初入链圈，很多人都可能被各种专业名词搞得晕头转向，因此，研究猿在这里整理了最常见48个区块链名词供大家参考。

1、Blockchain——区块链

区块链是分布式数据存储、点对点传输、共识机制、加密算法等计算机技术的新型应用模式。是一个共享的分布式账本，其中交易通过附加块永久记录。

2、Block——区块

在比特币网络中，数据会以文件的形式被永久记录，我们称这些文件为区块。一个区块是一些或所有最新比特币交易的记录集，且未被其他先前的区块记录。

3、区块头

区块头里面存储着区块的头信息，包含上一个区块的哈希值（PreHash），本区块体的哈希值（Hash），以及时间戳（TimeStamp）等等。

4、中本聪

自称日裔美国人，日本媒体常译为中本哲史，此人是比特币协议及其相关软件Bitcoin-Qt的创造者，但真实身份未知。

5、加密货币

加密货币是数字货币（或称虚拟货币）的一种。是一种使用密码学原理来确保交易安全及控制交易单位创造的交易媒介。

6、Node——节点

由区块链网络的参与者操作的分类帐的副本。

7、Oracles

Oracle通过向智能合约提供数据，它现实世界和区块链之间的桥梁。

8、去中心化

去中心化是一种现象或结构，必须在拥有众多节点的系统中或在拥有众多个体的群中才能出现或存在。节点与节点之间的影响，会通过网络而形成非线性因果关系。

9、共识机制

共识机制是通过特殊节点的投票，在很短的时间内完成对交易的验证和确认；对一笔交易，如果利益不相干的若干个节点能够达成共识，我们就可以认为全网对此也能够达成共识。

10、Pow——工作量证明

Proofof Work，是指获得多少货币，取决于你挖矿贡献的工作量，电脑性能越好，分给你的矿就会越多。

11、PoS——权益证明

Proofof Stake，根据你持有货币的量和时间进行利息分配的制度，在POS模式下，你的“挖矿”收益正比于你的币龄，而与电脑的计算性能无关。

12、智能合约

智能合约是一种旨在以信息化方式传播、验证或执行合同的计算机协议。智能合约允许在没有第三方的情况下进行可信交易，这些交易可追踪且不可逆转。

13、时间戳

时间戳是指字符串或编码信息用于辨识记录下来的时间日期。国际标准为ISO 8601。

14、图灵完备

图灵完成是指机器执行任何其他可编程计算机能够执行计算的能力。一个例子是Ethereum虚拟机(EVM)。

15、51%攻击

当一个单一个体或者一个组超过一半的计算能力时，这个个体或组就可以控制整个加密货币网络，如果他们有一些恶意的想法，他们就有可能发出一些冲突的交易来损坏整个网络。

16、Dapp——去中心化应用

是一种开源的应用程序，自动运行，将其数据存储在区块链上，以密码令牌的形式激励，并以显示有价值证明的协议进行操作。

17、DAO——去中心化自治组织

可以认为是在没有任何人为干预的情况下运行的公司，并将一切形式的控制交给一套不可破坏的业务规则。

18、DistributedLedger——分布式账本

数据通过分布式节点网络进行存储。分布式账本不是必须具有自己的货币，它可能

会被许可和私有。

19、DistributedNetwork——分布式网络

处理能力和数据分布在节点上而不是拥有集中式数据中心的一种网络。

20、预言机

预言机是一种可信任的实体，它通过签名引入关于外部世界状态的信息，从而允许确定的智能合约对不确定的外部世界作出反应。预言机具有不可篡改、服务稳定、可审计等特点，并具有经济激励机制以保证运行的动力。

21、零知识证明

零知识证明由S.Goldwasser、S.Micali及C.Rackoff在20世纪80年代初提出的。它指的是证明者能够在不向验证者提供任何有用的信息的情况下，使验证者相信某个论断是正确的。

22、PrivateKey——私钥

私钥是一串数据，它是允许您访问特定钱包中的令牌。它们作为密码，除了地址的所有者之外，都被隐藏。

23、PublicKey——公钥

是和私钥成对出现的，公钥可以算出币的地址，因此可以作为拥有这个币地址的凭证。

24、AES——高级加密标准

密码学中的高级加密标准(Advanced Encryption Standard，AES)，又称Rijndael加密法，是美国联邦政府采用的一种区块加密标准。

25、Wallet——钱包

一个包含私钥的文件。
它通常包含一个软件客户端，允许访问查看和创建钱包所设计的特定块链的交易。

26、冷钱包

通俗来说冷钱包就是将数字货币进行离线下储存的钱包，玩家在一台离线的钱包上面生成数字货币地址和私钥，再将其保存起来。而冷钱包是在不需要任何网络的情况下进行数字货币的储存，因此黑客是无法进入钱包获得私钥的。

27、SPV——轻钱包

轻钱包依赖比特币网络上其他全节点，仅同步与自己相关的数据，基本可以实现去中心化。

28、全节点

全节点是拥有完整区块链账本的节点，全节点需要占用内存同步所有的区块链数据，能够独立校验区块链上的所有交易并实时更新数据，主要负责区块链的交易的广播和验证。

29、Byzantinefailures——拜占庭将军问题

拜占庭将军问题是由莱斯利·兰伯特提出的点对点通信中的基本问题。含义是在存在消息丢失的不可靠信道上试图通过消息传递的方式达到一致性是不可能的。因此对一致性的研究一般假设信道是可靠的，或不存在本问题。

30、超级账本

超级账本（hyperledger）是Linux基金会于2015年发起的推进区块链数字技术和交易验证的开源项目。通过创建通用的分布式账本技术，协助组织扩展、建立行业专属应用程序、平台和硬件系统来支持成员各自的交易业务。

31、闪电网络

闪电网络的目的是实现安全地进行链下交易，其本质上是使用了哈希时间锁定智能合约来安全地进行0确认交易的一种机制，通过设置巧妙的“智能合约”，使得用户在闪电网络上进行未确认的交易和黄金一样安全。

32、P2P——对等网络

即对等计算机网络，是一种在对等者（Peer）之间分配任务和工作负载的分布式应用架构，是对等计算模型在应用层形成的一种组网或网络形式。

33、Mining——挖矿

挖矿是获取比特币的勘探方式的昵称。利用电脑硬件计算出币的位置并获取的过程称之为挖矿。

34、矿工

尝试创建区块并将其添加到区块链上的计算设备或者软件。在一个区块链网络中，当一个新的有效区块被创建时，系统一般会自动给予区块创建者（矿工）一定数量的代币，作为奖励。

35、矿池

是一个全自动的挖矿平台，使得矿工们能够贡献各自的算力一起挖矿以创建区块，获得区块奖励，并根据算力贡献比例分配利润（即矿机接入矿池—提供算力—获得收益）。

36、公有链

完全开放的区块链，是指任何人都可读取的、任何人都能发送交易且交易能获得有效确认的、全世界的人都可以参与系统维护工作，任何人都可以通过交易或挖矿读取和写入数据。

37、私有链

写入权限仅面向某个组织或者特定少数对象的区块链。读取权限可以对外开放，或者进行任意程度地限制。

38、联盟链

共识机制由指定若干机构共同控制的区块链。

39、主链

主链一词源于主网（mainnet，相对于测试网testnet），即正式上线的、独立的区块链网络。

40、侧链

楔入式侧链技术（pegged sidechains），它将实现比特币和其他数字资产在多个区块链间的转移，这就意味着用户们在使用他们已有资产的情况下，就可以访问新的加密货币系统。

41、跨链技术

跨链技术可以理解为连接各区块链的桥梁，其主要应用是实现各区块链之间的原子交易、资产转换、区块链内部信息互通，或解决Oracle的问题等。

42、硬分叉

区块链发生永久性分歧，在新共识规则发布后，部分没有升级的节点无法验证已经升级的节点生产的区块，通常硬分叉就会发生。

43、软分叉

当新共识规则发布后，没有升级的节点会因为不知道新共识规则下，而生产不合法的区块，就会产生临时性分叉。

44、Hash——哈希值

一般翻译做"散列"，也有直接音译为"哈希"的。简单的说就是一种将任意长度的消息压缩到某一固定长度的消息摘要的函数。

45、哈希率

假设挖矿是解一道方程题，而且只有把每个整数代入才能算出来，那么哈希率就是

每秒处理数据的速度。

46、hashtree——哈希树

哈希树是一种树形数据结构，每个叶节点均以数据块的哈希作为标签，而非叶节点则以其子节点标签的加密哈希作为标签。

47、SHA256

SHA-256是比特币一些列数字货币使用的加密算法。然而，它使用了大量的计算能力和处理时间，迫使矿工组建采矿池以获取收益。

48、Kyc

KYC是Know Your Customer的缩写，意思是了解你的客户，在国际《反洗钱法》条例中，要求各组织要对自己的客户作出全面的了解，以预测和发现商业行为中的不合理之处和潜在违法行为。