探讨 Taproot Assets 与闪电网络的结合及其意义

作者：Ben77 来源：X，@blapta

Taproot Assets和闪电网络结合的部分已经正式上线，这是一项备受期待的新能力。很多人认为这将使闪电网络具备类似以太坊的生态系统，但这种认知存在误区。作为Taproot Assets的贡献者之一，我与作者roasbeef常讨论相关设计。今天，我将为大家介绍一些关于Taproot Assets的重要知识点。

## 1. Taproot Assets只能做转账吗？

理论上是的。Taproot Assets的状态树是一种仅与金额相关并由单一资产绑定的稀疏默克尔树。如果需要智能合约的能力，理论上它没有额外的状态可验证机制可用。采用这种状态树设计是为了在用户进行转账时，仅需关注自己相关树分支的变更。

## 2. Taproot Assets能在Bitcoin主网实现交易所吗？

Taproot Assets与Runes、BRC20等最大的差异在于其资产验证由TAPD客户端处理，其VPSBT是一种链下的转移规则。换句话说，Taproot Assets的资产所有权并不是通过其Anchor的UTXO所有权转移便可实现。目前市面上基于Bitcoin级别的PSBT的DEX并不能直接接入Taproot Assets。

## 3. Taproot Assets相对于其他Bitcoin资产来说，安全性更强

Taproot Assets在安全性上有显著优势，资产的转移验证可以由用户自己进行，而不需要完全依赖某一单方面的indexer。用户可以选择加入多个universe进行同步，通过这些universe同步的数据进行验证。

## 4. Taproot Assets与Lightning结合后的最大用例是什么？

Taproot Assets与Lightning结合后的最大用例是现实生活中的稳定币支付，而不是资产的炒作和买卖。所有的通道技术都是建立在流动性锁定上，也就是说，用户和交易对手一开始都要有同样的资产进行锁定。因此，NFT类资产不可能在通道内流通，因为用户和对手不可能拥有同一个NFT资产。

## 5. 普通用户该如何接入Taproot Assets？

所有用户都需要拥有自己的TAPD节点。由于TAPD并没有本地私钥，最终由LN控制，所以用户需要同时拥有TAPD和LND节点。这需要专门定制的非托管钱包来帮助用户进行构建。既然使用了客户端验证的资产，如果客户端不在用户手里，那也没有意义，这样的做法也只是挂羊头卖狗肉。

通过以上对Taproot Assets的介绍，希望能够帮助大家更好地理解其功能和潜力。作为新兴技术，它的实际应用还在不断探索中，但其设计理念和安全性为其未来发展提供了坚实基础。