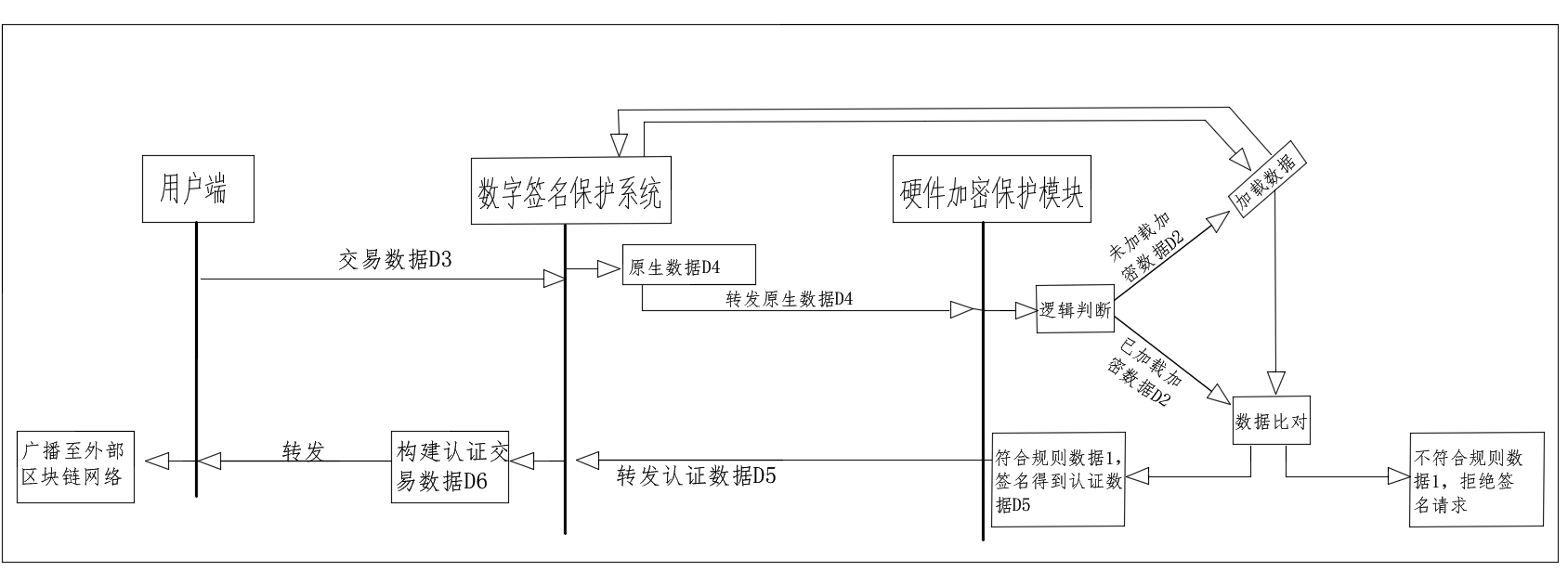
本发明公开了一种基于硬件加密保护的区块链数字签名系统及使用流程，包含包括用户端、管理端、数字签名保护系统、硬件加密保护模块，用户端通过数字签名保护系统与硬件加密保护模块双向通讯连接，管理端是离线系统，通过数字签名保护系统与硬件加密保护模块双向通讯连接，用户端与外部区块链网络通信连接，硬件加密保护模块为HSM硬件加密机或采用Intel SGX技术的CPU，本系统用户私钥和签名规则均位于硬件加密保护模块中，用户私钥位于硬件加密保护模块中持续在线，可适应高频交易，并且私钥和签名规则储存时也是以加密形态存在，有效降低了系统被入侵、用户账号被劫持、数字货币被盗取、区块链交易被冒充等风险。



1．一种基于硬件加密保护的区块链数字签名系统，其特征在于：所述系统包括用户端、管理端、数字签名保护系统、硬件加密保护模块，所述用户端通过数字签名保护系统与硬件加密保护模块双向通讯连接，所述管理端通过数字签名保护系统与硬件加密保护模块双向通讯连接，所述用户端与外部区块链网络通信连接，所述管理端为离线系统。

2．根据权利要求1所述的一种基于硬件加密保护的区块链数字签名系统，其特征在于：所述硬件加密保护模块为HSM硬件加密机或采用Intel SGX技术的CPU。

3．一种基于硬件加密保护的区块链数字签名系统的使用流程，包括数字签名保护系统的设置初始化过程和交易数据请求过程。

4．根据权利要求3所述的一种基于硬件加密保护的区块链数字签名系统的使用流程，其特征在于：所述规则数据D1包括用户的区块链私钥和签名规则。

5．根据权利要求4所述的一种基于硬件加密保护的区块链数字签名系统的使用流程，其特征在于：所述用户的数量至少为一个，且规则数据D1和交易数据D3中包含唯一性的标签数据。

6．根据权利要求4所述的一种基于硬件加密保护的区块链数字签名系统的使用流程，其特征在于：所述签名规则包含额度上限和地址白名单。

7．根据权利要求4所述的一种基于硬件加密保护的区块链数字签名系统的使用流程，其特征在于：所述签名规则包括时效。

8．根据权利要求4所述的一种基于硬件加密保护的区块链数字签名系统的使用流程，其特征在于：所述S5的步骤中，B2情况下，硬件加密保护模块将拒绝情况转发给数字签名保护系统，数字签名保护系统将拒绝情况反馈给用户端。

一种基于硬件加密保护的区块链数字签名系统及使用流程

**技术领域**

本发明涉及区块链技术领域，具体为一种基于硬件加密保护的区块链数字签名系统及使用流程。

**背景技术**

区块链一般被理解为一个分布式的账本，它实质上也是一个分布式计算和存储系统，不同区块链节点通过一定的计算规则达成共识，并且将共识后的交易执行结果以区块的形式存储至数据库中，多个区块组成了区块链。

在区块链技术体系中，各节点之间进行通讯并达成信任，需要依赖数字签名技术，它主要实现了身份确认并确保了信息完整性。数字签名涉及到私钥、公钥和钱包等工具。数字签名有两个作用，一是证明消息确实是由信息发送方发出来的，二是确定消息的完整性。通过私钥、公钥的非对称加密机制，使用特定接收人的公钥进行发送内容加密，只有此接收人的私钥才能解密发送内容，从而实现对指定接收人的信息传送安全保障，另外通过在发送端和接收端对报文内容执行同样的Hash计算并比较Hash值，确保发送信息的完整性。由此可见私钥是区块链技术中最重要的部分，因为能够唯一代表用户的身份，所以私钥的保存和使用必须绝对安全，一旦泄露并被他人使用则意味着此区块链用户完全被窃取并替代。

目前对私钥的保存和管理主要采用冷钱包的方式，即离线保存，使用时再读取上线的方式，虽具有一定的安全性，但使用效率非常低，完全不适应需要进行高频操作的应用场景，而且离线保存意味着一旦丢失或遗忘则无法有效找回，此外企业如果采取离线方式保存私钥意味着需要人工进行私钥的管理和取用，难以防范内鬼对私钥的窃取。

使用私钥进行数字签名的操作过程必须绝对可控，由于目前数字签名的使用方式是通过程序调用在计算机操作系统中进行，所以存在数字签名操作或数字签名功能接口被攻击者控制的风险。最近已经多次发生企业或者交易所被黑客攻击或内鬼窃取造成私钥丢失，最终损失大量虚拟货币的安全事件，区块链生态体系内需要一种技术能够安全可控地进行私钥和数字签名的管理和使用。为此，提出一种基于硬件加密保护的区块链数字签名系统及使用流程。

**发明内容**

本发明的目的在于提供一种基于硬件加密保护的区块链数字签名系统及使用流程，以解决上述背景技术中提出的问题。

为了实现上述目的，本发明提供了如下技术方案：

一种基于硬件加密保护的区块链数字签名系统，所述系统包括用户端、管理端、数字签名保护系统、硬件加密保护模块，所述用户端通过数字签名保护系统与硬件加密保护模块双向通讯连接，所述管理端通过数字签名保护系统与硬件加密保护模块双向通讯连接，所述用户端与外部区块链网络通信连接，所述管理端为离线系统，只能在本地或局域网进行访问，从而保障本系统的安全性。

进一步的，所述硬件加密保护模块为HSM硬件加密机或采用Intel SGX技术的CPU，HSM硬件加密机是一种实体的计算设备，可以是单独的硬件设备也可以是以硬件板卡形式安装在用户的计算机上， Intel SGX是对英特尔CPU技术体系的一个扩展，用于增强数据处理的安全性。Intel SGX的处理方式并不是识别和隔离操作系统上的所有恶意软件，而是将合法软件的安全操作封装在一个范围中，保护其不受恶意软件的攻击。借助Intel处理器的SGX技术，通过CPU的硬件模式切换，系统进入可信模式执行，只使用必需的硬件构成一个完全隔离的特权安全模式。Intel SGX技术可以提供HSM硬件加密机类似的安全处理功能，但大大节约了安装和制造成本，从而提高了本发明技术方案的应用性。

与现有技术相比，本发明的有益效果是：一种基于硬件加密保护的区块链数字签名系统及使用流程，通过硬件加密保护模块将用户私钥和签名规则与用户端隔离，使用时用户私钥和签名规则均位于硬件加密保护模块中，用户私钥位于硬件加密保护模块中持续在线，确保私用户钥安全和数字签名过程的安全可控的同时，能够很好地适应区块链技术条件下高频交易、多用户交易场景，防范攻击者，另外用户私钥和签名规则储存时也是以加密形态存储在数字签名保护系统中，被他人盗取也无法直接获取其中的信息，安全程度高，可以防范包括内鬼对私钥的窃取和数字签名功能的劫持。

**附图说明**

图1为本发明设置初始化过程的流程示意图；

图2为本发明交易数据请求过程的流程示意图。

**具体实施方式**

下面结合具体实施例对本发明中的技术方案进行清楚、完整地描述，显然，所描述的实施例仅仅是本发明一部分实施例，而不是全部的实施例。基于本发明中的实施例，本领域普通技术人员在没有做出创造性劳动前提下所获得的所有其他实施例，都属于本发明保护的范围。

参考图1-2，数据的安全是相对的，不可能存在绝对安全的方案，例如用户的账号密码信息虽然被高强度加密保管，但仍可能在某些情况下，用户自己不小心泄露密码明文，此种情况将可能造成用户账户被完全控制，其情形将与用户本人操作相同，所以本发明的方案需要建立在一个基本的信任环境下来讨论安全防盗性，对于本发明的技术方案来说基本的使用环境是无需考虑用户的账户基本信息被自身原因明文方式泄露而被他人盗取，无需考虑签名后的认证交易数据D6的数据被更改，并且用户自主加入到签名规则中地址白名单里面的地址均是安全受信任的，不考虑地址白名单中安全问题（如受信人、熟人的盗取）。

本发明系统采用硬件加密保护技术来保障区块链数字签名的安全性，用户私钥和签名规则都存储在硬加加密保护模块中，可以有效防止外部入侵窃取，能够在私钥持续在线的情况下，确保私钥安全和数字签名过程的安全可控，能够很好地适应区块链技术条件下高频交易，并且用户私钥和签名规则在外部备份存储时也是以加密形式存在，即使存储器被入侵盗取，也无法解读和盗用，大大提高了区块链交易的安全性。

尽管已经示出和描述了本发明的实施例，对于本领域的普通技术人员而言，可以理解在不脱离本发明的原理和精神的情况下可以对这些实施例进行多种变化、修改、替换和变型，本发明的范围由所附权利要求及其等同物限定。

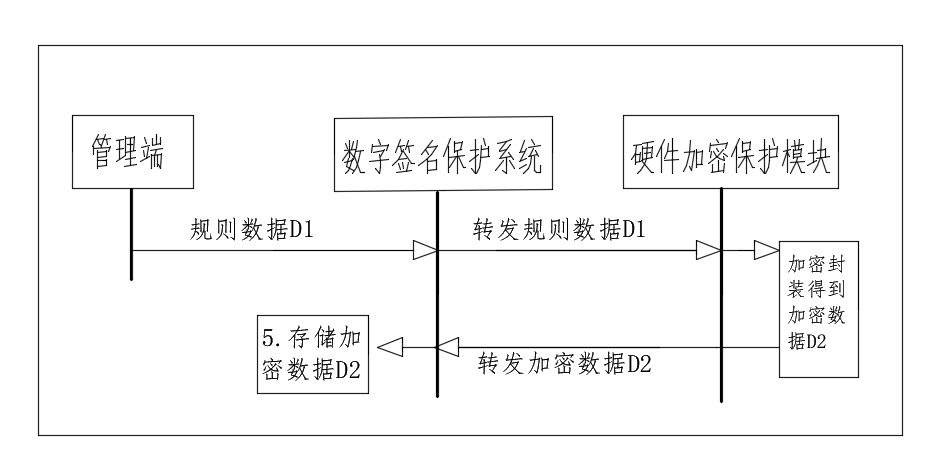


图1

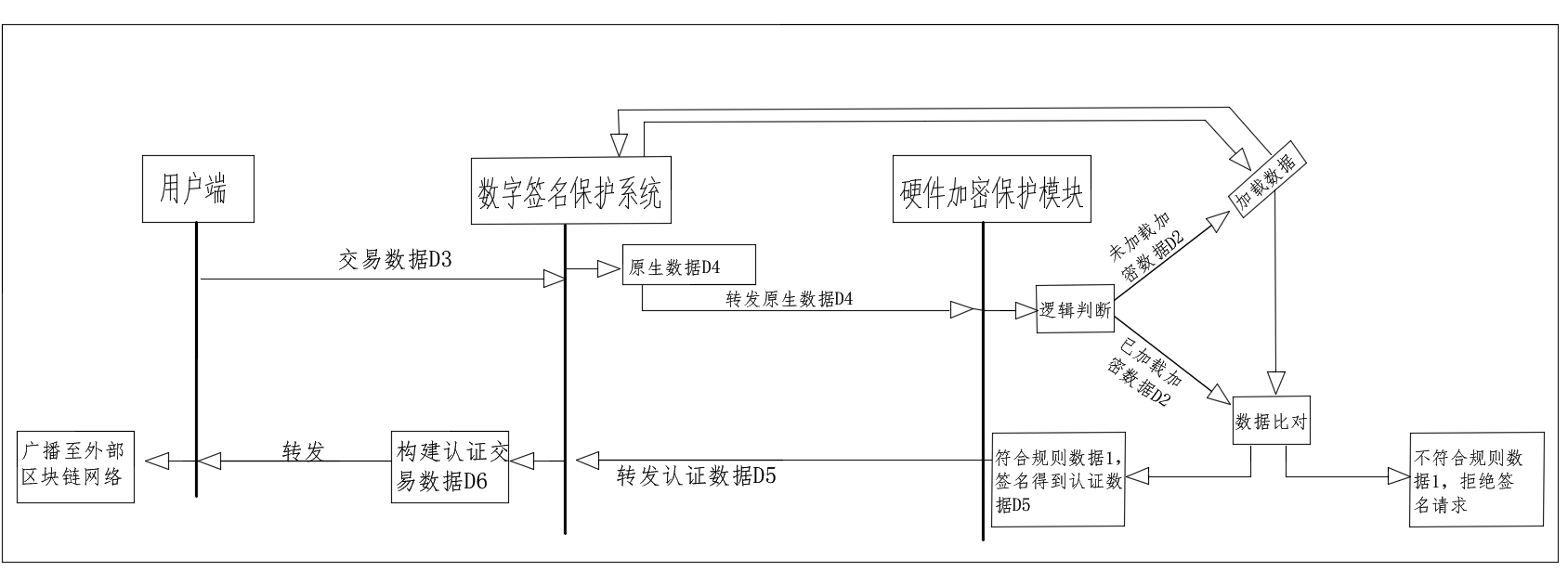


图2