(19)国家知识产权局

(12)发明专利申请

(10)申请公布号 CN 115550902 A
(43)申请公布日 2022.12.30

(21)申请号 202211346835.3

(22)申请日 2022.10.31

(71)申请人 中国联合网络通信集团有限公司
地址 100033 北京市西城区金融大街21号

(72)发明人 刘煜

(74)专利代理机构 北京天昊联合知识产权代理有限公司 11112
专利代理师 罗建民 杜丹丹

(51)Int.Cl.
H04W 8/18(2009.01)

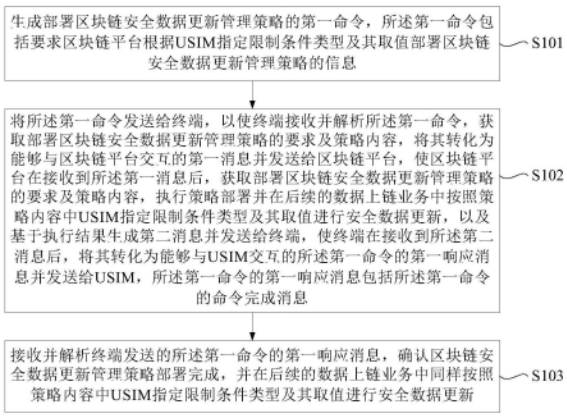
权利要求书5页 说明书24页 附图3页

(54)发明名称

安全数据更新方法、USIM、终端、设备及介质

(57)摘要

本发明提供一种安全数据更新方法、USIM、终端、设备及介质，涉及通信技术领域，其中方法包括：USIM生成部署区块链安全数据更新管理策略的第一命令并发送给终端，以使终端将第一命令转化为能够与区块链平台交互的第一消息并发送给区块链平台，使区块链平台执行策略部署并在后续的数据上链业务中按照策略内容更新安全数据，以及基于执行结果生成第二消息并发送给终端，使终端将第二消息转化为能够与USIM交互的第一命令的第一响应消息并发送给USIM；确认区块链安全数据更新管理策略部署完成，并在后续的数据上链业务中同样按照策略内容更新安全数据。本发明提供的技术方案实现了按照既定管理策略同步更新安全数据。



CN 115550902 A

1.一种安全数据更新方法,其特征在于,应用于通用用户识别模块USIM,所述方法包括:

生成部署区块链安全数据更新管理策略的第一命令,所述第一命令包括要求区块链平台根据USIM指定限制条件类型及其取值部署区块链安全数据更新管理策略的信息;

将所述第一命令发送给终端,以使终端接收并解析所述第一命令,获取部署区块链安全数据更新管理策略的要求及策略内容,将其转化为能够与区块链平台交互的第一消息并发送给区块链平台,使区块链平台在接收到所述第一消息后,获取部署区块链安全数据更新管理策略的要求及策略内容,执行策略部署并在后续的数据上链业务中按照策略内容中USIM指定限制条件类型及其取值进行安全数据更新,以及基于执行结果生成第二消息并发送给终端,使终端在接收到所述第二消息后,将其转化为能够与USIM交互的所述第一命令的第一响应消息并发送给USIM,所述第一命令的第一响应消息包括所述第一命令的命令完成消息;以及,

接收并解析终端发送的所述第一命令的第一响应消息,确认区块链安全数据更新管理策略部署完成,并在后续的数据上链业务中同样按照策略内容中USIM指定限制条件类型及其取值进行安全数据更新。

2.根据权利要求1所述的方法,其特征在于,所述USIM指定限制条件类型包括:区块链安全数据的使用时长、使用区块链安全数据上链的数据轮次,以及使用区块链安全数据上链的数据量中的一种或多种。

3.根据权利要求1所述的方法,其特征在于,所述第一命令还包括是否允许区块链平台对策略内容提出修正建议的信息;

在将所述第一命令发送给终端之后,还包括:

接收并解析终端发送的所述第一命令的第二响应消息;其中区块链平台在接收到所述第一消息后,响应于所述第一命令不允许区块链平台对策略内容提出修正建议,部署原有区块链安全数据更新管理策略并向终端发送所述第二消息,使终端在接收到所述第二消息后,将其转化为能够与USIM交互的所述第一命令的第一响应消息并发送给USIM,或者响应于所述第一命令允许区块链平台对策略内容提出修正建议,生成针对USIM指定限制条件类型的取值的修正建议,并发送给终端,使终端在接收到所述修正建议后,将其转化为能够与USIM交互的所述第一命令的第二响应消息并返回给USIM,所述第一命令的第二响应消息包括区块链平台对策略内容提出的修正建议;以及,

按照所述第一命令的第二响应消息中的修正建议部署新的区块链安全数据更新管理策略,并在后续的数据上链业务中按照新的策略内容中修正后的USIM指定限制条件类型的取值进行安全数据更新。

4.根据权利要求3所述的方法,其特征在于,在接收并解析终端发送的所述第一命令的第二响应消息之后,还包括:

判断USIM是否同意区块链平台对策略内容提出的修正建议;

响应于USIM同意区块链平台对策略内容提出的修正建议,根据区块链平台针对USIM指定限制条件类型的取值的修正建议生成第二命令,所述第二命令要求区块链平台根据修正后的USIM指定限制条件类型的取值部署新的区块链安全数据更新管理策略且不允许区块链平台再提出修正建议,并将所述第二命令发送给终端,以使终端接收并解析所述第二命

令,获取部署新的区块链安全数据更新管理策略及不允许区块链平台再提出修正建议的要求,将其转化为能够与区块链平台交互的第三消息并发送给区块链平台,使区块链平台在接收到所述第三消息后,获取部署新的区块链安全数据更新管理策略及不允许区块链平台再提出修正建议的要求,执行新的策略部署并在后续的数据上链业务中按照新的策略内容中修正后的USIM指定限制条件类型的取值进行安全数据更新,以及基于执行结果生成第四消息并发送给终端,使终端在接收到所述第四消息后,将其转化为能够与USIM交互的所述第二命令的响应消息并发送给USIM,所述第二命令的响应消息包括所述第二命令的命令完成消息;以及,

接收并解析终端发送的所述第二命令的响应消息,确认新的区块链安全数据更新管理策略部署完成。

5.根据权利要求4所述的方法,其特征在于,还包括:

响应于USIM不同意区块链平台对策略内容提出的修正建议,生成第三命令,所述第三命令要求区块链平台部署原有区块链安全数据更新管理策略且不允许区块链平台再提出修正建议,并将所述第三命令发送给终端,以使终端接收并解析所述第三命令,获取部署原有区块链安全数据更新管理策略及不允许区块链平台再提出修正建议的要求,将其转化为能够与区块链平台交互的第五消息并发送给区块链平台,使区块链平台在接收到所述第五消息后,获取部署原有区块链安全数据更新管理策略及不允许区块链平台再提出修正建议的要求,执行原有策略部署并在后续的数据上链业务中按照原有策略内容中USIM指定限制条件类型及其取值进行安全数据更新,以及基于执行结果生成第六消息并发送给终端,使终端在接收到所述第六消息后,将其转化为能够与USIM交互的所述第三命令的响应消息并发送给USIM,所述第三命令的响应消息包括所述第三命令的命令完成消息;以及,

接收并解析终端发送的所述第三命令的响应消息,确认原有区块链安全数据更新管理策略部署完成,并在后续的数据上链业务中同样按照原有策略内容中USIM指定限制条件类型及其取值进行安全数据更新。

6.一种安全数据更新方法,其特征在于,应用于终端,所述方法包括:

接收通用用户识别模块USIM发送的第一命令,其中USIM生成部署区块链安全数据更新管理策略的第一命令并发送给终端,所述第一命令包括要求区块链平台根据USIM指定限制条件类型及其取值部署区块链安全数据更新管理策略的信息;

解析所述第一命令,获取部署区块链安全数据更新管理策略的要求及策略内容,将其转化为能够与区块链平台交互的第一消息并发送给区块链平台,以使区块链平台在接收到所述第一消息后,获取部署区块链安全数据更新管理策略的要求及策略内容,执行策略部署并在后续的数据上链业务中按照策略内容中USIM指定限制条件类型及其取值进行安全数据更新,以及基于执行结果生成第二消息并发送给终端;

接收区块链平台发送的所述第二消息,将其转化为能够与USIM交互的所述第一命令的第一响应消息并发送给USIM,所述第一命令的第一响应消息包括所述第一命令的命令完成消息,以使USIM接收并解析终端发送的所述第一命令的第一响应消息,确认区块链安全数据更新管理策略部署完成,并在后续的数据上链业务中同样按照策略内容中USIM指定限制条件类型及其取值进行安全数据更新。

7.根据权利要求6所述的方法,其特征在于,所述USIM指定限制条件类型包括:区块链

安全数据的使用时长、使用区块链安全数据上链的数据轮次，以及使用区块链安全数据上链的数据量中的一种或多种。

8.根据权利要求6所述的方法，其特征在于，所述第一命令还包括是否允许区块链平台对策略内容提出修正建议的信息；

在将所述第一消息发送给区块链平台之后，还包括：

接收区块链平台发送的修正建议；其中区块链平台在接收到终端发送的所述第一消息后，判断所述第一命令是否允许区块链平台对策略内容提出修正建议，若允许，则生成针对USIM指定限制条件类型的取值的修正建议并发送给终端，若不允许，则部署原有区块链安全数据更新管理策略并向终端发送所述第二消息；

将所述修正建议转化为能够与USIM交互的所述第一命令的第二响应消息并返回给USIM，所述第一命令的第二响应消息包括区块链平台对策略内容提出的修正建议，以使USIM按照所述第一命令的第二响应消息中的修正建议部署新的区块链安全数据更新管理策略，并在后续的数据上链业务中按照新的策略内容中修正后的USIM指定限制条件类型的取值进行安全数据更新。

9.根据权利要求8所述的方法，其特征在于，在将所述第一命令的第二响应消息返回给USIM之后，还包括：

接收USIM发送的第二命令，其中USIM在接收到终端发送的所述第一命令的第二响应消息之后，判断USIM是否同意区块链平台对策略内容提出的修正建议，若同意，则根据区块链平台针对USIM指定限制条件类型的取值的修正建议生成第二命令，所述第二命令要求区块链平台根据修正后的USIM指定限制条件类型的取值部署新的区块链安全数据更新管理策略且不允许区块链平台再提出修正建议，并将所述第二命令发送给终端；

解析所述第二命令，获取部署新的区块链安全数据更新管理策略及不允许区块链平台再提出修正建议的要求，将其转化为能够与区块链平台交互的第三消息并发送给区块链平台，以使区块链平台在接收到所述第三消息后，获取部署新的区块链安全数据更新管理策略及不允许区块链平台再提出修正建议的要求，执行新的策略部署并在后续的数据上链业务中按照新的策略内容中修正后的USIM指定限制条件类型的取值进行安全数据更新，以及基于执行结果生成第四消息并发送给终端；

接收区块链平台发送的所述第四消息，将其转化为能够与USIM交互的所述第二命令的响应消息并发送给USIM，所述第二命令的响应消息包括所述第二命令的命令完成消息，以使USIM接收并解析终端发送的所述第二命令的响应消息，确认新的区块链安全数据更新管理策略部署完成，并在后续的数据上链业务中同样按照新的策略内容中修正后的USIM指定限制条件类型的取值进行安全数据更新。

10.根据权利要求8所述的方法，其特征在于，将所述第一命令的第二响应消息返回给USIM之后，还包括：

接收USIM发送的第三命令，其中USIM在接收到终端发送的所述第一命令的第二响应消息之后，判断USIM是否同意区块链平台对策略内容提出的修正建议，若不同意，则生成第三命令，所述第三命令要求区块链平台部署原有区块链安全数据更新管理策略且不允许区块链平台再提出修正建议，并将所述第三命令发送给终端；

解析所述第三命令，获取部署原有区块链安全数据更新管理策略及不允许区块链平台

再提出修正建议的要求,将其转化为能够与区块链平台交互的第五消息并发送给区块链平台,以使区块链平台在接收到所述第五消息后,获取部署原有区块链安全数据更新管理策略及不允许区块链平台再提出修正建议的要求,执行原有策略部署并在后续的数据上链业务中按照原有策略内容中USIM指定限制条件类型及其取值进行安全数据更新,以及基于执行结果生成第六消息并发送给终端;

接收区块链平台发送的所述第六消息,将其转化为能够与USIM交互的所述第三命令的响应消息并发送给USIM,所述第三命令的响应消息包括所述第三命令的命令完成消息,以使USIM接收并解析终端发送的所述第三命令的响应消息,确认原有区块链安全数据更新管理策略部署完成,并在后续的数据上链业务中同样按照原有策略内容中USIM指定限制条件类型及其取值进行安全数据更新。

11.一种通用用户识别模块USIM,其特征在于,包括:

命令生成模块,其设置为生成部署区块链安全数据更新管理策略的第一命令,所述第一命令包括要求区块链平台根据USIM指定限制条件类型及其取值部署区块链安全数据更新管理策略的信息;

第一发送模块,其设置为将所述第一命令发送给终端,以使终端接收并解析所述第一命令,获取部署区块链安全数据更新管理策略的要求及策略内容,将其转化为能够与区块链平台交互的第一消息并发送给区块链平台,使区块链平台在接收到所述第一消息后,获取部署区块链安全数据更新管理策略的要求及策略内容,执行策略部署并在后续的数据上链业务中按照策略内容中USIM指定限制条件类型及其取值进行安全数据更新,以及基于执行结果生成第二消息并发送给终端,使终端在接收到所述第二消息后,将其转化为能够与USIM交互的所述第一命令的第一响应消息并发送给USIM,所述第一命令的第一响应消息包括所述第一命令的命令完成消息;

第一接收模块,其设置为接收并解析终端发送的所述第一命令的第一响应消息,确认区块链安全数据更新管理策略部署完成;以及,

执行模块,其设置为在后续的数据上链业务中同样按照策略内容中USIM指定限制条件类型及其取值进行安全数据更新。

12.一种与通用用户识别模块USIM交互的终端,其特征在于,包括:

第二接收模块,其设置为接收USIM发送的第一命令,其中USIM生成部署区块链安全数据更新管理策略的第一命令并发送给终端,所述第一命令包括要求区块链平台根据USIM指定限制条件类型及其取值部署区块链安全数据更新管理策略的信息;以及,解析所述第一命令,获取部署区块链安全数据更新管理策略的要求及策略内容;

转化模块,其设置为将所述部署区块链安全数据更新管理策略的要求及策略内容转化为能够与区块链平台交互的第一消息;以及,

第二发送模块,其设置为将所述第一消息发送给区块链平台,以使区块链平台在接收到所述第一消息后,获取部署区块链安全数据更新管理策略的要求及策略内容,执行策略部署并在后续的数据上链业务中按照策略内容中USIM指定限制条件类型及其取值进行安全数据更新,以及基于执行结果生成第二消息并发送给终端;

所述第二接收模块还设置为,接收区块链平台发送的所述第二消息,将其转化为能够与USIM交互的所述第一命令的第一响应消息;

所述第二发送模块还设置为，将所述第一命令的第一响应消息发送给USIM，所述第一命令的第一响应消息包括所述第一命令的命令完成消息，以使USIM接收并解析终端发送的所述第一命令的第一响应消息，确认区块链安全数据更新管理策略部署完成，并在后续的数据上链业务中同样按照策略内容中USIM指定限制条件类型及其取值进行安全数据更新。

13.一种计算机设备，其特征在于，包括存储器和处理器，所述存储器中存储有计算机程序，当所述处理器运行所述存储器存储的计算机程序时，所述处理器执行根据权利要求1至5中任一项所述的安全数据更新方法，或者根据权利要求6至10中任一项所述的安全数据更新方法。

14.一种计算机可读存储介质，其上存储有计算机程序，其特征在于，所述计算机程序被处理器执行时，所述处理器执行根据权利要求1至5中任一项所述的安全数据更新方法，或者根据权利要求6至10中任一项所述的安全数据更新方法。

安全数据更新方法、USIM、终端、设备及介质

技术领域

[0001] 本发明涉及通信技术领域，尤其涉及一种安全数据更新方法、一种USIM、一种终端、一种计算机设备以及一种计算机可读存储介质。

背景技术

[0002] 现有技术中，终端加入区块链并提交数据上链，USIM(Universal Subscriber Identity Module，通用用户识别模块)因其在安全能力方面的优势，可以在数据上链过程中提供必要的安全保障，通过存储的密钥、证书等关键安全数据为上链流程提供数字签名。其中密钥的生成和证书的签发都是在终端加入区块链时完成的，为后续数据上链时使用，并在终端上链后的全周期中保持稳定。

[0003] 固定不变的关键安全数据的实现方式比较简单，可以满足数据上链的基本安全需求，但同时也存在一定的潜在风险，不仅长时间的使用增加了泄露、破解等风险的可能性，而且一旦安全事件发生，则波及范围会比较大，同时也缺少必要的防范和应对预案。为进一步提升区块链中此类数据管理的安全性和可靠性，有必要引入相对复杂的关键安全数据管理方式和机制，以更为灵活机动和合理多样的策略加强安全数据保护的效率和质量，然而现有技术尚缺乏相关实现方案，尤其是作为关键安全数据承载主体的USIM，本应在关键安全数据管理策略方面发挥更大的作用，目前也缺少可行的实现方法。

发明内容

[0004] 为了至少部分解决现有技术中存在的因终端对提交至区块链的数据进行数字签名所采用的关键安全数据在终端加入区块链后的全周期中保持不变而导致存在安全风险的技术问题而完成了本发明。

[0005] 根据本发明的一方面，提供一种安全数据更新方法，应用于通用用户识别模块USIM，所述方法包括：

[0006] 生成部署区块链安全数据更新管理策略的第一命令，所述第一命令包括要求区块链平台根据USIM指定限制条件类型及其取值部署区块链安全数据更新管理策略的信息；

[0007] 将所述第一命令发送给终端，以使终端接收并解析所述第一命令，获取部署区块链安全数据更新管理策略的要求及策略内容，将其转化为能够与区块链平台交互的第一消息并发送给区块链平台，使区块链平台在接收到所述第一消息后，获取部署区块链安全数据更新管理策略的要求及策略内容，执行策略部署并在后续的数据上链业务中按照策略内容中USIM指定限制条件类型及其取值进行安全数据更新，以及基于执行结果生成第二消息并发送给终端，使终端在接收到所述第二消息后，将其转化为能够与USIM交互的所述第一命令的第一响应消息并发送给USIM，所述第一命令的第一响应消息包括所述第一命令的命令完成消息；以及，

[0008] 接收并解析终端发送的所述第一命令的第一响应消息，确认区块链安全数据更新管理策略部署完成，并在后续的数据上链业务中同样按照策略内容中USIM指定限制条件类

型及其取值进行安全数据更新。

[0009] 可选地,所述USIM指定限制条件类型包括:区块链安全数据的使用时长、使用区块链安全数据上链的数据轮次,以及使用区块链安全数据上链的数据量中的一种或多种。

[0010] 可选地,所述第一命令还包括是否允许区块链平台对策略内容提出修正建议的信息;

[0011] 在将所述第一命令发送给终端之后,还包括:

[0012] 接收并解析终端发送的所述第一命令的第二响应消息;其中区块链平台在接收到所述第一消息后,响应于所述第一命令不允许区块链平台对策略内容提出修正建议,部署原有区块链安全数据更新管理策略并向终端发送所述第二消息,使终端在接收到所述第二消息后,将其转化为能够与USIM交互的所述第一命令的第一响应消息并发送给USIM,或者响应于所述第一命令允许区块链平台对策略内容提出修正建议,生成针对USIM指定限制条件类型的取值的修正建议,并发送给终端,使终端在接收到所述修正建议后,将其转化为能够与USIM交互的所述第一命令的第二响应消息并返回给USIM,所述第一命令的第二响应消息包括区块链平台对策略内容提出的修正建议;以及,

[0013] 按照所述第一命令的第二响应消息中的修正建议部署新的区块链安全数据更新管理策略,并在后续的数据上链业务中按照新的策略内容中修正后的USIM指定限制条件类型的取值进行安全数据更新。

[0014] 可选地,在接收并解析终端发送的所述第一命令的第二响应消息之后,还包括:

[0015] 判断USIM是否同意区块链平台对策略内容提出的修正建议;

[0016] 响应于USIM同意区块链平台对策略内容提出的修正建议,根据区块链平台针对USIM指定限制条件类型的取值的修正建议生成第二命令,所述第二命令要求区块链平台根据修正后的USIM指定限制条件类型的取值部署新的区块链安全数据更新管理策略且不允许区块链平台再提出修正建议,并将所述第二命令发送给终端,以使终端接收并解析所述第二命令,获取部署新的区块链安全数据更新管理策略及不允许区块链平台再提出修正建议的要求,将其转化为能够与区块链平台交互的第三消息并发送给区块链平台,使区块链平台在接收到所述第三消息后,获取部署新的区块链安全数据更新管理策略及不允许区块链平台再提出修正建议的要求,执行新的策略部署并在后续的数据上链业务中按照新的策略内容中修正后的USIM指定限制条件类型的取值进行安全数据更新,以及基于执行结果生成第四消息并发送给终端,使终端在接收到所述第四消息后,将其转化为能够与USIM交互的所述第二命令的响应消息并发送给USIM,所述第二命令的响应消息包括所述第二命令的命令完成消息;以及,

[0017] 接收并解析终端发送的所述第二命令的响应消息,确认新的区块链安全数据更新管理策略部署完成。

[0018] 可选地,所述方法还包括:

[0019] 响应于USIM不同意区块链平台对策略内容提出的修正建议,生成第三命令,所述第三命令要求区块链平台部署原有区块链安全数据更新管理策略且不允许区块链平台再提出修正建议,并将所述第三命令发送给终端,以使终端接收并解析所述第三命令,获取部署原有区块链安全数据更新管理策略及不允许区块链平台再提出修正建议的要求,将其转化为能够与区块链平台交互的第五消息并发送给区块链平台,使区块链平台在接收到所述

第五消息后,获取部署原有区块链安全数据更新管理策略及不允许区块链平台再提出修正建议的要求,执行原有策略部署并在后续的数据上链业务中按照原有策略内容中USIM指定限制条件类型及其取值进行安全数据更新,以及基于执行结果生成第六消息并发送给终端,使终端在接收到所述第六消息后,将其转化为能够与USIM交互的所述第三命令的响应消息并发送给USIM,所述第三命令的响应消息包括所述第三命令的命令完成消息;以及,

[0020] 接收并解析终端发送的所述第三命令的响应消息,确认原有区块链安全数据更新管理策略部署完成,并在后续的数据上链业务中同样按照原有策略内容中USIM指定限制条件类型及其取值进行安全数据更新。

[0021] 根据本发明的另一方面,提供一种安全数据更新方法,应用于与USIM交互的终端,所述方法包括:

[0022] 接收通用用户识别模块USIM发送的第一命令,其中USIM生成部署区块链安全数据更新管理策略的第一命令并发送给终端,所述第一命令包括要求区块链平台根据USIM指定限制条件类型及其取值部署区块链安全数据更新管理策略的信息;

[0023] 解析所述第一命令,获取部署区块链安全数据更新管理策略的要求及策略内容,将其转化为能够与区块链平台交互的第一消息并发送给区块链平台,以使区块链平台在接收到所述第一消息后,获取部署区块链安全数据更新管理策略的要求及策略内容,执行策略部署并在后续的数据上链业务中按照策略内容中USIM指定限制条件类型及其取值进行安全数据更新,以及基于执行结果生成第二消息并发送给终端;

[0024] 接收区块链平台发送的所述第二消息,将其转化为能够与USIM交互的所述第一命令的第一响应消息并发送给USIM,所述第一命令的第一响应消息包括所述第一命令的命令完成消息,以使USIM接收并解析终端发送的所述第一命令的第一响应消息,确认区块链安全数据更新管理策略部署完成,并在后续的数据上链业务中同样按照策略内容中USIM指定限制条件类型及其取值进行安全数据更新。

[0025] 可选地,所述USIM指定限制条件类型包括:区块链安全数据的使用时长、使用区块链安全数据上链的数据轮次,以及使用区块链安全数据上链的数据量中的一种或多种。

[0026] 可选地,所述第一命令还包括是否允许区块链平台对策略内容提出修正建议的信息;

[0027] 在将所述第一消息发送给区块链平台之后,还包括:

[0028] 接收区块链平台发送的修正建议;其中区块链平台在接收到终端发送的所述第一消息后,判断所述第一命令是否允许区块链平台对策略内容提出修正建议,若允许,则生成针对USIM指定限制条件类型的取值的修正建议并发送给终端,若不允许,则部署原有区块链安全数据更新管理策略并向终端发送所述第二消息;

[0029] 将所述修正建议转化为能够与USIM交互的所述第一命令的第二响应消息并返回给USIM,所述第一命令的第二响应消息包括区块链平台对策略内容提出的修正建议,以使USIM按照所述第一命令的第二响应消息中的修正建议部署新的区块链安全数据更新管理策略,并在后续的数据上链业务中按照新的策略内容中修正后的USIM指定限制条件类型的取值进行安全数据更新。

[0030] 可选地,在将所述第一命令的第二响应消息返回给USIM之后,还包括:

[0031] 接收USIM发送的第二命令,其中USIM在接收到终端发送的所述第一命令的第二响

应消息之后，判断USIM是否同意区块链平台对策略内容提出的修正建议，若同意，则根据区块链平台针对USIM指定限制条件类型的取值的修正建议生成第二命令，所述第二命令要求区块链平台根据修正后的USIM指定限制条件类型的取值部署新的区块链安全数据更新管理策略且不允许区块链平台再提出修正建议，并将所述第二命令发送给终端；

[0032] 解析所述第二命令，获取部署新的区块链安全数据更新管理策略及不允许区块链平台再提出修正建议的要求，将其转化为能够与区块链平台交互的第三消息并发送给区块链平台，以使区块链平台在接收到所述第三消息后，获取部署新的区块链安全数据更新管理策略及不允许区块链平台再提出修正建议的要求，执行新的策略部署并在后续的数据上链业务中按照新的策略内容中修正后的USIM指定限制条件类型的取值进行安全数据更新，以及基于执行结果生成第四消息并发送给终端；

[0033] 接收区块链平台发送的所述第四消息，将其转化为能够与USIM交互的所述第二命令的响应消息并发送给USIM，所述第二命令的响应消息包括所述第二命令的命令完成消息，以使USIM接收并解析终端发送的所述第二命令的响应消息，确认新的区块链安全数据更新管理策略部署完成，并在后续的数据上链业务中同样按照新的策略内容中修正后的USIM指定限制条件类型的取值进行安全数据更新。

[0034] 可选地，将所述第一命令的第二响应消息返回给USIM之后，还包括：

[0035] 接收USIM发送的第三命令，其中USIM在接收到终端发送的所述第一命令的第二响应消息之后，判断USIM是否同意区块链平台对策略内容提出的修正建议，若不同意，则生成第三命令，所述第三命令要求区块链平台部署原有区块链安全数据更新管理策略且不允许区块链平台再提出修正建议，并将所述第三命令发送给终端；

[0036] 解析所述第三命令，获取部署原有区块链安全数据更新管理策略及不允许区块链平台再提出修正建议的要求，将其转化为能够与区块链平台交互的第五消息并发送给区块链平台，以使区块链平台在接收到所述第五消息后，获取部署原有区块链安全数据更新管理策略及不允许区块链平台再提出修正建议的要求，执行原有策略部署并在后续的数据上链业务中按照原有策略内容中USIM指定限制条件类型及其取值进行安全数据更新，以及基于执行结果生成第六消息并发送给终端；

[0037] 接收区块链平台发送的所述第六消息，将其转化为能够与USIM交互的所述第三命令的响应消息并发送给USIM，所述第三命令的响应消息包括所述第三命令的命令完成消息，以使USIM接收并解析终端发送的所述第三命令的响应消息，确认原有区块链安全数据更新管理策略部署完成，并在后续的数据上链业务中同样按照原有策略内容中USIM指定限制条件类型及其取值进行安全数据更新。

[0038] 根据本发明的又一方面，提供一种通用用户识别模块USIM，包括：

[0039] 命令生成模块，其设置为生成部署区块链安全数据更新管理策略的第一命令，所述第一命令包括要求区块链平台根据USIM指定限制条件类型及其取值部署区块链安全数据更新管理策略的信息；

[0040] 第一发送模块，其设置为将所述第一命令发送给终端，以使终端接收并解析所述第一命令，获取部署区块链安全数据更新管理策略的要求及策略内容，将其转化为能够与区块链平台交互的第一消息并发送给区块链平台，使区块链平台在接收到所述第一消息后，获取部署区块链安全数据更新管理策略的要求及策略内容，执行策略部署并在后续的

数据上链业务中按照策略内容中USIM指定限制条件类型及其取值进行安全数据更新，以及基于执行结果生成第二消息并发送给终端，使终端在接收到所述第二消息后，将其转化为能够与USIM交互的所述第一命令的第一响应消息并发送给USIM，所述第一命令的第一响应消息包括所述第一命令的命令完成消息；

[0041] 第一接收模块，其设置为接收并解析终端发送的所述第一命令的第一响应消息，确认区块链安全数据更新管理策略部署完成；以及，

[0042] 执行模块，其设置为在后续的数据上链业务中同样按照策略内容中USIM指定限制条件类型及其取值进行安全数据更新。

[0043] 根据本发明的再一方面，提供一种与USIM交互的终端，包括：

[0044] 第二接收模块，其设置为接收USIM发送的第一命令，其中USIM生成部署区块链安全数据更新管理策略的第一命令并发送给终端，所述第一命令包括要求区块链平台根据USIM指定限制条件类型及其取值部署区块链安全数据更新管理策略的信息；以及，解析所述第一命令，获取部署区块链安全数据更新管理策略的要求及策略内容；

[0045] 转化模块，其设置为将所述部署区块链安全数据更新管理策略的要求及策略内容转化为能够与区块链平台交互的第一消息；以及，

[0046] 第二发送模块，其设置为将所述第一消息发送给区块链平台，以使区块链平台在接收到所述第一消息后，获取部署区块链安全数据更新管理策略的要求及策略内容，执行策略部署并在后续的数据上链业务中按照策略内容中USIM指定限制条件类型及其取值进行安全数据更新，以及基于执行结果生成第二消息并发送给终端；

[0047] 所述第二接收模块还设置为，接收区块链平台发送的所述第二消息，将其转化为能够与USIM交互的所述第一命令的第一响应消息；

[0048] 所述第二发送模块还设置为，将所述第一命令的第一响应消息发送给USIM，所述第一命令的第一响应消息包括所述第一命令的命令完成消息，以使USIM接收并解析终端发送的所述第一命令的第一响应消息，确认区块链安全数据更新管理策略部署完成，并在后续的数据上链业务中同样按照策略内容中USIM指定限制条件类型及其取值进行安全数据更新。

[0049] 根据本发明的还一方面，提供一种计算机设备，包括存储器和处理器，所述存储器中存储有计算机程序，当所述处理器运行所述存储器存储的计算机程序时，所述处理器执行前述安全数据更新方法。

[0050] 根据本发明的还一方面，提供一种计算机可读存储介质，其上存储有计算机程序，所述计算机程序被处理器执行时，所述处理器执行前述安全数据更新方法。

[0051] 本发明提供的技术方案可以包括以下有益效果：

[0052] 本发明提供的安全数据更新方法，通过USIM生成部署区块链安全数据更新管理策略的第一命令并发送给终端，由终端转化为能够与区块链平台交互的第一消息后发送给区块链平台，区块链平台根据第一命令的要求执行策略部署并基于执行结果生成第二消息后发送给终端，由终端转化为能够与USIM交互的第一命令的第一响应消息后发送给USIM，USIM接收到第一命令的第一响应消息后确认区块链安全数据更新管理策略部署完成，使得USIM和区块链平台都可以在后续的数据上链业务中按照同样的策略内容中USIM指定限制条件类型及其取值进行安全数据更新，实现了USIM和区块链平台都可以按照既定管理策略

自行同步更新安全数据，解决了现有技术中存在的因终端对提交至区块链的数据进行数字签名所采用的关键安全数据在终端上链后的全周期中保持不变而导致存在安全风险的问题。

[0053] 本发明的其它特征和优点将在随后的说明书中阐述，并且，部分地从说明书中变得显而易见，或者通过实施本发明而了解。本发明的目的和其他优点可通过在说明书、权利要求书以及附图中所特别指出的结构来实现和获得。

附图说明

[0054] 附图用来提供对本发明技术方案的进一步理解，并且构成说明书的一部分，与本发明的实施例一起用于解释本发明的技术方案，并不构成对本发明技术方案的限制。

[0055] 图1为本发明实施例提供的一种安全数据更新方法的流程示意图；

[0056] 图2为本发明实施例提供的另一种安全数据更新方法的流程示意图；

[0057] 图3为本发明实施例提供的又一种安全数据更新方法的流程示意图；

[0058] 图4为本发明实施例提供的USIM的结构示意图；

[0059] 图5为本发明实施例提供的终端的结构示意图；

[0060] 图6为本发明实施例提供的安全数据更新系统的结构示意图；

[0061] 图7为本发明实施例提供的计算机设备的结构示意图。

具体实施方式

[0062] 为使本发明实施例的目的、技术方案和优点更加清楚，以下结合附图对本发明的具体实施方式进行详细说明。应当理解的是，此处所描述的具体实施方式仅用于说明和解释本发明，并不用于限制本发明。

[0063] 区块链是一种分布式记账系统，它不再依赖于中心化，而是通过一种密码学计算使全网节点随机争夺记账权，记完后的账本发布给全网所有节点保存，区块链的区块被定义为一种具备一定信任机制、可执行读取或写入操作的数据集，其中包含交易及其它记录的确认、合约、存储、复制、安全等信息。区块链的核心应用能力主要包括三大特性，分别是：“去中心化”、“不可篡改”和“智能合约”。其中，“去中心化”特性是以无中心化的方式集体共享、维护数据体系，体系中每个节点的参与者都可根据自己的需求在权限范围内直接获取信息，而不需要中间平台传递。区块链的“不可篡改”特性旨在保证数据的稳定性和可靠性，降低数据被篡改的风险。而区块链的“智能合约”特性可一定程度上保障交易约定的可靠性。通过对分布式数据存储、点对点传输、共识机制、密码学和智能合约等技术的集成，区块链可有效地解决传统交易模式中的数据造假行为，被认为是构建未来可信任互联网的支撑性技术，受到了行业内的全面关注。区块链虽然最初从数字货币领域起源，但经过几年发展，目前已逐渐拓展到各个领域，包括供应链管理、征信系统、身份认证、物联网等。

[0064] 区块链可以分为公有链、联盟链和私有链等不同类别。公有链是可以完全开放的，大众都可以参与，联盟链是由若干个机构共同参与和管理的，私有链仅服务于某个组织或机构。从私有链、联盟链到公有链是去中心化的过程，而从公有链、联盟链到私有链则是中心化的过程。通常一个区块链至少分为三层：最底层是一些通用的基础模块，比如基础加密算法，网络通讯库，流处理，线程封装，消息封装与解码，系统时间等；中间一层是区块链的

核心模块,一般包含了区块链的主要逻辑,如P2P(peer to peer,点对点)网络协议,共识模块,交易处理模块,交易池模块,简单合约或者智能合约模块,嵌入式数据库处理模块,钱包模块等等;最上面一层,往往都是基于Json Standard RPC(Remote Procedure Call,远程过程调用)的交互模块,或可以做出Web Service(Web服务)等。如果区块链支持智能合约,可能还要分更多的层,比如增加BaaS层,区块链上的智能合约提供自治的服务。

[0065] USIM卡(Universal Subscriber Identity Module,通用用户识别模块)是UMTS(Universal Mobile Telecommunications System,通用移动通信系统)网络中使用的SIM卡(Subscriber Identity Module,用户识别模块)的延续与进步,用于存储用户身份信息和个人数据,保障接入移动网络服务的安全,可以利用必要的功能和数据,在用户访问移动网络服务时进行用户识别和用户授权,实现移动网络能够表示和识别用户应用的要求。USAT(USIM Application Toolkit,USIM应用工具箱)协议是USIM支持的一种服务机制,在传输层提供的服务基础之上实现,改变了原有USIM相对于终端处于被动地位,只能被动执行终端命令而无法主动向终端提出的命令要求的状态,USAT允许USIM应用与支持这种机制的终端进行交互和操作,使得USIM可以主动要求终端执行某个操作,USAT是电信智能卡通过终端实现业务的基础和主要方式。

[0066] 因为USIM在安全能力方面的优势,USIM与区块链可以相互结合,利用USIM为区块链提供信任根,使区块链应用具备更有效的安全保障,在此类方案中,通常需要实现终端的设备上链和数据上链,终端应用采集或生成数据,提供上链功能,USIM为上链提供证书存储、数字签名等服务,加强终端和终端数据的上链的安全性。然而,现有技术中终端对提交至区块链的数据进行数字签名所采用的安全数据的生成和部署是由终端上链行为触发,USIM在安全数据配置上只能被动接受终端和区块链平台管理,缺乏灵活性,且存在安全风险。为解决这一问题,本发明提出了一种USIM和区块链平台都可以按照既定管理策略自行同步更新安全数据的方案,该方案以USIM为主体,依据必要的管理策略对区块链安全数据实现常态化、规律性地有序更新和调整,改变目前安全数据固定不变的状态,加强安全数据的自我保护和自我修复的机制,一定程度上克服现有方式带来的易泄露、易破解等缺陷,并提升对风险事件发生前的防范能力和发生后的处置能力。下面通过具体的实施例予以详细描述。

[0067] 需要说明的是,本发明的说明书和权利要求书及上述附图中的术语“第一”、“第二”等是用于区别类似的对象,而不必用于描述特定的顺序或先后次序;并且,在不冲突的情况下,本发明中的实施例及实施例中的特征可以相互任意组合。

[0068] 在后续的描述中,使用用于表示元件的诸如“模块”、“部件”或“单元”的后缀仅为了有利于本发明的说明,其本身没有特定的意义。因此,“模块”、“部件”或“单元”可以混合地使用。

[0069] 图1为本发明实施例提供的一种安全数据更新方法的流程示意图。所述方法应用于USIM,如图1所示,所述方法包括如下步骤S101至S103。

[0070] S101.生成部署区块链安全数据更新管理策略的第一命令,所述第一命令包括要求区块链平台根据USIM指定限制条件类型及其取值部署区块链安全数据更新管理策略的信息。其中,区块链安全数据包括密钥、证书等。

[0071] 本实施例中,在USIM区块链应用的安全数据(如密钥、证书等)需要按照既定策略

进行更新时,就产生了部署区块链安全数据更新管理策略的需求,则USIM就可根据需求的具体内容(包括进行区块链安全数据更新的限制条件类型及其取值)生成部署区块链安全数据更新管理策略的第一命令,命令表示要求区块链平台在根据USIM指定限制条件类型及其取值部署区块链安全数据更新管理策略,并在满足相应条件时自行进行安全数据更新。

[0072] 具体地,在所述区块链安全数据更新管理策略的内容中,USIM指定限制条件类型包括:区块链安全数据的使用时长、使用区块链安全数据上链的数据轮次,以及使用区块链安全数据上链的数据量中的一种或多种。其中,USIM指定限制条件类型为区块链安全数据的使用时长时,表示区块链安全数据的使用时间达到一定时长后更新安全数据,该类型限制条件的取值表示面向安全数据使用时长的策略指定的限制条件值,即区块链安全数据使用多久需更新安全数据;USIM指定限制条件类型为使用区块链安全数据上链的数据轮次时,表示使用区块链安全数据上链的数据轮次达到一定数量后更新安全数据,该类型限制条件的取值表示面向使用安全数据的上链数据轮次的策略指定的限制条件值,即使用区块链安全数据上链的数据轮次达到多少轮时需要更新安全数据;USIM指定限制条件类型为使用区块链安全数据上链的数据量时,表示使用区块链安全数据上链的数据量达到一定数量后更新安全数据,该类型限制条件的取值表示面向使用安全数据的上链数据数量的策略指定的限制条件值,即使用区块链安全数据上链的数据量达到多少时需要更新安全数据。

[0073] 为部署区块链安全数据更新管理策略,需要为USIM增加新的USAT命令,即前述“第一命令”,其功能是USIM要求区块链平台按照区块链安全数据更新管理策略来更新、调整区块链安全数据。新增的命令例如可以命名为Blockchain Security Data Policy,其具体定义可如下表1所示。

[0074] 表1

[0075]

描述	内容		M/O	MIN	长度(字节)
主动式UICC卡命令标记	D0		M	Y	1
长度	后续总长度		M	Y	1或2
命令细节	命令细节标记	01或81	M	Y	5
	长度	03			
	命令序号	01~FE			
	命令类型	95			
	命令限定符	b1：是否允许提出修正 0- 不允许提出修正建议 1- 允许提出修正建议 b2：是否存在面向时长的策略 0- 不允许面向时长的策略 1- 允许面向时长的策略 b3：是否存在面向数据轮次的策略 0- 不允许面向数据轮次的策略 1- 允许面向数据轮次的策略 b4：是否存在面向数据量的策略 2- 不允许面向数据量的策略 3- 允许面向数据量的策略 其余保留			
设备标识	设备标识标记	02或82	M	Y	4
	长度	02			
	起始端设备标识	81=USIM卡			
	目的端设备标识	82=终端			
时长	时长标记	04或84	M	Y	4
	长度	02			
	时间单位	00- 分 01- 秒 02- 1/10秒 其余保留			
	时间长度	单位长度数量：01-255 00保留			
区块链数据轮次	区块链数据轮次标记	60或E0	M	Y	3
	长度	01			
	区块链数据轮次	轮次数量：01-255 00保留			
区块链数据量	区块链数据；量标记	61或E1	M	Y	5
	长度	03			

[0076]

	区块链数据量单位	00- B 01- KB 02- MB 03- GB 其余保留			
	区块链数据量	数据量：01-1023 00保留			

[0077] 注：

[0078] 1)“命令限定符”表示本次命令的基本属性和要求，其中b1表示本次命令是否允许区块链平台针对USIM策略内容提出修正建议；b2表示本次命令是否存在面向安全数据使用时长的策略，如果存在，则安全数据需要在使用时间达到指定长度后更新调整；b3表示本次命令是否存在面向区块链数据轮次的策略，如果存在，则使用安全数据上链的数据达到指定轮次后安全数据需要更新调整；b4表示本次命令是否存在面向区块链数据量的策略，如果存在，则使用安全数据上链的数据达到指定数量后安全数据需要更新调整。各位具体取值含义见上表所示，其余位保留。需要指出的是，b2/b3/b4可以有多于一位的取值为1，表示两方面或三方面策略同时存在，当其中任一策略条件满足时安全数据均需更新调整，如安全数据使用一定时长或使用安全数据上链一定轮次时都需更新调整安全数据。

[0079] 2)“时长”为条件必选数据对象，当命令限定符b2＝1时必须存在，表示面向安全数据使用时长的策略指定的限制条件值，具体含义见上表1所示。

[0080] 3)“区块链数据轮次”为新增数据对象，条件必选，当命令限定符b3＝1时必须存在，表示面向使用安全数据的上链数据轮次的策略指定的限制条件值，具体含义见上表1所示。

[0081] 4)“区块链数据量”为新增数据对象，条件必选，当命令限定符b4＝1时必须存在，表示面向使用安全数据的上链数据数量的策略指定的限制条件值，具体含义见上表1所示。

[0082] S102.将所述第一命令发送给终端，以使终端接收并解析所述第一命令，获取部署区块链安全数据更新管理策略的要求及策略内容，将其转化为能够与区块链平台交互的第一消息并发送给区块链平台，使区块链平台在接收到所述第一消息后，获取部署区块链安全数据更新管理策略的要求及策略内容，执行策略部署并在后续的数据上链业务中按照策略内容中USIM指定限制条件类型及其取值进行安全数据更新，以及基于执行结果生成第二消息并发送给终端，使终端在接收到所述第二消息后，将其转化为能够与USIM交互的所述第一命令的第一响应消息并发送给USIM，所述第一命令的第一响应消息包括所述第一命令的命令完成消息。

[0083] 本步骤中，由于USIM与区块链平台不具备直接交互的关系，需要借助于终端实现信息传递，换言之，USIM向终端发送的命令并不是由终端直接转发给区块链平台，而是由终端处理命令内容后生成符合终端和区块链平台间的协议的消息(即第一消息)，区块链平台向终端发送的消息也不是由终端直接转发给USIM，而是由终端处理消息内容后生成符合终端和USIM间协议的响应消息(即第一命令的第一响应消息)，本发明中所有涉及的命令(含第一命令，以及后续的第二、第三命令)与命令的响应消息(含第一命令的第一响应消息，以及后续的第一命令的第二响应消息、第二命令的响应消息、第三命令的响应消息)均为终端和USIM之间的命令，而终端和区块链平台之间因为与终端和USIM之间的协议不同，所以并

不能直接转发,均需经过终端的处理和重新生成,所以USIM需要将第一命令发送给终端,终端在接收到第一命令后,对第一命令进行解析,获取部署区块链安全数据更新管理策略的要求和策略内容,将其转化为能够与区块链平台进行交互的第一消息并发送到区块链平台,区块链平台接收到第一消息后进行解析,获取部署区块链安全数据更新管理策略的要求和策略内容;区块链平台按照第一命令的要求,执行策略部署,在后续的数据上链业务中按照策略内容中所要求的USIM指定限制条件类型及其取值自行进行安全数据更新,基于执行结果生成第二消息并发送给终端,终端在接收到第二消息后,将其转化为能够与USIM交互的第一命令的第一响应消息并发送到USIM。

[0084] S103.接收并解析终端发送的所述第一命令的第一响应消息,确认区块链安全数据更新管理策略部署完成,并在后续的数据上链业务中同样按照策略内容中USIM指定限制条件类型及其取值进行安全数据更新。

[0085] 本步骤中,USIM在接收到终端返回的第一命令的第一响应消息后,确认区块链安全数据更新管理策略部署完成,那么USIM和区块链平台都可以在后续的数据上链业务中按照同样的策略内容中USIM指定限制条件类型及其取值进行安全数据更新,实现了USIM和区块链平台都可以按照既定管理策略自行同步更新安全数据。

[0086] 在一种具体实施方式中,所述第一命令还包括是否允许区块链平台对策略内容提出修正建议的信息。那么在前述产生的部署区块链安全数据更新管理策略的需求的具体内容中,还包括是否允许区块链平台对策略内容提出修正建议。

[0087] 相应地,在步骤S102之后,还包括如下步骤S104和S105。

[0088] S104.接收并解析终端发送的所述第一命令的第二响应消息;其中区块链平台在接收到所述第一消息后,响应于所述第一命令不允许区块链平台对策略内容提出修正建议,部署原有区块链安全数据更新管理策略并向终端发送所述第二消息,使终端在接收到所述第二消息后,将其转化为能够与USIM交互的所述第一命令的第一响应消息并发送给USIM;或者响应于所述第一命令允许区块链平台对策略内容提出修正建议,生成针对USIM指定限制条件类型的取值的修正建议,并发送给终端,使终端在接收到所述修正建议后,将其转化为能够与USIM交互的所述第一命令的第二响应消息并返回给USIM,所述第一命令的第二响应消息包括区块链平台对策略内容提出的修正建议。

[0089] 本步骤中,修正建议仅可针对第一命令中所提供的同样的限制条件类型的取值进行修改;相应地,所述第一命令的第二响应消息中包含区块链平台提供的建议修正的同类型限制条件的取值。

[0090] 终端在接收到区块链平台发送的修正建议后,通过所述第一命令的第二响应消息向USIM返回结果。所述第一命令的第二响应消息例如可以命名为Terminal Response(for Blockchain Security Data Policy),其具体定义可如下表2所示。

[0091] 表2

[0092]

描述	内容		M/O	MIN	长度(字节)
命令细节	命令细节标记	01或81	M	Y	5
	长度	03			
	命令代码	01~FE			

[0093]

	命令类型	95			
	命令限定符	同命令对应部分要求，取值与命令对应部分相同			
设备标识	设备标识标记	02或82	M	Y	4
	长度	02			
	起始端设备标识	82=ME			
	目的端设备标识	81=USIM卡			
结果	结果标记	03或83	M	Y	3
	长度	02或01			
	一般结果：规定了结果及SIM卡适当的动作	0X/1X：命令已经完成； 2X：稍后有机会应重试此命令； 3X：不必用相同的命令重试。			
时长	时长标记	04或84	M	Y	4
	长度	02			
	时间单位	同命令对应部分要求			
	时间长度	同命令对应部分要求			
区块链数据轮次	区块链数据轮次标记	60或E0	M	Y	3
	长度	01			
	区块链数据轮次	同命令对应部分要求			
区块链数据量	区块链数据；量标记	61或E1	M	Y	5
	长度	03			
	区块链数据量单位	同命令对应部分要求			
	区块链数据量	同命令对应部分要求			

[0094] 注：

[0095] 1)第二响应消息中命令限定符、时长、区块链数据轮次、区块链数据量等数据对象均与第一命令中对应部分的要求相同，且必须以第一命令中存在同名数据对象为前提，不会出现第一命令中不存在的数据对象；

[0096] 2)当第一命令中命令限定符中b1＝1，即USIM允许区块链平台提出修正建议时，且区块链平台根据自身情况判断需要修正限制条件值时，时长、区块链数据轮次、区块链数据量等才会存在，表示区块链平台针对USIM策略限制条件值的修正建议。

[0097] S105.按照所述第一命令的第二响应消息中的修正建议部署新的区块链安全数据更新管理策略，并在后续的数据上链业务中按照新的策略内容中修正后的USIM指定限制条件类型的取值进行安全数据更新。

[0098] 本实施例中，在区块链平台针对策略内容提出修正建议后，即形成新的区块链安全数据更新管理策略，USIM与区块链平台在后续的数据上链业务中都会按照新的策略内容中修正后的USIM指定限制条件类型的取值进行安全数据更新，实现了USIM和区块链平台都可以按照新的管理策略自行同步更新安全数据。

[0099] 在一种具体实施方式中，在步骤S104之后，还包括如下步骤S106至S108。

[0100] S106.判断USIM是否同意区块链平台对策略内容提出的修正建议。

[0101] S107.响应于USIM同意区块链平台对策略内容提出的修正建议，根据区块链平台针对USIM指定限制条件类型的取值的修正建议生成第二命令，所述第二命令要求区块链平

台根据修正后的USIM指定限制条件类型的取值部署新的区块链安全数据更新管理策略且不允许区块链平台再提出修正建议，并将所述第二命令发送给终端，以使终端接收并解析所述第二命令，获取部署新的区块链安全数据更新管理策略及不允许区块链平台再提出修正建议的要求，将其转化为能够与区块链平台交互的第三消息并发送给区块链平台，使区块链平台在接收到所述第三消息后，获取部署新的区块链安全数据更新管理策略及不允许区块链平台再提出修正建议的要求，执行新的策略部署并在后续的数据上链业务中按照新的策略内容中修正后的USIM指定限制条件类型的取值进行安全数据更新，以及基于执行结果生成第四消息并发送给终端，使终端在接收到所述第四消息后，将其转化为能够与USIM交互的所述第二命令的响应消息并发送给USIM，所述第二命令的响应消息包括所述第二命令的命令完成消息。

[0102] 本步骤中，第二命令根据区块链平台提出的修正建议生成，其中的命令限制条件值与修正建议相同，同时命令限定符设置为不允许提出修正建议，命令具体结构如前表1所示。

[0103] 由于USIM与区块链平台不具备直接交互的关系，需要借助于终端实现信息传递，所以USIM需要将第二命令发送给终端，终端在接收到第二命令后，对第二命令进行解析，获取部署新的区块链安全数据更新管理策略及不允许区块链平台再提出修正建议的要求，将其转化为能够与区块链平台进行交互的第三消息并发送到区块链平台，区块链平台接收到终端发送的第三消息后，按照第二命令的要求执行新的策略部署，在后续的数据上链业务中按照新的策略内容中修正后的USIM指定限制条件类型的取值自行进行安全数据更新，基于执行结果生成第四消息并发送给终端，终端在接收到所述第四消息后，将其转化为能够与USIM交互的所述第二命令的响应消息并发送给USIM。

[0104] S108.接收并解析终端发送的所述第二命令的响应消息，确认新的区块链安全数据更新管理策略部署完成。

[0105] 本实施例中，如果USIM允许区块链平台对策略内容提出修正建议，那么在获取区块链平台针对USIM指定限制条件类型的取值的修正建议之后，先判断是否同意区块链平台对策略内容提出的修正建议，如果同意，则根据区块链平台针对USIM指定限制条件类型的取值的修正建议生成第二命令并发送给终端，由终端转化为第三消息发送给区块链平台，区块链平台执行新的策略部署并基于执行结果生成第四消息并发送给终端，由终端转化为第二命令的响应消息并发送给USIM，USIM在接收到终端发送的所述第二命令的响应消息后，确认新的区块链安全数据更新管理策略部署完成，那么USIM和区块链平台都可以在后续的数据上链业务中同样按照新的策略内容中修正后的USIM指定限制条件类型的取值进行安全数据更新。

[0106] 在一种具体实施方式中，在步骤S106之后，还包括如下步骤S109和S110。

[0107] S109.响应于USIM不同意区块链平台对策略内容提出的修正建议，生成第三命令，所述第三命令要求区块链平台部署原有区块链安全数据更新管理策略且不允许区块链平台再提出修正建议，并将所述第三命令发送给终端，以使终端接收并解析所述第三命令，获取部署原有区块链安全数据更新管理策略及不允许区块链平台再提出修正建议的要求，将其转化为能够与区块链平台交互的第五消息并发送给区块链平台，使区块链平台在接收到所述第五消息后，获取部署原有区块链安全数据更新管理策略及不允许区块链平台再提出

修正建议的要求,执行原有策略部署并在后续的数据上链业务中按照原有策略内容中USIM指定限制条件类型及其取值进行安全数据更新,以及基于执行结果生成第六消息并发送给终端,使终端在接收到所述第六消息后,将其转化为能够与USIM交互的所述第三命令的响应消息并发送给USIM,所述第三命令的响应消息包括所述第三命令的命令完成消息。

[0108] 本步骤中,第三命令基本维持了原有第一命令的要求,其中的命令限定符设置为不允许提出修正建议,其它命令要求和内容均与第一命令相同,命令具体结构如前表1所示。

[0109] 由于USIM与区块链平台不具备直接交互的关系,需要借助于终端实现信息传递,所以USIM需要将第三命令发送给终端,终端在接收到第三命令后,对第三命令进行解析,获取部署原有区块链安全数据更新管理策略及不允许区块链平台再提出修正建议的要求,将其转化为能够与区块链平台进行交互的第五消息并发送到区块链平台,区块链平台接收到终端发送的第五消息后按照第三命令的要求执行原有策略部署,在后续的数据上链业务中按照原有策略内容中USIM指定限制条件类型及其取值进行安全数据更新,基于执行结果生成第六消息并发送给终端,终端在接收到所述第六消息后,将其转化为能够与USIM交互的所述第三命令的响应消息并发送给USIM。

[0110] S110.接收并解析终端发送的所述第三命令的响应消息,确认原有区块链安全数据更新管理策略部署完成,并在后续的数据上链业务中同样按照原有策略内容中USIM指定限制条件类型及其取值进行安全数据更新。

[0111] 本实施例中,如果USIM允许区块链平台对策略内容提出修正建议,但是不同意区块链平台提出的修正建议,就会生成与所述第一命令中针对USIM指定限制条件类型及其取值均相同的第三命令并发送给终端,由终端转化为第五消息发送给区块链平台,区块链平台执行原有策略部署并基于执行结果生成第六消息并发送给终端,由终端转化为第三命令的响应消息并发送给USIM,USIM在接收到终端发送的所述第三命令的响应消息后,确认原有区块链安全数据更新管理策略部署完成,那么USIM和区块链平台都可以在后续的数据上链业务中同样按照原有策略内容中USIM指定限制条件类型及其取值进行安全数据更新。

[0112] 需要说明的是,上述步骤的顺序只是为了说明本发明实施例而提出的一个具体实例,本发明对上述步骤的顺序不做限定,本领域技术人员在实际应用中可按需对其进行调整;而且上述步骤的序号大小也不限制其执行顺序。

[0113] 图2为本发明实施例提供的另一种安全数据更新方法的流程示意图。所述方法应用于终端,如图2所示,所述方法包括如下步骤S201至S203。

[0114] S201.接收USIM发送的第一命令,其中USIM生成部署区块链安全数据更新管理策略的第一命令并发送给终端,所述第一命令包括要求区块链平台根据USIM指定限制条件类型及其取值部署区块链安全数据更新管理策略的信息。

[0115] 具体地,在所述区块链安全数据更新管理策略的内容中,USIM指定限制条件类型包括:区块链安全数据的使用时长、使用区块链安全数据上链的数据轮次,以及使用区块链安全数据上链的数据量中的一种或多种。其中,USIM指定限制条件类型为区块链安全数据的使用时长时,表示区块链安全数据的使用时间达到一定时长后更新安全数据,该类型限制条件的取值表示面向安全数据使用时长的策略指定的限制条件值,即区块链安全数据使用多久需更新安全数据;USIM指定限制条件类型为使用区块链安全数据上链的数据轮次

时，表示使用区块链安全数据上链的数据轮次达到一定数量后更新安全数据，该类型限制条件的取值表示面向使用安全数据的上链数据轮次的策略指定的限制条件值，即使用区块链安全数据上链的数据轮次达到多少轮时需要更新安全数据；USIM指定限制条件类型为使用区块链安全数据上链的数据量时，表示使用区块链安全数据上链的数据量达到一定数量后更新安全数据，该类型限制条件的取值表示面向使用安全数据的上链数据数量的策略指定的限制条件值，即使用区块链安全数据上链的数据量达到多少时需要更新安全数据。

[0116] 为部署区块链安全数据更新管理策略，需要为USIM增加新的USAT命令，即前述“第一命令”，其功能是USIM要求区块链平台按照区块链安全数据更新管理策略来更新、调整区块链安全数据。第一命令的具体定义如前述表1所示。

[0117] S202.解析所述第一命令，获取部署区块链安全数据更新管理策略的要求及策略内容，将其转化为能够与区块链平台交互的第一消息并发送给区块链平台，以使区块链平台在接收到所述第一消息后，获取部署区块链安全数据更新管理策略的要求及策略内容，执行策略部署并在后续的数据上链业务中按照策略内容中USIM指定限制条件类型及其取值进行安全数据更新，以及基于执行结果生成第二消息并发送给终端。

[0118] S203.接收区块链平台发送的所述第二消息，将其转化为能够与USIM交互的所述第一命令的第一响应消息并发送给USIM，所述第一命令的第一响应消息包括所述第一命令的命令完成消息，以使USIM接收并解析终端发送的所述第一命令的第一响应消息，确认区块链安全数据更新管理策略部署完成，并在后续的数据上链业务中同样按照策略内容中USIM指定限制条件类型及其取值进行安全数据更新。

[0119] 本实施例中，USIM和区块链平台都可以在后续的数据上链业务中按照同样的策略内容中USIM指定限制条件类型及其取值进行安全数据更新，实现了USIM和区块链平台都可以按照既定管理策略自行同步更新安全数据。

[0120] 在一种具体实施方式中，所述第一命令还包括是否允许区块链平台对策略内容提出修正建议的信息。

[0121] 相应地，在步骤S202之后，还包括如下步骤S204和S205。

[0122] S204.接收区块链平台发送的修正建议；其中区块链平台在接收到终端发送的所述第一消息后，判断所述第一命令是否允许区块链平台对策略内容提出修正建议，若允许，则生成针对USIM指定限制条件类型的取值的修正建议并发送给终端，若不允许，则部署原有区块链安全数据更新管理策略并向终端发送所述第二消息。

[0123] 本步骤中，修正建议仅可针对第一命令中所提供的同样的限制条件类型的取值进行修改。

[0124] S205.将所述修正建议转化为能够与USIM交互的所述第一命令的第二响应消息并返回给USIM，所述第一命令的第二响应消息包括区块链平台对策略内容提出的修正建议，以使USIM按照所述第一命令的第二响应消息中的修正建议部署新的区块链安全数据更新管理策略，并在后续的数据上链业务中按照新的策略内容中修正后的USIM指定限制条件类型的取值进行安全数据更新。

[0125] 本步骤中，终端在接收到区块链平台提出的修正建议后，通过所述第一命令的第二响应消息向USIM返回结果。所述第一命令的第二响应消息中包含区块链平台提供的建议修正的同类型限制条件的取值，其具体定义如前述表2所示。

[0126] 本实施例中，在区块链平台针对策略内容提出修正建议后，即形成新的区块链安全数据更新管理策略，USIM与区块链平台在后续的数据上链业务中都会按照新的策略内容中修正后的USIM指定限制条件类型的取值进行安全数据更新，实现了USIM和区块链平台都可以按照新的管理策略自行同步更新安全数据。

[0127] 在一种可选实施方式中，在步骤S205之后，还包括如下步骤S206至S208。

[0128] S206.接收USIM发送的第二命令，其中USIM在接收到终端发送的所述第一命令的第二响应消息之后，判断USIM是否同意区块链平台对策略内容提出的修正建议，若同意，则根据区块链平台针对USIM指定限制条件类型的取值的修正建议生成第二命令，所述第二命令要求区块链平台根据修正后的USIM指定限制条件类型的取值部署新的区块链安全数据更新管理策略且不允许区块链平台再提出修正建议，并将所述第二命令发送给终端；

[0129] S207.解析所述第二命令，获取部署新的区块链安全数据更新管理策略及不允许区块链平台再提出修正建议的要求，将其转化为能够与区块链平台交互的第三消息并发送给区块链平台，以使区块链平台在接收到所述第三消息后，获取部署新的区块链安全数据更新管理策略及不允许区块链平台再提出修正建议的要求，执行新的策略部署并在后续的数据上链业务中按照新的策略内容中修正后的USIM指定限制条件类型的取值进行安全数据更新，以及基于执行结果生成第四消息并发送给终端；

[0130] S208.接收区块链平台发送的所述第四消息，将其转化为能够与USIM交互的所述第二命令的响应消息并发送给USIM，所述第二命令的响应消息包括所述第二命令的命令完成消息，以使USIM接收并解析终端发送的所述第二命令的响应消息，确认新的区块链安全数据更新管理策略部署完成，并在后续的数据上链业务中同样按照新的策略内容中修正后的USIM指定限制条件类型的取值进行安全数据更新。

[0131] 本实施例中，区块链平台在USIM允许其对策略内容提出修正建议的情况下，向终端发送针对USIM指定限制条件类型的取值的修正建议，由终端将所述修正建议转化为能够与USIM交互的所述第一命令的第二响应消息并返回给USIM;USIM在接收到区块链平台提供的修正建议后，先判断是否同意区块链平台对策略内容提出的修正建议，如果同意，则根据区块链平台针对USIM指定限制条件类型的取值的修正建议生成第二命令并发送给终端，由终端将其转化为能够与区块链平台交互的第三消息并发送给区块链平台;区块链平台在收到第三消息之后，获取部署新的区块链安全数据更新管理策略及不允许区块链平台再提出修正建议的要求，执行新的策略部署并基于执行结果生成第四消息发送给终端，由终端转化为能够与UISM交互的第二命令的响应消息并返回给USIM;USIM在接收到所述第二命令的响应消息之后，确认新的区块链安全数据更新管理策略部署完成，那么USIM和区块链平台都可以在后续的数据上链业务中同样按照新的策略内容中修正后的USIM指定限制条件类型的取值进行安全数据更新。

[0132] 在另一种可选实施方式中，在步骤S205之后，还包括如下步骤S209和S211。

[0133] S209.接收USIM发送的第三命令，其中USIM在接收到终端发送的所述第一命令的第二响应消息之后，判断USIM是否同意区块链平台对策略内容提出的修正建议，若不同意，则生成第三命令，所述第三命令要求区块链平台部署原有区块链安全数据更新管理策略且不允许区块链平台再提出修正建议，并将所述第三命令发送给终端；

[0134] 本步骤中，第三命令基本维持了第一命令原有要求，其中的命令限定符设置为不

允许提出修正建议,其它命令要求和内容均与第一命令相同,命令具体结构如前表1所示;

[0135] S210.解析所述第三命令,获取部署原有区块链安全数据更新管理策略及不允许区块链平台再提出修正建议的要求,将其转化为能够与区块链平台交互的第五消息并发送给区块链平台,以使区块链平台在接收到所述第五消息后,获取部署原有区块链安全数据更新管理策略及不允许区块链平台再提出修正建议的要求,执行原有策略部署并在后续的数据上链业务中按照原有策略内容中USIM指定限制条件类型及其取值进行安全数据更新,以及基于执行结果生成第六消息并发送给终端;

[0136] S211.接收区块链平台发送的所述第六消息,将其转化为能够与USIM交互的所述第三命令的响应消息并发送给USIM,所述第三命令的响应消息包括所述第三命令的命令完成消息,以使USIM接收并解析终端发送的所述第三命令的响应消息,确认原有区块链安全数据更新管理策略部署完成,并在后续的数据上链业务中同样按照原有策略内容中USIM指定限制条件类型及其取值进行安全数据更新。

[0137] 本实施例中,如果USIM允许区块链平台对策略内容提出修正建议,但是不同意区块链平台提出的修正建议,就会生成要求区块链平台部署原有区块链安全数据更新管理策略且不允许区块链平台再提出修正建议的第三命令并发送给终端,由终端将其转化为能够与区块链平台交互的第五消息并发送给区块链平台;区块链平台在接收到第五消息之后,获取部署原有区块链安全数据更新管理策略及不允许区块链平台再提出修正建议的要求,执行原有策略部署并基于执行结果生成第六消息发送给终端,由终端转化为能够与UISM交互的第三命令的响应消息并返回给USIM;USIM在接收到所述第三命令的响应消息之后,确认原有区块链安全数据更新管理策略部署完成,那么USIM和区块链平台都可以在后续的数据上链业务中同样按照原有策略内容中USIM指定限制条件类型及其取值进行安全数据更新。

[0138] 此外,在第一命令允许区块链平台对策略内容提出修正建议的前提下,区块链平台还可根据自身对策略内容的接受程度,判断是否需要修正策略内容,若需要,则生成针对USIM指定限制条件类型的取值的修正建议;若不需要,则部署原有区块链安全数据更新管理策略并向终端发送所述第二消息。

[0139] 本实施例中,若USIM允许区块链平台对策略内容提出修正建议,并且区块链平台根据自身对策略内容的接受程度确定需要修正策略内容,再生成针对USIM指定限制条件类型的取值的修正建议;若USIM允许区块链平台对策略内容提出修正建议,但是区块链平台根据自身对策略内容的接受程度确定不需要修正策略内容,则无需生成修正建议,直接按照策略内容执行策略部署,并在后续的数据上链业务中按照原有策略内容中USIM指定限制条件类型及其取值进行安全数据更新。

[0140] 需要说明的是,上述步骤的顺序只是为了说明本发明实施例而提出的一个具体实例,本发明对上述步骤的顺序不做限定,本领域技术人员在实际应用中可按需对其进行调整;而且上述步骤的序号大小也不限制其执行顺序。

[0141] 本实施例中,允许USIM对区块链安全数据(密钥、证书等)的更新和调整实施一定的管理策略,因为安全数据的更新和调整同时涉及USIM和区块链平台,双方均需参与这一过程并保持一致,而USIM提供主要安全能力,是安全数据的承载实体,在策略管理方面发挥主导作用,同时区块链平台也承担了安全数据生成功能,也应同时配合策略管理行为,另外

USIM与区块链平台不具备直接交互的关系,需要借助于终端实现信息传递。

[0142] 在策略部署的过程中,由USIM首先依据自身或系统要求提出安全数据的更新管理策略并通过终端发送到区块链平台,在USIM设置允许区块链平台对策略内容提出修正建议的情况下,区块链平台可以根据自身情况提出修正建议,由USIM评估是否可以接受修正建议,并将其作为最后策略部署的结果并通知区块链平台。在策略部署完成之后,USIM和区块链平台均需执行策略,按照策略要求同步调整和更新区块链安全数据。

[0143] 图3为本发明实施例提供的又一种安全数据更新方法的流程示意图。如图3所示,所述方法包括如下步骤S301至S313。

[0144] S301.USIM区块链应用的安全数据需要按照既定策略进行更新时,产生了部署区块链安全数据更新管理策略的需求;

[0145] S302.USIM根据需求具体内容,生成部署区块链安全数据更新管理策略的第一命令并发送到终端,第一命令表示要求区块链平台在根据USIM指定限制条件类型及其取值部署区块链安全数据更新管理策略,并在满足条件时自行进行安全数据更新,命令具体结构如前表1所示;

[0146] S303.终端收到第一命令后对第一命令进行解析,获取部署区块链安全数据更新管理策略的要求和策略内容,并将其转化为能够与区块链平台进行交互的第一消息并发送到区块链平台;

[0147] S304.区块链平台收到终端发送的第一消息后进行解析,获取部署策略的要求和策略内容,判断第一命令是否允许区块链平台提出修正建议,如果允许,则继续后续步骤S305,如果不允许,则转到步骤S313;

[0148] S305.区块链平台根据对USIM制定的策略的接受程度,判断是否需要修正USIM指定的策略,如果是,则继续后续步骤S306,如果否,则转到步骤S313;

[0149] S306.区块链平台暂不执行策略部署,而是生成针对USIM指定限制条件类型的取值的修正建议,并通过消息发送给终端,修正建议仅可针对第一命令中提供的同样的限制条件类型的取值进行修改;

[0150] S307.终端收到区块链平台发送的消息后进行解析,获取区块链平台提供的修正建议,将其转化为能够与USIM交互的前述第一命令的第二响应消息并返回到USIM,所述第一命令的第二响应消息中包含区块链平台提供的建议修正的同类型限制条件值;

[0151] S308.USIM收到第一命令的第二响应消息后进行解析,获取区块链平台提供的修正建议并判断是否允许区块链平台对策略的修正,如果是,则继续后续步骤S309,如果否,则转到步骤S310;

[0152] S309.USIM生成部署新的区块链安全数据更新管理策略的第二命令并发送到终端,然后转到步骤S311;其中第二命令根据区块链平台提供的修正建议生成,命令限制条件值与修正建议相同,同时命令限定符设置为不允许提出修正建议,命令具体结构如前表1所示;

[0153] S310.USIM生成部署原有区块链安全数据更新管理策略的第三命令并发送到终端,其中第三命令基本维持原有第一命令的要求,命令限定符设置为不允许提出修正建议,其它命令要求和内容均与前述第一命令相同,命令具体结构如前表1所示,然后转到步骤S311;

[0154] S311.终端收到第二/第三命令后对命令进行解析,获取命令要求和内容,并将其转化为与区块链平台进行交互的第三/第五消息并发送到区块链平台;

[0155] S312.区块链平台收到终端发送的第三/第五消息后进行解析,获得第二/第三命令中的策略部署的要求和内容,并按照第一/第二/第三命令要求,执行相应策略部署,在后续的数据上链业务中按照相应策略要求自行进行安全数据更新,并返回第二/第四/第六消息到终端;

[0156] S313.终端收到第二/第四/第六消息后,将其转化为能够与USIM交互的第一命令的第一响应消息/第二命令的响应消息/第三命令的响应消息并返回到USIM,USIM在收到相应的响应后确认策略部署完成,在后续的数据上链业务中同样按照策略要求同步进行安全数据更新。

[0157] 本实施例中,策略执行情况包括在区块链安全数据使用达到一定时长、使用区块链安全数据上链的数据轮次达到一定数量、使用区块链安全数据上链的数据量达到一定数量后更新安全数据以及上述情况的组合,表示其中任一策略限制条件满足时均需更新安全数据。

[0158] 本发明实施例提供的安全数据更新方法,面向基于USIM安全的终端区块链业务,针对区块链安全数据需要从固定不变的形式升级为动态更新的形式以提升其安全性的需求,提出以USIM为主导来部署区块链安全数据更新管理策略的具体方案,具体地,USIM将其部署的区块链安全数据更新管理策略发送给终端,由终端转化为能够与区块链平台交互的消息后发送至区块链平台,由区块链平台根据自身需求提出对策略内容的修正建议并发送给终端,由终端转化为能够与USIM交互的消息后返回给USIM,使区块链平台和USIM均可以按照既定策略自行同步更新安全数据,改变目前安全数据固定不变的状态,加强安全数据的自我保护和自我修复的机制,一定程度上克服现有方式带来的易泄露、易破解等缺陷,并提升对风险事件发生前的防范能力和发生后的处置能力。而且,所述方法还定义了方案实现所需的扩展机卡交互USAT命令类型,规定了命令的作用和功能,并定义了命令的结构参数定义,同时定义USIM与区块链平台进行安全数据更新管理策略部署的步骤流程和具体规则要求等。

[0159] 图4为本发明实施例提供的USIM的结构示意图。如图4所示,USIM包括:命令生成模块401、第一发送模块402、第一接收模块403和执行模块404。

[0160] 其中,命令生成模块401设置为生成部署区块链安全数据更新管理策略的第一命令,所述第一命令包括要求区块链平台根据USIM指定限制条件类型及其取值部署区块链安全数据更新管理策略的信息;第一发送模块402设置为将所述第一命令发送给终端,以使终端接收并解析所述第一命令,获取部署区块链安全数据更新管理策略的要求及策略内容,将其转化为能够与区块链平台交互的第一消息并发送给区块链平台,使区块链平台在接收到所述第一消息后,获取部署区块链安全数据更新管理策略的要求及策略内容,执行策略部署并在后续的数据上链业务中按照策略内容中USIM指定限制条件类型及其取值进行安全数据更新,以及基于执行结果生成第二消息并发送给终端,使终端在接收到所述第二消息后,将其转化为能够与USIM交互的所述第一命令的第一响应消息并发送给USIM,所述第一命令的第一响应消息包括所述第一命令的命令完成消息;第一接收模块403设置为接收并解析终端发送的所述第一命令的第一响应消息,确认区块链安全数据更新管理策略部署

完成;执行模块404设置为在后续的数据上链业务中同样按照策略内容中USIM指定限制条件类型及其取值进行安全数据更新。

[0161] 在一种具体实施方式中,所述USIM指定限制条件类型包括:区块链安全数据的使用时长、使用区块链安全数据上链的数据轮次,以及使用区块链安全数据上链的数据量中的一种或多种。

[0162] 在一种具体实施方式中,所述第一命令还包括是否允许区块链平台对策略内容提出修正建议的信息。

[0163] 相应地,第一接收模块403还设置为接收并解析终端发送的所述第一命令的第二响应消息;其中区块链平台在接收到所述第一消息后,响应于所述第一命令不允许区块链平台对策略内容提出修正建议,部署原有区块链安全数据更新管理策略并向终端发送所述第二消息,使终端在接收到所述第二消息后,将其转化为能够与USIM交互的所述第一命令的第一响应消息并发送给USIM,或者响应于所述第一命令允许区块链平台对策略内容提出修正建议,生成针对USIM指定限制条件类型的取值的修正建议,并发送给终端,使终端在接收到所述修正建议后,将其转化为能够与USIM交互的所述第一命令的第二响应消息并返回给USIM,所述第一命令的第二响应消息包括区块链平台对策略内容提出的修正建议。执行模块404还设置为按照所述第一命令的第二响应消息中的修正建议部署新的区块链安全数据更新管理策略,并在后续的数据上链业务中按照新的策略内容中修正后的USIM指定限制条件类型的取值进行安全数据更新。

[0164] 在一种具体实施方式中,USIM还包括:第一判断模块。

[0165] 第一判断模块设置为在第一接收模块403接收并解析终端发送的所述第一命令的第二响应消息之后,判断USIM是否同意区块链平台对策略内容提出的修正建议;命令生成模块401还设置为,在所述第一判断模块的判断结果为USIM同意区块链平台对策略内容提出的修正建议时,根据区块链平台针对USIM指定限制条件类型的取值的修正建议生成第二命令,所述第二命令要求区块链平台根据修正后的USIM指定限制条件类型的取值部署新的区块链安全数据更新管理策略且不允许区块链平台再提出修正建议;第一发送模块402还设置为将所述第二命令发送给终端,以使终端接收并解析所述第二命令,获取部署新的区块链安全数据更新管理策略及不允许区块链平台再提出修正建议的要求,将其转化为能够与区块链平台交互的第三消息并发送给区块链平台,使区块链平台在接收到所述第三消息后,获取部署新的区块链安全数据更新管理策略及不允许区块链平台再提出修正建议的要求,执行新的策略部署并在后续的数据上链业务中按照新的策略内容中修正后的USIM指定限制条件类型的取值进行安全数据更新,以及基于执行结果生成第四消息并发送给终端,使终端在接收到所述第四消息后,将其转化为能够与USIM交互的所述第二命令的响应消息并发送给USIM,所述第二命令的响应消息包括所述第二命令的命令完成消息;第一接收模块403还设置为,接收并解析终端发送的所述第二命令的响应消息,确认新的区块链安全数据更新管理策略部署完成。

[0166] 在一种具体实施方式中,命令生成模块401还设置为,在所述第一判断模块的判断结果为USIM不同意区块链平台对策略内容提出的修正建议时,生成第三命令,所述第三命令要求区块链平台部署原有区块链安全数据更新管理策略且不允许区块链平台再提出修正建议,第三命令与所述第一命令中针对USIM指定限制条件类型及其取值均相同;第一发

送模块402还设置为，将所述第三命令发送给终端，以使终端接收并解析所述第三命令，获取部署原有区块链安全数据更新管理策略及不允许区块链平台再提出修正建议的要求，将其转化为能够与区块链平台交互的第五消息并发送给区块链平台，使区块链平台在接收到所述第五消息后，获取部署原有区块链安全数据更新管理策略及不允许区块链平台再提出修正建议的要求，执行原有策略部署并在后续的数据上链业务中按照原有策略内容中USIM指定限制条件类型及其取值进行安全数据更新，以及基于执行结果生成第六消息并发送给终端，使终端在接收到所述第六消息后，将其转化为能够与USIM交互的所述第三命令的响应消息并发送给USIM，所述第三命令的响应消息包括所述第三命令的命令完成消息；第一接收模块403还设置为，接收并解析终端发送的所述第三命令的响应消息，确认原有区块链安全数据更新管理策略部署完成；执行模块404还设置为，并在后续的数据上链业务中同样按照原有策略内容中USIM指定限制条件类型及其取值进行安全数据更新。

[0167] 本发明实施例提供的USIM，针对区块链安全数据需要从固定不变的形式升级为动态更新的形式以提升其安全性的需求，以自身为主导来部署区块链安全数据更新管理策略，并将其部署的区块链安全数据更新管理策略发送给终端，由终端转化为能够与区块链平台交互的消息后发送至区块链平台，由区块链平台根据自身需求提出对策略内容的修正建议并发送给终端，由终端转化为能够与USIM交互的消息后返回给USIM，使自身和区块链平台都可以按照既定策略自行同步更新安全数据，改变目前安全数据固定不变的状态，加强安全数据的自我保护和自我修复的机制，一定程度上克服现有方式带来的易泄露、易破解等缺陷，并提升对风险事件发生前的防范能力和发生后的处置能力。

[0168] 图5为本发明实施例提供的终端的结构示意图。如图5所示，终端包括：第二接收模块501、转化模块502和第二发送模块503。

[0169] 其中，第二接收模块501设置为接收USIM发送的第一命令，其中USIM生成部署区块链安全数据更新管理策略的第一命令并发送给终端，所述第一命令包括要求区块链平台根据USIM指定限制条件类型及其取值部署区块链安全数据更新管理策略的信息；以及，解析所述第一命令，获取部署区块链安全数据更新管理策略的要求及策略内容；转化模块502设置为将所述部署区块链安全数据更新管理策略的要求及策略内容转化为能够与区块链平台交互的第一消息；第二发送模块503设置为将所述第一消息发送给区块链平台，以使区块链平台在接收到所述第一消息后，获取部署区块链安全数据更新管理策略的要求及策略内容，执行策略部署并在后续的数据上链业务中按照策略内容中USIM指定限制条件类型及其取值进行安全数据更新，以及基于执行结果生成第二消息并发送给终端；所述第二接收模块501还设置为，接收区块链平台发送的所述第二消息，将其转化为能够与USIM交互的所述第一命令的第一响应消息；所述第二发送模块503还设置为，将所述第一命令的第一响应消息发送给USIM，所述第一命令的第一响应消息包括所述第一命令的命令完成消息，以使USIM接收并解析终端发送的所述第一命令的第一响应消息，确认区块链安全数据更新管理策略部署完成，并在后续的数据上链业务中同样按照策略内容中USIM指定限制条件类型及其取值进行安全数据更新。

[0170] 在一种具体实施方式中，所述USIM指定限制条件类型包括：区块链安全数据的使用时长、使用区块链安全数据上链的数据轮次，以及使用区块链安全数据上链的数据量中的一种或多种。

[0171] 在一种具体实施方式中，所述第一命令还包括是否允许区块链平台对策略内容提出修正建议的信息。

[0172] 第二接收模块501还设置为在第二发送模块503将所述第一消息发送给区块链平台之后，接收区块链平台发送的修正建议；其中区块链平台在接收到终端发送的所述第一消息后，判断所述第一命令是否允许区块链平台对策略内容提出修正建议，若允许，则生成针对USIM指定限制条件类型的取值的修正建议并发送给终端，若不允许，则部署原有区块链安全数据更新管理策略并向终端发送所述第二消息。转化模块502还设置为将所述修正建议转化为能够与USIM交互的所述第一命令的第二响应消息。第二发送模块503还设置为将所述第一命令的第二响应消息返回给USIM，所述第一命令的第二响应消息包括区块链平台对策略内容提出的修正建议，以使USIM按照所述第一命令的第二响应消息中的修正建议部署新的区块链安全数据更新管理策略，并在后续的数据上链业务中按照新的策略内容中修正后的USIM指定限制条件类型的取值进行安全数据更新。

[0173] 在一种可选实施方式中，第二接收模块501还设置为在第二发送模块503将所述第一命令的第二响应消息返回给USIM之后，接收USIM发送的第二命令，其中USIM在接收到终端发送的所述第一命令的第二响应消息之后，判断USIM是否同意区块链平台对策略内容提出的修正建议，若同意，则根据区块链平台针对USIM指定限制条件类型的取值的修正建议生成第二命令，所述第二命令要求区块链平台根据修正后的USIM指定限制条件类型的取值部署新的区块链安全数据更新管理策略且不允许区块链平台再提出修正建议，并将所述第二命令发送给终端；以及解析所述第二命令，获取部署新的区块链安全数据更新管理策略及不允许区块链平台再提出修正建议的要求。转化模块502还设置为将部署新的区块链安全数据更新管理策略及不允许区块链平台再提出修正建议的要求转化为能够与区块链平台交互的第三消息。第二发送模块503还设置为将所述第三消息发送给区块链平台，以使区块链平台在接收到所述第三消息后，获取部署新的区块链安全数据更新管理策略及不允许区块链平台再提出修正建议的要求，执行新的策略部署并在后续的数据上链业务中按照新的策略内容中修正后的USIM指定限制条件类型的取值进行安全数据更新，以及基于执行结果生成第四消息并发送给终端。第二接收模块501还设置为接收区块链平台发送的所述第四消息。转化模块502还设置为将所述第四消息转化为能够与USIM交互的所述第二命令的响应消息。第二发送模块503还设置为将所述第二命令的响应消息发送给USIM，所述第二命令的响应消息包括所述第二命令的命令完成消息，以使USIM接收并解析终端发送的所述第二命令的响应消息，确认新的区块链安全数据更新管理策略部署完成，并在后续的数据上链业务中同样按照新的策略内容中修正后的USIM指定限制条件类型的取值进行安全数据更新。

[0174] 在另一种可选实施方式中，第二接收模块501还设置为在第二发送模块503将所述第一命令的第二响应消息返回给USIM之后，接收USIM发送的第三命令，其中USIM在接收到终端发送的所述第一命令的第二响应消息之后，判断USIM是否同意区块链平台对策略内容提出的修正建议，若不同意，则生成第三命令，所述第三命令要求区块链平台部署原有区块链安全数据更新管理策略且不允许区块链平台再提出修正建议，并将所述第三命令发送给终端；以及解析所述第三命令，获取部署原有区块链安全数据更新管理策略及不允许区块链平台再提出修正建议的要求。转化模块502还设置为将部署原有区块链安全数据更新管

理策略及不允许区块链平台再提出修正建议的要求转化为能够与区块链平台交互的第五消息。第二发送模块503还设置为将所述第五消息发送给区块链平台，以使区块链平台在接收到所述第五消息后，获取部署原有区块链安全数据更新管理策略及不允许区块链平台再提出修正建议的要求，执行原有策略部署并在后续的数据上链业务中按照原有策略内容中USIM指定限制条件类型及其取值进行安全数据更新，以及基于执行结果生成第六消息并发送给终端。第二接收模块501还设置为接收区块链平台发送的所述第六消息。转化模块502还设置为将所述第六消息转化为能够与USIM交互的所述第三命令的响应消息。第二发送模块503还设置为将所述第三命令的响应消息发送给USIM，所述第三命令的响应消息包括所述第三命令的命令完成消息，以使USIM接收并解析终端发送的所述第三命令的响应消息，确认原有区块链安全数据更新管理策略部署完成，并在后续的数据上链业务中同样按照原有策略内容中USIM指定限制条件类型及其取值进行安全数据更新。

[0175] 本发明实施例提供的终端，针对区块链安全数据需要从固定不变的形式升级为动态更新的形式以提升其安全性的需求，在接收到USIM为主导所部署的区块链安全数据更新管理策略之后，根据自身需求提出对策略内容的修正建议并发送给终端，由终端转化为能够与USIM交互的消息后返回给USIM，使区块链平台和USIM均可以按照既定策略自行同步更新安全数据，改变目前安全数据固定不变的状态，加强安全数据的自我保护和自我修复的机制，一定程度上克服现有方式带来的易泄露、易破解等缺陷，并提升对风险事件发生前的防范能力和发生后的处置能力

[0176] 图6为本发明实施例提供的安全数据更新系统的结构示意图。如图6所示，安全数据更新系统包括：USIM601和终端602。

[0177] 其中，USIM601可采用前述实施例中USIM的具体结构，终端602可采用前述实施例中终端的具体结构，此处不再赘述。

[0178] 本发明实施例提供的安全数据更新系统，面向基于USIM安全的终端区块链业务，针对区块链安全数据需要从固定不变的形式升级为动态更新的形式以提升其安全性的需求，提出以USIM为主导来部署区块链安全数据更新管理策略的具体方案，具体地，USIM将其部署的区块链安全数据更新管理策略发送给终端，由终端转化为能够与区块链平台交互的消息后发送至区块链平台，由区块链平台根据自身需求提出对策略内容的修正建议并发送给终端，由终端转化为能够与USIM交互的消息后返回给USIM，使区块链平台和USIM均可以按照既定策略自行同步更新安全数据，改变目前安全数据固定不变的状态，加强安全数据的自我保护和自我修复的机制，一定程度上克服现有方式带来的易泄露、易破解等缺陷，并提升对风险事件发生前的防范能力和发生后的处置能力。

[0179] 基于相同的技术构思，本发明实施例相应还提供一种计算机设备，如图7所示，所述计算机设备包括存储器71和处理器72，所述存储器71中存储有计算机程序，当所述处理器72运行所述存储器71存储的计算机程序时，所述处理器72执行前述安全数据更新方法。

[0180] 基于相同的技术构思，本发明实施例相应还提供一种计算机可读存储介质，其上存储有计算机程序，所述计算机程序被处理器执行时，所述处理器执行前述安全数据更新方法。

[0181] 综上所述，本发明实施例提供的安全数据更新方法、系统、USIM、终端、计算机设备及存储介质，以USIM为主体，依据必要的管理策略对区块链安全数据实现常态化、规律性地

有序更新和调整，改变目前安全数据固定不变的状态，加强安全数据的自我保护和自我修复的机制，一定程度上克服现有方式带来的易泄露、易破解等缺陷，并提升对风险事件发生前的防范能力和发生后的处置能力。

[0182] 本领域普通技术人员可以理解，上文中所公开方法中的全部或某些步骤、系统、装置中的功能模块/单元可以被实施为软件、固件、硬件及其适当的组合。在硬件实施方式中，在以上描述中提及的功能模块/单元之间的划分不一定对应于物理组件的划分；例如，一个物理组件可以具有多个功能，或者一个功能或步骤可以由若干物理组件合作执行。某些物理组件或所有物理组件可以被实施为由处理器，如中央处理器、数字信号处理器或微处理器执行的软件，或者被实施为硬件，或者被实施为集成电路，如专用集成电路。这样的软件可以分布在计算机可读介质上，计算机可读介质可以包括计算机存储介质(或非暂时性介质)和通信介质(或暂时性介质)。如本领域普通技术人员公知的，术语计算机存储介质包括在用于存储信息(诸如计算机可读指令、数据结构、程序模块或其他数据)的任何方法或技术中实施的易失性和非易失性、可移除和不可移除介质。计算机存储介质包括但不限于RAM、ROM、EEPROM、闪存或其他存储器技术、CD-ROM、数字多功能盘(DVD)或其他光盘存储、磁盒、磁带、磁盘存储或其他磁存储装置、或者可以用于存储期望的信息并且可以被计算机访问的任何其他的介质。此外，本领域普通技术人员公知的是，通信介质通常包含计算机可读指令、数据结构、程序模块或者诸如载波或其他传输机制之类的调制数据信号中的其他数据，并且可包括任何信息递送介质。

[0183] 最后应说明的是：以上各实施例仅用以说明本发明的技术方案，而非对其限制；尽管参照前述各实施例对本发明进行了详细的说明，本领域的普通技术人员应当理解：其依然可以对前述各实施例所记载的技术方案进行修改，或者对其中部分或者全部技术特征进行等同替换；而这些修改或者替换，并不使相应技术方案的本质脱离本发明各实施例技术方案的范围。

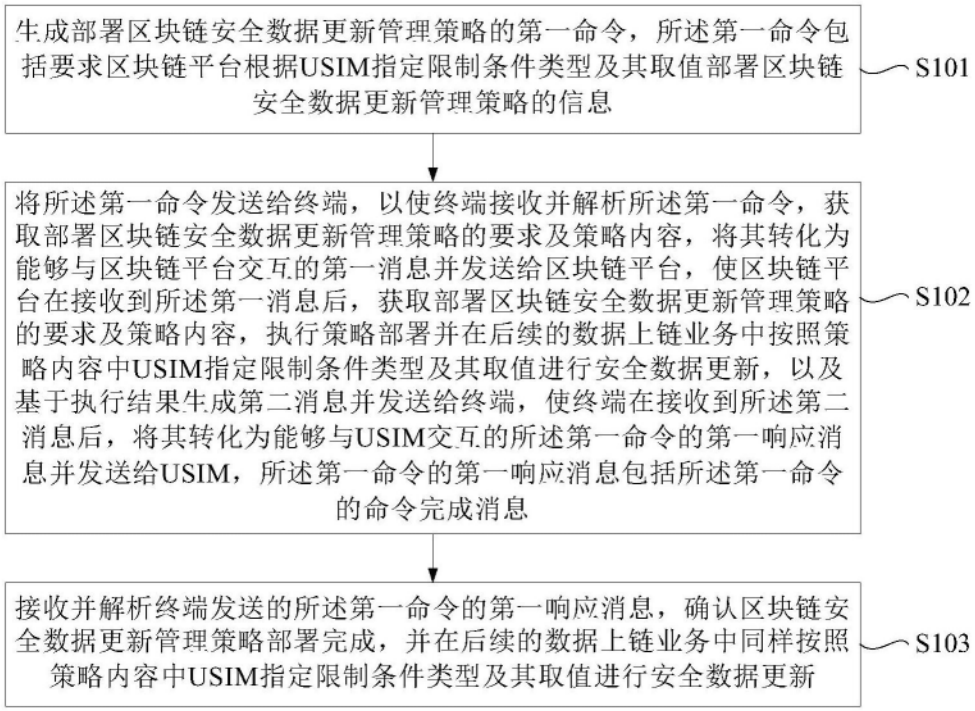

生成部署区块链安全数据更新管理策略的第一命令，所述第一命令包括要求区块链平台根据USIM指定限制条件类型及其取值部署区块链安全数据更新管理策略的信息
S101
将所述第一命令发送给终端，以使终端接收并解析所述第一命令，获取部署区块链安全数据更新管理策略的要求及策略内容，将其转化为能够与区块链平台交互的第一消息并发送给区块链平台，使区块链平台在接收到所述第一消息后，获取部署区块链安全数据更新管理策略的要求及策略内容，执行策略部署并在后续的数据上链业务中按照策略内容中USIM指定限制条件类型及其取值进行安全数据更新，以及基于执行结果生成第二消息并发送给终端，使终端在接收到所述第二消息后，将其转化为能够与USIM交互的所述第一命令的第一响应消息并发送给USIM，所述第一命令的第一响应消息包括所述第一命令的命令完成消息
S102
接收并解析终端发送的所述第一命令的第一响应消息，确认区块链安全数据更新管理策略部署完成，并在后续的数据上链业务中同样按照策略内容中USIM指定限制条件类型及其取值进行安全数据更新
S103

图1

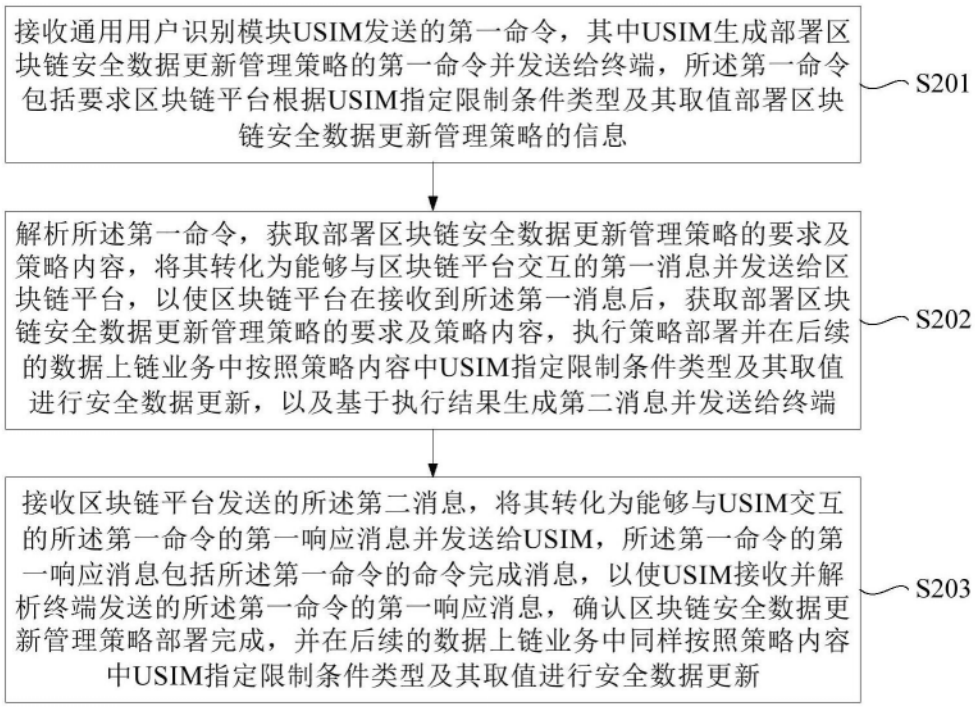

接收通用用户识别模块USIM发送的第一命令，其中USIM生成部署区块链安全数据更新管理策略的第一命令并发送给终端，所述第一命令包括要求区块链平台根据USIM指定限制条件类型及其取值部署区块链安全数据更新管理策略的信息
S201
解析所述第一命令，获取部署区块链安全数据更新管理策略的要求及策略内容，将其转化为能够与区块链平台交互的第一消息并发送给区块链平台，以使区块链平台在接收到所述第一消息后，获取部署区块链安全数据更新管理策略的要求及策略内容，执行策略部署并在后续的数据上链业务中按照策略内容中USIM指定限制条件类型及其取值进行安全数据更新，以及基于执行结果生成第二消息并发送给终端
S202
接收区块链平台发送的所述第二消息，将其转化为能够与USIM交互的所述第一命令的第一响应消息并发送给USIM，所述第一命令的第一响应消息包括所述第一命令的命令完成消息，以使USIM接收并解析终端发送的所述第一命令的第一响应消息，确认区块链安全数据更新管理策略部署完成，并在后续的数据上链业务中同样按照策略内容中USIM指定限制条件类型及其取值进行安全数据更新
S203

图2

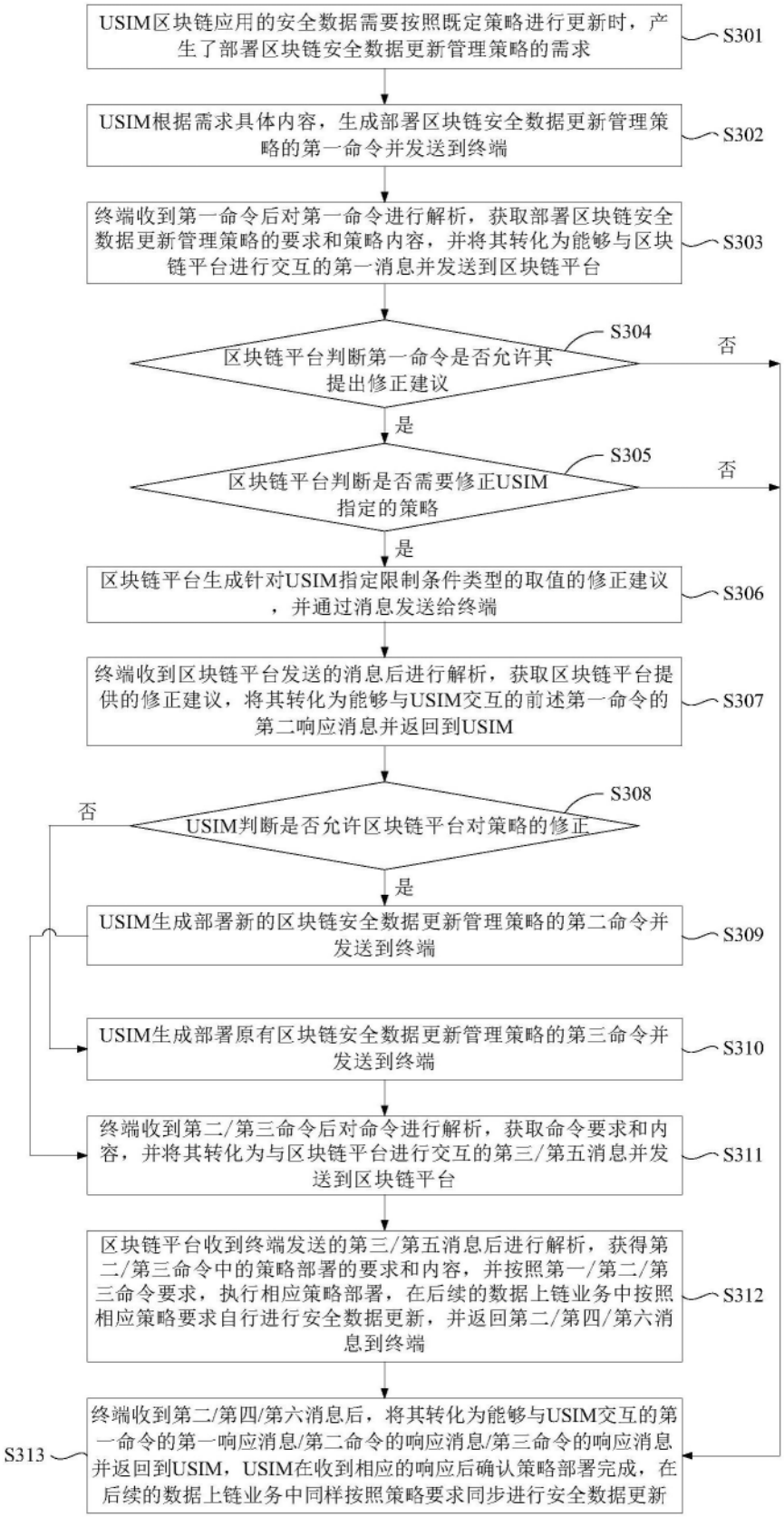

USIM区块链应用的安全数据需要按照既定策略进行更新时，产生了部署区块链安全数据更新管理策略的需求
S301
USIM根据需求具体内容，生成部署区块链安全数据更新管理策略的第一命令并发送到终端
S302
终端收到第一命令后对第一命令进行解析，获取部署区块链安全数据更新管理策略的要求和策略内容，并将其转化为能够与区块链平台进行交互的第一消息并发送到区块链平台
S303
区块链平台判断第一命令是否允许其提出修正建议
S304
否
是
区块链平台判断是否需要修正USIM指定的策略
S305
否
是
区块链平台生成针对USIM指定限制条件类型的取值的修正建议，并通过消息发送给终端
S306
终端收到区块链平台发送的消息后进行解析，获取区块链平台提供的修正建议，将其转化为能够与USIM交互的前述第一命令的第二响应消息并返回到USIM
S307
USIM判断是否允许区块链平台对策略的修正
S308
否
是
USIM生成部署新的区块链安全数据更新管理策略的第二命令并发送到终端
S309
USIM生成部署原有区块链安全数据更新管理策略的第三命令并发送到终端
S310
终端收到第二/第三命令后对命令进行解析，获取命令要求和内容，并将其转化为与区块链平台进行交互的第三/第五消息并发送到区块链平台
S311
区块链平台收到终端发送的第三/第五消息后进行解析，获得第二/第三命令中的策略部署的要求和内容，并按照第一/第二/第三命令要求，执行相应策略部署，在后续的数据上链业务中按照相应策略要求自行进行安全数据更新，并返回第二/第四/第六消息到终端
S312
终端收到第二/第四/第六消息后，将其转化为能够与USIM交互的第一命令的第一响应消息/第二命令的响应消息/第三命令的响应消息并返回到USIM，USIM在收到相应的响应后确认策略部署完成，在后续的数据上链业务中同样按照策略要求同步进行安全数据更新
S313

图3

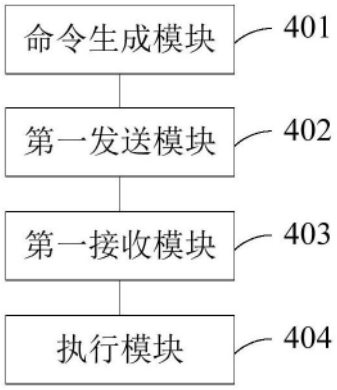

命令生成模块
401
第一发送模块
402
第一接收模块
403
执行模块
404

图4

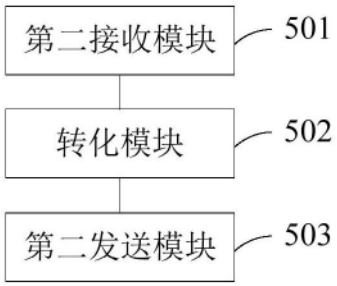

第二接收模块
501
转化模块
502
第二发送模块
503

图5

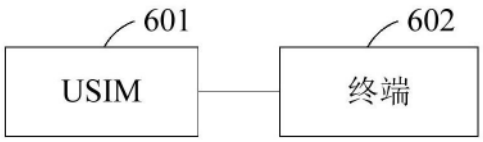

601
USIM
602
终端

图6

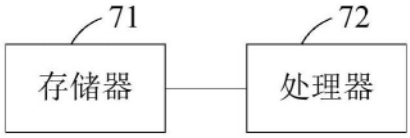

71
存储器
72
处理器

图7