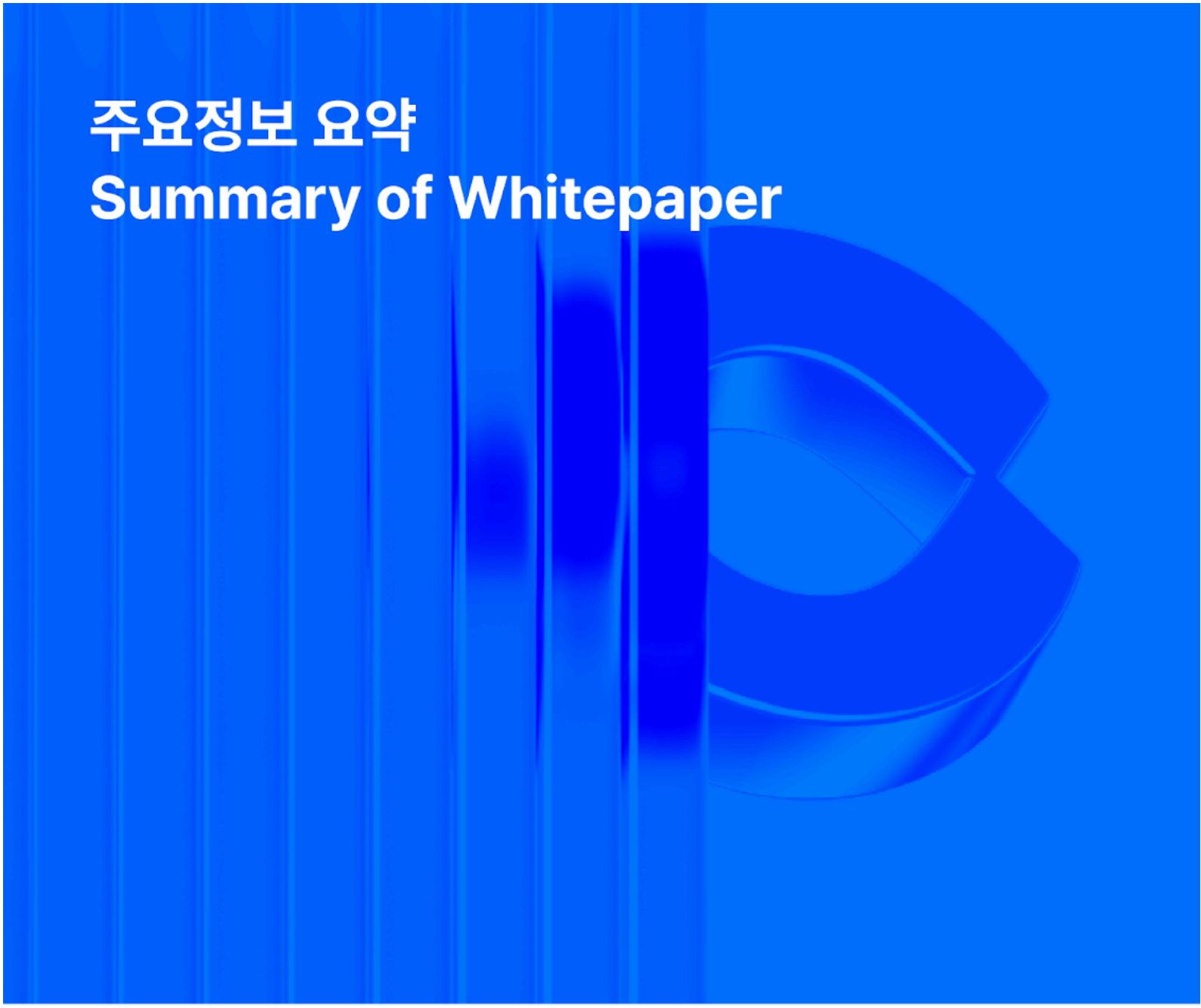
주요정보 요약
Summary of Whitepaper



본 문서는 거래지원 가상자산 백서의 주요 내용을 한글로 설명한 주요정보 요약입니다.
코인원은 거래지원 가상자산의 주요정보 요약을 주기적으로 점검하여 가능한 한 최신 정보를 제공할 예정입니다.

coinone

기본 정보

가상자산 카테고리	유틸리티
거래지원 네트워크	Ethereum
홈페이지	https://www.succinct.xyz/
참고문헌 (백서, Docs 등)	https://docs.succinct.xyz/
	https://docs.succinct.foundation/

1. 프로젝트 정보

Succinct Prover Network란?

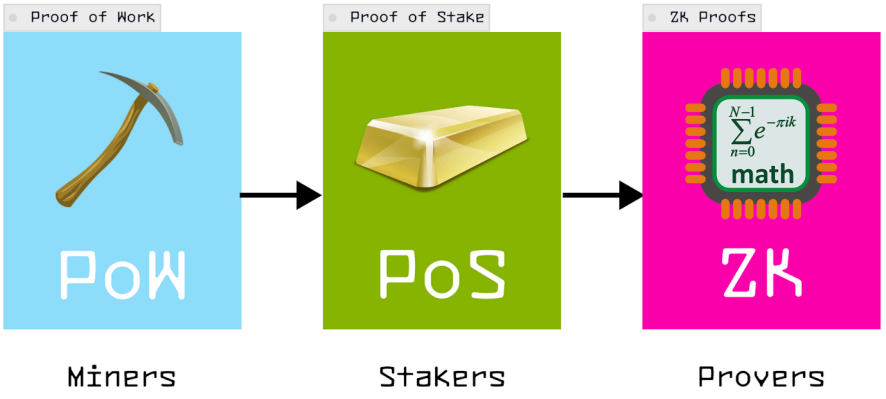
Succinct Prover Network는 이더리움 위에 구축된 프로토콜로, 전 세계 모든 소프트웨어에 대한 영지식 증명을 생성하기 위해 분산된 증명자 네트워크를 조율합니다. 이 프로토콜은 증명자와 요청자 간의 양면 시장을 형성하여, 블록체인, 브리지, 오라클, AI 에이전트, 비디오 게임 등 다양한 애플리케이션에 대한 증명을 누구나 생성할 수 있도록 합니다.

이전에는 개발자가 증명을 생성하기 위해 맞춤형 회로를 설계하고 복잡한 암호학 지식을 갖춰야 했습니다. 그러나 Succinct를 사용하면 일반적인 소프트웨어처럼 프로그램을 작성하고 영지식 증명을 자동으로 생성할 수 있습니다.

이러한 접근 방식은 흔히 “ZK 2.0”이라고 불리며, 이를 가능하게 하는 것은 SP1이라는 영지식 가상 머신입니다. SP1은 증명 생성의 복잡성을 추상화하여, 더 나은 개발자 경험을 제공하고, 전통적인 컴퓨팅처럼 프로그래밍 가능하게 만듭니다.

이로써 최초의 범용 증명 네트워크가 구축되었으며, 모든 사용 사례에 단일 네트워크로 증명 생성을 제공합니다. Succinct Prover Network는 경매 기반 시장을 통해 가장 효율적인 증명자를 선택하여, 애플리케이션이 증명 생성을 위해 가장 저렴한 옵션을 사용할 수 있게 합니다.

Succinct가 ZK를 세상에 소개하는 방법



Succinct는 블록체인 모델에서 채굴자와 스테이커를 넘어 세 번째 행위자인 증명자(prover)를 도입합니다. 작업 증명(PoW)에서의 채굴이나 지분 증명(PoS)에서의 스테이킹처럼, 증명 또한 개방적이고 허가가 필요 없는 과정입니다. 누구나 증명자를 실행하고 연산 자원을 네트워크에 기여함으로써 참여할 수 있습니다.

과거에는 증명 시스템이 ASIC과 유사하게 매우 특화되어 있어 분산 네트워크에서

증명자를 조율하는 것이 어려웠습니다. 기존 영지식 증명 시스템은 좁은 사용 사례에 맞춰 최적화된 맞춤형 회로와 전문 지식을 필요로 했기 때문에, 단일한 증명 네트워크의 구축이 불가능했습니다. 이를 근본적으로 변화시킨 것이 범용 영지식 가상 머신인 SP1입니다. SP1은 실행 가능한 연산을 증명까지 할 수 있는 CPU처럼 작동합니다. 일반 CPU가 모든 프로그램을 실행하듯, SP1은 표준 코드로부터 직접 영지식 증명을 생성할 수 있도록 하며, 이 과정에서 맞춤 회로나 암호학 전문 지식은 필요하지 않습니다.

이러한 구조에서 Succinct Network는 일종의 실행 레이어처럼 작동합니다. 스마트 컨트랙트를 완전한 프로그래머블 환경에 배포하고 실행할 수 있으며, 이는 전통적인 L1 블록체인과 유사합니다. 그러나 전통적인 블록체인 가상 머신은 모든 노드가 거래를 중복 실행하는 반면, Succinct Network는 경쟁 과정을 통해 소수의 증명자를 선별하여 실행 증명(cryptographic proof of execution)을 생성합니다. 증명자는 효율성과 비용을 기준으로 경쟁하며, 최적화된 연산과 탈중앙성을 동시에 유지할 수 있도록 설계되어 있습니다.

Succinct 프로토콜은 다음과 같은 순서로 작동합니다.

- 개발자는 Rust, C++ 등의 일반적인 프로그래밍 언어로 소프트웨어를 작성하고 이를 증명자 네트워크에 프로그램 형태로 배포합니다.
- 사용자는 해당 프로그램의 실행에 대한 증명 생성을 요청하는 트랜잭션을 제출합니다.
- 증명자들은 주어진 요청에 대해 증명 생성을 경쟁하며, 가장 효율적으로 증명을 생성한 증명자가 보상을 획득합니다.

Succinct 란?

Succinct: 세계 최초의 탈중앙화 증명자 네트워크
탈중앙화된 영지식 증명 프로토콜이라는 개념은 여러 측면에서 혁신적입니다.

첫째, 증명 생성은 매우 높은 연산 성능을 요구하는 작업입니다. 현재 단일 ZK 롤업의 증명을 생성하기 위해서도 수백 개의 GPU 클러스터를 조율해야 합니다. 따라서 전 세계 모든 애플리케이션을 증명하는 일은 단일 팀의 능력으로는 불가능하며, 이를 위해서는 전 세계의 컴퓨팅 자원(데이터센터 포함)을 통합해야 합니다.

둘째, 증명 생성은 마치 비트코인 채굴이나 AI 모델 훈련처럼, 고성능 하드웨어의 발전에 따른 성능 향상의 영향을 받습니다. 이와 같은 컴퓨팅 인프라의 확장을 조율하고 보상하는 탈중앙 프로토콜이야말로 영지식 증명의 확장성 확보를 위한 핵심입니다.

셋째, 영지식 증명은 자동 검증이 가능하다는 특성을 가집니다. AI 모델 학습과 같이 데이터센터 내부에서 이루어지는 작업을 외부 사용자가 직접 검증할 수 없는 구조와 달리, 영지식 증명은 제3자가 자동으로 검증할 수 있어 탈중앙 참여에 적합합니다.

Succinct Network가 등장하기 전까지는 수요와 공급의 단절로 인해 ZK 증명 확장이 병목에 걸려 있었습니다. Succinct는 처음으로 전 세계 소프트웨어에 대한 증명이 가능한 기반을 제공합니다.

Succinct Network의 핵심 기능
Succinct Network는 전 세계적인 양면 시장 구조를 형성하여, 증명자와 요청자가 서로 연결되는 장을 제공합니다. 증명자는 요청자가 제출한 프로그램에 대해 영지식 증명을 생성하며 경쟁합니다. 이 네트워크는 이더리움에 정산(settlement)되는 프로토콜로 구축되어 있으며, 다음과 같은 주요 특징을 갖습니다.

허가 없는 참여

누구나 증명자로 네트워크에 참여할 수 있고, 누구나 수수료를 예치함으로써 증명 요청을 제출할 수 있습니다. 이러한 개방성은 전 세계적인 경쟁을 촉진하고 보안성을 강화하며, 특정 주체가 증명 생성을 독점하지 못하게 합니다. 모든 애플리케이션이 영지식 증명을 활용할 수 있도록 보장합니다.

고성능 및 검증 가능한 아키텍처
이 네트워크는 이더리움에 정산되는 검증 가능한 애플리케이션(vApp) 구조로 설계되어 있습니다. 사용자는 고성능 웹 애플리케이션처럼 네트워크와 상호작용할 수 있으며, 누구든지 해당 애플리케이션의 상태를 독립적으로 검증할 수 있습니다. 이는 L2 시퀀서와 온체인 정산 간의 분리 구조와 유사합니다. 전체 아키텍처는 두 가지로 구성됩니다.

- 오프체인 경매자 서비스
  L2 시퀀서와 유사한 역할을 하는 경매자 서비스는 요청자와 증명자 간의 핵심 조율을 담당합니다. 증명 요청을 수집하고, 경매를 운영하며, 증명을 제공받는 과정을 처리합니다. 이 서비스는 블록체인의 처리 한계 없이 낮은 지연 시간으로 가장 경쟁력 있는 증명자를 매칭합니다.

- 온체인 정산 컨트랙트
  이더리움 상의 스마트 컨트랙트은 경매자가 게시한 상태 루트 및 증명 결과를 정산합니다. 이를 통해 사용자는 네트워크의 상태를 독립적으로 확인하고, 예치금을 안전하게 관리할 수 있으며, 경매자가 오프라인이 되어도 자금을 출금할 수 있습니다.

PROVE 토큰
PROVE는 Succinct Network의 고유 토큰으로, 결제 수단 역할을 하며 증명자의 경쟁을 유도하고, 네트워크를 스테이킹 및 거버넌스로 보호합니다. 이 토큰은 증명자 인센티브를 사용자의 비용 절감 방향과 정렬시키기 위해 설계되었습니다.

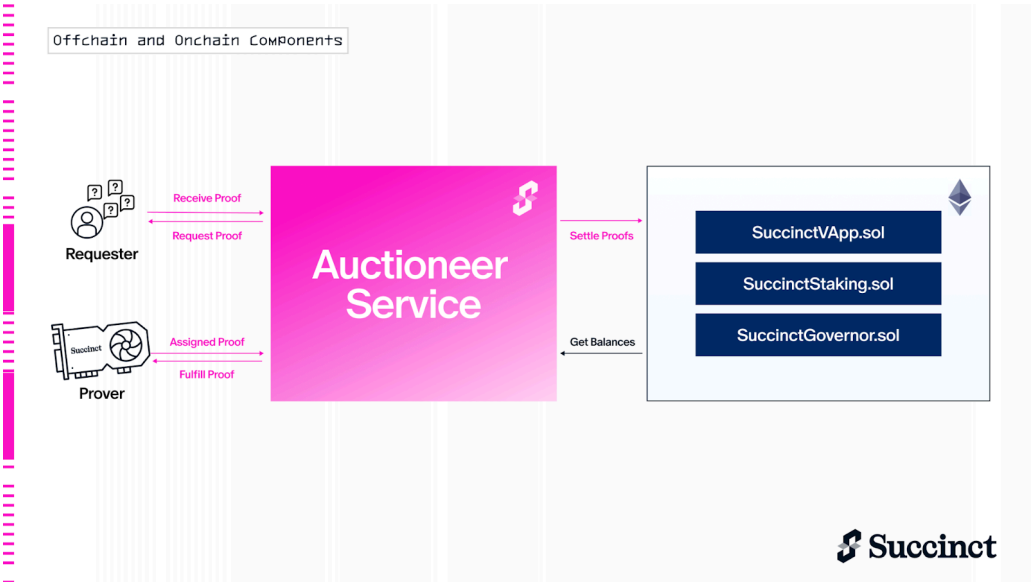
경쟁 기반의 가격 책정
전 세계 증명자들은 증명 경매(proof contest)라는 메커니즘을 통해 가격 경쟁을 벌입니다. 이 메커니즘에서 증명자는 PROVE를 스테이킹한 뒤, 가장 낮은 증명 가격을 제시하여 경매에 참여합니다. 이 구조는 증명 비용을 시장의 적정 수준으로 끌어내리고, 더 나은 알고리즘이나 하드웨어에 투자한 참여자에게 지속적인 보상을 제공합니다. 참여 증명자가 늘어날수록 네트워크 용량은 확대되고, 가격은 점점 더 효율화됩니다.

물리적 인프라 인센티브 모델에서 영감
Succinct Prover Network는 비트코인(채굴 장비 확산), 파일코인(탈중앙 스토리지 인프라) 등 성공적인 물리 기반 인센티브 모델을 영지식 증명 도메인에 확장 적용합니다. 이러한 네트워크와 마찬가지로, Succinct는 네이티브 토큰(PROVE)을 통한 프로토콜 수준의 인센티브를 활용하여 다음을 달성합니다:

- 고성능 GPU 클러스터 및 맞춤형 하드웨어와 같은 전문 역량 유치
- 서비스 품질과 가격에 대한 경쟁 유도
- 증명 시스템에 대한 지속적인 연구 개발 촉진

무엇보다도 기존 솔루션들이 사용자를 위한 효율적이고 주문형(on-demand) 증명을 제공하지 못하는 반면, Succinct Prover Network는 자유 시장 경쟁을 직접 유도하여 효율적인 증명 생성을 실현합니다.

프로토콜 아키텍쳐



경매자(Auctioneer) 및 정산(결제) 구조

Succinct Prover Network는 영지식 증명을 생성하기 위한 프로토콜입니다. 이 프로토콜은 요청자와 증명자를 연결하는 이중 시장 구조를 구현합니다. 요청자는 증명자들 간의 경쟁을 통해 가장 낮은 가격에 증명을 조달할 수 있습니다. 이 구조는 요청자와 증명자 간의 검증 가능한 매칭을 가능하게 하며, 모든 애플리케이션에 적합한 고성능 사용자 경험을 제공합니다.

프로토콜은 검증 가능한 애플리케이션(vApp) 구조로 설계되어 있습니다. 경매 및 증명 할당을 관리하는 오프체인 컴포넌트(일종의 L2 시퀀서 역할)와, 상태 루트 및 올바른 실행에 대한 증명을 이더리움에 정산하는 온체인 스마트 컨트랙트로 구성되어 있습니다. 이는 실행과 정산을 분리하는 L2 아키텍처와 유사한 설계입니다.

이러한 구조는 기존 체인의 처리량 한계를 회피할 수 있는 통합된 배포 방식을 제공합니다. 사용자는 현재의 블록체인 지연 문제를 겪지 않고, 실시간 저지연 환경에서 서비스를 이용할 수 있습니다. 동시에 이더리움 상에서 자신의 예치금을 확인하고, 네트워크 상태를 독립적으로 검증할 수 있습니다.

참여자

Succinct Network에는 다음 두 가지 주요 참여자가 존재합니다:

- **요청자**: 영지식 증명을 필요로 하는 애플리케이션
  요청자는 네트워크에 증명 생성을 요청하는 애플리케이션입니다. ZK 롤업, ZK 브리지, AI 에이전트, 게임 등 다양한 형태가 포함됩니다. 요청자는 다음과 같은 요소를 포함하여 요청을 제출합니다:
  - 프로그램: Rust로 작성된 계산 프로그램
  - 입력값: 공개 또는 비공개 입력
  - 최대 증명자 가스: PGU(Prover Gas Unit) 단위로 측정된 계산 복잡도의 상한
  - 최대 PROVE 수수료: 요청자가 지불 가능한 최대 금액
  - 최소 PROVE 스테이킹: 경매 참여를 위한 증명자의 최소 지분
  - 마감 시간: 증명이 제공되기까지 허용 가능한 최대 대기 시간
  - 검증 키: 온체인 또는 오프체인에서 증명을 검증하는 데 필요한 키
- **증명자**: 해당 증명을 생성하는 주체

증명자는 '증명 경매(proof contest)'에 입찰하여 요청에 대한 증명을 생성하는 참여자입니다.

- PROVE를 스테이킹하여 입찰 자격을 획득합니다.
- 노드 소프트웨어를 실행하여 요청을 수신하고 입찰 및 증명을 수행합니다.
- 증명자는 최소 가격을 제시하여 경매에 경쟁 입찰하며, 낙찰된 경우 기한 내에 증명을 제공해야 하며, 실패 시 지분이 슬래시될 수 있습니다.
- 필요에 따라 수백 개 GPU로 구성된 클러스터를 통해 고성능 증명을 제공할 수 있습니다.

네트워크 컴포넌트

Succinct Network는 두 가지 주요 컴포넌트로 구성됩니다:

오프체인 경매자 서비스

경매자 서비스는 요청자와 증명자를 매칭하는 오프체인 코디네이터 역할을 합니다.

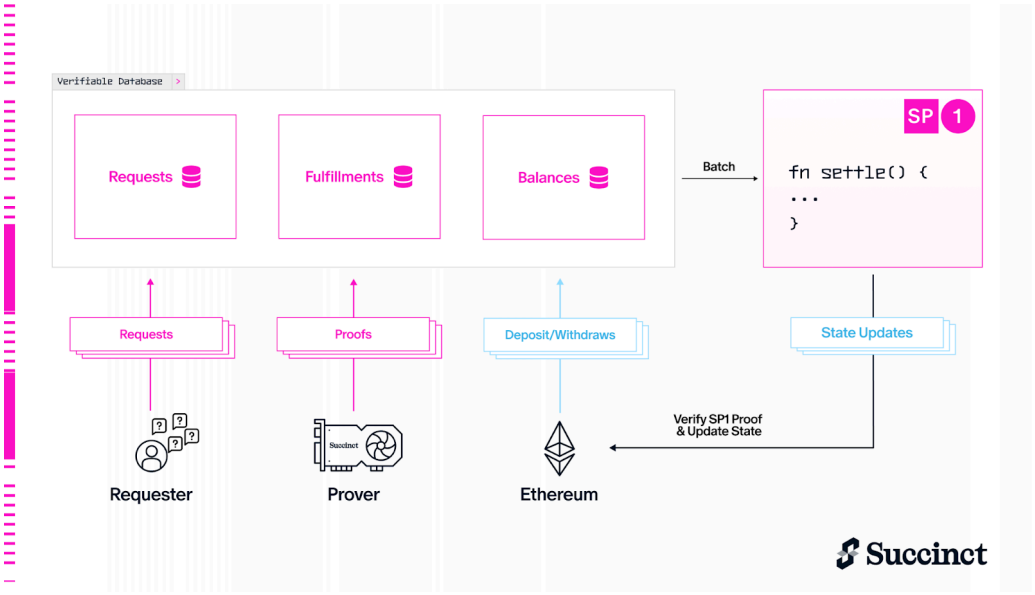
- 요청자는 증명 요청과 결제를 제출합니다.
- 증명자는 경매자에게 입찰을 제출합니다.
- 요청자는 증명을 수령하고, 증명자는 보상을 받습니다.
- 요청자는 RPC를 통해 직접 경매자와 상호작용하므로 실시간, 고성능 경험을 제공합니다.

온체인 정산 컨트랙트

정산 컨트랙트는 경매자가 주기적으로 제출하는 상태 루트 및 ZK 증명을 정산합니다.

- 상태 변경 내역: 요청 접수, 취소, 이행 등을 포함합니다.
- 사용자 자금은 항상 이더리움에 보관되며, 사용자는 직접 출금할 수 있습니다.
- 경매자는 사용자 자금을 보관하지 않으며, 자금의 보안은 정산 컨트랙트가 보장합니다.

경매자 서비스 및 검증 가능한 데이터베이스



검증 가능한 백엔드

Succinct는 일반 웹 애플리케이션 수준의 성능으로 사용자의 잔고 및 증명 상태 업데이트를 누구나 검증할 수 있도록 백엔드를 구성합니다. 경매자는 사용자의 상태 정보를 보유하며, 주기적으로 상태 증명(state proof)을 이더리움에 게시합니다. 경매자 서비스는 다음과 같이 구성됩니다:

- **검증 가능한 데이터베이스**: 사용자 잔고, 요청 대기 목록, 증명 완료 내역을 저장합니다. 읽기·쓰기 작업은 머클 증명으로 이더리움에 커밋됩니다.

- **증명자 프로세스**: SP1 기반 프로그램이 네트워크 상태 전이 함수를 실행하고, 이로부터 새로운 상태에 대한 증명을 생성하여 이더리움에 정산합니다.

데이터 가용성 레이어

현재는 임시 저장소를 사용하여 증명 요청 데이터를 보관하고 있으며, 향후 온체인 데이터 가용성이 확보되면 지속 가능한 저장소로 전환될 예정입니다. 이 레이어은 증명 데이터를 저장하고 빠르게 검증을 위한 조회를 제공할 수 있습니다.

이더리움 스마트 컨트랙트

이더리움 기반 스마트 컨트랙트는 Succinct Network의 신뢰 최소화 정산 레이어을 구성합니다. 주요 기능은 다음과 같습니다:

- 예치 및 출금
  요청자는 PROVE 토큰을 예치하여 증명 요청 비용을 지불하며, 경매자가 작동하지 않더라도 이더리움에서 직접 출금이 가능합니다.

- 스테이킹 및 슬래싱
  증명자는 PROVE 토큰을 스테이킹하여 경매에 참여하며, 낙찰 후 마감 기한 내에 유효한 증명을 제출하지 못하면 지분이 일부 또는 전부 슬래시될 수 있습니다. 타인의 스테이킹 위임도 허용됩니다.

- 결제 및 가치 분배
  요청자와 증명자 간의 수수료 및 결제 처리를 담당합니다.

- 네트워크 거버넌스
  vApp, 스테이킹, 슬래싱, 경매 등과 관련된 매개변수를 탈중앙 방식으로 운영합니다.

이 컨트랙트들은 중앙화된 기관에 의존하지 않고도 예금, 출금 및 삭감에 대한 경제적 보장을 시행할 수 있도록 합니다.

2. 토큰 이코노미

가상자산 소개

PROVE는 Succinct 생태계 내 유틸리티 토큰으로, 결제, 스테이킹, 거버넌스 참여수단으로 활용됩니다.

발행량 및 유통량계획

총 공급량은 10억 PROVE로 고정되어 있습니다.

토크노믹스

항목	내용
티커	PROVE
총 공급량	1,000,000,000 PROVE
토큰 유형	이더리움 기반 ERC-20

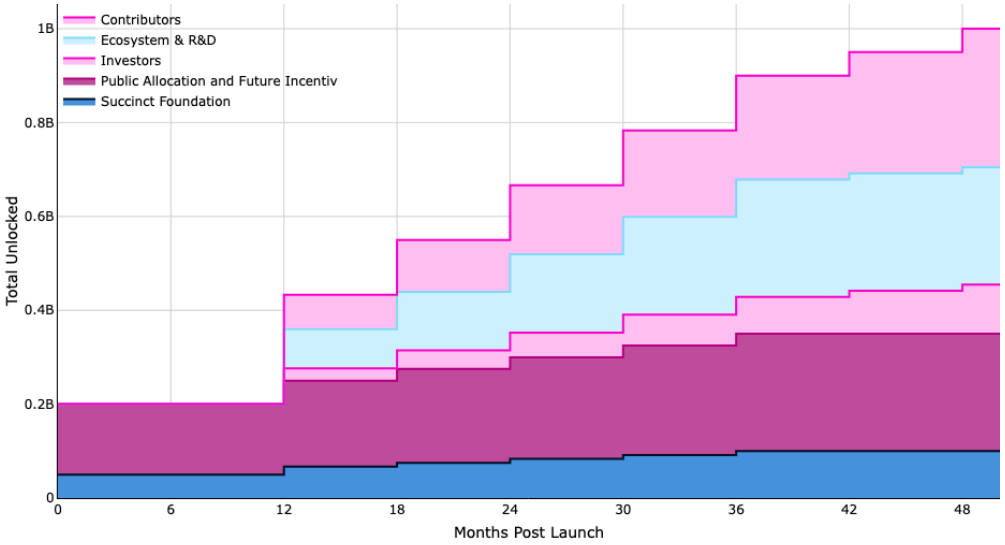
토큰 분배

아래 표는 PROVE 토큰이 Succinct 생태계 내 다양한 이해관계자에게 어떻게 분배되는지를 보여줍니다. 해당 수치는 최종 분배 기준입니다.

항목	설명	토큰 할당 (%)
퍼블릭 할당 및 향후 인센티브	증명자, 스테이커 및 기타 네트워크 참여자 및 지지자를 위한 인센티브. 최초의 PROVE 에어드롭은 전체 공급량 중 5%가 할당됨.	25%
Succinct 재단	운영 비용, 거버넌스 지원, 재단의 지속가능한 개발을 위한 할당.	10%
생태계 및 R&D	생태계 조성, 연구 및 개발 활동 지원, 네트워크의 장기적인 성장 지속을 위한 재원.	25%
투자자	시드 및 시리즈 A 투자자.	10.5%
기여자	Succinct Network의 핵심 기여자, Succinct Labs 팀원 및 향후 핵심 기여자 포함.	29.5%
총계	**총 토큰 공급량**	**100%**

유통계획
PROVE는 시간 경과에 따라 아래 일정에 따라 순차적으로 언락됩니다. 이 일정은 초기 지지자, 핵심 기여자, 생태계, 향후 인센티브 펀드, 재단 등 다양한 대상자에 대한 언락 흐름을 보여줍니다.

투자자 및 기여자는 1년 락업(클리프)이 적용됩니다. 12개월 시점에 할당량의 1/4이 최초로 언락되며, 이후 36개월에 걸쳐 6개월마다 1/8씩 순차적으로 언락됩니다. 전체 언락 기간은 총 48개월(4년)입니다.



토큰 유틸리티

- **결제**
  PROVE는 Succinct Prover Network의 결제 토큰입니다. ZK 애플리케이션은 증명 비용을 PROVE로 지불하며, 롤업, 베이스 레이어 블록체인, 검증 가능한 애플리케이션 등이 PROVE로 표시된 증명 요청을 네트워크에 제출할 수 있습니다. 증명 결제에 PROVE를 사용하는 방법은 여기에서 확인할 수 있습니다.

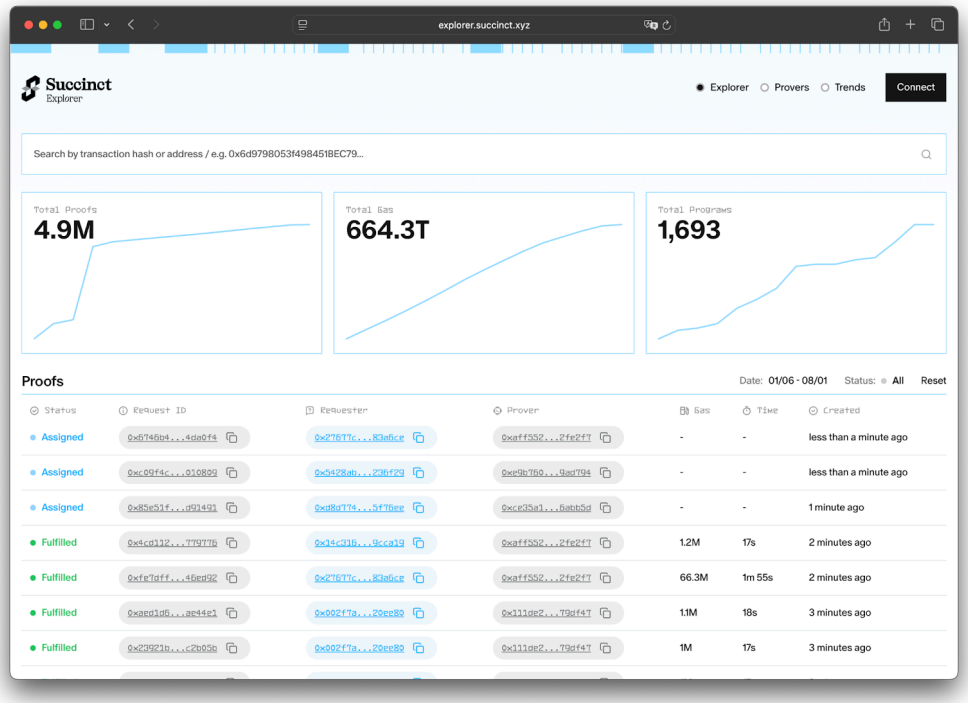
- **스테이킹**
  증명자는 PROVE를 스테이킹하여 네트워크 참여 자격을 확보합니다. Succinct Prover Network는 위임 스테이킹 시스템을 사용하며, 누구나 증명자에게 스테이킹하여 수수료 일부 및 Succinct 재단이 제공하는 추가 인센티브를 받을 수 있습니다. 이러한 인센티브는 네트워크 초창기 생태계 부트스트랩 단계에서 참여를 유도하기 위해 설계되었습니다.

  스테이킹 규모는 증명자가 동시에 참여할 수 있는 증명 요청 경매 수를 결정합니다. 스테이킹은 중첩된 금고 구조(nested vault structure)로 구현되어, 스테이커가 네트워크로부터 보상을 받을 수 있도록 설계되어 있습니다. 스테이킹에 대한 자세한 내용은 여기에서 확인할 수 있습니다.

- **거버넌스**
  초기에는 네트워크의 주요 파라미터가 보안 위원회에 의해 설정됩니다. 이후에는 PROVE를 스테이킹한 증명자들이 투표를 통해 네트워크 파라미터를 변경하는 방식으로 거버넌스가 전환될 예정입니다.

3. 참고자료

익스플로러



출처 : https://explorer.succinct.xyz

위험고지 안내
Disclaimer

본 문서에 기재된 정보는 당사(코인원)가 본 가상자산 심사 시점에 접근 가능한 정보 채널을 통하여 확인한 것으로, 정확하지 않거나 투자시점에는 변경 또는 유효하지 않을 수 있습니다.

가상자산 발행자가 공시한 내용 및 백서를 통해 정확한 정보를 확인하신 후 투자하시기 바랍니다.

가상자산은 법정화폐가 아니므로 특정 주체가 가치를 보장하지 않습니다.

coinone