 이익의 수령 방법에 따라 현재 지원되는 보너스에는 패시브 보너스 및 능동 보너스 두 가지가 있습니다.

패시브 보너스인 경우, 하나의 대체가능 토큰 내에서 매 트랜잭션 동안 이익을 수령하게 됩니다. 따라서 만약 하나의 대체가능 토큰 관리자들이 패시브 보너스를 설정하기로 한다면 모든 거래에서 EVT 는 연료로 부과될 뿐만 아니라 대체가능 토큰에 대한 추가 비용도 부과될 것입니다.

하나의 트랜잭션에서 수수료를 제어하는 몇 가지 옵션이 있습니다. 주요 옵션은 트랜잭션 수수료율입니다. 수수료는 수수료율에 거래 금액을 곱한 것입니다. 또한 최종 수수료의 상한과 하한 범위를 제한하는 최소 및 한계치 관리 옵션이 있습니다. 따라서 고부가가치 트랜잭션에 대한 과도한 비용이 방지됩니다.

대체가능 토큰 관리자는 수수료를 어떻게 부과할지 결정할 수 있습니다. 예를 들어 누가 수수료를 부담할 것인지와 요금 지불 방법을 선택할 수 있습니다. 첫 번째 방법은 신용 카드와 유사하며 납부자는 *n* 의 금액을 지불하지만 수수료는 최초 금액에서 차감되기 때문에 수취인은 *n* 보다 적게 받습니다. 두 번째 방법은 전통적인 은행거래에 가깝습니다. *n* 금액을 다른 금액으로 이체하고자 하는 경우, 원래 금액보다 더 많은 수수료를 지불해야 합니다.

액티브 보너스는 주식의 배당금과 유사하게 수작업으로 게시합니다. 상여금을 얼마나 나눌지는 대체가능 토큰 관리자가 결정합니다.

보너스 지급이 액티브든 패시브든 분배 규칙에 대한 정의가 설정되어 있어야 합니다. 현재 세 가지 유형의 규칙이 유효합니다. 고정, 백분율 및 나머지 백분율입니다. 고정 규칙은 수취인에게 보장되는 고정 금액이며, 백분율 규칙은 보너스 총 금액의 백분율 곱으로 계산됩니다. 나머지 백분율 규칙은 고정 규칙과 백분율 규칙과는 별개이며 나머지 양에 백분율 값을 곱한 값으로 구성됩니다.

각 규칙에 맞게 수취인을 선택해야 합니다. 수취인은 하나의 주소에만 국한된 것이 아니라 하나의 대체가능 토큰을 보유할 수 있으며 각 보유자는 그 대체가능 토큰의 총 공급과 관련하여 그의 잔액에 따라 금액을 받을 수 있습니다. 또한 대체가능 토큰의 이해관계자는 이익을 위해 사용되는 대체

가능 토큰에 국한되지 않고 등록되어 있는 모든 대체가능 토큰을 사용할 수 있습니다. 따라서 오로지 영리 목적으로만 '보너스 토큰'을 발행할 수도 있으며 everiToken 이 제공하는 투명성, 공정성, 유동성의 혜택을 받을 수 있습니다.

수취인이 2 개 이상의 주소를 가지고 있을 때 잔액과 모든 이해관계자의 주소의 스냅샷을 찍어야 합니다. 각 이해관계자 주소는 34 byte 가 소요되기 때문에 스토리지를 훨씬 더 차지합니다. 당사는 이 상황을 최적화했으며 대부분의 경우 각 주소를 저장하는 데 4 byte 밖에 들지 않습니다. 100 만 명 이상의 이해 관계자의 경우 비용은 약 4 Mbyte 에서 34 Mbyte 가 될 것입니다. 토큰 데이터베이스의 미세조정(fine-tune) 최적화 덕분에 시스템은 매우 낮은 비용으로 이해관계자 잔액을 읽고 업데이트할 수 있습니다.

락업(Lock) 기능

락업 기능은 everiToken 의 시스템에서 지원됩니다. 대체불가 토큰이나 대체가능 토큰을 일정 기간 락업할 수 있습니다. 이는 락업 제안 중에 설정된 조건에 따라 달라집니다. 락업 시간 동안 조건이 충족되었는지 안되었는지 간에 일정 기간 후에 락업 해제된 자산은 다른 등록된 주소로 전송됩니다. 현재 락업 조건은 공개 키로만 조정할 수 있으므로 락업 기간 동안 특정 제안에 대해 승인된 키만 접근할 수 있습니다.

기타 기술 세부사항

베이식체인

당사는 바퀴를 재발명하고 싶지 않습니다. 따라서 기존의 퍼블릭체인 시스템의 우수한 부분을 받아들이고 약점도 개선했습니다. Graphene(DPOS+PBFT)을 합의 알고리즘으로 채택하였으며 합의 알고리즘은 DPOS3.0(EOS 코드베이스)에서 생성되었으며 당사가 자체 개선하였습니다. EOS 가 훌륭한 코드 구조를 가지고 있다는 것을 인식하고, 코드 구조의 일부를 유지했습니다. 그러나 이 부분을 제외한 퍼블릭 체인의 다른 부분은 완전히 새로 개발하였습니다.

개발 방면으로는 Safe Contract(스마트 계약 대신), 새로운 데이터베이스 모델(성능 향상을 위한 RocksDB 기반)과 토큰 지불 프로토콜 everiPay 를 구축합니다.

다음과 같은 많은 이점이 있습니다:

- Graphene 은 오랜 기간을 통해 검증되었습니다. DPOS 및 기타 핵심 메커니즘은 BitShare 또는 EOS 와 같은 프로젝트에서 완전히 검증되었습니다.
- 합의 알고리즘을 재사용하면 작업량의 일부를 줄일 수 있으므로 핵심 기능 개발에 집중할 수 있습니다.

권한 작업

everiToken 의 권한 작업에는 다중 서명, 가중치 계산, 임계값 설정 등이 있습니다. 각 토큰의 전송은 다른 토큰과 독립적이므로 서로 다른 토큰의 전

송 작업을 동시에 실행할 수 있습니다. 또한 각 그룹의 허가 상태가 독립적이므로 발급 및 관리 작업도 서로 다른 그룹과 동시에 실행할 수 있습니다.

각 트랜잭션은 데이터 패킷과 서명 목록으로 구성됩니다. 인허가 확인의 경우, 각 서명만 확인하면 됩니다. 서명 간에 관계가 없으므로 권한 작업을 병렬로 실행할 수 있습니다.

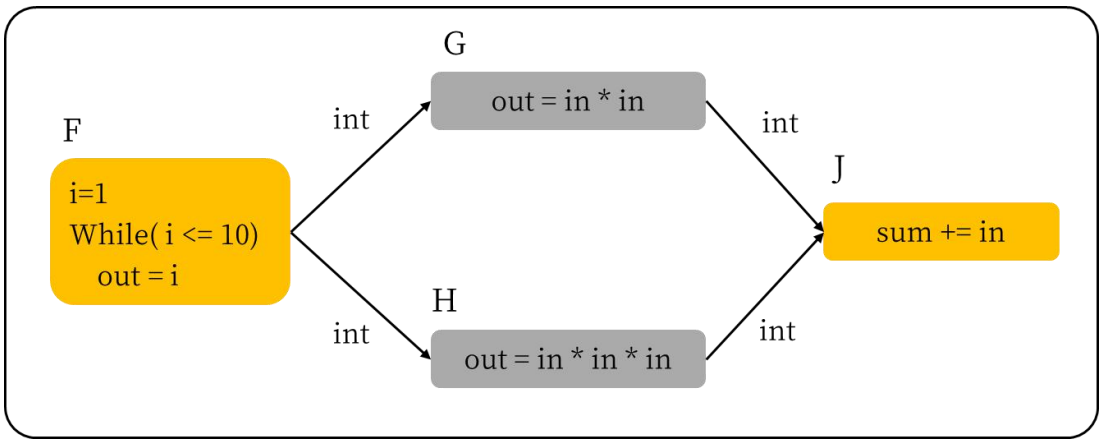
실행 엔진

everiToken 의 시스템에서는 각 토큰 작업이 완전히 독립적이기 때문에 병렬 과정에서 추가 파티션이 필요하지 않습니다. 또한 토큰 오퍼레이션의 유형이 제한되므로 코드도 기본 제공됩니다. 각 오퍼레이션을 반복적으로 테스트하는 한 시스템은 완전히 안정적입니다.

한개의 트랜잭션은 서명 복구, 권한 검사, 계산, 데이터베이스 작성 등과 같은 여러 단계로 나눌 수 있습니다. 모든 단계를 순차적으로 실행해야 하지만 일부 단계는 서로 다른 트랜잭션에서 서로 독립적입니다. 이러한 단계 중 하나는 *서명 복구(signature-recovering)*라고 합니다. 각 트랜잭션의 서명에 종속성이 없으며 트랜잭션의 각 서명도 독립적입니다. 따라서 서명을 다른 작업과 동시에 복구하는 것은 문제가 되지 않습니다. 또 다른 단계는 *권한 검사(authorization checks)*입니다. 언뜻 보면 서명을 복구하는 것과 같은 것으로 보이지만 토큰 전송의 두 가지 트랜잭션을 확인하는 것을

상상해 보십시오. 각 토큰이 다른 토큰의 기능에서 아무런 역할을 하지 않더라도 동일한 토큰을 전송하는 트랜잭션이 두 개 있을 때 시스템에서 계속 병렬로 검사하면 예기치 않은 동작이 발생합니다. 토큰 소유자가 검사에 참여하기 때문에 첫 번째 거래에서 토큰이 변경될 수 있습니다.

따라서 단계를 동시에 실행할 방법은 없지만 이러한 상황은 신중하게 계획될 수 있습니다. 당사가 구현한 것은 아래 *의존성(dependence) 그래프*에 나와 있습니다. 당사 시스템은 그래프 병렬 처리를 통해 데이터 흐름을 병렬화합니다. 계산은 노드로 표현되며 이러한 계산 사이의 통신 채널은 엣지(edges)로 표현됩니다.



위는 1 에서 10 까지의 정사각형과 큐브의 시퀀스 합계를 계산하는 방법의 예입니다. 구현 시 각 노드는 트랜잭션의 한 단계를 나타내며 트랜잭션을 수신하고 분할하여 전체 그래프를 작성하는 스케줄러가 있습니다.

일시정지된(Suspended) 트랜잭션

일시정지된 트랜잭션은 여러 번의 지연 후 완료된 트랜잭션입니다. 통상적인 거래는 한번에 이루어지며 모든 조건은 트랜잭션이 제출될 때 충족되어

야 합니다. 예를 들어 모든 서명자는 함께 서명해야 합니다. 그러나 실제로는 많은 트랜잭션은 과정을 통해 완료됩니다. 트랜잭션의 참가자는 동시에 서명을 못할 수 있습니다. 일시정지된 트랜잭션을 통해 트랜잭션이 성공할 때까지 서명을 단계별로 제공할 수 있습니다.

everiPay / everiPass / EvtLink

everiPay / everiPass

everiPay/everiPass 는 everiToken 퍼블릭 블록체인을 사용하여 대면(face-to-face) 마이크로페이를 위해 생성된 결제 방법입니다.

EvtLink 는 QR 코드 생성과 통신 프로토콜을 제공합니다.

다음은 everiPay/everiPass/EvtLink 와 관련된 몇 가지 주요 내용입니다:

- **즉각 승인**: 트랜잭션은 곧 결제입니다.
- **탈중앙화**: P2P 지불이 가능하고, 중앙화 플랫폼이 없고, 아무도 온체인 데이터를 수정할 수 없으며 누구나 가격경쟁에 참여할 수 있습니다.
- **최고의 보안**: 사용자 재산의 보호 및 보안을 극대화하기 위해 블록체인 내의 데이터와 콘텐츠를 위조하거나 변조할 수 없습니다.
- **최고의 편리함**: 인터넷에 연결할 수 없어도 트랜잭션을 완료할 수 있습니다. 수취인/지급인은 수동으로 금액을 입력할 필요가 없습니다. 지급인과 수취인은 거래가 성공하는 즉시 통지를 받게 됩니다.
- **호환성**: everiPay/everiPass 는 항상 everiToken 이 지원하는 모든 토큰과 화폐, 포인트, 심지어 문을 여는 열쇠까지 지원합니다. 가장 좋은 점으

로는 핸드폰만 있으면 어디에서든 사용할 수 있습니다.

- **빠른 속도:** everiToken 은 매우 높은 TPS 를 빠르게 달성했으며 장비나 네트워크의 품질에 따라 1~3 초 이내에 트랜잭션을 완료할 수 있습니다.

- **표준화**: EvtLink 는 전체 에코시스템을 위해 직접 만든 크로스 월렛, 크로스 체인 및 크로스 애플리케이션이 있습니다. 어떠한 앱도 생성하거나 파싱(parse)할 수 있습니다.

상기의 7 가지 특징을 바탕으로 everiPay/everiPass 는 대면(face-to-face) 결제 산업에서 가장 안전하고 편리하며 사용자 친화적인 서비스를 제공할 수 있습니다.

everiPay/everiPass 의 경우 수취인은 EvtLink 를 파싱(parsing)하고 everiToken 으로 트랜잭션을 보낼수 있는 애플리케이션을 사용해야 합니다. 개발자에게 사용하기 쉬운 API 와 코드를 제공하여 사용하기 편하고 쉽게 만들어졌습니다. 이는 해당 스토어에 대한 알리페이/위챗 지원을 추가하는 것과 유사하지만 훨씬 더 쉽습니다.

수취인 QR 코드

수취인 QR 코드는 everiPay 가 제공하는 많은 기능을 지원하지 않습니다. 예를 들어 수취인 QR 코드 트랜잭션을 완료하려면 지급인이 인터넷에 연결해야 하며 지급인와 수취인 모두 수동으로 거래 금액을 입력해야 합니다. 또한 결제 완료 시 자동 통지가 되지 않습니다.

수취인은 이런 결제 방식을 지원하는 애플리케이션을 사용할 필요가 없습

니다. 수취인은 지급인으로부터 돈을 받았는지 확인하기 위해 단말기에 있는 everiToken 이 지원하는 지갑을 사용하면 됩니다. 모든 종류와 규모의 벤더사와 사람간의 교환에도 적합합니다.

수취인 QR 코드 대신 everiPay 을 권장하는 이유는 투명하고 안전하며 사용자 친화적이기 때문입니다.

EvtLink 는 어떻게 작동합니까?

EvtLink 는 everiPay/everiPass 를 나타내는 바이너리 포맷(binary format)의 표준입니다. everiToken 퍼블릭체인은 evtLink 에서 트랜잭션을 실행하기 위해 everiPay 및 everPass 를 활용합니다.

다음은 기술적 관점에서 everiPay/everiPass 를 통한 결제 과정입니다:

1. 지급인이 사용할 토큰 종류를 선택하면 지급인의 지갑에는 고유한 128-bit LinkId, 지급인의 서명 및 지급에 사용되는 토큰의 심볼로 구성된 일련의 동적 QR 코드가 표시됩니다. 트랜잭션을 실행하지 않는 한 QR 코드 스와핑 중에는 LinkId 를 변경하지 않아야 합니다. 체인은 동일한 LinkId 를 사용하는 EvtLink 에서 두 가지 작업을 허용하지 않으므로 중복 지급의 위험이 방지됩니다.
2. 지급인의 지갑 애플리케이션은 유효한 트랜잭션 ID 를 반환할 때까지 'get_trx_id_for_link_id' API 를 호출하여 LinkId 와 관련된 트랜잭션을 지속적으로 쿼리(query)해야 합니다. 그런 다음 QR 코드가 표시

되면 LinkId 를 변경해야 합니다. 또한 트랜잭션 ID 를 쿼리(query)하여 트랜잭션 결과를 표시합니다. 지급인 지갑은 트랜잭션을 직접 보낼 필요가 없습니다.

3. 수취인은 자신의 전화, 스캐너 또는 스마트 게이트웨이를 사용하여 QR 코드를 스캔합니다. EvtLink 를 스캔하고 파싱한 후에는 래핑(wrap)해서 체인으로 옮겨집니다. 그 후 모든 체인 노드가 동기화되고 'get_trx_id_for_link_id'가 트랜잭션 ID 를 반환합니다.

Base42 인코딩

Base42 는 바이너리-스트링(binary-to-string)변환을 위한 인코딩 알고리즘입니다. hexadecimal 인코딩과 유사하지만 대신 42 를 기준으로 사용하고 그에 따라 고유한 알파벳 시퀀스를 사용합니다. 알파벳의 문자는 QR 코드의 알파뉴메릭 모드 인코딩의 문자와 동일하므로 base42 인코딩 문자열을 QR 코드로 적용하는 것이 효율적입니다. 따라서 QR 코드가 작아져 보다 편리한 스캔이 가능합니다.

everiToken 에서는 *base42* 가 EvtLink 의 콘텐츠를 인코딩하는 데 사용됩니다.

Part III. 경제 모델

가스 수수료/연료(EVT)

디도스(DDoS)에 대한 공격을 피하고, DPOS 투표에 대한 지분을 제공하고, 프로듀서에게 합리적인 보상을 하기 위해 연료로 쓰일 EVT 를 발행합니다. 어떤 작업이든 서비스 요금으로 특정 EVT 를 부과하며 프로듀서에게 보상이 됩니다. 청구된 EVT 는 자동으로 책정되고 수집된 요금은 악의적인 공격을 방지하기 위함이며 대부분의 사용자에게는 영향을 미치지 않습니다.

EVT 의 생성 및 전송방법은 블록체인의 암호화폐와 동일합니다. EVT 는 프로듀서가 제공하는 자원을 보상하고 악의적인 행동을 방지하기 위해 사용됩니다.

1 억 5 천만 개의 EVT(총 15%)가 코어 팀에 할당됩니다(everiToken 의 공동 설립자 5 명에게 14%, 핵심 기부자 1%).
4 억 개의 EVT(총 40%)가 everiToken 기반 애플리케이션을 구축하고 기술, 리소스, 프로모션, 펀딩 등을 통해 everiToken 에코시스템에 크게 기여하는 커뮤니티 구성원에게 할당됩니다.
4 억 5000 만개의 EVT(총 45%)는 다수 라운드의 투자자에게 할당됩니다.

everiToken 의 모든 서비스에는 서비스 연료비가 소요됩니다.

$$ServiceFuelCost = FuelUsed \times R$$

이 공식에서 $FuelUsed$ 는 특정 행동의 대가입니다. 가격 단위는 EVT 입니다. R 은 **조정 비율**을 나타냅니다. BP 노드는 체인이 너무 혼잡하거나 공격 당하는 중인 경우 언제든지 독립적으로 **요금 인상**을 결정할 수 있습니다. EVT 가격이 너무 높으면 요금 인하도 할 수 있습니다. 실제 값 R 은 15 BP 의 중앙값으로 계산됩니다.

체인의 사용자는 API 를 처음 콜(call) 할 때 R 을 1 이라고 가정할 수 있습니다. BP 에 의해 R 이 변경되지 않은 경우 콜이 완료됩니다. 변경된 경우 BP 응답으로 R 값은 콜이 실패합니다. 그러면 사용자가 다시 시도해야 합니다.

예를 들어, *creatingAccount* API 의 가격은 2 EVT 입니다.

일반적으로 사용자는 2 개의 EVT 로 *creatingAccount* API 를 콜 할 수 있습니다.

BP 가 R = 1.1 까지 요금을 인상하면 가격은 2.2 EVT 로 변경됩니다.

블록 프로듀서의 모든 R 분포의 중앙값 수를 사용할 것입니다. 3 명의 프로듀서가 R 을 1.15, 5 명의 프로듀서가 1.2, 2 명의 프로듀서가 1.1, 2 의 프로듀서가 1.3, 1 명의 프로듀서가 1.4 그리고 1 명의 프로듀서가 1.45 로 제안한다면 최종값 R 은 1.2 입니다.

고정된(Pinned) EVT

고정된 EVT 는 EVT 와 유사하지만 전송할 수 없습니다. 연료비로만 사용할 수 있습니다. EVT 에서 고정 EVT 로 변환할 수 있습니다. 고정 EVT 에 대한 EVT 의 환율은 항상 1 입니다. **고정 EVT 는 통화가 아니기 때문에** 고정 EVT 를 다른 사람에게 에어드롭 해도 무방합니다.

EVT 를 연료비로 사용할 수 있으므로 EVT 를 고정된 EVT 로 전환해서는 안 됩니다. EVT 를 고정된 EVT 로 변환하기로 결정하면 고정된 EVT 가 수취인에게 자동으로 고정되므로 **고정된 EVT** 라는 이름이 사용됩니다.

고정된 EVT 는 계정에 종속되며 다른 사람에게 양도할 수 없습니다. 따라서 고정된 EVT 는 사용자에게 에어드롭하는 것이 편리하고 안전합니다. 기업은 EVT 를 고정된 EVT 로 전환하여 특정 계정에 전송할 수 있습니다. 고정된 EVT 는 주소 간에 전송할 수 없습니다.

지급인은 특정 트랜잭션을 지불하는 계정입니다. everiToken 은 사용자가 트랜잭션에서 지급인을 지정할 수 있도록 합니다. 이 기능은 계정을 만드는 데 유용합니다. 안전을 위해 지급인은 거래에 대한 추가적인 서명을 받아야 합니다.

각 도메인에는 특별한 고정된 EVT 잔액이 있습니다.
체인은 도메인에서 토큰을 전송하거나 삭제하는 작업을 수행할 시 도메인의 고정된 EVT 잔액(0 이 아닌 경우)를 소비하는 것을 선호합니다.

사용자는 EVT 를 통해 도메인의 고정된 EVT 잔액 선불할 수 있습니다.

추가 EVT 발행

EVT 의 초기 공급량은 10 억개입니다. 체인은 1 년 단위로 추가 EVT 를 발행할 수 있습니다. 발행은 항상 everiToken 의 온체인 거버넌스 위원회에 의해 결정됩니다. 당사는 2020 년 1 월 1 일까지 추가 EVT 를 발행하지 않을 것입니다.

블록 프로듀서(BPs)

- BP 수: 유연하다

당사는 BP 에게 허가를 거의 주지 않기 때문에 BP 들이 악의를 가지기 매우 어렵습니다. BP 가 할 수 있는 유일한 악은 DoS(Denial of Service)입니다. BP 수익의 균형을 맞추고 탈중앙화를 보장하기 위해 당사는 유연하게 15 보다 크거나 같은 숫자를 사용합니다. 2019 년에는 15 개의 BP 를 사용할 예정입니다. 그 후 몇 년 동안 그 수는 온체인 거버넌스 위원회가 결정할 것입니다.

Part IV. 에코시스템

도구들

everiWallet

이름에서 알 수 있듯이 everiWallet 은 웹브라우저와 휴대전화 모두를 지원하는 everiToken 지갑입니다. 자세한 내용은 여기를 방문하십시오:

https://www.everiwallet.com/

EVTJS

EVTJS 는 everiToken 의 자바스크립트용 API 바인딩 라이브러리이며 NodeJS 와 브라우저를 모두 지원합니다. 또한 everiSigner 에서 지원되므로 라이브러리를 사용하여 언제든지 웹 앱을 만들 수 있습니다. 자세한 내용은 여기를 방문하십시오:

https://www.github.com/everitoken/evtjs

evtScan

evtScan 은 everiToken 의 블록체인 브라우저입니다. 누구나 메인넷의 노드에서 생성된 모든 현재 블록에 대한 특정 정보를 검색할 수 있습니다. 여기에는 트랜잭션, 계정, 그룹 및 체인의 도메인에 대한 세부 정보와 통계 및 분석이 있습니다. 개발자에게는 evtScan 은 정보가 체인에 제대로 연결되어 있는지 확인하는 효율적인 도구입니다. 사용자에게는 트랜잭션의 신뢰성을 확인시켜줍니다. 자세한 내용은 여기를 방문하십시오:https://evtscan.io/

탈중앙화 온체인 거버넌스 위원회

everiToken 퍼블릭체인은 탈중앙화 온체인 거버넌스 위원회를 통해 BP 의 수 및 EVT 의 추가 발행과 같은 중요한 사항을 결정합니다. 현재 진행중이며 위원회는 2020 년 1 월 1 일 이전에 온라인 상태가 될 것으로 예상됩니다.

에스크로 기업

everiToken 은 토큰 ID 를 제외한 사용자의 자산 또는 코인에 관여하지 않습니다. 토큰의 가치는 **에스크로 기업**에서 보증합니다. 에스크로 기업은 토큰 발행 시 별도의 서명을 할 수 있으므로 토큰에 서명을 하는 회사를 신뢰하면 누구나 토큰을 신뢰할 수 있습니다. 이것은 SSL 과 같습니다.

Part V. 결론

토큰 이코노미는 세계 구석구석까지 스며들고 있습니다. 이더리움과 EOS 스마트 계약은 좋은 출발이었지만 전 세계 사람들이 활용할 수 있는 토큰 이코노미를 개발하는 데는 적합하지 않습니다.

everiToken 은 토큰 기반 블록체인 기술을 개발하여 어디에서나 모든 사람에게 혜택을 주는 것을 목표로 탄생했습니다. 당사는 개발자, 기업, 사용자(end-users)가 시스템 내에서 토큰을 발행, 양도, 사용할 수 있도록 하는 혁신적인 시스템을 구축했습니다. 당사의 안전계약으로 튜링의 완전성(turing completeness)은 제거되었지만 결과적으로 시스템 내의 추상화와 복잡성은 크게 감소합니다. 당사는 끊임없이 맞춤형 모델을 만드는 대신 99%가 넘는 사람들에게 가장 적합한 모델(one-size-fits-all model)을 개발했습니다. 당사는 효율적이고 번성하는 토큰 이코노미를 만드는 데 필요한 속도, 보안, 운영성, 안정성 및 감독을 개선한 동시에 전 세계 모든 사람이 디지털 방식으로 가치를 배우고, 만들고, 교류하며, 교환할 수 있는 탈중앙화 플랫폼을 제공합니다. 웹 사이트를 방문하십시오: www.everitoken.io

창립자

Hengjin Cai , Chief Scientist

Hengjin Cai 박사는 2005 년부터 우한대 컴퓨터공학과 교수이자 박사 고문입니다. 글로벌 핀테크랩의 전문가이자 중국 과학원 심천첨단기술연구소 초빙연구원, 중국 인공지능(AI) 및 빅데이터 100 인 위원회 전문위원입니다. 또한 그는 SSME(서비스 과학, 경영, 엔지니어링), AI&블록체인 기술 등에 종사하고 있으며 최근 '*Blockchain System with Integrated Human-Machine Intelligence*' 라는 책을 출간했습니다. 2017 년에는 WU Wenjun 인공지능과학기술상을 수상했습니다. 2012 년에는 우한대학교 교육 특별 공헌으로 대통령상을 받았습니다. 그는 대학생들의 헌신적인 조언자로서 마이크로소프트의 이메진 컵, 마이크로소프트 및 모건 스탠리의 고성능 금융 대회, 인텔의 대학 소프트웨어 혁신 컨퍼런스, 대학생 기업가정신 대회 등 중국 전역의 영향력 있는 대회에서 학생들이 80 개 이상의 상을 수상하도록 도왔습니다.

Brady Luo, CEO Brady-everiToken

Brady 는 블록체인 기술의 글로벌 토큰 이코노미를 굳게 믿고 있습니다. 그는 베이징항공우주대학교 전기공학부에서 학사학위를 받고 미국 브란데이스대에서 금융학 석사학위를 받았으며 옥스퍼드대 경영대학원에서 블록체인 전략 커리큘럼을 공부했습니다. 연쇄 창업가인 그는 상하이 1000 인재계획(벤처 그룹)의 세 번째로 선출되었으며 이전 스타트업 중 두 개를 팔

았습니다. 그는 대체자산투자그룹의 미국 10 대 펀드매니저인 뉴욕 오펜하이머펀드와 일본 최대 금융그룹인 MITSUBISHI UFJ 증권(도쿄 본사, 홍콩, 상하이)에서 4 년 가까이 애널리스트로 활동했습니다.

Bozhen Chen, COO

Bozhen 은 정부 프로젝트 운영에 풍부한 경험을 가지고 있으며 커뮤니케이션과 홍보 전문가입니다. 그는 애스턴 대학에서 경영학 학사 학위를 받으며 졸업했습니다. 그는 전자 상거래 공급, 의류 공급망, B2B 서비스 및 정부 기관에서 일해 왔습니다. 그는 다양한 산업과 관심사에 걸쳐 수행, 커뮤니케이션, 그리고 홍보 기술을 터득했습니다. 인터넷 컨퍼런스의 진행자이자 통샹 전자상거래 공공서비스센터장, 청소년 인터넷 기업가정신 서비스 센터 소장입니다. 그는 자오싱의 '뛰어난 청년상', 중국공산청년동맹이 수여하는 2018 '동기부여 청년상' 등 중국의 젊은 지도자 중 한 명으로 수많은 상을 받았습니다.

Ceeji Cheng, CPO

Ceeji 는 10 년 이상의 소프트웨어 개발, 기업가 및 관리 경험을 가진 풀스택 개발자이자 시스템 설계자입니다. 그는 국가 정보 올림피아드에서 1 위를 차지했으며 이전에 자신의 스타트업(CTO 및 공동창업자)에서 근무했습니다.

Harry Wang, CTO

Harry 는 금융 및 인터넷 업계에서 10 년 이상의 전문 지식을 보유한 숙련된 시스템 설계자이자 엔지니어입니다. 앞서 상하이 티엔펑증권에서 근무한 뒤 퀀트 헤지펀드 회사를 기술 파트너로 설립했습니다. 그는 현재 전 세계 여러 시장에서 운영되는 고성능 퀀트 트레이딩 시스템을 개발했습니다.