状态通道专题研究

2018.6.21

引言

状态通道是区块链扩容的热门方向之一， 也是目前投资的热点。 状态通道与子链、侧链等一起被归类为 Layer 2 的扩容方案。同时，状态通道也是实现跨链互通性的潜在途径。对于许多纯粹的去中心化的信仰者来说，状态通道可以在保证 Layer 1 完全去中心化的前提下，在 Layer 2 将交易提速到 DApp 可以大规模应用的性能量级，因此该方向是比特币、以太坊等以牺牲性能保证去中心化的公链扩容的关键。

节点研究中心

作者 蔡晨曦 布朗大学经济学硕士 亚利桑那州立大学 MBA 在读

编辑 郎瀚威 研究中心负责人

支持媒体

金色财经 BlockMasterMail

目录

1 状态通道的概念

状态通道领域的总体思路是将本来在链上结算的交易在链下通过状态通道维护中间态，并且在发生纠纷时回到链上仲裁。链上仲裁的公平性和安全性在博弈论上保证了链下交易的对手不会作恶。

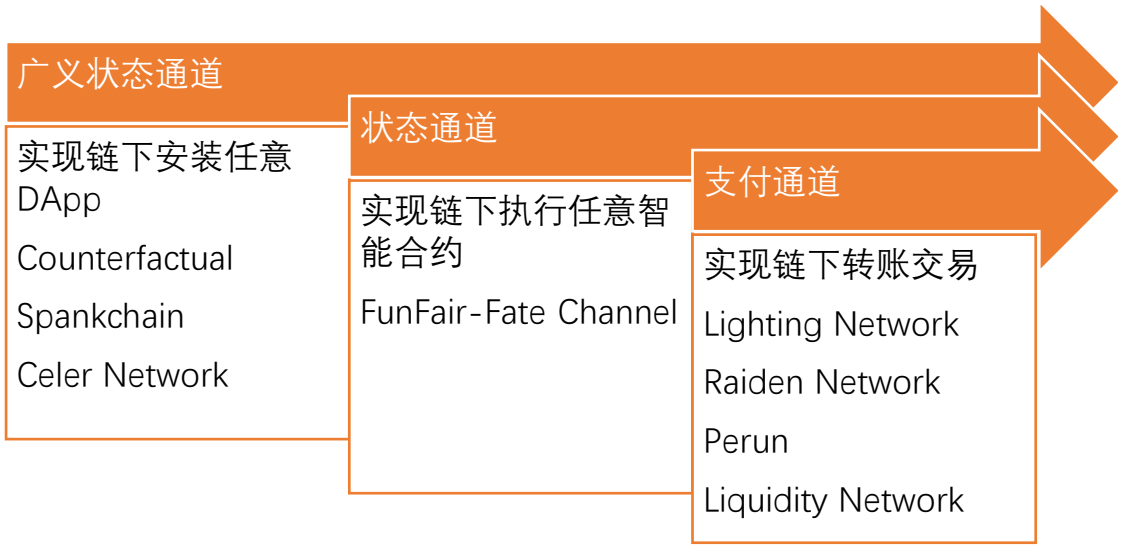
状态通道的交易流程一般如下：交易对手将一定的链上状态锁定在链上，然后在链下开辟状态通道进行状态交换，以实现零手续费及瞬时到账等特征，同时允许参与者在对手作恶时将之前的状态提交链上仲裁，以保证链下交易的安全性。一般来说，链上状态锁定的方式是多重签名钱包。

状态通道的思想很大程度上类似于淘宝卖家的信用担保：卖家支付一定的押金抵押给平台，买家在收到货物之前先支付货款给平台，如果收到货物一段时间之后没有提出异议货款就放行给卖家，如果没有按交易规则收到货物买家可以提出平台仲裁。所不同的是，原有中心化平台的功能，包括接受抵押款、履行交易规则、异议仲裁、链上结算等都由智能合约执行。

在应用中，一条状态通道可以由 2 方共同开启，也可以由多方共同开启。多方开启的通道可以应用于需要多人参与的 DApp，比如卡牌类游戏。

2 状态通道的几个层级

状态通道也分几个层级，对应着不同程度的链上功能替代度，概括如下图。



支付通道可以实现链下转账交易的功能，也是目前正在落地中的应用，由支付通道形成的支付网络可以通过通道间的虚拟连接在任意两个节点处实现瞬时转账。

状态通道可以将任何已经部署到链上的图灵完备智能合约放到链下执行，这样智能合约在执行的过程中不需要消耗 gas，而且速度奇快。

广义状态通道是该领域最前沿的方向，也即允许在已开辟的状态通道中安装、运行和终止 DApp 而不用执行任何链上操作。这是状态通道最终极的目标。

3 状态通道类项目的问题

3.1 保证金锁定的成本

目前状态通道项目类项目最大的挑战是需要锁定大量保证金的问题。举例来说，如果平均每笔交易金额为 1 个比特币，网络上有 1 万个节点，那么每个节点至少得存一个比特币作为保证金，总共就需要 1 万个比特币的保证金。这么大额的保证金的机会成本是非常高昂的，所以状态通道尽管在技术上实现了零手续费，仍然无法在经济模型上实现零交易费用。

3.2 状态通道平衡

此外，状态通道平衡也是个很大的技术挑战。举例来说，两个节点 A 和 B 之间，从 A 到 B 的交易和从 B 到 A 的交易总量只有相等的时候，A 和 B 才能达到均衡的状态，不会有其中一方的金额逐渐变为 0。一旦一个通道的一方金额变为 0，那么这个通道就会变成单向的，反向交易就不能继续进行，从而影响网络的连通性。

3.3 节点掉线的状态维护

状态通道的维护要求节点一定要在线，如果发生了节点被攻击或自行下线，那么原来的状态会发生丢失。比如，在游戏的过程中，落后的一方有可能选择自行下线，或者把领先一方 DDoS 下线。因此，状态通道需要额外的机制来保证节点在下线时能维护原来的状态。

4 状态通道项目的分类和对比

层级	项目名称	支持公链	主网上线时间	描述	团队背景
支付通道	Lightning Network	RSK	2018 Q2	比特币支付网络，最先上线的状态通道类项目	Blockstream
	Raiden Network	ETH, RSK	-	以太坊支付网络	德国公司
	Perun	ETH	2018 Q3	以太坊支付网络，支持虚拟支付通道，中间路由节点不需要参与交易过程	德国/波兰大学教授
	Liquidity Network	ETH, RSK, others	2018 Q2	以太坊支付网络及去中心化交易所，利用liquidity hub和通道平衡技术增加支付网络流动性	ETH Zurich研究者
状态通道	FunFair	ETH	封闭Beta测试版已上线	博彩平台，独有的随机数生成机制保证状态通道中游戏进程的随机性	英国游戏业开发者
广义状态通道	Counterfactual	ETH	-	研究项目，实现以太坊上的广义状态通道	L4 Ventures
	Spankchain	ETH	-	成人娱乐平台，是第一个将Counterfactual实现成PoC的项目	原Consensys开发者
	Celer Network	-	-	综合DApp平台，提出一套最优的通道平衡技术，同时利用侧链对状态通道进行补充	硅谷工程师

在项目进度方面，目前主网已经上线的项目是 Lightning Network，有最小可用产品的是 Liquidity Network，在公测阶段的有 FunFair，其余项目仍在开发过程中。

在保证金锁定方面，Liquidity Network 提出了节点间使用 Hub 进行流动性共享的机制，试图减少保证金锁定的问题。Hub 的作用类似于银行，本质是利用 Hub 间的交易可以互相抵消减少每个用户的保证金锁定。Celer Network 提出了类似的链下流动性提供者（OSP）机制，允许 OSP 通过智能合约拍卖从代币持有者处租借获得流动性。

在状态通道平衡方面，Liquidity Network 提出了经过同行评审的 Revive 的方法进行状态通道平衡；而 Celer Network 在白皮书中提出了一套分布式背压导流的算法(cRoute)，号称性能最优，但没有对算法的安全性进行评估。

在节点的掉线维护方面，Celer Network 提出了由状态守护者组成的侧链来维护状态，状态守护者需要抵押 CELR 代币以防止作恶，并且从节点处获得 CELR 代币作为激励。

5 状态通道类项目的投资逻辑

5.1 应用场景

1）交易所或钱包间进行交易

交易所或钱包类的实体有大量沉淀闲置存款，并且之间的交易长期可以双向抵消，因此更适合接入基于状态通道的支付网络。

2）博彩平台

依靠概率的博彩类项目，玩家互相之间有赢有输，总体来说可以大体互相抵消(不考虑平台的 take)，也很适合作为应用场景。

3）高频小额交易

对单次交易费用敏感的高频小额交易适合用状态通道，如直播打赏、IoT 设备、打印服务等。

5.2 节点激励机制

由于状态通道存在正向网络效应，每条通道可以服务开辟通道节点之外的大量节点，对运行状态通道的节点是否有合理的经济激励机制也是项目需要重点关注的方面。

6 节点研究中心介绍

关于节点研究中心


创始合伙人
杜均


管理合伙人
杨玉梅


研究中心负责人
郎瀚威

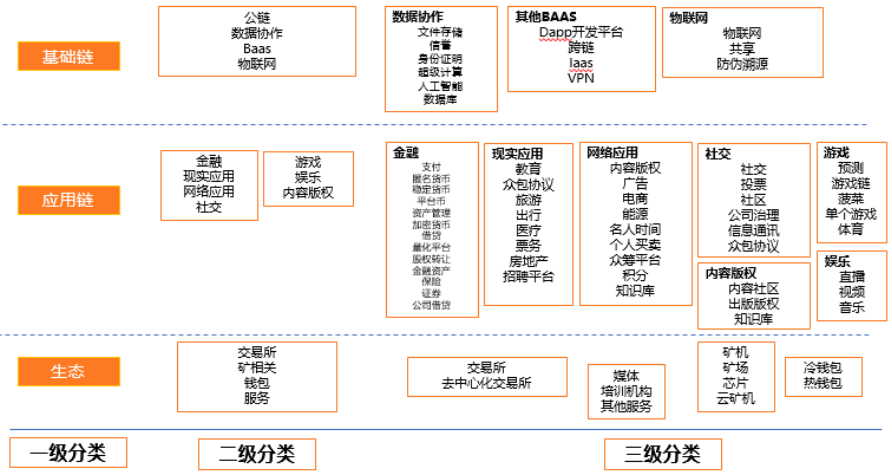

分析师
朱子川


分析师
武怡


助理分析师
蔡晨曦

- 节点研究中心 专注于区块链行业分析与投资
- 团队氛围良好 高效友善开放活泼 分析组成员来自清北复及海外高校
- 简历投递：langhanwei@nodecap.com

节点资本项目分类



本报告中的数据信息来自于公开资料，本公司对这些信息的准确性和完整性不做任何保证。报告中的内容和意见仅反映本公司于发布本报告当日的判断，不保证所包含的内容和意见不发生变化。

本评级报告仅供参考，不构成投资建议。在任何情况下，本报告中的信息或所表述的意见均不构成对任何人的买卖建议，任何直接或间接基于本报告所做出的投资行为，需自行承担全部风险，我公司及其雇员对任何人使用本报告及其内容所引发的任何直接或间接损失概不负责。