<Privacy Focused AltCoin>

- 특정 블록체인 소개
- Privacy 보호를 위해 어떠한 기술을 사용
- 해당기술에 대한 원리 추가
- 블록체인에서 사용하는 합의 알고리즘 설명

20155137 안원영

Privacy Focused AltCoin이란 블록체인에서 사용자 익명성을 보호하기 위해 사용된 정교화한 암호화 및 개인 정보 보호 기능이다. 대부분의 블록체인은 거래가 공개원장으로 기록되어 모두가 볼 수 있기 때문에 익명성에 취약하다. 따라서 특정 방법으로 비트코인에서 개인의 신원이나 거래 내역을 감출 수 있는 방법이 있다. 이제 이러한 블록체인에서의 익명화 방법을 소개하려 한다.

1. Monero

Monero는 RingCT, 스텔스 주소 및 Ring 서명과 같은 강력한 개인 정보 보호 기능을 사용하여 트랜잭션 세부 정보를 익명화해 많은 사람들이 시장에서 최고의 익명 암호화폐로 간주한다. 결제를 확인하거나 증명하기 위해 RandomX 알고리즘이 작업증명으로 사용되고 사용자는 Monero 트랜잭션 ID(해시) 이상을 제공해야 한다 . 대신 Monero 트랜잭션 ID, 개인 트랜잭션 키(자동으로 생성되는 일회성 키) 및 수신자의 공개 주소가 요구된다. 이 세 가지 정보를 통해 이해 관계자는 Monero GUI 지갑을 사용하여 확인할 수 있다. Monero는 개인 정보 보호 측면에서 Dash를 능가하지만 DASH는 XRM보다 훨씬 빠르고 사용 비용이 저렴하다. Monero는 링 서명, RingCT 등을 포함한 일련의 개인 정보 보호 강화 전략을 사용하여 Dash보다 추적이 불가능하다.

2. Zcash

2016년에 출시된 Zcash 는 Bitcoin 의 포크 인 Dash와 동일한 루트를 공유하는 또 다른 최고의 개인 정보 보호 코인이다. Zcash의 개인 정보 보호 전략은

본질적으로 거래가 발생할 때마다 코인의 "메모리", 즉 거래 내역을 지우는 것입니다. Electric Coin Company가 이끄는 익명의 암호화폐는 에너지 집약적인 Zero-Knowledge 증명을 사용하여 거래를 확인한다. 영지식 증명은 "상대에게 정보의 내용을 공개하지 않고도 자신이 그 정보를 알고 있다는 것을 증명" 하는 기술이다. 선택적인 개인 정보 보호를 장려하여 트랜잭션 및 zk-SNARKS 라고 하는 고급 암호화 기술을 사용해 개인 정보 및 추적 불가능 메커니즘을 통해 트랜잭션을 숨길 수 있는 선택을 제공한다. Zcash에서 사용자는 숨기고 싶은 거래와 공개하고 싶은 거래를 유연하게 선택할 수 있어 유연하고 익명의 암호화폐가 됩니다.

3. Horizen

Horizen은 개인 정보 보호 기반 애플리케이션을 누구나 구축할 수 있도록 하는 사이드체인 이 있는 개인 정보 중심 암호화폐이다 . 2017년 ZenCash라는 이름으로 출시되었다. Horizen은 또한 채굴자, 노드 운영자 및 검증자를 위한 기본 암호화폐인 ZEN을 제공한다. 채굴 보상으로서의 역할 외에도 ZEN에는 사용자가 디지털 발자국을 제어하는 데 사용할 수 있는 선택적 개인 정보 보호 기능이 있다. Bitcoin과 유사하게 작동하는 개인 정보 보호 (Z-주소) 및 공개 (T-주소)를 가진다. 그러나 Z 주소에서 T 주소로 자금을 보내면 받은 금액이 표시됩니다. Horizen은 또한 익명성을 개선하는 데 도움이 되는 광대한 노드 네트워크를 자랑한다. 현재의 금융 혁신은 금융 세계의 활동을 안정시키는 데 많은 것을 제공하고 있습니다. 업계 최대의 노드 네트워크가 지원하는 생태계를 갖춘 확장 가능한 개인 정보 기반 플랫폼으로 회사와 개발자에게 자체 퍼블릭 또는 프라이빗 블록체인을 생성할 수 있는 빠르고 저렴한 방법을 제공하는 데 중점을 둡니다. Horizen Network 토큰은 블록체인 기술의 가장 일반적인 두 가지 합의 알고리즘인 작업 증명(PoW)과 지분 증명(PoS)을 사용한다. 합의를 위해 네트워크의 메인 체인은 PoW 알고리즘을 사용하고 사이드 체인은 PoS 프로토콜의 수정된 버전을 사용합니다. 느린 트랜잭션 및 높은 요금과 같은 확장성 문제를 해결하는 혁신적인 사이드 인프라인 Zendoo를 제공한다. Zendoo는 현재 Horizen의 테스트 네트워크에서 실행 중이며 아직 메인 네트워크에 도달하지 않았다.

4. Verge

Verge는 추구하는 목적이 익명성을 보장하기 위한 탈중앙화폐이고 TOR와 i2p와 같은 다중 암호화 네트워크를 활용한다. 이는 비트코인이 사용하고 있는 블록체인 기술을 더욱 향상시켜주었다. Verge (XVG) 는 암호화 기술에 의존하는 대신 TOR (The Onion Router) 및 I2P(Invisible Internet Project) 의 기존 및 테스트된 기술을 기반으로 사용자의 신원을 보호한다. TOR는 전 세계에 흩어져 있는 node가 운영하는 분산 릴레이 및 터널 네트워크를 통해 사용자의 통신을 반송하여 사용자의 신원을 숨깁니다. 반면에 I2P는 사용자 데이터를 암호화한 후 익명의 P2P 및 node가 운영하는 전 세계적으로 분산된 네트워크를 통해 전송한다. 거래 참여자의 위치와 IP 주소를 숨길 수 있다. 따라서 사용자 사이에 노드(node)를 계속 만들어 그 연결고리 역할을 하는 노드를 무작위로 경유시켜 라우팅하는 데이터를 전송하고 거래를 가능하게 한다. 데이터와 코인은 수 많은 노드와 블록들을 거쳐서 라우팅을 하고 전송되기 때문에 추적이 불가능하게 만든다. Verge는 인기 있는 성인 웹사이트가 암호화폐 결제를 수락 하기 위해 이를 채택 했을 때 유명해졌다. 거래속도는 단 5초밖에 걸리지 않고 현재 다양한 거래소에 상장되어 있습니다.

5. Beam

Beam 암호화폐는 MimbleWimble과 Lelantus라는 두 가지 개인 정보 보호 지향 블록체인 프로토콜을 혼합하여 구현한 블록체인이다. 개인 정보 보호 외에도 이 기술은 다운로드가 더 빠르고 확인 및 동기화가 더 쉬운 소형 데이터 솔루션을 제공하여 PoW 프로토콜의 확장성을 향상시킨다. 또한 Beam은 식별할 수 없는 주소를 통해 추적할 수 없는 거래를 제공한다. 빔에서 거래할 때 가상화폐 자산의 송금인과 수령인만 서로의 주소를 볼 수 있다. 이 때 보이는 주소 자체도 보통 임시 주소입니다. 새로운 거래가 생성될 때마다, 빔은 신규 주소를 생성하지만 플랫폼 유저의 거래 기록을 추적하는 기능은 전혀 없다. Beam에서 거래할 때 암호화 펀드의 발신인과 수취인만 서로의 주소를 볼 수 있습니다. 이러한 주소도 일반적으로 임시 주소입니다. 각각의 새 트랜잭션에 대해 Beam은 새 주소를 생성하므로 플랫폼 사용자의 트랜잭션 내역을 추적할 수 없습니다. 거래유형에는

온라인거래, 오프라인 거래, 최대 프라이버시 거래가 있고, 주소 유형은 일반주소, 최대 익명주소, 오프라인 공개주소가 있다. Beam은 표준 트랜잭션 유형 외에도 아토믹 스왑도 지원합니다. 아토믹 거래소는 두 블록체인 사용자 간의 지능형 계약에 의해 활성화된 암호화 P2P 전송입니다. 트랜잭션의 두 부분은 같거나 다른 블록체인에 있을 수 있습니다.

6. Particl

PART는 개인 정보 보호 플랫폼 및 분산형 시장(많은 인기 있는 암호 화폐 지원) 에서 사용하기 위해 Particl 에서 만든 토큰이다. 개인정보 보호에 중점을 둔 마켓 플레이스 및 분산형 어플리케이션 플랫폼 이다. 최신 버전의 Bitcoin을 기반으로 하는 Particle은 CT(Confidential Transactions) 및 RingCT로 프로토콜을 향상시킨다. 모든 유형의 사용자를 수용할 수 있는 다양한 프라이버시를 지닌 코인이며, Particl 플랫폼의 마켓 플레이스 및 DApp을 사용해야 합니다. Particl은 기본 Segwit 블록체인이므로 모든 트랜잭션은 기본적으로 분리된 Segwit을 사용하여 플랫폼의 확장성을 높인다. 특징으로는, 비밀거래시 거래 생다방에게만 거래 내역이 보이며 비밀/보안 채팅을 통해 비밀 대화도 나눌수 있다. 사용자에게 개인 정보 제어 권한을 다시 제공한다. PART 토큰은 소유자의 통제를 벗어나지 않고 개인 정보 보호에 대한 권리를 침해하지 않으면서 공개와 비공개 간에 원활하게 전환할 수 있으므로 여러 계층의 개인 정보 보호를 제공합니다.

7. Komodo

코모도(Komodo)는 지캐시와 비트코인 블록체인 네트워크를 사용하는 보안성 및 확장성이 뛰어나고 개인 정보 보호에 중점을 둔 암호화폐 프로젝트이다. 코모도는 도마뱀(Komodo Dragon)처럼 강한 보안을 상징하는 브랜드이다. 코모도의 화폐 단위는 KMD이다. 코모도는 익명성을 중시하는 프라이버시 코인 계열의 암호화폐인 지캐시에서 포크 되었기 때문에 영지식증명을 통해 익명성을 보장한다. 또한 코모도 자체의 블록체인 이외에 추가로 기존 비트코인의 블록체인도 사

용하는 지연작업증명(DPoW) 방식의 합의 알고리즘을 도입함으로써 위변조가 불가능한 안전한 보안을 달성하였다.

코모도는 지캐시에서 하드포크된 코인으로, 합의구조는 DPOW(Delayed Proof OfWork)를 채택하고 있다. DPOW란 기존 코모도 코인의 채굴 이외에도 비트코인의 블록체인도 사용해 보안성을 높인 것을 말한다. 비트코인의 블록체인에서 다시 한 번, 공증을 받기 때문에 비트코인 만큼 안전성을 보장한다. 또한, 코모도는 이더리움과 같이 플랫폼의 역할도 수행하며, 현재 코모도 기반 탈중앙거래소(DEX)가 존재한다. 기본적으로 지캐시와 같이 영지식증명을 통해 익명성을 구현한다.