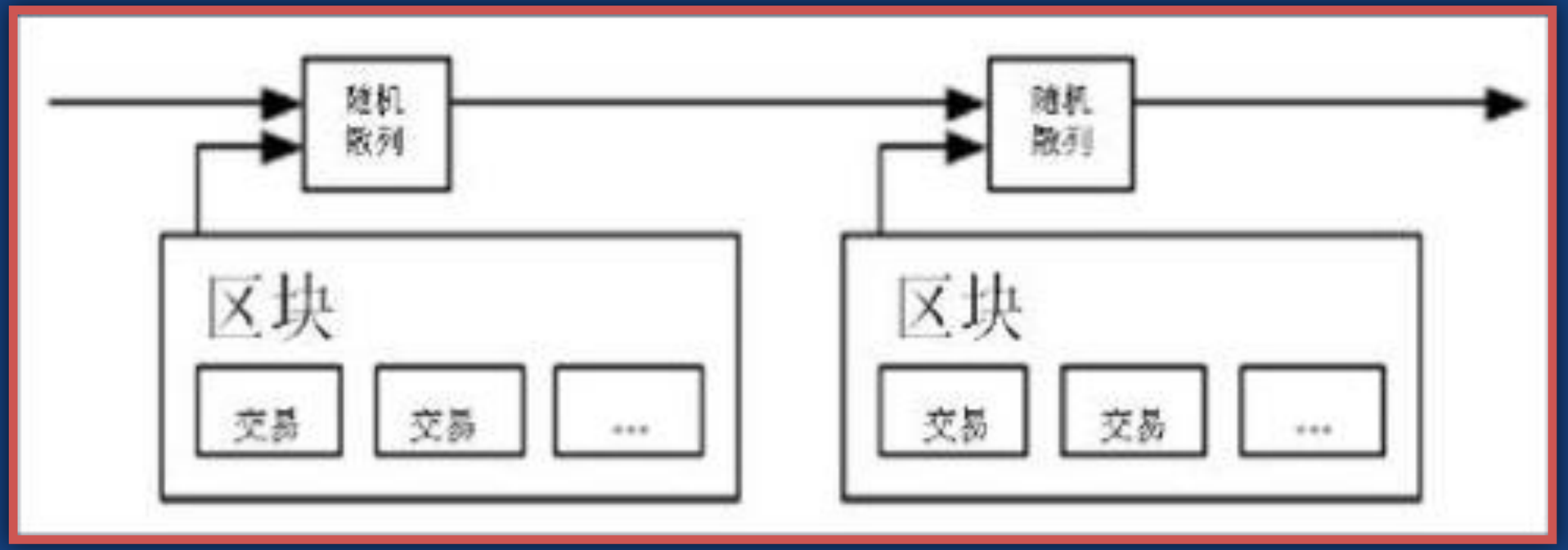
区块链技术与应用

第十四讲 分布式帐本

主讲人：赵其刚

数据层——区块链

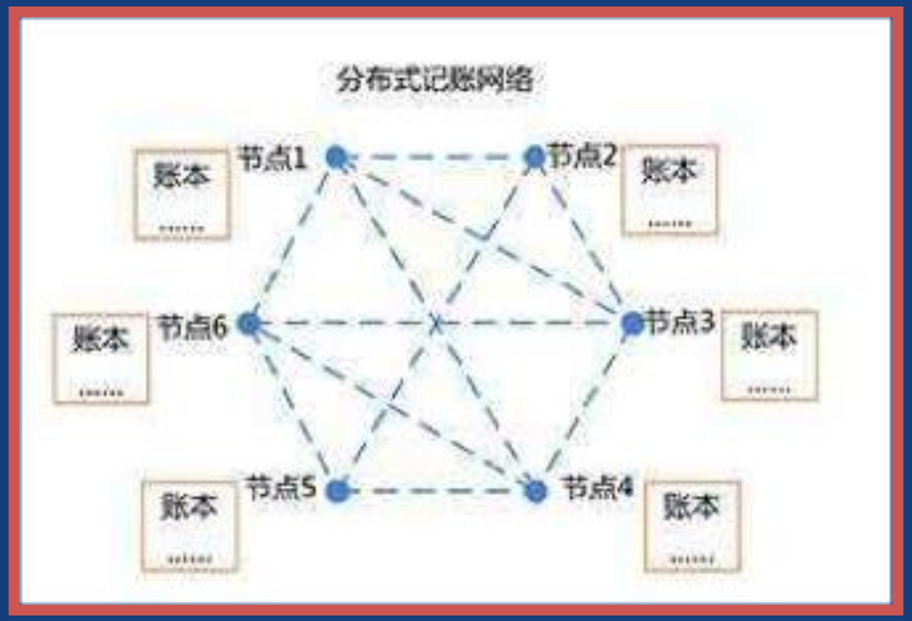
数据层是区块链技术架构的最底层或者说最基础的层，最核心的层，是整个区块链工作的“核心”。



数据层——区块链

分布式账本

- 是整个区块链网络运行的核心信息流
- 意味着区块链的数据存储是分布式存储的



- 分布式帐本

区块链

状态库

区块

是在某段时间内区块链网络中的“交易”的打包

- 比特币：每10秒钟左右
- 以太坊：15秒中内

区块

是在某段时间内区块链网络中的“交易”的打包

由用户所发出的对区块链中的相关账户状态发生改变的指令集

- 区块链

区块链

指从区块链网络创建以来，网络中用户所发出的所有账户改变指令的全体集合。

状态库

指当前网络中所有账户的当前状态的集合，这个状态就是以前一区块的状态作为基础，以新区块作为变量，在状态转移函数的作用下生成的。

区块链的核心工作原理

$$S(t+1) = F((S(t), B(t+1))$$

- S(t+1)代表（t+1）区块时的状态
- S(t)代表的是t时刻的状态
- B(t+1)代表的（t+1）时刻的区块
- F（）指的状态转移函数

账户

以太坊

用户账户 ▸ 由区块链网络中的用户自行创建并由用户的密钥控制

合约账户 ▸ 由用户通过部署智能合约生成，合约账户由合约中的代码控制

非对称密钥体制

对称密钥

- 即我们加密密码和解密密码完全一样

- 不适合用在通信环境中

非对称密钥体制

公 钥	公之于众
私 钥	由用户自己掌握并严格保密

非对称密钥体制

公 钥

- 所加密的信息仅能由私钥解密

私 钥

- 所加密的信息仅能由公钥解密

非对称密钥体制

确保了信息在通信传输中的安全

非对称密钥体制

非对称加密

- 实现对信息的签名

非对称密钥体制是区块链点对点可靠通信的基础性技术，甚至可以说是区块链的基石。

用户帐户

密钥文件 存储有用户的私钥

公钥生成的账户地址

- 是用户在区块链网络中活动的身份码或地址码
- 是区块链中状态库记载的关键字段

合约账户

合约账户

账户余额

合约代码 ▶ 实现了对合约账户的控制

仅能由所存储的合约代码的逻辑规则来控制

合约账户

合约代码的执行实质上是被动的

仅能由掌握有私钥的用户账户发起并由用户私钥签名的交易来调用合约代码。

哈希散列计算

哈希计算

哈希（Hash）算法，即散列函数。它是一种单向密码体制，即它是一个从明文到密文的不可逆的映射，只有加密过程,没有解密过程。

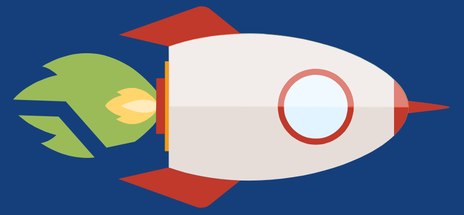
哈希散列计算

- 哈希函数可以将任意长度的输入经过变化以后得到固定长度的输出。
- 哈希函数的这种单向特征和输出数据长度固定的特征使得它可以生成消息或者数据。

哈希散列计算

- 对原始数据进行任一改变，所生成的哈希码将大大不同

不可能通过哈希码来推导出原始数据



哈希散列计算

数据指纹

- 用一固定大小并大大压缩的数据码来代表原始数据本身。

哈希散列计算

- 区块封装
- 工作量证明的随机数计算

哈希散列计算

分布式
账本

- 区块封装
- 回溯验证

哈希散列计算

前一区块已不可更改

- 区块链

通过对前一区块进行哈希验证与回溯，可以从当前区块出发一直到创始区块验证整个链的产生历史和全程可信。

总结

1. 分布式账本是区块链工作的基石，存储于区块链中的诸多节点上，并具有完全相同一致的结构与内容；

2. 分布式账本包括有存储交易序列集的区块链账本与表达区块链当前所有账户状态的状态库两大部分；

总结

3 区块链的核心工作原理是当前状态库等于以前一状态库与当前区块作为输入数据，执行节点软件的状态转移函数所生成的状态转移结果；

4 非对称密钥体制是区块链实现点对点安全通信的基础性技术，哈希计算是实现区块链数据不可篡改及溯源的基础性技术。

- 签名发出一个向指定账户发送2个以太币的转账交易