

RSK, 분산형 페그 메커니즘 PowPeg 런칭

지브롤터 - 2020년 12월 8일

IOVlabs가 RSK smart contract 플랫폼의 기존 페그 기술을 크게 업그레이드한 PowPeg의 런칭을 발표했다.

PowPeg는 작업 증명 보안 양방향 페그로 RSK 사이드체인과 비트코인 사이드체인 간의 소통에 사용된다. Powpeg는 비트코인의 작업 증명에 기반한 안전 보장을 제공하는 첫 번째 비트코인 페그로, 이로써 오늘날 이용할 수 있는 페그 중 가장 안전하고 가장 무허가성을 유지하는 페그가 되었다.

RSK의 고유 통화인 RBTC는 BTC에 1:1로 묶여 있다. RBTC를 생성하는 유일한 방법은 비트코인 블록체인에서 BTC를 멀티시그 주소로 보내거나 “페그인”을 수행하는 것이다. 해당 주소는 BTC를 잠그며, 해당 거래의 증명, 또는 SPV 증명이 생성되어 브리지 smart contract로 전송된다. 브리지 컨트랙트는 해당 증명을 받고 나서 사용자에게 동일한 양의 RBTC를 돌려준다. “페그아웃”은 이와 동일하나 반대로 진행되는 과정이다.

원래 이 과정은 멀티시그 주소를 제어하는 여러 공증인이 관리하였으며 과반수가 자금을 해제해야 하는 식으로 진행되었다. Powpeg의 런칭은 RBTC를 생성하는 새로운 분산형 접근법을 시행한다. 이는 하드웨어와 노드의 연결을 유지하고, 항상 라이브 상태인지를 확인할 책임이 있으나 거래 서명에는 아무 역할도 하지 않는 Pignatory 그룹에 의지한다. 해당 그룹은 비트코인 예금이 RSK 체인에 정확하게 통지되는지를 확인하는 감시탑 역할을 한다.

Pignatory의 개인 키는 PowHSM이라 불리는 특별 목적의 하드웨어 보안 모듈에 저장된다. SPV 증명이 생성되면 이는 거래를 PowHSM에 전달해 서명 과정을 자동화한다.

Powpeg는 “비토크라시”로, 한 독립체나 공모한 그룹이 페그를 제어하거나 무작위로 거래를 검열할 만큼의 힘을 모을 수 없는 방식이다. 이미 세간의 주목을 받는 12개의 회사가 RSK에서 Powpeg 지원에 참여하는 중이다. 해당 참가자는 몇 주 안에 발표할 예정이다.

이는 RSK smart contract 플랫폼을 완전 분산화하는 데 아주 중요한 이정표로 남을 것이다. RSK 커뮤니티는 무허가성의 경쟁 페그를 소개하는 기능을 포함하여 페그를 더욱더 분산화하기 위한 추가 기술을 개발하는 중이다. RSK는 비트코인과 병합 채굴되며 비트코인 네트워크 해시율의

50% 이상을 차지한다. 따라서 이러한 새로운 혁신의 목적은 비트코인 채굴자가 RSK 네트워크에서 활동적인 Pegnatory 역할을 할 수 있게 하는 것이다.

RSK 사이드체인은 이제 Money on Chain과 Sovryn 등의 완전한 DeFi 앱 모음을 보유하고 있으며 사용자는 비트코인 생태계 안에서 비트코인을 빌려주고, 빌리고, 거래할 수 있다. 따라서 이러한 RSK의 최신 작업은 비트코인 DeFi 생태계를 더욱더 분산화된 상태로 발전시켜, 중앙화된 서비스를 이용하지 않고도 BTC를 빌리고 거래하고자 하는 비트코인 애호가들의 목표를 달성할 수 있게 하며, 기업이나 프로젝트가 BTC와 RBTC의 주조와 페그에 참여할 수 있는 새로운 방안을 마련한다.

RSK 소개

병합 채굴을 통해 최고의 비트코인 해시 파워의 보장을 받는 RSK 네트워크는 전 세계에서 가장 안전한 스마트 컨트랙트 플랫폼이다.

RSK는 smart contract, 즉각적 결제 및 더 높은 확장성을 실현해 비트코인 생태계에 가치와 기능을 추가한다.

해당 네트워크는 분산형을 유지하며 초당 최대 100개의 거래로 확장될 수 있으며, 확률 검증, 사기 탐지 등을 이용해 저장 공간과 대역폭을 줄인다.

자세한 내용은 다음 링크를 참고하기 바란다. <https://www.rsk.co/rsk-blockchain/>