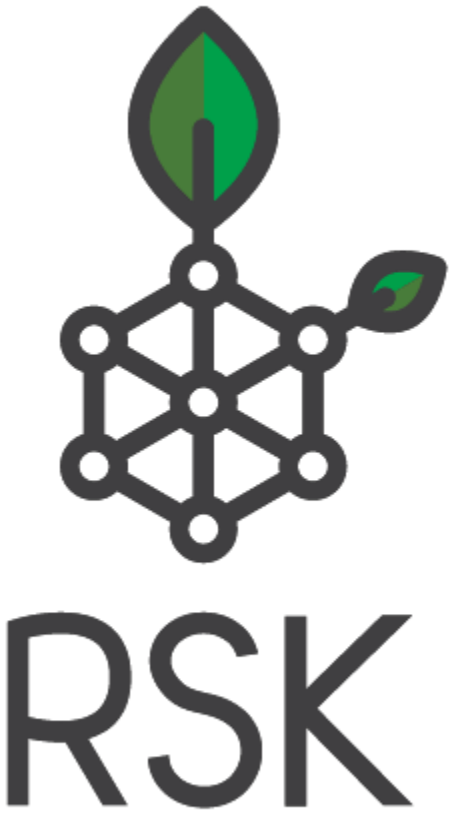

백서 개요

개정: 9
날짜: 2015 년 11 월 19 일
작성자: Sergio Demian Lerner

소개

2008 년, 사토시 나카모토는 비트코인을 만들어 결제에 혁명을 일으켰습니다. 비트코인은 닉 자보가 1993 년에 소개한 개념인 "스마트 컨트랙트"라는 존재의 아주 제한된 구현을 포함했습니다.

그 이후로 아주 많은 연구가 완전한 튜링 완전 분산 프로그램을 지원하는 새로운 암호화폐의 탄생에 집중해 왔습니다. 이제는 이 목표를 달성하기 위해 유용하고, 안전하며, 확정적인 가상 머신을 구축할 수 있다는 확신이 있습니다.

저희는 비트코인이 글로벌 암호화폐의 선두주자가 되려면 새로운 사용례가 필요하며, 스마트 컨트랙트 기능을 더하는 것이 바로 그런 미래를 보장할 수 있는 열쇠라고 믿습니다. 저희는 바로 그런 생각으로 튜링 완전 가상 머신(Turing Complete Virtual Machine)을 비트코인과 통합한 스마트 컨트랙트 플랫폼인 RSK 를 만들었습니다. RSK 는 또 네트워크에 더 빠른 거래 속도와 더 나은 확장성 같은 다른 개선을 제공합니다. 이러한 기능은 나아가 새로운 사용 시나리오를 만들어낼 수 있을 것이라고 믿습니다.

RSK 는 2013 년 같은 개발 팀이 만든 튜링 완전 암호화폐인 QuixCoin 의 진화 형태입니다. RSK 는 거의 즉각적인 거래 확인과 더 나아진 결제 경험을 제공합니다. RSK 는 또 현재 300 tps 를 달성하고 있으며, 대부분의 결제를 20 초 안에 확인할 수 있습니다. 그러나 RSK 는 여전히 비트코인과 동일한 보안 보증에 기반하여 SHA-256D 병합 채굴을 지원합니다.

RSK 는 비트코인의 사이드 체인으로 작용합니다. 비트코인은 RSK Blockchain 으로 이동했을 때 "스마트 비트코인(SBTC, SmartBitcoins)"이 됩니다. 스마트 비트코인은 RSK Blockchain 에 존재하는 비트코인과 같으며, 추가 수수료 없이 (RSK 기본 거래 수수료 제외) 언제든지 다시 비트코인으로 이동할 수 있습니다. RSK 사이드 체인이 채굴자에게 거래와 컨트랙트 처리 비용을 지불하는 데 사용하는 통화는 SBTC 입니다. 여기에는 새로운 화폐가 발행되지 않습니다. 모든 SBTC 는 비트코인 블록체인에서 오는 비트코인에서 생성됩니다.

RSK 는 다음 분야에서 비트코인을 보완합니다.

- 스마트 컨트랙트를 허용하는 튜링 완전 RSK 가상 머신(RVM, RSK Virtual Machine)
- 평균 거래 최초 확인 시간 10 초 이내
- PoW 와 백업 임계치 서명 기반 연합 채굴을 통합한 안전한 병합 채굴
- 저지연(low-delay) 고속 릴레이 백본을 P2P 가십 네트워크에 내장함.
- 사이드 체인을 사용한 양방향 페그 (현재 연합 페그이며, 완전히 자동적인 페그는 비트코인 개선에 달려 있음)

머리글자: "RSK"란 Rootstock(플랫폼)을 뜻하며, 이와 관련된 용어로는 "RSK 프로토콜" (사양), "RSK 레퍼런스 노드" (레퍼런스 구현)가 있습니다. RSK 고유 통화는 "스마트 비트코인(SmartBitcoin)"이며, 스마트 비트코인 통화의 상징은 "SBTC"입니다. 이때 "BTC"는 비트코인 통화를 뜻하며 "비트코인"은 비트코인 프로토콜을 뜻합니다.

RSK 는 왜 비트코인 생태계에 중요한가?

비트코인 이해 당사자의 정비와 가치 보호

RSK 거버넌스의 주요 목표는 비트코인의 주요 이해 당사자의 현 활동과 완전히 뜻을 같이 하는 보상을 만들어 주요 이해 당사자를 정비하는 것입니다.

이 철학은 비트코인 채굴자가 작업 증명 블록 검증에 필요한 해시 파워를 제공하고, 업계의 리더들이 (거래소, 월렛 및 결제 프로세서) 검증 체크포인트를 만들고 양방향 페그의 보완 거래에 서명하는 연합을 통합하는 RSK 의 핵심 구조에 직접 반영되어 있습니다.

그 뿐만이 아니라 RSK 는 플랫폼 내 개선 사항을 채굴자, 업계 리더, 비트코인/RSK 보유자와 주요 개발자가 최종 결정을 할 수 있는 투표 시스템에 기반해 진행합니다.

그럼 다음은 이런 인센티브가 어떻게 적용되는지를 설명하도록 하겠습니다.

거버넌스 모델

커뮤니티 내의 플레이어라면 모두 커뮤니티에 최고인 노하우가 있을 것입니다. 거래소와 웹 월렛은 비트코인 절약을 보호하는 법을 알고 있고, 채굴자는 규모가 큰 스케일의 채굴 작업을 실현해 사용자의 거래를 확보하는 법을, 블록체인 회사는 새로운 사용례의 혁신을 불러와 꿈을 현실로 만드는 법을, 주요 개발자는 다가오는 기술적인 어려움을 다루는 법을, 노드 유지자는 인프라와 네트워크 연결성을 제공하는 법을, 그리고 마지막으로 사용자는 시스템의 핵심으로 신뢰와 유동성을 제공하는 법을 알고 있습니다.

RSK 거버넌스 모델은 5 개의 자리로 된 거버넌스 위원회를 제공해 커뮤니티 내 모든 행위자를 대표하고자 합니다. 채굴자는 해시 파워(1 표)와 함께 투표를 할 수 있으며, 비트코인 및 RSK 사용자는 지분 증명으로 (1 표), 거래소와 웹 월렛은 연합을 통해(1 표), RSK 및 비트코인 코어 개발자는 특별한 한계치 투표 시스템을 통해(1 표) 투표를 하게 됩니다. 그리고 마지막 표는 비영리 설립 기관인, 비트코인 재단과 같은 비트코인 기관에 제공되어 이러한 기관이 더 넓은 생태계를 대표할 수 있게 합니다. 또한, 제도적 투표가 이더리움 커뮤니티를 대표하는 경우, 이더리움 재단에 이를 제안할 수도 있습니다.

비트코인 채굴자의 투자 보호

2016 년 8 월에 비트코인 채굴 수익성 마진은 25 BTC 에서 12.5 BTC 로의 블록 보상 감소로 인해 50% 이하로 떨어질 것입니다. 따라서 수백만 명의 채굴 하드웨어가 바로 쓸모없어지게 될 것입니다. 2 세대에 걸친 칩이 (더 빠르고 더 낮은 전력을 소모하는) 모두 2017 년 전에 개발되고 판매될 것이므로 여기에는 아마 오늘날 시장에 존재하는 채굴 기계 모두가 포함될 것입니다. 하드웨어를 교체하지 않은 현재 채굴자 대부분은 자신의 채굴 사업을 잃게 됩니다. RSK 는 병합 채굴 능력 덕분에 이런 채굴자에게 사업을 적어도 4 년 이상 유지할 수 있는 기회를 선사합니다. 비트코인 병합 채굴자들은 두 가지 코인 모두를 한계 비용이 전혀 없이 채굴할 수 있으므로, 채굴자는 RSK 채굴이 제공하는 추가 수익이 수익성 갭을 보상해 주는 한 여전히 비트코인 채굴을 계속할 수 있을 것입니다.

추가로 반감으로 인해 발생하는 채굴 수익성의 감소는 저가 채굴자에 추가 밀집을 일으켜 비트코인의 네트워크 취약성을 높일 것입니다. 따라서 RSK 는 비트코인의 보안과 가치를 높여 주는, 수익성이 높은 채굴자의 폭넓은 베이스를 홍보하는 데 중요한 역할을 할 수도 있습니다.

또, 오늘 바로 최소 가격으로 채굴을 시작하고 RSK 를 위한 애플리케이션을 만듦으로써 비트코인 채굴자는 자신의 투자를 보호할 수 있을 뿐만이 아니라, 완전히 새로운 사업 기회를 만들어낼 수 있게 됩니다.

비트코인 / RSK 양방향 페그 확보하기

선도적인 비트코인 회사들은 비트코인과 RSK Blockchain 간의 자금 이동을 확보하는 데 중요한 역할을 할 연합을 통합할 것입니다. 그 댓가로 이들은 자금 유입과 유출 간의 결산이 창출하는 수수료로부터 수익을 얻을 수 있습니다.

더 저렴한 비트코인 거래 수수료와 안정적인 가치 자산 발행

현 비트코인 보유자와 장래의 사용자는 주로 비트코인 가격의 변동성 때문에 자신의 금전 시스템 사용이 특정 사용례에만 국한되는 것을 바라봐야 했습니다 (투자, 글로벌 결제 네트워크와 같은). 그러나 이러한 제약은 그 다음 비트코인 삭감 시의 수수료 증가 가능성으로 인해 미래에 더욱 더 심화될 수도 있습니다.

RSK 는 거의 즉각적인 거래 확인 (20 초)와 신용 화폐나 다른 안정적인 화폐에 맞게 고정된 가격의 자산 발행을 제공해 이 문제에 대한 해결책을 선사합니다. 거래의 변동성 노출을 줄이는 동시에 비트코인을 준비 통화로 유지하는 것은 비트코인의 전체 가치를 높여 줍니다.

비트코인 보안 강화하기

다음 비트코인 보상 삭감 시에는 수백만 달러의 더이상 쓸모가 없어진 채굴 하드웨어가 사적으로, 또는 온라인으로 값싸게 팔리게 될 것입니다. 이는 공격자가 아주 적은 양의 돈으로 아주 커다란 해시 파워를 구입해 51%의 공격을 수행할 수 있는 취약함의 가능성을 열어 주게 됩니다. 또한, 보안의 감소가 코인의 지각 가치에 영향을 줄 수도 있습니다. 비트코인 네트워크는 RSK 병합 채굴로 비트코인 채굴의 수익성을 높여 해시율이 폭락하는 것을 막을 수도 있습니다.

저렴한 BTC 결제 네트워크로서의 RSK

비트코인 블록 크기가 하드 포크를 통해 증가하지 않는다면, 다음 비트코인 보상이 삭감될 때 비트코인 거래 수수료는 특정 애플리케이션의 경우 더이상 해당 앱을 사용할 이유가 없을 정도로 높아질 수도 있습니다. RSK 블록은 비트코인 블록보다 더 많은 거래를 보유할 수 있으므로, 자연적으로 RSK 는 더 낮은 수수료를 제공하게 됩니다. 거래 수수료에 관한 미래 시나리오 분석은 다음 섹션을 참고하시기 바랍니다.

비트코인과 그 거래 수수료의 미래는 아직 불확실합니다. 현재로서 최대 블록 크기 변화에 대해 논쟁을 일으키는 제안이 미래 거래 수수료에 큰 영향을 줄 것입니다. 저희는 다음 표에서 미래 시나리오를 예측하고 RSK 와 비트코인의 성장과 분기점을 합리적인 가정 아래 비교하려는 시도를 해 보았습니다.

파라미터	비트코인	RSK
사토시와 동량이고 보안이 비슷할 때의 확인 시간	10 분	10 초
반전 확률 0.1%의 최소 확인 시간	20 분(블록 2 개)	30 초(블록 3 개)
초당 최대 거래 수	3.3 tps (평균 크기 tx 가정)	런칭 시 300 tps 1000 tps 로 스케일링 가능
현 표준 거래 사용자 평균 지출 비용	6 센트 가정: - 1.5 tps	제공된 시장가 없음
기본 거래 포함을 위한 현재 채굴자 지출 비용	1 센트 가정: - 빠른 릴레이 네트워크 사용 - UTXO 메모리 - tx 마다 1 ms 처리 시간 - 25.2 BTC 평균 블록 보상 5 센트 가정: - 표준 릴레이 네트워크 사용	<1 센트 (예상) 가정: - RSK 특별 하드웨어 교체 없음 - RSK 거래가 거의 없음 1 센트 (예상) - 새로운 헤더를 불러오기 위해 채굴자를 방해하는 것은 10 ms 의 처리 시간을 잃게 함
2016 년 말까지의 거래 수수료	1.6 USD 가정: - 블록 사이즈 증가 없음 - BTC/USD 환율 변화 없음 - 동일한 수준의 보안 - 3 tps	1 센트 (예상) 가정: - 3 tps

위의 표에 나타난 예상 거래 수수료는 BTC 가격이 2016 년 동안 약 240 BTC/USD 에 머무릴 것이라는, 증명되지 않은 사실에 기반한 것임을 꼭 참고하시기 바랍니다. 이 기간 동안 가격이 엄청나게 증가해 버린다면, 거래 수수료 또한 크게 증가할 것이며, 비트코인 블록체인은 은행 간의 청산 시스템으로는 사용할 수 있으나 결제 네트워크로는 사용하기가 힘들어져 버립니다. 또 더 값싼 결제를 제공하는 동시에 네트워크를 중앙 집권화하며 분산화 구조를 바꾸어 놓는 오프 체인 결제 시스템이 나타날 수도 있음을 참고해야 합니다.

다음 표는 네트워크 해시의 어려움이 BTC 가격과 동일한 비율로 증가한다는 가정 아래 2016 년 말까지 발생 가능한 미래의 시나리오를 나타내고 있습니다.

시나리오	채굴자들의 비트코인 tx 비용	채굴자들의 RSK tx 비용
비트코인 가격 10 배 증가	USD $16	2 센트
하드 포크를 통해 TPS 10 배 증가	11 센트	0.2 센트
BTC 가격과 TPS 10 배 증가	USD $1.1	2 센트

비트코인 거래를 포함하는 비용이 높아질수록 사용자는 계속 RSK 와 같이 수수료가 더 낮은 플랫폼으로 옮겨가게 될 것입니다.

RSK 사용례

RSK 플랫폼은 1993 년 닉 자보가 제안한 대로 튜링 완전 스마트 컨트랙트를 제공합니다. RSK 의 VM 은 그와 동시에 이더리움 VM 과 하위 호환성을 지닙니다. 따라서 RSK 는 이더리움 작업을 하는 개발자가 비트코인 블록체인의 강건함에서 오는 혜택을 누릴 수 있는 기회를 제공합니다. 아래는 RSK 에서 개발할 수 있는 가능한 스마트 컨트랙트와 사용례의 목록입니다.

소액 결제 채널과 허브 앤 스포크 네트워크

소액 결제 채널은 두 팀의 이해 당사자가 각 결제 시마다 수수료를 낼 필요 없이, 채널이 닫혔을 때 단 한 번만 수수료를 지불하고 안전하고 주기적인 낮은 가치의 결제를 진행할 수 있게 합니다.

허브 앤 스포크 네트워크는 서로 간의 신뢰가 없는 사용자가 아주 작은 양의 신뢰만을 필요로 하는 제삼자를 통해 낮은 가격의 1 회 결제를 간접적으로 진행할 수 있게 합니다. RSK 는 허브 앤 스포크 네트워크가 번거로움을 최소화한 방식으로 직접 구현되며 기본적으로 표준 e-월렛과 접속할 수 있게 합니다.

P2P 분산화 거래

RSK 는 TierNolan 의 프로토콜을 이용해 P2P 거래로 작용하는 컨트랙트를 지원합니다. 오더 북 내의 자동 매칭 또한 쉽게 생성이 가능합니다. 이는 분산화된 시장이 독립된 블록체인 위에 존재하며 제삼자 없이 암호 자산을 교환할 수 있게 합니다.

소매 결제 시스템

RSK 는 BTC 가 일일 소매 거래에 글로벌하게 채택될 수 있게 합니다. 비트코인의 소매 사용 내 주요 한계는 그 확인 시간에 있습니다. (불가역성을 보장하는 데 10 분에서 1 시간까지 소요됨) RSK 는 소비자들이 단 몇 초만의 거래 확인으로 비트코인 보안의 혜택을 누릴 수 있게 합니다. 그 덕분에 판매자는 제삼의 게이트웨이 없이도 바로 결제를 수락할 수 있을 것입니다. 소매 시장에서 성공하기 위해 모든 플랫폼이 꼭 갖추어야 하는 주요 요소는 많은 양의 초당 거래(tps, transaction per second)를 지원하는 능력입니다. RSK 네트워크는 DÉCOR+ 프로토콜을 사용해 비트코인 블록체인 내에서 최대 300 tps(Paypal 의 두 배)까지를 처리할 수 있습니다

에스크로 서비스

RSK 는 오라클이 에스크로에 있는 자금과 접촉하지 않고 거래에 서명을 해(또는 하지 않고) 그 거래가 실행되어야 하는지를 (또는 실행되지 않아야 할지를) 판단하는 스마트 에스크로 서비스의 생성을 허용합니다.

암호 자산 창출

RSK 는 비트코인 네트워크가 보장하는 암호 자산(또는 알트코인)의 생성을 허용합니다. RSK 의 컨트랙트 연료 가격 측정에 대한 유연함을 고려했을 때, 이러한 애플리케이션은 (다른 애플리케이션과 마찬가지로) 학생에서부터 은행과 기업에 이르기까지 널리 사용될 수 있습니다.

자산 증권화

RSK 는 또한 실제 자산이 뒷받침하는 전자 토큰의 생성을 허용합니다. 이는 REIT 나 주식을 전자 상에서 상업화하거나 부채 또는 다른 자산을 발행하는 데 사용할 수 있는 기능입니다. 이 특정 사용례는 전통적인 금융 시장이 운전 자본이나 자본의 성장에 대한 수요를 충족하지 못하는 개발 도상국의 소규모 사업체에게 특별한 솔루션을 제공할 것입니다.

분산화된 송금

이 특정 사용례는 은행을 사용하지 못하거나 필요한 서류가 없는 사람들이 가족에게 음식과 거처를 위한 비용을 보낼 때 고리대금 비용을 지불해야 하는 개발 도상국 경제에 특히 중요합니다.

IP 보호 / Registry

RSK 는 사람들과 회사와 같은 이들이 언제든지 비트코인 블록체인의 보안과 함께 특정 서류(또는 재산권)의 존재를 증명할 수 있게 하는, 존재 증명이라고 알려진 것을 복제할 수 있는 컨트랙트의 개발을 허용합니다. 이는 신뢰할 수 없는 토지 등록 매커니즘이 존재하는 라틴 아메리카, 아프리카 및 아시아와 같은 사회에 특히 더 중요할 수 있습니다.

투표 시스템

RSK 는 암호 자산의 특정 케이스로, 최소 비용만으로도 아주 안전하고 투명한 선거를 할 수 있게 하는 전자 투표의 생성을 허용합니다.

소액 대출

현재, 전 세계 인구의 50% 이상이 전통적인 금융 시스템에 대한 접근을 할 수 없는 상태입니다. 사람들이 신용에 접근할 수 없는 이 상태는 우리의 글로벌한 사회가 오늘날 마주한 경제 불평등의 직접적인 원인입니다. RSK 는 전 세계에서 가장 가난한 30 억 명의 사람들이 신용에 접근하게 할 수 있는 확장 가능한 전자 소액 대출 컨트랙트의 개발을 허용합니다.

공급망 추적 능력

RSK 는 또한 특정 제품이나 배치의 물리적 위치를 종추적하는 전자 월렛의 생성을 허용하기도 합니다. 이러한 유형의 컨트랙트는 소매, 식품 및 의료 산업 등에 특히 유용할 수 있습니다. 다른 사용례 모두와 같이 이는 RSK 를 사용하면 최소 비용만으로 비트코인의 보안과 함께 이룰 수 있는 사항입니다.

온라인 평판 및 전자 신원

개발 도상국에 발생하는 중요한 문제 중 하나는 가난한 이들에게 필요한 서류나 신분증이 부족하다는 것입니다. 이는 가난한 이들이 투표를 하거나, 의료 서비스를 이용하거나, 범죄/학대를 보고하거나, 재정 지원을 받을 수 없게 합니다. RSK 는 비트코인 블록체인 만큼이나 안전한 전자 글로벌 레지스트리의 생성을 아주 저렴한 가격으로 허용하고 있습니다.

게임 내 글로벌 통화

많은 멀티 플레이어 게임이 게임 내 현금 거래를 허용합니다. 여기에는 고유 통화가 포함됩니다. 이런 게임들이 진화함과 동시에 가상 화폐는 사용자에게 신용 화폐만큼이나 가치 있는 존재가 되며, 2 차 시장에서 자주 거래되는 통화가 됩니다. 이에 따라 사용자는 인플레이션, 부정 행위, 그리고 온라인 절도를 우려하게 됩니다. 또 게임 회사는 사용자 가상 화폐 위탁에 대한 법적 및 보안 장애물에 맞닥뜨릴 수 있습니다. 세상이 점점 더 글로벌해지면 게임도 글로벌해집니다. 따라서 플레이어들은 한 게임에서 획득한 돈을 다른 게임에서 쉽게 사용할 수 없다는 것을 불편해할 것입니다. RSK 는 게임이 게임 내 결제에 BTC(RSK 코인과 동일한 양으로)를 수락하게 하거나 RSK 가 보호하는 비공개 전자 자산을 생성해 이런 문제를 해결할 수 있습니다. RSK 결제는 낮은 액면가를 위한 폐쇄 루프 시스템만큼 빠를 수 있으며, 이로 인해 게임 엔진은 RSK 를 게임 내 구매 시스템, 플레이어 간 거래, 그리고 회사와 플레이어 간의 가상 제공에 사용할 수 있습니다. URL 을 클릭하거나 QR 코드를 스캔하기만 하면 플레이어의 표준 외부 e-월렛 소프트웨어를 사용해 거래가 트리거될 수 있으며, 게임 회사에 수수료를 지불할 수도 있습니다.

인터넷 도박 및 예측 시장

빠른 결제는 곧 빠른 페이아웃을 뜻합니다. SatoshiDice 와 같은 비트코인 도박 사이트는 확인이 필요 없는 시스템과 연결 고리식 거래를 사용해 등록이 필요 없는 빠른 베팅 경험을 제공하고 있으나, 이는 도박 사이트에는 보안 위험을 가져오는 방식입니다. RSK 는 블록 확인으로 거의 즉각적인 페이아웃과 함께 베팅을 할 수 있게 합니다.

공정한 플레이

RSK 는 스마트 컨트랙트를 채택하고, Mental Poker 와 같이 많은 연구가 존재하는 암호 프로토콜을 함께 사용해 제 3 의 신뢰 기관에 수수료를 지불할 필요 없이 오픈되고 공정한 카드 게임 플랫폼을 제공할 수 있습니다.

이는 RSK 플랫폼에서 내재된 비트코인 기술을 사용해 개발하고 프로그래밍할 수 있는 여러 가지 예 중 몇 가지 예에 불과합니다. 하지만 결국 이 컨트랙트를 실행하고, 컨트랙트 실행에 사용되는 연료 대부분이 주는 혜택을 누리는 것은 비트코인 채굴자라는 점(병합 채굴을 통해)을 강조하고 싶습니다.

기술 개요

RSK 플랫폼은 핵심적으로 다음 형태의 결합입니다.

- 튜링 완전 자원 회계 결정론적 가상 머신 (스마트 컨트랙트를 위해)
- 양방향 페그 비트코인 사이드 체인(BTC 표시 거래)
- 역동적인 하이브리드 병합 채굴/연합 컨센서스 프로토콜 (컨센서스 보안을 위해), 그리고 저지연 네트워크 (빠른 결제를 위해)

튜링 완전 가상 기기

RSK 가상 머신(RVM, RSK Virtual Machine)은 스마트 컨트랙트 플랫폼의 핵심입니다. 높은 퍼센티지의 네트워크 노드가 스마트 컨트랙트를 병행 수행합니다. 이러한 스마트 컨트랙트 수행 결과는 컨트랙트 간의 메시지 처리, 금전 거래 생성, 그리고 컨트랙트 상태 영구 메모리 변화가 될 수 있습니다. RVM 은 EVM 과 연산 코드 수준에서 호환이 가능하며, 이더리움 컨트랙트가 RSK 에서 완벽하게 실행될 수 있게 합니다. 첫 번째 출시 형태의 VM 은 해석을 통해 수행됩니다. 그 다음 출시 시기의 VM 은 EVM 연산 코드를 조정해 역동적인 방식으로 자바와 비슷한 바이트코드의 부분 집합에 맞추는 형식으로 EVM 을 모방할 예정이며, 다져진 안보와 제한된 메모리의 자바와 비슷한 VM 이 새로운 VM 이 될 예정입니다(RVM2). 이는 RSK 코드 수행이 자연어 코드에 가까운 성능을 자랑할 수 있게 할 것입니다.

주요 기능:

- 독립 VM, 그러나 연산 코드 수준에서 EVM과 호환 가능.
- RSK는 이더리움 사용자가 자신의 프로젝트를 비트코인 네트워크의 보안과 함께 실행할 수 있는 가능성을 선사합니다.
- 더 나은 성능을 위한, 빠른 int32 연산을 위한 새로운 연산 코드와 더 나은 적시 번역 (예정됨).

사이드 체인

사이드체인은 지불 증명을 사용해 고유 통화가 다른 블록체인 통화의 가치에 자동으로 페그된 독립 블록체인입니다. 여기에는 두 개의 통화가 자유롭게 자동으로 가격 흥정의 필요가 없이 교환될 수 있는 양방향 페그가 존재합니다. RSK 에서 스마트비트코인(SBTC)는 BTC 에 양방향으로 페그가 되어 있습니다 (더 정확하게 말하자면 RSK 의 최소 계산 화폐인 Rootoshi 는 비트코인의 최소 계산 화폐인 Satoshi 에 페그되어 있습니다).

실제 사용 시에, BTC 를 RTS 와 교환하는 경우, 단일 거래에서 블록체인 간에 실제로 “이동되는” 화폐는 없습니다. 이는 비트코인이 다른 블록체인 내 잔액의 정확함을 검증할 수 없기 때문입니다. 거래가 발생하는 경우, 일부 BTC 가 비트코인에 잠기고 동일한 양의 RBTC 는 RSK 에서 잠금 해제됩니다. SBTC 가 다시 BTC 로 전환되어야하는 경우, SBTC 는 RSK 에 다시 잠기고 같은 양의 BTC 가 비트코인에 잠금 해제됩니다.

세미 트러스트 프리 사이드체인

완전히 신뢰할 수 있으며, 제삼자가 필요 없는 양방향 페그는 두 가지 플랫폼 모두에 스마트 컨트랙트를 사용해 만들어낼 수 있습니다. 그러나 현재 비트코인이 스마트 컨트랙트를 지원하지 않으며, 외부 SVF 증명을 검증할 네이티브 연산 코드 또한 지원하지 않으므로, RSK 내의 양방향 페그 시스템의 일부는 세미 트러스트 제삼자(STTP, Semi-Trusted Third-Parties)의 모임을 필요로 합니다. 잠겨진 BTC 를 제어할 수 있는 단일 STTP 는 없으나, 그 중의 일부만이 BTC 자금을 방출할 수 있는 능력이 있습니다. STTP 는 잠겨진 BTC 를 일시적으로 보관하며, BTC 를 잠금 해제해 비트코인 사용자에게 비용을 지불합니다. SBTC 는 RSK 에 잠겨져 다시 비트코인으로 전송됩니다.

RSK 에서는 잠겨있는 자금을 보호하는 STTP 가 바로 연합 회원입니다. 이는 연합 인센티브가 STTP 와 매우 비슷하기 때문입니다. 둘 다 대학처럼 높이 평가받는 커뮤니티 내 행위자여야 하며, 반드시 안전한 네트워크 노드를 유지할 수 있는 기술력을 갖추고 있어야 합니다. 바로 이 안전한 네트워크 노드가 인력 개입 없이 자금의 잠김과 잠금 해제를 수행합니다. 따라서 연합의 일원이 되기 위한 필수 조건 중 하나는 노드에 권한을 부여하는 소프트웨어의 적절한 동작, 그리고 그 중에서도 특히 BTC 자금을 해제하기로 결정한 구성 요소의 정확성에 대한 것을 감사하는 능력입니다. 저희는 연합 검증 알고리즘이 더 보안을 개선할 수 있게 할 부정 조작이 불가능한 하드웨어를 만들고자 합니다.

비트코인이 SPV 증명을 하드 포크로 검증할 수 있도록 특별 연산 코드나 연장성을 추가하고 나면, 그리고 새로운 시스템이 안전하고 신뢰할 수 있음이 입증되면, 연합의 STTP 역할은 더이상 필요하지 않게 되며, RSK 팀은 RSK 가 신뢰할 수 있는 시스템을 채택할 수 있게 변화를 시행할 것입니다.

역동적인 하이브리드 병합 채굴/연합

저희는 PoW 가 저렴한 비용으로 블록체인 기록의 재작성을 방지하는 유일한 컨센서스 시스템이라고 믿습니다. 채굴에 중요한 리소스를 사용하지 않는 다른 컨센서스 시스템에는 모두 다 이러한 결점이 있으며, 평판에 의존하고, 익명 채굴 참여를 방지합니다. 다른 컨센서스 시스템은 모두 신규 사용자가 장부의 입증된 체크포인트를 찾는 데 일련의 당사자를 신뢰하게 만듭니다.

주기적 블록에 기반하며 고아 블록 소모가 낮은 높은 비율의 PoW 컨센서스는 네트워크가 새로운 블록을 해결할 때마다 채굴자가 자신의 하드웨어 채굴을 멈추고 재시작해 상태 중간에 새로운 헤더로 채굴할 것을 요구합니다. 이는 평균적으로 채굴 시간 간격이나, 상태 중간에서의 전환에 더 큰 네트워크 지연을 불러옵니다. 이러한 간격은 몇 밀리세컨드만을 사용한다고 해도 결과적으로 비트코인 채굴의 효율성을 감소시킵니다. RSK 는 따라서 DECOR+ 블록 보상 공유 제도를 사용해 경쟁을 줄이고 채굴자가 RSK 최고 블록으로 늦게 전환할 수 있게 합니다. 채굴자가 RSK 블록을 발견할 때마다 자신의 하드웨어를 바꾼다면, 이들은 완전한 RSK 블록 보상을 두고 경쟁하게 됩니다. 하지만 늦게 전환하고, 블록 팁을 넘어서 채굴을 계속하면, 이는 엉클 블록을 만들어내며 블록 보상의 일부를 얻게 됩니다. 이 모든 사례에서 완전히 고아 블록이 된 경우는 하나도 없습니다. 이는 DECOR+가 엉클 블록에 대한 보상을 지불하며, GHOST 규칙이 엉클 블록을 일반 블록으로 치고 최고의 체인을 확보하기 때문입니다. 이에 따라 결국 BTC 채굴의 효율성이 최대화됩니다.

저희는 RSK 해시 파워가 총 BTC 해시 파워의 50% 미만이 될 시기를 예상하고 있습니다. 이는 네트워크가 남은 해시 파워가 기존의 RSK 해시 파워의 두 배 사용을 능가해 51% 공격에 취약하게 만듭니다.

RSK 는 이런 상황을 방지하기 위해 PoW 채굴 블록을 위한 연합 체크포인트를 포함합니다. 연합 회원은 연합 체크포인트에 서명하며 클라이언트는 대부분의 서명을 사용해 어느 체인이 가장 좋은지를 결정할 수 있습니다. RSK 는 또한, 채굴 파워가 비트코인 해시 파워의 5% 미만으로 떨어지는 경우, 연합이 서명 블록을 생성할 수 있게 하는 최종 보루 프로토콜을 보유하고 있습니다. 클라이언트는 기본으로 Roostock 해시 파워가 최고의 체인에서 관측한 BTC 해시의 최대 어려움의 66%를 넘어섰으며, 블록으로 지불한 비용이 비트코인 블록 평균 보상보다 높거나 이와 같을 때 기본으로 연합 체크포인트 사용을 중단하게 되어 있습니다.

RSK 플랫폼은 잘 알려지고 커뮤니티에서 존경받는 회원의 연합과 함께 런칭될 예정입니다. 각 회원은 체크포인트 서명 제도를 위한 공개 키로 식별됩니다. 연합은 내장된 투표 시스템을 사용해 회원을 추가하거나 제거할 수 있으나, 이러한 행동에는 높은 비율의 회원 투표가 필요합니다.

RSK 창립자들의 목표는 RSK 네트워크가 병합 채굴을 인센티브화하는 것입니다. 그러나 RSK 는 병합 채굴 부족에 매우 강합니다. 이러한 경우에 연합이 자동으로 네트워크를 확보하게 되어 있기 때문입니다.

주요 기능:

- 채굴 보상 성숙도 1 일
- 연합 회원 체크포인트
- 부트스트랩 기간 동안의 코드 내장 체크포인트
- 병합 채굴에서 비트코인 채굴 효율성 손실을 예상하지 않아도 됨(즉각적인 상태 중간 전환에는 0.1% 미만, 늦은 전환에는 0%)

빠른 결제와 저지연 네트워크

RSK 는 더 나은 결제 네트워크가 되고자 합니다. 빠른 결제를 달성하기 위해 다음과 같은 여러 가지 솔루션을 개발해 보았습니다.

- 경쟁에서 자유로운 블록 선택 사용 (예: Hyperledger, Ripple, 페쇄 루프 시스템)
- 허브 앤 스포크 네트워크 사용 (예: 비트코인 라이트닝 네트워크)
- 높은 PoW 블록 비율 사용

허브 앤 스포크 네트워크는 새로운 중앙 집권화 노드를 추가하며, 클라이언트 월렛이 새롭고 완전히 다른 결제 모델을 완전 채택하도록 요구합니다. RSK 는 이러한 대안을 쉽게 수행할 수 있으나, 이는 빠른 결제의 네이티브 시스템은 아닙니다. RSK 는 채굴 중앙 집권화에 대한 인센티브를 생성하지 않고, 이기적인 채굴에서 자유로우며, 인센티브와 호환되고, 평균 10 초 블록 비율 달성을 허용하는 DECOR+와 FastBlock5 프로토콜을 채택합니다.

주요 기능:

- 블록 간격 10 초
- 2 단계 블록 전파(2SBP, Two Stage Block Propogation) 프로토콜
- 분실된 거래 푸쉬(PMT, Push Missing Transactions) 프로토콜
- 마지막 경쟁 블록을 완전히 네트워크에 전파해 이기적인 채굴을 방지하고 스테일 블록의 비율을 줄입니다.
- 거래 지연 포함 (DTI, Delayed Transaction Inclusion) 휴리스틱. 모든 거래는 각 채굴자의 블록 거래 대기열에서 5 초 동안 지연되어 가장 빠른 블록 검증을 가능하게 합니다. 이는 거래가 이미 네트워크 내 모든 노드의 풀에 존재하기 때문입니다.
- 블록 헤더를 임계 시간 우선 사항과 함께 퍼트릴 수 있는 새로운 네트워크 명령.
- 블록 거래 해시 목록을 블록 헤더가 전파되자마자 바로 퍼트릴 수 있는 새로운 네트워크 명령.
- 검증되지 않은 블록의 채굴(MUB, Mining on Unverified Blocks) 휴리스틱. 5 초 수정 시간(폴백)이 따르는 검증되지 않은 거래의 블록 헤더 채굴.
- 거래가 없는 블록에는 표시가 됩니다 (코인베이스 제외).
- 각 연결 프로토콜에 대한 두 가지 우선 스트림(2PSC, Two Prioritized Stream for Each Connection Protocol). 우선 순위가 서로 다른 평행 세션 두 개를 허용하는 메시지 슬라이싱이 포함된 새로운 메시지 전송 레이어. 이는 우선 순위가 높은 세션으로 블록 헤더를 보낼 수 있게 하며 우선 순위가 낮은 세션으로 전송되고 있던 메시지를 방해합니다.
- 로컬 루트 최적화 프로토콜(LRO, Local Route Optimization) 피어 우선 순위에 기반한 로컬 최적화 블록 루팅. 피어 우선 순위에 기반한 로컬 최적화 거래 루팅.
- 경쟁 블록 간의 보상 공유를 위한 DECOR+ 프로토콜
- 체인 가중치 계산을 위한 GHOST 프로토콜

RSK 기능 비교

저희는 RSK 를 다른 블록체인들과 비교해 기본적으로 RSK 가 분산화를 무너뜨리지 않는 더 나은 기술적 선택임을 보여주고자 했습니다. 이때 분산화는 풀 노드의 경우를 실행하는 비용의 역으로 측정됩니다.

아이템	비트코인	이더리움 (Ethereum)	팩톰 (Factom)	타회사	RSK
평균 확인 시간	10 분	12 초 (GHOST)	1 분 (연합 서버)	10 분	10 초 (DECOR+GHOST)
보안 한계 (이기적인 채굴로 발생하는)	~30%	30%에서 50% 사이	~30%	~30%	50% (DECOR+GHOST)
튜링 완전 스마트 컨트랙트	아니오	예	예	계획됨	예
비트코인에 가치를 더해줌	-	아니오	아니오	아니오	예 (병합 채굴)
비트코인과 통합 가능	-	아니오	오버레이 프로토콜	오버레이 프로토콜	사이드 체인
확률적 검증 및 사기 증명을 통한 확장성	아니오	아니오	아니오	아니오	예
SPV 클라이언트	예	예	아니오	아니오	예
블록 릴레이 백본	예	아니오	예	예	예
유저 정의 접근 구조에 대한 고유 지원	예	아니오	예	아니오	예
유저 정의 서명 형식에 대한 고유 지원	아니오	아니오	아니오	아니오	예
손쉬운 하드웨어 월렛 통합	아니오	예	아니오	아니오	예
보안 보증	SHA256D 채굴자	Ethash 채굴자	SHA256D 채굴자 + 연합	SHA256D 채굴자	SHA256D 병합 채굴자 + 연합
거래 비밀 유지	아니오	컨트랙트를 통해	외부 프로그램을 통해	아니오	AppeCoin 프로토콜을 사용해 고유 지원 계획
고유 거래 ID	아니오 (가단성 있음)	예	아니오	아니오	예
확장성(스케일링 가능) [tps]	3 에서 24	제한 없음	제한 없음	3 에서 24	런칭 시 300
고유 토큰	BTC	ETH	FACTOID	XCP	양방향 페그를 통한 BTC

즉각적 결제 기술 프리뷰

비트코인의 탄생 이래로 PoW 블록체인 기반 암호화폐 간에는 더 낮은 간격을 향한 경쟁이 진행되어 왔습니다. 먼저 10 분 간격의 비트코인이 있었으며, 그 다음 등장한 것은 2.5 분 간격의 LiteCoin 이었습니다. 그 다음은 1 분 간격의 DogeCoin, 30 초 간격의 QuarkCoin, 그리고 12 초 간격의 이더리움입니다. 새로운 암호 화폐가 탄생할 때마다 이 간격은 조금씩 좁아집니다. 그러나 이 간격이 좁아진다는 것이 무엇을 뜻하는지를 아는 디자이너는 몇 명 되지 않습니다. 블록 간격이 암호화폐 네트워크의 안정성과 수용력에 어떤 영향을 미치는지를 이해하려면 여러 가지 요소를 고려해야 합니다. 먼저 짧은 확인 간격의 실행 가능성에 영향을 미치는 가장 중요한 요소는 생생된 스테일 블록의 수입니다. 스테일 블록 비율에 영향을 미치는 주요 요소에는 두 가지가 있습니다. 바로 블록 전파 프로토콜과 톱 채굴자들 간의 블록 전파 시간입니다. RSK 의 경우 저희는 이러한 요소를 신중하게 분석하고 시뮬레이션을 실행해 네트워크의 성능, 유용성 및 보안을 검증했습니다. 이 섹션에서는 RSK 가 스테일 블록 비율을 줄이기 위해 사용하는 새로운 프로토콜을 검토해 보도록 하겠습니다.

DECOR+ 프로토콜

비트코인에서는 두 명 이상의 채굴자가 동일한 높이에 있는 블록을 해결하면 명확한 이해 충돌이 발생합니다. 각 경쟁 채굴자는 나머지 채굴자가 자기 블록을 최고의 체인 팁으로 선택하기를 원합니다. 반면 그 나머지 채굴자들은 어느 것이 선택되든 전체적으로 별로 신경쓰지 않습니다. 그러나, 남아있는 정직한 채굴자와 사용자들은 자연적 전환 확률을 낮추기 때문에 모두가 동일한 블록 팁을 선택하는 것을 선호합니다. 이때 이상적인 해결책은 분쟁을 겪는 채굴자들이 같은 부모를 고르는 것을 인센티브화하는 것이며, DECOR+는 채굴자 간의 상호 작용을 더 이상 요구하지 않고 수렴 선택을 위해 경제적 인센티브를 설정합니다. DECOR+는 다음과 같은 형식으로 경제적으로 분쟁을 해결하는 것을 인센티브화하는 보상 공유 전략입니다.

1. 모든 당사자가 같은 블록 체인 상태 정보에 접근할 수 있으면 분쟁이 결정론적으로 해결됨.
2. 선택한 해결은 분쟁 중인 채굴자와 나머지 채굴자들 모두에게 모든 채굴 수익을 최대화하는 존재임.
3. 이해 충돌을 해결에는 아주 짧은 시간만이 소요됨.

블록 전파 프로토콜

비트코인과 이더리움은 블록 헤더를 블록 내에 포함된 모든 거래로 패킹하여 각 블록을 포워딩합니다. 이 전략은 분석하기 가장 쉬운 반면에 블록 전파 지연과 대역폭 사용량 (다른 전략의 두 배) 모두에서 좋지 않은 성능을 보이는 것으로 알려져 있습니다. 비트코인 채굴자는 빠른 릴레이 네트워크를 사용함으로써 이 문제를 일부 해결했습니다. 이 네트워크는 블록을 압축된 형태로 릴레이하는 중앙 집권화된 백본으로, 단일 사용자가 유지하는 네트워크입니다. RSK 는 네트워크 프로토콜 내에 빠른 릴레이 네트워크가 내장된 채로 탄생되었으며, 저지연적인 성격이 네트워크의 토폴로지 내에서 드러나 중앙 집권화를 필요로 하지 않습니다.

2 단계 블록 전파 (2SBP)

RSK 블록은 두 단계로 전파되는데, 첫 번째 단계에서는 블록 헤더만이 전송됩니다. 두 번째 단계에서는 블록에 포함된 거래의 해시 목록이 전송됩니다. 2SBP 를 사용하면 채널 수용량이 두 배가 되며, 각 블록에 더 많은 거래를 저장할 수 있게 합니다. 각 노드가 블록 헤더를 전송받고 각 거래 해시 리스트가 블록 헤더와 연관지어지고 나면 노드는 블록을 재구성해 완전히 검증하려는 시도를 하게 됩니다.

분실된 거래 푸쉬(PMT, Push Missing Transactions) 프로토콜

각 노드는 그 피어가 홍보하는 거래의 해시를 저장하므로, 채굴자 역시 각 피어의 풀에 없다는 것을 알고 있는, 블록에 포함된 거래를 전송하게 됩니다. 이는 추가 거래를 요청해야 하는 두 번째 접촉의 필요를 완전히 없애 줍니다. 피어가 요청하기 전에 없는 거래를 보내는 것은 2SBP 프로토콜의 세 번째 단계입니다.

거래 지연 포함 (DTI, Delayed Transaction Inclusion) 휴리스틱.

채굴자들은 몇 초 전에 수신된 거래만을 포함시킵니다. 이는 높은 확률로 블록이 채굴되기 전에 피어들이 이미 거래를 받았을 가능성을 보장합니다. 이때 거래를 지연시키는 것이 블록 검증 시간을 줄이고 경쟁 블록의 가능성을 감소시키므로 채굴자에게는 최선임을 참고하시기 바랍니다. 이러한 최적화는 검증되지 않은 블록 채굴의 휴리스틱(MUB, Mining on Unverified Blocks)이 네트워크에서 실행되고 있는 경우에는 필요하지 않습니다.

즉각적 블록 헤더 전파(IBHP, Immediate Block Header Propogation)

최신 블록의 블록 헤더가 수신되면, 노드는 거래를 확인하거나 블록을 검증하기 전에 블록 헤더를 포워딩하며, 블록 PoW 와 높이는 포워드 타임에만 확인하게 됩니다. 이는 헤더가 네트워크에 전파되는 데 1 초 미만이 걸리게 합니다.

각 연결 프로토콜에 대한 두 가지 우선 스트림(2PSC, Two Prioritized Stream for Each Connection Protocol).

각 네트워크 연결은 우선 순위가 다른 두 개의 논리적인 양방향 스트림으로 구성되어 있습니다. 우선 순위가 높은 스트림은 우선 순위가 낮은 메시지가 우선 순위가 낮은 스트림 내에서 전송되고 있다고 해도 블록 헤더를 즉시 전송하는 데 사용됩니다.

검증되지 않은 블록의 채굴(MUB, Mining on Unverified Blocks) 휴리스틱.

그러면 노드는 고정 간격 중에서 거래가 아직 없더라도 헤더 위에서 빈 블록을 채굴하기 시작할 수 있습니다. 그 간격이 지나면 이들은 계속해서 전에 채굴하던 블록을 채굴합니다. 이 빈 블록은 효과적인 대역폭과 블록체인 저장 공간 사용을 감소시키나, 시뮬레이션으로 본 결과 DBI 를 사용하면 생성된 빈 블록의 수와 빈 블록을 보관하는 데 필요한 공간과 TPS 감소가 모두 낮은 것을 확인할 수 있었습니다.

로컬 루트 최적화 프로토콜(LRO, Local Route Optimization)

스테일 블록의 수를 줄이는 것은 채굴자 간의 전송 지연을 줄이는 데 중요한 문제입니다. RSK 네트워크는 채굴자 간의 지연을 줄이고 채굴자 간의 트래픽을 우선화하기 위해 역동적으로 최적화되어 있습니다. 다시 말해서 RSK 는 피어 네트워크 내에 빠른 릴레이 네트워크를 내장시켜 가십 프로토콜을 지리적 위치(지오로케이션)와 최적의 로컬 루트로 강화한다는 뜻입니다. 채굴자 간의 블록 포워딩 경로는 블록 전파에 아주 중요한 경로이며 피어 네트워크에도 아주 중요합니다. 결정적인 경로에서 피어 네트워크 내 비채굴자 네트워크 노드의 존재는 스테일 블록의 비율을 증가시키곤 합니다. 결정적인 경로의 비채굴자 노드(최종 사용자나 모니터링 노드 등)는 채굴자들에게는 약한 익명화 홉스밖에 되지 않습니다. 로컬 노드 결정만으로 결정적인 경로를 생성하려면 LRO 프로토콜을 사용해 노드를 우선화해야 합니다. 이 프로토콜은 RSK 네트워크의 랜덤한 토폴로지 내에 방향성 비사이클 그래프(DAC, Directed Acrylic Graph)의 역동적인 삽입을 생성하며, DAC 는 여기서 이 랜덤한 토폴로지를 최적으로 연결시킵니다.

비트코인 채굴 네트워크 재사용하기

집중된 채굴 네트워크는 넓은 채굴 풀로 인해 완전히 분산화된 채굴 토폴로지보다 스테일 블록을 훨씬 덜 생성하곤 합니다. 따라서 빠른 결제의 경우에는 SHA-256D PoW 에 기반한 암호코인이 ASIC 비호환 PoW 기반 암호코인보다 더 유리합니다.

네트워크의 실제 토폴로지

비트코인 디자인은 네트워크가 특정 평균 출력 차수와 진입 차수를 갖춘 랜덤한 그래프와 비슷하다고 가정합니다. 이는 물론 사실과는 많이 다르지만, 네트워크 노드는 지리학적 무리를 이루는 것을 방지하기 위해 (적어도 아웃바운드 연결에서는) 로컬 결정을 내립니다. 이는 블록 전파를 돕는 데는 최상의 토폴로지가 아닙니다. 블록 전파의 최상인 토폴로지는 톱 채굴자 간의 직접적인 연결을 장려하거나 톱 채굴자 사이에서 블록을 더 빠르게 루팅하여 톱 채굴자에게 더 유용한 토폴로지입니다. 채굴자 간의 직접적인 백본은 무엇보다도 스테일 블록의 수를 줄이는 데 도움이 될 수 있습니다. 이는 공격으로부터의 탄력성을 높이기 위해 비트코인이 제안한 방법이기도 합니다. RSK 는 LRO 휴리스틱을 사용해 채굴자 간 인증 비용이나 채굴자 프라이버시, IP 주소 공개 및 관련이 있을 수 있는 DoS 공격 없이 역동적인 채굴자 백본을 설립하고 있습니다.

PoW 기능 검증 시간

SHA-256 의 평가는 아주 빠르며 그에 따라 비트코인 PoW 검증 시간 역시 아주 짧습니다. 반면 Scrypt PoW 에는 선택한 매개 변수에 따라 (GPU 또는 ASIC "저항") 3 에서 30 ms 정도의 평가 시간이 소요될 수 있습니다. 네트워크를 스팸과 DoS 공격으로부터 보호하기 위해 각 노드는 블록 헤더를 포워딩하기 전에 블록 PoW 를 검증해야 합니다. 따라서 검증 지연 시간은 채굴자 간의 블록 결정적인 경로 내 홉스의 수로 곱해집니다.

클라이언트 네트워킹 스택

노드가 일단 블록 헤더를 수신하고 나서 네트워크 내 스테일 블록 생성 수를 줄이기 위해 할 수 있는 가장 좋은 것은 이를 최대한 빨리 포워딩하는 것입니다. 이는 다른 모든 노드 활동이 일시 중지되거나 멈춰진다는 것을 뜻합니다. RSK 는 우선 순위가 낮은 작업이 바로 취소되고 재시도를 허용하게 설계되어 있습니다. 클라이언트 네트워킹 스택은 즉각적인 포워딩을 허용하기 위해 거래 검증 절차나 체인 재정비와 같은 다른 관리 활동 중인 클라이언트를 차단하지 않게 됩니다. 이는 멀티 스레드(다중 일련 처리)를 허용하고 역동적으로 스레드 우선 순위를 배정해 블록 헤더를 수신한 스레드를 촉진하는 RSK 클라이언트로 인해 가능합니다.

블록 오버헤드

대부분의 암호 화폐 내 블록 헤더는 크기가 작습니다(~100 바이트). 따라서 헤더 크기에는 (전체 블록 크기에 비해) 큰 사전 준비가 필요하지 않습니다. RSK 헤더는 더 큰 편이나, 저수준 네트워크 MTU 가 일반적으로 1500 바이트 정도이고, 블록 헤더 크기보다 크기 때문에, 블록 헤더 사전 준비는 전파 시간에 뚜렷하게 부정적인 영향을 미칩니다.

시뮬레이션

저희는 이 목적을 위해 특별히 구축한 별개의 이벤트 시뮬레이션을 사용해 블록 전파를 실험해 보았습니다. 이 시뮬레이터는 작은 그룹의 톱 채굴자 간의 작용을 실험하며, 각 채굴자는 서로 간의 홉 간격이 네트워크 내 노드 간의 평균 간격에 가까운 랜덤 그래프로 표시됩니다. 이러한 경우는 최악의 시나리오는 아니지만, 톱 채굴자들은 영향력이 높을수록 유리하므로, 평균보다 못한 성과를 보이지는 않을 것으로 예상합니다. 시뮬레이션 내의 이벤트는 여러 장소 중 하나의 블록 생성과 각기 다른 채굴자의 장소로의 블록 전파입니다. 다음 결과는 시뮬레이션에서 RSK 가 5 블록 간격과 300 TPS 를 기록했음을 보여주고 있습니다(현재 블록 간격은 10 초). 이 시뮬레이션의 주요 결과는 거래가 20.35 초가 지나기 전에 99.98%의 확률로 수락된다는 것입니다 (반전 확률 0.02%). 이때 반전 확률은 대체 포크가 제거된 거래를 포함할 가능성을 고려하지 않으므로, 실제로는 훨씬 더 낮을 수 있음을 참고하시기 바랍니다.

안전한 병합 채굴

병합 채굴은 비트코인 채굴자가 거의 0 에 가까운 한계 비용과 함께 다른 암호화폐를 채굴할 수 있게 하는 테크닉입니다. 비트코인 채굴에 사용되는 것과 동일한 채굴 인프라와 설정이 RSK 를 동시에 채굴하는 데 재사용됩니다. 이는 RSK 가 추가 거래 수수료를 지불하므로 병합 채굴의 인센티브가 높음을 뜻합니다. 그러나 이는 또한 펌프 앤 덤프나 평행 체인을 사용해 네트워크를 공격하는 비용이 병합되지 않은 암호화폐를 공격하는 것보다 더 낮다는 뜻이기도 합니다. RSK 는 초기 부트스트래핑 단계에서 공격을 방지하기 위한 여러 가지 보호 조치를 마련해 두었습니다. 이는 다음과 같습니다.

- 연합 체크포인트: RSK 클라이언트가 연합 회원이 서명한 체크포인트를 기대함. 연합은 거래소 및 기타 플랫폼의 성공과 관련된 매우 안전한 이들을 포함할 것임. 노드는 연합 체크포인트를 사용해 시빌 공격을 감지하고 사용자에게 이를 알림.

- 채굴 코인 성숙도: 각 채굴 코인은 24 시간의 성숙 시간이 있으며, 이는 비트코인보다 약간 길음. 코인 성숙도 증가는 펌프 앤 덤프 공격의 인센티브를 줄여줌.

- 체크포인트는 소스 코드에 내장됨

거래 개인 정보 보호

RSK 는 혼자만으로 비트코인보다 더 나은 거래 프라이버시를 제공하지 않으며 별칭(가명)에 의존하고 있습니다. 그럼에도 불구하고 RSK 의 VM 은 튜링 완전 VM 이므로, CoinJoin 이나 Appecoin 과 같은 익명화 기술을 제 3 자의 개입 없이 안전하게 실행할 수 있습니다.

보안

알트코인은 주로 병합 채굴을 많이 사용하지 않는데, 이는 초기 암호화폐 부트스트랩 기간 동안 병합 채굴이 커다란 비트코인 채굴 풀의 51%의 공격을 통한 새로운 암호 화폐 방해를 허용하기 때문입니다. RSK 는 플랫폼을 부트스트랩하는 안전한 방법으로 연합 체크포인트를 실행하고 있으며 그에 따라 이러한 위험을 크게 줄이고 있습니다. RSK 는 또한 비트코인 해시 파워의 30%에 해당하는 최소 해시 파워와 함께 런칭될 예정입니다. RSK 재단은 네트워크 건강을 감독하고 알림 시스템을 사용해 사용자들에게 알림을 전달하며 네트워크를 롤백 공격에서 보호할 것입니다.

확장성

현 상태로의 RSK 는 비트코인보다 확장성이 훨씬 높습니다. RSK 결제는 표준 비트코인 결제의 5 분의 1 에 불과한 규모이며, 시간 간격당 블록 페이로드는 비트코인보다 8 배 높습니다. RSK 는 또한 사용자가 선택할 수 있는 여러 가지 서명 제도를 제공할 예정입니다. ECDSA, Schnorr 및 Ed25519 이 바로 그 것입니다. 이때 Ed22519 는 일반적으로 비트코인 ECDSA 커브보다 몇 배 더 훨씬 성능이 뛰어납니다.

다른 모든 조건이 동일할 때 RSK 는 비트코인보다 대역폭을 평균 50% 덜 소모합니다. 이는 블록이 거래 데이터를 포함하지 않고 기존에 알려진 거래의 레퍼런스만을 포함하기 때문입니다. 저장 공간 및 대역폭 사용은 확률적인 검증과 사기 증명 기술을 사용해 더 크게 줄일 수 있습니다.

확률적 검증 및 사기 증명

풀 노드를 소유하는 비용은 암호화폐의 중앙 집권화 정도에 영향을 미치는 주요 요소입니다. 이 비용이 높을수록 중앙 집권화의 정도가 더 높습니다. 그러나 저희는 분산화에 있어 과격주의 포지션을 유지하는 것이 암호화폐가 글로벌한 결제 네트워크가 될 수 없음을 암시한다고 생각합니다. 이 목표는 서로와 상충됩니다. 비트코인은 대부분의 개인 사용자가 참여할 수 있음을 보장하기 위해 블록체인 크기 제한이 충분히 낮으므로 이미 크게 분산화된 네트워크를 제공하고 있습니다. 이는 RSK 사이드체인이 비트코인 네트워크가

통화 제어의 중앙 집권화에 맞서는 보호 장치로 작용하게 하는 동시에 비트코인을 넘어서는 높은 확장성을 달성할 수 있게 합니다.

저희는 제삼자 신뢰, 네트워크 노드 신뢰와 자가 검증 간의 교환이 가능하다고 믿으며, 사용자들이 가장 편한 비율을 직접 찾을 것을 권장합니다. RSK 플랫폼은 노드 비용을 줄이기 위해 노드가 풀 블록 체인의 하위 집합을 보관하고 검증할 수 있게 합니다. 이는 확률적 검증 및 사기 증명 블록을 통해 진행됩니다. 확률적 검증은 (일부) 노드가 검증할 블록을 무작위로 선택하고, 남은 블록을 특정 조건이 충족되는 한 괜찮은 것으로 수락하는 기술입니다. 이때 그 조건은 특정 시간이 지났을 것, 어느 정도의 확인 블록이 추가되었을 것, 네트워크 연결성이 충분할 것, 유효한 사기 증명 블록이 전파되지 않았을 것, 그리고 옵션으로 일부 권위적 체크포인트가 전파되었을 것입니다. 사기 증명은 "사기"임이 표시되는 블록입니다. 노드는 사기 증명 블록을 수신하면 같은 높이의 블록이 자체에서 승인된 적이 있는지(그러나 검증되지 않은 적이 있는지)를 확인하고, 만약 그런 경우 블록을 검증합니다. 블록이 유효하지 않으면 로컬 최고 체인은 알맞게 재정비됩니다. 사기 증명 블록은 작업 증명도 보관하고 있기 때문에, 실제 사기인 사기 증명 블록을 전파하는 비용은 높습니다. 피어에게서 실제 사기인 사기 증명 블록을 수신하는 노드는 부정 행위를 저지른 피어를 영구 차단합니다. 필요한 경우, 노드는 피어들에게 초기 작업 증명을 요청해 값싼 DoS 가 훼손된 IP 를 사용하는 것을 방지합니다. 채굴자들은 (PoW 와 연합 채굴자 모두) 블록 데이터를 원천 징수하는 공격자가 최고 체인에 영향을 미칠 수 없게 반드시 풀 노드여야 합니다. 이는 채굴자들이 빠르게 공격자의 블록을 버릴 것이기 때문입니다.

결론

RSK 는 4 년 간의 블록체인 기술 개선의 정점을 대표하며, 암호화폐 생태계가 비트코인 (통화) 가치를 높이는 동시에 프로그래밍 가능한 금전과 결제의 최고 기능을 활용할 수 있게 할 것입니다.

이는 또한 전 세계의 개발자가 세계에서 가장 안전한 네트워크를 통해 여러 가지 니즈에 맞는 낮은 거래 비용으로 개인 및 기업의 분산화 솔루션을 생성할 수 있게 할 것입니다.

이는 또한 비트코인 채굴자들이 스마트 컨트랙트 시장에 참여할 수 있게 함으로써 채굴 산업에 중요한 가치를 더하고 시장의 장기적 지속성을 보장할 것입니다.

또, 이는 더 넓은 채굴자 베이스의 생성에 기여해 비트코인 네트워크의 보안을 강화할 것입니다.

마지막으로 이는 분산화되고, 즉각적이며 저렴해, 은행을 이용할 수 없고 금융 면에서 어려움을 겪고 있는 전 세계 30 억 명의 사람들을 화합하고 이들에게 기회를 제공하는 금융 시스템의 개발을 활성화할 것입니다.

RSK 코어 팀