1 什么是区块链？区块链与云计算、物联网技术相比，有什么特点和不同？

区块链本质上是一个去中心化的分布式账本数据库，其本身是一串使用密码学相关联所产生的数据块，每一个数据块中包含了多次比特币网络交易有效确认的信息。分为公有链、私有链以及联盟链。

去中心化

由于使用分布式核算和存储，不存在中心化的硬件或管理机构，任意节点的权利和义务都是均等的，系统中的数据块由整个系统中具有维护功能的节点来共同维护。任一节点停止工作都会不影响系统整体的运作。

去信任

与云计算与物联网相比，区块链系统中所有节点之间无需信任也可以进行交易，因为数据库和整个系统的运作是公开透明的，在系统的规则和时间范围内，节点之间无法欺骗彼此。

开放性

相比于物联网，系统是开放的，除了交易各方的私有信息被加密外，区块链的数据对所有人公开，任何人都可以通过公开的接口查询区块链数据和开发相关应用，因此整个系统信息高度透明。

自治性

区块链采用基于协商一致的规范和协议，使得整个系统中的所有节点能够在去信任的环境自由安全的交换数据，使得对“人”的信任改成了对机器的信任，任何人为的干预不起作用。

信息不可篡改

相对于物联网和云计算，区块链的信息具有不可篡改的性质，一旦信息经过验证并添加至区块链，就会永久的存储起来，除非能够同时控制住系统中超过 51% 的节点，否则单个节点上对数据库的修改是无效的，因此区块链的数据稳定性和可靠性极高。

匿名性

相对于物联网和云计算，区块链的信息具有匿名的性质，由于节点之间的交换遵循固定的算法，其数据交互是无需信任的(区块链中的程序规则会自行判断活动是否有效)，因此交易对手无须通过公开身份的方式让对方自己产生信任，对信用的累积非常有帮助。

区块链与云计算联系

区块链技术的开发、研究与测试工作涉及多个系统，时间与资金成本等问题将阻碍区块链技术的突破，基于区块链技术的软件开发依然是一个高门槛的工作。云计算服务具有资源弹性伸缩、快速调整、低成本、高可靠性的特质，能够帮助中小企业快速低成本地进行区块链开发部署。两项技术融合，将加速区块链技术

成熟，推动区块链从金融业向更多领域拓展。

区块链与物联网联系

物联网作为互联网基础上延伸和扩展的网络，通过应用智能感知、识别技术与普适计算等计算机技术，实现信息交换和通信，同样能满足区块链系统的部署和运营要求。另外，区块链系统网络是典型的 P2P 网络，具有分布式异构特征，而物联网天然具备分布式特征，网中的每一个设备都能管理自己在交互作用中的角色、行为和规则，对建立区块链系统的共识机制具有重要的支持作用。

2 共识机制主要有哪些？他们之间的区别和联系是什么？

什么是区块链共识：

所谓区块链共识过程，是指如何将全网交易数据客观记录并且不可篡改的过程。

分布式共识问题，简单说，就是在一个或多个节点提议了一个值应当是什么后，使系统中所有节点对这个值达成一致意见。这样的协定问题在分布式系统中很常用，比如说选主（Leader election）问题中所有节点对 Leader 达成一致；原子组播（Atomic broadcast）中节点对消息传递（delivery）顺序达成一致。对于这些问题有一些特定的算法，但是，分布式共识问题试图探讨这些问题的一个更一般的形式，如果能够解决分布式共识问题，则以上的问题都可以得以解决。

为了达到共识，每个节点都提出自己的提议(propose)，最终通过共识算法，所有正确运行的节点决定（decide）相同的值。

共识算法的正确性要求是在运行中满足以下条件：

- 终止性（Liveness）：所有正确节点最后都能完成决定。
- 协定性（Safety）：所有正确节点决定相同的值。
- 完整性（Integrity）：如果正确的节点都提议同一个值，那么所有正确节点最终决定该值。

POW：Proof of Work，工作证明。

依赖机器进行数学运算来获取记账权，资源消耗大，共识机制高科监管性弱，同时每次达成共识需要全网共同参与运算，性能效率比较低，容错性方面允许全网 50%节点出错。好处是 pow 完全去中心化，节点自由进出，有分叉。

POS：Proof of Stake，股权证明。

POS：也称股权证明，类似于财产储存在银行，这种模式会根据你持有数字货币的量和时间，分配给你相应的利息。

DPOS：Delegated Proof of Stake，委任权益证明

比特股的 DPoS 机制，中文名叫做股份授权证明机制（又称受托人机制），作为 pos 的变形，继承了 pos 的优点并且通过缩小选举节点的数量以减小网络压力，是一种典型的分治策略。将所有节点分为领导者与跟随者，只有领导者之间达成共识后才会通知跟随者。该机制能够在不增加计算资源的前提下有效减少网

络压力

PBFT：Practical Byzantine Fault Tolerance，实用拜占庭容错算法。

PBFT 是一种状态机副本复制算法，即服务作为状态机进行建模，状态机在分布式系统的不同节点进行副本复制。每个状态机的副本都保存了服务的状态，同时也实现了服务的操作。将所有的副本组成的集合使用大写字母 R 表示，使用 0 到|R|-1 的整数表示每一个副本。为了描述方便，假设|R|=3f+1，这里 f 是有可能失效的副本的最大个数。尽管可以存在多于 3f+1 个副本，但是额外的副本除了降低性能之外不能提高可靠性。

Rcp：使一组节点能够基于特殊节点列表达成共识。初始特殊节点列表就像一个俱乐部，要接纳一个新成员，必须由一定比例的该俱乐部会员投票通过。Ripple 的共识算法中，参与投票节点的身份是事先知道的，因此，算法的效率比 PoW 等匿名共识算法要高效，交易的确认时间只需几秒钟。当然，这点也决定了该共识算法只适合于权限链（Permissioned chain）的场景。

共识算法联系与区别。

从时间上来看，这个顺序也是按该共识算法从诞生到热门的顺序来定。

对于 POW，直接让比特币成为了现实，并投入使用。而 POS 的存在主要是从经济学上的考虑和创新。因此后来又出现 DPOS，这种不需要消耗太多额外的算力来进行矿池产出物的分配权益方式。但要说能起到替代作用，DPOS 来单独替代 POW，POS 或者 POW＋POS 也不太可能，毕竟存在即合理。每种算法都在特定的时间段中有各自的考虑和意义，无论是技术上，还是业务上。

3 比特币特点有哪些？

比特币是一种开源的、基于网络的、点对点的匿名电子货币，由中本聪于 2008 年设计开发，是世界上第一个分布式的匿名数字货币。

- **去中心化**,整个网络由用户构成，没有中央银行。
- **全世界流通**、无国界：比特币可以在任意一台接入互联网的电脑上管理。不管身处何方，任何人都可以挖掘、购买、出售或收取比特币。
- **专属所有权**：操控比特币需要私有密钥，除了用户自己之外无人可以获取。
- **交易便捷**：免监管、无隐藏成本，用比特币交易，知道对方比特币地址就可以进行支付，无额度和手续限制，不经过任何管控机构，也不会留下任何交易记录。
- **匿名性**，购买后存储账户完全匿名，无人知晓。
- **价格波动大**：大量炒家介入，导致比特币兑换现金价格波动大。
- **存着灰色领域**，可能被用来从事非法活动。
- **交易平台的脆弱性**，交易平台通常是带有交易功能的网站，会遭到黑客

攻击，比特币并不依赖于任何金融机构运行，用户需要对自己的资金安全负上全部责任。

4 比特币是如何应用到区块链技术的？

（答出:需要回答出一个区块里有哪些信息,即区块的数据结构,说明每一个信息表示什么,块和块如何组成链）

区块是一种记录交易的数据结构。每个区块由区块头和区块主体组成，区块主体只负责记录前一段时间内的所有交易信息，区块链的大部分功能都由区块头实现。

区块头的结构：

版本号，标示软件及协议的相关版本信息

父区块哈希值，引用的区块链中父区块头的哈希值，通过这个值每个区块才首尾相连组成了区块链，并且这个值对区块链的安全性起到了至关重要的作用

Merkle 根，这个值是由区块主体中所有交易的哈希值再逐级两两哈希计算出来的一个数值，主要用于检验一笔交易是否在这个区块中存在

时间戳，记录该区块产生的时间，精确到秒

难度值，该区块相关数学题的难度目标

随机数(Nonce)，记录解密该区块相关数学题的答案的值

区块体：

包含该区块中所有交易信息以及所有交易信息的 Merkle 树。

块和块如何组成链？

从创世区块开始，每一个后续区块将记录前一个区块的哈希，以此方式形成一个后向追溯的链条

结构上

比特币区块链的一个区块不能超过 1 MB，将主要包括如下内容：

- 区块大小：4 字节；
- 区块头：80 字节：
- 交易个数计数器：1~9 字节；
- 所有交易的具体内容，可变长，匹配 Merkle 树叶子节点顺序。

其中，**区块头信息**十分重要，包括：

- 版本号：4 字节；
- 上一个区块头的 Hash 值：链接到上一个合法的块上，对其区块头进行两次 SHA256 操作，32 字节；
- 本区块所包含的所有交易的 Merkle 树根的哈希值：两次 SHA256 操作，32 字节；
- 时间戳：4 字节；
- 难度指标：4 字节；
- Nonce：4 字节，PoW 问题的答案。

可见，要对区块链的完整性进行检查，只需要检验各个区块头部信息即可，

无需获取到具体的交易内容，这也是简单交易验证（Simple Payment Verification，SPV） 的基本原理。另外，通过头部的链接，提供时序关系的同时加大了对区块中数据进行篡改的难度。

比特币的三个核心范畴即数字签名技术、哈希技术、博弈论与区块链的特性相结合，解决比特币系统中去中心化存储、货币发行、货币交易三个问题。

去中心化存储

通过 P2P 协议进行节点之间的数据传输，无需中心节点，任意两个节点之间能够实现彼此的信息传递，在这个协议的基础上，任何节点都可以随时加入或离开比特币网络集群，而不会对比特币网络集群产生影响，即便出现故障机器未能及时修复，也不会影响整个系统的运行。

如果想要破坏比特币系统，就必须同时篡改整个网络一半以上的数据，这还有可能做到的，但是成本太高。这就涉及到比特币的三个核心范畴之一的“博弈论”，区块链技术采用了一种社会学博弈的激励措施，形成了一种典型的负反馈效应，即完全信息静态博弈中的平衡机制“纳什均衡”，利用其稳定状态保证了比特币系统的参与者不会单独改变策略，也就是说没有节点可以通过不诚实的行为获得更高的回报。最终让作恶变得成本高昂。从而达到维护比特币网络集群不被轻易破坏的目的。

哈希技术

我们知道区块链是由若干区块链接而成，而数据区块由区块头和区块体两部分组成：区块链在交易存储上是采用 Merkle 树结构，并且每笔交易都会生成一个 hash 值，然后不同的 hash 值向上继续做 hash 运算，最终生成唯一的 Merkle 根。随即把这个 Merkle 根放入数据区块的区块头。利用 Merkle 树和哈希算法，以确保每一比交易都不可伪造和没有重复交易。这里涉及到比特币的第二个核心范畴“哈希技术”，哈希算法是区块链中保证交易信息不可篡改的单向密码机制，将信息压缩成散列字符串，计算得到哈希值标识每个区块，以此构建区块链全局公共账本，使既有交易不可抵赖，离线破坏交易难。

在 Merkle 树和哈希算法的基础上，还涉及到比特币的最后一个核心范畴“数字签名技术” 即依靠公钥加密技术，实现信息加密和解密两个过程。发送者用自己的私钥对信息进行加密后传送给接收者，接收者只有用发送者的公钥才能解密被加密的信息，整个过程利用离散对数难题(针对 ECC 算法而言)进行保护，因此每一次交易都难以遭到在线破坏。

比特币通过区块链技术解决比特币系统中去中心化存储、货币发行、货币交易三个问题。简单来说比特币是用区块链技术来管理他的账单的。

具体来说实现去中心化的解决办法就是采用分布式系统，把原先存储在某个第三方机构的信息数据，分布存储在一个 P2P 的网络结构中，同时借助区块链技术实现数据的不可篡改、达到最终一致性。如果想要破坏比特币系统，就必须同时篡改整个网络一半以上的数据，这还有可能做到的，但是成本太高。区块链技术采用了一种社会学博弈的激励措施，形成了一种典型的负反馈效应，即完全信息静态博弈中的平衡机制“纳什均衡”，利用其稳定状态保证了比特币系统的参与者不会单独改变策略，也就是说没有节点可以通过不诚实的行为获得更高的回报。最终让作恶变得成本高昂。从而达到维护比特币网络集群不被轻易破坏的目的。

5 比特币如何解决重复支出

如果同一笔钱（数字货币）被重复支付两次，就是双重支付问题，解决这个问题就相当于数字货币的防伪技术。这个问题在物理货币世界并不存在，因为你无法复制黄金。在纸币中，由于纸币由造币厂发行的，设计有复杂的防伪技术，如果有人制造了假币，可以通过法律来制止这些行为。但在数字货币中，比特币会对前一次的交易和下一位拥有者的公钥签署一个数字签名，将这个签名附加在比特币的末尾发送给下一位所有者。而由于没有第三方机构去做监控，所以需要一个机制去确保比特币之前的所有者没有对更早发生的交易实施签名。比特币是怎样解决这个问题的呢：

1、 **所有的交易全网公开**：历史交易全网公开，那么每个账号里面有多少比特币，并不是由一个数据来表示的，而是根据历史交易得出来的。而这个历史交易链是经过全网公认的，才能保证不被造假。

2、 **需要有时间戳**，所有交易有先后顺序：所有交易，要按照先后顺序，给其加上时间戳，前面一笔交易成功后，整个交易链被公认后，下一笔交易是基于上一笔交易来生成的，整个交易就是一个交易链，这样才能保证不被双重支付。

3、 **需要投入计算资源对交易进行确认**：交易的确认，需要投入计算资源来确认，比特币引入了工作量证明，矿工投入计算力来打包交易，若需修改某个区块上的交易，需重新计算自区块以来所有区块，参考比特币网络目前的算力，这在数学上几乎是不可能的。

整个比特币系统中的每一个节点都获知每一笔交易的发生，且它们是有时间顺序的，有一个公认的交易序列。那么，只有当大部分节点都认同这笔交易是首次出现时，这笔交易才能发生。唯一可能造成这个系统崩溃的是，有一个人拥有超过整个系统 51%的计算能力，那么他就能随意更改每笔交易记录，这就是所谓的“51%攻击”，但这几乎是无法实现的。

6　超级账本是什么？有哪些特点

超级账本（Hyperledger）项目是全球最大的开源企业级分布式账本平台。超级账本项目致力为透明、公开、去中心化的企业级分布式账本技术提供开源参考实现，并推动区块链和分布式账本相关协议、规范和标准的发展。“利用块链式数据结构来验证与存储数据”“利用密码学的方式保证数据传输和访问的安全”

特点：

1 超级账本的核心是通过成员合作的方式来进行的，没有单一方能够进行决策
2 超级账本本身是一个项目集合(与 Apache 相似)，将最终变得可以被整合和重复使用
3 人人记账，每个人均有机会参与记账过程
4 难以篡改，因为是是区块链的应用，继承其特性
5 去中心化。相比传统方式，区块链可以实现某个体系在没有中心机构管理的情况下自动运行

7　如何利用超级账本的特点提升实际的业务性能

将超级账本应用于对部分或者所有的记录信息需要或者有潜在需求的实际业务中，，以其反篡改的特性对数据的安全性有很重要考虑的业务，例如打击假冒药品，提升这些业务的性能

超级账本是对传统区块链模型的革新，通过提供针对身份识别、可审计和隐私的安全和健壮模型，在某种程度上是允许创建授权的和非授权的区块链，使得缩短计算周期、提高规模效率和响应各个行业的应用需求成为可能。
同时超级账本项目的目标是为商业区块链应用提供底层支持，在知识产权上采用了商业友好的使用许可。所有项目中的代码都要使用 Apache V2.0 的许可协议，这是非常宽泛的许可协议，可以满足绝大部分商业应用的需求。项目的文档遵循知识共享 4.0 国际许可协议，适合商业和非商业用途。
案例 1：金融资产处置
诸如证券这样的金融资产必须能在区块链网络上实现去中心化，这样所有同种资产的利益相关方就能直接访问这一资产，进而发起交易，获取相关信息而不需要通过层层中间环节来进行了。交易可以在利益相关者之间商定的时间期限内解决，交易可以实现实时结算，利益相关者都可以实时掌握资产情况。对于任何种类的资产，利益相关方应该有权增加商务规则，这样也能通过自动化逻辑的应用来降低成本。创建资产的人必须像用例保证的那样，实现资产和相关交易规则保密或者公开。
案例 2：供应链
区块链的框架必须满足供应链中每一位参与者的如下需求：录入并追踪原材料的来源；记录部件生产的遥测数据；追踪航运商品的出处；保证包括成品生产、储存、销售及后续事宜在内的所有数据都不被篡改。除了之前描述的商务合约和资产存管模式的特征，供应链这一用例更多强调的是其深度可搜索性，保证能够在过去的层层交易中追溯所需记录。其核心是为每一个基于其它部件构成的商品创建出处（可追溯的源）。

8　什么是分叉？有哪些分叉的实验法？他们的区别是什么？

分叉 指 区块链中某一个新的区块被挖出之后，区块链系统会产生新的协议，而这个协议又与旧协议难以兼容。
分为软分叉和硬分叉。
硬分叉就是指，新协议将不再允许旧协议继续工作。就像以太坊，为了拿回资金才更改了协议，所以发生了硬分叉，
注意：以上情况基于新节点算力>50%

软分叉是指：当系统中出现了新版本的软件（或称协议），并且和前版本软件不能兼容，新节点无法接受老节点挖出的全部或部分区块（认为不合法）。因为新节点算力较大，老节点挖出的区块将没有机会得到认可，新老双方从始至终都工作在同一条链上，这称为软分叉。
注意：以上情况基于新节点算力>50%

区别：
硬分叉之后，几乎一定会产生让老节点拒绝接受的区块，所以，硬分叉会破坏前向兼容性；
软分叉之后，产生的新区块肯定是老节点也愿意接受的，前向兼容性得以保留

9　智能合约 batchTransfer 函数

BEC 在合约中加入一个批量转账的函数，它的实现如下：

```
function batchTransfer(address[] _receivers, uint256 _value) public whenNotPaused returns (bool) {
    uint cnt = _receivers.length;
    uint256 amount = uint256(cnt) * _value;
    require(cnt > 0 && cnt <= 20);
    require(_value > 0 && balances[msg.sender] >= amount);

    balances[msg.sender] = balances[msg.sender].sub(amount);
    for (uint i = 0; i < cnt; i++) {
        balances[_receivers[i]] = balances[_receivers[i]].add(_value);
        Transfer(msg.sender, _receivers[i], _value);
    }
    return true;
```

这个函数的作用是，调用者传入若干个地址和转账金额，在经过一些条件检查之

后，对 msg.sender 的余额进行减操作，对每一个对每一个传入的地址进行加操作，以实现 BEC 的转移。
问题出在 uint256 amount = uint256(cnt) * _value; 这句代码，当传入值 _value 过大时（接近 uint256 的取值范围的最大值），uint256 amount = uint256(cnt) * _value 计算时会发生溢出，导致 amount 实际的值是一个非常小的数（此时 amount 不再是 cnt * _value 的实际值），amount 很小，也使得后面对调用者余额校验可正常通过（即 require(_value > 0 && balances[msg.sender] >= amount)语句通过）。

10 区块链有哪些优势？能应用在哪些地方？

优势：
去中心化：任一节点的损坏或者失去都不会影响整个系统的运作。
可靠性和不可篡改性：通过数字签名和共识协议等技术保证了形成数据的真实性。破坏区块链系统需要攻击 51%以上的节点。
去信任性：参与整个系统中的每个节点之间进行数据交换是无需互相信任的，因为每个节点都有这个网络的所有数据。
集体维护：系统中的数据块由整个系统中所有具有维护功能的节点来共同维护，而这些具有维护功能的节点是分布式的，任何人都可以参与
完全透明：整个系统的运作规则（算法）、数据（账本）都是公开透明的，可即时审计的

应用场景：
金融交易系统已经开始验证和使用区块链系统。包括征信管理、跨国交易、跨组织合作、资源共享和物联网等诸多领域。
金融服务：区块链带来的潜在优势包括降低交易成本、减少跨组织交易风险等。该领域的区块链应用目前最受关注，全球不少银行和金融交易机构都是主力推动者。部分投资机构也在应用区块链技术降低管理成本和管控风险。从另一方面，要注意可能引发的问题和风险。例如，DAO（Decentralized Autonomous Organization 是史上最大的一次众筹活动，基于区块链技术确保资金的管理和投放）这样的众筹实验，提醒应用者在业务和运营层面都要谨慎处理。

征信和权属管理：征信和权属的数字化管理是大型社交平台和保险公司都梦寐以求的。目前该领域的主要技术问题包括缺乏足够的数据和分析能力；缺乏可靠的平台支持以及有效的数据整合管理等。区块链被认为可以促进数据交易和流动，提供安全可靠的支持。征信行业的门槛比较高，需要多方资源共同推动。

资源共享：以 Airbnb 为代表的分享经济公司将欢迎去中心化应用，可以降低管理成本。该领域主题相对集中，设计空间大，受到大量的投资关注。

贸易管理：区块链技术可以帮助自动化国际贸易和物流供应链领域中繁琐的手续和流程。基于区块链设计的贸易管理方案会为参与的多方企业带来极大的便利。另外，贸易中销售和法律合同的数字化、货物监控与检测、实时支付等方向都可能成为创业公司的突破口。

物联网：物联网也是很适合应用区块链技术的一个领域，预计未来几年内会有大量应用出现，特别是租赁、物流等特定场景，都是很合适结合区块链技术的场景。但目前阶段，物联网自身的技术局限将造成短期内不会出现大规模应用。