全面比较：什么是 zk-SNARKs 和 zk-STARKs？

来源：链登社区

什么是 zk-SNARKs 和 zk-STARKs？它们都是零知识证明，但它们的特性是什么，彼此之间如何比较。

零知识证明（ZKP）是加密协议，允许一方（证明者）在不透露任何超出声明本身有效性的信息的情况下，使另一方（验证者）相信某个声明是真实的。ZKP 是区块链生态系统的革命性技术，能够通过二层解决方案实现区块链的可扩展性，并构建隐私保护应用程序。两种最突出的 ZKP 类型是 zk-SNARKs 和 zk-STARKs，它们各自具有不同的特性和用例。

在本文中，我们将讨论 zk-SNARKs 和 zk-STARKs，它们的关键特性，以及它们之间的比较。

## 前提条件

理解 ZKPs: 你需要知道电路、约束、见证、验证者和证明者是什么。

## 什么是 zk-SNARK（简洁非交互知识论证）

Zk-SNARKs 是一类广泛的 ZKP 系统，它们是非交互的，这意味着在初始证明生成后，证明者和验证者之间没有来回通信。它们以高效著称，提供短小的证明大小和快速的验证时间，无论复杂性如何，这些都保持不变。

### zk-SNARKs 的关键特性

可信设置：SNARKs 需要一个可信的设置阶段，其中生成一组初始参数，通常称为结构化参考字符串（SRS）。这个设置阶段使用一个秘密，如果暴露，将会破坏所有使用该设置创建的后续证明的安全性。这个设置数据通常被称为“有毒废物”。可信设置通常被视为一个缺点，因为它们引入了潜在的信任问题：用户必须相信设置是正确执行的，并且秘密在之后被销毁。

椭圆曲线加密（ECC）：许多 SNARK 构造依赖于椭圆曲线加密，这取决于离散对数问题（DLP）的难度。虽然这对经典计算机提供了强大的安全性，但它使 SNARKs 可能容易受到未来量子计算机的攻击，因为量子计算机可以高效地解决 DLP。

### 流行的 zk-SNARK 协议

Groth16：Groth16 是最广泛使用的 SNARK 协议之一。它需要特定电路的可信设置，并且非常高效，生成非常小的证明和快速的验证时间。由于其紧凑的证明大小，它通常用于区块链项目，如 Zcash。

PLONK（基于拉格朗日基的普世非交互知识论证的置换论证）：PLONK 是一个更灵活的 SNARK 协议，使用通用和可更新的 SRS，这意味着它可以用于任何电路，并且可以修改以支持更大的电路。与 Groth16 不同，PLONK 的设置不是特定于任何特定电路的，可以重复使用多个电路。这减少了重复可信设置的需求，并且可以更容易地添加新程序或电路而无需重新进行整个设置。

### zk-SNARKs 的特性

证明大小：小，这使得 SNARKs 适用于带宽和存储有限的应用。

后量子安全性：有限，由于依赖于 ECC。SNARKs 不是量子抗性的，因为足够强大的量子计算机可能会解决 DLP。

可信设置：这是必需的（ 在大多数 SNARKs 中 ）。设置阶段引入了一个信任假设，如果管理不当，可能会带来潜在的安全风险。

可扩展性：对于需要紧凑证明和快速验证的应用程序非常高效，尽管需要可信设置在高度动态的环境中可能是一个限制。

## 什么是 zk-STARK（可扩展透明知识论证）

Zk-STARKs 是另一类 ZKP，旨在解决 zk-SNARKs 的缺点。它们被设计为可扩展和“透明”的，这意味着它们不需要可信的设置阶段。相反，zk-STARKs 使用哈希函数和公开已知的随机性来构建证明，从而增强了它们的安全性和可扩展性。

### zk-STARKs 的关键特性

透明设置：STARKs 不依赖于秘密参数。相反，它们的证明是使用公开随机性生成的，这意味着它们没有可能破坏系统的“有毒废物”，并且不需要可信设置。

基于哈希的安全性：STARKs 依赖于哈希函数 ，如 SHA-256，而不是椭圆曲线加密。这使得它们对量子攻击具有抵抗力，因为在当前的加密假设下，哈希函数被认为在量子计算机面前是安全的。

### STARKs 的特性

证明大小：STARK 证明可能比 SNARK 证明大几倍，这增加了验证时间，并且在带宽或存储有限的环境中是一个缺点。这是由于它们的透明性、使用多项式承诺以及实现可扩展性的方法。

后量子安全性：强。由于 STARKs 使用哈希函数而不是椭圆曲线加密，它们在当前的加密假设下不易受到量子攻击。

可信设置：不需要。STARKs 使用透明设置，消除了设置阶段的信任需求，增强了安全性。

可扩展性：高度可扩展，特别是对于大型计算，它们在复杂性增加时表现出更明显的性能优势。由于不需要可信设置，它们更加灵活，因为设置不需要为每个新应用或用例重新进行。

## zk-SNARKs 与 zk-STARKs 的比较

## 总结

Zk-SNARKs 是零知识证明系统。它们提供高效的证明大小和快速的验证时间，但需要可信设置，并使用椭圆曲线加密，使其易受量子攻击。

Zk-STARKs 则不需要可信设置。相反，它们依赖于哈希函数进行安全性（使其具有量子抗性），并且对于大型计算更具可扩展性。然而，它们的证明大小较大，对于较小的计算验证速度较慢。

这两种主要的 ZKP 对于在区块链生态系统中构建 ZK 协议至关重要，能够通过二层解决方案实现区块链的可扩展性，并构建隐私保护应用程序。