区块链百问

深入浅出全面了解区块链，
专业易懂的区块链扫盲读本

链得得

区块链特刊

前言

2019 年注定已成为中国区块链发展的重要里程碑式年份，10 月 24 日也成为了一个标志性的日子。

这一天，中共中央政治局就区块链技术发展现状和趋势进行第十八次集体学习。同时，中共中央总书记习近平在主持学习时强调，区块链技术的集成应用在新的技术革新和产业变革中起着重要作用。我们要把区块链作为核心技术自主创新的重要突破口，明确主攻方向，加大投入力度，着力攻克一批关键核心技术，加快推动区块链技术和产业创新发展。

而就在此次政治局集体学习区块链技术的前几天，Facebook 的 CEO 扎克伯格在美国国会听证会上再次就 Libra 阐述其想法，他在听证会上提到：“中国是 Libra 最大的竞争对手，中国的金融 IT 基础设施领先于美国。”美国国会议员也提到，中国的移动支付（支付宝、微信支付等）已经全面超过并且冲击着 Facebook 和美国企业。

Coinbase 联合创始人透露，美国高级官员在讨论 Libra 的合法性同时，也一直在探讨另外一个可能性，那就是如何利用区块链发行数字美元。可以说，数字美元未来也将势在必行。

习主席的这次表态不是偶然的，习主席也很少亲自对某一特定技术做专门阐述，说明这是高层经历了长时间的观察和学习，做的国家战略意义层面和世界科技、金融新格局层面更深邃的思考。中国和美国都在这场争夺战中试图占领先机和高地。

但通往区块链之路，注定艰难。难在过程，考验各国、各级政府的治理智慧，各类企业的投入决心和克制、民间机会主义博弈，以及前所未有的技术、经济与金融伦理挑战。这样激发国家、社会和全人民的技术趋势挑战与分歧，已经在第三次工业革命后多年都未曾有过了。而几乎每一次技术革命，都引发了一场思想变革。

回顾历史，在此之前，每一次工业革命，也几乎都是一次社会撕裂的过程，更是一次社会阶层与财富的重新分配过程。

但是区块链世界还才刚刚开始萌芽，怪现状也层出不穷。一边如火如荼，一边一头雾水，左右彷徨；一边激情四射，一边萎靡切割，骗局不断。可能整个市场疑惑的最大问题都暂时还不是区块链未来会变成什么样，而是区块链到底是什么，能做什么，能怎么和我相关。所以在最近的一个月，我们走访了中、美、欧、日、韩市场众多区块链关心者，筛选了 100 多个大家最关心的区块链问题，并采访了诸多专业人士，通过问答的方式梳理出来。

我们的笨功夫，最终由钛媒体和链得得联合制作并形成了这份特刊《**区块链 100 问——深入浅出全面了解区块链**》，帮助大家清楚辩解理解区块链，辩析区块链，**希望这本特刊小册也能成为你学习区块链的重要助手“红宝书”。**

* 小帖士：自 2018 年初开始，钛媒体基于对区块链趋势的判断和重力投入的决心，拆分区块链内容和数据相关业务，成立了链得得科技和 ChainDD 美国公司，在过去近两年链得得 ChainDD 在获得高速发展的同时，也愈发理解这个领域与乱象并存的巨大价值，我们宁愿放弃了诸多投机机会，做了很多这样的原创笨功夫，希望这样的笨功夫能够让更多人受益。如果你还有进一步交流的想法，也欢迎出席即将于 2019 年 12 月 8 日由链得得参与举办的 CHAINSIGHTS 金融科技与区块链中国峰会，该会也是 2019 T-EDGE 全球创新大会重要组成部分，众多国内外金融政策层、传统金融机构、新兴区块链巨头等各界领袖都将齐聚。

目录

区块链 100 问

一、核心概念篇

1. 什么是区块链?

区块链是一个集合了密码学、分布式储存、智能合约、共识算法等多种新兴技术的数据传输方式，本质上是一种集成技术，而非一个特定技术的发明。

区块链本质上是一个应用了密码学技术的，多方参与、共同维护、持续增长且不可篡改的分布式数据库系统，也称为分布式共享账本。在数据上传的过程中，数据会被打包到一起形成一个个数据块，而被打包好的数据块又有另一个学名叫做区块，将每个区块按照时间顺序连在一起，就形成了链式的网络，因为整个网络结构时由区块和链构成的，所以就给他取名叫 Blockchain。作为共享账本，就可理解为，每一个账页就是一个区块，每一个区块写满了交易记录，区块首尾衔接，紧密相连，形成链状结构。

所以，区块链用一种去中心化的方式，解决了信任背书和价值传递的问题。

2. 区块链有哪些特点?

区块链的特点：匿名性、可扩展性、开放性，不可撤销、不可篡改和加密安全性。

区块链是透明共享的总帐本，这帐本在全网公开，你拿到它的公钥，你就知道它帐里面到底是有多少钱，所以任何一次的价值转换，全世界有兴趣的人都能在旁边看着你，转换是由矿工来帮你确认的，所以它是一个互联网共识机制。这个帐本是没有办法篡改的，因为你的行为不是由你来记录，不是由你来说是还是不是，是由这个网络上其他的人来决定这是不是这么一回事。

3.什么是比特币，与区块链什么关系?

2008 年 11 月 1 日，一位叫做中本聪的人在网上发表了一篇名为《比特币：一种点对点式的电子现金系统》的论文，这是比特币第一次出现在人们的视野中。2009 年 1 月 3 日推出了比特币算法客户端，正式启动了这个特殊的金融系统，这天也是比特币第一个“创世块”出现。第一个区块奖励是 50 个比特币，创世块出了 10 分钟后，第一批 50 个比特币生成了，而此时的货币总量就是 50。随后比特币就以约每 10 分钟 50 个的速度增长。所以，2009 年 1 月 3 日一直被定义为比特币诞生日。

根据中本聪的比特币白皮书算法，比特币发行总量限制为 2100 万个，当总量达到 1050 万时（2100 万的 50%），区块奖励减半为 25 个。当总量达到 1575 万（新产出 525 万，即 1050 的 50%）时，区块奖励再减半为 12.5 个。该货币系统曾在 4 年内只有不超过 1050 万个，之后的总数量将被永久限制在约 2100 万个。

随着比特币自 2009 年开始的自动良好运行，越来越多的全球用户开始持有比特币，交易比特币，这套支持比特币运行的技术底层系统也开始受到技术界的关注。后人开始研究区块的形成机制，链接机制，发现比特币底层区块系统本质上就是一个去中心化的数据库，同时作为比特币的底层技术，是一串使用密码学方法相关联产生的数据块，每一个数据块中包含了一批次比特币网络交易的信息，用于验证其信息的有效性（防伪）和生成下一个区

块，并将此命名为 Blockchain。Blockchain（区块链）作为比特币的底层技术系统开始为人熟知，并且越来越多的人开始挖掘区块链在其他应用层面的价值。故也有人将比特币成为称为区块链第一个成功应用，但从概念出现的时间上来说，是先有比特币，后有区块链。

4. 谁是中本聪?

中本聪作为比特币的发明者，被人们称为“比特币之父”。但自从 2010 年开始，他逐渐淡出，项目也移交给比特币社区的其他成员。

值得一提的是，中本聪为人十分低调，直到今天他的身份仍是一个谜，但是疑似他名下的比特币账户却至今没有动过，仍然是比特币全球最大持币账户。尽管人们对他的身份进行过诸多猜测，并且也有人跳出来表示自己就是中本聪，但这些说法的的可信度都实在是太低。

* 链得得曾经邀请并且与中本聪比特币项目第一个核心开发人员 Martii Malmi 做过一期对话，谈到了中本聪和早期比特币的开发过程，*

《【链得得全球行 · 北京】寻找中本聪：后比特币时代的区块链未来》

5. 区块链的去中心化是什么意思，安全性如何?

去中心化，比如，像平时淘宝购物用的淘宝，他实际上中心化的，不管是选择商品还是支付交易，对于买家和卖家来说，都有一个绕不开的平台，阿里巴巴，它作为中心平台，维护着整个网络购物生态，所谓去中心化，就是把阿里这个中心去掉，重新建立一套大家可以共同管理数据，且能自由交易的新规侧，中心化有很多问题，在中心话的模式里，数据都存储在中心服务器里，一旦这个服务器瘫痪，整个网络都会出现问题，除此之外，行业数据集中在少数几家巨头公司，由于数据管理不透明，一旦数据泄露，后果是灾难性的。

而去中心化的好处就在于人人参与数据维护，数据信息不再集中，从而解决了这些问题，所以去中心化可以说是互联网世界的未带变革，每个人都可以平等地参与数据的管理与维护。区块链之所以被誉为趋势，是因为去中心化的公平性。

区块链是一种分布式数据库技术。分布式技术主要指的是存储架构。区块链采取的分布式架构不仅将账本数据存储在每个结点上，而且每个结点都必须包含整个账本的数据。这种彻底的分布式架构带来的是比中心化更高的安全性，没有人可以同时摧毁所有的节点。

6. 什么是点对点传输?

对点技术（peer-to-peer，简称 P2P）又称对等互联网络技术，网络中不存在中心节点，各个节点间的权利都是相同的，任意两个点之间都可以进行交易，交易成功后全网所有节点都会记录这个交易这种模式的好处是不把依赖都聚集在较少的几台服务器上，从而避免单点故障。

7. 什么是区块链节点?

负责维护网络运行的终端就可以称之为——节点。在互联网领域，企业所有的数据运行都集中在自己的服务器中，那么这个服务器就是一个节点。比如我们使用的微信，每天处理着这么多的聊天信息、转账等。这些数据的存储和运行都在腾讯的公司的服务器里面。那么这个处理数据的服务器，就可以称之为“节点”

区块链是去中心化的分布式数据库，他不依托于哪一个中心化的服务器，而是由千千万万个“小服务器”组成。只要我们下载一个区块链客户端，我们就变成了那千千万万个“小服务器”中的一员。

节点分为“全节点”和“轻节点”，全节点就是拥有全网所有的交易数据的节点，那么轻节点就是只拥有和自己相关的交易数据节点。节点分布越多、越广泛，区块链网络就更加的去中心化，网络运行也就越安全稳定。

8. 什么是区块高度?

比特币网络大概每 10 分钟生产一个记录交易的区块。从最初的 1 个区块、2 个区块慢慢累积，到现在将近 500000 个区块。而比特币区块高度，就是指生成到第多少个区块。比如 BCX 在高度 498888 分叉，意思就是比特币在生成第 498888 个区块时执行分叉操作。

9. 什么是智能合约?

智能合约(Smart Contract)并不是一个新的概念，早在 1995 年就由跨领域法律学者 Nick Szabo 提出：智能合约是一套以数字形式定义的承诺(Promises)，包括合约参与方可以在上面执行这些承诺的协议。在区块链领域中，智能合约本质可以说是一段运行在区块链网络中的代码，它以计算机指令的方式实现了传统合约的自动化处理，完成用户所赋予的业务逻辑。

10. 什么是共识机制?

共识机制就是所有记账节点之间怎么达成共识，去认定一个记录的有效性，这既是认定的手段，也是防止篡改的手段。区块链提出了四种不同的共识机制，适用于不同的应用场景，在效率和安全性之间取得平衡。

区块链的共识机制具备“少数服从多数”以及“人人平等”的特点，其中“少数服从多数”并不完全指节点个数，也可以是计算能力、股权数或者其他的计算机可以比较的特征量。“人人平等”是当节点满足条件时，所有节点都有权优先提出共识结果、直接被其他节点认同后并最后有可能成为最终共识结果。

* 关于共识机制内容，下载链得得 App， 参考详文：

《【得得白话】以太坊完成最终升级的路上，为何要换共识机制？》

11. 什么是隔离见证?

通常简写为 SegWit，是区块链的一种扩容方式。

目前区块链上每个区块内不仅记录了每笔转账交易的具体信息，即在哪个时间点账户收到或转出多少比特币，还包含了每笔交易的数字签名，且数字签名占比较大。矿工在打包区块的时候需要用数字签名一一验证每笔交易，确认没有问题之后才会将该笔交易记录在区块里。隔离见证就是把区块内的数字签名信息拿出去，让每个区块可以承载更多笔交易，从而达到扩容的目的。”

12. 什么是数字货币?

数字货币也被称为加密货币，是一种基于节点网络和数字加密算法的虚拟货币。

不由央行或当局发行，也不与法币挂钩，但由于被公众所接受，所以可作为支付手段，也可以电子形式转移、存储或交易。

	电子货币	虚拟货币	数字货币
发行主体	金融机构	网络运营商	无
使用范围	一般不限	网络企业内部	不限
发行数量	法币决定	发行主体决定	数量一定
储存形式	磁卡或账号	账号	数字
流通方式	双向流通	单向流通	双向流通
货币价值	与法币对等	与法币不对等	与法币不对等
信用保障	政府	企业	网民
交易安全性	较高	较低	较高
交易成本	较高	较低	较低
运行环境	内联网，外联网，读写设备	企业服务器与互联网	开源软件以及P2P网络
典型代表	银行卡，公交卡	Q币，论坛币	比特币，莱特币

13. 什么是代币（Token）？

在区块链领域可看作是一种可流通的加密数字权益证明。

1) 权益证明（一种数字形式存在的权益凭证，代表一种权利，一种固有的内在价值和使用价值）；
2) 加密（为了防止篡改，保护隐私等）；
3) 可流通性（可以进行交易，兑换等）。

14. 什么是挖矿？

挖矿，就是利用芯片进行一个与随机数相关的计算，得出答案后以此换取相应的数字货币作为奖励。

此前挖矿是利用计算机进行相关的计算来获取数字货币奖励，但随着算力的不断增加，使用计算机挖矿的成本越来越高。后出现了专门获取数字货币的机器，这种机器也就是所谓的矿机。

15.矿机是什么？

用于挖掘（生产）加密货币的机器。

广义的说，矿机可以是一切可以运行挖矿程序的机器，比如专业矿机、家用电脑、智能手机、服务器、智能路由器、智能手表、智能电视机等等。

狭义的说，矿机指的是专业挖矿设备，比如 ASIC 矿机、显卡矿机，以及一些币种的专属矿机（PFS 矿机）等。

16. 什么是算力？

算力（也称哈希率）是比特币网络处理能力的度量单位。即为计算机（CPU）计算哈希函数输出的速度。

在通过“挖矿”得到比特币的过程中，我们需要找到其相应的解 m，而对于任何一个六十四位的哈希值，要找到其解 m，都没有固定算法，只能靠计算机随机的 hash 碰撞，而一个挖

矿机每秒钟能做多少次 hash 碰撞，就是其“算力”的代表，单位写成 hash/s,这就是所谓工作量证明机制 POW(Proof Of Work)。

17.什么是矿池、矿场?

在全网算力提升到了一定程度后，单台机器挖到块的概率变得非常的低。这种现象的发展，促使一些“bitcointalk”上的极客开发出一种可以将少量算力合并联合运作的方法，使用这种方式建立的网站便被称作“矿池”(MiningPool)。

矿池的收益分配主要有：PPLNS、PPS、PROP 三种形式。

所谓的比特币矿场就是建造一个工厂,将数十台、数千台采矿机器放在一起进行数学运算和挖掘比特币。这涉及电力消耗问题。一个矿场的成本包含:建设成本、设备成本、维护成本网络成本、还有其他成本。

* 有关挖矿、算力、矿机、矿场等内容，链得得曾发表一系列文章进行科普和讨论，下载链得得 App， 参考详文：

《【得得白话】算力与挖矿，为何总让币圈魂牵梦绕？》
《【大文观链】ASIC：为什么没人用显卡挖比特币了？》
《【大文观链】比特币算力和矿池集中化趋势有没有解？》

18. 什么是钱包、钱包地址、私钥、公钥?

加密数字货币钱包能提供钱包地址的创建、加密数字货币转账、每个钱包地址交易历史的查询等基础金融功能。

钱包一般分为冷钱包和热钱包，主要区别是互联网是否能访问到秘钥。

每个钱包地址都对应着一个公钥和一个私钥。私钥只有用户可以拥有，而公钥可公开发行配送，只要有要求即可取得。

举例：一个送信者需要传送一个信息给一个收信者，而信息的秘密性是必要的，送信者以收信者的公开的钥匙来加密，而仅有收信者的私有的钥匙能够对此信息解密。

19. 什么是区块链的扩容?

当初为了保证比特币的安全性及稳定性，中本聪将区块的大小限制在 1MB。然而随着区块链上交易数不断增长，每秒 7 笔交易的处理速度已经明显无法满足用户需求。所以便通过修改比特币底层代码的方式，达到提高交易处理能力的目的。

目前比特币扩容有两种技术方案：1、通过改变区块链共识部分的内容，使区块容量变大。2、把大量的计算移到链下，即通过侧链的技术加以解决问题。

*了解更多关于区块链的扩容问题，下载链得得 App， 参考详文：

《【大文观链】链下交易：为什么交易所的处理速度这么快？》
《【大文观链】分片技术是区块链扩容的完美解吗？》
《【大文观链】透析 DAG：区块链结构扩容的双刃剑》
《【大文观链】链下交易方案的应用实例：闪电网络、雷电网络》

每日报告

不要错过让你洞察整个商业世界的每日报告

如何免费入群？扫码加好友后回复【入群】

每日精选3份最值得学习的资料给您，不定期分享顶级外文期刊

撩他！ 撩他！

二、技术开发篇

20.现在有哪些主流的区块链技术?

比特币(Bitcoin)，是最早的真正意义的去中心化区块链技术。

以太坊（Ethereum），配备了强大的图灵完备的智能合约虚拟机，因此可以成为一切区块链项目的母平台。

IBM HyperLedger fabric，是联盟链的优秀实现。

Ripple，世界上第一个开放的支付网络，是基于区块连的点到点全球支付网络。

21.区块链由哪些结构组成?

区块链是由区块相互连接形成的链式存储结构，区块就是链式存储结构中的数据元素，其中第一个区块被称为创始区块。

一般区块包括区块头和区块体两部分。区块头包含每个区块的身份识别信息，如版本号、hash 值、时间戳、区块高度等信息；区块体主要包含具体的交易数据。

22.数据存在哪里呢？是否每个节点都要有足够大的存储介质?

区块链采用分布式存储的方式，区块链的数据是由区块链节点使用和存储的，而多个节点通过网络进行链接最终形成了完整的区块链网络。

关于节点的大小，以比特币网络节点为例，有完整节点 (Full node)、修剪节点 (Pruning node)、SPV 轻量节点 (Lightweight node)之分，这种分类方式基于两点差异：一是这个节点是否下载了最新最完整的比特币区块链；二是该节点能否独立验证比特币的转账交易，即能否独立实现作为一个节点的基本功能。

完整节点下载了最新的完整区块链数据，是比特币网络的主心骨。使用此类节点的主要包括两类人，一是独立挖矿的矿工，二是使用默认设置运行比特币软件 (Bitcoin core) 的用户。
修剪节点同样可以独立完成比特币转账的确认，但是它并没把整个区块链都下载到本地。

轻量节点一般使用在移动计算设备上，由于容量限制以及对于便携性的高要求，人们通常不会下载区块链到本地。因此，钱包的运营者会通过 SPV (Simple payment verification) 协议，将每个用户钱包中的转账与网上的完整区块链进行核对与确认。

在以太坊网络中，也有类似的全节点、轻节点、归档节点之分，所以并不是每个节点都需要巨大的存储空间 ，要根据节点功能来选择。

23.区块链中的密码学是怎么应用的?

在区块链技术中，密码学机制主要被用于确保交易信息的完整性、真实性和隐私性。

区块链中的密码学 包括布隆过滤器，哈希函数、加解密算法，数字证书与数字签名，同态加密，PKI 体系等。

*了解更多关于区块链隐私和密码学内容，下载链得得 App， 参考详文：

《【大文观链】区块链隐私保护方案：群签名与环签名》
《【大文观链】ECDHM：基于数学和密码学的隐私保护方案》

24.区块链中分布式数据存储是什么意思？

区块链本质是一个去中心化的数据库 ，区块链技术的数据共享是一个分布式的记账薄， 它的本质上是一个按照时间顺序串联起来的链，创世块开始的所有交易都记录在区块中。交易记录等账目信息会被打包成一个个的区块并进行加密，同时盖上时间戳，所有区块按时间戳顺序连接成一个总账本。区块链由多个独立，地位等同的节点按照块链式结构存储完整的数据，通过共识机制保证存储的一致性，一旦数据被记录下来，在一个区块中的数据将不可逆。

25.区块链的分布式存储是怎么保证安全性的？

由于区块链块链结构，区块之间相互串成一条链条，如果想篡改数据，只篡改一个节点并没有用，需要同时篡改整条链上的节点才可以真正篡改数据，这种篡改难度极高，几乎不可能完成。区块链 通过数据加密和授权技术，存储在区块链上的信息是公开的 但是账户身份信息是加密的 只有数据拥有者授权的情况下才能访问到，以此保证数据的安全和个人隐私。

26.共识机制现在大致有几种，有什么区别？

比较常见的有九种：

1) 工作量证明—多劳多得

PoW 机制中根据矿工的工作量来执行货币的分配和记账权的确定。算力竞争的胜者将获得相应区块记账权和比特币奖励。因此,矿机芯片的算力越高,挖矿的时间更长,就可以获得更多的数字货币。

优点：算法简单，容易实现；节点间无需交换额外的信息即可达成共识；破坏系统需要投入极大的成本。

缺点：浪费能源；区块的确认时间难以缩短；新的区块链必须找到一种不同的散列算法，否则就会面临比特币的算力攻击；容易产生分叉，需要等待多个确认；永远没有最终性，需要检查点机制来弥补最终性。

目前基于 PoW 共识机制的数字货币有很多，比特币、莱特币、狗狗币、达士币、门罗币等初期的数字货币大多都是 PoW 共识机制。

2) PoS（Proof of Stake）股权证明算法——持有越多，获得越多

POS 机制采用类似股权证明与投票的机制，选出记帐人，由它来创建区块。持有股权愈多则有较大的特权，且需负担更多的责任来产生区块，同时也获得更多收益的权力。POS 机制中一般用币龄来计算记账权，每个币持有一天算一个币龄，比如 持有 100 个币，总共持有了 30 天，那么此时的币龄就为 3000。在 POS 机制下，如果记账人发现一个 POS 区块，他的币龄就会被清空为 0，每被清空 365 币龄，将会从区块中获得 0.05 个币的利息(可理解

为年利率 5%)。

优点：在一定程度上缩短了共识达成的时间；不再需要大量消耗能源挖矿。

缺点：还是需要挖矿，本质上没有解决商业应用的痛点；所有的确认都只是一个概率上的表达，而不是一个确定性的事情，理论上有可能存在其他攻击影响。

最先开始运用权益证明共识机制的区块链项目是 2012 年诞生的 PeerCoin，以太坊前三阶段均采用 PoW 共识机制，在第四阶段开始以太坊将采用权益证明机制，此外，量子链和 Blackcoin 都采用 POS 共识机制。

3) DPOS（Delegated Proof-of-Stake）股份授权证明

股份授权证明（简称：DPoS)与 PoS 的主要区别在于节点选举若干个代理人，由代理人验证和记账，但其监管、性能、资源消耗和容错性与 POS 相似。通俗的理解类似于董事会投票，持币者投出一定数量的节点，由节点进行代理验证和记账。

整个投票的模式是：成为代表----授权投票----保持代表诚实----抵抗攻击

优点：大幅缩小参与验证和记账节点的数量，可以达到秒级的共识验证。

缺点：共识机制还是需要代币而很多商业是不需要代币的。

4) PBFT（Practical Byzantine Fault Tolerance）实用拜占庭容错——分布式一致性算法

实用拜占庭容错在保证活性和安全性（liveness & safety）的前提下提供了(n-1)/3 的容错性。在分布式计算上，不同的计算机透过讯息交换，尝试达成共识；但有时候，系统上协调计算机（Coordinator / Commander）或成员计算机 （Member /Lieutanent）可能因系统错误并交换错的讯息，导致影响最终的系统一致性。拜占庭将军问题就根据错误计算机的数量，寻找可能的解决办法，这无法找到一个绝对的答案，但只可以用来验证一个机制的有效程度。

而拜占庭问题的可能解决方法为：在 N ⩾ 3F+1 的情况下一致性是可能解决。其中，N 为计算机总数，F 为有问题计算机总数。信息在计算机间互相交换后，各计算机列出所有得到的信息，以大多数的结果作为解决办法。优点：系统运转可以脱离币的存在，pbft 算法共识各节点由业务的参与方或者监管方组成，安全性与稳定性由业务相关方保证；共识的时延大约在 2~5 秒钟，基本达到商用实时处理的要求；共识效率高，可满足高频交易量的需求。缺点：当有 1/3 或以上记账人停止工作后，系统将无法提供服务；当有 1/3 或以上记账人联合作恶，且其它所有的记账人被恰好分割为两个网络孤岛时，恶意记账人可以使系统出现分叉，但是会留下密码学证据；去中心化程度不如公有链上的共识机制；更适合多方参与的多中心商业模式。

讲通俗些就是采用“少数服从多数”来选举领导者并进行记账的共识机制，该机制允许拜占庭容错，允许强监管节点参与，具备权限分级能力，性能高，耗能低，而且每一轮记账都会由全网节点共同选举领导者，允许 33%的节点作恶，容错性为 33%。

5) dBFT（delegated BFT）授权拜占庭容错算法

在实用拜占庭容错的基础上进行了改进：

1. 将 C/S（客户机/服务器）架构的请求响应模式改进为合适 P2P 网络的对等节点模式；

2.将静态的共识参与节点改进为可动态进入、退出的共识参与节点；

3.为共识参与节点的产生设计了一套基于持有权益比例的投票机制，通过投票决定共识参与节点（记账节点）；

4.在区块链中引入数字证书，解决了投票中记账节点真实身份的认证问题。

优点：专业化的记账人；可以容忍出错；记账由多人协同完成；每一个区块都有最终性，不会分叉；算法的可靠性有严格的数学证明。

缺点：当 1/3 及以上的记账人停止工作后，系统将无法提供服务；当 1/3 及以上的记账人联合作恶，且其他所有的记账人被恰好分割两个网络时，恶意记账人就可以使系统出现分叉。

总之，授权拜占庭容错机制最核心的一点，就是最大限度地确保系统的最终性，使区块链能够适用于真正的金融应用场景。

6) DAG(Directed acyclic graph)有向无环图——无区块链概念

DAG 最初出现就是为了解决区块链的效率问题。其通过改变区块的链式存储结构，通过 DAG 的拓扑结构来存储区块。在区块打包时间不变的情况下，网络中可以并行的打包 N 个区块，网络中的交易就可以容纳 N 倍。之后 DAG 发展成为脱离区块链，提出了 blockless 无区块的概念。新交易发起时，只需要选择网络中已经存在的并且比较新的交易作为链接确认，这一做法解决了网络宽度问题，大大加快了交易速度。

优点：交易速度快；无需挖矿；极低的手续费。

缺点：网络规模不大，导致极易成为中心化；安全性低于 PoW 机制。

7) Pool 验证池——私有链专用

Pool 验证池，基于传统的分布式一致性技术，加上数据验证机制；之前曾是行业链大范围在使用的共识机制，但是随着私有链项目的逐渐减少渐渐开始势微。
优点：不需要代币也可以工作，在成熟的分布式一致性算法（Pasox、Raft）基础上，实现秒级共识验证。
缺点：去中心化程度不如 bictoin；更适合多方参与的多中心商业模式。
自定义共识机制以及混合共识机制——私人订制

8) Ripple——RPCA（Ripple Protocol consensus algorithm）

瑞波共识机制 RPCA 是一个类似 PBFT 的共识机制，属于节点投票的共识机制。初始特殊节点列表就像一个俱乐部，要接纳一个新成员，必须由 51%的该俱乐部会员投票通过。共识遵循这核心成员的 51%权力，外部人员则没有影响力。由于该俱乐部由“中心化”开始，它将一直是“中心化的”，而如果它开始腐化，股东们什么也做不了。与比特币及点点币一样，瑞波系统将股东们与其投票权隔开，并因此比其他系统更中心化。Stellar 的共识机制 SCP（Stellar Consensus Protocol）就是在“Ripple 共识算法”的基础上演化而来的。

9) Hcash——PoW+PoS 共识机制

Hcash 采用混合共识机制后，有 Hcash 的用户与矿工均可以参与到投票中，共同参与

Hcash 社区的重大决定；

Hcash 的 PoS 还为不合格的矿工提供了一个制衡机制；通过 PoS+PoW 公平的按持币数量与工作量分配投票权重，可以实现社区自治；通过 PoW,使得 Hcash 有挖矿的硬性成本作为币价的保证，又制约了单独 PoS 机制里数字货币过于集中的问题；PoS 让中小投资者着眼于项目的中长期的发展，中小户更倾向于把币放在钱包里进行 PoS 而不是放在交易所随时准备交易使得 Hcash 生态更加健康，人们会将注意力更多的放在 Hcash 技术与落地应用上，而不是仅仅关注短期的价格波动；在安全性上，由于 PoW 必须通过 PoS 的验证才可生效，PoW 矿工不能自行决定并改变网络规则，这有效的抵挡了 51%攻击。

*了解更多关于技术文章，下载链得得 App， 参考详文：

《【大文观链】区块链安全面面观：51%攻击和女巫攻击》

27.区块链是否有性能瓶颈?

区块链的性能指标主要包括交易吞吐量和延时。交易吞吐量表示在固定时间能处理的交易数，延时表示对交易的响应和处理时间。在实际应用中，需要综合两个要素进行考察——只使用交易吞吐量而不考虑延时是不正确的，长时间的交易响应会阻碍用户的使用从而影响用户体验；只使用延时不考虑吞吐量会导致大量交易排队，某些平台必须能够处理大量的并发用户，交易吞吐量过低的技术方案会被直接放弃。

目前，比特币理论上每秒最多只能处理七笔交易，每十分钟出一个区块，相当于交易吞吐量为 7，交易延时为 10 分钟，实际上，等待最终确认需要 6 个左右的区块，也就是说实际交易延时是 1 个小时。以太坊稍有提高，但也远远不能满足应用需求。所以区块链先用技术是有性能瓶颈的。

从区块链技术来看，目前影响区块链性能的因素主要包括广播通信、信息加解密、共识机制、交易验证机制等几个环节。比如，共识机制的目标是为了使得参与节点的信息一致，但在高度分散的系统达成共识本身就是一件耗时的任务，如果考虑会有节点作恶，这会更加增加处理的复杂性。

28.区块链如何做到数据共享?

区块链技术关心的并非是数据的共享，而是数据控制权限的共享，此处的权限主要是指数据的修改和增加的权力，它主要包含两个含义：一是谁可以进行数据的修改；二是以何种方式进行修改。

在互联网模式下，数据读取、写入、编辑和删除一般都伴随着身份认证操作，只有特定的人才能对数据进行修改，而在区块链模式下，尤其是公有链体系下，任何人都可以参与对数据的读写，并且以分布式账本的方式构建了一个去信任的系统，参与读写的各个组织或个体可以互不信任，但能对系统存储数据的最终状态达成共识。

简单地说，区块链式共享和互联网式共享的本质区别在于区块链共享的不仅仅是数据，而是数据的控制权。

由于网站运营方完全控制了中央服务器，这些组织可以随意地编辑和处理数据。虽然组织也需要在一定的法律和协议下完成数据修改等行为，但由于其是掌握资源的一方，个人用户很难享有完全的控制权。

举一个简单的例子，某一用户上传了一张照片到网站平台上，并且希望朋友们能看到这张照片。排除掉一些非法要素，这张照片最后的控制权是归谁呢？显然，从用户的角度来看，这张照片是归自己所有的，但事实上，这些社交网站才是真正的控制方，他们可以随意的进行修改，用户却毫无办法。也就是说，在现有互联网体系下，只要掌握了网站平台的运营权，就能完全地控制平台上的数据。

而在区块链体系下，数据不被任何权威方掌握，其权限是由规则来进行控制的，这些规则的主要目标是来规定什么样的信息是有效的，同时还规定了参与者应当如何对其进行反馈。

这些规则通常是预先定义的，加入区块链网络的参与者必须遵守规则。当然，从技术上来说，参与者可以自行忽略某些规则，并根据自身利益来构建一些无效的数据。但是，由于区块链共识机制的存在，其他参与者可以根据预定义的规则将这些无效数据排除在网络之外。

总的来说，区块链根据技术层面的规则体系来规范数据的写入行为，而互联网是通过权力和资源来控制数据，这是区块链式共享和互联网式共享的根本性区别。

区块链是以权限分享的形式，让每个参与者同时作为数据提供方、验证方和使用方，共同维护区块链数据的安全和有效性。

29.为什么区块链可以做到不可篡改？

区块链是从零开始有序的链接在一起的，每个区块都指向前一个区块，称为前一个区块的子区块，前一区块称为父区块。

每个区块都有一个区块头，里边包含着父区块头通过算法生成的哈希值，通过这个哈希值可以找到父区块。当父区块有任何改动时，父区块的哈希值也发生变化。这将迫使子区块哈希值字段发生改变，以此类推，后边的子子区块，子子子区块都会受影响。一旦一个区块有很多后代以后，除非重新计算此区块所有后代的区块，但是这样重新计算需要耗费巨大的计算量，所以区块链越长区块历史越无法改变。

30.区块链系统中不同节点之间是如何建立信任的？

节点 A 是第一次连入区块链网络，那它首先会通过一种算法找到距离它最近的一个网络节点。

节点将一条包含自身 IP 地址的消息发送给相邻节点，相邻的节点再将这条消息向与自己连接的节点进行分发广播，以此类推，最终导致新节点的 IP 地址在全网进行分发，每个网络节点都知道节点 A 的地址，可以与之建立直接连接。

新节点建立更多的连接，使节点在网络中被更多节点接收，保证连接更稳定。

31.区块链为什么会分叉？

区块链分叉其实是区块链系统升级导致的，每次升级可能会伴随着区块链的共识规则改变，这会导致整个网络中升级了系统的节点与未升级系统的节点在不同的规则下运行，于是分叉就产生了。例如我们使用的 App，当有新版本出现，有的人升级了，有的人没有升级，两个版本同时可以用。

32.区块链密码朋克是什么？

中本聪的比特币白皮书最早发布于“密码朋克”。狭义地说，“密码朋克”是一套加密的电子邮件系统。

1992 年，英特尔的高级科学家 Tim May 发起了密码朋克邮件列表组织。1993 年，埃里克•休斯写了一本书，叫《密码朋克宣言》。这也是“密码朋克”（cypherpunk）一词首次出现。“密码朋克”用户约 1400 人，讨论的话题包括数学、加密技术、计算机技术、政治和哲学，也包括私人问题。早期的成员有非常多 IT 精英，比如“维基解密”的创始人阿桑奇、BT 下载的作者布拉姆•科恩、万维网发明者 Tim-Berners Lee 爵士、提出了智能合约概念的尼克萨博、Facebook 的创始人之一肖恩•帕克。当然，还包括比特币的发明人中本聪。

据统计，比特币诞生之前，密码朋克的成员讨论、发明过失败的数字货币和支付系统多达数 10 个。

33.区块链效率提升？

地址是公钥进行了一系列的转换而获得的，其中主要的是进行了多重的哈希运算。

由于转换过程中采用了不可逆的哈希运算，所以从地址是不能够反向运算出公钥的，所以还是安全的。

34.一个区块上可以有几笔交易？

以比特币区块为例，一个区块大小上限大概是 1MB 左右，每一笔交易大小不一，一般一个交易平均大小在 250 字节左右，算下来 1M 大概能容纳 3000 多笔交易。

35.比特币交易为什么确认 6 个区块以上就可以证明？

为了避免双花造成的损失，一般认为，等 6 个区块确认后的比特币交易基本上就不可篡改了。举个例子来解释双花过程：假设小黑给大白发了 666BTC，并被打包到第 N 个区块。没过几分钟，小黑反悔了，通过自己控制的超过 50% 的算力，发起了 51% 算力攻击，通过剔除发给大白的 666BTC 那笔交易，重组第 N 个区块，并在重组的第 N 个区块后面继续延展区块，使之成为最长合法链。

一般来说，确认的区块数越多，越安全，被 51% 攻击后篡改、重组的可能性越低，所以 6 个区块并不是硬性的，只是说有了 6 个区块，被篡改的可能性较低。对于大额交易，当然是区块越多越好，但是对于小额效益，一个区块就够了。

36.区块链分叉后是分别独立的吗？

区块链分叉分为两类：一类是硬分叉，一类是软分叉。两者最大的区别在于是否兼容旧版本协议，硬分叉是完全不兼容，而软分叉是可以兼容的。所以硬分叉后是分别独立的，而软分叉不是。

37.工作量证明难度怎么计算？

难度值 = 最大目标值/目标值
其中，最大目标值为一个恒定值：

0x00000000FFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFF
难度值的大小与目标值成反比关系。

38.如何搭建公链?

搭建以太坊公链，其实就是在本地运行一个以太坊节点，然后连接到以太坊主网。考虑到主网的区块会占用很大的硬盘空间，启动节点的时候可以指定存放数据的目录，运行命令：./geth --ipcpath gethdir/geth.ipc --datadir gethdir console 成功启动节点后，进入控制台交互界面，主网的区块信息会主动同步。

39.公有链有什么必须要知道的概念?

1) 零知识证明

“零知识证明”zero-knowledge proofs，简写为 ZKPs，指的是证明者能够在不向验证者提供任何有用信息的情况下，使验证者相信某个论断是正确的协议。看上去非常复杂，但实现的方式很简单：A 要向 B 证明他知道特定数独的答案，但又不能告诉 B 这个数独的解。B 可以随机指定某一行、列或九宫格，A 将这一行、列、九宫格里所有的数字按照从小到大的顺序写下来，其中包含了 1-9 的所有数字，就可以证明 A 的确知道这个数独题目的答案。

在这个过程当中，一旦 A 提前知道了 B 指定的行、列或九宫格，就可以在验证过程中作弊，所以 B 需要一个真正的随机数来确保这个验证方式是安全的。
在区块链中，节点之间利用零知识证明的方式就可以在不向验证者提供任何有用信息的情况下，使验证者相信这个区块是合法的。

2) 非对称加密算法

非对称加密算法也叫公开密钥密码学（英语：Public-key cryptography，是密码学的一种算法，它需要两个密钥，一个是公开密钥，另一个是私有密钥；一个用作加密，另一个则用作解密。使用其中一个密钥把明文加密后所得的密文，只能用相对应的另一个密钥才能解密得到原本的明文；甚至连最初用来加密的密钥也不能用作解密。由于加密和解密需要两个不同的密钥，故被称为非对称加密；不同于加密和解密都使用同一个密钥的对称加密。虽然两个密钥在数学上相关，但如果知道了其中一个，并不能凭此计算出另外一个；因此其中一个可以公开，称为公钥，任意向外发布；不公开的密钥为私钥，必须由用户自行严格秘密保管，绝不透过任何途径向任何人提供，也不会透露给被信任的要通信的另一方。

3) 公有链的“不可能三角”

指在公有链设计的过程当中，安全性、去中心化和高吞吐量三者无法同时实现，必须对其中一种进行妥协。

4) 拜占庭将军问题

拜占庭将军问题（Byzantine Generals Problem），是由莱斯利·兰波特在其同名论文中提出的分布式对等网络通信容错问题。

在分布式计算中，不同的计算机通过通讯交换信息达成共识而按照同一套协作策略行动。但有时候，系统中的成员计算机可能出错而发送错误的信息，用于传递信息的通讯网络也可能导致信息损坏，使得网络中不同的成员关于全体协作的策略得出不同结论，从而破坏系统一致性。拜占庭将军问题被认为是容错性问题中最难的问题类型之一。

具体来说，拜占庭将军问题是一个思想实验，即一组拜占庭将军分别各率领一支军队共同围困一座城市。各支军队的行动策略限定为进攻或撤离两种。因为部分军队进攻部分军队撤离可能会造成灾难性后果，因此各位将军必须通过投票来达成一致策略，即所有军队一起进攻或所有军队一起撤离。因为各位将军分处城市不同方向，他们只能通过信使互相联系。在投票过程中每位将军都将自己投票给进攻还是撤退的信息通过信使分别通知其他所有将军，这样一来每位将军根据自己的投票和其他所有将军送来的信息就可以知道共同的投票结果而决定行动策略。

问题在于，将军中可能出现叛徒，他们不仅可能向较为糟糕的策略投票，还可能选择性地发送投票信息。假设有 9 位将军投票，其中 1 名叛徒。8 名忠诚的将军中出现了 4 人投进攻，4 人投撤离的情况。这时候叛徒可能故意给 4 名投进攻的将领送信表示投票进攻，而给 4 名投撤离的将领送信表示投撤离。这样一来在 4 名投进攻的将领看来，投票结果是 5 人投进攻，从而发起进攻；而在 4 名投撤离的将军看来则是 5 人投撤离。这样各支军队的一致协同就遭到了破坏。

由于将军之间需要通过信使通讯，叛变将军可能通过伪造信件来以其他将军的身份发送假投票。而即使在保证所有将军忠诚的情况下，也不能排除信使被敌人截杀，甚至被敌人间谍替换等情况。因此很难通过保证人员可靠性及通讯可靠性来解决问题。
假使那些忠诚（或是没有出错）的将军仍然能通过多数决定来决定他们的战略，便称达到了拜占庭容错。在此，票都会有一个默认值，若消息（票）没有被收到，则使用此默认值来投票。

40.如何实现去中心化与分布式账本?

实现去中心化

在比特币白皮书《比特币：一个点对点电子现金系统》中，中本聪详细地解释了他是如何设计这个系统的。在其中，他确立了此后所有区块链系统的主要设计原则。

1) 一个真正的点对点电子现金应该允许从发起方直接在线支付给对方，而不需要通过第三方的金融机构。

2) 现有的数字签名技术虽然提供了部分解决方案，但如果还需要经过一个可信的第三方机构来防止（电子现金的）“双重支付”，那就丧失了（电子现金带来的）主要好处。

3) 针对电子现金会出现的“双重支付”问题，我们用点对点的网络技术提供了一个解决方案。

4) 该网络给交易记录打上时间戳（timestamp），对交易记录进行哈希散列处理后，将之并入一个不断增长的链条中，这个链条由哈希散列过的工作量证明（hash-based proof-of-work）组成，如果不重做工作量证明，以此形成的记录无法被改变。

5) 最长的链条不仅仅是作为被观察到的事件序列的证明，并且证明它是由最大的 CPU 处理能力池产生的。只要掌控多数 CPU 处理能力的计算机节点不（与攻击者）联合起来攻击网络本身，它们将生成最长的链条，把攻击者甩在后面。

这个网络本身仅需要最简单的结构。信息尽最大努力在全网广播即可。节点可以随时离开和重新加入网络，只需（在重新加入时）将最长的工作量证明链条作为在该节点离线期间发生的交易的证明即可。

41.量子计算机能否能摧毁比特币？

大的量子计算机可以成为比特币杀手呢？微软的研究表明，解开椭圆曲线离散对数所需的量子位比需要 4000 量子位的 2048 位 RSA 还要少。然而，这些都是完美的“逻辑”量子位。由于误差校正和其他必要步骤，我们需要更多的物理量子位。John Preskill 在他的量子信息讲座中提到，一个标准的 256 位密钥大约需要 2500 量子位，破解这个密钥需要 1000 万个物理量子位的和 1 万个逻辑量子位的量子计算机。

目前的量子技术距离这个里程碑还相差甚远。IBM 宣布他们在 2017 年底实现了一个 50 量子位的系统；谷歌在 2018 年初宣布实现 72 量子位；使用离子阱的 IonQ 公司，发布了一款包含 160 量子位元的量子计算机，并对其中的 79 量子位执行了运算；DWave 发布了自己 2048 量子位系统，然而，它是一个量子软化装置，不能用于 Shor 的算法。

最终要建立的是足够大型的量子计算机用于化学、优化和机器学习。不过，虽然目前能够完成这些任务的大型量子计算机还遥不可及，但正在流通当中的加密货币日后可能会受到这类量子计算机的影响。

42.区块链项目的代码都需要开源吗？为什么？

区块链是一个共识机制，这意味着这种参与者必须是透明的，也就是说，这种运行的代码必须是开源代码，所谓开源代码，就是代码都是可见的。

每个人可以编译并执行自己编译的程序，也意味着每个人都可以修改其中的代码并运行，现在机制下，可以做到不管如何修改代码，只要这些修改代码的人没有超过 51%，那这种修改是没有意义的，反而浪费自己的算力。

从理念角度去看，将区块链项目比作机器的话，本身的工作机制是透明的，是一个可以信任的机器。对此是这样理解的，第一，开源是区块链项目的一个必选项，而不是可选项，不论是公有链还是联盟项目都需要进行开源；第二，开源和交付源代码，是两个不同的概念，交付源代码并非是公开、透明，大家共同参与的一个过程。

比如在以太坊中，曾经因为在其平台上运行的某个平台币，存在漏洞，需要进行修改，这种修改是直接体现在代码上的，阅读代码的过程中，就发现有多处出现该币的相关代码，就是用于处理一旦碰见了这个问题，节点应如何处理，这些处理方法都是开源代码里写的，每个人都可以阅读，如果节点的负责人认可这种解决方案，他就会运行这个程序，相当于支持这种代码的决定，事实上区块链也就是通过这种机制来实现。

*更多详细分析文章，下载链得得 App， 参考详文：

《【得得分析】打开代码“黑匣子”，联盟链不再“圈地自盟”》

三、数字资产篇

43.加密数字货币与区块链有什么关系？

加密数字货币通常指是在区块链网络上发行的一种数字资产。通过区块链浏览器，用户可以查询到数字货币交易的全部流程。在生活中，我们往往把区块链机构或项目方发行的数字资产称为“加密数字货币”，它与央行发行的数字货币存在本质性区别，即：央行数字货币是对 M0 的替代，本身并没有增发新的货币；而区块链项目方所发行的数字货币，是凭空“创造”了一种货币，缺乏主权机构背书，存在较大的信用风险。

从定义来看，区块链是一种新的技术形式，它具有透明性、可追溯、不可篡改等特征，可以赋能供应链金融、产品溯源、存证等行业领域。通过区块链，可以建立一个可信赖的价值网络。

44.币市与股市一样吗？

币市和股市是不一样的，但是币市往往是借鉴了传统股票二级市场的交易逻辑。从形式上来看，币市和股市都会经历一级市场的募资和二级市场的交易。但是他们之间存在诸多不同，主要体现在以下几方面：

1) 发行方式不同：币通过区块链发行，有总量的设置，不可增发，且伴随着销毁机制，大多数属于“通缩型”货币；股是企业通过证券交易所发行的一种证券资产，并不具备货币属性，是一种收益型资产，通过持股数*股价来确定股份的价值；

2) 交易方式不同：加密数字货币可以同时上线多家数字货币交易所，并可以 7*24 小时交易，而首次证券发行的公司往往会选择一家证券交易所发行股票，逢节假日会休市；

3) 监管不同：币市目前仍处在无监管状态，没有权威、独立的监管机构，发行加密数字货币更大程度上属于个人意愿；而全球股市都会有证券监督委员会这样的官方监管机构，他们往往起到市场监督、防范金融风险的作用。

4) 功能不同：币除了用于二级市场交易外，还可以用于日常消费、购买相关业务产品等，根据功能不同，币可分为功能性、证券型和商品型，比特币就是典型的商品型；而股一般都指证券，只能用于一级市场或二级市场的转让、交易。目前各国也在探索分类监管模式，将证券型功能的币与股票证券市场一样进行监管。

45.央行数字货币是怎么回事？老百姓能用吗？如何获取？

央行发行的数字货币可以理解为“人民币的数字化“，它是对人民币 M0 的替代，M0 即流通中的日常消费用的货币。央行数字货币的发行，可以直接解决纸币在发行、印制、回笼、贮藏等环节的损耗，而且“数字化”可以让人民币交易更便捷、更安全，并且具备匿名性的特征。通过数字化的形式，可以为人民币在国际贸易交易中提供较大便利。

央行数字货币是一套“双层运营结构”，即人民银行先把数字货币兑换给银行或者其他运营机构，再由这些机构兑换给公众。老百姓可以通过商业银行或其他机构来直接兑换央行数字货币并可以在日常消费中直接使用。

与比特币的主要区别就在于：央行数字货币有国家主权做背书，且背后有等额的人民币储备资产；但比特币是一种无主权的加密数字资产，它通过“挖矿”来产出，总量 2100 万枚，

每四年进行一下对半减产，具有明显意义的“通缩”特质。

* 链得得曾就央行数字货币问题进行过多次讨论和研究，下载链得得 App， 参考详文：

《【链得得独家】专访 Circle CEO：美国议员不懂加密资产，中国数字货币领先全球》
《【链得得独家】前方解读央行数字货币：市场力量将被充分认可和调动》

46.国内目前有哪些活跃的数字货币交易所，运营主体都是谁?

目前中国政府对数字货币交易所是持否定态度的，尚未有明确监管政策出台。所以大多数交易所名义注册在海外，但是实际运营主体和实际平台用户都在国内，部分交易所注册地也选择在国内。由于政策不明朗，运营主体多为私人企业或者个人，包括也有部分区块链媒体尝试开设交易所。不过媒体开设交易所可能面临更大风险，容易引发从操纵信息到操纵市场的风险。

中国国内活跃交易所汇总

交易所名称	创办人/机构	注册地	平台币	其他关联业务
币安（Binance）	赵长鹏	马耳他	BNB	教育、项目孵化、区块链资产发行平台、区块链研究院以及区块链公益慈善
火币（Huobi）	李林	塞舌尔	HT	钱包、矿池、教育、项目孵化、社交、资本
OKCoin/ OKEX	徐明星	马耳他	OKB	/
KuCoin	Michael Gan	塞舌尔	KCS	/
抹茶（MXC）	MX	新加坡	MX	MXC Labs、PoS 矿池、OTC、合约交易服务
龙网（DragonEx）	张帆	新加坡	DT	游戏、抵押借贷
CoinEgg	Dr.Peter	英国	ET	/
Lbank	何伟	英国	/	C2C交易服务
ZB网	李大伟	瑞士	/	电子钱包、投资基金、研究机构和媒体在内的业务网络
ZBG	/	中国香港	/	区块链项目上市、加密资产投资
BiKi	Winter	新加坡	/	/
gate.io	韩林	开曼群岛	/	/
Bibox	于洋	爱沙尼亚	/	人工智能、期货
ZG.com	赵昌宇/比特币中国	新加坡	/	产业区块链孵化基地
币赢国际站	李谷	中国香港	/	/
可可金融	王峰/火星财经	中国	/	交易所、钱包、资讯媒体、教育、项目孵化、基金
BitZ	Omar Chen	中国香港	Bitz	数字货币交易所
BKEX	纪京言	英属维尔京群岛	/	数字钱包、提供投资项目交易
T网	Tokencan团队	中国香港	/	/
币团网	美国链谷团队	塞舌尔	BT	/
雷盾交易所	/	塞舌尔	/	公链、钱包、量化渠道、区块链学院、矿场、加密社交、区块链孵化基金、公益基金
DigiFinex	石乐琦（Kiana Shek）	塞舌尔	DFT	教育
BG交易所	Terry	中国香港	BG	线下商家、资讯媒体、矿机矿场
ZT	M.j. Lin	开曼群岛	ZT	交易所联盟（云交易所）、新闻资讯
ZZEX	Wayne	新加坡	ZZEX Coin（ZZEX）	/
BTB.io	Sam Wang	开曼群岛	BTB	区块链生态投资基金
FUBT	任长远	中国香港	FUCoin（FUC）	项目投融资、模式设计优化、新币发行上线、社群建设维护、综合运营推广等
ZG.TOP	钱超	蒙古国	ZGT	区块链资讯服务、区块链应用募资平台
瓦特交易所	Bella Fang	新加坡	WPT	矿池
VVBTC	于海	加拿大	VVT	游戏、预测合约、C2C场外交易
BitMart	夏尔特	开曼群岛	BMX	区块链项目孵化、区块链优质项目加速
A网(AEX)	37度	英国	GAT	区块链资讯社区、金融服务（定期活期理财、抵押借币、算力理财、Staking、糖果池）
HCoin	David-L	塞舌尔	HCOIN	大数据分析、数字资产专业管理
东方交易所（DFEX）	/	新加坡	DF	C2C交易服务、钱包、糖果游戏
币万（BIONE）	/	新加坡	BIC	/
BigONE	老猫/李笑来	美国	ONE	区块链数字资产托管、法币交易、数字资产天使平台、PoS 矿池
XT网	ZB集团	塞舌尔	XT	电子钱包、投资基金
Q网	李双	开曼群岛	QBTC TOKEN（QT）	理财、现货交易、场外交易

数据来源：链得得—得得智库及公开资料

CHAINDD 链得得

47.未来数字货币会替代现在的实体货币吗?

由于纸质货币存在成本高、易丢失、安全系数低、难追溯等特点，导致金钱犯罪的案例比比皆是。当今社会，“数字化”已经成为一种趋势，实体货币通过实现电子化，可以提高货币的安全系数，提高交易的便利性。不可置疑的是，有国家主权信用做背书、有等额金融资产抵押的数字货币将成为未来的一种新型货币形式

48.数字货币会对现有的金融体系产生哪些影响?

对“数字货币”的定义需要明确。不能把央行发行的数字货币与比特币、以太坊或其他区块链项目发行的数字货币混为一谈。从防范金融风险的角度来讲，央行数字货币是对货币的一种数字化补充，在本质上并没有影响到人民币的发行、承兑和流通；但是比特币、以太坊以及区块链项目发行的数字货币，由于它具备国际化、匿名性的特征，会存在国有资产流失、洗钱交易、黑市买卖等问题，对金融体系的稳定性造成了巨大冲击。

49.普通老百姓买加密货币，未来需要实名认证吗?

拿比特币来讲，它通过“挖矿”产生，普通老百姓可以建立一个比特币钱包，形成一个独一无二的区块链钱包地址，自己收到的比特币会存放在该钱包中，并不需要进行实名认证。但是目前已经形成了为比特币等加密数字货币提供交易流通的交易场所，用户可通过币安、火币、Coinbase 等交易场所进行二级市场的交易，买卖比特币等加密数字货币。而对于这些交易场所来说，他们往往要求用户进行严格的实名认证，主要是为了实现风险可控。

50.普通人能参与挖矿吗，怎么挖?

“挖矿”其实是一种计算程序，挖矿的程序本质上是一种记账的过程。拿比特币来讲，总量发行 4800 万枚，每四年进行一次减半，在生产过程中，每 10 分钟会打包形成一个区块，哪个“矿工”抢到这个区块的打包权，也就是抢到了这笔帐的记账权，并由此获得打包区块的奖励，一个一个的区块连接起来，就形成了“区块链”。

“挖矿”主要是通过计算机来运行一种记账程序来进行的。普通电脑都可以运行该程序，不过随着挖矿人数的增加，挖矿难度也在增加，这也就要求更高性能的显卡来支持运算。所以，专业的 ASIC 显卡矿机成为市场需求，挖矿也从个人参与的历史逐渐演变为一种专业的行为，矿场也随之诞生。

从目前来看，普通人可通过投资矿机、并由矿场托管的形式来参与挖矿；也可以通过购买云算力的形式间接进行挖矿。

51.所有的币种都需要靠挖矿产生吗?

这是由不同的共识机制决定的。比特币采用的是 PoW 模式，即“工作量证明”，意味着你投入的计算工作量越大，你越容易获得区块打包的记账权，越有机会获得奖励。

此后，市场上也诞生了 PoS、DPow 等机制，其中都包含着不同的挖矿规则。但是对于诸多项目方发行的加密数字货币来说，它并不需要靠挖矿来产生，它本质上是凭空发行一种可交易的数字资产，通过锁仓、市场投放、交易等形式，来实现流通和转让。

52.数字货币的价值本质是什么?

它本质是一种去中心化的、透明且安全的数字资产。它通过运行一种程序，来自动实现资产的发行，不受任何组织和机构的干预。货币的价值建立在人们的信任基础上，但同时又受到供需关系的影响。但是交易基于人们对现实的需求和对未来价值的判断。同样拿比特币来讲，比特币初期想作为一种可用于支付的货币，但是其价格的巨大波动性决定了其无法用于交易。

此后，比特币更被看作一种储值资产来看待，从形势来看，每半年减产一次，且持有比特币的用户在不断增加，似乎大多数人都看好比特币未来的增值空间。但是从供需结构来看

，如果人们看好比特币，就不会选择卖出比特币，如果市场没有卖方，比特币就没有市场，自然也就没有价值。这似乎是一个难以解释的矛盾点。

53.我个人想发一个自己的币要怎么操作？

2017 年 9 月 4 日开始，中国境内禁止一切有关的 ICO（数字货币发行）活动。并多次重申“炒币”存在的巨大风险性。目前属于我国法律严厉禁止的行为。

54.挖矿时应该注意什么？

你需要考虑矿机的损耗、电力成本和全网算力值。从矿机损耗来讲，专业的显卡矿机在寿命、功效、电力成本上都具有优势，而全网算力的大小就意味着目前有多少“矿工”在用矿机挖矿。对于许多矿场来说，他们都逐水而建，来寻求更便宜的电力成本，从而实现收益的最大化。

55.挖矿产生的币都有交易价值吗？

“交易价值”是相对而言的，如果有足够的买方和卖方，就可以形成交易的流通性，就可以形成一个有交易价值的对手盘。其实无论是挖出来的币还是区块链项目方发行的代币，只要在二级市场上具备流动性，也就具有“交易价值”。但是，这些币本身是否具有价值，就值得更多的探讨了。

56.什么样的加密钱包最安全？什么样的钱包最方便？

加密数字货币钱包主要分为“冷钱包”和“热钱包”。“冷钱包”就是离线钱包，也可以理解为不联网的硬件钱包，它就像家里的保险柜。“热钱包”就是联网的钱包，它可以通过网络进行实时交易。

从安全系数上来讲，冷钱包最安全，黑客无法通过网络攻击的形式来盗取存放于冷钱包中的加密数字资产。从交易便捷性上看，热钱包最方便，它可以通过 APP、电脑网页或客户端来进行线上交易和存储。目前主流加密货币交易所均使用“冷+热”的钱包配置模式，大额资产存放于冷钱包中，可供流通交易的资产存放于热钱包中。

57.如何存储和交易比特币？

存储：用户可以将比特币存放于自己的加密数字货币钱包中，主流的钱包均支持比特币的存取。用户也可以将比特币存放于加密数字货币交易所中，交由交易所代为托管。

交易：比特币的交易分为“场内交易和场外交易”。场内交易，通过加密数字货币交易所来挂单交易，也就是通俗意义上的“二级市场交易”；场外交易：通过寻找一个交易对手，双方实现面对面或点对点的交易，也就是直接通过钱包地址转账的方式来实现比特币交易。

但是在交易比特币之前，除了挖矿或者别人直接赠予比特币外，需要通过法币来购买比特币。用户可以通过场外市场，把法币给持有比特币的个人，这个人再将比特币转到你的比特币账户中。

58.区块链上的交易需要手续费吗，怎么定的？多少由谁决定？

区块链上的交易需要手续费。因为从原理上来看，交易的过程也就是矿工打包的过程，只有用户支付手续费，矿工才会选择将这笔交易打包并进行全网公布。手续费的大小主要取

决于目前全网算力难度的大小。

当全网算力来到一个峰值时，用户往往需要更多的手续费来吸引矿工对这笔交易进行优先打包，打包速度越快，交易速度也就越快。反之，当全网算力竞争没那么大时，用户即使支付较少的手续费，也能够快速被矿工打包交易。

59.比特币交易怎么样才算成功交易？

比特币的交易数据被打包到一个“数据块”或“区块”（block）中后，交易就算初步确认了。当区块链接到前一个区块之后，交易会得到进一步的确认。在连续得到 6 个区块确认之后，这笔交易基本上就不可逆转地得到确认了。比特币对等网络将所有的交易历史都储存在“区块链”（blockchain）中。区块链在持续延长，而且新区块一旦加入到区块链中，就不会再被移走。

当我们提交一个交易，正常情况下，这个交易最终会被矿工放到某个区块中，这个时候，我们可以说，这笔交易获得了 0 个确认。当有另外一个区块链到这笔交易所在区块，也就是把这笔交易所在区块为父区块时，我们就说这笔交易获得了 1 个确认，以此类推。一笔交易获得了多少个确认，就是这笔交易所在区块后面又链接了多少个区块。

60.Facebook 推出的 Libra 是哪一种数字货币？与区块链有关系吗？

Libra 是一种由 Facebook 提出的加密货币，计划于 2020 年发行，但由于还有许多争议所以目前这个计划暂时暂停发行。Libra 是一种稳定币，它是一种数字加密货币行业里对于加密货币的分类。

根据白皮书显示，Libra 运行于 Libra Blockchain 之上，它是一个目标成为全球金融的基础架构，它可以扩展到数十亿账户使用，支持高交易吞吐量。也就是说，这个区块链的容量足以支撑全球数十亿人的交易量。

* 稳定币相关内容下载链得得 App， 参考详文：

《【链得得深度】全球 59 家主流稳定币解析，“寡头市场”下一个机会何在？》

61.ICO、STO、IEO 是什么？

ICO（Initial Coin Offering），首次代币发行，指区块链项目首次向公众发行代币，募集比特币、以太坊等主流加密货币以获得项目运作的经费。

IEO（Initial Exchange Offerings），首次交易发行，指以交易所为核心发行代币；代币跳过 ICO 这步，直接上线交易所。

STO（Security Token Offering）证券化通证发行，指受到证券法的监管，以公司股权、债权、黄金、房地产投资信托、区块链系统的分红权等作为对应的通证的公开发行。

*ICO、IEO 都有什么区别？下载链得得 App， 参考详文：

《【得得白话】从 ICO 到 IEO，万变不离其宗》

62.暗网、加密货币和区块链是什么关系？

暗网是存在于黑暗网络、覆盖网络上的互联网内容，只能用特殊软件、特殊授权、或对电脑做特殊设置才能访问。因为在暗网上进行交易经常使用可以匿名的加密货币，因此两者常常被相提并论。暗网与区块链技术没有直接的关系。

63.公链、私链、联盟链怎么区分?

公有链是指全世界任何人可以读取、发送交易却能获得有效确认的共识区块链。也就是说，公有链上的行为是公开透明的，不受任何人控制，也不受任何人所有，是“完全去中心化”的区块链。

私有链对单独的个人或实体开放，仅在私有组织，比如公司内部使用，私有链上的读写权限，参与记账的权限都由私有组织来制定。

联盟链是指有若干个机构共同参与管理的区块链，每个机构都运行着一个或多个节点，其中的数据只允许系统内不同的机构进行读写和发送交易，并且共同来记录交易数据。所以联盟链上的读写权限、以及记账规则都按联盟规则来“私人定制”。

* 联盟链如何落地？详情下载链得得 App， 参考详文：

《【大文观链】苏宁：如何在联盟链中实现去中心化》

四、应用落地篇

64.区块链应用的发展历程是怎样的?

区块链的发展历程可以分为三个阶段。区块链科学研究所创始人梅兰妮·斯万，在她的《区块链：新经济蓝图及导读》这本书中，根据区块链的应用发展状况分为三个阶段：区块链 1.0、2.0 和 3.0。

一、区块链 1.0 加密货币时代（2008-2013）
2008 年，中本聪首次提出了比特币和区块链的概念，随后在 2009 年 1 月，第一个区块链问世。在这个阶段，人们更多关注的加密货币的交易，区块链仅仅作为底层技术，充当“公共帐薄”的作用。

二、区块链 2.0 智能合约时代（2014-2017）
2014 年，"区块链 2.0”成为去中心化区块链数据库的代名词。在这个阶段，人们主要关注平台的应用。任何人都可以在区块链上上传和执行智能合约，并且执行完毕后会自动获得奖励。由于这个交易过程不需要任何中介，因此人们的隐私得到了极大的保护。

三、区块链 3.0 大规模应用时代（2018-）
这个阶段，人们开始构建一个完全去中心化的数据网络，区块链技术的应用也不再局限于经济领域，而是扩大到艺术、法律、房地产、医院、人力资源等领域。

65.目前限制区块链发展的因素有哪些?

为什么现在区块链落地很难：一方面它是技术门槛高，另外一方面它是监管不明朗，所以导致主流资金不能够进场。

第一个，技术门槛高。对于普通用户来说操作相对复杂，比如你现在要转一个数字货币，你需要有钱包、要知道怎么翻墙、还要有一定密码学的知识，这对很多人来讲是非常麻烦的。另外，想要企业上链或者进行币改，都需要一定的技术和理论基础。
第二，技术壁垒依旧难以攻克。比如扩容问题，比如算法的突破和改进等，以及难以实现的完全去中心化等等。

第三个，它离“钱”太近。所以各国政府对它会秉持小心谨慎的态度，因为它对于货币政策、财政政策都会有很大的影响。要知道，各国政府对于新技术都需要有一个很慎重的研究过程。

66.中国的区块链现状是什么?

2019 年中国区块链产业发展迅速，主要体现在以下几点：

第一，国家高层战略引导和支持，营造良好政策环境。据不完全统计，2019 年上半年全国超过 23 个省市发布了超过 112 条涉及区块链的政策信息。政府高层强调区块链技术的应用在技术革新和产业变革中起到重要作用，支持加快推动区块链技术和产业创新的发展。

此外关于区块链的市场监管政策也逐渐完善，一方面，对于虚拟货币的交易和服务进行严格的警惕和检测；另一方面，对区块链应用的相关行业监管体系也在进一步建设完善，为产业区块链项目深入服务实体经济提供有力保障，市场趋于规范，产业环境逐渐清晰；此外，对于技术突破和人才鼓励的扶持上，也通过设立区块链产业园、区块链专项投资基金

等方式，对技术创新和人才引进的贴补，促进区块链产业的发展。

第二，国内企业积极参与区块链技术研发和应用，开展区块链战略布局。如阿里巴巴等电商巨头，利用区块链技术运用到产品溯源、跨境结算等领域，京东利用透明供应链体系打击假冒伪劣产品，腾讯重点研发电子发票等金融领域的应用。

67.区块链的应用和应用成功例子有哪些?

区块链可以应用到各行各业，以电子商务为例，为了解决电商在假货、物流、诚信、监管等方面的痛点，各大企业、平台也是各显身手，招式尽出。区块链就作为其中一种较为可行的手段被使用，那它究竟如何解决这些问题呢?

第一，对商品生产过程进行监督。在逛网店的时候，最担心的就是买到假货，尤其是海外商品，此外还有假货带来的价格问题。如何在确保真货的情况下，买到价格合理的商品，真是一件非常头疼的事情。而区块链技术的透明性、不可逆，可以让消费者随时查看商品的生产地、生产商、原材料等。

第二，对商品运输进行追溯跟踪。电商涉及的供应链、存货、物流等一系列运营活动中会涉及多个中间机构，而区块链去中心化、不可篡改、可追溯的特征将整个流程变得透明，任何一个合作方都可以查看库存和支付情况，能很好的解决供应链的“牛鞭效应”问题。（牛鞭效应：指供应链上的一种需求变异放大现象。其产生的根本原因在于供应链中上、下游企业间缺乏沟通和信任机制，需求信息在沿着供应链向上传递的过程中被不断曲解。）同时区块链的智能合约可以用于规范中介机构，如物流和支付管理合作伙伴。将庞大的管理体系变得简化，从而提高效率。

第三，对商品销售和售后服务进行保障。目前中国电子商务市场四分之三的交易是在移动端完成，支付信任是平台需要解决的一大难题，而区块链被人们称为是“信任机器”，给大家举个例子，很多网店为了好评会出现刷单或者是伪造数据的现象，而购买信息上链后，是不可篡改的，保证真实性，你可以查看商家真实的交易记录，来确保商家是否可信。
第四，对用户隐私进行保护。区块链的私钥、公钥、加密算法就能够解决这一问题，每个用户有自己独立的地址，且由于区块链的匿名性，企业也不能公布或者储存用户信息，也免受黑客的攻击。

具体的落地应用，我们以国内两大电商巨头为例。从 2016 年开始阿里巴巴就开始引入区块链，首先是蚂蚁金服上线区块链技术应用于支付爱心捐赠平台，进行区块链技术的第一次试水；到 17 年蚂蚁金服技术实验室宣布开放区块链技术，支持进口食品安全、商品正品溯源；18 年菜鸟和天猫国际宣布，启用区块链技术用于跟踪、查证跨境进口商品的物流全信息，这些数据包括了商品的原产国、启运国、装货港、运输方式、进口口岸、保税仓检验检疫单号、海关申报单号等等。

物流和商品追溯确实是区块链入驻电子商务领域一个很好的切入点，作为国内电商巨头之一的京东当然也不甘示弱，在 2017 年，京东宣布成立“京东品质溯源防伪联盟”，联合各级政府部门通过联盟链的方式，搭建京东区块链防伪追溯平台；同年 12 月，与沃尔玛、IBM、清华大学电子商务交易技术国家工程实验室共同宣布成立中国首个安全食品区块链溯源联盟。

*下载链得得 App， 参考详文：

《对话“最烧钱”的蒋国飞：蚂蚁区块链足够强大也必须强大》

68.国内目前有哪些活跃的矿机厂商，技术及经营情况如何？

国内目前活跃的矿机厂商包括主要有三家，分别是比特大陆、嘉楠耘智、亿邦国际，三者的市场份额加起来超过全球矿机市场总额的 80%。另外还有一些小型矿机厂商，如比特微、芯动科技、比飞力等。从市场占比来看，2018 年，比特大陆占全球矿机市场份额的 74.5%。

国内活跃矿机及业务汇总

公司名称	产品名称	简介	其他业务
比特大陆	蚂蚁矿机	比特大陆总部位于北京，从事加密货币相关产业和人工智能产业，其中包括生产机器人、生产矿机、提供矿池和云端挖矿等服务。	蚂蚁矿池、算丰人工智能芯片
嘉楠耘智	阿瓦隆矿机	嘉楠耘智成立于2013年，是一家以集成电路设计和芯片自主研发为核心的企业，是世界超芯片和人工智能芯片开发商和配套服务提供商。	勘智人工智能芯片
亿邦国际	翼比特矿机	亿邦国际是我国最早的比特币矿机制造商，除此之外，亿邦国际还从事通信技术应用的研发工作，主要包括5G技术网络接入、专属网络接入及最先进的宽带技术。	宽带技术解决方案、传输设备制造
比特微	神马矿机	成立于2016年，主营业务为区块链、人工智能等领域专用集成电路芯片及产品/方案的研发、生产及销售，并提供相应的系统解决方案及技术服务。	/
芯动科技	芯动矿机	芯动科技有限公司地处苏州工业园和武汉东湖高新区两地，是最早的28nm矿机生产商之一，产品覆盖多种主流数字货币。	/
Bitfly	雪豹矿机	比飞力成立于2017年，隶属于希格斯（HIGGS）超算集团,现设研发中心于深圳市南山区，并在宝安区设有测试工厂。	超级计算机芯片生产
Baikal	Baikal矿机	Baikal成立于2008年，致力于芯片的研发以及软件开发。2016年5月成功推出了第一款矿机——Baikal mini X11。	/

数据来源：链得得—得得智库及公开资料

CHAINDD 链得得

从技术来看，比特大陆、嘉楠耘智已经实现使用更高效率的 7nm 芯片制造工艺的矿机量产，亿邦国际采用的则是 10nm 芯片从技术实力来说稍逊一筹。

69.目前有多少知名公链？

活跃公链汇总

公链名称	是否已发币	通证简称
Bitcoin	已发	BTC比特币
Ethereum	已发	ETH以太坊
EOS	已发	EOS
Bitcoin Cash	已发	BCH
Bitcoin SV	已发	BSV
Litecoin	已发	LTC
Binance Chain	已发	BNB
Huobi Chain	已发	HT
OKchain	已发	OKB
TRON	已发	TRX
NEO	已发	NEO
Ontology	已发	ONT
VeChain	已发	VET
Quantum Blockchain	已发	QTUM
Bytom	已发	BTM
TrueChain	已发	TRUE
Zilliqa	已发	ZIL
IOST	已发	IOST
Elastos	已发	ELA
Metaverse ETP	已发	ETP
Factom	已发	FCT
WaltonChain	已发	WTC
GXChain	已发	GXC
YOYOW	已发	YOYOW
VNTchain	已发	VNT
Conflux	未发通证	/

数据来源：链得得—得得智库及公开资料

CHAINDD 链得得

70.区块链适合什么行业?

区块链作为一个技术可以运用到很多行业，我们先要了解区块链技术有哪些特性和优点：区块链技术可以提供去中心化、不可篡改、高信任度、可追溯、匿名性、分布式账本等多重功能保证。每个行业都可从自身需求入手，从而结合区块链技术。

第一，金融与区块链结合。金融领域算是区块链运用最早最广的一个领域之一。区块链技术可以运用到金融的结算和清算、数字货币、跨境支付、保险、证券等多个应用。

第二，物联网和供应链。供应链行业会涉及很多实体，如资金、物流、信息等。区块链的去中心化等核心特征就可以对物品、物流进行实时追溯，利用智能合约加强信任，区块链的开放透明性，使得所有人都可以实时查询，由此也减少时间和金钱成本，提高合作效率。私钥公钥的匿名性也能够保护消费者隐私，同时区块链的不可篡改对商品销售和售后服务进行保障。同理，也可以运用到版权、医疗、游戏能领域。

第三，博彩类。博彩行业像在美国的 powerball，它是每天大约有一千万美元的收入。为什么有这么高的收入呢，关键还是通过政府的背书，产生了很高的信任而区块链技术就能很好的代替政府的信任作用。

* 目前来看区块链适合什么行业？链得得已发布多篇文章进行论述，下载链得得 App， 参考详文：

《【大文观链】区块链颠覆传统金融：保险业》
《【大文观链】《逆水寒》和区块链：网易游戏弯道超车的新尝试》
《【大文观链】民政部牵头的区块链+慈善能够做什么？》

71.区块链在"去中心化金融"中起到什么角色?

去中心化金融全称 Decentralized Finance，简称 De.Fi，也被称做 Open Finance。按照目前的发展来看，智能合约与区块链技术相结合的应用和服务是 De.Fi 的重要组成部分。

2018 年 8 月，借贷协议 Dharma Labs 联合创始人及首席运营官 Brendan Forster 发表文章《Announcing De.Fi，A Community for Decentralized Finance Platforms》，首次提及 De.Fi 这一概念。在文中，Brendan Forster 提到 De.Fi 是一个分散的金融平台社区，应该符合以下标准：1.采用区块链技术；2.服务于金融业；3.代码开源；4.有强大的开发者平台。

随着区块链技术的不断发展，De.Fi 被赋予的意义也越来越广：利用开源软件和分散式网络，传统金融产品逐渐变为无信任且透明的协议运动，无需担心信任问题。

De.Fi 可以看做是 FinTech（金融科技）的细化分类，但 FinTech 还是在围绕传统金融模式做改良，因为区块链技术以及开源代码等技术加持，De.Fi 相比 FinTech 而言，对体制与信任度的需求更少，更有利于实现国际化资产流动。

注：金融科技（Financial technology，简称 FinTech），金融科技可以理解为利用大数据、人工智能、征信、区块链、云计算、移动互联等新科技手段，服务于金融效率提升的科技产业。

* 关于"去中心化金融"的一系列详细内容，下载链得得 App， 参考详文：

《【得得白话】细说"去中心化金融"系列一：De.Fi 概念的缘起和分类》
《【得得白话】细说"去中心化金融"系列二：解析去"中心化借贷与交易所"》

72.什么是链改？企业如何通过通证经济改造上链?

链改就是利用区块链技术对企业进行改造，其实也就是我们常说的企业上链。目的在于降低成本、提升效率、创新商业模式、增强竞争壁垒等。说了半天，那究竟要怎么改呢？
第一种方法，进行区块链技术的链改。最直观的就是把企业传统账本换成区块链。还记得区块链的本质吧：去中心化的分布式账本。这里的账本不仅包含资金的变动转移，还可以包含企业生产的商品物流信息、交易信息等等。

那进行区块链技术改造有什么好处呢？就拿跨境转账来说，小明要从香港转 100 欧元到巴黎，那么电汇通常要 3 到 4 个工作日到账，遇到节假日还要延后，当然不同的汇款方式时间也会不一样，而且小明还要交手续费、电讯费，这些费用可能都快赶上他的本金了。（境外汇款的到账时间跟国家和时区及清算路径有关，还要看中转行数量及节假日时间）
所以总体来说，跨境汇款具有高手续费、耗时长的缺点。而且不仅用户体验感很差，中间涉及的银行也表示很无奈。小明这一转账，中间可能会涉及中国香港银行、中国巴黎分行等一系列银行的账本，还会涉及巴黎方面的银行，各家银行的账本都是独立的，定期两两对账，可能一家银行同一个账单就要对好几遍，而且每一次对账也是要花钱的，如果哪家

账本出了问题，可能还要推翻重来，光想想这期间要花费的成本还有时间，真是心疼这些银行。

而上述说的这些问题，就显出区块链技术的优势了。通过设立一个统一的区块链账本，由所有银行一起来记录和维护，当发生交易的时候，自动刷新账本并且无法篡改，这样每次交易就只需要进行一次对账，极大的降低了企业成本和信任危机，这也是链改最大的价值所在。
我们刚才说了第一种方法是进行区块链技术的链改，第二种方法，就是经济学链改，也就是用 Token 进行的通证改造。

通证是指流通的加密数字权益证明，英文为 token。传统企业通过发行 token，将权益下放重新分配，激励用户，从而让生产方、消费方、第三方平台都获得收益，达到共赢，改善协作关系的目的，形成自治的通证经济体。

通常企业发行 Token 会确定一个数额，比如一亿个，然后拿出三分之二流通在用户中和企业里面，剩下的当做原矿，等着用户来挖，怎么挖？用户在进行交易的时候，使用了 Token 让它流通起来，就相当于挖矿的过程，这里的交易范围就很广了，包括产品销售、用户消费、发送广告等等，所以也有了那套很火的理论“交易即挖矿”。而这一切都基于区块链技术、智能合约而实现去信任的环境，在不知不觉中通过链改将产业链的各个环节都整合起来。

同时发行的 Token 也隐含了公司的现金收入和股东权利，将员工、股东、客户之间的权益进行再分配，从而改善企业结构，其实就像我们上面说的币改。

需要注意链改并不完全等同于币改，有些领域上链就不需要 Token，比如区块链发票等。

73.“区块链概念股”有什么？

所谓“区块链概念”就是有区块链相关业务的上市公司。根据东财 Choice 显示，A 股上市公司包含 185 只区块链概念股，其中包括工商银行、中国平安、工业富联、中国联通、三六零、顺丰控股等千亿级市值规模以上的公司。

此外，像阿里巴巴、腾讯、百度、京东、迅雷等海外上市公司，同样已经布局了区块链相关业务。也被称为“区块链概念股”。

在 2019 年的 3 月 30 日和 10 月 18 日，国家网信办先后公布了两批境内区块链信息服务项目备案，总共涉及到 506 个备案项目，其中就包括多家国内外上市公司。根据这样一份权威名单，链得得做梳理后发现，这两批项目备案中共涉及到 39 家上市公司：

京东、迅雷、阿里巴巴、百度、爱奇艺、东港股份、信息发展、远光软件、平安银行、工商银行、新晨科技、苏宁、海联金汇、暴风集团、航天信息、巨灵信息、东方财富、汉得信息、江苏银行、恒生电子、同花顺、南威软件、南方航空、广电运通、全碟软件、美的、中国平安、浙商银行、众安在线、腾讯、爱奇艺、易见股份、安妮股份、晨鑫科技、好未来、金山软件、顺丰控股、华大基因、卓尔智联。

* 关于“区块链概念股”的详细内容，下载链得得 App， 参考详文：

《90 只开盘涨停！全面复盘 A 股区块链概念整装待发的一年丨得得分析》

74.初创公司在区块链行业如何找到方向和定位？这是大厂之间的游戏吗？

区块链是一种全新的分布式帐本系统，这也就意味着大公司如果把他们已经成熟完备的业务或应用迁移到一套全新的区块链底层平台上，这里面的成本是非常大的。所以，从这个方面来讲，如果一家区块链初创型公司有明确的业务定位和商业模式，那么他们应用区块链技术的成本会很低。

而从技术的角度来讲，区块链同样是一门全新的学科，这里面涉及到智能合约、非对称加密、分布式存储、零知识证明等全新的理论知识。从这点上来看，大厂和初创型企业都在一条水平线上，大家都是一个探索和尝试的状态。对于大厂来说，他们有资本和资源优势，但是对于初创公司来说，他们应该在某一专业领域有所建树，这样才能够在商业竞争中实现突围。

75.区块链产品应用场景

银行业：银行是一个安全的存储仓库和价值的交换中心，而区块链作为一种数字化的、安全的以及防篡改的总账账簿可以达到相同的功效。

交易和跨境支付：区块链可能绕开笨重的转账系统，创建一个更直接的支付流，它可在国内或跨国界，并且无需中介，以超低费率几乎瞬时速度的方式支付。

供应链金融：基于区块链的供应链金融和贸易金融是基于分布式网络改造现有的大规模协作流程的典型。区块链可以缓解信息不对称的问题，十分适合供应链金融的发展。

物联网：区块链可以成为大量设备的一种公共账簿，它们将不再需要有一个中央化的路由在他们之间居中交通。在没有了中央控制系统来验证之后，设备将能够在它们之间互相匿名传输，并管理软件的更新、错误，或者进行能源管理。

医疗：区块链技术可以让医院、患者和医疗利益链上的各方在区块链网络里共享数据，而不必担忧数据的安全性和完整性。

政务：政务信息、项目招标等信息公开透明，政府工作通常受公众关注和监督，由于区块链技术能够保证信息的透明性和不可更改性，对政府透明化管理的落实有很大的作用。
供应链管理：区块链技术最具普遍应用性的方面之一就是它使得交易更加安全，监管更加透明。简单来说，供应链就是一系列交易节点，它连接着产品从供应端到销售端或终端的全过程。从生产到销售，产品历经了供应链的多个环节，有了区块链技术，交易就会被永久性、去中心化地记录，这降低了时间延误、成本和人工错误。

云服务：目前提供云存储的公司大都将客户数据放在中心化的数据库中，这提高了黑客盗取信息的危害性。区块链云存储方案允许去中心化的存储。

大数据：区块链以其可信任性、安全性和不可篡改性，让更多数据被解放出来。基于全网共识为基础的数据可信的区块链数据，是不可篡改的、全历史的、也使数据的质量获得前所未有的强信任背书，也使数据库的发展进入一个新时代。

76.区块链行业人才市场情况怎么样？（平均工资、用户需求）

从 2019 年第三季度区块链招聘需求的城市分布来看，区块链行业人才需求主要集中于一线和新一线城市，与人才求职城市分布对应，且人才供给明显更集中在一线城市。目前，一线城市区块链存量人才占比 61.96%，其次是新一线城市占比 26.01%，一线城市人才储备充足。

2019 年三季度，区块链招聘需求城市分布中，深圳、上海、北京位于第一梯队，招聘人数占比分别达到 21.07%、16.07%、13.9%，广州和成都紧随其后，分别占比 5.79%、5.34%。从薪酬来看，区块链领域平均招聘薪酬达到 16317 元，是全国平均的近两倍。这或许也是其人才吸引力如此之大的关键原因。但从变化趋势看，与全行业平均薪酬的持续增长不同，区块链领域的招聘薪酬近两年持续在 1.6 万元/月上下波动。

根据智联招聘提供的数据，区块链招聘人数数量 TOP10 职位中，热门岗位软件工程师平均招聘薪酬为 16008 元/月；销售代表平均招聘薪酬 10094 元/月；高级软件工程师平均招聘薪酬 23606 元/月。其中合伙人平均招聘薪酬最高，为 75975 元/月，位居薪酬榜首。除此之外，其他高薪岗位多为高级专业技术岗。

77.全国各地区块链市场规模对比

2019 年上半年，香港的区块链项目融资金额远超国内其他城市，占到了约 41% 的比重，同时也是唯一一个融资金额超过 10 亿元的城市。

杭州市的融资金额超过北上广深四大城市，达到 7 亿元，占到了全国前十总量的 28%；
北京市位列第三，虽然在融资事件数量上有优势，但是具体的融资数额不及香港和杭州，约占全国区块链融资总额的 18%；广州市紧随其后，融资额超过 2 亿元，约占全国区块链项目前十融资总额的 8%。

在融资数量方面，北京独占鳌头，有 36 起，是国内发生区块链融资事件最多的城市，占据了全国（包括港澳台）前十榜单中融资数量总数的 50% 左右。上海、深圳、香港和杭州紧随其后，分别发生 9 起、6 起、6 起、4 起融资事件。

从地理位置分布来看，除北京外，由于区块链相关企业注册地点大多在沿海省市，与区块链相关的融资事件也多在沿海地区。其中，浙江省是国内区块链融资事件涉及城市最多的省份。

据统计，全国共有 22 个区块链产业园区。从地理区域划分来看，全国区块链产业园区主要集中在华东、华南等地区，其中浙江省和广东省各有 4 家区块链产业园区，并列全国区块链产业园区数量首位。而从城市分布来看，杭州、广州、上海最多，三大城市区块链产业园数量占比全国 50% 以上。

78.投资机构对于区块链的最新看法

近年来，中国区块链行业的快速发展逐渐获得投资机构关注，中国区块链行业投资年增速已连续多年超过 100%。专注于区块链行业的投资机构正在飞速成长，在区块链产业积极布局，构建自己的版图，而持开放态度的传统投资机构也在跑步入局。

从投资项目分类来看，投资机构普遍看好区块链平台类的公司。
从投资标的地域来看，投资机构更多的投资于海外项目。
从国内项目角度来看，北京地区项目占比最高。
从投资轮次来看，大部分投资发生在天使轮及 A 轮，反映行业仍处于早期阶段。

79. 区块链可以给社会带来什么变化?

此前大家看到的新闻“怎么证明我是我”这一问题，便是可以用区块链就能解决的问题。通过区块链的去中心化特质，让信用制度，不再由集权化，中心化的机构制定，而是通过全

民认可的区块链技术完成，创造一个真正的公平的社会。

现在人们越来越意识到隐私的重要性，通过区块链技术，可以做到让个人的数据不会泄露出去。例如，个人医疗的历史数据，未来看病或对自己的健康做规划就有数据可供使用，而这个数据真正的掌握者是患者自己，而不是医院或某个第三方机构。

在交易与货币流通上，采用区块链技术的数字货币可以进行点对点交易，而不再需要支付宝等第三方机构，通过银行机构产生的手续费也就不存在了。

80.目前区块链市场环境的概况和未来发展？

我国区块链产业目前处于高速发展阶段，创业者和资本不断涌入，企业数量快速增加。区块链应用加快落地，助推传统产业高质量发展，加快产业转型升级。利用区块链技术为实体经济“降成本”、“提效率”，助推传统产业规范发展。

此外，区块链技术正在衍生为新业态，成为经济发展的新动能。区块链技术正在推动新一轮的商业模式变革，成为打造诚信社会体系的重要支撑。与此同时，各地政府积极从产业高度定位区块链技术，政策体系和监管框架逐步发展完善。

81. 为什么国家要重推区块链技术？

政治局讲话中，首先给区块链技术做了定调：
1. 区块链是全球性争夺技术。
2. 区块链对整个技术和产业领域都会发挥重要作用。
3. 中国有很好的基础，区块链技术未来会全面融入经济社会。

第一，科技导向。目前，全球主要国家都在加快布局区块链技术发展。在区块链技术发展上，中国正在抢占跑道。在中美贸易摩擦的大背景下，中国企业越来越强调对最核心的「硬技术」的掌控，从政府政策引导来看，也更加鼓励企业进行区块链核心技术的自主创新。讲话中「最前沿」「制高点」「新优势」，三个词无疑说明中国在区块链竞争领域的目标确定而唯一：就是争夺第一。

第二，产业导向。此次讲话指明了区块链技术要服务实体经济。总共 1000 字的讲话中，提到了 5 次融合。区块链技术的关键在于「融合」。区块链技术一定要解决某一领域的具体问题，这就要求区块链技术能深入到具体场景中。区块链技术在产业应用中，也不是一个点的应用，更多是融合的应用。用总书记的话来说就是「打通创新链、应用链。价值链」。

第三，民生导向。区块链技术不可篡改、多方参与的特性是提升社会治理的重要工具。区块链在民生与公共服务领域有天然的优势，未来在教育、就业、养老、精准扶贫、医疗健康、商品防伪、食品安全、公益和社会救助等方面的应用价值会逐步显现出来。

82.区块链中有哪些行话？那些“行话”都是什么意思？

币圈：指的是专注于炒币，甚至发行自己的数字货币进行筹资的人群，一般来讲，区块链项目方、交易所、一些区块链媒体，他们都属于币圈。

链圈：指专注于区块链的研发、应用或区块链底层协议的人群。没有链圈的技术支撑，币圈也不可能存在，未来区块链场景的落地，还要依靠链圈的技术作为支撑。

矿圈：指的是专注于“挖矿”的“矿工”人群。

炒币：指的是为了获取高额的收益，而反复通过交易平台买卖数字货币的行为。

梭哈：是英文 Show Hand 的音译，原本是赌博游戏中的名词，将手中全部的可用筹码一次性押出的行为。引申到区块链投资，是指为了炒币，把自己所有的可用资产来投资数字货币，有一种“押上身家赌一把”的含义。

佛系持币：指持币后不关心加密货币价格走势，无论加密货币资产价格跌到什么程度，都不会减持 手中的加密货币的行为。

庄家：是指拥有雄厚的资金体量，强大的关系网和最灵通消息的投资者，庄家能够在较大程度上影响或决定某个币种的价格走势。

大户：是指拥有雄厚资金的投资者，但没有庄家那么强大的资金量和关系网。

散户：是指资金量小，买卖数量不大、无组织的投资者。

韭菜：是一个形象的比喻，韭菜的生长能力和适应能力都很强，可以一茬接着一茬儿地大范围繁殖。比喻一些不了解市场情况的散户投资者，他们大多容易受到投资情绪左右，高位买入、低价卖出，有人亏损离场后又会有新生力量进入，就像韭菜一样割一茬很快又长一茬。

割韭菜：是指庄家低位买入，炒高币价，等散户进来后高价卖出获利，再砸盘砸到低位，这样一来散户就会蒙受损失，而庄家就会获利。庄家和大户不断重复着这样的套路，就是“割韭菜”行为，而散户源源不断入场，庄家便重复着割韭菜的套路。

空投糖果：是指区块链项目起步时候，为了推广项目，而免费向用户发放一定数量的数字货币，这些免费的数字货币就被用户们称之为“糖果”。

私募/ICO：一种融资行为。ICO，首次币发行，源自股票市场的首次公开发行（IPO）概念，是区块链项目首次发行代币，募集比特币、以太坊等通用数字货币的行为。

交易对：EOS/ETH ,这样的显示为交易对，指购买一个 EOS 需要支付多少个 ETH，类似于‘克/元’的概念。

钱包：一般指区块链钱包，新人还不了解的情况下不建议使用。点击查看钱包使用教程
白皮书：就是项目介绍官方专业版。

空投/糖果：项目方赠送代币的行为叫空投，送的代币叫糖果

KYC：身份验证，一般需要提供身份证件或者护照。

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。

牛市：它是指市场行情呈现普涨，很长一段时间的大升势。在币圈主要是 BTC 的上涨带领其他各主流币，山寨币的上涨。牛市阶段，基本是人人赚钱，因为牛市只需要“博傻”就行。如果你在牛市赚不到钱，那只能说你在瞎胡乱搞或者是你点背到了极点。

熊市：刚好与牛市相反，它是指市场行情持续走低，市场情绪表现低迷，市场呈现普跌的现象。你当前经历的就是熊市。这一阶段，最重要的是咱们需要活下来。然后就是进一步的行动，囤币，抄底之类的操作。

利空：也是消息面，多指对行情不利的消息。但是市场上也有这样的说法：利空出尽就是利多。

搬砖：看准平台之前的差价，跨平台来赚取其中的差价。搬砖需要注意的就是转币速度，有时候会因为转币速度的问题影响你的收益。

场外交易：很多平台也叫法币交易。就拿火币来说，平台无法充值人民币，很不方便。但是平台提供法币交易，就很方便了。平台做担保，商家或个人可以直接用人民币交易，购买或出售自己手里的主流币或 USDT。

割肉：好听点叫“斩仓”。你们部分人经常干的一件事，跌了也卖，害怕跌的更厉害。

做多：大部分人每天做的就是做多，低买指望高卖。一般指看涨。

做空：做期货合约的人会玩的操作。你看跌后市，买跌就是做空。

法币：法定货币，是由国家和政府发行的，只有政府信用来做担保，如人民币、美元等。

Token：通常翻译成通证。Token 是区块链中的重要概念之一，它更广为人知的名字是“代币”，但在专业的“链圈”人看来，它更准确的翻译是“通证”，代表的是区块链上的一种权益证明，而非货币。

对冲：是同时进行两笔行情相关、方向相反、数量相当、盈亏相抵的交易。在期货合约市场，买入相同数量方向不同的头寸，当方向确定后，平仓掉反方向头寸，保留正方向获取盈利。

83.区块链对于普通人实际生活有什么作用或影响?

跨境支付：减少用户重复提交证明材料，提升效率等。

知识产权：数字确权、认证、溯源、身份验证。

社会公益：公益透明化、公共治理、提升政府工作效率。

食品安全：食品溯源、食品认证。

医疗：实现病历管理、隐私保护、数据共享、简化就诊流程、药品溯源、处方管理等。

能源：电力交易、碳排放、加油站。

教育：学历信息存储，学生信用体系建立。

84.日常生活中是否可以用比特币等数字货币来购买商品?

披萨：第一个用比特币买披萨的土豪吃货名字叫 Laszlo Hanyecz，他曾用 1 万枚比特币买了两个披萨。

太空票：理查德布兰森的维珍银河可以使用比特币进行太空旅行。

环游世界：皇家加勒比海水手在马来西亚停留了数百艘从新加坡到泰国的巡洋舰。巡洋舰有一个共同点：他们都用比特币支付了旅程的费用。其次，他们召集了最大的比特币主题游轮。

豪华度假村：特朗普酒店接受比特币用于公寓。

学费：美国国王学院，柏林 ESMT 和基于 UL 的坎布里亚大学。瑞士的应用科学和艺术学院卢塞恩自去年 9 月以来也一直接受 BTC 付款。

豪车：日本加密货币交换 bitFlyer 和几家豪华汽车销售商合作，为高端汽车提供比特币支付。

艺术品许可证：Ato Gallery 以惊人的 150 比特币出售了一件估计价值不超过 10 万美元的艺术品。

电子产品：微软，NewEgg 和 Overstock.com 接受加密支付。笔记本电脑和智能手机等电子产品是 BTC 付款的首批产品。

整形手术：在佛罗里达州迈阿密 Vanity 整形医院，做腹部抽脂、隆胸等整形手术，都可以通过比特币支付。

五、政策篇

85.国内大力发展区块链的背景下，政府对数字货币市场态度是否会有转变?

数字货币的快速崛起，大量私人和机构投资者的参与，以及巨大的价格波动，促使各国监管者越来越重视这个行业。然而，我们不得不强调一个经常被忽略的事实——数字货币行业还非常年轻，只有 11 年的历史，真正引起监管层的注意也只有近 3 年时间，加上数字货币本身的定义充满争议，因此对数字货币的监管还处在雏形阶段，不仅全球各国区别很大，而且一直处于快速的动态变化中。

86.未来企业可否自主发币融资?

2017 年 9 月 4 日，我国下发了《关于防范代币发行融资风险的公告》，明确指出所有利用数字货币融资的行为都属于非法集资。

代币发行融资是指融资主体通过代币的违规发售、流通，向投资者筹集比特币、以太币等所谓“虚拟货币”，本质上是一种未经批准非法公开融资的行为，涉嫌非法发售代币票券、非法发行证券以及非法集资、金融诈骗、传销等违法犯罪活动。

因此企业发币融资之路在中国目前暂时并不可行。但是随着政策的完善和明确，未来不排除会进一步放开，为实体经济服务，解决中小企业融资难问题。

目前中国香港已经开始进行部分证券化实践，2019 年 3 月 28 日，香港证券及期货事务监察委员会（证监会）官网发布有关证券型代币发行的声明，旨在提醒从事证券型代币发行（security token offering，简称 STO）的公司或个人有关适用的法例及监管规定，并再次希望提醒投资者注意，与虚拟资产（包括 STO 关涉的代币，即证券型代币）有关的风险。

香港证监会指出，如推广及分销属于证券的证券型代币，中介人必须遵循法律及监管规定，只能发售给专业投资者，应进行尽职调查，须以清晰且易懂的方式向客户提供相关 STO 的资料。中介人在从事任何有关 STO 的活动以前必须先与证监会讨论其计划，而且必须落实足够的系统与监控措施，确保在进行分销 STO 活动前符合相关规定，否则持牌资格可能受到影响，并可能导致证监会采取执法行动。

87.当前全球对区块链和数字货币的态度如何?

整体而言，监管升级和规范化是大势所趋。近些年全球各个国家和地区对区块链和数字货币的监管政策有以下几个特点：

1、监管趋严，全球数字货币监管逐步规范化
2、监管分化，亚洲国家较欧美国家对待数字货币更为谨慎
3、放宽监管，小众国家多进行合法化尝试

根据对加密货币的合法性及监管程度，将全球各个国家和地区对数字货币的监管可分为五类。

1) 明确交易合法，并设立法律规范交易。当地政府明确数字货币交易合法，同时或多或少建立相关法律对其进行规范。

2) 明确交易非法，严格控制数字货币交易。当地政府严格控制数字货币交易，明文规定交易违法，甚至提供和使用数字货币将构成犯罪。

3) 对交易进行部分限制。当地政府对涉及数字货币的一部分交易存在限制，不允许国内出现 ICO 或数字货币交易，但并不限制私人持有数字货币。

4) 未公开合法化，保持中立。当地政府并未对数字货币交易进行明确表态，既不限制交易也未公开合法化。

5) 尚未置评。即目前尚未表态或无信息考证。

近期监管进展中，中国香港证券及期货事务监察委员会（香港证监会）于 11 月 6 日发布《立场书：监管虚拟资产交易平台》及《有关虚拟资产期货合约的警告》。

《立场书》明确了证监会对虚拟资产交易平台的监管方针、监管框架和未来预期，对虚拟资产交易平台实行了牌照准入制度，并在资产托管、KYC、AML、审计、风控等方面进行了规定。

《警告》则表明销售虚拟资产期货合约的平台有可能违反香港法例，而由于此类期货合约附带极大风险，投资者在投资时应保持警觉。

香港证监会称，虚拟资产期货合约下的虚拟资产价格极端波动，相关虚拟资产难以估值；其高度杠杆化的性质令投资者的风险倍增；这些产品的复杂性和固有风险可能令投资者难以理解，而且不时有报道指出，销售或买卖这类合约的平台涉及操纵市场和违规活动；这些资产交易平台的交易规则可能不清晰、不公平。其他地区的部分监管机构一直在积极审视这类平台，并考虑采取介入行动，如完全禁止向散户投资者销售这类期货合约。

另一方面，由于数字货币价格巨幅波动，日本金融厅开始升级监管。2019 年 9 月 30 日，日本金融厅官网公布《面向金融商品交易业者监督管理方针》，该方针表示，因为数字资产的投机成分等原因，金融厅将对于包含数字资产的金融商品组合、交易等都会谨慎对待。10 月 18 日，日本内阁决议发布《政治资金管理法》又间接将数字货币排除在"金钱及有价证券"范围内。

而根据日本经济新闻 11 月 5 日的报道，日本金融厅将制定新的条例， 2019 年内禁止成立与交易以暗号资产为投资对象的投资信托。虽然在法律上，尚未有明文写出来，但是本次发布的监管指南无一不透露着封杀数字货币的味道。日经新闻甚至表示，这次监管指南可以被认为是"具有实际意义上的强制性"。

* 链得得长期追踪全球各地区对于数字货币监管政策并作出对应专业解读，目前已发表一系列文章，更多详情可下载链得得 App， 参考详文：

《称"数字货币"为资产，G20 成员国监管政策全梳理丨链得得独家》
《【链得得深度】"九四"一周年：全面复盘全球数字货币监管政策与市场趋势》
《【链得得独家】2018- 2019 全球加密货币市场年报丨第三章：224 个国家地区监管政策汇总与研究》
《解读香港"监管交易所立场书"：虚拟资产领域迫切需要全面立法丨链得得独家》
《【链得得独家】律师解读《立场书》：无证开展期货合约，或被追究刑事责任》
《日本金融厅：禁止交易以虚拟货币为对象的投资信托》
《【链得得独家】政策技术双瓶颈：日本币圈凉凉，链圈还有救吗？》

88.当前全球对 Libra 的看法是什么？

中国：较为关注，继续推进中国央行数字货币研究。

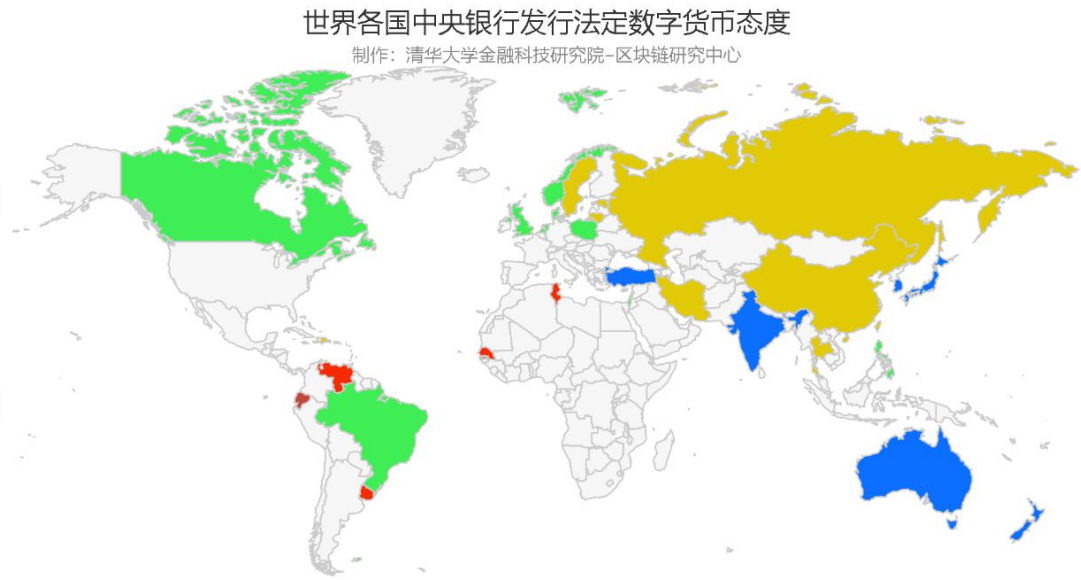
美国（美联储）：谨慎关注。迄今为止美联储、美国国会已累计三次召集 Libra 相关负责人出席听证会，由于 Libra 声称在获得美国各方监管批准前 Libra 不会在世界任何国家和地区发行，目前美国监管部门对 Libra 持谨慎态度。

欧盟：反对居多。德国与法国财政部长联合申明反对 Facebook 计划发行的加密数字货币 Libra 在欧洲推行。其指出，货币权力属于国家主权，不应由私人实体掌握。同时由于欧盟地区对个人隐私保护的规定较为严格，目前来看 Libra 在欧洲推行较难。

89.当前各国对央行数字货币的看法是什么？

8 月 10 日，中国人民银行支付结算司副司长穆长春在中国金融四十人论坛上表示，央行数字货币即将推出，将采用双层运营体系。

清华大学金融科技研究院-区块链研究中心的报告显示，在 25 家央行中，计划推出 CBDC 的央行有 7 家，探索中 9 家，已发行 6 家，暂不考虑 3 家。目前来看，发达国家多都是出于避免私人支付公司垄断考虑发行，发展中国家和非洲国家多因为金融普惠，突破制裁等。



90.当前中国各地方政府都已出台了哪些区块链相关政策？

中央：2019 年 10 月 24 日，国家主席习近平在中央政治局第十八次集体学习时强调区块链技术的集成应用在新的技术革新和产业变革中起着重要的作用。我们要把区块链作为核心技术自主创新的重要突破口，加快推动区块链技术和产业创新发展。

北京：2018 年 12 月，北京市西城区发布《关于支持北京金融科技与专业服务创新示范区(西城区域)建设若干措施》，要大力扶持金融科技应用示范，倡导安全、绿色、普惠金融服务，对人工智能、区块链、量化投资、智能金融等前沿技术创新最高给予 1000 万元资金奖励，切实助力产业和经济发展，助力城市智慧运行。

上海：2019 年 9 月 6 日，上海市发布《2019 上海区块链技术与应用白皮书》，从企业、技术、应用、人才培养等多个维度详细分析和解读了国内外、特别是上海地区区块链产业的发展现状，在行业中十分具有指导意义和影响力。

深圳：2019 年 8 月 18 日，中共中央、国务院发布关于支持深圳建设中国特色社会主义先行示范区的意见。意见指出，支持在深圳开展数字货币研究与移动支付等创新应用。

杭州：2019 年 6 月 20 日，浙江省数字经济发展领导小组办公室、省经信厅、省大数据发展管理局联合印发了《浙江省“城市大脑”建设应用行动方案》。方案指出，要推进“城市大脑”产业生态圈发展，带动面向人工智能的操作系统、数据库、中间件、开发工具等基础软件，以及关键芯片、器件、模组、智能终端等硬件发展，加快培育网络安全、区块链、数字创意等新业态。

2019 年 10 月 29 日，经中国人民银行同意，由中国互金协会和世界银行共同支持建设的全球数字金融中心在杭州正式成立。

河北省（雄安）：2019 年 11 月 1 日，河北省长许勤主持召开省政府常务会议。会议指出，要强化规划和政策引领，把区块链纳入河北省数字经济“十四五”发展规划，加快制定专项行动计划。

2019 年 10 月 10 日，《中国（河北）自由贸易试验区管理办法》在省政府第 65 次常务会议通过。其中第三十三条，支持雄安片区数据资产交易。推进公共数据利用改革试点，建立大数据资产评估定价、交易规则、标准合约等政策体系，依托现有交易场所开展数据资产交易，推进基于区块链、电子身份（eID）确权认证等技术的大数据可信交易，支持开展数据资产管理、安全保障、数据交易、结算、交付和融资等业务。

贵阳：2017 年 5 月，贵阳高新区推出《贵阳国家高新区促进区块链技术创新及应用示范十条政策措施（试行）》，在入驻、运营、成果奖励、人才、培训、融资、风险、上市十个方面提供政策支持；

2017 年 6 月 7 日，贵阳市发布《关于支持区块链发展和应用的若干政策措施（试行）》，加速推进区块链发展和应用，促进区块链各类要素资源集聚。

长沙市：2018 年 6 月 22 日，长沙经济技术开发区管委会下发红头文件《长沙经开区关于支持区块链产业发展的政策（试行）》，将设立总额 30 亿元的区块链产业基金，投资区块链企业。区块链企业自落户之日起，3 年内给予最高 200 万元的扶持资金。

云南省：2019 年 4 月 15 日，云南省政府网站公布的《云南省实施“补短板、增动力”省级重点前期项目行动计划（2019—2023 年）》提出，推动数字产业化。重点以区块链技术应用为突破口，引进一批区块链创新企业，率先在跨境贸易、数字医疗、数字小镇实现区块链示范应用场景落地。

山东省：2019 年 7 月 19 日，山东省印发《山东省支持数字经济发展的意见》，意见提出到 2022 年，重要领域数字化转型率先完成，数字经济规模占全省地区生产总值比重年均提高 2 个百分点。山东省提出，要将数字产业打造成山东的支柱产业，做大做强大数据、云计算、物联网等核心引领产业，超前布局人工智能、虚拟现实、区块链等前沿新兴产业，巩固发展集成电路、基础电子等关键基础产业，全面提升高性能计算机、高端软件、智能家居等特色优势产业。

福建省：2019 年 3 月 20 日，福建省政府办公厅近日印发《2019 年数字福建工作要点》，提出在数字经济方面，在数字经济方面，我省积极创建国家数字经济（福厦泉）示范区，加快建设福州软件园县（市、区）分园，推动数字福建（长乐）产业园、马尾物联网基地产业集聚；同时支持福州创建区块链经济综合试验区。

91.听说香港开始发放虚拟银行牌照，目前已有几家公司获得牌照?

香港金融管理局（金管局）至今分三批共发放 8 张虚拟银行牌照，但部分虚拟银行正式投入市场运作的时间未定。11 月 6 日，香港金管局总裁余伟文表示，部分虚拟银行的目标是于今年底至 2020 年初推出市场，但个别虚拟银行在推出之初，或只供特定客户群在"沙盒"环境试用一段时间，然后再作修改或优化，待准备妥当才正式推出给公众使用。

3 月 27 日，金管局副总裁阮国恒公布了首批虚拟银行牌照名单，三家获牌机构分别为： 1. Livi VB：中银香港（控股）、京东数科及怡和集团成立的合资公司； 2. SC Digital Solutions：渣打（香港）、电讯盈科、香港电讯及携程金融成立的合资公司； 3. 众安虚拟金融：由众安在线及百仕达集团合资成立。

4 月 10 日，金融科技集团 WeLab Holdings 在其官网上宣布旗下全资子公司 WeLab Digital Limited 获得，这是金管局第二次颁发虚拟银行牌照，

5 月 9 日，金融管理专员已经根据《银行业条例》向四家发放牌照，分别为：1、蚂蚁商家服务(香港)有限公司；2、贻丰有限公司；3、洞见金融科技有限公司；4、平安壹账通有限公司授予银行牌照以经营虚拟银行。

公开资料显示，蚂蚁商家服务(香港)有限公司是阿里巴巴旗下蚂蚁金服的全资子公司；贻丰有限公司为腾讯控股有限公司、中国工商银行（亚洲）有限公司、香港交易及结算所有限公司、高瓴资本和香港商人郑志刚通过 Perfect Ridge Limited 投资的合资公司；洞见金融科技有限公司由小米集团与尚乘集团共同出资设立，小米集团占比 90%，尚乘集团占比 10%；平安壹账通有限公司为中国平安旗下金融壹账通的全资子公司。

自今年 3 月底启动发放虚拟银行牌照以来，香港金管局已累计发出八张牌照，香港的持牌银行数增加到 160 家。

92.未来中国将如何推进区块链行业发展?

中共中央总书记习近平在近日中共中央政治局第十八次集体学习主持学习时强调，我国在区块链领域拥有良好基础，要加快推动区块链技术和产业创新发展，积极推进区块链和经济社会融合发展。

1) 强化基础研究，提升原始创新能力，努力让我国在区块链这个新兴领域走在理论最前沿、占据创新制高点、取得产业新优势。

2) 推动协同攻关，加快推进核心技术突破，为区块链应用发展提供安全可控的技术支撑。要加强区块链标准化研究，提升国际话语权和规则制定权。

3) 加快产业发展，发挥好市场优势，进一步打通创新链、应用链、价值链。

4) 构建区块链产业生态，加快区块链和人工智能、大数据、物联网等前沿信息技术的深度融合，推动集成创新和融合应用。

5) 加强人才队伍建设，建立完善人才培养体系，打造多种形式的高层次人才培养平台，培育一批领军人物和高水平创新团队。

93.有序发展区块链，中国需要做些什么?

1) 加强对区块链技术的引导和规范；

2) 加强对区块链安全风险的研究和分析，密切跟踪发展动态，积极探索发展规律；

3) 要探索建立适应区块链技术机制的安全保障体系，引导和推动区块链开发者、平台运营者加强行业自律；

4) 落实安全责任。要把依法治网落实到区块链管理中。

94.中国大力发展区块链对相关管理部门有什么要求?

相关部门及其负责领导同志要注意区块链技术发展现状和趋势，提高运用和管理区块链技术能力，使区块链技术在建设网络强国、发展数字经济、助力经济社会发展等方面发挥更大作用。

六、风险篇

95. 区块链的弊端有哪些?

首先是安全性问题，基于 POW 共识机制的区块链存在 51%攻击问题，即掌握了全网超过 51%的算力便可以篡改和伪造区块链的数据。

其次是效率问题，去中心化网络在各个节点之间达成一致的效率很低，很难像中心化支付方式那样快速。

* 链得得曾发布多篇文章进行区块链安全性分析，具体详情可下载链得得 App， 参考详文：

《【得得白话】51%算力实施的“双花攻击”，会如何毁掉区块链信任原则？》
《【大文观链】ETC 遭遇的 51%攻击是什么？有多严重？》

96.数字货币有被盗的风险吗?

有，仅 2019 年上半年，全球出现了至少 10 起加密货币交易所被盗事件，与此同时，数字资产诈骗事件也频频发生。被盗或被诈骗的数字货币总额或已超过了 50 亿美元。

97.加密交易所如果被盗，用户要如何用法律追回损失?

目前在我国 ICO 等交易行为是非法的、被禁止的。受相关政策影响，各公司纷纷选择出海开展虚拟货币相关业务。由于各个国家对于 ICO 的监管态度不一，监管手段和程度各异，投资者也会因此面对各种不确定的风险。

根据现行法规政策，通过发行数字货币进行融资在我国被视为扰乱金融秩序，是不被法律保护的交易行为。交易所的数字货币也不视为合法财产，因此很难用法律手段追回损失。

98.如何简单区分一个区块链项目是否是骗局（空气币）？

“1 年收益率 500%”、“开盘就翻倍”、“年底百倍”，直接承诺收益的项目往往是骗局。还有很多和区块链并无太大关系的“空气币”，仅以集资为目的。

如果白皮书中根本就没有讲到区块链的必要性，或者理由不够充分、没有落地应用场景，都是讲一些大而空、理想主义的东西，那么这种项目往往是骗局。

而判断一个人是否在操作骗局，很简单的判断方式，就是这个人是不是一直在不断募资，而没有什么实际成功案例。以及如果一个项目历程无从查证，这种项目往往是骗局，或者传销。

* 链得得曾做过全球五大地区数字货币诈骗项目拆解，下载链得得 App， 参考详文：

《【链得得 3·15 重磅起底】深度拆解全球五大地区数字货币诈骗项目》

99.如何识别一个区块链项目是否为传销币?

1） 发行方式

数字货币依据特定算法，通过大量的计算产生，是去中心化的发行方式。每个不同的终端节点负责维护同一个账本，而这个维护过程主要是算法对交易信息进行打包和加密。

而传销币则主要由某个机构发行，传销头目在国内或国外注册成立空壳公司并设立网站，通过微信、讲座等形式大力度宣传某种“虚拟货币”的价值，以多至百倍收益的“高额返利”为噱头、不断吸纳会员会费达到敛财目的。

2) 交易方式

数字货币是市场自发形成的零散交易，形成规模后逐渐由第三方建立交易所来完成交易。而传销币则受到机构或个人控盘，无法自由交易。此类平台发行的假虚拟货币往往无法在交易所交易，因此多采用场外交易或自有交易所交易，同时价格被机构或个人高度控制。

3) 实现方式

虚拟货币本身是开源程序，在 Github 社区维护。其总量限制的参数和方式，均显示在开源代码中。

而传销币的开源是完全抄袭别人的开源代码，且未使用开源代码来搭建程序，无法产生区块或在区块上运行，因此多采用人为拆分的方式进行代币奖励，通过在短期内不断拆分，产生大量积分或代币，造成财富“暴涨”的错觉。

4) 是否给出源代码链接

去中心化数字货币都会在官网的显要位置给出源代码的链接，这样做是为了公开透明地展示货币系统的运作机制。而传销币重点宣传的是充值购买交易流程，并不提及其运作机制，甚至网站都没有源代码的链接地址。

5) 官网是否是 https 开头

一般的去中心化数字货币的官网和交易网站地址都以 https 开头，其目的是这类网址可以很好地保护用户的数据不被非法窃取。但传销货币的官网、交易网站等在内的相关网站都没有以 https 开头。

*链得得曾经做过一个完整的传销币拆解，具体详情可下载链得得 App， 参考详文：

《【重磅起底】2018 上半年 100 大传销币清单》
《【链得得 3 · 15 重磅起底】2018 下半年 100 大传销币实录清单》

100.如果我将加密币打错地址了，或者被骗被盗了，还能否找回，有哪些保护自己合法权益的法律渠道?

币地址是可以自我校验的，本身就有合法地址和错误地址之分。但如果打错合法地址往往是无法找回的。

目前国家未认可“虚拟货币”的货币属性，禁止其作为货币进行流通使用等金融活动，但并未否认虚拟货币可以作为一般法律意义上的财产受到法律的平等保护。据过往判例来看，目前我国的司法对于人民认可的财产都予以认可、尊重和保护，不论是房屋，汽车等有形资产，还是数字货币等虚拟资产。具体适用的法律条款则按照案件具体情况而定。

---链得得介绍---

链得得作为一家面向全球、专注区块链的媒体、数据和金融服务平台，目前在北京、东京、纽约、旧金山、香港拥有分支，其核心产品包括中文产品：链得得 App 和网站、一站式聚合加密交易工具 ChainDDX；英文产品：ChainDD App（含加密钱包）和网站。同时还运营了链得得指数科技公司、加密投资基金 DDVC、链得得国际创新学院、CHAINSIGHTS 全球峰会及其他多种行业知名活动。

链得得于 2018 年 9 月成立了美国纽约本土公司 ChainDD Inc.，通过 ChainDD PC 英文版和 ChainDD App（含钱包）向北美和其他地区的英语用户提供区块链和数字货币市场的相关资讯、数据和金融服务。由前美银美林、美国银行董事总经理 Catherine Li 担任创始合伙人 &COO。由美国哥伦比亚大学商学院 SIPA 前院长 Robin Lewis 担任高级顾问。

在内容端，链得得 App 注册用户总数达 300 万+，社区活跃用户为 28 万+人。迄今共发布文章 12000+篇，其中独家原创文章 6000+篇，独家深度调查 400+篇，数据研究报告 260+篇，2018 年全年页面浏览量为 1.3 亿+；全面且实时无缝覆盖全球各大市场区块链技术、商业和应用市场，以及数字货币交易市场与各国监管政策动态。链得得原创内容开放平台“得得号”，自 2018 年 5 月 10 日上线以来，“得得号”入驻作者已突破 1800+人，优质文章 5000+篇，累计曝光 1 亿+。

链得得(ChainDD)官方主页：www.chaindd.com

微信公众号：链得得(ChainDD)

新浪微博：@链得得 App

联系我们：support@chaindd.com

商务合作：bd@chaindd.com

扫描二维码关注链得得

Beijing ChainDD Tech Co., Ltd.