

2022 오픈소스 컨트리뷰션 아카데미

Open Source
Contribution
Academy



Ethereum Privacy & Scaling Explorations



Project Guide



주최



과학기술정보통신부

주관

nipa

정보통신산업진흥원





프로젝트 개요

프로젝트 분야 · 활용 언어 · Repository · 난이도 · 참가자 모집
유형 및 우대사항 등



1 프로젝트 개요

프로젝트 명 : Ethereum Privacy & Scaling Explorations

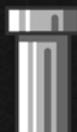
프로젝트 분야 : Ethereum, Privacy, ZKP, Cryptography

프로젝트 저장소 : <https://github.com/appliedzkp>

<https://github.com/semaphore-protocol> 외 다수

활용 언어 : Typescript / Rust / Circom / Solidity

프로젝트 난이도 : 상



1 프로젝트 개요

참가자 모집 유형

이더리움의 프라이버시 및 확장성을 개선하는 연구중심 오픈소스 컨트리뷰션에 관심있으신 분들을 모집합니다.

- 이더리움을 잘 이해하고 있어야 합니다.
- 타원곡선암호학 및 영지식 증명에 대해 공부하고 이해할 수 있어야 합니다.

우대 사항

- 타입스크립트 및 기타 다른 언어를 활용한 소프트웨어 구현 스킬이 있으실 경우 다양한 기여를 하실 수 있습니다.



프로젝트 소개

프로젝트 상세 소개 내용



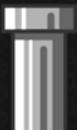
2 프로젝트 소개

주요내용 1

이더리움 재단의 Privacy & Scaling Explorations 팀(이하 PSE팀)은 이더리움에 꼭 필요한 프라이버시 및 확장성과 관련해 필요한 연구들을 수행하고 있습니다. 본 컨트리뷰션 아카데미에서는 PSE팀에서 진행하고 있는 다양한 연구 프로젝트에 기여하는 것을 목표로 합니다.

주요내용 2

PSE팀에서 주로 연구하는 내용은 영지식증명에 대한 개선방안, 영지식증명 및 암호학을 활용한 다양한 응용 프로그램들입니다. 기여를 위해서는 이더리움에 대한 이해가 필수적으로 필요하고 암호학에 대해 공부해야 합니다.



2 프로젝트 소개

주요내용 3

기여가능한 주요 프로젝트로는

- 영지식증명을 활용해 완전탈중앙 네트워크에서 스팸을 방지할 수 있는 Rate Limiting Nullifier 프로젝트
- 익명송금을 가능하게 하는 Zkopru 프로젝트
- BLS 서명을 활용해 확장성을 개선하는 프로젝트
- 그룹의 일원임을 증명할 수 있는 프로토콜인 Semaphore 프로젝트
- Semaphore 프로토콜을 사용해 익명화된 레putation 관리 시스템인 Interep
- 익명 소셜 네트워크인 Unirep Social
- 이더리움의 상태관리머신인 EVM을 영지식 증명으로 증명하는 zk-EVM 프로젝트

등이 있습니다.



컨트리뷰션 가이드

단계별 컨트리뷰션 커리큘럼



3. 컨트리뷰션 가이드

컨트리뷰션 코스 1

온보딩 과정

- 참여자는 제공된 리스트(RLN, Zkopru, BLS, zkEVM 등) 중에서 기여하고자 하는 프로젝트를 선정하고 멘티끼리 그룹을 구성합니다.
- 각 그룹별로 프로젝트에 대해 자세하게 이해하기 위해 개별 세미나를 진행하고 발표하는 시간을 가집니다.

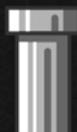
세미나 발표는 모든 멘티가 준비해서 진행합니다.
겉치는 내용을 준비했더라도 괜찮습니다. 서로 보완할 수 있는 부분 중심으로 발표를 진행합니다.

3 컨트리뷰션 가이드

컨트리뷰션 코스 2

프로젝트 코드베이스 이해

- 각 프로젝트별로 코드를 클론하고 로컬환경에서 테스트를 구동하며 개발환경을 구축합니다.
- 필요할 경우 프로젝트 오너/메인테이너들과 콜을 통해 핸즈온세션을 가집니다.



3. 컨트리뷰션 가이드

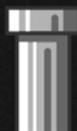
컨트리뷰션 코스 3

이슈 탐색 및 PR

- 개발환경 구축이 완료되었을 경우 이슈탐색 후 PR을 전송합니다.
- 프로젝트 오너/메인테이너들과 PR이 머지/클로즈 되기까지 소통합니다.

기여완료후

- 기여 완료에 따른 배지를 수여받습니다.





컨트리뷰션 운영 방안

컨트리뷰션 단계별 상세 운영 방안



4. 컨트리뷰션 운영 방안

1주차

아이스 브레이킹
멘티별 기여 프로젝트 선정

- RLN
- Zkopru
- BLS signature
- zk-EVM
- ...

(본 프로젝트 목록은 상황에 따라 변경될 수 있습니다)

2주차

팀별로 온보딩 문서 습득



4. 컨트리뷰션 운영 방안

3주차

세미나 1차

4주차

세미나 2차



4. 컨트리뷰션 운영 방안

5주차

프로그램 개발 환경 구축

6주차

이슈 탐색 후 기여 방안 정리



4. 컨트리뷰션 운영 방안

7주차

- 1차 스프린트(~8주차)
- 참가자 당 PR 2개 목표

8주차

- 1차 스프린트(~8주차)
- 참가자 당 PR 2개 목표

4. 컨트리뷰션 운영 방안

9주차

- 2차 스프린트(~12주차)
- 참가자 당 PR 2개 목표

10주차

- 2차 스프린트(~12주차)
- 참가자 당 PR 2개 목표

4. 컨트리뷰션 운영 방안

11주차

- 2차 스프린트(~12주차)
- 참가자 당 PR 2개 목표

12주차

- 2차 스프린트(~12주차)
- 참가자 당 PR 2개 목표

4. 컨트리뷰션 운영 방안

13주차

컨트리뷰션 배지 수령

마무리

마무리 보고서 작성 및 해산



4. 컨트리뷰션 운영 방안

ONLINE



- 세미나 진행(구글 미트)
- 디스코드 통해서 프로그램 운영

OFFLINE



- 온보딩 오프라인 미팅(7월)
- 1차 스프린트(8월)
- 2차 스프린트(9월)

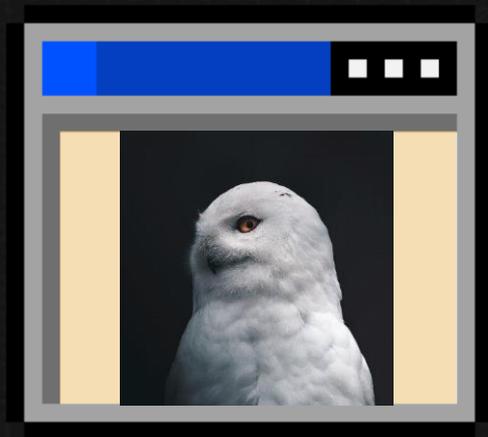


멘토 소개

컨트리뷰션 프로젝트팀 멘토단 소개

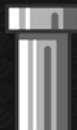


5 멘토 소개



임완섭

- Ethereum Foundation Applied ZKP Developer



2022 오픈소스

컨트리뷰션 아카데미

Open Source
Contribution
Academy



Ethereum Privacy & Scaling Explorations

컨트리뷰션에 도전해 보세요!



THANK YOU



주최



과학기술정보통신부

주관

nipa

정보통신산업진흥원

