区块链作业三

学号：16340023

姓名：陈明亮

一、为什么要有stateRoot?

- 首先，链上的区块`Header`结构会包含大量与当前区块挂钩的相关信息。除了区块自身特殊的哈希值，`nonce`，难度值等等数值，往往每一个区块`Header`都会包含状态树根节点`stateRoot`，交易树根节点`transactionsRoot`，收据树根节点`receiptsRoot`。
- `stateRoot`是每个区块内容必须包含的字段，它是当前链上状态树的根节点`root`，存储当前该树上的保存的所有状态信息的整体数据哈希值。
- 它的作用是：方便节点之间的最新状态的相互验证，实际上保证了不论在什么时候，在交易的每个区块信息在所有节点上的存储状态完全一致。若不同节点上的交易区块存储状态信息不同步，可能会导致某一节点上主链的交易无法被验证，从而导致每个节点之间拥有不同的链状态。

二、nonce值有什么用?

- 区块内部的`nonce`值是随机生成的64位随机数，其实实际上是无实际意义的数值，只用于在工作量证明`POW`来验证是否满足条件，这个过程实际上就是挖矿工作。
- 交易内部的`nonce`值用于区分同一账户发出的不同交易的标记，有利于确认该账户发出的所有交易的交易顺序，同时也防止了双花情况的发生。双花情况：即账户在前一笔交易还没有被矿工添加进区块内部时，又产生了一个带有高`gasPrice`的交易，试图使前一个交易无效化，从而做到不断消耗某个账户的余额。
- 通过使用`nonce`值，此时第二笔交易往往只能在第一笔交易后面才被添加打包进新的区块中，因为矿工在打包交易时不能跳过`nonce`进行操作，必须按照累加一的规则来识别并打包每一个账户发起的交易。如此一来，就可以按照正常的顺序执行交易，防止双花产生。
- 同时，`nonce`值还可以用作唯一标识字段值来撤销某一账户发起的，还未确认的，位于交易池中等待`pending`的交易。此外，智能合约内部的`nonce`值可用于确定所生成合约的地址，因为`contract`内部的`nonce`也相当于是一个计数器，只在一个合约创建另外一个合约的时候才启用`nonce`值的累加，调用关系不累加`nonce`。

三、Hyperledger Fabric的特点，和Composer的关系?

- `Hyperledger Fabric`采用模块化架构，实际上相比于以太坊，它更加面向于商业应用，提供的功能基本上围绕商业逻辑，同时却不乏灵活性，提供高度的保密性、弹性、灵活性与可扩展性。它的目的是支持不同组件的可插入实现，并适应经济系统中存在的复杂性。`Fabric`针对企业，希望通过`BlockChain`技术简化公司间的流程，实际上是在解决的企业之间的信任问题。
- `Fabric`采用分层模块化思想，将架构分为三部分：`Identity`、`ChainCode`、`Ledger`。此处的Identity为身份管理模块，`Chaincode`是其智能合约的称呼，与以太坊不同的是，其底层智能合约与交易账本完全分开，采用逻辑与数据分离的烦恼方式，解决每次升级合约内容时就需要迁移账本数据的问题。同时，`ChainCode`使用容器化思想，使用`Docker`容器运行其智能合约，做到支持几乎所有高级语言编程实现智能合约。`Ledger`实现建立在HTTP/2上的P2P协议来管理分布式账本。
- `Hyperledger Composer`的目的是为了简化整个区块链应用开发过程，通过提供一些方便的接口功能，目前主要用于与`Hyperledger Fabric`对接，通过脚本语言，接收用户输入内容，打包成`.bna`文件，然后部署到相

应的`Fabric`链上。实际上两者之间的最大关系在于，`Composer`为开发者提供了简易的链上基本操作的图形化接口，实际上大大简化了开发过程。

四、联盟链智能合约 和 中心账本的区别?

- 联盟链是指其共识过程受到预选节点控制的区块链，故联盟链可以视为*部分去中心化*。而联盟链智能合约它具有事件驱动，自动执行，价值转移等特点。与中心账本对比，中心账本过于中心化，出错难以追溯，大额交易不可靠。
- 联盟链智能合约就是基于联盟链设计的计算机程序，它也不是任何人都可以使用的，由联盟链的持有者限定参加合约的用户结点，不需要任何中介结构。中心账本是记录在唯一一个中心的数据记录，具有交易风险以及可信度问题。