区块链dot是什么

在《比特币、以太坊的发展瓶颈即将消失，盘点过去4大方向的扩容方案，你看好哪些？》中，我们引入了通道、DPOS、大块和侧链等扩展方法。

在本文中，我们将讨论当前流行的“新扩展方法”，如汇总、切片、分层、工作历史证明和DAG。

01

上卷和等离子体

汇总可以说是目前拓展ETH最重要的手段。可以说，Rollup的成功直接决定了ETH的可持续发展。换句话说，如果Rollup失败了，ETH也不会成功。

如果能区分侧链和Layer2的区别，可以作为扩容的基本认识，那么能否区分Plasma、Rollup和Validium的区别，可以作为扩容的高级测试。

一切都在下图中。如果你看懂了这张图，你就完全明白了等离子体，两个Rollup和Validium的区别。

简单来说，区别如下：

1.一切都始于等离子

等离子是V神提出的第一个扩展方案，也是这个图中最高的TPS方案。

首先，你可以把等离子体看成一个侧链，但它完全独立于侧链，只向Eth提交一个结果是不一样的。等离子会通过主链合约，传递等离子计算处理的块的散列，在ETH主链上做一个“公平”的交易，链下有成百上千的交易，最后的缠绕可能只有几十个字节。你可以理解等离子=ETH侧链运营ETH主链是公平的。

如果有人在离开等离子链时发现他们的传输数据不正确或被篡改了怎么办？提交挑战！所以会有一个证明需求的过程(类似于法院判决)，这也是为什么Plasma的挑战期，或者说资金的提取时间，是7-14天左右(是的，很长，很反人类……)。

等离子最大的两个特点是：(1)默认，或者说乐观，认为每一个“正义”都是对的；

(2)“原始数据”存储在链下。

2.汇总来了

关于等离子体的改进，一开始就出了ZK-
卷积，但是最接近等离子体的是最优性卷积(简称or)，所以先说OR。

OR大致可以理解为“原始数据存储在ETH主链”，所以比Plasma安全。毕竟节点破坏或者篡改原始数据怎么办？

当然，如果把原始数据放在链上，成本会比链下大，所以OR的TPS跑不过Plasma。

另一方面，Zk-Rollup可以理解为“原始数据存储在ETH主链中”。每当主链的散列正义被ZKP(零知识证明)自动证明有效时，就没有挑战或挑战期。

但是原始数据不仅要上传，而且每次都是零知识证明才是公平的，所以开销极大，所以ZK的TPS最差。

因此，有一个相对折中的方案，即Validium -Plasma主链的hash justice被ZKP(零知识证明)自动证明为有效。像等离子体一样，原始数据被抛入链中，牺牲一些安全性来换取性能的大幅提高。

看到这一点，如果你回头看看上面的对比图，你应该有一个框架。

虽然等离子体性能最好，但由于数据链下的安全性和没有ZKP零知识证明的保护，它已被放弃。其他三家公司各有利弊。未来12-24个月，也将是ETH分群，或者说碎片化的时代。不知道那个时候会花谁。只有市场和时间会给我们答案。

02

分层和碎片化

先说分层。如果一个链条天生就有Layer2，“不可能三位一体”不是问题吗？

Nervos就是这么做的，市场上好像只有它一家。很多在Nervos里懂技术的玩家都很喜欢，甚至被评价为“这才是ETH应该有的样子”，其实也不算太意外。总建筑师简毕竟是ETH核心团队中最早的人，堪称“国内最了解Ethereum的人”。

Nervos最大的特点是分层，Layer1负责达成共识，保证整个网络的安全；第二层是一个应用链解决方案，以确保在各种场景下的性能实现，并通过协议锚定到第一层，这样第一层的安全性可以转移到第二层，这有点类似于以太网中的汇总。

但是Nervos其实有两点很容易被很多人忽略，可能和TPS没有直接关系，但是作为底层架构还是值得一提的。

1.第1层是POW UTXO。这在新的公链中是很少见的，关于POW和POS的争论太多，应该跳过。但是，POW总有POW的好处。至少最初的令牌分配是一个更公平的过程。以后也保留改造POS的可能性。届时，可能会采取一种ETH“后续”策略。ETH踩的坑可以吸取经验，尽量避开。