区块链扩容技术分析

16350027 黄俊

background

说到区块链的扩容技术，一开始就讲怎么扩容多没有意思，当然是需要从为什么需要扩容开始讲起啦，因为随着区块链（比特币，以太坊）的用户不断增多，单位时间的交易也在不断变多，与之相伴的很严重的一个问题就是这样导致一次同步所需要的时间变长，与之相对的就是完成一次交易到最后确认的时候会变得难以接受，所以就需要扩容的策略，具体而言就是希望同一个区块链网络能够同时承载更多的用户以及更多的交易。

现在主流的扩容策略大家广为接受的分别有4种：分别是Casper,Sharding,Raiden Network和Plasma。

我先大概介绍一下这些东西都是些什么玩意。

1. Casper Casper是一种基于共识协议。协议中的节点都必须付出保证金才可以参与出块和共识形成。Casper共识协议通过对这些保证金的直接控制来约束验证人的行为。具体来说就是，如果一个验证人作出了任何Casper认为"无效"的事情，他的保证金将被罚没，出块和参与共识的权利也会被取消。保证金的引入解决了经典POS协议中做坏事的代价很低的问题。
2. sharding sharding其实算起来应该是我在所有扩容协议里面最喜欢的一个了，就是把单独的一个大的区块链分成自治的子网，并且在子网里因为信任程度的提高可以进行分工来提高效率，并且之前的信息传递由于子网的划分可以有效地减少同步所需的传播次数也就可以减少同步的时间。
3. raiden network 双方需要在以太坊区块链上开设通道并各自锁定以太。这步动作可通过向Raiden智能合约发送一条双方签名认可的报文来实现。报文中的关键信息包括：双方公钥、双方锁定资产数量、双方签名。 此后的任何支付动作都可以发生在以太坊区块链外，参与双方只需要私下传递一系列报文。 相当于就是直接进行链外的交易。确定的速度有多快可想而知。
4. plasma 也就是侧链技术，通过把把大量交易和计算放在侧链上来实现，之所以更有效率的原因就在与主链处于安全原因使用pow共识算法，侧链因为其性质可以使用pos或者更快的共识机制，所以相当于是利用侧链提供了可扩展性，主链来保证安全。

具体谈论侧链

具体说到侧链的实现，其实就是和比特币绑定在一起，被担保可以和比特币保持兑换关系的特殊货币的网络。具体而言，如果想让比特币流入侧链网络中就只需要把比特币送到对应区块并且把这个作为侧链的起始区块，并且锁定起来，只有侧连中实现交易了，再把侧链中的货币换成比特币时区块中的比特币才解锁。

所以说到底，起始侧链的机制就是一种主动的分片的机制。侧链有独立的网络，其中发生的交易只需要在这个小的网络里面广播，可以大大减少同步的时间。

至于在以太坊实现侧链，还是跟自己建立一个局域的区块链网络一样，需要建立新的起始区块，并且很重要的是需要找到足够多的节点来运行这一个侧链。当然设计到一些底层的api，侧链完全利用主链的基础设施，相当于说到底还是和一个应用一样，设计起来不会太艰难。

至于怎么可以在不同链上来转移对应货币就可以Plasma。来保证不同货币之间的保证关系。