区块链入门必备 108 知识点

（欢迎同频者交流）

微信：eben079

1、什么是区块链

把多笔交易的信息以及表明该区块的信息打包放在一起，经验证后的这个包就是区块。每个区块里保存了上一个区块的 hash 值，使区块之间产生关系，也就是说的链了。合起来就叫区块链。

2. 什么是比特币

比特币概念是 2009 年中本聪提出的，总量是 2100 万个。比特币链大约每 10 分钟产生一个区块，这个区块是矿工挖了 10 分钟挖出来的。作为给矿工奖励，一定数量的比特币会发给矿工们，但是这个一定数量是每四年减半一次。现在是 12.5 个。照这样下去 2040 年全部的比特币问世。

3. 什么是以太坊

以太坊与比特币最大的区别是有了智能合约。使得开发者在上边可以开发，运行各种应用。

4. 分布式账本

它是一种在网络成员之间共享，复制和同步的数据库。直白说，在区块链上的所有用户都有记账功能，而且内容一致，这样保证了数据不可篡改性。

5. 什么是准匿名性

相信大家都有钱包，发送交易都用的钱包地址(一串字符串)这就是准匿名。

6. 什么是开放透明性/可追溯

区块链存储了从历史到现在的所有数据，任何人都可以查看，而且还可以查看到历史上的任何数据。

7. 什么是不可篡改

历史数据和当前交易的数据不可篡改。数据被存在链上的区块上，有一个 hash 值，如果修改该区块信息，那么它的 hash 值也变了，它后边的所有区块的 hash 值也必须修改，使成为新的链。同时主链还在进行交易产生区块。修改后链也必须一直和主链同步产生区块，保证链的长度一样。代价太大了，只为修改一条数据。

8. 什么是抗 ddos 攻击

ddos:黑客通过控制许多人的电脑或者手机，让他们同时访问一个网站，由于服务器的宽带是有限的，大量流量的涌入可能会使得网站可能无法正常工作，从而遭受损失。

但区块链是分布式的，不存在一个中心服务器，一个节点出现故障，其他节点不受影响。理论上是超过 51%的节点遭受攻击，会出现问题。

9. 主链的定义

以比特币为例，某个时间点一个区块让 2 个矿工同时挖出来，然后接下来最先产生 6 个区块的链就是主链

10．单链/多链

单链指的是一条链上处理所有事物的数据结构。多链结构，其核心本质是公有链+N 个子链构成。只有一条，子链理论上可以有无数条，每一个子链都可以运行一个或多个 DAPP 系统

11. 公有链/联盟链/私有链

公有链:每个人都可以参与到区块链
联盟链:只允许联盟成员参与记账和查询
私有链:写入和查看的权限只掌握在一个组织手里。

12. 共识层数据层等

区块链整体结构有六个:数据层，网络层，共识层，激励层，合约层，应用层。数据层:记录数据的一层，属于底层技术;网络层:构建区块链网络的一种架构，它决定了用户与用户之间通过何种方式组织起来。共识层:提供了一套规则，让大家接收和存储的信息达成一致。激励层:设计激励政策，鼓励用户参与到区块链生态中;合约层:一般指“智能合约”，它是一套可以自动执行，根据自己需求编写的合约体系。应用层:区块链上的应用程序，与手机的 app 类似前分布式存储研发中心

13. 时间戳

时间戳是指从 1970 年 1 月 1 日 0 时 0 分 0 秒 0...到现在的当前时间的总秒数，或者总纳秒数等等很大的数字。每个区块生成时都有一个时间戳，表明生成区块的时间。

14．区块/区块头/区块体

区块是区块链的基本单元，区块头和区块体是区块链的组成部分。区块头里面包含的信息有上一个区块的 hash，本区块的 hash，时间戳等等。区块体就是区块里的详细数据。

15. Merkle 树

Merkle 树，也叫二叉树，是存储数据的一种数据结构，最底层是所有区块包含的原始数据，上一层是每个区块的 hash 值，这一层的 hash 两两组合产生新的 hash 值，形成新的一层，然后一层层往上，-直到产生一个 hash 值。这样的结构可以用于快速比较大量的数据，不需要下载全部的数据就可以快速的查找你想要的最底层的历史数据。

16 什么是扩容

比特币的一个区块大小大约是 1M 左右，可以保存 4000 笔交易记录。扩容就是想把区块变大，能保存更多的数据。

17. 什么是链

每个区块都会保存上一个区块的 hash，使区块之间产生关系，这个关系就是链。通过这个链把区块交易记录以及状态变化等的数据存储起来。

18．区块高度

这个不是距离上说的高度，它指是该区块与所在链上第一个区块之间相差的区块总个数。这个高度说明了就是第几个区块，只是标识作用。

19. 分叉

同一时间内产生了两个区块(区块里的交易信息是一样的,只是区块的 hash 值不一样)，之后在这两个区块上分叉出来两条链，这两条链接下来谁先生成 6 个区块，谁就是主链，另外的一条链丢弃。

20．幽灵协议

算力高的矿池很容易比算力低的矿机产生区块速度快，导致区块链上大部分区块由这些算力高的矿池产生的。而算力低的矿机产生的区块因为慢，没有存储到链上，这些区块将会作废。

幽灵协议使得本来应该作废的区块，也可以短暂的留在链上，而且也可以作为工作量证明的一部分。这样一来，小算力的矿工，对主链的贡献比重就增大了，大型矿池就无法独家垄断对新区块的确认。

21. 孤块

之前说过分叉，孤块就是同一时间产生的区块，有一个形成了链，另一个后边没有形成链。那么这个没形成链的块就叫孤块。

22. 叔块

上边说的孤块，通过幽灵协议，使它成为工作量证明的一部分，那它就不会被丢弃，会保存在主链上。这个区块就是下

23 重放攻击

就是黑客把已经发送给服务器的消息，重新又发了一遍，有时候这样可以骗取服务器的多次响应。

24．有向无环图

也叫数据集合 DAG(有向非循环图)，DAG 是一种理想的多链数据结构。现在说的区块链大都是单链，也就是一个区块连一个区块，DAG 是多个区块相连。好处是可以同时生成好几个区块，于是网络可以同时处理大量交易，吞吐量肯定就上升了。但是缺点很多，目前属于研究阶段。

25. 什么是挖矿

挖矿过程就是对以上这六个字段进行一系列的转换、连接和哈希运算，并随着不断一个一个试要寻找的随机数，最后成功找到一个随机数满足条件:经过哈希运算后的值，

比预设难度值的哈希值小，那么，就挖矿成功了，节点可以向邻近节点进行广播该区块，邻近节点收到该区块对以上六个字段进行同样的运算，验证合规，再向其它结点转播，其它结点也用同样的算法进行验证，如果全网有 51%的结点都验证成功，这个区块就算真正地“挖矿”成功了，每个结点都把这个区块加在上一个区块的后面，并把区块中与自己记录相同的列表删除，再次复生上述过程。另外要说的是，不管挖矿成不成功每个节点都预先把奖励的比特币 50 个、所有交易的手续费(总输入-总输出)记在交易列表的第一项了(这是“挖矿”最根本的目的，也是保证区块链能长期稳定运行的根本原因)，输出地址就是本结点的地址，但如果挖矿不成功，这笔交易就作废了，没有任何奖励。而且这笔叫作“生产交易”的交易不参与“挖矿”计算。

26. 矿机/矿场

矿机就是各种配置的计算机，算力是他们的最大差距。矿机集中在一个地的地方就是矿场

27. 矿池

就是矿工们联合起来一起组成一个团队，这个团队下的计算机群就是矿池。挖矿奖励，是根据自己的算力贡献度分发。

28. 挖矿难度和算力

挖矿难度是为了保证产生区块的间隔时间稳定在某个时间短内，如比特币 10 分钟出块 1 个。算力就是矿机的配置。

29. 验证

当区块链里的验证是对交易合法性的一种确认，交易消息在节点之间传播时每个节点都会验证一次这笔交易是否合法。比如验证交易的语法是否正确，交易的金额是否大于 0，输入的交易金额是否合理，等等。验证通过后打包，交给矿工挖矿。

30. 交易广播

就是该节点给其他节点通过网络发送信息。

31. 矿工费

区块链要像永动机一样不停的工作，需要矿工一直维护着这个系统。所以要给矿工们好处费，才能持久。

32. 交易确认

当交易发生时，记录该笔交易的区块将进行第一次确认，并在该区块之后的链上的每一个区块进行再次确认:当确认数达到 6 个及以上时,通常认为这笔交易比较安全并难以篡改。

33. 双重交易

就是我有 10 块钱，我用这 10 块钱买了一包烟，然后瞬间操作用这还没到付的 10 块钱又买了杯咖啡。所以验证交易的时候，要确认这 10 块钱是否已花费。

34. UTXO 未花费的交易输出

它是一个包含交易数据和执行代码的数据结构，可以理解为存在但尚未消费的数字货币。

35. 每秒交易数量 TPS
也就是吞吐量，tps 指系统每秒能处理的交易数量。

36. 钱包
与支付宝类似，用来存储数字货币的，用区块链技术更加安全。

37. 冷钱包/热钱包
冷钱包就是离线钱包，原理是储存在本地，运用二维码通信让私钥永不触网。热钱包就是在线钱包，原理是将私钥加密后存储在服务器上，当需要使用时再从服务器上下载下来，并在浏览器端进行解密。

38. 软件钱包/硬件钱包
软件钱包是一种计算机程序。一般而言，软件钱包是与区块链交互的程序，可以让用户接收、存储和发送数字货币，可以存储多个密钥。硬件钱包是专门处理数字货币的智能设备。

39. 空投
项目方把数字货币发送给各个用户钱包地址。

40. 映射
映射跟区块链货币的发行相关，是链与链之间的映射。比如有一些区块链公司，前期没有完成链的开发，它就依托于以太坊发行自己的货币，前期货币的发行、交易等都在以太坊上进行操作。随着公司的发展，公司自己的链开发完成了公司想要把之前在以太坊上的信息全部对应到自己的链上，这个过程就是映射。

41. 仓位
指投资人实有投资和实际投资资金的比例

42. 全仓
全部资金买入比特币

43．减仓
把部分比特币卖出，但不全部卖出

44．重仓
资金和比特币相比，比特币份额占多

45．轻仓
资金和比特币相比，资金份额占多

46. 空仓

把手里所持比特币全部卖出，全部转为资金

47. 止盈
获得一定收益后，将所持比特币卖出以保住盈利

48. 止损
亏损到一定程度后，将所持比特币卖出以防止亏损进一步扩大

49. 牛市
价格持续上升，前景乐观

50. 熊市
价格持续下跌，前景黯淡

51. 多头（做多）
买方，认为币价未来会上涨，买入币，待币价上涨后，高价卖出获利了结

52. 空头（做空）
卖方，认为币价未来会下跌，将手中持有的币（或向交易平台借币）卖出，待币价下跌后，低价买入获利了结

53. 建仓
买入比特币等虚拟货币

54. 补仓
分批买入比特币等虚拟货币，如：先买入 1BTC，之后再买入 1BTC

55. 全仓
将所有资金一次性全部买入某一种虚拟币

56. 反弹
币价下跌时，因下跌过快而价格回升调整

57. 盘整（横盘）
价格波动幅度较小，币价稳定

58. 阴跌
币价缓慢下滑

59. 跳水（瀑布）
币价快速下跌，幅度很大

60. 割肉
买入比特币后，币价下跌，为避免亏损扩大而赔本卖出比特币。或借币做空后，币价上涨，赔本买入比特币

61. 套牢

预期币价上涨，不料买入后币价却下跌；或预期币价下跌，不料卖出后，币价却上涨

62. 解套

买入比特币后币价下跌造成暂时的账面损失，但之后币价回升，扭亏为盈

63. 踏空

因看淡后市卖出比特币后，币价却一路上涨，未能及时买入，因此未能赚得利润

64. 超买

币价持续上升到一定高度，买方力量基本用尽，币价即将下跌

65. 超卖

币价持续下跌到一定低点，卖方力量基本用尽，币价即将回升

66. 诱多

币价盘整已久，下跌可能性较大，空头大多已卖出比特币，突然空方将币价拉高，诱使多方以为币价将会上涨，纷纷买入，结果空方打压币价，使多方套牢

67. 诱空

多头买入比特币后，故意打压币价，使空头以为币价将会下跌，纷纷抛出，结果误入多头的陷阱

68. 什么是 NFT

NFT 全称“Non-Fungible Tokens” 即非同质化代币，简单来说，即区块链上一种无法分割的版权证明，主要作用数字资产确权，转移，与数字货币区别在于，它独一无二，不可分割，本质上，是一种独特的数字资产。

69. 什么是元宇宙

元宇宙是一个虚拟时空间的集合，由一系列的增强现实（AR），虚拟现实（VR）和互联网（Internet）所组成，其中数字货币承载着这个世界中价值转移的功能。

70. 什么是 DeFi

DeFi，全称为 Decentralized Finance，即“去中心化金融”或者“分布式金融”。“去中心化金融”，与传统中心化金融相对，指建立在开放的去中心化网络中的各类金融领域的应用，目标是建立一个多层面的金融系统，以区块链技术和密码货币为基础，重新创造并完善已有的金融体系

71. 谁是中本聪？

中本聪是比特币的开发者兼创始者。2008 年 11 月 1 日中本聪发表了比特币白皮书，并于 2009 年 1 月 3 日首次挖出比特币，谁能动用创世区块里的比特币谁便是中本聪本人，所以谁是中本聪呢？历史上出现过很多个“中本聪”：2013 年，有人爆料在数

学领域有过卓越贡献的望月新一就是中本聪，但是并没有提出直接证据。2014 年，黑客黑进了中本聪用过的邮箱，并找到了邮件的主人多利安•中本（Dorian Nakamoto），随后多利安表示自己只是偶然获取了邮箱的地址和密码，并不是中本聪。2016 年，克雷格•赖特(CraigWright)表示他是中本聪，且能提供中本聪的私钥。但随后，赖特因为无法面对大家的质疑而撤回自己的声明。

72. 比特币和 Q 币不一样

比特币是一种去中心化的数字资产，没有发行主体。Q 币是由腾讯公司发行的电子货币，类似于电子积分，其实不是货币。Q 币需要有中心化的发行机构，Q 币因为腾讯公司的信用背书，才能被认可和使用。使用范围也局限在腾讯的游戏和服务中，Q 币的价值完全基于人们对腾讯公司的信任。

比特币不通过中心化机构发行，但却能够得到全球的广泛认可，是因为比特币可以自证其信，比特币的发行和流通由全网矿工共同记账，不需要中心机构也能确保任何人都无法窜改账本。

73. 矿机是什么？

以比特币为例，比特币矿机就是通过运行大量计算争夺记账权从而获得新生比特币奖励的专业设备，一般由挖矿芯片、散热片和风扇组成，只执行单一的计算程序，耗电量较大。挖矿实际是矿工之间比拼算力，拥有较多算力的矿工挖到比特币的概率更大。随着全网算力上涨，用传统的设备（CPU、GPU）挖到比特的难度越来越大，人们开发出专门用来挖矿的芯片。芯片是矿机最核心的零件。芯片运转的过程会产生大量的热，为了散热降温，比特币矿机一般配有散热片和风扇。用户在电脑上下载比特币挖矿软件，用该软件分配好每台矿机的任务，就可以开始挖矿了。每种币的算法不同，所需要的矿机也各不相同。

74. 量化交易是什么？

量化交易，有时候也称自动化交易，是指以先进的数学模型替代人为的主观判断，极大地减少了投资者情绪波动的影响，避免在市场极度狂热或悲观的情况下做出非理性的投资决策。量化交易有很多种，包括跨平台搬砖、趋势交易、对冲等。跨平台搬砖是指，当不同目标平台价差达到一定金额，在价高的平台卖出，在价低的平台买入。

75. 区块链资产场外交易

场外交易也叫 OTC 交易。用户需要自己寻找交易对手，不通过撮合成交，成交价格由交易双方协商确定，交易双方可以借助当面协商或者电话通讯等方式充分沟通。

76. 时间戳是什么？

区块链通过时间戳保证每个区块依次顺序相连。时间戳使区块链上每一笔数据都具有时间标记。简单来说，时间戳证明了区块链上什么时候发生了什么事情，且任何人无法篡改。

77. 区块链分叉是什么？

在中心化系统中升级软件十分简单，在应用商店点击“升级”即可。但是在区块链等去中心化系统中，“升级”并不是那么简单，甚至可能一言不合造成区块链分叉。简单说，分叉是指区块链在进行“升级”时发生了意见分歧，从而导致区块链分叉。因为没有中心化机构，比特币等数字资产每次代码升级都需要获得比特币社区的一致认可，如果比特币社区无法达成一致，区块链很可能形成分叉。

78. 软分叉和硬分叉

硬分叉，是指当比特币代码发生改变后，旧节点拒绝接受由新节点创造的区块。不符合原规则的区块将被忽略，矿工会按照原规则，在他们最后验证的区块之后创建新的区块。软分叉是指旧的节点并不会意识到比特币代码发生改变，并继续接受由新节点创造的区块。矿工们可能会在他们完全没有理解，或者验证过的区块上进行工作。软分叉和硬分叉都"向后兼容"，这样才能保证新节点可以从头验证区块链。向后兼容是指新软件接受由旧软件所产生的数据或者代码，比如说 Windows 10 可以运行 Windows XP 的应用。而软分叉还可以"向前兼容"。

79. 区块链项目分类和应用

从目前主流的区块链项目来看，区块链项目主要为四类：第一类：币类；第二类：平台类；第三类：应用类；第四类：资产代币化。

80. 对标美元的 USDT

USDT 是 Tether 公司推出的对标美元（USD）的代币 Tether USD。1USDT=1 美元，用户可以随时使用 USDT 与 USD 进行 1:1 兑换。Tether 公司执行 1:1 准备金保证制度，即每个 USDT 代币，都会有 1 美元的准备金保障，对 USDT 价格的恒定形成支撑。某个数字资产单价是多少 USDT，也就相当于是它的单价是多少美元（USD）。

81. 山寨币和竞争币

山寨币是指以比特币代码为模板，对其底层技术区块链进行了一些修改的区块链资产，其中有技术性创新或改进的又称为竞争币。因为比特币代码开源，导致比特币的抄袭成本很低，甚至只需复制比特币的代码，修改一些参数，便可以生成一条全新的区块链。

82. 三大交易所

币安：https://accounts.binancezh.ac/zh-CN

Okex: https://www.ouyi.top/

火币：https://www.huobi.af/zh-cn

83. 行情软件

Mytoken：http://www.mytoken.com/

非小号：https://www.feixiaohao.co/

84. 资讯网站

巴比特：https://www.8btc.cn

金色财经：http://www.jinse.com/

币世界快讯：http://www.bishijie.com

85. 区块链浏览器

BTC：https://btc.com/

ETH：https://etherscan.io/

BCH：https://blockchair.com/bitcoin-cash/blocks

LTC：http://www.qukuai.com/search/ltc

ETC：https://gastracker.io/

86. 钱包

Imtoken：https://imatoken.net/

比特派：https://bitpie.com/

MetaMask（小狐狸）：https://metamask.io/

87. 去中心化交易所

uniswap： https://uniswap.org

88. NFT 交易所

Opensea：https://opensea.io
Super Rare：https://superrare.com/

89. 梯子

自备，购买靠谱梯子

90. 平台币

平台发行的数字货币，用于抵扣手续费，交易等

91. 牛市、熊市

牛市：上涨行情
熊市：下跌行情

92. 区块链 1.0

基于分布式账本的货币交易体系，代表为比特币

93. 区块链 2.0

以太坊（智能合约）为代表的合同区块链技术为 2.0

94. 区块链 3.0

智能化物联网时代，超出金融领域，为各种行业提供去中心化解决方案

95. 智能合约

智能合约，Smart Contract，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，简单说，提前定好电子合约，一旦双方确认，合同自动执行。

96. 什么是通证？

通证经济就是以 Token 为唯一参考标准的经济体系，也就是说相当于通行证，你拥有 Token ,就拥有权益，就拥有发言权。

97. 大数据和区块链的区别

大数据是生产资料，AI 是新的生产力，区块链是新的生产关系。大数据指无法在一定时间范围内用常规软件工具进行捕捉、管理和处理的数据集合，是需要新处理模式才能具有更强的决策力、洞察发现力和流程优化能力的海量、高增长率和多样化的信息资产。简单理解为，大数据就是长期积累的海量数据，短期无法获取。区块链可以作为大数据的获取方式，但无法取代大数据。大数据只是作为在区块链运行的介质，

没有绝对的技术性能，所以两者不能混淆。(生产关系简单理解就是劳动交换和消费关系，核心在于生产力，生产力核心在于生产工具)

98. 什么是 ICO

ICO，Initial Coin Offering，首次公开代币发行，就是区块链数字货币行业中的众筹。是 2017 最为热门的话题和投资趋势，国家 9.4 出台监管方案。说到 ICO，人们会想到 IPO，两者有着本质不同。

99. 数字货币五个特征

第一个特征：去中心化
第二个特征：有开源代码
第三个特征：有独立的电子钱包
第四个特征：恒量发行的
第五个特征：可以全球流通

100. 什么叫去中心化？

没有发行方，不属于任何机构或国家，由互联网网络专家设计、开发并存放于互联网上，公开发行的币种。

100. 什么叫衡量（稀缺性）？

发行总量一旦设定，永久固定，不能更改，不能随意超发，可接受全球互联网监督。因挖掘和开采难度虽时间数量变化，时间越长，开采难度越大，所开采的币就越少，因此具有稀缺性。

101. 什么叫开源代码？

用字母数字组成的存放在互联网上，任何人都可以查出其设计的源代码，所有人都可以参与，可以挖掘，全球公开化。

102. 什么叫匿名交易？ 专有钱包私密？

每个人都可以在网上注册下载钱包，无需实名认证，完全由加密数字代码组成，全球即时点对点发送、交易，无需借助银行和任何机构，非本人授权任何人都无法追踪、查询。

104. 什么是合约交易？

合约交易是指买卖双方对约定未来某个时间按指定价格接收一定数量的某种资产的协议进行交易。合约交易的买卖对象是由交易所统一制定的标准化合约，交易所规定了其商品种类，交易时间，数量等标准化信息。合约代表了买卖双方所拥有的权利和义务。

105. 数字货币产业链

芯片厂家～矿机厂商～矿机代理～挖矿～出矿到交易所～散户炒币

106. 二本是谁？

二本：数字货币价值投资者

投资风格：稳健

建立社群：二本杂谈（高质量价投社群）

107. 二本投资策略

长短结合，价投为主，不碰合约，不玩短线

合理布局，科学操作，稳健保守，挣周期钱

108. 如何联系二本？

有且仅有一个微信：eben079，其余均为冒充，欢迎币友交流，共谋发展