zkSTARK

Zero-Knowledge Scalable Transparent Argument of Knowledgeの略

StarkWare社のスケーラビリティ技術基盤

SNARKの後に出てきた(6年後らしい)

NotebookLMでの調査内容

特徴

スケーラブルな検証

証明する計算が複雑になっても検証に必要な計算量は比較的小さいまま

透過性

証明の生成や検証プロセスに信頼された第三者による初期設定(トラステッドセットアップ)が不要

ゼロ知識性

証明者が検証者に計算結果の正しさを伝えつつ、その計算に関する秘密情報を公開しない

量子コンピュータ耐性がある

数学的根拠

zkSNARKと比較して.....

✔構築にTrusted Setupが不要

✔検証計算の複雑度は低い

❌検証データサイズが大きめ(10〜100倍)

❓検証が遅いらしいとあったがよくわからない

---

zkSNARKとの違い

似たような技術に zkSNARK がある。

zk-SNARK vs zkSTARK - Explained Simple - Chainlink

/layerx/zk-SNARKsとzk-STARKsの比較

Zero-Knowledge Succinct Non-interactive Argument of Knowledge の略で「ゼロ知識証明プロトコル」の1つ。

zkSNARKは数ミリ秒で検証できて高速なのだが、その代わり一部のSNARKはセキュリティ

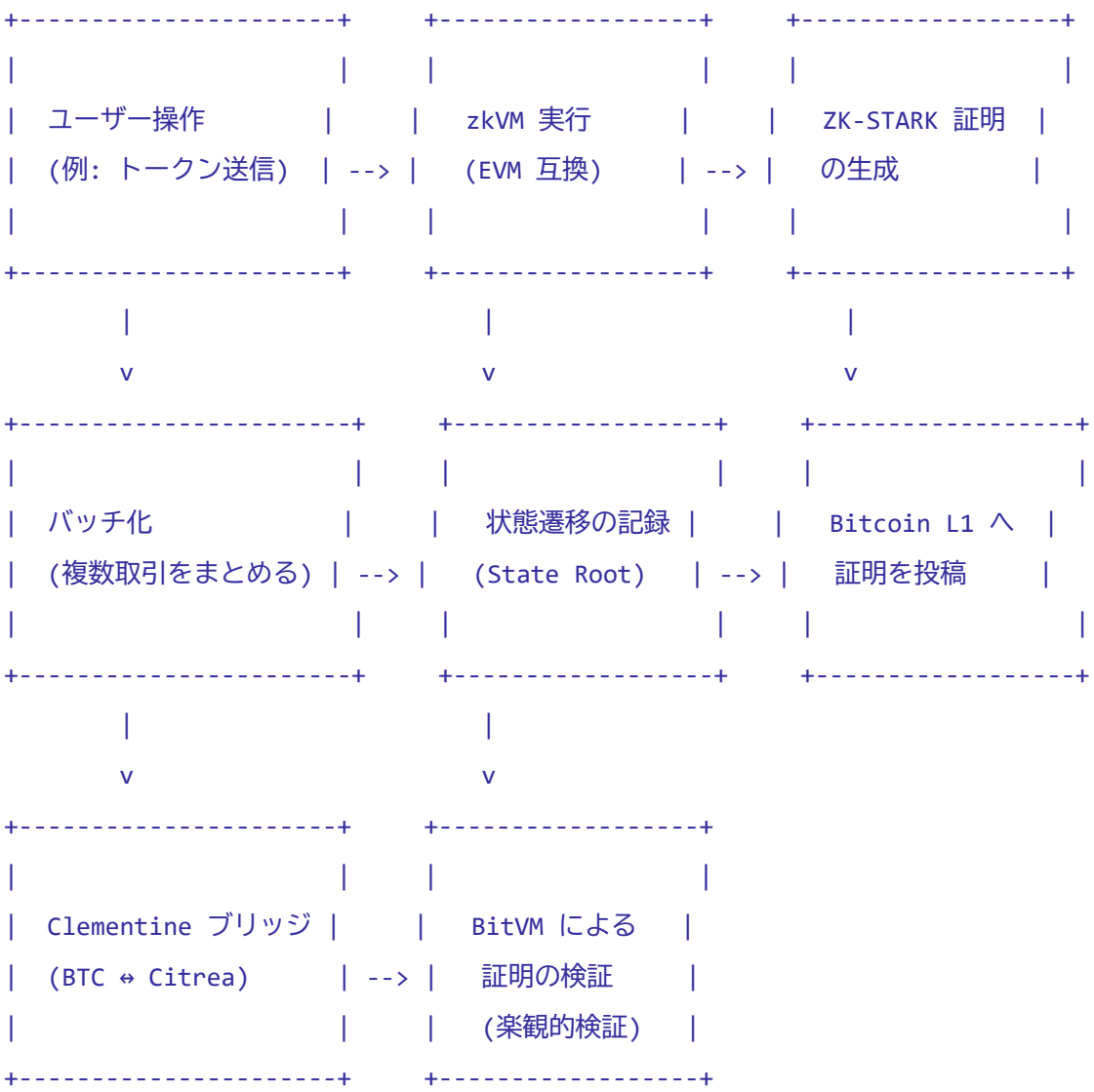
上の潜在的な弱点である「Trusted Setup」に依存している
zkSTARKはTrusted Setupが不要なのでセキュリティ的にはzkSNARKよりも高くなるが、検証の効率は下がる。また検証データもzkSNARKより大きくなる傾向にある(10〜100倍といわれている(Binance Academy))。
が、zkSTARKの検証は外部パラメータに依存しないのでzkSNARKより監査が容易になる可能性がある。

ちなみに zkSync は zkSNARK の方らしい。
Bitcoinの ZeroSync には StartWare の名がある。

Citrea

Bitcoin L2 の Citrea は zkSTARK 系である。
https://www.blog.citrea.xyz/introducing-citrea/

chatgpt



🔍 フローの詳細説明

ユーザー操作:

ユーザーが Citrea 上でトークン送信などの操作を行います。

zkVM 実行:

Ethereum Virtual Machine（EVM）互換の zkVM 上で、ユーザーの操作が処理されます。

ZK-STARK 証明の生成:

処理結果に対する ZK-STARK 証明が生成されます。

バッチ化:

複数の取引をまとめてバッチ化し、効率的に処理します。

状態遷移の記録:

バッチ化された取引の状態遷移（State Root）が記録されます。

Bitcoin L1 へ証明を投稿:

生成された証明が Bitcoin の L1 に投稿され、セキュリティが確保されます。

Clementine ブリッジ:

Bitcoin と Citrea 間で資産の移動を可能にするブリッジが機能します。

BitVM による証明の検証:

Bitcoin 上で BitVM を用いて証明の検証が行われ、セキュリティが確保されます。

実装

zkSNARKはいろいろフレームワークなどの組み合わせがあるのだが、STARKはStarkWare社だけしかやっていないということはないだろうか？

Getting Started - Starknet.js

Layer2のゼロ知識証明を実装してみる｜株式会社ブロックス

STARKを用いてRISC-Vの実行履歴証明を行うフレームワークRISC Zeroの紹介 - HashPort技術ブログ

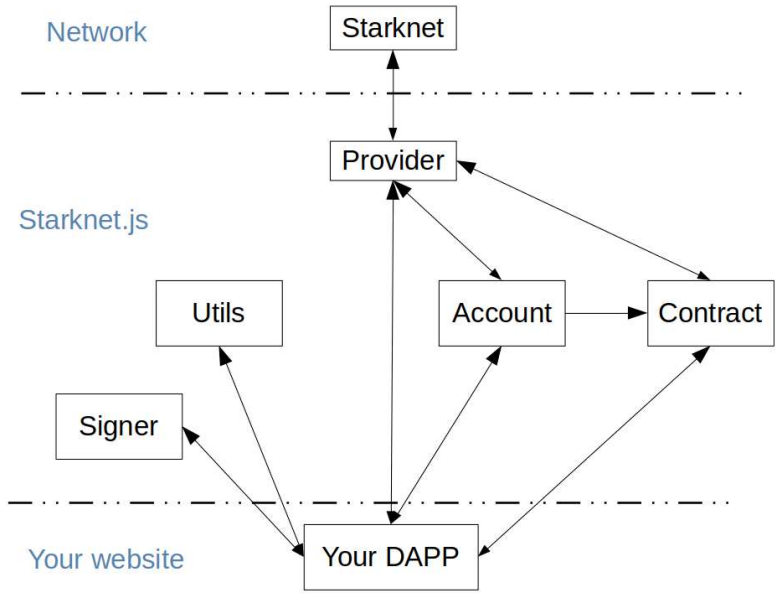
RISC Zero v1系でzk-STARKによるRustプログラムの証明と検証をする - HashPort技術ブログ

ライブラリ

Starknet.js

Getting Started - Starknet.js

zkSTARK用というよりは starknet 用



GuildOfWeavers/genSTARK: A library for generating zk-STARKs.

JavaScriptライブラリ

検索して最初に出てきた。

elibensasson/libSTARK: A library for zero knowledge (ZK) scalable transparent argument of knowledge (STARK)

C++ライブラリ

いろいろ紹介

https://tech.hashport.io/4281/ (2023年11月22日)

ethSTARK

winterfell

ministark

2025年5月は Cairo v2 になったので古いかも