甲方，乙方之间的合作、协议。甲方作为用户、客户；乙方作为项目承揽方，开发方。首先甲方会做一个项目可行性分析报告，项目需求分析报告，招标书（少三份为废标）然后双方开始需求规格说明书（只不过时间粗略采集，客户的业务及目标），乙方决定后写下项目解决方案（投标书）双方选定进行合同拟定，接着就是需求规格说明书（用户体验，细致采集客户业务及目标），最后，确认需求，乙方开始开发。

这里分析一下需求的种类 系统需求：业务需求：组织客户对产品高层次的目标需求。

用户需求：用户使用产品必须完成的任务。

功能需求：实现系统功能，使用户完成任务，满足业务。

非功能需求：产品要遵从的标准、规范和合约及外部界面的具体情节。

除了这些，还有客户的隐性需求、性能需求、升级需求等等。

大概流程就是 系统结构设计->软件结构设计->软件模块划分与功能和性能分析->编写代码->软件模块集成->软件子系统集成->测试->最后改善，投入市场。

1.了解了区块链是什么

区块链的工作原理，分类

2.了解了区块链特点（4个重要特性）

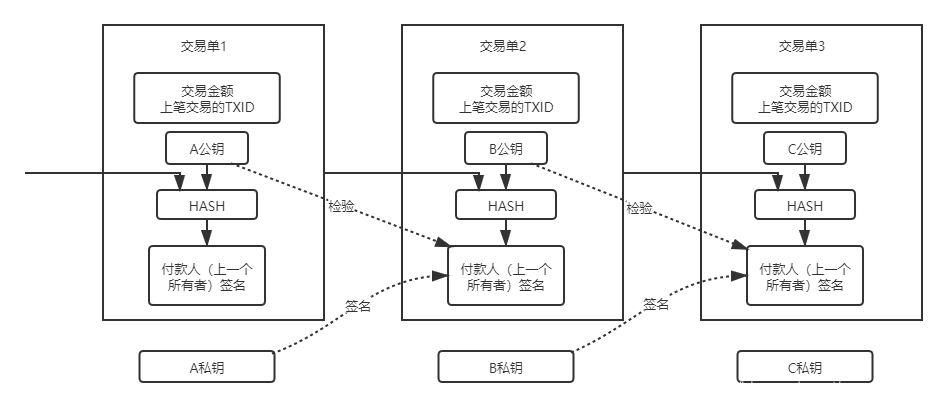
3.了解了以太坊，比特币的概念

4.了解了pow共识

区块链的工作原理

区块链中的区块根据存储内容可以划为区块头和区块体，区块头主要存储的是上一个区块的哈希值等信息，区块体主要存储的是网络内各节点的交易账本。由此相连的区块形成了区块链的链状的数据结构和存储方式。

￼



区块链的工作原理如下：

（１）客户端将发起的交易经数字签名后在网络上广播并等待确认；

（２）网络中节点对收到的数据记录信息进行校验，通过校验后数据记录被记录到一个区块中；

（３）区块链网络中的接收节点对收到区块实施特定的共识算法，区块通过共识后存储至区块链的同时生成该区块的哈希值并将其存储至下一个区块链中的区块头中。由此不断生成新的区块进而连成区块链。

区块链分类：公共链，私有链，联盟链

区块链技术平台，比特币 、 以 太坊等

比特币

比特币是最早全球使用最广泛的区块链技术，具有最去中心化、最多分布节点、最公平等特点。比特币提出了一个无需信用中介的数字货币系统，通过数字签名使得在线支付能够直接由一方发起并支付给另外一方，中间不需要通过任何的金融机构，并提出了一种通过工作量证明的机制的点对点网络来记录交易的公开信息，该网络通过随机散列对全部交易加上时间戳，将它们合并入一个不断延伸的基于随机散列的工作量证明的链条作为交易记录，形成的交易记录不可更改。每个节点都不需要明确自己的身份，可以随时离开或加入网络。比特币发展至今强有力的证明了区块链技术在数字货币领域的应用完全是有意义且有价值的，而比特币只是区块链应用的一个方向且不具有图灵完备的编程语言平台，也没有为用户提供开展宽阔的分布式账本系统应用。

以太坊

以太坊是一个通用的数字代币平台，它通过一套图灵完备的脚本语言建立应用并采用多种编程语言实现协议，通过Go语言编写的客户端作为默认客户端。以太坊的关键是智能合约，可比喻为以太坊系统里的自动代理人。存在单独的以太币地址从而实现以太坊用户之间的交易渠道，当以太坊用户进行交易是，设置好的智能合约将会被触发并且向用户返回该合约的结果。用户之间的交易除了以太币之外通常会包含一些附带的消息。开发人员可通过智能合约和易于交互的页面来开发广泛的DApp应用。

四个特性

1.不可篡改性

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。

2.唯一性

在数字世界中，最基本单元是比特，比特的根本特性是可复制。但是价值不能被复制，价值必须是唯一的。之前我们已经讨论过，这正是矛盾所在：在数字世界中，我们很难让一个文件是唯一的，至少很难普遍地做到这一点。这是现在我们需要中心化的账本来记录价值的原因。比特币系统带来的区块链技术可以说第一次把“唯一性”普遍地带入了数字世界。

3.智能合约

智能合约的出现使得基于区块链的两个人不只是可以进行简单的价值转移，而可以设定复杂的规则，由智能合约自动、自治地执行，这极大地扩展了区块链的应用可能性。

当前把焦点放在通证的创新性应用上的项目，在软件层面都是通过编写智能合约来实现的。利用智能合约，我们可以进行复杂的数字资产交易。

4.去中心自组织

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。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。

PoW共识机制

proof of work，也就是工作量证明。比特币挖矿就是pow机制。原理就是计算机通过变量（nonce）变化，不断的计算产生一串串数字，直到某一串数字满足指定的难度要求，才停止这次计算。这串数字就是新生成区块的hash

了解了区块链的基础知识后感觉区块链应用于金融方面的部分真的非常大，未来在金融方面发展空间也一定非常大，二者联系非常密切。