서싱트(Succinct)

본 주요내용설명서는 가상자산의 발행주체 또는 운영주체가 작성한 가상자산 관련 중요사항을 설명하는 자료 참분석 주요 내용 및 가상자산 관련 중요사항에 대한 최신 변경내용을 기재한 한글 파일이며, 본 설명서가 법률도 되는 사항에 대해 내용이 차이가 있을 수 있습니다. 보다 자세한 사항은 원문을 참고해 주시기 바랍니다.

(원문 링크)

개요

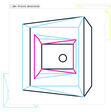
탈중앙 시스템인 블록체인은 분산 합의를 기반으로 하며, 모든 참가자가 트랜잭션을 공유하고 확인하여 정합성을 검증한다. 이는 무신뢰성(trustless) 실행을 장려하지만, 큰 비용을 초래한다. 따라서 일각에서는 오늘날의 블록체인이 느리고, 비싸며, 주류 수요를 감당하지 못하는 상태라고 평가하며, 이러한 블록체인의 특성은 상업적 사용 가능성을 제한하고, 중앙집중형 대안보다 훨씬 비효율적이게 만든다고 주장한다.

서싱트(Succinct)는 이러한 문제를 영지식(Zero Knowledge, ZK) 증명을 통하여 해결할 수 있는 답을 제시한다. ZK 증명은 진술일 진짜가 아닌, 짧은 증명만으로도 검증자가 정확성을 확인할 수 있게 해준다. 트랜잭션 실행과 검증을 분리함으로써, ZK 증명은 소수의 참가자가 무거운 연산을 처리하고 다수는 저렴하게 검증할 수 있는 확장 가능한 블록체인을 가능하게 한다. 이를 통해 L2, 브릿지, 라이트 클라이언트, 오라클, AI 에이전트 등에서 신뢰 없는 온체인 검증을 유지하면서 오프체인 계산을 수행할 수 있게 한다.

다만, 이러한 기술의 영지식 증명(Zero Knowledge) 기반 증명 작업은 인감한 정보 보호 등 정보 교류 관련된 이슈나 보안에 있어서 장점을 보유하는 대해 반해, 개발에 있어서 복잡하고 느리고 비용이 많이 든다는 단점이 존재한다. 서싱트는 이러한 영지식 증명 기술의 단점을 보안하기 위해 증명자와 증명 요청자간 하한 플레이스를 형성하고 증명 작업을 빠르고 효율적이게 할 수 있는 인프라를 구축하였다.

이러한 서싱트의 서비스를 포괄하는 서싱트 프루버 네트워크(Succinct Prover Network)는 빠른 증명 생성 속도, 개발의 편의성, 비용 경쟁성을 제공하기 위해 노력 중이며 이를 통해 '언 서싱트 프루버(증명한다)'(prove the world's software)는 시장을 우뚝 소개 중이다.

PROVE는 서싱트의 유틸리티 토큰으로 요청자 요청수수료 지불, 디깅 스테이킹, 거버넌스 등의 용도로 사용될 예정이다.



출처: 서싱트 웹사이트

기술 및 특징

서싱트 – 탈중앙화 증명 네트워크

서싱트는 이더리움(Ethereum)에 존재하는 프로토콜로, 전 세계적 소프트웨어에 대한 증명을 생성하는 것을 목표로 한다. 해결과제에선 개발자는 러스트(Rust) 언어로 작성된 프로그램을 SP1이라고 불리우는 영지식 가상 머신(zkVM)로로 래핑(wrap)한 후 서싱트 네트워크 전송하면, 서싱트는 이를 바탕으로 프루버(Prover)라고 불리우는 인프라 레이어 및 하드웨어 일부에 해당 애플리케이션 프로그램 실행에 대한 증명 생성을 요청한다.

이러한 서싱트 프로토콜에는 크게 두 주요 참여자가 포함한다.

1. 요청자(Requesters) :
   영지식 증명이 필요한 애플리케이션을 의미하며 증명 요청을 네트워크에 제출하는 주체를 뜻한다. 이러한 요청자의 예시로는 ZK 롤업(Rollup), 브릿지(Bridge), AI 에이전트, 개발 등이 포함한다. 요청이 이루어질 때 일반적으로 증명할 연산을 정의한 프로그램, 요청자가 지불할 의향이 있는 최대 PROVE 수수료, 결제 장치 역할을 한 최소 PROVE 스테이킹 수량 등이 포함된다.
2. 프루버 :
   증명 요청에 응답하여 증명자과 증명을 생성하는 참여자를 뜻한다. 프루버들은 PROVE 토큰을 스테이킹하여 입찰 자격을 획득하고, 가장 낮은 가격을 제시하여 다른 프루버들과 경쟁한다. 낙찰을 받은 프루버는 하급 기한 내에 증명을 제출해야 하며, 실패할 경우 일부 스테이킹 된 PROVE 토큰이 슬래싱 된다.

또, 서싱트는 두 네트워크 구성 요소를 기반으로 작동한다.

1. 오프체인 자사(Auctioneer) 서비스 :
   자사는 오프체인 상에서 요청자와 프루버를 연결해주는 핵심 서비스로, 경쟁 요청과 경쟁 제출, 입찰 처리, 증명 수령, 보상 수령을 모두 처리하는 서비스이다. RPC 호출을 통해 온체인 컨트랙트와 직접 상호작용하기에 사용자는 실시간으로 요청을 시스템 경험을 할 수 있다.
2. 온체인 세틀먼트 컨트랙트(Settlement Contracts) :
   세틀먼트 컨트랙트는 자사나 주기적으로 제출하는 상태 루트 및 증명을 전산하는 역할을 하는 온체인 컨트넌트로, 요청 하소 이벤트 등의 상태 변경 내용을 확인하고 기록하며, 사용자들이 이더리움 상에 자금 인출 및 PROVE 스테이킹 등의 활동을 할 수 있도록 지원한다. 오프체인 구성 요소인 자사는 사용자와 자금을 보관하지 않으며, 모든 자금은 세틀먼트 컨트랙트를 통하여 이더리움에 존재한다.

이렇게 서싱트 네트워크는 하지 레이어 2에 같이 오프체인 컴포넌트가 경매 및 증명 할당 등의 과정을 처리하며 레이어 2에서의 시퀀서와 같은 역할을 수행하고, 온체인 스마트 컨트랙트가 이더리움 상에서 상태 루트 및 올바른 실행의 증명을 기록하고 검증(verify)하는 역할을 수행한다. 이러한 구조는 기존 개인의 자리만 복잡한 회계면서 단일 통합 버로 한 증명을 제공하며, 사용자는 블록 지연 없이 실시간으로 네트워크를 사용할 수 있도록 지원한다.

출처: 서싱트 독스

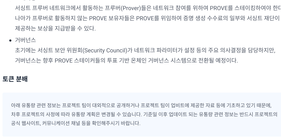
서싱트의 시장 구조

서싱트의 프루버 네트워크 시장에서 수요와 공급 네트워크가 형성되지 않는다면 증명 시장은 애플리케이션과 프루버 간의 개별 계약 혹은 애플리케이션 내부 증명 인프라를 직접 구축하는 방식으로 흘러갈 가능성이 높다. 그러나 이러한 방식은 모두가 전문 기술 및 운영 역량을 갖추어 하는 비효율이나 낮은 가격을 통한 시장 내 변동을 초래할 수 있다는 단점이 존재한다.

따라서 서싱트는 사용자, 하드웨어 팀, 인프라 운영자 간의 생태계를 성공경제적 인센티브로 조율하며, 전문화된 참여자들이 가장 효율적인 증명 인프라를 제공하기 위해 경쟁할 수 있는 시장 구조를 형성한다.

또, 서싱트 네트워크는 무허가 하청을 보유하여 효율적인 가격 책정을 가능하게 한다. 전 세계 어디에서나 프루버가 네트워크에 참여할 수 있기 때문에, 경쟁적인 데이터센터는 훨씬 가장등 GPU와 하드웨어를 보유한 개인도 가격 경쟁에 참여할 수 있다. 가장등 프루버는 유휴 자원 활용 및 저렴한 전기 요금 덕분에 운영 비용이 낮고 초기 투자 비용도 적다는 장점이 존재하고, 추후 자속적으로 ZK 증명을 위한 가속 하드웨어(FPGA, ASIC 등)의 등장하여 사용자 측 가격은 더욱 낮아질 것으로 예상된다.

이렇게 서싱트의 무허가 참여(Permissionless Participation)는 궁극적 규모의 인프라 구축을 촉진하며, 모든 애플리케이션에 대해 영지식 증명 생성 비용과 지연 시간을 낮추는 결과를 이끈다.



출처: 서싱트 독스

SP1

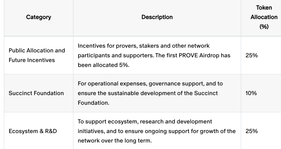
영지식 증명 기술은 지금까지 기술의 복잡성으로 인하여 제약하여 활용되기 어려운 기술이었다. 개발자들은 특수한 개발 언어를 습득하고, 커스텀 서킷을 설계하여 하며, 복잡한 암호학을 잘 이해해야 하였고, 이로 인하여 영지식은 전문가들이나 특정 목적의 분야에서만 활용되었다.

SP1은 RISC-V 아키텍처용으로 컴파일 된 프로그램의 올바른 실행을 증명하는 영지식 가상 머신(zkVM)이다. RISC V는 공개 표준으로 소스코드 공개된 32비트의 명령어 집합 구조로 RISC V 표준으로 설계된 프로그램이면, 해당 명령어 집합 구조를 따르는 CPU에서 실행 가능하도록 변환된 코드를 뜻한다. 즉, SP1에서는 Rust, C++, C 등 RISC-V로 컴파일 가능한 모든 언어로 작성된 프로그램을 실행하고 증명할 수 있다. 이렇게 컴파일 된 프로그램에 있어 영지식 증명을 생성하는 작업을 영지식 가상머신이 수행한다.

이런 프로그램이 함수 f(x)를 계산하여 결과값 y를 만들었다는 사실을 증명하여 실제 계산 과정을 공개하지 않도록 하는 zkVM의 동작 과정은 다음과 같다.

1. 함수 f 정의
2. 해당 프로그램에 대해 ELF 파일 기반으로 프루빙 키(Proving Key, pk)와 베리파잉 키(Verifying Key, vk)를 생성
3. prove(pk, x)를 사용하여 f(x) = y임을 나타내는 증명 π 생성
4. verify(vk, x, y, π)를 통하여 증명의 유효성 검증

이렇게 SP1은 영지식이 보유한 장벽을 하향고 개발자들이 쉽게 증명 가능한 프로그램을 만들 수 있도록 지원한다. SP1을 사용하려면 개발자는 익숙한 언어(Rust 등)로 증명 가능한 프로그램 개발이 가능하고, 복잡한 서킷 설계나 암호학 지식 없이 단순한 로직 작성으로 증명을 생성할 수 있다.



출처: 서싱트 독스

토큰 이코노미

토큰 유틸리티

PROVE는 서비스 이용 비용 지불 수단, 거버넌스 참여 및 스테이킹 수단으로 사용된다.

- 지불 수단
  PROVE는 서싱트 프루버 네트워크(Succinct Prover Network)에서 ZK 애플리케이션들이 증명 생성을 위해 지불하는 수단으로 사용된다.
- 스테이킹
  서싱트 프루버 네트워크에서 활동하는 프루버(Prover)들은 네트워크 참여를 위하여 PROVE를 스테이킹하여야 한다. 나아가 프루버로 활동하지 않는 PROVE 보유자들은 PROVE를 위임하여 증명 생성 수수료의 일부와 서싱트 재단이 제공하는 보상을 지급받을 수 있다.
- 거버넌스
  초기에는 서싱트 보안 위원회(Security Council)가 네트워크 파라미터가 설정 등의 주요 의사결정을 담당하지만, 거버넌스는 향후 PROVE 스테이킹을 통 투표 기반 온체인 거버넌스 시스템으로 전환될 예정이다.

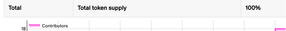
토큰 분배

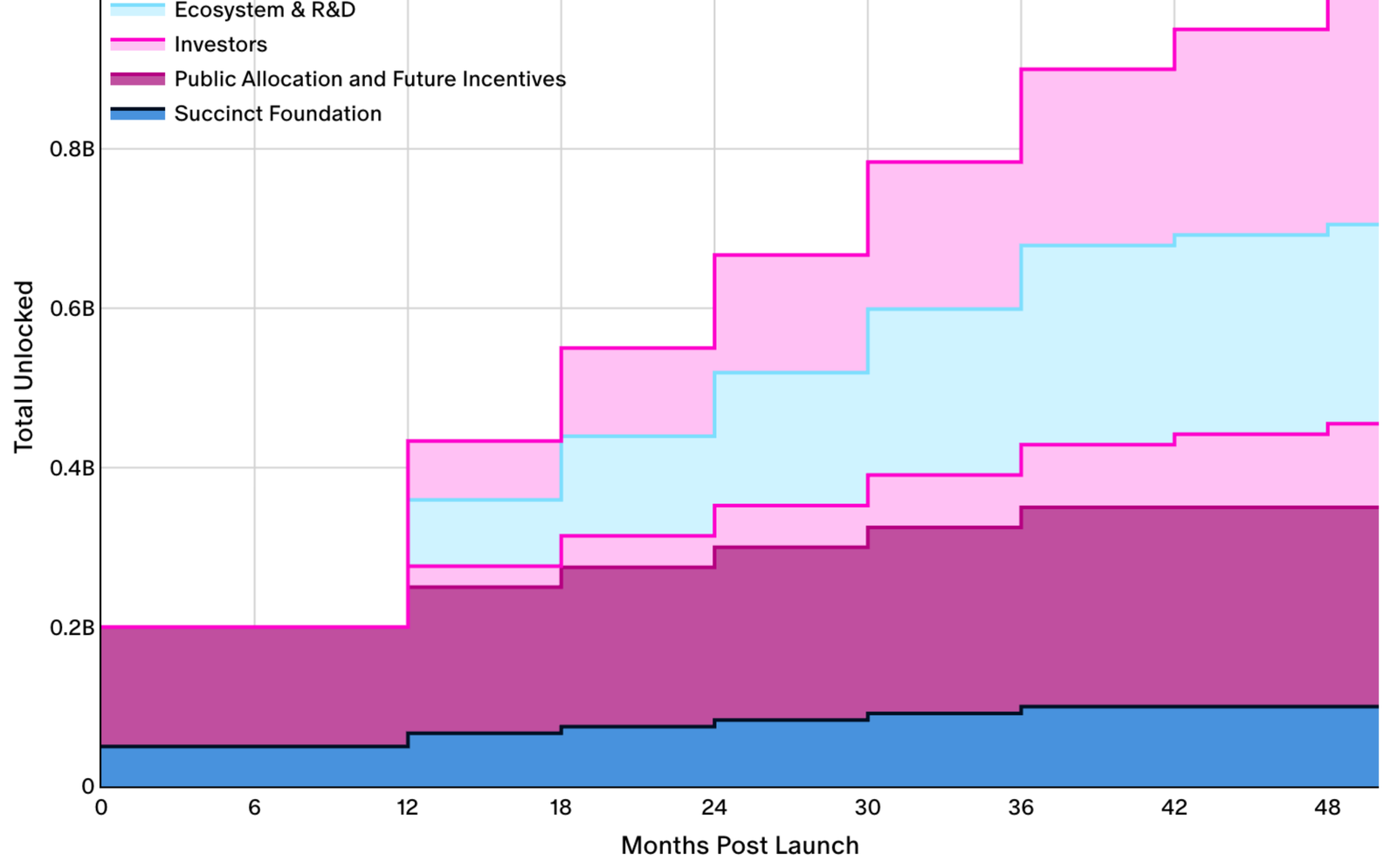
아래 유통량 관련 정보는 프로젝트 팀이 대략적으로 공개하거나 프로젝트 팀이 입증되게 제공한 자료 등에 기초하고 있기 때문에, 자료 프로젝트의 사정에 따라 유통량 예측은 변경될 수 있습니다. 기준일 이후 업데이트 되는 유통량 관련 정보는 반드시 프로젝트의 공식 웹사이트, 커뮤니케이션 채널 등을 확인해주시기 바랍니다.

PROVE의 총 발행량은 10억 개이다. PROVE의 초기 물량은 다음과 같이 분배되었다.

- 주요 기여자(29.5%)
- 생태계와 R&D(25%)
- 미래 인센티브 및 대응 배분(25%)
- 투자자(10.5%)
- 재단(10%)

Category	Description	Token Allocation (%)
Public Allocation and Future Incentives	Incentives for provers, stakers and other network participants and supporters. The first PROVE Airdrop has been allocated 5%.	25%
Succinct Foundation	For operational expenses, governance support, and to ensure the sustainable development of the Succinct Foundation.	10%
Ecosystem & R&D	To support ecosystem, research and development initiatives, and to ensure ongoing support for growth of the network over the long term.	25%
Investors	Seed and Series A investors	10.5%
Contributors	Core contributors to the Succinct Network, including members of the Succinct Labs team, and future core contributors.	29.5%
Total	**Total token supply**	**100%**





출처: 서싱트 독스

참고문헌

- 서싱트 웹사이트
- 서싱트 독스
- 서싱트 블로그

2025.08.06 13:55 업데이트

- 본 자료는 두나무(이하 당사)가 거래지원한 가상자산과 관련하여 작성한 것으로 이용자에게 투자를 권장하거나 유도할 목적이 없으며, 이용자의 투자 판단에 참고가 되는 정보 제공을 목적으로 작성되었습니다.
- 본 자료는 제3자로부터 제공받거나 제3자가 작성한 원문을 참고하여 작성 당시의 당사의 신뢰할 수 있는 내용 및 정보를 바탕으로 작성되었으나, 오차가 있을 수 있고 상이한 정보가 포함되어 있을 수 있습니다. 이에 당사는 어떠한 경우에도 정보의 정확성이나 완전성을 보장하지 않으며, 필요한 경우 이용자는 발행인이 직접 작성·공개한 정보를 통해 사실 여부를 확인하여야 합니다.
- 당사는 본 자료가 공개 되기 이전 제3자에게 사전 제공한 사실이 없습니다. 본 자료의 발행인을 포함하여 그 누구도 본 가상자산의 가치 또는 지급을 보증하지 않습니다. 본 가상자산은 시장 상황, 기술적 변화, 규제 동향 등에 따라 가치가 크게 변동할 수 있으며, 가상자산 투자는 원본 손실이 발생할 수 있습니다.
- 당사는 본 자료와 관련한 이용자의 투자 결과 일체에 대하여 어떠한 책임도 지지 않습니다.
- 본 자료는 어떠한 경우에도 이용자의 투자 결과에 대한 법적 책임 소재의 증빙자료로 사용될 수 없습니다. 본 자료의 저작권은 당사에 있고, 국내 코인 마켓거래소가 본 자료의 출처를 정확하게 명기하여 사용하는 경우 외에는 어떤 형태로든 당사의 동의 없이 복제, 변형, 재배포 될 수 없습니다.

UPbit Copyright © 2017 - 2024 Dunamu Inc. All rights reserved.