Taproot Assets：稳定币赛道超越万亿市值的下一个增长点

作者：Evan, Peter, Boris, Haozhe

区块链本质是支付场景的延伸。就支付场景而言，稳定币不仅在加密货币市场中占据重要地位，并且在全球支付、跨境结算等方面正发挥着越来越重要的作用。目前，中心化稳定币市场仍然占据 90% 以上的市场份额。其中，泰达（Tether）公司发行的USDT占据稳定币中绝对的统治地位。此外，尽管稳定币已经发行了超过1500亿美元，但根据2024年美联储报告的M1数量20万亿美元（包括所有流通中的现金、旅行支票、活期存款账户中的资金等）来说，稳定币市值仅是M1的0.75%。稳定币在支付上的应用仍然任重而道远。Taproot Assets协议的推出预示着稳定币出现在高频小额的支付场景中具有广阔的想象空间，也预示使用稳定币作为常规支付手段的大规模采用成为可能。

一、稳定币是未来的下一个万亿美元赛道

稳定币市场的蓬勃发展标志着其赛道成为未来金融领域的一个万亿美元市场的潜力。当前，稳定币市值已超过1600亿美元，日交易量更是高达1000亿美元以上。主流国家纷纷出台稳定币相关的政策法规；同时，多方机构预测稳定币将引来新的万亿市场，并且新的增量市场主要来自于稳定币在全球化支付的广泛应用。

稳定币可以分为中心化稳定币和去中心化稳定币两大类；其中去中心化稳定币又可以被细分为算法稳定币和抵押加密资产进行发行的稳定币，以及两者兼之的类型。目前中心化稳定币占据市场绝对的统治地位，两大巨头USDT和USDC——Tether和Circle分别发行了发行了1144.6亿美元和341.5亿美元数量的美元稳定币。其中Tether更以125人的公司规模，一年毛利就有45亿美元。如此诱人的机会自然也吸引了许多大机构进场布局：

贝莱德在以太坊上发行了代币化基金BUILD，该基金旨在提供稳定价值并赚取收益，成为市值达3.84亿美元的大型代币化基金。

7 月 24 日，据财联社报道，京东币链科技 (香港) 将在香港发行与港元 1:1 锚定的加密货币稳定币。

中心化稳定币已然实现在加密生态中的广泛采用，我们日常在DEX或CEX的交易和结算都是透过中心化的稳定币来进行结算和交易；而去中心化稳定币背后的抵押资产多为加密资产，通常用于借贷。

虽然稳定币在加密货币的交易和DeFi中发挥了重要的作用，但是它跟实体商业相结合的探索还非常早期。从长远来看，稳定币最有潜力的应用场景在于支付领域，尤其是跨境支付。目前，跨境支付涉及多个中介机构，包括发卡行、支付网关、支付处理器等复杂流程，不仅费用高昂，而且结算时间漫长。而稳定币不仅仅是另一种更优选择，更是是经济参与的重要渠道。随着稳定币监管逐渐向合规化发展，其在全球支付场景中的地位将愈发重要。不仅如此，未来伴随稳定币在支付场景的大规模采用，更能与DeFi融合催生出Pay Fi，实现支付场景中的互操作性、可编程性和可组合型，形成传统金融无法实现的新金融范式和产品体验。

二、Taproot Assets协议+闪电网络有望成为全球性支付网络的基础设施

目前稳定币主要流通于ETH和TRON区块链网络，但是他们手续费一般会超过1U，链上转账时间超过1分钟。相比之下，闪电网络（Lightning Network）具有更快速、低成本和高扩展性的优势。

2.1 什么是闪电网络？

闪电网络是比特币网络第一个比较成熟的二层拓展方案。在闪电网络的白皮书问世之后，多个团队开始独立地开发闪电网络，包括Lightning Labs、Blockstream和ACINQ等。而Taproot Assets正是Lightning Labs 开发的一个资产发行协议。

那具体是如何实现呢？双方先是建立起一个双向流通的状态通道（State Channel），发起支付的双方A和B在链上创建一个2-2多签的地址，使得A和B都可以从这个新地址转出或者转入限额内的比特币。在转出之前，双方发送一些锁定数据并记账，形成交易支付，可以多次往来支付。直到交易记账结束，双方结算，新地址的比特币按结算数量被转给双方。因此，只有最新版本才是有效的，这是由哈希时间锁合约（HTLC）实现并强制执行的。任何一方都可以通过将最新版本广播到区块链来随时关闭此条目，而无需任何信任或托管。

因此，双方可以不受限制地进行链下交易，并使用比特币链作为仲裁者，但最终交易完成后或者交易有一方出现错误的情况（比如其中一方钱包里余额不足）出现时，智能合约才会介入并在区块链上执行。这类似于A与B签订许多法律合同，但不会每次签订合同时都上法庭，只有最终的合同确认后或者不合作的情况发生时，法院才会介入。

2.2 闪电网络成为稳定币全球化支付最好的基础设施

也就是说，用户可以在链下互相发送无限次的交易，而且也不会对比特币本身的网络造成拥堵；同时，还能依托于比特币网络的安全性。理论上来说，闪电网络的 Scalability（可扩展性）没有上限。

目前为止，闪电网络运行了9年，并建立在目前加密生态中最具安全性的网络之上——比特币网络（拥有超过57000+节点和Pow工作量证明机制），能够最大程度地确保闪电网络的安全性。

截止当前，闪电网络已经超过5000个比特币的容量，全球18000+个节点，50000+个通道；通过建立双向支付通道实现了即时且低成本的交易，闪电网络正在全球范围内被大量的支付商、商家集成和使用，正在逐渐成为全球化支付最广泛共识的去中心化解决方案。



比特币资产占据加密市值的半壁江山，伴随此轮周期回归比特币生态的热潮；闪电网络作为第一个比特币的二层扩展解决方案，真正解决了中本聪所构建的点对点全球化支付的设想。闪电网络已然成为最正统性、共识最强的比特币社区，是理想中的全球化支付最佳解决方案。

2.3 Taproot Assets协议补齐了闪电网络的最后一公里

美中不足的是，在Taproot Assets协议出现之前，闪电网络仅支持比特币作为支付用的货币，应用场景非常的局限。在比特币已然成为数字黄金的今天，绝大部分人不愿意付出自己的比特币。

尽管之前已经有一些比特币一层的发行协议了，例如Atomical，基于Odinals的BRC20，但他们都不支持直接进入闪电网络，Taproot Assets协议的推出刚好可以解决这个问题。它是Lightning Labs 所主导研发，基于BTC网络的资产发行协议。与Odrinals协议一样，任何人或者机构都可以使用Taproot Assets协议发行自己的代币，同样也支持发行法币对应的稳定币，如USD，AUD，CAD，HKD对应的稳定币等。

相对于其他资产协议的优势是，Taproot Assets协议的资产将跟闪电网络完全兼容，使得在闪电网络上使用稳定币进行支付成为可能。因此意味着未来将会有大量基于比特币网络发行的新资产（特别是稳定币）会流通到闪电网络，此举反过来又赋能了闪电网络在全球范围内的支付布局和影响力。

依赖于比特币的安全性和去中心化，Lightning Labs 所提倡的“让美元和世界金融资产比特币化”正在成为现实。Taproot Assets主网协议的上线，意味着稳定币的万亿支付场景已正式拉开帷幕。

三、Taproot Assets协议（以下简称TA）详解

TA协议的运作原理深植于比特币的UTXO模型，并且其实现依托于比特币网络的Taproot升级。其两者作为TA协议的最核心元素，驱动着协议的有效运行。

3.1 UTXO模型和Account模型的异同与利弊

UTXO（未花费交易输出）是一个很重要的概念，它是所有比特币二层和Ordi，Runes协议实现的基础；事实上，几乎绝大部分的公链如以太坊和Solana都采用的Account（账户）模型。以下是两者的概念的诠释和对比：



账户模型很好理解，就和我们的支付宝账户一样；每一笔收入和支出，对应到个人的直观感受就是账户界面里数字的变化。

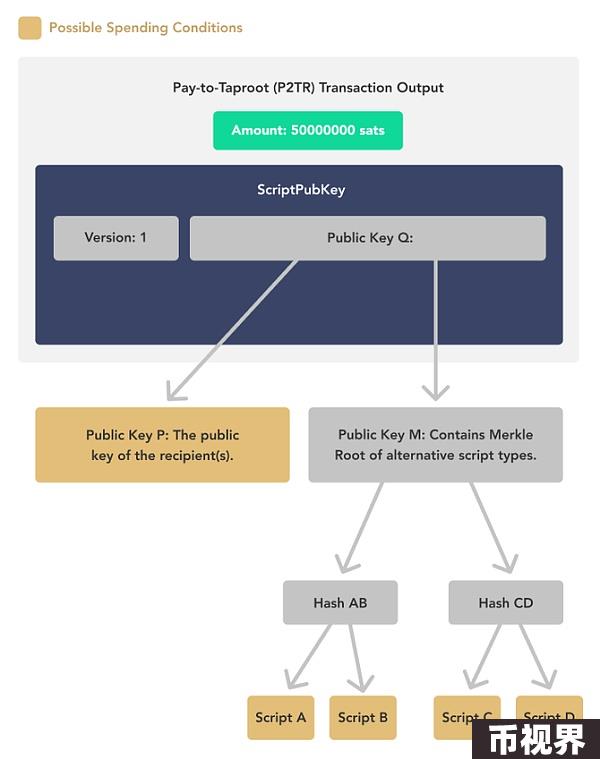
UTXO模型可以理解为某个人“A”的一个钱包。里面存放着B,C,D授权给A可以兑换的支票，也包含A授权给E，F，G可供兑换的支票；此时A钱包的余额=（B，C，D给A的支票面值）-（A给E，F，G的支票面值）。比特币网络就相当于可以承兑这些支票的银行，它可以通过用户互相交易这些支票的最新情况来计算每个用户地址里的最新余额。

由于UTXO模型的独特性质，它天然排除了双花问题，相较于基于账户的模型，提供了更高的安全保障。此外，TA协议完全继承了比特币网络层的安全特性，避免了错误转账或漏转的风险。

此外，TA协议采用了一次性密封的概念，即每一笔UTXO确认花费后就不可以再次使用；确保了资产随UTXO移动。在这种机制下，挖到最长链的矿工拥有对该UTXO的最终解释权，并能支配其使用。与依赖链下索引识别资产的BRC20不同，TA协议增强了交易的安全性，避免了双花攻击，同时也消除了中心化机构可能导致的错误或恶意行为的风险。这些特性使得TA协议+闪电网络成为了一个可靠的支付场景基础设施。

3.2 Taproot升级，实现更复杂的功能

2021年的Taproot协议升级为比特币网络带来了简单的智能合约功能，比如P2TR格式的钱包地址能够通过Bitscript实现一些较为复杂的逻辑，让新的、复杂的交易类型在链上成为可能。Taproot升级的示意如下图：



Taproot Mechanism, River: https://river.com/learn/what-is-taproot/

其中最关键的改进是实现了多重签名（多签）。这一功能使机构用户的交易更为安全，在公钥地址上，多签地址与私人钱包地址的长度相同，外界无法区分，从而增强了安全性和隐私保护。这一技术进步也为机构与B2B（企业对企业）交易提供了坚实的基础，推动了更广泛的商业应用。

呈现在用户前最直观的感受就是钱包地址的格式变化，以“bc1p…”为开头的钱包地址即已经支持Taproot升级后的钱包地址。

3.3 TA技术原理

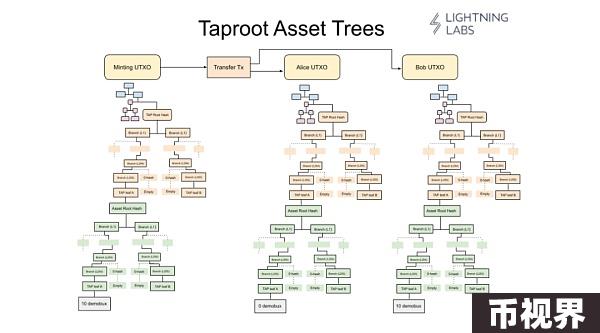
起初，点燃比特币生态的Ordinal与衍生的BRC20协议都基于账户模型，余额与地址绑定；资产的发行是通过加入特定的标识或数据来“标记”比特币的最小单位“聪”（Satoshi），将“聪”映射为某种资产发生的，而资产状态对应的数据以JSON 格式存储在区块里的隔离见证部分（保存交易签名或见证数据的地方）中。一旦双方发生资产交易，记录资产变化的脚本就会被“铭刻”（Inscribe）进区块中，并通过链下索引器（Indexer）解释。

然而，这种做法会导致每笔Ordinals会BRC20资产的交易发生都需要被记录在区块中，这会使区块体积增大，导致无效数据积累并永久存储在比特币链上，最终对全节点的数据存储造成越来越大的压力。相比之下，TA协议采用了更为高效的方法，资产被标记在每个UTXO上，仅在链上存储脚本树的根哈希，脚本则被保存在链下。

此外，TA资产可以被存入闪电网络的支付通道中，并通过现有的闪电网络进行转移，意味着TA资产是可以在BTC主网和闪电网络流通的新型资产。

顾名思义，Taproot Assets是利用了比特币的Taproot升级（BIP 341）开发的协议。Taproot升级使得花费一个UTXO，既可以使用原本的私钥，也可以使用默克尔树上的一个脚本。

简而言之，Taproot Assets协议在Taproot升级之上进行扩展，将资产状态的转换记录在Taproot的默克尔树上；同时，利用比特币UTXO“一次性密封”的特质，在BTC链上取得资产状态转换的共识，这也使得Taproot Assets协议不需要运行其他协议的链下索引器（Indexer）。Taproot Assets协议使用了下图的资产管理结构，采用了稀疏默克尔求和树（Merkle-Sum Sparse Merkle Tree, MS-SMT）来管理资产状态，Taproot Assets协议定义了资产状态转换所要遵循的标准。



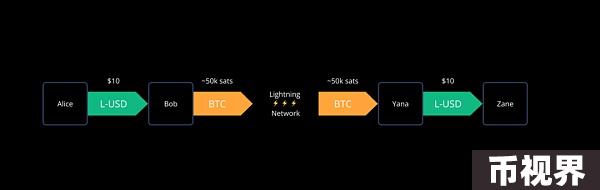
Taproot Assets Trees, Lightning Labs: https://docs.lightning.engineering/the-lightning-network/taproot-assets/taproot-assets-protocol

需要注意的是，并不是默克尔树的所有数据都写入到比特币链上，写入到链上的仅仅是默克尔树的根哈希。也就是说，无论资产数据多么庞大，比特币链上的交易长度不变，从这点来说，Taproot Assets是一个不污染比特币链的协议。

3.4 TA协议与闪电网络的关系

在Lightning Labs的最新产品发布中，Taproot Assets协议资产已可以无缝进入到比特币二层闪电网络里，这是通过TA通道（Taproot Assets Channel）实现的。之前的闪电网络一直是一个点对点的比特币支付网络，网络里面除了比特币之外，没有其他的加密资产流通。Taproot Assets协议的出现改变了这个情况，允许在比特币主链上通过Taproot Assets协议发行资产，尤其是稳定币，然后资产进入闪电网络里进行流通。

如下图所示，通过Taproot Assets协议发行了稳定币资产L-USD，Alice将价值$10的L-USD通过闪电网络转给了Zane。



An example of a Taproot Assets payment made to the wider Lightning Network, Lightning Labs: https://docs.lightning.engineering/the-lightning-network/taproot-assets/taproot-assets-on-lightning

TA通道的实现原理和状态通道（State Channel）一样，也是基于哈希时间锁合约。因为Taproot Assets资产本身就是在一个UTXO内，那么TA通道的实现机制并没有变，只是之前Channel只能流通比特币，而现在的Channel还支持流通TA资产。TA协议使得通过闪电网络流通比特币以外的资产成为可能，实现了稳定币等资产在闪电网络上的无缝转移。

3.5 用户使用成本过高，中心化托管问题仍需解决

尽管TA协议仅记录每笔交易的根哈希在链上以保证比特币链的简洁，然而这样做的代价却是资产数据需要保存在链下每一个客户端上。同RGB协议一样，需要客户端验证（CSV）资产的有效性。如果用户想要像使用BTC一样使用Taproot Assets资产，一是要有资产对应的UTXO（Virtual UTXO）的私钥（key），二是要有默克尔树上该资产的相关数据。

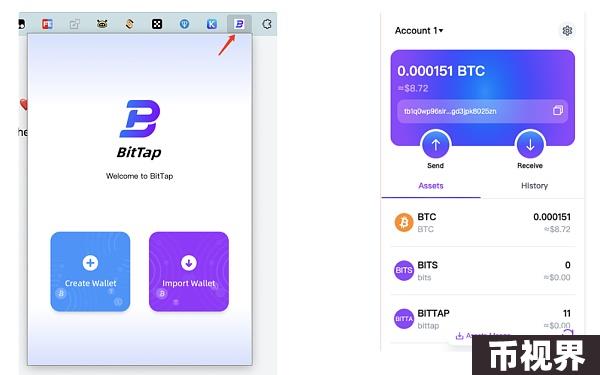
同时，Taproot Assets协议的官方实现（Tapd）深度依赖于闪电节点 （LND）的钱包服务，且无账户管理机制，闪电网络独特的架构决定了它的去中心化方式就是用户自建节点，而普通用户很难参与节点的搭建，这也是闪电网络仍未大规模普及的重要原因之一。

所以目前闪电网络上的钱包服务基本上都是托管钱包的解决方案，也就意味着TA发行的新资产也会被储存在托管钱包内。未来当TA资产上流通大量稳定币时，大额的资产会优先选择存储在TA上，也就是比特币主网上，因为主网上的安全性更高、共识度最强；只有小额资产、零钱才会充值到闪电网络来满足支付的需求。所以对于大额资产的存储和安全管理，用更加去中心化的方式让用户可以完全拥有稳定币所有权就显得尤为重要。

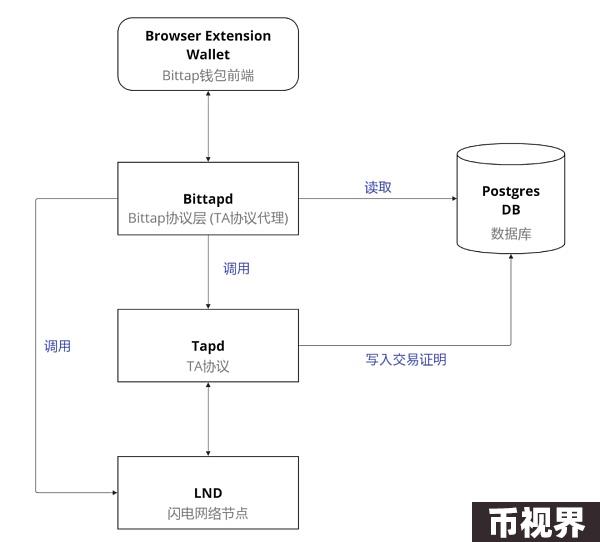
四、自托管解决方案——补齐闪电支付网络的最后一块拼图

目前市场上已经出现了多种团队针对TA资产在闪电网络上流通的去中心化解决方案。例如，LnFi提出了一种云托管方案，可以让用户轻松部署自己的闪电网络节点，有效降低了用户的参与门槛。

以及专注于做TA协议生态去中心化基础设施的BitTap团队，研发了TA的去中心化浏览器插件钱包，为TA上的用户提供了自托管钱包的权利。



BitTap提出的的创新钱包协议（Bittapd），用户的私钥完全掌握在钱包用户手里，在需要对交易签名时由Bittapd代表用户与Tapd进行交互，进而用户可以享受到类似Metamask钱包一样完全去中心化的体验和安全保障。待稳定币在TA上发行和流通时，用户可以利用BitTap钱包来存储和转移在BTC主网上的稳定币资产，并且可以自由支配将零钱转移到闪电网络。BitTap的技术原理如下所示：



BitTap wallet architecture, Bittap Docs: https://doc.bittap.org/developer-guides/overview

Bittapd协议相当于是TA协议的去中心化代理，它将Tapd原生的中心化托管式账户体系变成了去中心化的解决方案；也充当了插件钱包用户在交易请求时的网络通信和转发任务的角色。

五、总结

稳定币在全球范围内获得了广泛关注和应用，逐渐从加密货币交易的狭义场景扩展为全球化支付的重要选择。闪电网络（Lightning Network）凭借其低费用、快速交易的特点，成为实现全球支付的理想基础设施，与此同时，Taproot Assets协议的推出进一步增强了闪电网络的功能，使得在比特币网络上发行和流通稳定币成为现实。这一协议解决了比特币波动性较大的问题，显著提升了其在支付领域的适用性。

此外，针对闪电网络及其钱包服务的中心化问题，市场上出现了如BitTap团队开发的去中心化钱包解决方案，为用户提供了更为安全和去中心化的资产管理方式。补齐了Taproot Assets+闪电网络成为全球性支付设施的最后一块拼图。

尽管传统支付基础设施如Alipay、PayPal和Stripe利用本身的交易量，庞大的用户数，和政府合作并受其监管，以及品牌知名度作为背书，但它们托管的特性，和依赖于复杂的互联网和银行系统仍会导致其效率低下，和恶意行为或面临政府制裁的可能发生。此外，在跨境支付领域，由于受到严格的监管政策和机构本身的限制，支付账户往往会受到归属地和转账额度的制约。这些因素共同影响了传统支付方式的安全性和灵活性。

TA协议+闪电网络组成的支付基础设施不仅在即时性比肩传统支付机构；并且通过精巧的代码设计实现了支付的去可信化，同时生态中的自托管解决方案保障了用户对资产的自主权，能支持TA协议代币随时随地，无限制条件的自由转账；将支付自由度提升到了一个前所未有的高度。