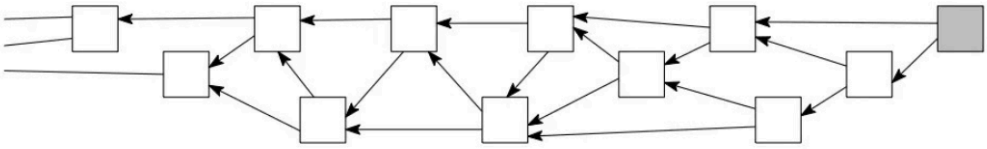
一、 DAG（Directed Acyclic Graph）的定义：

- 有向无环图，“有向”指所有数据顺着同一方向存储；“无环”指数据结构间不构成循环。
- 算法图论中的一种数据结构，常用来解决动态规划、最短路径、数据压缩等问题。



传统的区块链技术存在以下几个问题：

1）效率问题：传统区块链技术基于Block区块，比特币的效率一直比较低，由于BlockChain链式的存储结构，整个网络同时只能有一条单链，基于POW共识机制出块无法并发执行；例如比特币每十分钟出一个块，6个出块才能确认，大约需要一个小时；以太坊大幅改善，出块速度也要十几秒。

2）确定性问题：比特币和以太坊存在51%算力攻击问题，基于POW共识的最大问题隐患，就是没有一个确定的不可更改的最终状态；如果某群体控制51%算力，并发起攻击，比特币体系一定会崩溃；考虑到现实世界中的矿工集团，以及正在快速发展量子计算机的逆天算力，这种危险现实存在。

3） 中心化问题：基于区块的POW共识中，矿工一方面可以形成集中化的矿场集团，另一方面，获得打包交易权的矿工拥有巨大权力，可以选择哪些交易进入区块，哪些交易不被处理，甚至可以只打包符合自己利益的交易，这样的风险目前已经是事实存在。

4）能耗问题：由于传统区块链基于POW算力工作量证明，达成共识机制，比特币的挖矿能耗已经与某个国家耗电量持平，IMF和多国政

府对虚拟货币挖矿能源消耗持批评态度。

DAG技术被用于尝试解决区块链的上述问题。DAG的特点：把数据单元的写入操作异步化，大量的钱包客户端可以自主异步地把交易数据写入DAG，从而可以支持极大的并发量和极高的速度。

传统区块链和DAG的区别：

1）单元：区块链组成单元是Block，DAG组成单元是TX（交易）；

2）拓扑：区块链是由Block区块组成的单链，只能按出块时间同步依次写入，好像单核单线程CPU；DAG是由交易单元组成的网络，可以异步并发写入交易，好像多核多线程CPU；

3）粒度：区块链每个区块单元记录多个用户的多笔交易，DAG每个单元记录单个用户交易。

二、DAG发展现状

DAG开始引发大量关注始于IOTA在2017年下半年市值冲入币值排行榜第四名，之后基于DAG技术的新项目不断进入人们的视野。

目前最知名的采用DAG结构的区块链项目包括：IOTA、Byteball、Raiblocks（Nano）。

1）IOTA

- 较高的交易吞吐量（通过平行验证），1000 TPS。
- 无手续费。
- 每个点都是一个交易，共识的最小单位是交易。
- 在 IOTA 中，要验证新的交易前，必须直接验证之前的两个交易，这也使得在这两个交易之前所有被验证过的交易得到间接验证。
-

IOTA背后最主要的创新Tangle（纠缠），在Tangle中，每一个节点代表的是一个交易。IOTA里没有区块的概念，也没有挖矿和矿工的概念，这就代表没有交易费，整个网络的吞吐量也很高，这是IOTA的最吸引人

的亮点之处。

IOTA创建了物联网应用的基础环境，离线异步处理（让交易从网络中剥离出来或者合并回去）使得在物联网领域应用。

IOTA的共识就是它自身内化特性，可以使它在没有交易费用的情况下进行规模化使用。IOTA中不再有区块的概念，共识的最小单位是交易。

IOTA目前的问题是：

- IOTA 使用的哈希函数名为 Curl，是一个三进制算法，由 Keccak (SHA-3) 的发明者设计。MIT报告指出curl算法的哈希值极易发生碰撞，于是就能伪造数字签名。（三进制架构的电路功耗低，适合 IoT 设备，但传统计算机都是基于二进制的，效率下降）。
- 共识是由全网交易确定的，那么理论上来说，如果有人能够产生1/3的交易量，他就可以将无效交易变成有效交易。
- IOTA无手续费，没有矿工激励，导致IOTA面临着拒绝服务攻击和垃圾信息攻击可能。
- IOTA引入闭源的中心化组件Coordinator来对全网交易进行检查（例如双花），如何有效移除Coordinator并建立一个具有良性激励机制的去中心化「Coordinator群体」，IOTA还没有给出解决方案。

2）Byteball

具有DAG体系家族中最完善的应用生态。

Byteball在DAGCoin的基础上，引入主链与见证人概念，鼓励验证多个父辈交易单元，形成一个随着交易增长、相互验证，安全性不断加强的数字签名Hash网络，Byteball创造性的发明了「主链」概念，也就是经过见证人认定的最短路径MC的Parents优选算法。主链创造了一个全网共识确定的交易时间序列，避免了双花问题。

基于见证人+主链的共识机制：12个见证人发布的交易单元，在理论上无限宽广的DAG并发交易网络中划出了一道确定性的交易时间序

列。正是这道无限延伸基于时间的确定性交易序列，打造了Byteball中的主链，在宽广无序的有向无环哈希世界中形成了强健有序的唯一主干。

Byteball取消了区块链和工作量证明挖掘的概念，选择了DAG数据存储技术。所有交易都是以加密方式相互关联的。新产生交易将添加到tips交易单元后面。这样让网络上的所有节点（用户）都参与验证交易，完全的去中心化。更快地验证付款，还可以让网络保持足够的分散。

通过收取存储在DAG网络的每字节数据存储费用，通过类似Gas机制减少网络上的SPAM垃圾信息。

Byteball由于每个交易都有发起者的私钥签名，同时每笔交易都验证与引用从前发生的交易，以此编织成一个巨大的网络，对网络的篡改牵一发而动全身，同时不可能有人拥有全网所以用户的私钥，所以Byteball具备银行级最终确定性。

Byteball的问题是：

- 由于主链算法和见证人发布频率有关系，交易确认的时间是不确定的；
- 由于Byteball基于关系数据库来存储数据，SQL语言过于紧耦合算法逻辑，在一定程度上限制了Byteball目前的扩展能力和速度。

3）NANO(XRB)

一种基于区块点阵(Block Lattice)结构的新型加密货币。

一个用户一条链的方式，只记录自己的交易，也只有自己可以修改记录，不与其它帐户共享数据，从而使所有的交易都可以并行执行，能提供秒级的交易速度和无限可扩展性，并且允许他们异步地更新到网络的其余部分，从而以极小的资源开销获得快速的交易确认。

Nano一个节点可以存贮所有账户的历史账本，也可以只存贮每个账户的最后修剪记录。当一笔交易发生的时候，发出金额的一方会生成一

个send tx的区块，包含记录扣除的金额；而收款账户则生成receive tx区块记录对应获得的金额。交易数据的收发是可以异步进行的，所以就算同时有多笔金额汇入一个账户也没有问题，最终的金额是收到的金额的加法。如果接收方不在线也没关系，未到账的金额会单独标记，等到接收账户上线之后，这笔金额就会从未结算区打入接收区块，完成交易。

NANO使用了DPOS共识机制，账户可以指定代表为其投票，得票最多的代表将处理分叉，这个代表会将分叉广播到网络，并观察来自高权账户节点在固定时间内的投票接结果，以此来确定保留哪一个区块。DPOS可以保证区块的合理低能耗运行。NANO也使用到了POW机制，确认交易需要非常少的工作证明（PoW）。

NANO的问题是：没有被充分测试、缺乏同行评议，共识算法可能有严重缺陷的风险。例如，如果没有足够的法定人数投票来解决网络冲突会发生什么？另一个大问题：如果NANO网络的某些部分长时间分离，当分离的网络重新加入时会发生什么？重新加入的网络是否会在不可避免发生的投票过程中瘫痪?

三、DAG创新与趋势

1）HashGraph（哈希图）

Hashgraph是由Leemon Baird开发的一种Gossip八卦协议共识算法。所有节点随机地与其他节点共享其已知交易，因此最终所有交易可传递到各个节点。Hashgraph速度非常快（每秒交易250,000次以上），由于闭源和专利，HG适用于私链或者联盟链，短期内不会应用于公链和得到规模验证。

Hashgraph开创性的在公链环境下做异步BFT共识，传统BFT的一大问题是消息复杂度太高，大量消耗系统的网络带宽，无法很好的应对动

态网络。这里Hashgraph引入了传统Gossip Protocol，并加以独特的创新，另外再加上虚拟投票机制，这样在需要共识的时候不会引起突发大规模消息传递风暴。

Hashgraph和Algorand通过从不同角度改良了BFT应用的场景和条件来使得BFT共识可以被应用到公链系统中，HG通过八卦传播哈希图以及基于哈希图做虚拟投票将传统共识所需的瞬时通信要求降到了最低，并且本地计算保证了共识高效性。

最新的Hashgraph的商业介绍书上讲述计划切换到 POS，并且支持DOPS，并可以让不运行全节点的持币者选择代理人，分享收益。

Hashgraph集各家所长，在扩展性，安全性和共识达成成本上都有很大突破，但是技术难度大，还未在大规模公链环境下运行，如果能够实现严密的数学及应用检验HG白皮书中描述，那么 Hashgraph足以成为可信互联网上探索的一个重要里程碑。

2）SPECTRE/PHANTOM

https://eprint.iacr.org/2018/104.pdf

SPECTRE Protocol采用了Block+DAG的「区块有向无环图」技术，可以并行挖矿，从而带来更大的吞吐量和更快的交易确认时间；2018年2月SPECTRE的扩容协议–Phantom发布，能够大大扩充网络交易容量，并兼容智能合约。该项技术是「对中本聪提出的区块链的泛化」，解决了前者需在安全性与扩容能力之间进行取舍的问题，因而更加适合建立速度更快或规模更大的区块。

不同于闪电网络等链下解决方案，PHANTOM是链上扩容方案。同时PHANTOM采用线性排序会在一定程度上牺牲SECTRE可实现的交易确认速度。

PHANTOM在BlockDAG上使用了一种贪婪算法，来区分诚实节点挖出的区块和通过偏离DAG挖矿协议的非协作节点挖出的区块。利用这个区别，PHANTOM以最终由所有诚实节点同意的方式在blockDAG上提供全序。

PHANTOM协议与SPECTRE协议类似，但又有区别。SPECTRE协议是通过签名的区块递归投票来确认交易的。与SPECTER协议不同的是，SPECTRE拥有较高吞吐量和快速确认时间。它使用DAG的结构来表示关于每对块之间的顺序的抽象投票。PHANTOM解决了SPECTRE中可能由于Condorcet循环可能无法扩展到全线性排序的问题，并提供了DAG块的线性排序。因此，PHANTOM可以支持关于任何一般计算的共识，也称为智能合约，而SPECTRE不能。但是由于其线性结构，会牺牲SPECTER协议所提供的更快速的确认时间。同一个系统中，将这两种协议相互结合，可能得到的效果会更好。

3）Hycon

https://icodrops.com/hycon/

Hycon是韩国的DAG项目，定位平台型公链，还要做生态，包括价值交换媒介去中心化交易所，准备募集近一个亿美金的资金，另外70%是要靠以后挖矿挖出来的。

Hycon整个生态系统的建立分为三个阶段：价值交换媒介、区块链平台以及去中心化交易所，旨在打造集价值交换、商业应用以及 Token 流通等属性于一身的价值生态系统。其中，区块链平台是整个生态系统的核心，将解决交易确认速度低、吞吐量有限的区块链性能瓶颈，从而实现商业级应用。

Hycon公链平台的主要特性是：快速交易确认时间、链上交易扩展性（在2MB/S的连接中高达3000TPS交易吞吐量）、同步出块（可基于DAG结构位置而不是时间先后链接区块）以及智能合约。

4）Algorand

https://eprint.iacr.org/2017/454.pdf

Algorand是权益证明(POS)的一个升级，彻底消除区块链分叉的可能性，可以在一小段时间内确认交易，Algorand的核心使用称为BA⋆的拜占庭协议，同时扩展到许多用户。即使一些用户是恶意的，网络被临时分区，Algorand也确保用户从未对已确认的交易有不同意见。在

Algorand的BA*协议中，除了私钥之外，用户不会保留任何私有状态。

最近在海内外大火的明星项目Algorand，目标是建立一个低能耗、高速度、民主化、可拓展性好而且几乎不会出现分叉的分布式账本。Algorand没有引入激励机制或发行数字加密货币。Algorand由图灵奖得主、MIT教授SivioMicali募集400万美元开发。

四、部分已知的基于DAG技术的典型项目：

1）ITC（万物链）

https://iotchain.io/whitepaper/ITCWHITEPAPER.pdf

基于区块链的安全物联网轻操作系统，解决方案融合了区块链技术，结合密码学非对称加密技术，半同态加密秘文计算技术，以及无数据中心的分布式架构，旨在解决目前物联网严重的安全问题，满足物联网高度并发的使用场景，实现万物互联互通。

2）TrustNote

https://github.com/trustnote/document/blob/master/TrustNote-WhitePaper-cn.pdf

TrustNote是支持POW挖矿的DAG公有链，具有创新的双层共识机制，面向数字通证发行、区块链游戏和社交网络等应用场景，基础代币称为「TTT」，核心在于底层公链开发，应用生态可以应用在金融征信、信息安全、物联网、游戏、社交等领域。目前，已经在应用领域有所涉及。

3）Bsure（必信链）

Bsure是专业数字保险和大健康区块链智能平台，构建基于DAG技术的数字保险和健康医疗行业公链。目前测试链已经上线，并在开发Bsure.cloud链云基础设施，赋能健康医疗和保险科技行业产品与服务创新。

Bsure行业公链平台的开发中的主要特性包括：快速交易确认时间（instant payment）、交易扩展性（通过内存计算，优化主链算法，提

升交易并发能力）、Package+DAG共识创新（结合本地偏序包和公证人主链全序算法），分层赋能架构：包括独立的智能合约层、去中心化存储层、DAPP应用层、同构跨链等等。

4）Nerthus（纳尔图）

http://www.nerthus.io/static/downfile/NerthusWhitePageV0.0.2Ch.pdf

在 Byteball 的基础上，做了进一步的改进——维护用户级别的见证人列表。并受 DPOS 机制的启发，交易单元一旦发布且经所有见证人共同签署的见证单元验证后，该交易单元就是最终确认的。

2017年下半年发起的低调项目，Nerthus基于的是字节雪球DAG结构加以改良，并使用GO语言实现了服务层，核心层，和应用层三层架构。目前还没上交易所。纳尔图应该是中国第一个的基于DAG技术开发的平台型公链项目，项目正在开发中。

5）CyberVein（数脉链）

https://www.cybervein.org/

CyberVein是基于DAG架构，包含了自己的Vein编程语言、虚拟机、新型智能合约的底层系统，致力于从技术层面和商业逻辑两方面解决大数据时代面临的数据价值定义和管理问题。

CyberVein由DAG+PoC机制+数据库虚拟机共同完成的，DAG架构只是CyberVein的一部分，CyberVein平台上还可以创建自己的智能合约，拥有操作数据库的虚拟机和编程语言，共识机制还有创新。