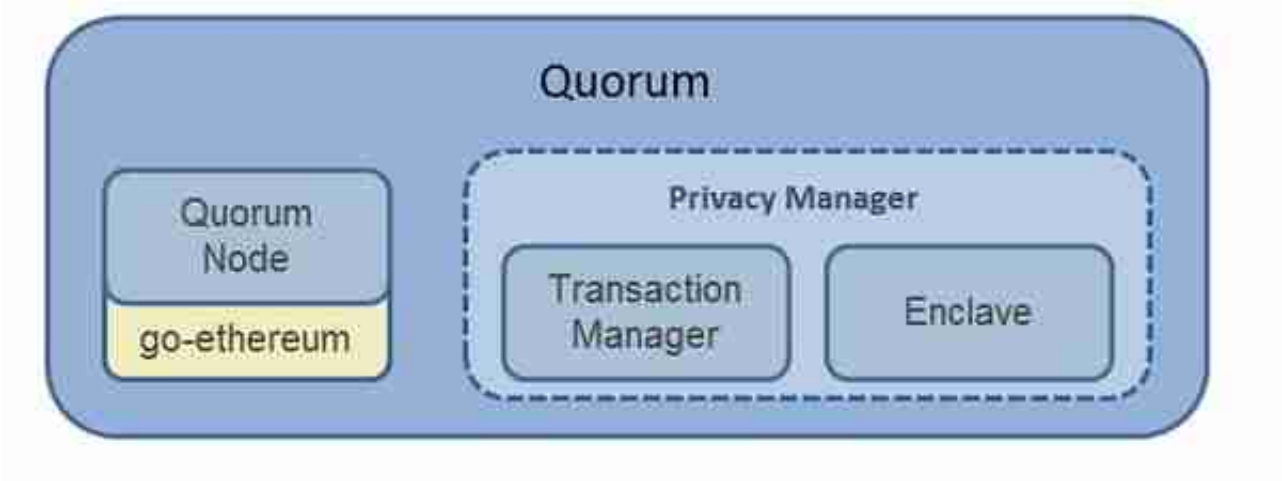

· Quorum节点

Quorum节点被特意设计成geth的一个轻量级分支，以便可以持续利用不断增加的以太坊社区中正在进行的研发成果。因此，Quorum将随未来geth的版本一起更新。Quorum节点包括以下对geth的修改:

- 共识是达成Raft或伊斯坦布尔BFT共识算法，而不是使用工作证明。

- P2P层已经被修改为只允许与许可节点之间连接。

- 块生成逻辑已被修改，将“全局状态根”检查替换为新的“全局公共状态根”检查。

- 块验证逻辑已被修改，将块头中的“全局状态根”替换为“全局公共状态根”。

- 帕特里夏·特里结构状态被一分为二：一个公共特里结构和一个私人特里结构。

- 块验证逻辑已被修改为处理“私人交易”。

- 交易创建已被修改，允许用加密的哈希替换交易数据，以便在需要时保留私人数据。

- 气体价格已经取消，但气体本身仍然存在。

· 隐私管理器

Constellation和Tessera实现使用通用系统的Haskell和Java来以一种安全的方式提交信息。它们可以与使用PGP加密消息的MTA（消息传输代理）网络相比较。它不

是特定于区块链的，也可能适用于许多其他类型的想要在对方网络中进行单独密封消息交换的应用程序。Constellation模块和Tessera模块由两个子模块组成:节点（用于Quorum私人交易管理器的默认执行）和 Enclave （飞地）。

交易管理器

Quorum的交易管理器负责交易隐私。它存储和允许访问加密的交易数据，与其他参与者的交易管理器交换加密的有效负载，但不能访问任何敏感的私钥。它利用Enclave实现加密功能（尽管Enclave可以选择由交易管理器本身承载）。交易管理器是平静的/无状态的，可以轻松实现负载平衡。

The Enclave （飞地）

分布式账本协议通常利用加密技术来实现交易真实性、参与者身份验证和历史数据保存（比如通过加密的散列数据链）。为了实现分散关注点，并通过对某些加密操作的平行化来提供性能改进，包括对称密钥生成和数据加密/解密在内的许多加密工作都委托给Enclave来做。

Enclave与交易管理器携手合作以加强私隐，以一种隔离的方式管理加密/解密。它持有私钥，本质上是一个与其他组件隔离的“虚拟HSM”。

第三部分：设计

· 公开/私有状态

Quorum支持双重状态:

- 公开状态:可由网络中的所有节点访问；

- 私有状态:只有具有正确权限的节点可以访问。

区别是通过使用加密的（私有的）和非加密的有效负载（公开的）来实现的。节点可以通过查看签名的v值来确定交易是否是私有的。公开交易的v值为27或28，私人交易的v值为37或38。

如果交易是私有的，则节点只能在允许访问和解密负载的情况下执行交易，不涉及交易的节点根本没有私有负载。因此，所有节点共享一个通过公开交易创建的公开状态，并且具有本地唯一的私有状态。

这个模型对私有交易中修改状态的能力施加了限制。由于从公开合约读取数据是（私有）合约的常见用例，因此虚拟机能够进入只读模式。对于从私有合约到公开合约的每次调用，虚拟机将更改为只读模式。如果虚拟机处于只读模式，并且代码试图更改状态，那么虚拟机将停止执行并出现异常。

允许进行以下交易:

1. S -> A -> B

2. S -> (A) -> (B)

3. S -> (A) -> [B -> C]

不支持以下交易：

1. (S) -> A

2. (S) -> (A)

注: S = 发送者 (X) = 私人 X = 公开 -> = 方向 = 只读模式

· 状态验证

为了确定节点是否处于同步状态，在块中包含了根哈希。由于私人交易只能由相关节点处理，因此不可能就私人状态达成全球共识。

为了克服这个问题，可以使用RPC方法“eth_storageRoot（地址[，区块号]）->哈希”。它可以给（可选的）块号返回给定地址的存储根。如果没有给出可选的块号，则使用最新的块号。存储根哈希由相关方比较后决定，可以是on或off链。

结语

当人们谈论起分布式账本时，总会将分布式账本和区块链认为是一回事，其实这是一个误解。分布式账本技术，简称DLT，指的是一种不需要被任何中心化主体存储或者确认的数据记录方式。分布式账本最突出的特征是其不由任何单个机构或个人维护，而是由网络中的每个节点单独构建和记录。在技术层面，分布式账本具有去中心化的特点，而且依赖于共识原则。但是，在中心化主体对一个去中心化网络掌有控制权的情况下，从意识形态上说，并完全不符合去中心化组织的特点。而区块

链是比特币、以太坊和其它加密货币的底层技术。它是分布式账本技术的一种形式，是一个由去中心化网络中，基于公式算法而达成的不可篡改的的账本。通过加密数字签名（Cryptographic Signing），并用“账本”将记录连在一起，就形成了一个链条，这就是区块链和分布式账本技术的不同。

每个区块链都是一个分布式账本，但不是每个分布式账本都是区块链。两者虽然都涉及到了去中心化和节点之间的共识。区块链不仅仅在技术和结构层面是去中心化的，它的管理组织和发展也是去中心化的。而在分布式账本里，只有技术是去中心化的，运营主体并不是。因此，分布式账本技术更多的被运用在金融和政府事务领域。

来源：quorum官网

翻译：Emily|达瓴智库