ゼロ知識証明

zkSNARK

zkSTARK

概要

パスワードをハッシュ化して一致を確認するというだけのやり方でもゼロ知識証明になる。

LiquidのConfidential Transactionは宛先や送金額を見えなくしても検証できるようになっているが、あれもゼロ知識証明

古典的ZKPは相手と対話するが、汎用ZKPは対話が不要なのでブロックチェーンに向いている。

zkSNARKやzkSTARKは汎用ZKPという分類になる

一般に・・・

zk-SNARKsは「証明の生成は遅いがProofのサイズが小さく検証が早い」

Trusted Setupが不要なSNARKもあるらしい

zk-STARKsは「証明の生成は早いが、Proofのサイズが大きく検証が遅い」

そもそも比較するものでもないという話もある

ゼロ知識証明の現在地 - 日本総研



汎用ZKPの基本プロトコル

汎用ZKPには、それぞれ特徴の異なる複数の基本プロトコルがあり、ユースケースの要件に応じて使い分ける必要がある。
（どのユースケース（P.13）にどのプロトコルが適するかは研究途上。）

	zk-SNARK (Zero-Knowledge Succinct Non-interactive Argument of Knowledge)	zk-STARK (Zero-Knowledge Scalable Transparent Argument of Knowledge)	BulletProof
Trusted Setup*（信頼されたセットアップ）	必要	不要	不要
Proof値のサイズ	・かなり小さい ・0.3～数キロバイト程度	・大きい ・50～数百キロバイト程度	・小さい ・数キロバイト程度
証明者がProof値を生成する時間	・早い ・数ミリ～数秒程度	・早い ・数ミリ～数秒程度	・かなり遅い ・数十秒程度
検証者がProof値を検証する時間	・早い ・数ミリ秒程度	・早い ・数ミリ秒程度	・遅い ・数秒程度
量子耐性	無	有	無
特徴	・Proof値が小さくブロックチェーンに格納が容易で、証明/検証の実行時間も効率的であるため幅広いユースケースに適する。 ・アプリケーション構築/運用時に「誰が」「いつ」「どのように」、"信頼されたセットアップ"を行うのか設計が必要である。	・量子耐性があり、依拠する暗号の仮定も少ないため、より安全性が高い。 ・"信頼されたセットアップ"が不要のため、構築/運用は、よりシンプルになる。 ・大規模なデータセットでは証明/検証時間が長くなる。 ・Proof値のサイズが大きくなるため、ブロックチェーンへの格納が難しく、スマートコントラクト上での検証などが高コストになる。	・Proof値が小さくブロックチェーンへの格納が容易。 ・"信頼されたセットアップ"が不要のため、構築/運用は、よりシンプルになる。 ・証明/検証の実行時間が長くなる。複雑なアプリケーションには向かず、現状は、範囲証明（送金額などがある値の範囲以下に収まっているかの証明）のユースケースが主。

表内のProof値サイズや時間については、証明したい知識の内容（アプリケーション）の複雑性や入力データセットのサイズによって大きく変動することに留意。
表の数値記載は、各種ベンチマーク資料を基に、認証などで用いられるような「あるハッシュ値の原像を知っていること」を証明するアプリケーションを想定し作成。
*:Trusted Setup（信頼されたセットアップ）とは、プロトコルが正しく機能するために必要な共通パラメータの生成プロセス。通常、複数の異なる利害関係者間で実施する。
利用者は、これら共通パラメータを基に証明鍵や検証鍵を生成し、管理する必要がある。このためZKPシステムは複雑になる。

© 2024 The Japan Research Institute, Limited

zkRollup

Understanding ZK Rollups: Validity Rollups and Ethereum Scalability