5.5 无链之链Corda概述

01 Corda

Corda是由R3CEV公司专门为**金融服务**设计的**分布式账本平台**。

Corda是**分布式账本技术**的独特实现，也是**金融机构与技术合作伙伴之间合作**的成果。

Corda的**目标**是让真实世界的实体管理者具有法律效力的合同，在没有技术限制和隐私泄露的情况下实现价值转移。

02 Corda的特性

1、分布式账本技术

- **Corda平台**由互不信任的分布式节点组成，用于记录机构和个人之间的交易状态、债务及其他协议信息。
- 该技术可以减少当前机构或个人之间为同步彼此隔离的账本所进行的大量手动和耗时的工作。
- 该技术可以为各行业带来更高水平的**代码共享**，从而降低每个参与者的**交易成本**。

03 Corda的特性

2、身份认证

- 身份认证是用户从真实世界的身份到网络身份(公钥) 的唯一映射
- Corda严格要求这种映射的唯一性
- 身份认证用于让用户确信跟他们交易的人与他们预期的一样，确保交易可信赖进行

04 Corda的特性

3、网络经济模型

- Corda全球网络**支持法定数字货币**，是**首个**能大规模接入而且支持法定数字货币的区块链网络。
- 接入Corda网络需要符合全球支付系统的**监管**。
- Corda网络支持**基于特定应用的原生资产或者通证**，采用相同的标准表示、存储和交换通证。

05 Corda的特性

4、智能合约

- 智能合约**封装了交易的业务逻辑**。
- 智能合约逻辑设置了**约束条件**，确保能够按照预先约定的规则进行有效的状态转换，并将规则写在**合约代码**内。
- Corda的智能合约由一段**纯函数**构成，用与接受或拒绝交易提案，且可以由更简单、可重复使用的函数组成。

06 Corda的特性

5、共识机制

- 与所有区块链平台一样，Corda也需要共识机制的支撑。
- 共识服务处理完毕后，参与方才能确信交易已经得到确认。
- Corda的独特之处在于可支持单个网络中超过数十亿次日交易数。
- Corda允许在同一网络中存在多个针对不同目的共识服务，被称为公证人池。

07 Corda的特性

6、隐私保护

- Corda有独特的隐私保护方案：
  - 1、交易信息只保存在交易的相关方和其他一些有权限查看的节点，而非全网广播；
  - 2、节点间通信完全加密的，避免消息泄露；
  - 3、使用自动身份管理对密钥进行轮换和随机化处理，确保交易匿名化；
  - 4、交易通过Merkle树构建，可选择性披露信息；
  - 5、采用英特尔软件防护扩展技术，在消息加密情况下即可对数据进行校验，确保交易信息的隐私性。

08 Corda的特性

7、互操作性

- 所有的参与者以点对点的方式在节点之间进行交易。
- 不同商业网络中可以有互操作性，避免资产只存在于一个数据孤岛中。

09 Corda的特性

8、预言机

- 预言机是一种信息服务的提供商，为Corda网络中的节点提供外部服务。
- 预言机所提供的信息会签署，确保交易各方可验证其来源。
- 在交易过程中及在后续审计中，预言机签署信息均不可改变。

10 Corda采用的模型

Corda采用了一种**扩展了外延的UTXO模型**

不仅可以描述价值转移，还可以描述准价值、非价值类型的单据的鉴别、确认、记录和以此为基础的流程展开

架构模型

- 比特币：UTXO模型
- 以太坊：账户-余额模型

最大不同：UTXO模型直接记载原始事实，而账户-余额模型记载根据原始事实推断出来的余额

余额直接可用，但有时不足以完整解释余额状态何以发生

Corda以注重原始单据合法合规性的银行应用为背景，因而采用UTXO模型