XDAG 技术白皮书（草案）

Dr. Edward Wang, Bei Wang
XDAG 中国基金会

摘要

XDAG 是新一代基于工作量证明（Proof of Work，PoW）和有向无环图（Directed Acyclic Graph，DAG）的分布式账本技术，是世界上第一个可挖矿的 DAG 项目。

比特币底层使用的区块链技术是最近几年兴起的一项新技术，实现了在无中心化授信机构的条件下，通过点对点网络实现价值的转移。区块链是一项极具创新性的突破性技术，然而目前处于初期的阶段，存在以下的问题：

1、 以比特币、以太坊为代表的区块链以PoW作为共识算法，交易吞吐量有限，大约为10 tx/sec，无法满足人们的需求。
2、 以EOS为代表的区块链以PoS/DPos作为共识算法，存在去中心化程度不够的问题，容易遭受贿赂、共谋攻击，安全性不足。

XDAG结合了DAG高并发的特点和PoW去中心化的属性，解决了目前区块链无法解决的不可能三角问题。XDAG具有以下特点：

1、 交易吞吐量高。相比于区块链使用的链状数据结构，XDAG使用的有向无环图（DAG）具有更高的交易吞吐量。
2、 交易即区块，地址即区块。巧妙地将交易、区块、地址三者结合，高效简洁，适应各种场景需求。
3、 交易速度快。DAG技术采用的并行结构使得交易速度大幅提升。

概述

2008 年 10 月 31 日，一个化名为中本聪的匿名黑客发布了比特币的白皮书《比特币：一种点对点的电子现金系统》，并提出了通过去中心化的点对点网络实现价值转移的设计思想。在比特币系统中，交易发起方使用密码学方法签名交易，交易接收方与其他人验证并确认交易，并将交易数据以区块+链的结构存储于各个节点，使得交易双方在没有中心化机构的前提下也能进行交易。

2014年1月，Vitalik在美国佛罗里达州迈阿密举行的北美比特币会议上正式宣布了以太坊。以太坊在区块链之上实现了智能合约，使得区块链技术从单纯地处理数值账目上升到可通过智能合约处理各种复杂逻辑，使区块链迈上了一个新台阶。

随着对区块链技术研究的不断加深，出现了各种以PoS/DPoS作为共识算法的区块链。2017年5月，Bytemaster（BM）在美国纽约共识大会上介绍了EOS。EOS通过运行超级节点的方式提升交易的吞吐量。然而，依赖于超级节点的设计存在去中心化程度不足的问题，容易遭受贿赂、共谋攻击，在安全性方面存在不足。

尽管众多区块链研究者都在尝试寻找各种技术手段解决当前区块链存在的问题，但是从当前技术发展现状来看，各种尝试并没有取得突破性进展。目前遇到的问题主要有以下两个方面：

1、 交易吞吐量低。

2、 去中心化程度不足，安全性不高。

针对以上两个问题，不管是EOS偏中心化的解决方案，还是目前如火如荼的分片技术、侧链技术都存在一些无法解决的问题。

XDAG从区块链技术底层的数据结构开始重新设计，采用DAG结构，巧妙地将PoW共识算法和DAG相结合，继承了DAG高吞吐量的特点，同时又具备PoW的

安全特性，在保证网络安全性的前提下，提升了交易吞吐量，减小了交易响应时间，尽可能地解决了区块链技术存在的问题。

数据结构

区块

区块是XDAG的基本结构。一条交易是一个区块，一个钱包地址也是一个区块。一个区块拥有固定的大小——512 字节。区块通过区块地址进行索引，区块地址为base64格式编码的区块哈希值。

哈希

对区块进行两次Sha256计算。
Hash(block) = Sha256(Sha256(block))
因此，XDAG使用的工作量证明算法为SHA256D。

短哈希

哈希以小端字节序（little-endian）表示的低24字节。

时间戳

区块时间戳代表区块产生的时间，记录在区块头中，以 1/1024 秒为单位，从 1970 年 1 月 1 日开始计算。

结构

区块由16个字段组成。每个字段的大小为32字节。区块字段有16种类型，目前已经使用的类型有8种，剩下的类型预留以后使用。一般地，区块的第0个字段的类型为区块头。

表1具体说明了不同字段类型的含义。

类型	描述

Nonce	可包含任意数值。该字段被用于工作量证明过程，通过枚举不同Nonce值来搜索使得区块难度尽可能大的Nonce。
区块头	区块头结构如下： - 传输层头。长度为8个字节。当计算区块哈希时，该字段必须设为0； - 字段类型掩码。表示该区块16个字段的类型。长度为64比特，采用小端字节序编码，每个类型用4比特表示。0号字段的类型写在低4位中； - 时间戳。长度为64比特，采用小端字节序编码； - 交易费用。长度为64比特，采用小端字节序编码。
输入交易	链接到另一个区块的哈希值。结构如下： - 区块的短哈希值（区块哈希以小端字节序表示的低24字节），长度为24比特； - 从区块输入的金额，长度为64比特，采用小端字节序编码。
输出交易	链接到另一个区块的哈希值。结构如下： - 区块的短哈希值（区块哈希以小端字节序表示的低24字节），长度为24比特； - 输出到区块的金额，长度为64比特，采用小端字节序编码。
输入交易半签名	输入交易的签名由2个输入交易半签名组成。第一个半签名代表r，第二个半签名代表s。r和s表示ECDSA算法的签名结果。签名使用ECDSA算法，使用私钥对区块摘要进行签名。区块摘要的计算公式为： hash(modified_block # key_prefix_byte # public_key) - #表示字符串连接； - modified_block表示待签名的区块数据，modified_block中所有的输入交易和输出交易的签名字段都置为0； - key_prefix_byte表示公钥参数y的奇偶性，如果公钥参数y是偶数，key_prefix_byte为0x02；如果公钥的参数y是奇数，key_prefix_byte为0x03； - public_key表示公钥的参数x，长度为32字节。

输出交易半签名	结构与输入交易半签名类似。
偶公钥	如果 ECDSA公钥的参数y是偶数，使用该字段类型存储ECDSA公钥的参数x。
奇公钥	如果 ECDSA公钥的参数y是奇数，使用该字段类型存储ECDSA公钥的参数x。
类型8-15	预留。

表1：区块字段类型描述

有效性校验

一个区块由若干输入交易、输出交易、公钥、输入/输出交易签名、费用组成。当满足以下条件时，区块是有效的：

- 区块时间戳大于XDAG纪元（XDAG主网上线的时间戳，以Unix系统格式表示为0x5A500000，即2018.1.6, 22:45:20 GMT）；
- 每一条输入交易和输出交易的时间戳小于区块的时间戳；
- 每一条输入交易和输出交易都是有效的区块（交易）；
- 所有的输入交易的金额之和小于2^64；
- 所有的输出交易的金额之和加上交易费用小于2^64；
- 所有的输入交易的金额之和不小于所有的输出交易的金额之和加上交易费用；
- 对于区块中的每一条输入交易，满足以下条件：记区块为A，输入交易为区块B，区块B使用的公钥记为K，公钥K对应的私钥记为P，输入交易B的签名记为S，S为使用私钥P对区块A的签名。区块B的输出交易签名为使用私钥P对区块B的签名。（换言之，只有区块B的所有者才能从区块B中提取币）；
- 输出交易签名占用的字段必须是偶数，而输入交易签名占用的字段有可能是奇数。当最后一个输入交易签名字段被用做Nonce，Nonce可被修改而不必重新签名。

账户

每一个区块都能包含金额，因此账户也是一个区块。用户只有拥有一个区块的输出交易签名的私钥，才拥有区块的所有权。用户通过区块的地址访问账户。区块的地址使用base64编码，通过计算区块的短哈希值得出。区块地址是32字节长度的字符串，包含A-Z，a-z，0-9，/，+。用户能够将他自己的账户中的金额转账到任意的区块。

Token

每一个区块都可包含XDAG Token。开始阶段，每一个区块的XDAG Token数额都是0。

区块的XDAG Token在以下情况发生变化：

- 区块通过挖矿产生新的XDAG Token。区块增加的Token数量为挖到的XDAG Token。
- 区块A是区块B的输入交易。当区块B被执行时，区块A的余额减少，减少量为区块B中区块A相对应的输入交易金额。
- 区块A是区块B的输出交易。当区块B被执行时，区块A的余额增加，增加量为区块B中区块A相对应的输出交易金额。
- 区块A是链接区块B的最小排序区块（可以理解为区块A直接引用区块B），当区块B执行时，区块A增加区块B的交易费用。

当区块的所有输出交易金额加上交易费用小于所有的输入交易金额，区块的金额增加，增加量为所有的输入交易金额之和减去所有输出交易金额之和与交易费。（区块的输入金额大于输出金额，差值为区块增加的金额）

交易执行

当满足以下条件时，区块可被执行：

- 区块中的每一条输入交易拥有的金额不小于区块中相应的输入金额。（每一条输入交易有足够的余额）
- 所有的输入交易金额之和加上交易本身的金额不小于所有输出交易金额之和加上交易费用。

主链

区块难度

区块难度用于衡量产生一个区块所包含的工作量证明。区块难度的计算公式为：

$$diff(block) = \frac{2^{128} - 1}{hash(block)/2^{160}}$$

hash(block)为区块的哈希值所代表的 256 位整数。
在 XDAG 中，每一个区块都可以计算难度。区块可包含一个 Nonce 字段，Nonce 字段可包含任意数值，不同的 Nonce 值使得区块计算出不同的区块难度。在工作量证明过程中，节点通过大量计算搜索使得区块难度值尽可能大的 Nonce 值。

链接

区块 A 链接区块 B 指的是，区块 A 直接指向区块 B。详细地说，区块 A 包含一个字段，该字段的类型为输入交易或者输出交易，值为区块 B 的哈希。

引用

区块 A 引用区块 B 指的是，存在从区块 A 到区块 B 的序列，序列中每一个区块都链接下一个区块。

i-引用

区块 A i-引用区块 B 指的是，区块 A 中第 i 个字段链接区块 C，而区块 C 引用区块 B。

链

链表示一个区块的序列，链中的每一个区块链接前一个区块。

链难度

一条链的难度为该链所包含的所有的区块的难度之和。

时间帧

时间帧表示一个长度为 64 秒的时间片。XDAG 将时间划分成一个个时间片，每个时间片的长度为 64 秒。t 是 Unix 系统格式表示的绝对时间，t 转换成二进制之后低 6 位为 0，从 t 秒到 t + 64 秒的时间段即为一个时间帧。第一个时间帧从 XDAG 纪元开始计算。

独立链

如果一条链中任意 2 个区块都属于不同的时间帧，我们称这样的链为独立链。

最短链

区块 A 到区块 B 的最短链指的是：从区块 A 到区块 B 的链上的每一个区块都 i-引用区块 B，且 i 为最小。

主链

XDAG 结构中难度最大的独立链称为主链。任意时刻都存在一条主链。

主块是指主链上的区块，主链中的任意一个区块都是主块。第一个主块为创世区块，主链中后一个主块指向前一个主块。任意 2 个主块属于不同的时间帧。所以每一个时间帧至多存在 1 个主块。

每一个主块可产生新的 XDAG Token。主链中的前 2^21 个主块每个主块可产生 1024 个 XDAG Token，之后的 2^21 个主块每个主块可产生 512 个 XDAG Token。每过 2^21 个主块，每个主块产生的 XDAG Token 都会减半。

算法

有向无环图

在图论中，如果一个有向图无法从某个顶点出发经过若干条边回到该点，则这个图是一个有向无环图（DAG 图）。

因为有向图中一个点经过两种路线到达另一个点未必形成环，因此有向无环图未必能转化成树，但任何有向树均为有向无环图。有向无环图示例如图 1 所示。

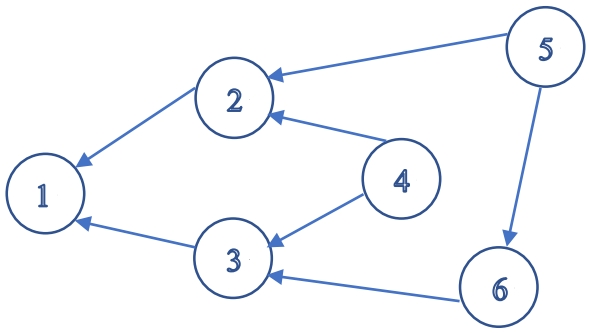

图 1：有向无环图示例

双花问题

DAG 应用于分布式账本无法解决双花问题。在 DAG 中，我们无法定义一个可应用于任意两条交易的偏序关系。如果尝试双花的两条交易不存在偏序关系，节点无法判断两条交易的先后顺序，也无法判断哪一条交易为有效的。
如图 2 所示，我们无法在交易 A 与交易 B 之间定义偏序关系，如果交易 A 和交易 B 存在双花问题，我们无法判断哪一条交易是有效的。

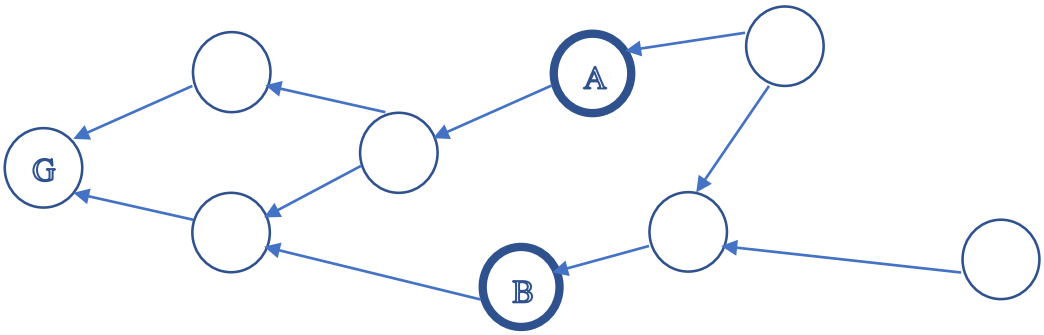

图 2：不存在偏序关系的两条交易

为了解决双花问题，XDAG 定义了主链的概念。XDAG 将所有的区块按照被主链引用的先后顺序进行排序，在任意两条交易之间建立了偏序关系，因此在所有区块之间建立了全序关系。对于存在双花问题的两条交易（交易即区块），认为在全序中排序靠前的交易是有效的，排序靠后的交易是无效的，以此解决了双花问题。

全序

XDAG 按照以下规则对区块建立全序关系：

规则1. 存在任意一个主块M，如果区块A被主块M引用，而区块B不被主块M引用，则区块A优先于区块B。

换言之，对于区块A和区块B，如果区块A被更早生成的主块引用，则区块A比区块B在全序中的排序更靠前。

规则2. 如果区块A和区块B在规则1下具有同等地位，即主块M同时为引用区块A的最小主块和引用区块B的最小主块，区块C是主块M到区块A和区块B的最短路径上的公共区块。若区块A被区块C i-引用，区块B被区块C j-引用，i < j，则区块A优先于区块B。

规则3. 如果区块A和区块B在规则1、2下具有同等地位，若区块A被区块B引用，则区块A优先于区块B。

图3为按照全序关系对区块进行排序的示意图。

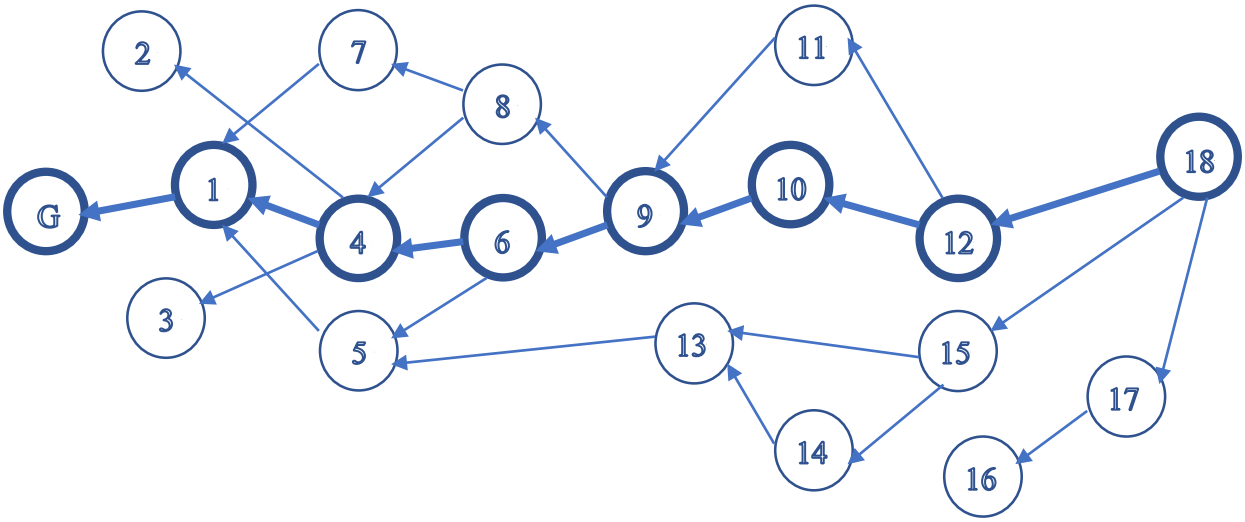

图 3：区块按全序关系排序示意图

工作量证明

XDAG 使用 Pow 生成区块的步骤如下：

1、 用户使用自己的私钥将交易进行签名，并将签好名的交易发送给XDAG网络中的节点，节点收到用户发送过来的交易之后，将交易存储在自己的交易缓存池中，并将交易广播给网络中的其他节点。

2、 网络中的矿工节点收到其他节点发送的交易，将交易存储在自己的交易缓存池中。在一个新的时间帧开始时，矿工节点会从交易缓存池中选择若干交易组织成DAG结构，并生成一个工作量证明的任务（我们称之为任务区块），这个工作量证明的任务是一个包含但未确定Nonce字段的区块，该区块引用了其他未打包的交易。

3、 在接下来的时间中，矿工节点通过穷举，不断调整任务区块的Nonce值，搜索使任务区块的哈希值尽可能小的Nonce（根据区块难度的计算公式，区块的哈希值越小，区块难度越大）。

4、 在一个时间帧结束时，矿工节点将搜索到的使得任务区块的哈希值最小的Nonce写入到任务区块，得到自己的候选主块，参与主块的竞争，并将该候选主块广播到XDAG网络中。

5、 XDAG网络中的节点收到矿工节点发送的候选主块，选择区块难度最大的候选主块，作为上一个时间帧的主块。产生主块的矿工将获得XDAG Token的奖励。

图4为XDAG工作量证明机制生成区块的示意图。

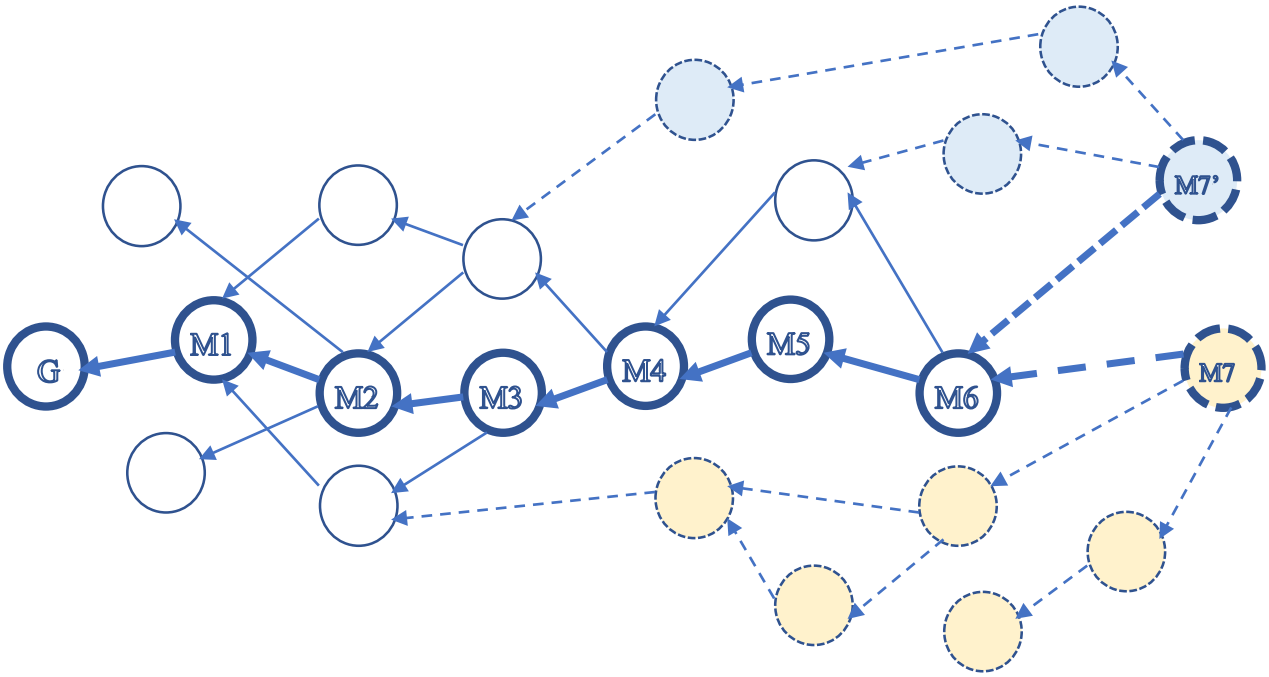

图4：工作量证明机制生成区块的示意图

加密和安全

签名

签名采用标准的 ECDSA算法。使用的椭圆曲线为Secp256k1。私钥的长度为32字节。公钥的长度为32字节（椭圆曲线的X坐标）加上1比特（椭圆曲线的Y坐标的奇偶性）。
签名的长度为64字节，由2个字段组成，即 ECDSA签名算法的r和s。

私钥

私钥的长度为32字节。公钥可以通过私钥计算得到，因此不必存储。

随机种子

当用户第一次启动程序时，程序要求用户输入一个随机的字符串。该字符串序列为用户随机数产生器的种子，被用来产生随机数。用户所有的私钥都是通过该随机种子产生。

网络通信

DNET

XDAG节点可以通过任何协议交换区块。区块的前8个字节被用来指定协议相关的信息。当计算区块的哈希值时，前8个字节必须设为0。XDAG程序默认使用dnet网络作为传输层。区块加密之后在网络上进行传输。每个区块通过半对称加密算法和临时key进行编码，并在接收方使用相同的key进行解码。临时key由发送方产生，使用发送方的私钥进行加密，并在接收方通过发送方的公钥进行解密。区块加密解密过程使用了8192位RSA算法。

控制块

控制块包含了节点向另一个节点发送的数据请求或者节点对其他节点数据请求的回复。控制块不是真正的区块，只是将请求信息或回复信息封装成区块的格式发送给其他节点。

控制块的第0个字段必须设置为0，第1个字段包含其他字段的类型掩码。

控制块的消息类型描述如表2所示：

类型	描述
类型0	请求一定时间段内的所有区块。开始时间存储在区块头中的时间戳字段，结束时间存储在区块头中的金额字段。
类型1	对类型0的控制块的请求的回复。后面跟随所有的请求区块。

类型2	请求一定时间段内的区块信息。开始时间存储在区块头中的时间戳字段，结束时间存储在区块头中的金额字段。
类型3	对类型2的控制块的请求的回复。回复内容用一个区块的格式表示，区块最后256字节是16个结构。时间段被平均分为16个子时间段，每一个结构和一个子时间段相对应。结构有2个字段： - 第一个64bit表示该段时间内所有区块的总大小，采用小端字节序编码。 - 第二个64bit表示该段时间内所有区块的校验sum，采用小端字节序编码。

表2：控制块的消息类型

统计信息

每一个包含请求信息的控制块在第1个字段中都包含一个ID。每一个包含回复信息的控制块的第1个字段也必须包含相同的ID。每一个控制块的第2、3字段以及第4字段的开头包含区块统计信息。

统计信息结构如下：

- 发送节点的主链的难度，16字节
- 网络中已知的主链最大难度，16字节
- 发送节点的有效区块数，8字节
- 网络中已知的最大有效区块数，8字节
- 发送节点的主区块数量，8字节
- 网络中已知的最大主区块数，8字节
- 发送节点已知的节点数，4字节
- 网络中已知的最大节点数，4字节

节点地址

控制块中的其余部分存储了发送节点已知的节点地址，每一个地址的长度为 6 字节，包含 IP 地址和端口。IP 地址用 4 字节表示，采用大端字节序编码。端口用 2 字节表示，采用小端字节序编码。

术语

区块地址：以base64格式编码的区块哈希值
区块：XDAG的基本结构。每一个区块拥有固定大小512 Bytes。
链：由多个区块组成的区块序列，序列中每一个区块指向前一个区块。
XDAG纪元：XDAG主网上线的时间戳，以Unix系统格式表示为0x5A500000，即2018.1.6, 22:45:20 GMT。
区块难度：用于衡量产生一个区块所包含的工作量证明。
链难度：一条链的难度为该链所包含的所有区块的难度之和。
哈希：对数据进行两次Sha256计算。
引用：区块A引用区块B指的是，存在从区块A到区块B的序列，序列中每一个区块都链接下一个区块。
链接：区块A链接区块B指的是，区块A直接指向区块B。
i-引用：区块A i-引用区块B指的是，区块A中第i个字段链接区块C，而区块C引用区块B。
时间帧：表示一个长度为64秒的时间片。
独立链：链中任意 2 个区块都属于不同的时间帧。
主链：难度最大的独立链。
主块：主链中的任一区块都是主块。
最短链：区块 A 到区块 B 的最短链指的是，从区块 A 到区块 B 的链上的每一个区块都 i-引用区块 B，且 i 为最小。
区块时间戳：记录在区块头中，以1/1024秒为单位，从1970年1月1日开始计算。
交易：交易即区块。
短哈希：哈希以小端字节序（little-endian）表示的低24字节。

赞助商

VBITEX交易所： VBITEX有限公司注册地为塞舌尔共和国，由专业运营团队成立于2017年11月。主站于2018年3月正式上线，致力打造五星级服务交易所。VBITEX遵循100%储备金原则，拥有双重风险控制监督部门对运营进行严格监督，以确保客户资金安全。

王博士の池子： 王博士の池子是全球领先的 xdag 矿池，以安全、稳定、专业著称，深得矿工信赖。王博士团队积极参与 xdag 社区建设，推动 xdag 技术在中国的发展，力争将 xdag 打造成最受欢迎的分布式账本项目。矿池查询地址：info.xdagmine.com，矿工交流 QQ 群：830894594。

吉池 Jeepool： 吉池 Jeepool 团队专注于挖矿项目的研究，包括 PoW 挖矿、PoS 挖矿、MN 主节点等服务，具有很强的独立研发能力。其中，吉池 JEEPOOL 旗下的 XDAG 矿池，以稳定高收益获得矿工信任，并在社区发展过程中持续传播高质量原创内容，推动了 XDAG 生态进步。

XDAG赞助地址： KhpddDKy625IYCBlOFojie9MzBq09qtz

感谢以上合作伙伴对 XDAG 白皮书的赞助和对 XDAG 中国基金会的支持。