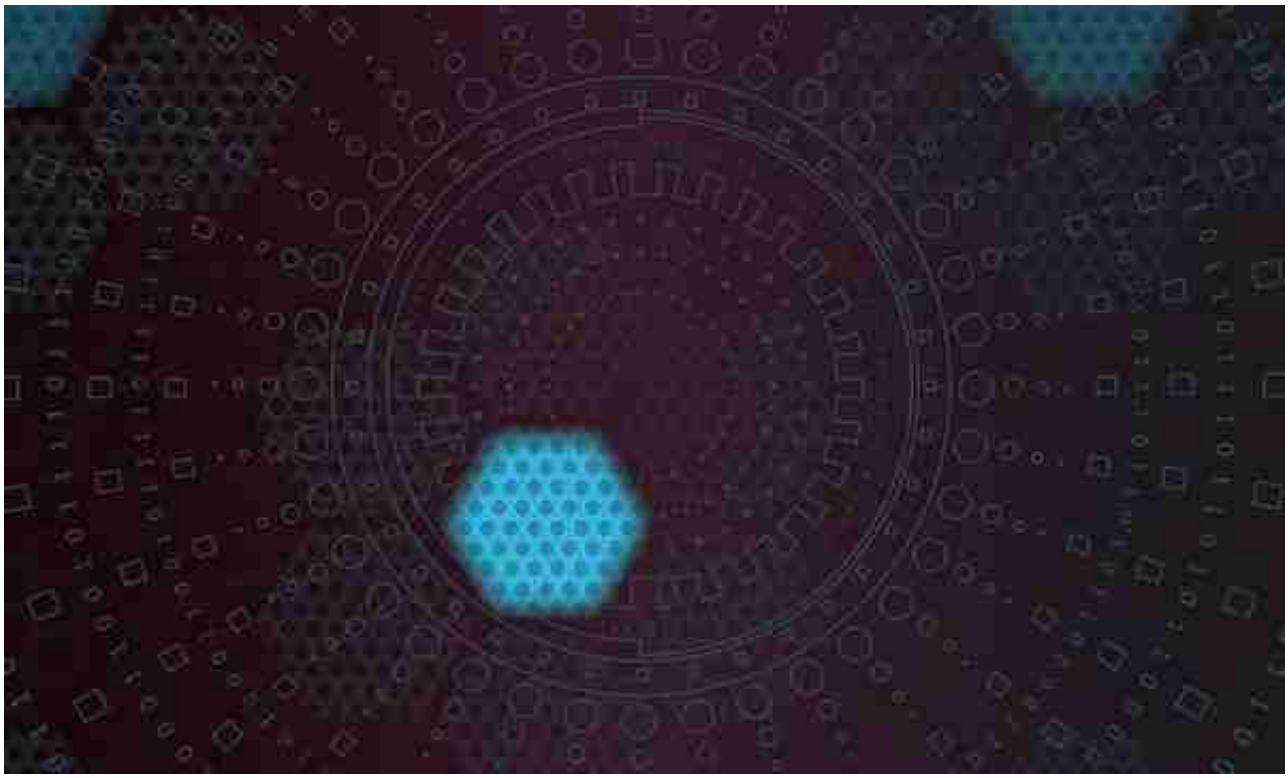
密码学的进步可能对区块链技术及其潜力产生深远的影响。我们将研究行业专家对最新密码学进展及其对加密货币的潜在影响的看法。



区块链公司Blockstream研究主管和数学家Andrew Poelstra表示，零知识证明（ZK-Proof）系统是密码学领域“最令人兴奋的发展领域之一”。众所周知，这种密码技术是隐私保护解决方案的基础。

ZK-Proofs是所谓的匿名币Zcash（ZEC）中包含的隐私保护技术的基础。根据Poelstra的说法，密码学家在这项技术的应用效率方面已取得了重大进展，现在“采用了更加健壮和公认的密码假设”。

区块链公司Suterusu目前正在致力于将ZK-Proof实现的隐私作为在比特币和以太坊的区块链之上的第二层解决方案。该公司的首席技术官Huang Lin（曾声称对密码学进行了十多年的研究）告诉Cointelegraph：

“将有效的零知识证明应用于分布式匿名支付时，可以显着改善其隐私和性能。”

Jelurida的联合创始人兼董事总经理Lior Yaffe（区块链NXT，Ardor和Ignis背后的公司）还表示，ZK-Proofs可以对可扩展性产生非常积极的影响。他解释说：

“矿工可以使用ZKP生成小的数据集，而不显示大量的交易并通过网络进行传播，而仅显示帐户余额变化以及一种证明没有发生双重支付的加密证明。”

Syscoin（SYS）的联合创始人兼首席核心开发人员Jag Sidhu说，新的递归ZK-Proofs可以允许更便宜，更小且与普通交易一样快的私人交易。

实现零知识证明的比特币侧链

过去，Poelstra表示ZK-Proofs还可以允许开发无需信任的侧链，这可能将山寨币的功能引入比特币（BTC）。在2019年2月，他在与《福布斯》交谈时阐明了这种系统的要求：

“我认为，现在，如果我们想做一个真正的双向锚定，我们可能需要获取完整，高效，通用的零知识证明，并且我们需要一种让比特币验证器能够验证在侧链上正在发生的事情的方法。”

当Cointelegraph向他询问基于ZK-Proof的无需信任的侧链的进展时，Poelstra解释说，在这样的系统变得可行之前，必须完成许多工作。他解释说，高效的ZK-Proofs将使您能够验证是否遵循了另一个区块链的规则，并以太坊扩展解决方案Plasma为例。

尽管如此，Poelstra还解释说，采用此类技术进行侧链验证“将需要效率更高许多个数量级的新证明系统。”此外，要实施这样的系统，研究人员首先需要解决复杂的激励问题。他总结说：

“作为一个社区，我们继续朝着这些目标迈进，但我们还有很长的路要走。”

虽然发展前景广阔，但到目前为止，比特币侧链仅取得了有限的成功。实际上，截至2019年10月中旬，只有近7700万美元的比特币（约占0.054％）被锁定在侧链上。同月，Blockstream首席执行官兼联合创始人亚当·巴克（Adam Back）表示，侧链开发缓慢的一个明显原因是，与在比特币上创建侧链相比，创建一种山寨币的财务激励更大。

零知识证明可以使比特币更加私密

Poelstra告诉Cointelegraph，ZK-Proofs还可以使比特币更具私密性，并以Taproot为例。他解释说，Taproot可以潜在地使任何交易在区块链上彼此之间几乎无法区分。他仍然指出，“交易额和交易图仍然存在，这是更难解决的问题。”

Lin解释说，Suterusu致力于开发和实施“免设置，高效的零知识证明计划，该计划具有几乎恒定的证明大小，专为智能合约平台中的机密支付量身定制。”

该公司的系统允许将加密资产从其第二层网络上的主要区块链中移出，并在隐藏“发送者和接收者身份以及交易金额”的同时进行移动。此外，该解决方案支持智能合约。他还表示，加密货币行业应更多地关注隐私。

后量子密码学

Sidhu还建议后量子密码学（Post-quantum cryptography是指可以抵抗量子计算机攻击的密码算法）的最新发展值得研究。这种密码学的重点是确保一旦量子计算成熟，仍然可以对数据进行加密并保护其安全。 它还消除了人们对量子计算的最新进展可能导致加密货币终结的担忧。

通常，后量子密码设计算法的目的是要使量子计算与传统计算相比没有优势。他还建议比特币在设计时要考虑到量子计算的威胁：

“中本聪看到了这种情况的出现，这就是为什么他创建一种以哈希方式作为地址而不是公共密钥的原因，因为公共密钥密码技术容易受到量子暴力攻击。[...]这也是为什么每个钱包都有一个更改地址策略的原因。”

密码学的发展及其对加密货币的影响

Yaffe说，多方计算（MPC）是密码学研究中最活跃的领域之一。他通过以下方式解释了MPC对Cointelegraph的功能：

“MPC使那些彼此不信任甚至可能容易被疏忽或存在恶意的实体能够一起执行计算并就结果达成共识。”

区块链的共识算法是MPC的一个例子，这一领域的进展可以给加密货币领域带来不同的进展。 Yaffe还引用了可验证延迟函数（VDF）作为另一项重大进展，解释说它类似于允许进行工作量证明（PoW）挖矿的算法，“但是与挖矿不同，VDF无法并行化为小矿工均衡竞争环境而打开潜力的可能性。”Yaffe与Cointelegraph分享了他对未来区块链将如何工作的预测：

“使用以上所有内容，我预计未来的区块链产品将为外部查看者提供类似的信息，而实际持有密钥的用户将能够查看其交易的全部历史记录。这些技术中的一些还没有为主流使用做好准备，但是在最近几年中，该领域有了许多改进，并且还在不断改进。”

Sidhu的Syscoin桥技术虽然不是侧链，但允许用户仅凭密码原理就无需中间人或保管就可以跨区块链转移价值。他解释说：

“这是朝着我们所拥有的跨链共识愿景的方向迈出的一步，用户应该能够自由地在具有各种属性（例如链的安全性，便利性（性能）和技术特征）的任何链之间移动。”

Poelstra还引用了交互式多重签名，并解释说，这种技术显着简化了闪电网络正常运行所需的复杂合约，例如托管费用或哈希时间锁合同。更准确地说，这种加密技术允许将此类合约表达为一种单签名。