

大家好，感谢邀请，今天来为大家分享一下元宇宙合约钱包交易链接的问题，以及和元宇宙zkn合约地址的一些困惑，大家要是还不太明白的话，也没有关系，因为接下来将为大家分享，希望可以帮助到大家，解决大家的问题，下面就开始吧！

本文目录

1. [佛萨奇怎么下载](#)
2. [bxen币怎么换xen币](#)
3. [“虚拟币”骗局曝光,有人被骗百万](#)
4. [区块链入门108个知识点](#)
5. [区块链入门必备108知识点](#)

佛萨奇怎么下载

你好，您可以去佛萨奇官方网站进行下载，或者去应用商店进行下载。

在以太坊DApp用户榜与Gas消耗榜上，一个名为Forsage（中文名为佛萨奇）的项目自年初以来长期占据榜单前三的位置，最高单日交易笔数超4万笔、活跃地址超2万，总参与地址超过110万，资金参与价值超3亿美金。

看看老外

今年经常在以太坊相关数据网站查看信息的投资者或许都看到过这个名字，再进一步了解或许能知道这是资金盘项目，但大多对Forsage如何运作、为何吸引到庞大用户群体不甚了解。

据了解，Forsage项目由据称为俄罗斯居民的LadoOkhotnikov于今年2月初发起，是一个使用以太坊智能合约运作的类金字塔模式项目，用户通过向智能合约支付一定ETH后加入该计划，并通过邀请更多用户向智能合约支付ETH获得佣金奖励，带有明显的传销性质，但其走红更关键的原因在于其中的双矩阵、奖励滑落等设计。

今年8、9月，Forsage项目开始大规模入华宣传，通过线下与线下等多种渠道诱导民众参与该项目，目前国内参与者预计超过3万，已经导致大量参与者遭受损失。

资金盘游戏的设计Forsage的走红不仅仅在于将常见的多级分销网络搬到以太坊智能合约上，更在于充分利用智能合约的特性最大程度刺激参与者的心理弱点与参与热情。根据各方面资料显示，用户参与Forsage项目首先需要打开来自上级推荐者的链接，并向Forsage智能合约支付0.05个ETH，该智能合约不沉淀任何资金，而

是会将这部分资金分为两部分通过x3矩阵与x4矩阵自动转入上级或更上级推荐者的以太坊钱包，即各有0.025个ETH。

国内社区的宣传资料不同矩阵有不同的运作机制，x3矩阵的设计是每个用户ID下设有3个点位，即三个被推荐者位置，前两个被推荐者的0.025个ETH会直接转入推荐者钱包地址，第三个被推荐者的资金会自动转入其推荐者的更上一级推荐者用户地址。此后的推荐用户则会重复进行这个流程，即每发展两名下线的奖金归自己，每发展第三名下线的奖励归自己的上级。x4矩阵的设计是每个用户ID设有6个推荐者点位，前2个推荐者的0.025个ETH都会转入该用户上线推荐者的钱包地址，第3、4、5个推荐者的发展资金则归该用户，第6个推荐者的资金则会随机转入附近点位的用户钱包。进入这个资金盘的门槛虽然是0.05ETH，但这两个矩阵分别还设有12个级别，门槛从0.05ETH、0.1ETH最高可至51.2ETH，每个级别的资金门槛都是前一级别的两倍，用户每投入一笔ETH都会按照前述机制转入更高级别推荐者钱包。

Forsage诱导用户投入更多ETH、提升矩阵级别的机制在于，如果某用户的矩阵级别低于其下线的级别，那么来自下线的奖励就会绕过该用户钱包，「滑落」至推荐层级更高、矩阵级别不低于该用户的上线钱包。举例而言，如果某用户只开通到0.5 ETH级别的矩阵，如果其下线投入3.2个ETH开通更高级别矩阵，那么这名下线的资金分配会完全绕过该用户，从而产生类似加密货币交易领域的「FOMO」心理。

在官网通过引人注目的数据刺激用户加入在这种情况下，Forsage用户在投入参与后的收益就可以来自两部分，一部分为所谓的动态收益，即源于自己直接推荐用户的奖励，需要投入大量精力拓展下线；另一部分则是所谓的静态收益，只要用户开通的矩阵级别够高并发展了一定数量的下线，那么就可能出现其下线在进一步发展下线时，出现矩阵级别低于更低下线的情况，那么就可以享受到这些下线的「滑落」收益。更具体而言，Forsage相比于过去的传销与资金盘项目，主要有以下几个特点：设有极低的资金门槛，声称「几百即可参与国际项目」，后续再通过各种机制刺激投入；层级关系与收益高低没有直接关系，用户可以通过开通更高级别的矩阵提升自己「拦截」滑落奖励的可能；声称基于智能合约运行，不存在资金沉淀与崩盘风险。

从以上种种来看，Forsage完全具有金字塔骗局与资金盘的特征，参与者不直接创造任何价值，而是通过发展下线用户参与来获得收益，但对于市场拓展能力不强以及较后期的参与者不利，很可能出现收益低于投入的情况。

尽管如此，由于Forsage相对新鲜的玩法机制，很快在部分地区流行起来，特别是今年5、6月份开始，该项目在菲律宾、印尼等经济相对落后地区引起大范围的传播与参与，大部分日期的活跃地址都超过1万个。

bxen币怎么换xen币

有人一天零撸20万美元的XENCrypto到底是什么？

初晓链

2022年10月12日15:19江苏

关注

这几天加密圈子有一个项目XENCrypto很火，初晓链尝试来介绍下什么是XEN。

XEN是在10月9日在Ethereum网络上线的，是PoP(Proof of Participation参与证明)模式，全民共建虚拟挖矿项目。

创始人是谷歌前21号员工Jack Levin，没有预先铸造，没有管理员密钥，不可变合约，从零供应开始，100%透明和链上。

项目没有参与门槛，任何玩家只要链接钱包支付少量gas费即可领取，铸造后可以选择质押1天或以上时间，质押时间长短决定收获的XEN数量。

质押到期需及时领取，否则XEN数量会逐渐减少，7天后只剩下1%。

图片

ETH网络XEN当前总供应量超过100亿

XEN上线第二天就有人创建了XEN/ETH的LP流动性，XEN就开始有价格了。

从上线最初的0.005U短时间涨到0.01美元然后持续下跌，目前价格是0.00016。

据说有人在第一天铸造了1000个地址，第二天领取卖出，平均每个钱包撸了200刀，妥妥地一天零撸20万刀。

真是有人看热闹，有人闷声赚大钱。

质押一天的钱包，从最初几百刀的收益变成8刀，扣除铸造、领取、交易的gas费，已经不值得短期参与了。

如果也想参与社会实验，可以选择更长时间周期的，看看未来有没有新的故事。

毕竟这样全民参与，说不定真的能带来全新体验，有意外收获。

质押一天的收益已经不够GAS费了

XEN已经计划在多链上布局。

目前BSC网络已上线，8个小时，已经有超过150万个钱包地址铸造了。

玩家已经把ETH网络上玩法搬到BSC链上来，明天质押到期的XEN不知道会不会有新的财富效应，或直接归零了。

后期XEN还会在Avalanche、Polygon/MATIC、Arbitrum、Optimism、Cronos、Fantom等网络陆续上线。

不同网络上的XEN不能等比例兑换，可以按照一定的比例转换并相互跨链。

BSC网络上的XEN铸造地址数150多万

热度来得非常快，去得也很快。

XEN上线4天，已经走过一轮牛熊了。

第二天领取的XEN，第一时间可以卖出600多多，随后快速下跌，6个小时之后就只有80刀，到第三天就只剩下8刀了，已经不够gas费了。

随着财富效应消失，短期参与的人越来越少。

当然，还有上线质押了100天，200天，300天等更长时间的玩家，不知那时是否还有热度，还是已经无人问津了。

XEN项目已经燃烧了4076个ETH

项目创始人JackLevin是一个连续创业者，从谷歌离职后开启了很多项目。

从2010年开始接触点对点支付的比特币，2011年开始挖比特币。

但他认为POW挖矿方式浪费电力，工作量证明是过时的方式，他希望通过其他方

式探索区块链，推出了XEN的尝试。

XEN是区块链免费提供的token，基于自我托管、无需信任的共识和去中心化，是全民可参与的。

没有预先铸造，没有集中所有权，没有控制权，开源的智能合约。

所有人在XEN面前具有同等机会，随着时间推移以及共识越来越大，XEN有可能发挥更重要的作用。

当然，这一切都有待时间揭晓，是创造更美好的体验，还是归零尝试，都不确定。

图片

最初有人质押一天收获668美元

在加密世界，任何创新玩法，都有可能被传播出圈。

从BTC、ETH，到DOGE、SHIB等，还有PEOPLE，XEN，每个新尝试都是全民狂欢，不断刷新玩法，带来全新体验。

如果你也有好的点子，加密世界是绝好的实验平台。

以上，只是我个人的看法，无投资建议。

我是初晓链，我在关注元宇宙和web3。

“虚拟币”骗局曝光,有人被骗百万

“虚拟币”骗局曝光，有人被骗百万

“虚拟币”骗局曝光，有人被骗百万，通过区块链代币游戏实现获利是不稳定的，甚至很有可能是一场骗局。不要轻信所谓的好机会，对于能在短时间内赚快钱的说法要谨慎，“虚拟币”骗局曝光，有人被骗百万。

“虚拟币”骗局曝光，有人被骗百万1

在元宇宙概念的加持下，各种NFT链游项目蓬勃发展，犯罪团伙也紧跟风口，开发所谓的链游项目、发行游戏代币并上线去中心化交易所。

凌风透露，以虚拟货币为噱头的这类网络传销案早在三四年前就已出现，国外则更多。“这类案件特征明显，基本都是用新的虚拟货币相关概念炒作，吸引民众参与投资。”他说。

凌风表示，“在推特、贴吧等平台上，如果有人主动私聊，给你介绍他们的项目，那么这些基本可判断为骗局；如果有人发邀请码，则基本可判定为传销。”

根据知帆科技发布的《2021年区块链和虚拟货币犯罪趋势研究报告》（以下简称《报告》），虚拟货币传销类案件的模式主要包括交易所模式、钱包模式、虚假“智能合约”模式、智能合约模式、矿机租赁模式、云矿机模式、量化机器人模式、短视频模式、矩阵DAPP模式、链游元宇宙模式这10种典型情况。

以当下火热的“元宇宙”为例，在元宇宙概念的加持下，各种NFT链游项目蓬勃发展，犯罪团伙也紧跟风口，开发所谓的链游项目、发行游戏代币并上线去中心化交易所。

《报告》指出，该类案件通常为项目方通过蹭热点、挂靠知名项目等手法吸引投资人入场，不断拉升游戏代币价值，又靠动静结合的高额收益来吸引更多投机者加入，其本质仍是靠用户兑换平台币消耗的主流币来扩大资金池，项目方趁机套钱跑路。

业内人士分析称，作为新型网络传销形式，虚拟货币传销隐蔽性强，但骗术万变不离其宗，不外乎三大典型特征：一是入门费，投资者需通过交纳费用取得加入资格；二是拉人头，传销参与者的收益来源于其所发展的下线成员交纳的费用；三是复式计酬，以直接或间接发展人员的数量作为依据给付报酬。

针对前述这些情况，相关部门也在加大监管力度。比如2022年2月底，最高人民法院首次将虚拟币交易纳入非法吸收资金的情形之中。另外，中国银保监会此前也发布了关于防范以“元宇宙”名义进行非法集资的风险提示。

记者注意到，在今年两会期间，多名人大代表、政协委员也表达了加强元宇宙相关产业监管的观点。全国政协委员、第五空间信息科技研究院院长、上海市信息安全行业协会名誉会长谈剑锋表示，目前，以区块链技术为基础的NFT虚拟艺术品（如卡通人像、电子油画）等在“元宇宙”大行其道，而监管却较难落实，可能形成新的洗钱通道。

“数字经济要深化发展，必须要和实体经济融合发展，但同时要谨防资本利用国家

发展规划和热点概念，制造新的虚拟经济泡沫，防止个别人钻政策红利‘空子’、割投资者‘韭菜’。”谈剑锋说。

中国人民大学副教授王鹏对记者表示，目前包括电信诈骗、非法集资等网络诈骗层出不穷，主要是利用了大众两个心态，一是新技术、新要素或者新的应用产生，大家普遍不理解；二是投机心理，未经了解就去投机、想去赚一笔快钱。

为此，王鹏提出以下建议以便防范以元宇宙、NFT等概念为噱头的网络诈骗，一是相关政府监管部门要加强打击力度，及时发现相关的线索，及时切断、及时处置，而不是说把小问题转化成了大的社会性问题才去处置；

二是行业协会等相关专业化机构要针对元宇宙、NFT等新技术出台相关的行业守则，加强对大众的教育；三是大众媒体要加强相关的宣传，一方面是对技术应用本身加强宣传，去掉技术的神秘感，另一方面是让大家提高风险意识。

“最后，我觉得从自身角度出发，一是要加强对于技术的学习，不要人云亦云，风险和收益是成正比的，收益越高风险越高；二是不要轻信所谓的好机会，对于能在短时间内赚快钱的说法要谨慎，要从长远出发考虑问题。”王鹏说。

“虚拟币”骗局曝光，有人被骗百万2

近来，菲律宾国内有超过15万年轻人沉迷于玩一款宠物养成游戏赚钱。其原理是玩家通过饲养一个小精灵获得电子卡牌。这种卡牌其实是一种虚拟货币，玩家可在专门的网络加密交易平台自由交易，从而换取现实中的货币。

这些年轻人靠“挖矿”得到虚拟货币，每月能获得几百美元不等的收入。这本质上就是包着游戏外衣的区块链代币游戏，然而在人均月收入约200美元的菲律宾，玩游戏还能获得一笔不菲的收入，对于年轻人来说无疑有着巨大的吸引力。

然而要看到，通过区块链代币游戏实现获利是不稳定的，甚至很有可能是一场骗局。比如今年年初风靡一时的“火星志愿者”区块链游戏，虽然蹭上了元宇宙和马斯克，宣传“边玩边赚”、收益高达万倍，但是需要先花600多元购入虚拟币，最终游戏宣传的高收益因币值崩溃化为泡影。

针对此类行为，今年2月18日中国银保监会发布的《关于防范以“元宇宙”名义进行非法集资的风险提示》中就提到，一些不法分子蹭热点，以“元宇宙投资项目”“元宇宙链游戏”等名目吸收资金，涉嫌非法集资、诈骗等违法犯罪活动。从本质

上来说，打着玩游戏的旗号获得的虚拟代币到底能换多少钱，是基于极不稳定的市场交易价值，一旦崩溃，最后就会沦为了一场泡沫游戏。

因此，中国一直注重对比特币等的监管，去年5月，国务院金融稳定发展委员会召开会议，要求坚决防控金融风险，打击比特币挖矿和交易行为。从纯技术的角度看，专业矿机在区块链“挖矿”效率上远胜过一般玩游戏的机器。中国一度占据全球“矿场”算力60%以上，许多“矿工”在中国寻找小水电等能源便宜的地方布设了海量矿机。

然而，中国即使能通过挖比特币等各类币种获取一些海外收益，仍然坚决关停了各地的矿场，算力占全球比例迅速降到5%以下。这是正确的决策，因为浪费巨量的能源只是用来生产赌场的筹码，对中国整体而言没有益处，许多人发现之前显卡的价格大涨，就是与大量显卡被用于挖矿有关。如果引发年轻人参与区块链货币炒作，后果则会更加糟糕。

但是像中国如此坚决监管并关停各类区块链货币炒作的国家在全球范围内并不多。韩国青年因生活压力巨大，纷纷参与数字货币游戏，指望一夜暴富。2017年冬天，全球最大宗的比特币交易有三分之二发生在韩国。

毫无疑问，数字技术的发展是新世纪以来全球经济的亮点，但是对“e时代”的年轻人来说不见得全是好事。全球大多数国家的年轻人生长于数字技术飞速发展的时代，受各种暴富神话的影响，他们对财富的认知也在发生变化。上一代人在工厂流水线上辛苦工作积累财富的方式在年轻人心中“大势已去”，没有吸引力了。

其实对于菲律宾等劳动力众多、缺少就业机会的国家，即使是收入一般的工厂流水线工作，对年轻人来说也是不错的发展起点，而且工厂还能解决大量就业，当地政府非常欢迎。然而，电子文化先于工业文化侵袭了这些国家，只需要低档的电脑和手机就足以让整个国家的年轻人沉迷其中。

因此，有的国家意识到这个问题，会将数字技术引导向正确的用途，如在疫情期间提倡远程教学、限制青少年打游戏的时间、对游戏内容进行监管。但是世界各国发展水平不一，能通过发展享受到数字技术的成果已经不容易，想要进一步兴利除弊则提出了更高的挑战。

无论科技如何进步，国家想要实现长远发展，年轻人奋发向上的精神内核不能丢。拨开技术编织的迷雾，正确认识种种新包装下的庞氏骗局或者泡沫经济炒作，是正能量社会的应有之义。

随着人工智能、机器人、新能源等各种科技的不断进步，也许有朝一日，传统行业的劳动性质会发生本质上的改变，但这种改变需要将年轻人引向真正的科技创新，而非越来越多地沉溺于“资本与人性”的泡沫游戏。

“虚拟币”骗局曝光，有人被骗百万3

日常生活中，经常有陌生电话号称免费拉人进股票群；网络平台上，也经常有各种股票讲课的广告。很多人抱着不花钱只是进群看看、听听课的心态，没想到却一步步陷入被骗的漩涡，损失惨重。记者在调查过程中发现，这些股票群里所谓的“老师”首先推荐股票，取得信任后，就会推荐自行发行的虚拟数字货币，来骗取投资者钱财。

“虚拟币”号称100倍溢价网站关闭卷款跑路

记者以投资者的身份潜伏进股票群后发现，全国各地有不少受害者因为免费而入群。

声音来源——某股票群讲课音频：贝特曼是我国首家、唯一一家数字货币平台即将上线。该平台要发行它的平台币相当于它的股票，相当于IPO。我预计它的平台币有10到20倍的溢价，甚至有100倍的溢价。

在所谓10倍到100倍暴利诱惑下，很多人买入大量“虚拟币”。突然，贝特曼虚拟货币交易平台一夜之间关闭，毫无征兆，股票群被解散，再也联系不到任何一个所谓的“老师”或“客服”，受害者投入的所有资金都无法提取。有受害者表示，被骗金额最高达百万元。

北京市投资者：4月9日凌晨1点钟，半夜醒了以后拿手机看一眼这个盘面怎么样，发现平台点不开了，所有数字都不见了，自己账号也空了，那些群都没了，所有链接都打不开了。我一共被骗了40多万元，多的被骗100多万元。

广东省深圳市投资者：我老公生病了，我们贷款出来，基本上这100多万元都是贷的。现在最主要的问题是有小孩子读书，信用卡还不上会影响征信，小孩子读书读不了，我的信用都会出问题，已经走头无路了。

一位股龄近20年的女士，投资非常谨慎，觉得自己肯定不会被骗，刚开始看着群里其他人纷纷跟着老师操作数字货币也不为所动。但是，随着群里人不停晒一些超高利润的盈利截图，以及“老师”的不断洗脑，于是也抱着试试的心态投进了第一

笔钱。

河南省平顶山市投资者：还是禁不住诱惑，先转进去了4000元，打新又中奖了，晚上12点又买进，等于44000元全投入进去了。投入进去之后，他说这是锁仓期，又开始发行了平台币，平台币又是10倍的利润。

北京市康达律师事务所律师夏禹：我国《刑法》的第二百六十六条的规定，涉嫌诈骗罪，根据具体的犯罪情节，最高有可能判处10年以上有期徒刑，甚至无期徒刑。

用股票讲课当幌子人情关怀蒙骗老年人

为何这种常见的诈骗套路能屡试不爽？记者发现，除了打感情牌取得受害者的信任，最重要的是，这些诈骗团伙多次冒充一些大型的正规金融平台为自己背书，编造一些虚假的一夜暴富故事，引诱受害者上钩。

记者在股票群中看到，这个网络讲课平台名为“朗盛翻倍大讲堂”。投资者通过其发布的股票授课广告而加入，很多人一开始抱着试试看的心态进入平台听课。除了讲课，每天半夜所谓的“老师”还会发长文为“学员”答疑解惑，配上美女头像的“助理老师”，随时解答“学员”的股票疑问。在逐渐取得信任后，“老师”游说“学员”购买虚拟数字货币。

广东省深圳市投资者：开始给你推荐几只股赚钱了，后面推荐的几只股，他就不管了，一直叫你拿着，然后说现在大行情不好，就让你把股票全部卖了，来买新币。

北京市投资者：虚拟币利润太高了，高到一会儿几元、几十元就涨上去了，我们这一拨最终炒的是要达到10倍。他循循善诱地讲课，人情味特浓，特别关心人。

不少受害者告诉记者，他们也曾有过怀疑，但诈骗团伙屡屡用一些大型券商的身份作为背书来迷惑投资者，记者在股票群里看到，一旦有投资者表达出疑惑，马上就会被禁言或踢出群，最后留下的都是一些没有接触过虚拟货币，缺乏金融知识的受害者。

受害人向记者透露，直到现在他们都没见过这个所谓的证券公司李总，甚至都不知道他的全名。

并且，事后他们才反应过来，“贝特曼虚拟货币交易平台”实际上并不存在，所谓的“虚拟货币”打新和涨跌幅也并不真实，完全是诈骗平台自导自演的数字假象。

五类网络诈骗屡禁不止警方提示风险

目前，多名受害者已经报案。记者在调查中发现，目前还有很多类似的诈骗团伙仍在行骗。那么，普通投资者应该如何避免被骗？

多名受害者告诉记者，他们最近发现又有新的股票讲课平台和新的数字货币交易平台出现。当他们用自己的手机号及身份证信息注册登录时，发现只要以前在贝特曼交易平台上注册过的人，在新的所谓的“奥斯曼交易平台”注册后，账号都显示处于冻结状态无法进入。

北京市投资者：我发现了一个奥斯曼平台，也是数字货币。内容跟贝特曼一样，就是名字不一样。币种有些区别，其他的操作方式，包括资金管理、新币申购、流水查询等内容都一模一样。

记者又在多个网络平台发现，还有非常多受害者在不同时间也被同样的手段骗过，除了平台名字及讲课老师名字不同，其他行骗手段几乎完全一样。在得知被骗后，多位受害者已经报警。

北京市公安局大兴分局红星派出所工作人员：这个案子已经立案并展开调查，后期刑警负责查。

警方表示类似的诈骗案件非常多，投资者一定要提高警惕，向陌生账户转账过后，一旦感觉异常，应该立即报警。

目前公安机关发现的诈骗类型已经超过50种，其中5种主要类型案件高发多发，分别是网络刷单返利、虚假投资理财、虚假网络贷款、冒充客服、冒充公检法。

北京市康达律师事务所律师夏禹：在此提醒广大投资者应选择正规、合法的投资渠道。谨记“天上不会掉馅饼”，应警惕那些超高收益的投资。

区块链入门108个知识点

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，并把区块中与自已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段内，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-FungibleTokens”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DecentralizedFinance，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？

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篡改账本。

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Windows10可以运行WindowsXP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TetherUSD。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/>

87.去中心化交易所

uniswap：<https://uniswap.org>

88.NFT交易所

Opensea：<https://opensea.io>

SuperRare：<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，SmartContract，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。

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)

ICO, InitialCoinOffering,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。

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

108.二本？

欢迎币友，共谋发展

区块链入门必备108知识点

区块链入门必备108知识点

(欢迎同频者交流)

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-FungibleTokens”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DecentralizedFinance，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？

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篡改账本。

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Windows10可以运行WindowsXP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TetherUSD。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

Okex

火币

83.行情软件

Mytoken

非小号

84.资讯网站

巴比特

金色财经

币世界快讯

85.区块链浏览器

BTC

ETH

BCH

LTC

ETC

86.钱包

Imtoken

比特派

MetaMask (小狐狸)

87.去中心化交易所

uniswap

88.NFT交易所

Opensea

SuperRare

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，SmartContract，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，InitialCoinOffering,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。

101.什么叫衡量（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。

102.什么叫开源代码？

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。

103.什么叫匿名交易？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.北枫是谁？

北枫：数字货币价值投资者

投资风格：稳健

建立社区：北斗社区（高质量价投社区）

107.北斗投资策略

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.北枫？

欢迎币友，共谋发展

如果你还想了解更多这方面的信息，记得收藏关注本站。