区块链的扩容方案和主要的二层网络 (Layer 2) 方案

原创: 白话区块链 白话区块链

作者 | JackyLHH 出品 | 白话区块链 (ID: hellobtc)

今年的"双 11"全民购物狂欢节,根据阿里云公布的数据,订单创建峰值创下了新的纪录,达到了每秒 54.4 万笔,远远超过去年的每秒 49.1 万笔,是 2009 年第一次"双11"的 1360 多倍。

这就是中心化系统的优势。

相比之下,去中心化的区块链技术,在性能上就相形见绌了: 比特市区块链每秒只能处理大约 7 笔交易,以太坊区块链每秒能处理约十几笔交易,<u>当初打着"百万 TPS"旗帜的 EOS 区块链</u>在测试中的最高 TPS 也只有四五千,平时运行时的 TPS 只有两位数。



EOS 区块链实时 TPS 只有两位数 来源: eosflare.io

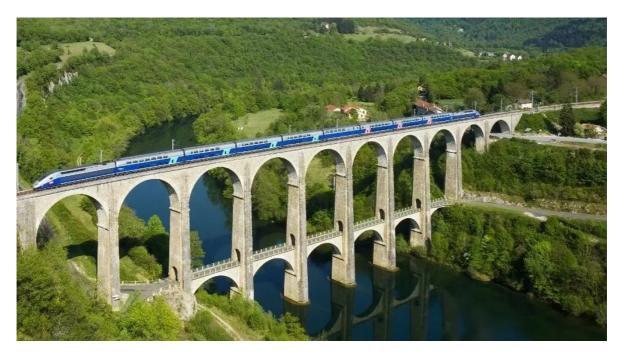
虽然性能并不是区块链技术的优势,但如果成为"短板",毫无疑问会推迟区块链技术的大规模应用。

所以近年来,不断有技术开发人员和项目团队提出各种各样的解决方案。这些解决方案,主要可以分为两大类: 链上扩容和链下扩容。

链上扩容,就是直接在区块链上"动手术"——修改规则,包括区块大小、共识机制等等。比如,将比特币区块链的区块大小直接从 1M 扩容到 32M、128M 甚至是 2G(<u>这就是 BTC、BCH 和 BSV 在区块大小上的分歧</u>),再比如现在被给予厚望的、"以太坊 2.0"将会采用的技术方案——分片技术(Sharding)。如果你想了解更多关于分片技术的知识,请阅读白话之前的推文《一文看懂区块链件能解决方案:分片》。

链下扩容,是指在主链之外建立第二层交易网络,因此链下扩容也被称为"Layer 2"。

如果将链上扩容类比为道路的拓宽,那么链下扩容就是在旁边新建高架桥、隧道、小路等等。如果你想了解更多关于链上扩容和链下扩容的区别,请阅读白话之前的推文《<u>什么是链上扩容和链下扩容</u>》。



目前的链下扩容方案中,主要可以分为三类:一类是用于扩展支付,比如比特币上的闪电网络;一类是用于扩展智能合约;还有一类是用于链下计算。

那么,都有哪些相对比较被大众所熟知的链下扩容方案呢?

毫无疑问,知名度最广的链下扩容方案就是比特币的闪电网络(Lightning Network)。2016年1月14日,闪电网络的"白皮书"(论文)发表,随后大量的开发者对此进行了开发和测试。2017年1月,第一个闪电网络的实现——Ind,发布了 Alpha 版本。2017年夏天,比特币闪电网络的基础工作已经完成。截至目前,闪电网络一共有 10423 个节点,34780 条通道,锁定了 821.1BTC。

Number of Nodes	Number of Channels	Network Capacity	Node Countdown
10,423 🛊 +2.50%	34,780 4-1.3%	821.20 BTC ↑+0% \$7,197,711.18	989,577

2019.11.14 比特币闪电网络现状,来源: 1ML

当然,目前的闪电网络也还处于发展阶段,并不是特别成熟。2018年3月,闪电网络节点就遭受到了 DDOS 攻击,导致大约 200 个节点离线。【附《<u>什么是闪电网络</u>》】。

跟比特币闪电网络类似的,是以太坊上的链下扩容方案——雷电网络 (Raiden Network)。雷电网络 支持即时转账、低成本、可扩展和保护隐私,但底层协议相当复杂,实现起来也不容易。

Liquidity Network 是雷电网络的竞争对手。其主要目的是将交易从以太坊转移到支付渠道上,同比特币的闪电网络一样,Liquidity Network 的用户也能够来回进行交易,在这个过程中无需支付手续费,只有在开启通道和关闭通道时需要支付一定的费用。

以上都属于链下扩容中的支付扩展,分层侧链 Plasma 则属于智能合约的扩展。Plasma 是开发者 Joseph Poon 与以太坊创始人 Vitalik Buterin 合写的以太坊分层侧链,主要的目标是将大量的智能合约 计算转移到侧链上,而不是在以太坊主链上执行。

Celer Network 也是一个知名度较高的链下扩容方案。其主要目标是建立一个在现有和未来区块链之上运行的通用网络系统,让每个人都可以快速构建、运营和使用高度可扩展的 DApp。

截至目前,已知的链下扩容方案已有三十多种,但都处于发展的早期。究竟哪些扩容方案能够率先成熟并帮助现有公链解决可扩展性问题,还有待时间的检验。