DAG 也许是真正的区块链 3.0IOTA 中国社区 IOTAChina

埃欧塔

从 15 年开始，区块链概念被单拎出来，这之前区块链还只是比特币技术里的一个数据结构，中本村白皮书里把 block 和 chain 连一起的时候也只是 a chain of blocks 。随着以太坊去中心化计算机的概念提出来，很多人开始把以太坊称作区块链 2.0，而比特币被归到了区块链 1.0。至于区块链 3.0，市场上为了抢夺区块链 3.0 的冠名权打的不可开交，没准会是 DAG。DAG(Directed acyclic graph) ，有向无环图，是计算机领域一个常用的数据结构，因为独特的拓扑结构所带来的一些特性，经常被用到处理动态规划，导航中寻求最短路径，数据压缩等场景中。第一次提出 DAG 跟区块链结合是在 Nxt 社区，可以发现 DAG 最初出现就是为了解决区块链的效率问题。比特币的效率一直比较低，基于工作量证明共识下的出块机制是一个原因，由于链式的存储结构，整个网络中同时只能有一条链，导致出块无法并发执行。社区有人提出 DAG 的拓扑结构来存储区块，这个时候更多还是类似侧链的解决思路，不同的链条存储不同类型的交易，这样降低出现双花的可能，在之后某个节点需要合并的时候，几个分支再归并到一个区块。简单介绍下，目前比特币区块链存储结构如下，每个区块存储着当前时间段所有的交易，

矿工一直在拼命争夺某个时段交易的打包权利，把当前时间段所有的交易打成一个区块。目前比特币网络平均出块时间在 10 分钟。比特币区块链存储结构而 Nxt 社区提出，改变区块的链式存储结构， 变成区块 DAG 。在区块打包时间不变的情况下， 网络中可以并行的打包 N 个区块， 网络中的交易就可以容纳 N 倍。 Ext 社区提出的 DAG of blocks 发现这个时候 DAG 跟区块链的结合还是停留在侧链的思路，不同类型的交易可以并行在不同的链条进行，达到提升性能的目的。这时候的 DAG 还是有区块的概念。我们发现不管是最近风头正盛的 iota，还是也备受瞩目的 byteball ，都提出了 blockless 无区块的概念。 不管是比特币还是以太坊， 我们总会提到出块速度这样的概念，比特币每十分钟才出一个块，6 个出块确认就要一个小时，以太坊好很多，但是出块速度也要十几秒。为什么一定需要区块呢？ 15 年社区有提出 DAGCoin 的概念， DagCoin: a cryptocurrency without blocks 。这里把区块和交易融合到了一起。我们回想下比特币网络中区块和交易的概念，很多笔交易先打包到区块中，区块和区块之间通过 prehash 来维护全网的交易顺序。而 DAGCoin 的思路，让每一笔交易直接参与维护全网的交易顺序。这样交易被发起后直接跳过打包区块的阶段，直接融入全网，如此达到所谓的 blockless 效果。这样确实连打包交易出块的时间都省去了， 如前文提到的， DAG 最初跟区块

链的结合就是为了解决效率问题，现在不用打包确认，交易发起后直接进入确认网络，理论上效率自然提高很多。自此，以 blockless 独树一帜的 DAG 区块链雏形基本形成。又以 IOTA 和 Byteball 在市场上的表现最为耀眼。DAG 系的区块链有些概念很有趣，了解这些概念更容易理解 DAG 技术。1 从概率的角度来看双花问题。在比特币网络中，通过 UTXO 模型，一个用户对自己可以解锁的 UTXO 只能发起一次转账，如此解决双花问题。比特币白皮书中也有提到，有可能多个矿工会同时解决哈希难题，获得同一时间段的交易打包权就是出块权，会有临时分叉的可能性。从这个角度来看，比特币网络中所谓的 "global ledger state" 也是一个不确定的状态。某一笔交易状态的确认是由其后挂靠交易的数量决定的，其后挂靠的交易越多，交易状态回滚的概率越低，这笔交易越安全。 2 网络宽度 iota 的 tangle 网络 DAG 网络一个重要的问题就是解决网络宽度，DAG 网络中，每笔交易被确认，需要链接到已经在网络中存在的并且比较新的交易，如果都选择网络中比较早的交易，会导致网络宽度过宽，新的交易难以得到确认。理想的状态是，新的交易发起时，选择网络中已经存在的并且比较新的交易做链接确认，这样网络的宽度保持在一定范围，能让新的交易有足够快的确认时间。在 IOTA 中， tangle 也提出了自己控制交易宽度的算法，有兴趣可以参考 tangle 白皮书。那么 DAG 究竟有哪些特点，居

然让 iota 市值一度排到了虚拟货币第四的位置。 1 交易速度快如上文提到，由于 DAG 摒弃了区块概念，交易直接进入全网中（需要指出， iota 网络中每发起一笔交易，会类似 hashcash 一样的机制做简单的 pow 证明）, 所以交易速度预期比基于 pow 和 pos 的需要出块的区块链会快不少。 2 无需挖矿 DAG 把交易确认的环境直接下放给交易本身，无需由矿工打包成区块后同意交易顺序。所以 DAG 网络中没有矿工的角色。 3 无手续费 iota 的 tangle 网路中，交易发起只需要做简单的 POW 工作量证明，整个网络中的 POW 都是发起交易者自己做的， 而不是交给矿工。 发起交易无需手续费。4 智能合约支持目前 iota 还不支持智能合约，但是官方 roadmap 中有计划在 18 年开始实现对智能合约的支持。而 byteball 也还不支持智能合约。 5 需要见证节点不管是 iota 还是 byteball ， 目前的网络结构中，还是需要见证人机制的存在。这一部分不管是 DPOS 、 POS 、 PBFT ， 大家最终都会在效率、安全性上寻求一种平衡。市场上 iota 和 byteball 的市值已经引起了很多关注，相信对 DAG 的技术讨论也会变多。从技术角度来看， DAG 给我们提供了完全不一样的区块链实现，高性能和无手续费这些点确实引人注目。随着社区对 DAG 技术的进一步完善和发展，也许， DAG 会是真正的区块链 3.0 呢。最近在做区块链方面的创业项目，在找各种技术栈的小伙伴一起搞事情。也欢迎大家加微信交流沟通

qqwww5　最近在做一个区块链技术相关的公众号，　　欢迎大家关注　JustBurning　　喜欢　(18)