DAG 研究报告

2018.06.06

引言

有向无环图(Direct Acyclic Graph 或 DAG)是近些年来区块链项目的技术热点之一。许多业内人士认为，这项技术有可能在根本上解决区块链的扩容问题，因此相关的项目都有较高的热度。然而，由于其更高的技术门槛和开发难度，采用这项技术的区块链项目仍为少数，在国内更是凤毛麟角。

传统的线性架构的区块链，在维持良好的去中心化与安全性的前提下，在底层上的吞吐容量有根本的瓶颈问题。因此这些区块链项目的扩容方案，一种是以牺牲去中心化的记账方式来换取整个链的吞吐容量，一种是依赖侧链、分片等第二层（Layer 2）技术来处理小额交易。要根本性地获得更好的底层链效率，需要采取与完全不同的架构。DAG 就是较被看好的潜在挑战者。

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 什么是 DAG

按照数学上的定义，DAG 是一个没有有向循环的、有限的有向图。具体来说，它由有限个顶点和有向边组成，每条有向边都从一个顶点指向另一个顶点；从任意一个顶点出发都不能通过这些有向边回到原来的顶点。

在数学学科中，DAG 与代数拓扑学中被深入研究的偏序集（Partially Ordered Set 或 Poset）有紧密联系。事实上，任何一个 DAG 都唯一对应一个 Poset，而所有的 Poset 都是 DAG，所以它们在本质上是一种事物。

在区块链的应用上，DAG 图的每个顶点代表在某一个时间新挖出的区块。一般的线性区块链是 DAG 的一种特殊情况，也即每个时间段整个系统只能产生一个区块。不同的是，DAG 允许不同节点按自己的节奏生成区块，只要每个区块选择一个或多个区块作为自己的子区块。

2 DAG 的优势

DAG 相对于传统线性区块链的优势是非常明显的，主要在于可延展性和交易吞吐量上。

2.1 可延展性

由于采取 DAG 的数据结构的话，每个节点不需要再等其它节点的数据达到统一就可以处理新的交易，避免了因网络延迟和数据同步造成的时间浪费。因此，参与 DAG 记账的节点很容易大幅延展。因此，DAG 非常适合 IoT 一类设备非常多且网络状况往往不稳定的应用。

相比之下，在线性区块链系统中，节点一旦碰到通信延迟而数据不统一，就无法参与下一次区块的生成，甚至在极端情况下有网络分叉的危险。

2.2 交易吞吐量

此外，DAG 的尾端可以平行增加任意多的新数据，因此天生具有很强的交易吞吐量。这一点更是完胜线性区块链

线性区块链每次只能增加一个区块大小的数据量，所以可以处理的交易量是很难改变的。

3 DAG 的主要安全问题

3.1 双花

DAG 异步处理数据的特征导致攻击者可能利用节点间的信息差进行双花。具体来说，如果两个顶点间没有明确的父子关系，攻击者可以分别在只看到这两个顶点中的一个的不同节点处，对同一笔存款进行双花。这种双花只有在同时看到两个区块的节点处才能被检测到，并且只有在两个顶点重新汇合到一个新顶点时才能最终判定哪一笔是双花。

为了防止这种双花的发生，需要额外通过制定更周密的双花检测规则。

3.2 影子链攻击

DAG 允许多重并行交易的特征，导致攻击者可能暗中生成一条影子链，并且时不时地将影子链跟主链进行对接以逃避检测算法。极端情况下，这条影子链有可能代替主链成为全网的共识。

4 已上线的 DAG 公链项目比较

	Byteball	IOTA	NANO
共识机制	见证人	PoW（目前依赖协调员）	DPoS+PoW
防双花	转账时必须包含之前的交易记录	PoW+权重计算	DPoS 投票
防影子链	见证人宣布见到的顶点，投票选择主链	MCMC 检测顶点与主链的耦合程度	DPoS 投票
目前的问题	需要交易费	哈希算法易遭到攻击	治理更为中心化

4.1 Byteball

Byteball 要求每当一个地址要进行转账时，它必须直接或间接包含所有之前从这个地址转出的交易记录。这样，如果攻击者进行双花，由于所有之前转账记录都包含在交易里，双花的检测就变得更容易了。我们只需要将第二笔转账同一存款的交易确定为双花就可以了。

Byteball 要求从创始块开始确定一条所有参与者公认的主链，而将其它的顶点看作是附属在这条主链上。每一条主链对应着一种不同的主观上的时间顺序，从而对应着不同的双花交易的确认。另外，为了防止攻击者暗中生成影子链并且链嫁接在主链上，Byteball 提出见证人（Witness）制度进行主链选择。每当见证人看到一个顶点，就公开宣布看到过这个顶点，而系统选择主链时就依照选择被见证次数最多的顶点的原则。在这种制度下，只需要保证大多数的见证人不会与攻击者窜通作恶，就可以保证主链选择过程的安全性。

为了激励见证人的服务，Byteball 会收取一定的交易费用以支付见证人。相比之下，另外两个主流 DAG 项目不收取交易费。因此，Byteball 可能不适于 IoT 领域极其小额的交易。

4.2 IOTA

IOTA 在防止双花上采取了不同的策略。IOTA 将主链的概念普遍化为扭结（tangle），实际上代表厚度任意的主链。在新顶点产生的时候，每个新顶点会选择 2 个旧顶点作为父顶点，并进行 PoW 挖矿。IOTA 在确定扭结时，按照所有的父顶点关系进行权重计算，给予较多子顶点支持的父顶点更多的权重。

在防止影子链攻击上，IOTA 使用 MCMC(Markov Chain Monte Carlo)算法进行顶点排除。具体方式是，随机选取一部分顶点，从它们开始做随机漂移，直到达到某个边缘顶点，但是丢弃掉过早到达边缘的“懒顶点”，最后统计每个边缘顶点到达的概率。IOTA 宣称这种方法可以以很高概率排除掉影子链，但在这个结论上白皮书并没有给出明确的量化或者数学证明。

IOTA 目前存在的问题是，它采用的号称量子抵抗的哈希算法存在一定的漏洞，导致一个账户在转账后有一定概率让黑客解密私钥。官方立场是从账号发起转出资金后，不建议再次使用该账号。据报道已经发生几起用户私钥被破解的事件。

4.3 Nano

Nano 采取的 DAG 架构是给每个账户安排一条单独的链，这些链只有每当有发送或者接受转账时会更新相关交易的信息，这样每条链都只处理跟自己账户有关的交易，大大减少了需要处理的交易总量。

Nano 使用 DPoS+PoW 混合共识机制， 一旦交易出现了争议由 DPoS 投票仲裁决定。Nano 设计成零交易费，所以为了防止垃圾交易，每笔交易入账需要进行一个小算力的 PoW 挖矿。与比特币不同，由于 Nano 每个账户有单独的链，对未来的交易可以提前进行 PoW 挖矿。Nano 白皮书对于事先提前挖矿的攻击并没有防御措施。

在实际应用中，Nano 的一账户一链架构给中心化交易所的出入金造成不便，因为交易所的账户会需要进行非常大量的交易，因此需要大量的 PoW 挖矿。Nano 目前的解决方法是手动免除交易所的 PoW 挖矿，但这种措施进一步加强了 Nano 网络对于中心化治理的依赖。

5 DAG 共识机制研究方面的进展

DAG 的共识机制的学术研究方面，很大一部分由以色列的 DAGLabs 团队推进，但国内的团队也在快速崛起。以下对目前处于研究阶段的 DAG 共识机制进行总结。

项目名称	时间	研究方	创新点
Inclusive	2015.7	DAGLabs	最早提出将 DAG 用于区块链，并且进行节点间的博弈论分析
SPECTRE	2016.12	DAGLabs	提出用 DAG 提高区块链扩容/安全性的方案
PHANTOM	2018.2	DAGLabs	通过对 DAG 进行交易全排序，提出用 DAG 实现智能合约级高并发的方案
Avanlanche	2018.5	DAGLabs	提出一套新的 BFT+DAG 方案，实现智能合约级高并发
Conflux	2018.5	清华-多伦多团队	提出一套不同的用 DAG 实现智能合约级高并发的方案，兼容 PoS，并且第一次对 DAG 性能进行大规模实验对比

最早提出将 DAG 应用于区块链的 DAGLabs 团队，目前也是在基础研究上走得最远的。然而，目前为止该团队还没有代币发行的计划。与该团队无关的公链 DAG 项目 HYCON，则宣称将会使用 SPECTRE 共识机制，并且在今年已经完成 ICO。

国内清华为主的一个团队最近发布了 Conflux 共识协议，并且首度进行了上万台 AWS 服务器的大规模实验对比，证明了协议在 tps，确认时间和可延展性方面的绝佳表现，有在 DAG 领域弯道超车的希望。该白皮书中还指出了一种针对 PHANTOM 协议的影子链攻击方式。

6 DAG 项目的投资逻辑

目前已经落地的 DAG 公链项目都不具备智能合约的功能，因此目前新募集的 DAG 项目都会以具备图灵完备智能合约平台，或者提供智能合约跨链执行的接口作为卖点。由于目前 DAG 共识机制的学术研究尚处于进展过程中，这些号称能实现智能合约的 DAG 项目是否能在近期实现所宣称的功能，仍要打上一个问号。

由于 DAG 高并发、异步的特征，非常适合 IoT 类应用，许多 IoT 类项目都会偏爱 DAG 架构。IOTA 就是以处理机器间小额高频交易为应用场景。另一方面，IoT 设备一般不具备 PoW 挖矿所需的算力，因此 PoS/DPoS+DAG 或者 BFT+DAG 更有可能成为未来 DAG 项目的共识机制。

7 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

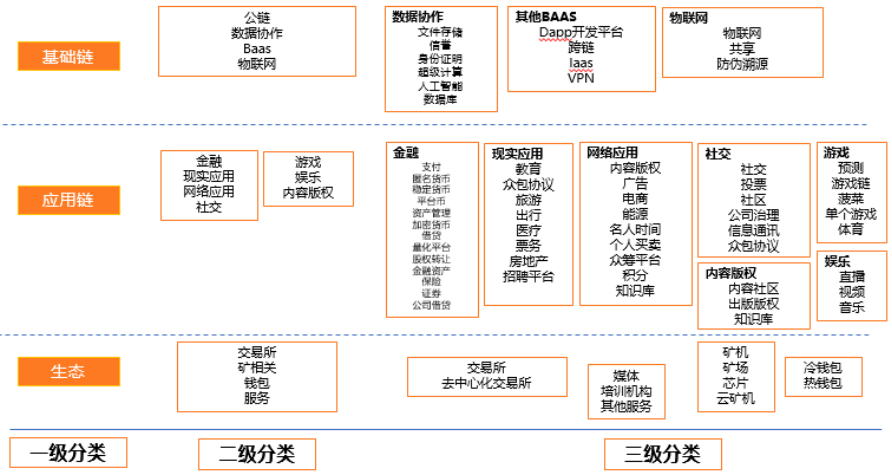
- 节点研究中心 专注于区块链行业分析与投资
- 团队氛围良好 高效友善开放活泼 分析组成员来自清北复及海外高校
- 简历投递：langhanwei@nodecap.com


分析师
朱子川


分析师
武怡


助理分析师
蔡晨曦

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。