https://github.com/nobitex/sigmab

==> circom
CIRCUIT COMPILER

python™

سیگما-بی

اثبات اندوخته‌ی نوبیتکس با تکنولوژی اثبات‌های دانش-صفر

مستندات

اولین بار در دنیا

نوبیتکس لبز به‌عنوان بازوی تحقیقاتی نوبیتکس، با در کنار هم قرار دادن تکنولوژی‌ها و روش‌های روز دنیای رمزنگاری، پروتکل جدیدی برای اثبات اندوخته طراحی و پیاده‌سازی کرده است که در آن علاوه بر حریم خصوصی کاربران، حریم خصوصی کیف پول‌های امانی نوبیتکس نیز حفظ می‌شود.

README

اثبات دانش-صفر

فرض کنید که f تابعی است که چند ورودی میگیرد و یک خروجی می‌دهد. اثبات‌های دانش-صفر، پروتکل های رمزنگاری هستند که ما را قادر می‌سازند ثابت کنیم ورودی هایی را می‌دانیم که در صورت اعمال f روی آنها، خروجی برابر یک مقدار خاص می‌شود. با استفاده از اثبات‌های دانش-صفر و تعهد های رمزی، می‌توانیم نوعی «لیست بدهی خصوصی» طراحی کنیم.

لیست بدهی خصوصی

فرض کنید که بجای انتشار عمومی لیست بدهی، از آن Hash میگیریم و آن را انتشار می‌دهیم. با اینکار به لیست بدهی متعهد می‌شویم. حال فرض کنید که تابع f_1 با مشخصات زیر داریم:

$$f_1(L, i) = (h(L), \sum_k L[k]_{balance}, L[i]_{id}, L[i]_{balance})$$

این تابع لیست بدهی (L) و یک اندیس (i) را به عنوان ورودی دریافت می‌کند و یک چهارتایی را به عنوان خروجی برمی‌گرداند:

- $h(L)$ هش لیست بدهی است.
- $\sum_k L[k]_{balance}$ مجموع همه بدهی های موجود در لیست است.
- $L[i]_{id}$ شناسه i-امین کاربر موجود در لیست بدهی است.
- $L[i]_{balance}$ موجودی i-امین کاربر موجود در لیست بدهی است.

حال فرض کنید که نوبیتکس ابتدا لیست بدهی L را با توجه به لیست کاربران خود می‌سازد و هش آن را ($C = h(L)$) بصورت عمومی منتشر میکند. سپس با استفاده از اثبات‌های دانش-صفر ثابت می‌کند که ورودی هایی را برای تابع f_1 می‌داند که باعث خروجی (C, T, K, V) می‌شود. در صورت برابر بودن C خروجی با C اولیه اعلام شده توسط نوبیتکس، عملا نوبیتکس ثابت کرده است که:

- اولا: مجموع موجودی های کاربران برابر T است.
- دوما: شخصی داخل لیست وجود دارد که شناسه او برابر K است.
- سوما: موجودی همان شخص داخل لیست برابر V است.

آتوسا با دریافت این اثبات و بررسی برابر بودن C با تعهد لیست بدهی ها که نوبیتکس از قبل اعلام کرده بود، قانع می‌شود که هنگام متعهد شدن نوبیتکس به لیست بدهی، آتوسا (با شناسه K) و V واحد رمزارز او نیز در نظر گرفته شده اند. همچنین آتوسا متوجه می‌شود که مقدار کل بدهی اعلامی نوبیتکس برابر T است.

آتوسا می‌تواند مقدار T را با مقدار کل اندوخته های نوبیتکس (که n است) مقایسه کند.

شرکت کننده ها

لیست افرادی که در فرایند راه‌اندازی امن سیگما-بی شرکت کرده اند:

- کیوان کامبخش
- محمدعلی حیدری
- پردیس طولابی
- حمید باطنی
- علیرضا مفتخر
- امیرحسین آذرپور
- امیرحسین حسینی
- امیرعلی آذرپور
- محمد سهراب ثامنی
- نیما یزدان مهر
- پریسا حسنی زاده
- شهریار ابراهیمی
- سیاوش تفضلی
- پدرام میرشاه
- عباس آشتیانی
- علی مقصودی
- آرش فتاح‌زاده
- امید مسگرها

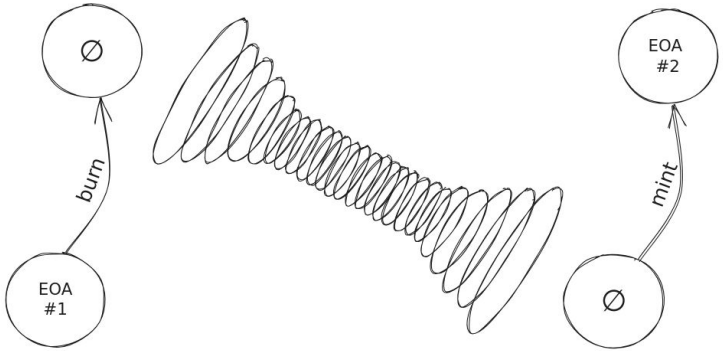
Contributors 16

+ 2 contributors

دور ریختن زباله ها سمی حتی توسط یکی از این افراد باعث می‌شود اطمینان حاصل کنیم که تولید اثبات‌های جعلی امکان‌پذیر نیست.

EIP-7503

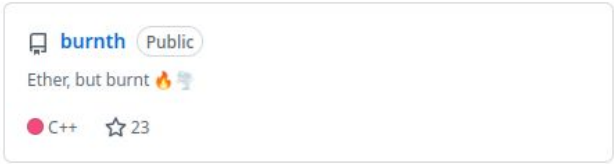
Zero-Knowledge Wormholes



EIP | Slides | GitHub | Discuss

By Nobitex Labs

https://github.com/nobitex/burnth



==>circom
CIRCUIT COMPILER

SOLIDITY

python™

Draft | Standards Track: Core

EIP-7503: Zero-Knowledge Wormholes

Enable minting of secretly burnt Ethers as a native privacy solution for Ethereum

Authors	Keyvan Kambakhsh (@keyvank), Hamid Bateni (@irnb), Amir Kahoori <a.kahoorizadeh@gmail.com>, Nobitex Labs <labs@nobitex.ir>, 0xwormhole (@0xwormhole)

Created	2023-08-14
Discussion Link	https://ethereum-magicians.org/t/eip-7503-zero-knowledge-wormholes-private-proof-of-burn-ppob/15456
Requires	EIP-2718, EIP-4844, EIP-7708

Table of Contents

- Abstract
- Specification
    - Parameters
- Rationale
    - Scalability Implications
- Backwards Compatibility
- Reference Implementation
    - ZK-SNARK Implementation
- Security Considerations
- Copyright

Abstract

While researching on privacy solutions and applications of ZKP, we discovered a technique, by which people can burn their digital asset (E.g ETH) by sending it to an unspendable address, and later build a ZK proof showing that some amount of tokens reside in an account that are

https://github.com/nobitex/xevm

About

Tiny implementation of EVM in pure Rust

rust evm

Readme
MIT license
Activity
Custom properties
27 stars