스택스 2.0: 비트코인을 위한 앱과 스마트 컨트랙트

Muneeb Ali
Translated by GM Chung gm@despread.io

백서 초안 **v0.1**
2020년 12월

Stacks

개요

본 백서는 스마트 컨트랙트와 탈중앙 앱을 비트코인에 가져오는 레이어-1 블록체인, 스택스(Stacks) 2.0 블록체인에 대한 개요를 제공하며, 두 블록체인을 이어주는 최초의 합의 알고리즘에 대해 다루고 있습니다. 스택스 2.0은 스마트 컨트랙트 및 탈중앙 앱을 비트코인의 보안, 안정성, 및 경제력과 통합합니다.

블록체인은 30년 전 웹(Web)이 탄생한 이래 가장 중요한 인터넷 업그레이드입니다. 블록체인은 최초로 개방형 프로토콜을 사용하여 디지털 자산을 정의하고 참여하게 해줌으로써, 이전에는 불가능했던 새로운 비즈니스 모델과 기능을 탄생시켰습니다.

비트코인은 가장 먼저 생겨난 안전한 블록체인으로, 개인이 통제하거나 변경할 수 없는 새로운 유형의 돈을 제공합니다 [1]. 비트코인 네트워크는 비트코인 암호화폐뿐만 아닌 일반적인 결제 프로토콜을 위한 토대를 제공합니다.

블록체인은 새로운 유형의 컴퓨터 프로그램을 가능하게 합니다: (a) 블록체인에 퍼블리싱 할 수 있는 스마트 컨트랙트는 신뢰가 필요 없이 실행되고 누구나 해당 결과 값을 확인할 수 있으며 (b) 사용자 소유이고 중앙 집중식 서버를 사용하지 않는 탈중앙 앱입니다. 이더리움은 스마트 컨트랙트의 힘을 입증했으며, 스택스는 입증된 스마트 컨트랙트 기능을 비트코인에 제공합니다.

우리는 탈중앙 앱과 사용 사례가 연결이 끊어진 네트워크가 아닌 가장 강력하고 가장 널리 사용되는 블록체인 네트워크인 비트코인을 기반으로 구축될 것이라 믿습니다. 초창기 인터넷에도 여러 경쟁 프로토콜이 존재하였으며, TCP/IP가 성공한 표준으로 자리 잡음과 동시에 모든 것들이 그 위에 구축되었습니다. 비트코인은 암호화폐에 있어 표준과도 같습니다.

비트코인을 가치 저장을 위한 표준이라 생각하기 때문에, 우리는 비트코인과 스택스 블록체인을 연결하고 비트코인의 기능을 확장시켜주는 두 블록체인 간의 첫 번째 합의 알고리즘인 전송증명(PoX)를 탄생시켰습니다. 리더 선정(Leader election)은 비트코인 체인에서 이뤄지며 새로운 블록은 연결된 스택스 체인에 기록됩니다.

스택스 2.0 블록체인은 비트코인을 수정하지 않고 (a) 확장 가능한 트랜잭션과 (b) 범용 스마트 컨트랙트를 비트코인에 가져옵니다. 스택스 채굴자는 비트코인(BTC)를 사용하여 새롭게 발행된 스택스(STX)를 채굴합니다. 스택스 보유자는 합의에 STX를 락업하여 비트코인을 획득할 수 있으며, STX는 기본적으로 BTC로 가격이 책정되고 BTC 수익을 제공하는 고유한 암호화폐 자산이 될 것입니다.

안전하고 예측 가능한 스마트 컨트랙트 언어인 클래러티(Clarity)는 스택스 2.0 메인넷 출시와 함께 활성화됩니다. 지난 2년 동안 프린스턴 및 MIT 연구원들이 개발해왔으며, 클래러티는 스마트 컨트랙트에 버그가 덜 발생하고 개발자가 비트코인 상태(state)에 대한 로직을 직접 작성할 수 있게 합니다. 우리는 비트코인에 스마트 컨트랙트 기능을 불어넣음으로써 BTC가 더 이상 수동적인 자산이 아닌 생산적인 용도로 사용될 수 있기 때문에 BTC의 가치를 높일 수 있을 것이라 믿습니다.

스택스 암호화폐는 2019년 SEC로부터 최초로 승인받은 토큰 오퍼링을 통해 일반 대중들에게 배포되었습니다. 스택스(STX)는 클래러티 스마트 컨트랙트를 위한 연료로 사용됩니다.

면책 조항: 본 문서는 증권형 혹은 토큰 투자 권고가 아닌 정보 전달 목적으로만 사용됩니다. 백서에는 불명확한 미래에 대한 예측 진술이 포함됩니다. 또한 본 백서에 담긴 정보는 시간이 지남에 따라 내용이 오래될 수 있습니다.

왜 비트코인인가

비트코인은 가장 강력한 블록체인입니다. 비트코인은 변조 불가능한 진실 공급원(source of truth)이자 가치 저장 프로토콜입니다. 궁극적인 진실 공급원을 확보한다면, 이를 응용한 다른 탈중앙 프로토콜 및 사용 사례를 구축할 수 있습니다. 기존 인터넷에서 TCP/IP 프로토콜이 표준으로 등장함과 동시에 사람들은 더 이상 이를 혁신하기 위해 수정할 필요가 없어졌으며, 한번 확립된 프로토콜은 경쟁을 필요로 하지 않게 됨을 알 수 있었습니다. 비트코인은 주권이자 가치 저장 프로토콜로, 세상은 하나의 가치를 기준으로 수렴하게 될 것입니다. 우리는 네트워크 효과, 보안, 암호화폐 시장 점유율을 고려하였을 때 이 시장의 가치 표준이 비트코인이 될 것이라 믿습니다.

비트코인이 단순히 “one-trick pony”이며 가치 저장 수단 외 사용처가 없다는 오해가 있습니다. 하지만 비트코인 결제 프로토콜을 중심으로 혁신하고 범용 스마트 컨트랙트 및 탈중앙 앱을 활성화할 수 있으며, 비트코인을 변경할 필요가 없습니다.

비트코인 상에서 앱과 스마트 컨트랙트를 구축함에 있어 두 가지 근본적인 문제가 존재합니다:

1) 확장성(Scalability): 비트코인 블록체인은 거래 용량이 제한되어 있습니다.

2) 안전한 컨트랙트(Secure contracts): 비트코인 블록체인은 제한된 스크립팅 언어를 사용하기 때문에 일반적인 스마트 컨트랙트를 사용할 수 없습니다. 이러한 설계로 인해 베이스 레이어의 높은 보안성을 자랑합니다.

스택스 블록체인은 확장성의 한계와 제한된 스마트 컨트랙트 문제를 해결하여 비트코인을 위한 앱과 스마트 컨트랙트를 가능하게 합니다. 이는 두 블록체인 간 실행되는 고유한 합의 알고리즘을 통해 이뤄집니다. 비트코인 블록체인은 스마트 컨트랙트가 스택스 체인에서 실행되는 동안 결제 레이어 및 진실 공급원 역할을 수행합니다.

비트코인 상에서 직접적으로 확장 가능한 스마트 컨트랙트를 가능하게 하는 것은 오랜 기간 해결하지 못한 숙제였으나, 스택스 블록체인이 이 문제를 해결하게 됩니다. 이때 스택스가 고려한 중요한 설계 요구 사항은 비트코인에 앱과 스마트 컨트랙트를 활성화하기 위해 비트코인을 별도로 수정하지 않는다는 점입니다.

비트코인은 현재 (수동적인) 가치 저장고로써 역할하고 있으며, 비트코인 암호화폐는 비트코인 블록체인의 주요 사용 사례입니다. 현재 다른 블록체인에서 테스트되고 있는 성공적인 사용 사례는 비트코인을 사용하여 쉽게 이식하거나 직접 구축할 수 있습니다.

비트코인 수익(Earning):

비트코인 네트워크의 보안과 비트코인 암호화폐 자본에 대한 접근성은 스택스 설계의 이점입니다. 또한 STX 보유자가 STX를 락업하여 합의 알고리즘에 참여함으로써 BTC를 보상받을 수 있는 스택스 암호화폐만 의 고유한 경제적 특징이 존재합니다.

비트코인 수익 모델은 비트코인의 한정된 공급량과 인플레이션에 대한 햇징 수단으로 사용됨을 미뤄보았을 때 더욱 매력적으로 느껴지게 됩니다. 또한 스택스 블록체인의 스마트 컨트랙트 사용이 증가함에 따라 BTC 수익률은 증가하게 됩니다.(6 페이지 참고)

스택스 **2.0** 디자인

스택스 2.0은 레이어-1 블록체인으로 비트코인에 연결하여 보안을 확보하고 탈중앙 앱과 예측 가능한 스마트 컨트랙트를 사용할 수 있습니다. 스택스 2.0은 비트코인 보안에 앵커링된 PoX 마이닝(채굴)을 구현합니다. 리더 선출은 비트코인 블록체인을 통해 이뤄지며 STX 채굴자는 연결된 스택스 블록체인에 새로운 블록을 기록합니다. PoX를 사용하면 비트코인을 수정 필요 없이 스마트 컨트랙트 및 앱을 활성화할 수 있습니다.

PoX 합의 메커니즘에는 다음과 같이 두 가지 유형의 참여자가 존재합니다: (a) STX 채굴자, (b) STX 보유자.

STX 채굴자는 비트코인 블록체인과 스택스 블록체인의 상태(state)를 확인할 수 있습니다. STX 채굴자들은 비트코인 블록체인으로부터 트랜잭션을 전송하여 리더 선출에 참여하고, VRF(Verifiable Random Function)를 통해 각 라운드의 리더를 무작위로 선택하고 (더 많은 BTC 입찰에 많은 가중치를 부여), 리더는 스택스 체인에 새로운 블록을 기록합니다. STX 채굴자는 새롭게 채굴된 STX (코인베이스 보상), STX로 지불된 거래 수수료, STX로 지불된 각 블록의 클래러티 컨트랙트 실행 수수료를 받습니다. STX 채굴자는 BTC를 채굴 비용으로 사용하고, BTC를 사용하여 리더 선거에 참여합니다. STX 채굴자는 새로운 스택스 블록의 총 가치를 BTX/STX 온체인 거래 페어로 모델링 할 수 있으며, 외부 거래소보다 채굴을 통해 STX를 더 저렴하게 얻을 수 있다면 채굴에 참여하게 될 것입니다.

STX 보유자는 스택킹(stacking)을 통해 합의에 참여하고 BTC를 보상받을 수 있습니다. 참여를 위해 사용자는 보상주기 (약 2주) 동안 STX를 락업하고, 풀노드를 실행 또는 지원하고, STX 트랜잭션을 통해 네트워크에서 유용한 정보를 전송합니다. 스택킹에 적극적으로 참여하는 STX 보유자는 해당 주기 동안 사용된 비트코인을 보상받습니다. 지분증명과는 달리 STX 보유자는 슬래싱 (프로토콜 상에서 발생하는 경제적 패널티)에 대한 위험이 존재하지 않습니다.

스택스 1.0은 제한된 기능을 갖춘 초기 디자인으로 2018년 가을 비트코인 기반으로 론칭되었습니다. 스택스 2.0은 주요 업그레이드와 함께 모든 기능을 갖춘 디자인으로 2021년 1월 메인넷 론칭을 예상하고 있습니다. 본 백서는 스택스 2.0만 다루고 있으며 이전 스택스 1.0의 기술 디자인을 대체합니다 [2].

트랜잭션 확장성:

스택스 블록체인 트랜잭션은 비트코인과 독립적으로 확장 가능합니다. 트랜잭션은 완결성(finality)을 위해서만 비트코인에 의존합니다. 수천 개의 스택스 트랜잭션은 비트코인의 단일 해시에 담깁니다; 스택스 트랜잭션은 합의의 일부로서 매 비트코인 블록마다 자동으로 정산(settle) 됩니다. 또한 스택스는 몇 초 만에 초기 확인(confirmation)을 가능하게 해주는 마이크로블록(microblock) 개념을 도입하였습니다. 마이크로블록은 미래 확장성 연구를 위한 주요한 개념으로, 이론상 마이크로블록은 비트코인 블록 당 더 빠른 합의 알고리즘을 통해 데이터를 처리할 수 있습니다.

비트코인은 스택스의 결제(settlement) 프로토콜로 사용됩니다. 이는 궁극적으로 진실 공급원 역할을 수행하며 스택스 블록 기록의 해시를 보관합니다. 거래 완결성은 현재 비트코인과 연결되어 있으며 비트코인이 우리의 디자인을 위한 강력한 완결성을 제공할 것입니다.

스택스 2.0 블록체인은 Rust로 작성되었습니다. 프로토콜 세부 정보와 오픈 소스 코드는 Stacks GitHub 레포지토리 [3]를 통해 확인할 수 있습니다.

PoX 합의

PoX(Proof of Trasfer, 전송증명)는 두 블록체인을 이어주는 최초의 합의 알고리즘입니다. 비트코인을 베이스 체인으로 사용하고 스택스를 연결된 체인으로 사용하여 PoX 구현합니다. PoX에서의 리더 선출은 비트코인 블록체인을 통해 이뤄집니다. PoX는 작업증명 방식과 같이 전기를 사용하는 것이 아닌, 이미 발행된 비트코인을 "계산 증명(proof of computation"으로 재사용하고 채굴자는 비트코인을 채굴 비용으로 사용합니다.

STX 채굴자들은 다음 라운드의 리더로 선출되기 위해 입찰(bid)합니다. 프로토콜은 VRF를 통해 라운드에서 이긴 채굴자 (즉, 리더)를 선택합니다. 리더는 스택스 블록체인에 새로운 블록을 기록하고 보상을 얻습니다: 블록을 통해 새롭게 발행된 스택스, 스마트 컨트랙트 및 트랜잭션 수수료.

채굴자 입찰에 사용된 비트코인은 합의에 적극적으로 참여하는 스택스(STX) 토큰 보유자의 특정 주소 집합으로 전송됩니다. 따라서 채굴 과정에서 사용된 비트코인은 없어지지 않고 스택스 보유자들에게 스택스 보유 및 스택스 알고리즘 참여에 대한 보상으로 전송됩니다.

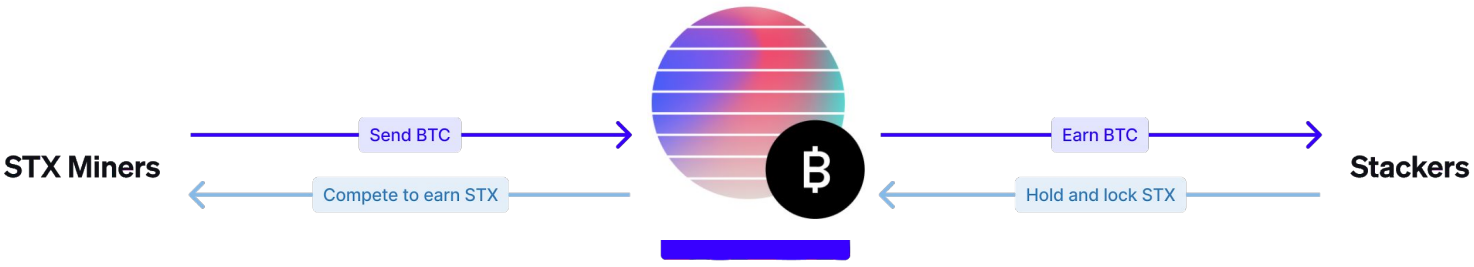
PoX 매개 변수:

- 블록 보상: 첫 4년 동안 블록 당 1000 STX; 이후 4년 동안 블록 당 500 STX; 그 후 4년 동안 250 STX; 이후 영구적으로 블록당 125 STX가 발행됩니다.

- 블록 시간: 스택스 블록체인은 비트코인과 동일한 속도로 블록을 생성합니다. 비트코인 블록은 대략 10분에 한 번씩 생성되므로 이는 스택스 2.0 메인넷의 속도가 됩니다. 그러나 마이크로블록을 통해 더 빠른 초기 확인 (confirmation)이 가능합니다.

- 블록 보상 만기(maturity window): 100 블록, 즉 채굴자가 블록을 생성하면 100 블록이 경과한 뒤 해당 블록에 대한 코인베이스 보상을 획득합니다.

- 스택킹 임계값: 필요한 최소 STX 수는 참여율에 따라 달라집니다. 참여율이 25%에서 100% 사이일 경우 STX 참여 수량의 0.025%이고, 참여율이 25% 미만일 경우 한도 수량은 항상 STX 유동 공급량의 0.00625%입니다.



Proof of Transfer consensus mechanism

Pox 합의 관련 세부 사항은 PoX 기술 문서 [4]를 통해 확인 가능합니다.

클래러티 스마트 컨트랙트

클래러티(Clarity)는 스마트 컨트랙트를 위한 새로운 프로그래밍 언어입니다. 클래러티 언어는 예측 가능성과 보안을 위해 최적화되어 있습니다. 스택스 2.0은 클래러티 스마트 컨트랙트를 비트코인에 앵커링시켜 스마트 컨트랙트를 가능하게 하며, 비트코인 블록체인에서 본 행동(action)을 기반으로 작동합니다.

제대로 설계된 스마트 컨트랙트는 버그를 예방할 수 있지만 부실하게 설계된 컨트랙트는 문제를 악화시킬 수 있습니다. 이는 스마트 컨트랙트가 디지털 화폐를 다루고 있기 때문에 굉장히 중요합니다. 우리는 클래러티를 통해 WYSIWYG(What you see is what you get) 접근방식을 택했습니다. 클래러티는 개발자와 자동 검증을 위해 스마트 컨트랙트가 어떻게 작동하고, 얼마만큼의 비용이 필요로 하며, 어느 정도의 성능을 발휘할 수 있는지 미리 파악할 수 있게 도와줌으로써 사전 안전성을 제공합니다.

결정 가능 언어:

클래러티는 결정 가능한 언어입니다. 프로그래밍 언어가 프로그램에서 무엇을 실행할지 코드를 통해 확실하게 알 수 있다면 결정 가능(decidable)하다고 합니다. 클래러티는 "튜링 복잡성(Turing complexity)"을 방지하기 때문에 의도적으로 튜링 불완전합니다. 때문에 주어진 스마트 컨트랙트의 전체 콜 그래프에 대한 완전한 정적 분석이 가능합니다. 또한 유형 및 유형 검사기에 대한 지원은 의도하지 않은 캐스트, 재진입 버그 및 초기화되지 않은 값 읽기와 같은 전체 버그 클래스를 제거할 수 있습니다. 마지막으로 클래러티 코드는 런타임 비용 및 데이터 사용량에 대해 분석 가능합니다. 개발자는 특정 클래러티 프로그램이 수행할 작업과 비용을 예측할 수 있습니다.

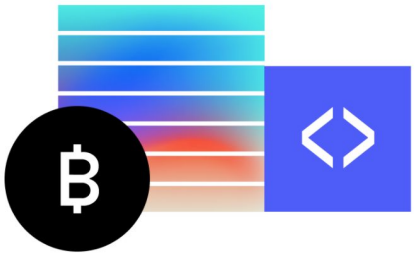
이더리움에서 계약을 구현하는 언어 솔리디티(Solidity)는 결정 불가능한 언어입니다. 특정 상황에서 계약을 실제로 실행하지 않고는 계약이 어떻게 작동할지 정확히 알 수 없습니다. 두 가지 유형의 프로그래밍 언어 모두 장점이 있습니다. 그러나 수십억 달러의 코드를 락업하는 스마트 컨트랙트의 경우 위험을 최소화하는 것이 매우 중요합니다.

컴파일러(Compiler) 부재:

결정 가능한 언어일 뿐만 아니라 클래러티는 해석 가능합니다. 컨트랙트 소스 코드 자체는 블록체인 노드에 의해 퍼블리싱되고 실행됩니다. 중간의 컴파일된 표기 (예를 들어 솔리디티 용 EVM 바이트 코드)를 제거하면 버그를 유발할 수 있는 확률이 더욱 최소화됩니다. 컨트랙트 소스 코드를 퍼블리싱하면 이해도도 향상됩니다. 프로그래밍된 소스 코드에 오류가 존재하지 않을 수 있지만 최종 프로그램이 블록체인에 도달할 수 있기 때문에 컴파일러 버그는 블록체인에서 두 배로 손상을 입히게 됩니다. 그러나 오류를 해결하려면 잠재적으로 하드포크가 필요로 할 수 있습니다.

비트코인 상태에 대한 가시성:

클래러티 컨트랙트는 비트코인 상태에 대한 가시성을 갖추고 있으며, 이는 컨트랙트 로직이 순수한 비트코인 트랜잭션을 기반으로 트리거될 수 있음을 의미합니다. 클래러티 컨트랙트에는 비트코인에 대한 SPV 증명이 내장되어 있으며 개발자가 비트코인 상태와 훨씬 쉽게 상호작용 할 수 있습니다. 클래러티는 비트코인과 포크를 계약하므로 개발자는 비트코인 포크와 스마트 컨트랙트가 포크에 맞춰 조정해야 하는 코너 케이스에 대해 걱정할 필요가 없습니다.



스택스 **(STX)** 암호화폐

스택스 암호화폐 (STX)는 클래러티 스마트 컨트랙트를 실행하기 위한 “연료"로 사용되도록 설계되었습니다. 스택스는 디지털 자산 등록, 거래 수수료 지불, 블록체인에 클래러티 컨트랙트 퍼블리싱과 같은 네트워크 기능에 사용됩니다.

스택스는 STX 보유자가 합의에 참여하고 비트코인 보상을 받기 위해 락업할 수 있습니다. 이 과정을 스택킹(Stacking)이라고 합니다. 참여를 위해 STX 보유자는 풀노드를 실행하고 STX를 락업하고 유용한 정보를 주기적으로 네트워크에 퍼블리싱합니다. 비트코인 보상의 연간 수익률은 다양한 요인에 의해 결정됩니다. 예를 들어, 가정된 매개 변수와 함께 유동 공급량의 50%가 참여하면 수익률은 약 9%가 될 수 있습니다. 자세히 보기 [5].

스택스 암호화폐는 미국 역사상 최초로 SEC로부터 승인받은 토큰 오퍼링을 통해 4,500 명이 넘는 개인 및 단체가 참여하였으며 대중에 배포되었습니다.

PoX 합의 메커니즘은 STX와 BTC 간 기본 교환 페어를 설정하고 비트코인에서 수익을 얻기 위해 이를 락업할 수 있다는 점에서 STX를 고유한 자산으로 만듭니다. 이는 동일한 암호화폐로 수익을 제공하는 지분증명 자산과는 차이가 존재합니다.

장기적 가치:

다른 암호화폐와 마찬가지로 스택스 암호화폐에는 암호화 자산의 가치에 부정적인 영향을 미칠 수 있는 몇 가지 위험 요소가 존재합니다. 이에 대한 위험성이 담긴 포괄적인 항목을 확인하고자 한다면 2019년 SEC 오퍼링의 위험 요소 섹션을 참조하면 됩니다 [6].

스택스의 장기적 가치는 일반적으로 스택스 네트워크의 성장과 클래러티 스마트 컨트랙트에 대한 수요에 달려있습니다. 네트워크에서 클래러티 컨트랙트를 실행하려면 사용자가 STX를 연료(가스 요금)로 지불해야 합니다. 예를 들어, 클래러티 컨트랙트로 구축된 탈중앙화 거래소는 각 사용자 상호작용에 있어 거래소 컨트랙트 로직을 실행하기 위한 수수료로 STX를 필요로 합니다.

비트코인 수익이라는 고유한 특징으로 인해 STX 유동 공급량의 일부가 락업되고 실제 사용 가능한 유동 공급량은 줄어들 것으로 예상됩니다. 이렇게 장기 보유자들은 적극적으로 합의에 참여함으로써 비트코인 보상을 얻을 수 있습니다. STX 보유자가 얻게 되는 비트코인 보상은 (a) 코인베이스 보상 그리고 (b) 네트워크 사용량에 따라 달라집니다. 네트워크에서 더 많은 클래러티 컨트랙트가 실행되면 스택킹에 대한 비트코인 보상도 증가하게 됩니다. 초기에는 새로운 블록 당 1000 STX가 코인베이스 보상으로 새롭게 발행됩니다. 코인베이스 보상 외에도 컨트랙트 및 거래 수수료는 채굴자가 블록을 평가하는 방식을 결정하게 됩니다. 네트워크 사용량이 증가함과 동시에 더 많은 컨트랙트 및 거래 수수료가 발생할 것이며 채굴자들의 블록 가치는 올라가게 될 것입니다. 이는 블록에 대한 더 많은 비트코인 입찰이 이뤄지고 합의에 적극적으로 참여하는 STX 보유자들에게 더 많은 BTC 보상이 주어질 수 있음을 의미합니다.

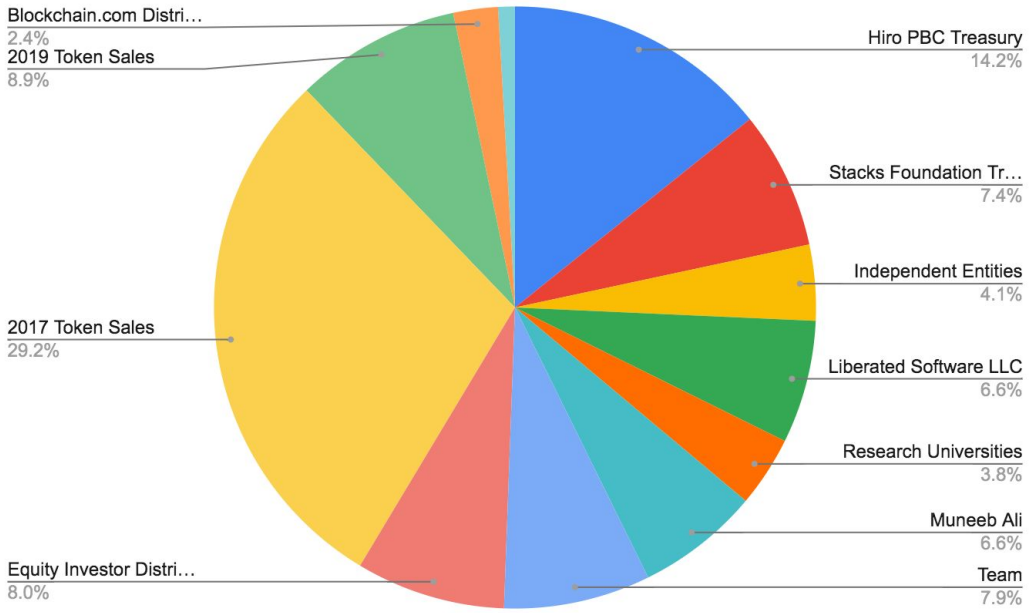
코인베이스 STX	클래러티 수수료	트랜잭션 수수료

* 코인베이스 STX는 정해진 일정에 따라 진행됩니다.
* 클래러티 & 거래 수수료는 네트워크 사용량에 따라 증가 혹은 감소합니다.

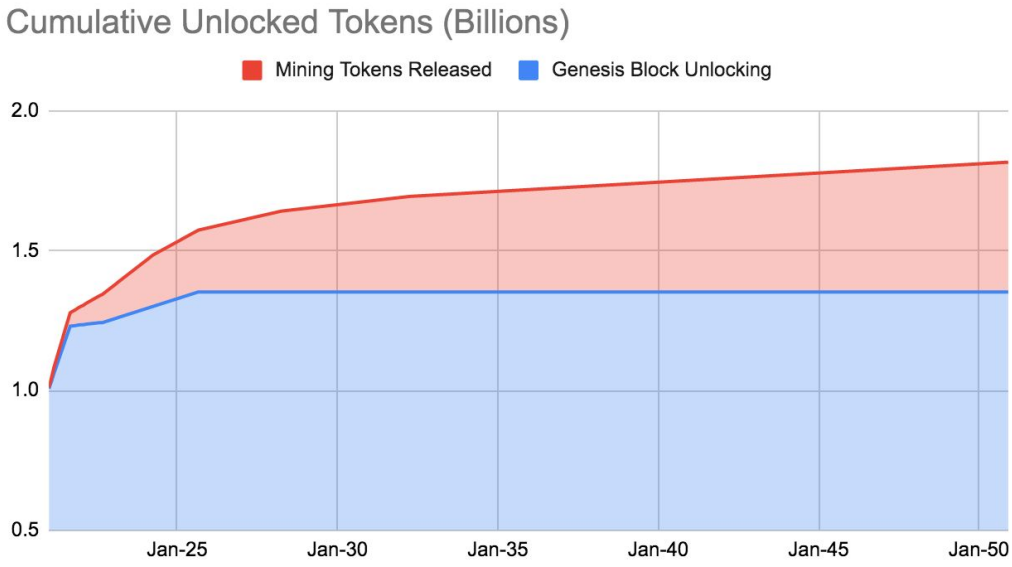
[BTC는 STX 블록의 가치에 비례하여 입찰]

토큰 이코노미

스택스 암호화폐는 제네시스 블록을 통해 13억 2천만 STX가 발행되었습니다 [14]. 해당 STX는 2017년과 2019년에 다양한 오퍼링을 통해 배포되었습니다. 2017년 오퍼링은 $0.12, 2019년 Reg S 오퍼링은 $0.25, 2019년 SEC 승인 오퍼링은 $0.30에 STX가 분배되었습니다. 아래 그림 1은 제네시스 블록 토큰에 대한 분석을 보여주고 있습니다.



스택스 암호화폐의 2050년 미래 공급량은 약 18억 1800만 STX입니다. (이전 20억 4000만 보다 감소한 수치 [14]). 2021년 1월 말까지 제네시스 블록의 13억 2천만 STX 중 약 10억 6백만 개가 유동되었으며 나머지는 다양한 락업 조건에 따라 매월 락업이 해제됩니다. 예를 들어, 창립자와 직원에게 할당된 STX는 3년 락업 해제 후 2021년 1월과 2021년 11월 사이에 락업 해제될 예정입니다. 그림 2는 2050년까지의 총 유통량 증가를 보여주고 있습니다. 자세한 내용은 [7]를 통해 확인 가능합니다.



스택스 생태계

스택스 생태계는 비트코인으로부터 사용자 소유 인터넷을 구축하기 위해 노력 중인 독립 엔티티, 개발자 및 커뮤니티로 이뤄져 있습니다.

프로젝트 역사:

본 프로젝트는 더 나은 인터넷을 구축하기 위해 2013년 프린스턴 대학 컴퓨터 과학부로부터 시작되었습니다. 무니브 알리(Muneeb Ali)와 라이언 시어(Ryan Shea)는 2014년 Y Combinator를 통해 초기 R&D를 위한 프린스턴 컴퓨터 과학자들을 모집했습니다. 이를 위한 초기 투자자로 Union Square Ventures, Naval Ravikant, SV Angel 등이 있습니다. 무니브의 2017년 박사 논문은 블록체인에 구축된 사용자 소유 인터넷을 위한 기술적 토대가 되었습니다 [8].

2017년 스택스 암호화폐에 대한 토큰 오퍼링을 통해 $47M을 모금했으며, SEC로부터 승인받은 최초의 US Reg A 오퍼링과 2019년 Reg S 오퍼링을 통해 추가적인 $23M를 모금 받았습니다. 4,500명 이상의 스택스 보유자들이 오퍼링에 참여하였으며, USV, Lux, DCG, Winklevoss Capital, Blockchain Capital, Foundation Capital, Hashkey, Fenbushi 등 여러 VC가 참여하였습니다.

탈중앙 생태계:

공익 단체 Blockstack PBC는 2017년 시리즈 A를 받은 이후 초기 R&D, 프로토콜 설계 및 공용 인프라를 위한 작업을 진행하였습니다. 공용 인프라 구축 단계는 2020년 말 완료되었으며, 스택스 2.0 론칭 이후 Blockstack PBC는 개발자 도구 개발에 전념하기 위해 Hiro Systems로 브랜드를 변경합니다.

2020년 탈중앙화 과정에 따라 스택스 생태계에 여러 독립 엔티티가 탄생하였습니다. 비영리 목적의 Stacks Foundation, 커뮤니티 중심의 독립체 Freehold, 채굴 및 아시아 시장에 초점을 둔 기업 Daemon Technologies, 독립 사용자 클라이언트를 위한 New Internet Labs와 Secret Key Labs가 있습니다. 스택스 생태계에는 독립 개발자 및 엔티티로부터 개발된 400 개 이상의 앱이 존재합니다.

2020년 가을, Blockstack PBC는 스택스(STX) 암호화폐가 미국에서 비-증권형 토큰으로 전환될 것이라는 자세한 내용이 담긴 법률 의견서 요약본을 발표했습니다 [9].

Hiro

Stacks Foundation

地灵科技 DAEMON TECHNOLOGIES

FREEHOLD

New Internet Labs

스택스 **2.0** 메인넷 출시

현재 2021년 1월 14일로 예상되는 스택스 2.0 출시는 스택스 1.0 업그레이드와는 달리 완전히 새로운 프로젝트를 출시하는 것과 같습니다. 스택스 2.0은 우리의 마스터 디자인으로, 비트코인 (a) 트랜잭션의 확장성 문제를 해결하고 (b) 비트코인 블록체인 자체를 수정하지 않고 스마트 컨트랙트 기능을 활성화시켜 줍니다.

채굴 시작:

스택스 2.0 메인넷이 출시되기 위해서는 최소 20명의 독립 채굴자로부터 채택되어야 합니다. 채굴자는 .miner 네임 스페이스에 등록하고 다음 단계를 따라야 합니다 [10]. 채굴이 시작되면 블록당 1000 STX가 새롭게 발행됩니다 (STX 채굴자들이 새로운 STX 블록을 패키징하고 기록하는 인센티브로). 채굴의 시작은 생태계에서 온라인으로 제공되는 소규모의 새로운 탈중앙 거래소라 생각할 수 있습니다. 하루에 대략 150K STX가 BTC/STX 온체인 페어에서 채굴을 통해 “거래"됩니다. 다른 블록체인과 마찬가지로 채굴자는 수익성이 있는 경우에만 새로운 블록을 채굴합니다. 이는 채굴자가 BTC/STX 채굴 페어 거래를 통해 BTC/STX 페어를 지원하는 타 거래소(예를 들어 바이낸스 거래소)보다 더 저렴하게 획득할 수 있음을 의미합니다. 바이낸스와 같은 거래소가 현재 수백만 STX 거래량을 처리하고 있다는 점을 감안했을 때 채굴 거래 페어의 “거래량"은 일반 거래소에 비해 상대적으로 작을 것으로 예상됩니다 (마이닝 페어의 150K STX 상한과 비교).

비트코인 수익:

스택스 2.0 메인넷 출시와 함께 STX 유동 공급량의 일부가 합의에 적극적으로 참여하기 위해 락업될 수 있습니다. 유동 공급량의 50%가 다른 매개 변수와 함께 BTC 보상 획득에 참여하게 되면 BTC 수익은 약 9%가 될 수 있습니다 [5].

합의에 참여하는데 필요한 최소 STX 수는 계속해서 바뀌며 적극적으로 참여하는 유동 공급량 비율에 따라 달라지게 됩니다. 유동 공급량의 50%가 참여하고 950M이 유동 공급량인 경우 스택킹에 참여하기 위해서 최소 120,000 STX가 필요합니다. 그러나 STX 보유자는 풀링 서비스를 사용할 수 있으며 서비스 제공자에 대한 위임은 네트워크에서 지원됩니다.

클래러티 컨트랙트:

클래러티 스마트 컨트랙트를 퍼블리싱하고 실행할 수 있는 기능은 스택스 2.0 메인넷 출시와 함께 활성화됩니다. 모든 거래 수수료와 클래러티 컨트랙트 가스 수수료는 채굴자에게 STX로 지급됩니다.

업그레이드 가이드:

스택스 2.0 메인넷 출시는 스택스 1.0의 하드포크로부터 시작되며 모든 STX 잔액과 디지털 자산의 소유권은 스택스 2.0으로 자동 이전됩니다. 스택스 1.0과 스택스 2.0 간 별도의 토큰 스왑은 필요로 하지 않습니다. STX 보유자는 스택스 2.0 지갑 [11]으로 업그레이드해야 하며 거래소 및 기타 노드 운영자는 통합 가이드 [12]를 따르면 됩니다.

요약 및 향후 작업

스택스 2.0은 앱과 스마트 컨트랙트를 비트코인에 제공합니다. 우리의 논문은 다양한 블록체인의 성공적인 실험이 결국 비트코인으로부터 생겨날 것이라는 것입니다. 비트코인의 네트워크 효과는 비트코인 주변의 스마트 컨트랙트가 더 많은 암호화폐 자본에 액세스하고 더 높은 보안 혜택을 받을 수 있음을 의미합니다. 우리는 비트코인이 기존 인터넷의 TCP/IP와 같이 더 나은 사용자 소유 인터넷을 위한 기반이 될 것이라 믿습니다.

스택스 2.0은 사용자가 합의에 적극적으로 참여하여 비트코인을 획득할 수 있는 새로운 방법을 제공합니다. 우리는 수동적인 비트코인 자본을 보다 동적인 자본으로 전환시키고 비트코인 생태계에 더 많은 앱과 스마트 컨트랙트를 가져와 비트코인의 가치를 더 높이고자 합니다.

스택스 2.0 출시 이후 블록 공간에 대한 경매, 더 많은 처리량 및 마이크로블록의 속도, 고급 클래러티 언어 기능 [13] 등 Stacks Foundation과 여러 커뮤니티를 통해 함께 개선할 예정입니다.

참조:

[1] S. Nakamoto. “Bitcoin: A Peer-to-Peer Electronic Cash System”, Oct 2008. https://bitcoin.org/bitcoin.pdf

[2] M. Ali, R. Shea, J. Nelson and M. J. Freedman, “Blockstack: A New Internet for Decentralized Applications”, Whitepaper Version 1.1, Oct 2017.

[3] Stacks GitHub repository. https://github.com/blockstack/

[4] M. Ali, A. Blankstein, M. J. Freedman, L. Galabru, D. Gupta, J. Nelson, J. Soslow, P. Stanley, “PoX: Proof of Transfer Mining with Bitcoin”, Whitepaper v1.0 May 2020. https://blockstack.org/pox.pdf

[5] M. Ali, “Stacking Earnings Model: Projecting Consensus Participation Rewards for STX Holders”, Oct 2020. https://blog.blockstack.org/stacking-earnings-model/

[6] Blockstack Token LLC, SEC Offering Circular, May 2019. https://www.sec.gov/Archives/edgar/data/1719379/000110465919029828/a18-15736_1partiiandiii.htm

[7] STX future supply spreadsheet. https://github.com/zone117x/stx-supply-schedule/

[8] M. Ali, “Trust-to-Trust Design of a New Internet”, PhD dissertation, Princeton University, June 2017. https://muneebali.com/thesis

[9] M. Ali, “Stacks Cryptocurrency Expected To Reach Non-Security Status in the United States”, Dec 2020. https://blog.blockstack.org/stacks-cryptocurrency-expected-to-reach-non-security-status-in-the-united-states/

[10] D. Gupta, “[RFC] Stacks 1.0 → 2.0 Upgrade Process”, Nov 2020. https://forum.stacks.org/t/rfc-stacks-1-0-2-0-upgrade-process/11346

[11] Stacks 2.0 wallet. https://wallet.blockstack.org

[12] Stacks 2.0 Integration Guide, https://docs.blockstack.org/stacks-blockchain/overview

[13] J. Nelson, “After Stacks 2.0: Potential Features for Stacks 2.1”, Nov 2020. https://forum.stacks.org/t/after-stacks-2-0-potential-features-for-stacks-2-1/11376

[14] M. Ali, "Stacks Token Economics and Incentive Mechanisms", Whitepaper Ver 2.0.7, Oct 2019.

[15] V. Buterin, “A next-generation smart contract and decentralized application platform,” Ethereum whitepaper 2013. https://ethereum.org/en/whitepaper/.