1. **两种软件系统架构**

实现一个软件系统，首先需要决定的是该系统的各模块之间如何相互关联，即确定它的基础架构，就架构而言可以分为两种：中心化架构和去中心化架构。

1. **去中心化系统的优势**

* 更强的计算能力

一个去中心化系统的计算能力表现为系统中所有计算机计算性能之和

* 更低的成本
* 更高的可靠性

即使一个节点宕机也不会对整个系统产生影响

* 自增长的能力(扩展性)

可以通过增加节点来提高系统的计算能力

1. **去中心化系统的劣势**

* 节点之间的协调

系统的协作需要每个成员节点自己完成，需要耗费额外的计算资源

* 节点间的冗余通信
* 对网络过度依赖
* 系统的编程实现难度高
* 安全问题

系统对成员节点使用网络的权限限制越大，去中心化系统越安全可靠

1. **混合系统**

两种混合系统架构：拥有中心节点的去中心化系统，去中心化系统作为中心节点的中心化系统。

如何识别一个去中心化系统？

答：如果存在一个单独的中心节点，比如其有一个单独的关闭按钮可以切断整个系统，那么这个系统就不是去中心化系统

1. **区块链的作用**

区块链是去中心化系统中用来实现并确保系统完备性的工具。

1. **点对点系统的定义**

点对点系统是由若干节点(个人PC)组成的分布式软件系统，系统中的单一节点的计算资源(CPU的处理能力、存储容量等)可直接被其他节点调用。当加入点对点系统时，用户按照其权限将其转换为系统的节点。尽管用户对系统的贡献的资源可能有所不同，但系统的所有节点具有相同的功能和责任。

在一个点对点文件共享系统中，各文件存储于各用户的计算机上。当有人想在这样的系统中下载文件时，可以直接从另一个人的计算机上下载即可。

1. **点对点系统的优势**

允许成员不通过中间人直接进行交互，能够加快信息的处理速度，降低成本。随着数字化的发展，越来越多的虚拟化产品和服务将受益于点对点系统的效率提升。

1. **点对点系统架构**

点对点系统有两种架构：完全去中心化的系统架构、混合式的拥有中心节点的去中心化系统架构。前者没有任何中央节点进行控制协调，系统中所有的节点都执行相同的任务，既是资源和服务的提供者，也是消费者；后者通过维护一个中心节点促进系统成员之间的交互，同时维护不同节点提供的服务目录，或者是执行节点的查找和标识任务。

1. **点对点系统和区块链间的关系**

区块链可被认为是实现和维护分布式系统完备性的工具，完全分布式的点对点系统可以使用区块链技术来实现和维护系统的完备性。

1. **点对点系统中的信任与完备性**

在一个点对点系统中，人们如果相信这个点对点系统，并且这个点对点系统运行的结果增强了他们的信任，他们就会进一步进入这个系统，并且持续给这个系统做出贡献。为了实现用户对系统的信任，核心的问题就是：我们如何在一个完全去中心的点对点系统中提供并确保完备性？

满足并确保一个完全去中心化系统的完备性，需要具备很多条件，其中最重要的有两点：

* 了解系统中的节点数目
* 了解节点的可信任程度

1. **点对点系统中的完备性威胁**

主要的两点：技术性故障和恶意节点。

* 技术性故障

点对点系统时网络中相互连接的独立计算机组成的，任何一台计算机的任意硬件(或核心软件)，或这个系统所依赖的网络都有发生故障的奉献。

* 恶意节点

不可信节点和恶意节点构成了点对点系统面临的最大威胁，因为他们破坏了这个系统的存在基石：信任。一旦用户无法信任他们的连接方，他们就不会信任这个系统，并转而离开。

1. **区块链解决以上核心问题**

通过使用区块链技术，即使是在一个不知道内部节点数目，也不知道各节点可信度的点对点系统中，也可以实现并确保整个系统的完备性。在计算机科学领域，这是一个由来已久的问题：拜占庭将军问题。

1. **区块链的定义：一种数据结构**

当区块链作为一种数据结构被使用时，其指代将数据整合进入一个个“区块”中。可以把“区块”这个概念成为一本书当中的一页，而一个个区块相互之间连接起来像一个链条一般，因此成为区块链。

在区块链中，数据形成的链状数据结构是通过一个特殊的编码系统来实现的，这个编码系统与一本书当中的页码的编写方法类似，但要更复杂一些。

1. **区块链的定义：一种算法**

当我们把“区块链”作为一种算法考虑时，指的是在一个完全去中心化的点对点系统中，将大量特定数据结构的数据妥善协调组织在一起的算法，类似于一种完美的民主投票方法。

1. **区块链的定义：一个完整的技术方案**

当我们把“区块链”作为一个完整的技术方案提出时，“区块链”指的是将区块链数据结构、区块链算法、密码学以及安全技术综合在一起，来确保完全去中心化点对点系统完备性的一个完整技术方案。

1. **区块链的定义：在普通应用场景下完全去中心化点对点系统的一个概括性术语**

“区块链”可以被看作利用区块链技术方案实现完全去中心化点对点分布式账本系统的方法。在这种情况下，“区块链”指的是一个完全的去中心化系统，而不是一个完整去中心化系统的一部分。

1. **总结**

一般情况下，我们会使用对区块链的第四种定义，即是将“区块链”看作一个利用区块链技术方案，实现完全去中心化点对点分布式账本系统的方法。对于其他三种术语，我们一般会直接使用“区块链数据结构”、“区块链算法”、“区块链技术方案”等表述方式。

总结下来，可以将区块链定义为：区块链是一个完全分布式的点对点账本系统，其利用一个特殊的算法，实现对区块内信息生成顺序的协调，并使用加密技术对区块数据进行连接，从而确保了系统的完备性。

1. **所有权的证明**

所有权的证明一般需要以下3个要素：

* 对所有者的证明
* 对事物被拥有的证明
* 提供一个所有者和事物之间的连接

因此所有权的证明需要对所有者和财产的鉴定，以及明确二者之间的所属关系。所有者与被所有事物之间的关联会象征性地通过一个账本进行记录，这个账本会记录每一次所有权的变更，一个过期的账本会失去证实所有权的公信力。

1. **三个与安全相关的概念**

这三个概念分别是：身份认证、鉴定、授权

* 身份认证

身份认证是指通过提供可以作为标识符的相关信息来确认使用者的身份，比如身份证。但是仅仅持有身份证无法证明你确实就是身份证上的这个人，身份认证只是意味着申明你是某一个人。

* 鉴定

鉴定的目的就是为了防止有人冒充他人，即使说要核实你的确是你所声明的这个人，比如说核对身份证上的照片。

* 授权

授权意味着根据对应人的身份特征准许其访问特定资源或使用特定服务。授权的进行意味着一次鉴定的成功，授权的完成意味着对其所拥有的权利的准确评估的完成。授权通常是身份认证和鉴定之后的步骤。

* 总结

身份认证指的是确认使用者的身份；鉴定指的是证明你确实是你所声称的这个人；授权指的是让你根据之前的身份鉴定能访问特定的资源或得到特定的服务。

1. **账本的性质和意义**

一个账本必须同时履行两种相对的功能。一方面能够通过读取账本中的数据证明所有权，另一方面账本需要能够写入记录每一次所有权的转移。

当账本对所有人开放时，证明所有权是很容易的。因此公开是证明所属权的基础；但是所属权的转让应该专门限定开放给合法的转让对象。因此隐私是所有权变更的基础。

向账本写入数据意味着更改所有权，因此我们希望绝对可信的实体才能够具有对账本进行数据写入的权限。

区块链是一个能够被任何人访问，拥有类似账本功能的巨大去中心化点对点系统，简单理解为一个去中心化的账本。

1. **所有权与区块链**

作为证明文件的账本保存的信息存在被破坏和篡改的风险，也或者是因为更新速度不够快，导致证明信息无法发应真实情况。

因此我们必须抛弃只拥有一个账本的想法，而是应该构建一个完全去中心化的账本系统，而且在这个系统中所有权的证明需要通过绝大多数的节点的同意才能完成。

通过账本和区块链来进行所有权管理之间的联系可以总结为以下5点：

* 单个账本可以用来记录与所有权相关的信息，可以看做一份区块链中存储于所有权相关数据的账本。
* 单个账本存储在一个点对点系统的节点上。
* 区块链算法确保了单个节点在每一次投票之后，能够同步到一个相同的状态
* 系统的完备性是系统具备提供真实且正确所有权描述的关键
* 在身份认证、鉴定、授权以及确保数据安全性时，必须采用密码学知识

**双花问题**

1. **双花问题的含义**

在一个点对点系统中，每一个节点都有一份对账本的备份，一旦账本中一间房屋的所有权从一个人转移到另一个人，整个系统上的所有账本都需要进行同步，以保证更新到最新的状态。然而，在节点之间传递信息并更新各节点上的账本都需要时间，直到系统的最后一个节点收到最新的信息，并且完成对自己账本的更新之后，系统才可以达到一个稳定的状态。这就意味着有的节点会比其他的节点更早的得知最新一次所有权的转让的信息，这就给那些提前获取账本更新信息的节点留下了一个利用这一信息作恶的机会。

比如说：A将房屋买给B，从A到B的所有权变更会被记录在去中心化点对点系统的一个账本中，维护这个账本的节点需要将这条信息告知它所知道的其他所有的节点，并进一步通过这些节点将这条信息扩散出去，直到所有节点完成对这条信息的更新。但是，若在进行转让时，A迅速访问了存有另一个账本的节点，并将这条信息更改为“A将房屋买给C”，该节点就会记录这一信息并对此次转让提供证明。这一过程中，A利用去中心化系统同步信息需要时间这一漏洞将自己的房屋出售了两次，而实际上B和C中只能有一人成为房屋新的合法拥有者。

以上A的所作所为导致的问题，就称之为双花问题。

1. **双花问题的解决**