医结区块链安全审查报告

上海点融信息科技有限责任公司

2019-05-15

摘要

医结区块链网络是一个经由点融区块链云服务平台(以下简称BaaS平台)部署和管理的联盟链。该区块链基于原生的Hyperledger Fabric v1.4.0版本作为底层基础设施。依赖于BaaS平台功能强大的联盟治理能力，医结区块链网络可以方便地联合多个参与方共建账本，并基于智能合约实现业务逻辑协同和数据共享，同时有效地保护了数据隐私。通过充分利用Fabric的各项安全机制，医结区块链网络可以确保任何参与方无法通过各种手段恶意篡改区块链上的数据。

本文将从联盟链治理、通道和私有数据隔离、以及智能合约的权限控制等方面来说明医结区块链网络的所具备的诸多安全特性。

1. 联盟链治理

在医结区块链网络中，每一个参与方都拥有独立的BaaS账号。通过BaaS平台各参与方将己方的Orderer和Peer节点部署在自己的IT环境中，独立运维和管理，并与其他参与方的节点共同组成一个联盟链网络。在Fabric中，通道（channel）与账本几乎是等同的概念，但在本质上它是一个由各参与方构成的信任域，在此信任域中各参与方通过共同运行智能合约来读写账本数据。通道以外的其他人无法读写账本数据，也无法调用部署在通道内的智能合约。因此，通道的创建和管理非常重要，必须各参与方能共同治理。

医结区块链网络的各参与方依托于BaaS平台共同组建了一个全局唯一的通道。当创建通道时，由一方牵头（称为“盟主”）发起创建申请，然后由各个成员使用自己的私钥签名同意，才使得该通道得以创建成功。当有新的参与方加入时，必须已有参与方签名同意，才能使该参与方得以加入。

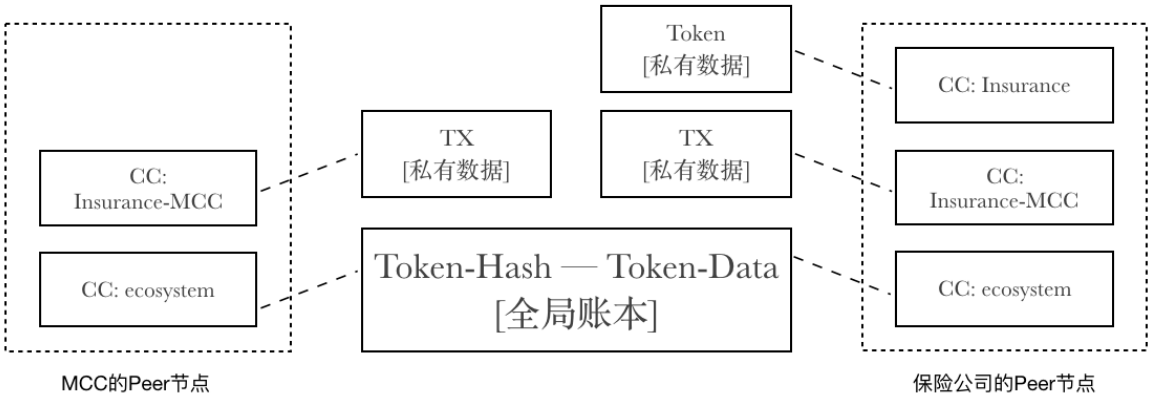
另外，BaaS平台没有保存用户的任何私钥，各参与方的私钥通过自己本地的点融区块链客户端被加密保存在本地的保险箱文件中，客户端不使用时可以离线，大大降低了私钥泄漏的风险。

2. 通道和私有数据隔离

在Fabric中，一个通道对应一个账本，数据是以Key-Value的形式保存在账本中，通道中的数据在所有通道参与方的Peer节点之间共享。为了保护数据隐私，Fabric提供了基于智能合约的私有数据机制。它支持在通道的范围内，允许在某些参与方之间共享Key-Value的明文，而在通道的账本中只有该Key-Value的Hash值（即：hash(key)-hash(value)）。Fabric用私有数据集合来定义这个数据共享的范围，集合中的参与方将Key-Value的明文保存在自己的Peer节点上。

也就是说，私有数据机制可以确保私有数据集合以外的其他通道参与方只能看到账本中的hash(key)-hash(value)，而无法获知其真正内容。

在医结区块链网络中，只有一个全局唯一的通道，即一个账本。在其上部署了三类智能合约，其中有两类智能合约应用了私有数据机制来限制其数据的可见范围。如下图所示：



1. ecosystem智能合约: 负责产生、更新Token-Data。Token-Hash作为Key, Token-Data作为value被明文记录在全局账本中。Token-Data中记录Token的产生者、拥有者、Token类型、过期时间、Token产生者的签名、转移日期等信息。通道的所有参与方都共同保存这些信息。

2. Issurance智能合约：产生、更新Token。并通过调用ecosystem智能合约将Token-Hash和Token-Data记录在全局账本中，而Token字符串的明文记录在自己独有的私有数据集合中。

3. Issurance-MCC智能合约：产生交易数据(TX)，并将TX数据保存在仅限于MCC和保险公司之间的私有数据集合中，而在全局账本中只记录TX的Hash值。同时通过调用ecosystem智能合约变更Token的拥有者，将Token转移至MCC名下。

3. 智能合约的权限控制

智能合约的权限控制包括两个方面：1）谁有权限来访问该合约的哪些接口；2）该合约产生的交易须经过哪些参与方进行背书才能被允许写入账本。在Fabric中，所谓“背书”，即调用某个Peer节点上的指定智能合约的指定方法，并获取该Peer节点对合约运行结果进行签名的过程。采用智能合约的背书策略，可以指定一个合法的交易必须获得哪些参与方的背书，当通道内的Peer节点在验证交易时会检查是否满足背书策略的要求，通过验证的交易才会被写入账本。另外，背书策略与智能合约的版本是绑定在一起的，进行交易时也要求参与背书的合约版本也完全一致。

运行于医结区块链网络上的所有智能合约都实现了以上两个方面的权限控制。

2.2.1. Issurance智能合约

安装在保险公司的Peer节点上，该合约的所有接口只允许保险公司自己一方的应用程序来调用。产生Token时，该合约会使用自己的私钥对该Token进行签名，并将签名信息作为Token-Data的一个属性被记录全局账本中，Token被转移时会通过校验该签名来核查Token生产者的身份。另外，该合约的背书策略被设置成：必须保险公司进行了背书。

通过以上机制确保了：1）其他参与方无法调用保险公司的Peer节点上的Issurance智能合约来产生Token；2）即使某个恶意参与方私自安装了Issurance智能合约来产生Token，他也无法伪造出保险公司的Token。

2.2.2. Issurance-MCC智能合约

Issurance-MCC智能合约：分别安装在保险公司和MCC的Peer节点上。合约的所有接口只允许MCC一方的应用程序来调用。该合约生成交易数据之后，转移Token时

会验证该Token的签名来确保的确是该保险公司所产生的。另外，该合约的背书策略被设置成：必须要MCC和保险公司双方都背书。

通过以上机制确保了：1）其他参与方无法调用Issurance-MCC智能合约来产生交易和转移Token；2）杜绝了使用伪造的Token来进行交易的行为；3）基于双方背书的策略，防止了MCC和保险公司任意一方通过升级己方的Issurance-MCC智能合约的方式来绕开校验逻辑，从而伪造交易和转移Token的风险。

2.2.3. ecosystem智能合约

任何参与方可以直接访问ecosystem智能合约，但ecosystem智能合约的所有接口的入参要求提供Token字符串的原文。因为该原文只有保险公司一方才拥有，所以其他参与方因为无法获知Token原文而不可能恶意修改、删除已有的Token-Data。另外，为了防止恶意参与方通过升级己方Peer节点上的ecosystem智能合约而绕开“必须提供Token原文”的逻辑，ecosystem智能合约采用了Fabric的key level 背书策略机制：1）当Issurance智能合约调用ecosystem智能合约产生Token时，ecosystem智能合约将该Token的key level 背书策略设置成：要求保险公司背书即可；2）当Issurance-MCC智能合约调用ecosystem智能合约转移Token时，ecosystem智能合约将该Token的key level 背书策略设置成：要求MCC和保险公司双方都背书。

4. 结论

综上所述，医结区块链网络的各参与方既能独立运维自己的节点，又能共同组建一个联盟链网络，并且具备协同治理联盟链的能力。该系统依托于分层设计智能合约的创新理念，充分利用Fabric的隐私保护和智能合约背书策略机制，针对不同数据类型有所区别地进行共享和隐私保护；并且针对各种恶意行为实现了较为完备的防范机制。相信医结区块链网络能在业务实践中经受住现实的考验，并不断扩大生态系统规模，有力支撑业务的蓬勃发展。