基于智能合约的公钥证书发放方案

文/张成成

摘要

基于以太坊智能合约平台，提出了一种新的公钥证书发放方案。本方案使用智能合约实现，用户和证书发放机构将自己的数据以智能合约的形式存放到区块链上，其他人可以公开验证。本方案利用智能合约全网公开的安全特性有效降低了在不安全信道上签署和发放公钥证书的安全风险。依托于以太坊区块链，本方案具有防篡改，防拒绝服务式攻击等特点。

【关键词】区块链 智能合约 公钥证书 以太坊

1 前言

公钥证书是当前一种应用广泛的公钥分配解决方案，最早由 Kohnfelder 提出。由于公钥证书方案不需要维护含有姓名和公钥的目录，从而成为一种较为安全的公钥分配方式。公钥证书中最重要的包含公钥和公钥拥有者的标志，为了保证证书的真实有效性，则证书内容必须由可信第三方进行签名。在这个过程中，用户必须以一种安全的方式将他的公钥信息传递给可信第三方机构。但是，因为没有绝对安全的通信信道，则用户将公钥信息传递给可信机构的过程中极易被攻击者拦截，则用户最后得到的公钥证书极有可能被攻击者篡改。怎样保证用户公钥信息传递过程的安全是当前亟待解决的一个问题。与此同时，可信机构的数据处理量又是有限的，攻击者在获取可信机构真实网络位置的情况下，可以发动拒绝服务式攻击。因此，隐藏可信机构的真实的网络位置是保障公钥证书系统正常工作的关键。

区块链技术随着比特币的出现而逐渐被人们所知。区块链网络没有中心节点，所有节点地位均等，采用工作量证明，权益证明等共识机制将区块链网络内的交易数据打包写入到区块中。在这个去中心化网络中，所有的节点保存着全网的数据备份。区块链采用的共识机制保障了在不可信信道上的信息传递的真实有效性。区块链网络中的巨大算力使得攻击者想要篡改区块链中的交易数据需要付出巨大的代价。区块链的这些特性既能防止数据在传输过程中遭到篡改，又能防止防止节点遭受拒绝服务式攻击。

以太坊是 2013 年由 Vitalik Buterin 提出的一种开源的公共区块链平台，它基于区块链技术建立，最大特点就是支持智能合约。以太坊智能合约（以下简称智能合约）与比特币脚本类似，但是智能合约具有图灵完备性，可以完成更加复杂的任务。用户可以将编写的智能合约编译成以太坊特有的以太坊虚拟机代码，即 EVM 代码。EVM 代码可以访问发送者和接收到的消息中的数据，代码还可以返回数据的字节队列作为输出。用户在与智能合约交互的过程中需要消耗一定量的燃料，燃料需要使用以太币兑换。这种机制就保证了攻击者想要通过短时间内与智能合约的大量交互进行拒绝服务式攻击需要耗费巨大的以太币资源。同时，智能合约灵活的数据访问特性能够保障公钥信息的公开透明访问以及数据完整性。

根据以上所述，我们提出了一种基于基于智能合约的公钥证书发放方案。本方案充分利用了区块链技术的去中心化和全网公开访问账本等特点保障了公钥证书在不可信信道上的安全签署，防范了攻击者对用户和可信机构的拒绝服务式攻击。

2 总体设计结构

本方案的总体设计框架如图 1 所示，各个部分功能如下。

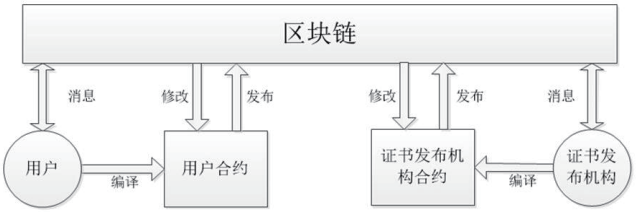

图 1：总体设计结构图

2.1 用户User

该用户可以是任何需要申请公钥证书的实体结构。

2.2 区块链

表示以太坊区块链，区块链上面的信息全网公开可见，任何人都可以查看合约的执行情况。

2.3 证书发布机构Ca

表示对用户的证书进行认证签名的机构，这个结构的公钥可以被所有人验证合法。之后，经过该结构签署的公钥证书可以被全网验证。

2.4 用户合约Contract-user

表示用户 User 发布的合约，该合约存储用户 User 的公钥证书信息。实际上，用户的公钥证书信息就是用户合约的核心内容。

2.5 证书发布机构合约Contract-ca

表示签证机构 Ca 处理其他用户认证请求的合约。用户通过改变该合约的一些数据内容向签证机构传递信息。

我们使用区块链代替传统不可信信道，同时将公钥证书以智能合约的形式发布出来。这里的合约 Contract-user 和合约 Contract-ca 都属于区块链的一部分，为了清楚地说明整个系统的工作过程，将这两个合约独立于以太坊区块链表示。而在实际中，这两个合约均存在于以太坊区块链中。而用户 User 和签证机构 Ca 都是匿名连接以太坊区块链的各个实体结构，即他们均不需要公布自己的真实的网络位置。

3 具体方案设计

签证机构 Ca 需要将自己的合约 Contract-ca 发布到以太坊区块链上，然后全网用户可以获取签证机构的合约 Contract-ca 的合约地址。之后用户 User 将自己的公钥证书以智能合约的形式发布到以太坊区块链上。此时的合约 Contract-user 不能被用作公钥证书，因为此时的公钥证书还没有被签证机构 Ca 签署生效。用户 User 可以将合约 Contract-user 的地址通过区块链传递给合约 Contract-ca，请求签证机构 Ca 对合约 User 进行认证。签证机构 Ca 从合约 Contract-ca 中获取需要请求的合约 Contract-user 的地址，然后在区块链上查询到合约 Contract-user 的相关信息，签证机构 Ca 在后台数据库中查到合约 Contract-user 合法后就可以通过区块链向合约 Contract-user 发送一个交易，对合约 Contract-user 的相关数据状态进行更改。最终合约 Contract-user 得到签证机构 Ca 的签署，整个过程并不在传统信道上传递公钥信息和签署信息。

3.1 证书发布机构合约

证书发布机构合约的编写与发布过程：

（1）初始化：Ca 与以太坊节点连接；生

●基金名称：西华大学研究生创新基金资助项目（ycjj2016072）。

表 1：认证合约的相关变量

数据项	功能
Id-ca	认证机构 Ca 唯一身份标识
Pk-ca	Ca 的公钥
Addr-ca	认证机构 Ca 的账户地址
Addr-contract-user	将要认证的用户合约地址，默认为空
Set-contract-user-address（addr）	函数，设置 Addr-contract-user 为 Addr
Get-contract-user-address（）	函数，获取 Addr-contract-user

表 2：用户合约的相关变量

数据项	功能
Id-user	User 的唯一身份标识
Pk-user	User 的公钥
Addr-user	User 的以太坊账户地址
Pk-ca	认证机构 Ca 的公钥
Addr-ca	认证机构 Ca 的以太坊账户地址
Addr-contract-ca	认证机构合约的地址
Signature-hash	Ca 对证书信息 Hash 值的签名
Set-signature-hash（str）	函数，如果发起交易的地址为认证机构的地址 Addr-ca，则令 Signature-hash 与 Str 相等
Get-signat-hash（）	返回 Signature-hash 值

成以太坊账户地址 Addr-ca，公私钥对 Pk-ca 和 Sk-ca。

（2）编写智能合约 Contract-ca，合约包含表 1 所列内容。

（3）将编写的合约 Contract-ca 编译发布到以太坊区块链上，返回 Contract-ca 的合约地址 Addr-contract-ca。

上述过程中使用的变量如表 1。

3.2 用户合约的编写与发布

用户合约的编写与发布：

（1）初始化：User 与以太坊节点连接；生成以太坊账户地址 Addr-user，公私钥对 Pk-user，Sk-user。

（2）编写智能合约 Contract-user，合约包含表 2 所列内容。

（3）将编写的合约 Contract-user 编译发布到以太坊区块链上，返回合约地址 Addr-contract-user。

上述过程中使用的变量如表 2。

3.3 证书发布机构签署用户合约

证书发布机构签署用户合约的步骤：

（1）User 修改区块链中 Contract-ca 合约中的 Addr-contract-user 为自己的证书合约的地址；

（2）Ca 从合约中获取 Addr-contract-user；

（3）Ca 查询以太坊区块链上 Addr-contract-user 所处合约；

（4）Ca 计算合约 Contract-user 中 Cert（Id-user，Pk-user，Addr-user，Pk-ca，Addr-ca，Addr-contract-ca）的 Signature-hash 值；

（5）Ca 使用自己的私钥 Sk-ca 对 Signature-hash 进行签署；

（6）被 Ca 签署的用户合约可以被 User 使用。

3.4 用户使用证书合约

用户使用证书合约的步骤：

（1）User 向其它用户公布自己的合约证书地址；

（2）验证者访问以太坊区块链获取合约证书内容；

（3）验证者通过证书内的 Addr-contract-ca 找到认证机构的地址；

（4）验证者通过 Addr-contract-ca 查找到认证机构的合约；

（5）验证者在认证机构的合约中查找到认证机构的公钥；

（6）验证者使用公钥解开 Signature-hash，获取证书信息的 Hash 值；

（7）验证者将得到的 Hash 值与自己计算的 Hash 值比较，如果两者相同，则 User 的证书信息真实有效。

4 总结

本文提出的方案充分利用了智能合约的特点解决了公钥证书发放过程中的问题。区块链的去中心化特点，使得全部节点地位相等，依靠 P2P 技术传播的交易信息在每个节点都能够完全验证。在不可信信道上传播的公钥证书信息因为在每个节点传播的时候都能够被验证，就极大地降低了被攻击者篡改的可能性。攻击者想要篡改证书信息，则必须拥有一半以上的全网算力才能保证供给成功。而实际上，当前以太坊区块链的全网总算力远远超过全球超级计算机总算力之和。攻击者想要攻击成功，则需要付出极大的代价。区块链节点与用户或者可信机构进行的是匿名链接。因为在区块链上，任何拥有与机构地址相对应的私钥的实体，即被认为是机构本身。因此，用户和可信机构只需保留相应的公私钥对即可，可以隐藏或者变换网络地址，这样攻击者就极难发现真实的实体位置。综上，本方案既可以在不可信信道上保障公钥信息的完整性，又能防止攻击者对某个机构进行拒绝服务式攻击。

然而，区块链在完美解决拜占庭问题的同时也带来了整体效率低下的问题。最突出的问题就是以太坊作为一个公有链，当前使用的是工作量证明作为共识机制。工作量证明机制是要求矿工完成一定的工作量才能取得记账权。在以太坊区块链中，矿工新建立一个区块需要大概 15 秒钟的时间，而一个新的区块容纳的交易数量是有限的。实际上，在智能合约的状态量改变过程中，每个状态量的改变都需要全网节点的共同确认才算合法。因此，我们就可以发现，智能合约在执行过程中的效率是很低的。但是，在随后的以太坊大都会阶段，以太坊执行分片，则智能合约的执行效率就会大大地增加。在未来的工作中，如何提高公钥证书合约的灵活性，使之适应越来越复杂的网络状况是我们的关注重点。

参考文献

[1]Kohnfelder L M. Towards a practical public-key cryptosystem[D]. Massachusetts Institute of Technology, 1978.

[2] 唐明，李莉，杜瑞颖 .William S. 密码编码学与网络安全——原理与实践（第六版）[M]. 北京：电子工业出版社，2015.

[3]Satoshi N.Bitcoin:A peer-to-peer electronic cash system[EB/OL].[2009-03-25].https://bitcoin.org/bitcoin.pdf.

作者简介

张成成（1991-），男，安徽省阜阳市人。硕士学位。西华大学计算机与软件工程学院学生。研究方向为信息安全。

作者单位

西华大学计算机与软件工程学院　四川省成都市　610039