ゼロ知識証明に出てくる用語

ZKP向けのハッシュ

ZKPの回路にしたときにサイズが大きくなるなどの理由で向き不向きが出てくるそうだ。

ChatGPTに比較表を作ってもらった。

hash

ハッシュ関数	ZKP回路コスト	実装の難易度	暗号強度	ZKPでの採用例	備考
SHA-256	非常に高い（~25000constraints）	中	非常に高い	zkEVM（互換性目的）、zk-SNARK（非効率）	通常の暗号用途では標準。ZKPド
Keccak(SHA-3)	非常に高い（~20000constraints）	やや複雑	非常に高い	zkEVM、zkSync、PolygonzkEVM	Solidity互換のために選ばれるが
Blake2s	高い（~8000〜10000constraints）	中	高い	zkEVM系、Aztec	SHAよりは軽いがまだZKPには不
Pedersen	中程度（~500〜2000constraints）	やや難（EC演算あり）	中程度	Zcash（Sapling）、TornadoCash	楕円曲線との親和性が高い、Me
MiMC	低い（~200〜500constraints）	非常に簡単	中程度（構造に依存）	Aleo、StarkWare、zkLLVM	ラウンド関数が単純。分析がやや
Poseidon	非常に低い（~100〜300constraints）	やや難（パラメータ設計あり）	高い（ZKP設計）	Circom、Halo2、zkSync、Aztec	現在最もZKPフレンドリー。ZKI
Rescue	低い（~200〜400constraints）	中	高い	STARK-basedsystems（例：Winterfell）	Poseidonより強めのセキュリテ

Baby Jubjub

楕円曲線の名前。Ethereum の EIP にも出てくる。Pedersen Hash を調べているときに出てきた。

https://duckduckgo.com/?q=circomlib+pedersen+babyjubjub&t=newext&atb=v441-1&ia=web

データ可用性 Data Availability、DA

ChatGPT

L2の状態を再構成するために必要なデータが、誰でもアクセス可能な状態であること。

つまり、「この取引が正しく処理された」と主張するだけでなく、その根拠となるデータが公開されているかどうかが問われます。

LNでいうところの Commitment Transactionのようなものか。

基本的に L1 に展開しておく

オペレーター、シーケンサー、プルーバー、リレイヤー

zkRollupの運用側の役割名(ChatGPTより)。

オペレーター(Operator)

以下の役割の総称だと思う

シーケンサー(Sequencer)

トランザクションの順序を決定し、処理をまとめる役割。

プルーバー(Prover)

状態変更に対する**ZK証明（zkSNARK/zkSTARK）**を生成する役割。

リレイヤー(Relayer) ※場合によって

Proverが生成した証明をEthereumに送信する役割。

iden3

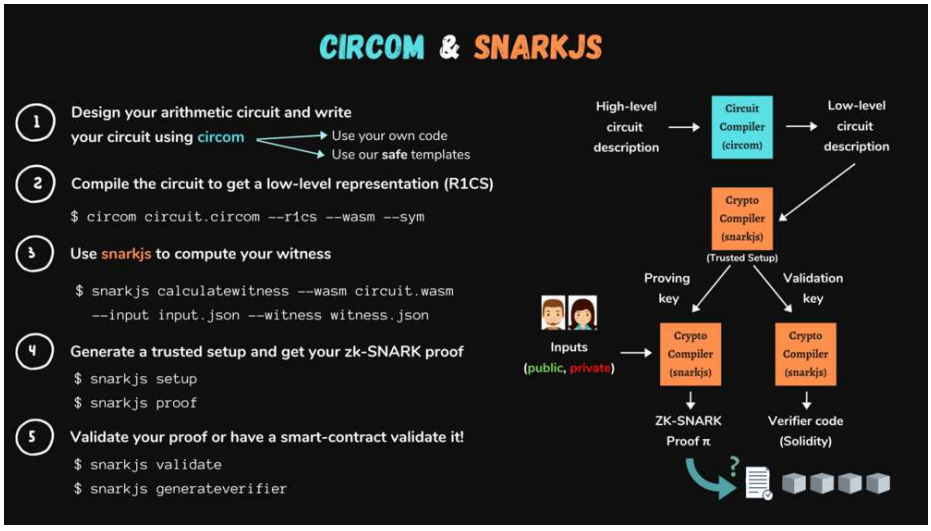
https://iden3.io/

https://docs.circom.io/

zkSNARK の実装でしばしば見かける会社。認証関係の会社なので、"web3" みたいな感じで "iden3" としたのか。

Tornado Cach もここにあるリポジトリから fork していた。

https://github.com/iden3



iden3/circom

https://github.com/iden3/circom

zkSNARKの回路用コンパイラ。

回路用の言語名も circom で、拡張子も `.circom` にする。

iden3/circomlib

https://github.com/iden3/circomlib

circomライブラリ。次の `circomlibjs` と間違いやすい。

> This repository contains a library of circuit templates.

iden3/circomlibjs

https://github.com/iden3/circomlibjs

JavaScriptライブラリ。前の `circomlib` と間違いやすい。

proof や witness の算出に使われる。

> circomlibjs is a Javascript library that provides programs to compute the witness of several circuits of circomlib.

iden3/snarkjs

https://github.com/iden3/snarkjs