密码学技术是信息技术的基石，区块链中大量使用了现代信息安全和密码学的技术成果，主要包括：哈希算法、对称加密、非对称加密、数字签名、数字证书等。哈希算法解决了信息完整性验证问题，对称算法提高了加密运算效率，非对称算法解决了对称密钥传递问题，数字证书则为公钥所有者背书，解决了公钥持有者的证明问题，PKI/CA
体系形成了解决信息安全、信息机密性、完整性和抗抵赖的完整解决方案。

目前在中国主流发展的区块链技术被称为开放许可链，什么叫做许可链呢？就是所有组成许可链的节点所有者，其身份都是被认证过，被许可授权后，才能加入到该区块链网络的。

在这种场景中，网络向授权的组织或机构开放，链上各参与方之间是一种协作关系，存在准入机制。PKI/CA 体系作为完整解决方案，可以为许可链各参与方提供身份认证证书，实现准入权限控制。可以说，证书机制是许可链网络安全的基石。本文对 PKI/CA 基本概念进行必要描述后，详细阐述 Ultrain 证书管理体系。

01 公钥基础设施

公钥基础设施（Public Key Infrastructure，简称 PKI）是一个包含硬件、软件和策略等集合，用来实现基于公钥密码体制的密钥和证书的产生、管理、存储、分发和撤销等功能的完整系统。

1.1 PKI 系统

PKI 系统包括证书机构 CA（Certificate Of Authority，认证中心）、注册机构 RA 和相应的 PKI 存储库。CA 用于签发并管理证书；RA 可作为 CA 的一部分，也可以独立，其功能包括个人身份审核、CRL管理、密钥产生和密钥对备份等；PKI
存储库包括 LDAP（Lightweight Directory Access Protocol，轻量目录访问协议）目录服务器和普通数据库，用于对用户申请、证书、密钥、CRL（Certificate revocation lists）和日志等信息进行存储和管理，并提供一定的查询功能。

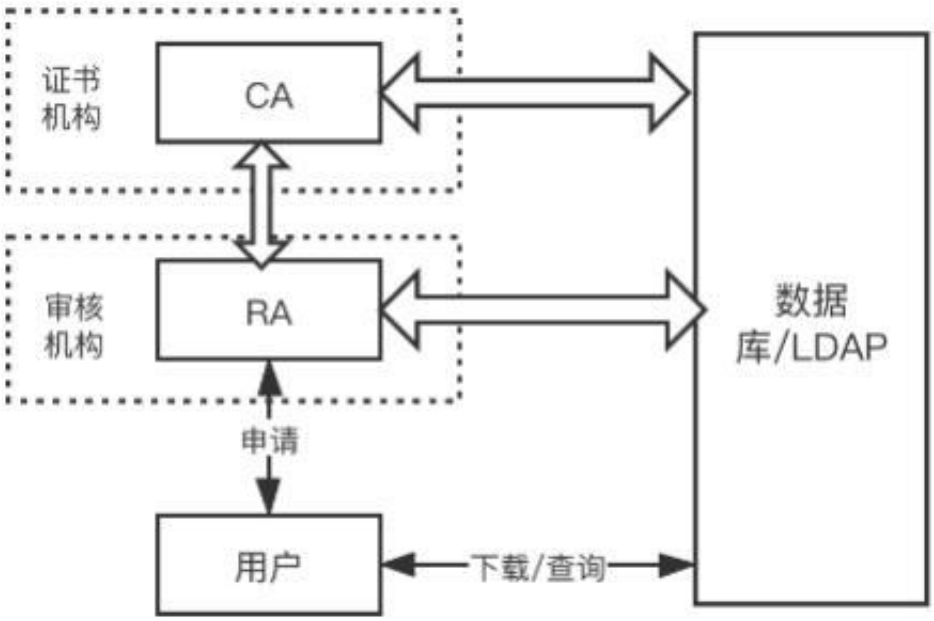

图1 PKI系统

1.2 证书申请过程

? 用户申请：

用户生成自己的公钥和私钥，将公钥和自己的身份信息提交给安全服务器，安全服务器将用户的申请信息传送给 RA 服务器。

? RA 审核：

用户向 RA 证明自己的身份，RA 收到用户的申请后进行核对。如果 RA 同意用户申请证书的请求，则对证书申请信息做数字签名；否则拒绝用户的申请。

? CA 发行证书：

RA 将用户申请和 RA 签名传输给 CA，CA 对 RA 数字签名做认证，如果验证通过，则同意用户请求，颁发证书，然后将证书输出。如果验证不通过，则拒绝证书申请。

? RA 转发证书：

RA 从CA 得到新的证书，首先将证书输出到 LDAP 服务器以提供目录浏览，再通

知用户证书发行成功，告知证书序列号，到指定的网址去下载证书。

? 用户证书获取：

用户使用证书序列号去指定网址下载自己的数字证书。

1.3 X.509 证书格式

主流的证书格式为 X.509 格式。X.509
标准规定了证书可以包含什么信息，并说明了记录信息的方法。

X.509 结构中包括版本号（Version Number）、序列号（Serial
Number）、签名算法（Signature Algorithm）、颁布者（Issuer）、有效期（V
alidity）、主体（Subject）、主体公钥信息（Subject Public Key
Info）、主体公钥算法（Public Key Algorithm）、主体公钥（Subject Public
Key）、证书签名算法（Certificate Signature
Algorithm）和证书签名（Certificate Signature）。

1.4 证书验证原理

1. 对证书中的明文利用相同的散列函数得到摘要值 H1。

2. 用 CA 根证书验证客户证书的签名合法性，即证书中的签名用 CA
根证书的公钥解签，解签的结果与步骤 1 中的 H1
对比，如果一致，说明证书是由信任的根证书签发，且证书的内容没有被篡改。

3. 检查客户证书是否有效 (当前时间在证书结构中的所定义的有效期内)。

4. 检查客户证书是否作废 (OCSP 方式或 CRL 方式)。

5. 验证客户证书结构中的证书用途。

上述所有信息都验证通过，那么证书中客户的公钥信息就能够在后续的操作中使用
。

02 Ultrain 证书管理体系

许可链经过授权的节点组成联盟从而共享和访问数据。PKI
体系是一套用户审核、身份管理和隐私保护的完整的、成熟的体系，Ultrain 定义

了一套从上而下的证书管理流程，从而实现许可链节点的权限管理和访问控制。

2.1 Ultrain 证书体系

Ultrain 采用面向 CA 的准入机制，实现基于 X.509
格式证书的认证和动态管理。根据现有业务场景，证书体系如图 2
所示，自上而下包含以下类型：根证书、链证书、节点证书和用户证书。

根证书：根证书是一个自签名的证书，为所有证书的根，对应的私钥 key
文件由联盟委员会共同管理。

链证书：在多链架构中，单链管理机构生成链私钥，并生成请求文件 chain.csr
发送给联盟委员会，联盟委员会审核通过后签发链证书 chain.crt。

节点证书：节点证书由链证书签发。节点生成并保存自己的私钥文件
node.key，并生成请求文件 node.csr
发送给链管理机构，链管理机构审核通过后签发节点证书 node.crt。节点证书是节点的身份凭证，拥有节点证书的节点能够与区块链网络中节点建立 SSL
链接，实现节点间的加密通信。

用户证书：用户证书由提供链访问接口的节点签发。用户生成并保存自己的私钥文件 sdk.key，并生成请求文件 sdk.csr
发送给需要访问的节点管理机构，节点管理机构审核通过后签发用户证书 sdk.crt。用户证书是客户端的身份凭证，拥有用户证书的客户端才能正常访问链接口。

Ultrain 提供了一套证书申请签发管理程序，方便各级证书的申请、验证及签发。

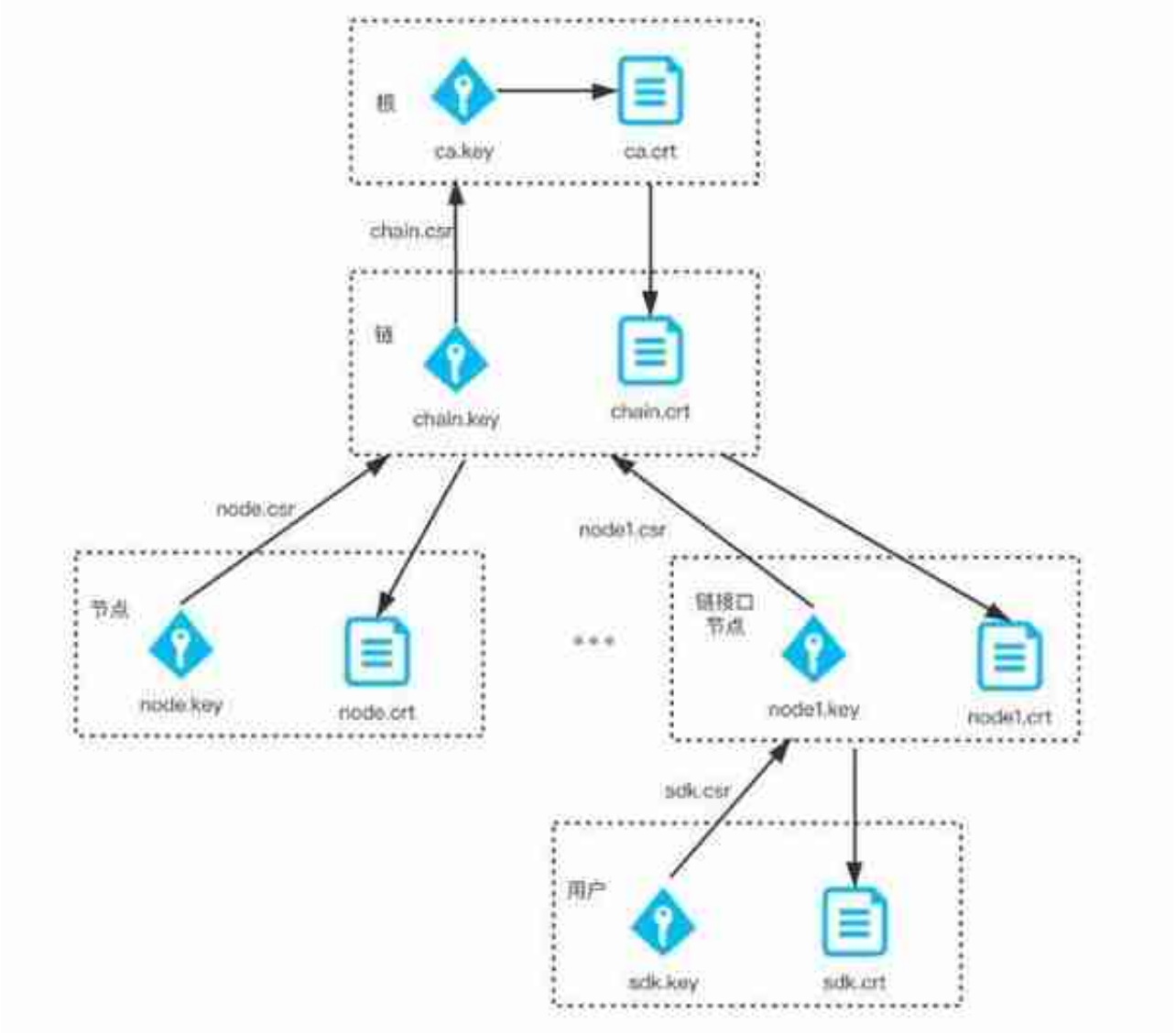

图2 Ultrain 证书体系

2.2 证书使用场景及验证

根证书由 Ultrain 联盟委员会共同管理，目前采用自签名证书，也可以与商业证书签发机构对接，使用权威机构签发的证书。当业务需要建立新的侧链时，该侧链管理机构提交证书请求文件，联盟委员会审核通过后使用根证书签发链证书；链证书由该链管理委员会进行管理，链管理委员会接收联盟成员成为运行节点的证书请求文件，委员会审核通过后签发节点证书；联盟成员使用节点证书以接入该侧链节点网络，才可以进行共识及交易信息的正常收发。如果该节点提供链上数据访问接口，则需签发用户证书提供给客户端使用；客户端使用特定节点签发的用户证书，才可以正常访问该节点提供的数据接口，进行数据读取、交易发送等操作。

节点证书验证

节点证书在节点间建链时使用。基于证书验证的链接建立之后，节点才能组成 P2P 网络，从而实现共识协议信息和交易信息的传播，下图为节点证书的使用流程。

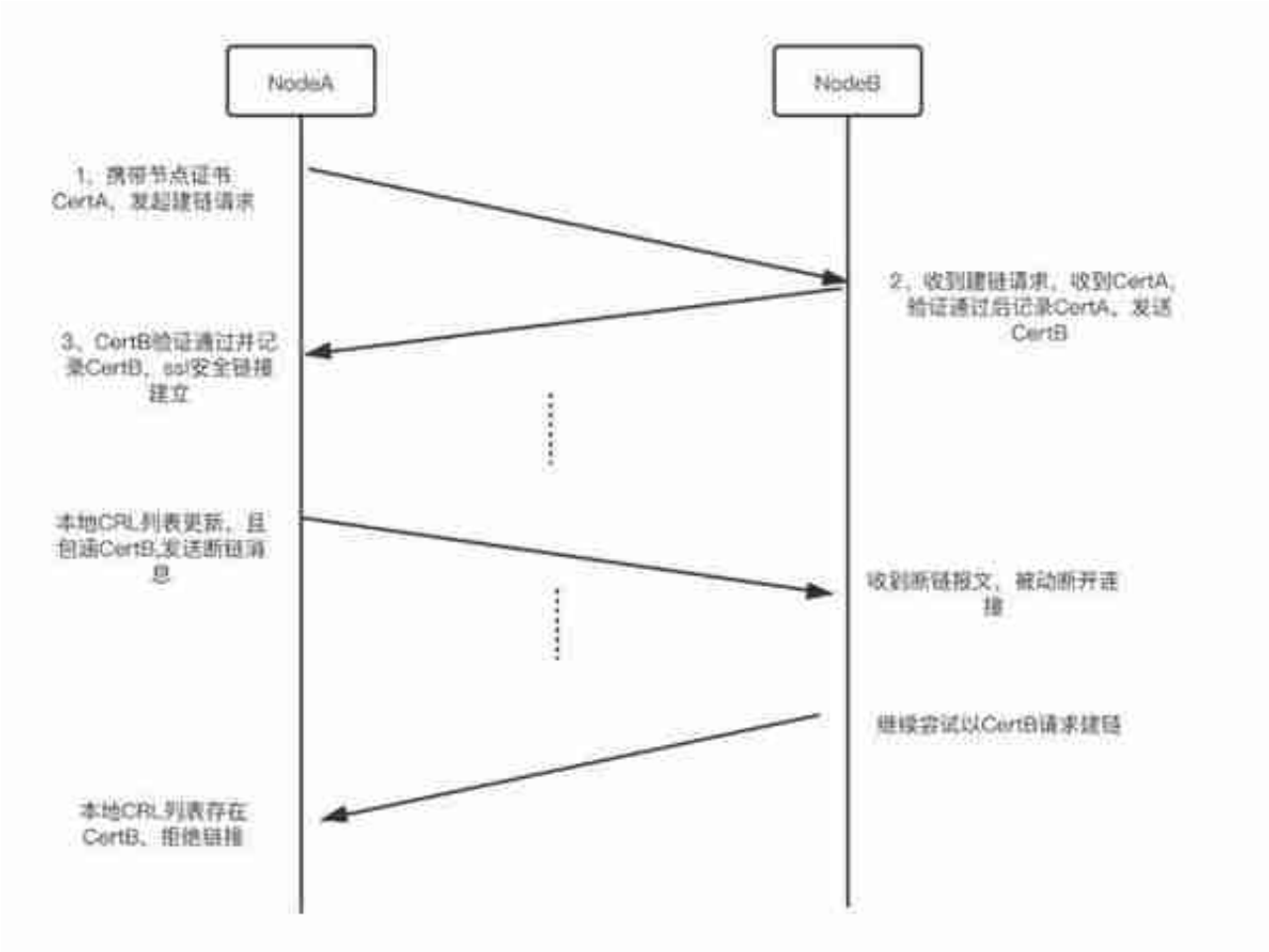

图3 Ultrain 节点证书验证流程

节点在启动时，携带自己的节点证书可以与同样拥有节点证书的节点建立 SSL 安全链接。当证书过期、被篡改时，不能加入到 P2P 网络中，从而不能共享和传播链上数据。

在 Ultrain 的证书吊销（CRL）管理体系中，证书的吊销由该证书签发机构完成。节点可以向 CA 管理中心定期获取 CRL 列表。节点间的心跳报文中需携带自己的节点证书，当不携带节点证书或携带的证书在 CRL 列表时，心跳报文检测端会主动拆掉与被检测端的链接，实现实时的接入管理控制。

用户证书验证

客户端访问节点提供的链接口时，可以选择校验节点证书，以验证节点身份，此时需使用根证书、链证书组成的证书链对节点证书校验。另外，客户端需提供用户证书给节点，节点的 HTTPS 服务会校验客户端所提供的用户证书（使用根证书、链证书以及节点证书组成的证书链进行校验），同时会检查 CRL
吊销列表，校验通过且该用户证书不在 CRL 列表时，则成功建立 SSL 链接，进行正常通信，否则则不能建立链接，从而保证了客户端与节点间的通信安全。