(19)中华人民共和国国家知识产权局

(12)发明专利申请

(10)申请公布号 CN 111461712 A
(43)申请公布日 2020.07.28

(21)申请号 202010186424.7

(22)申请日 2020.03.17

(71)申请人 江苏华能智慧能源供应链科技有限公司
地址 210000 江苏省南京市江宁区麒麟科创园沧园路1号金元天甲1号楼3楼

(72)发明人 李俊华 贾宁 邢海涛

(74)专利代理机构 南京苏科专利代理有限责任公司 32102
代理人 徐振兴

(51)Int.Cl.
G06Q 20/38(2012.01)
G06Q 20/40(2012.01)
G06Q 40/04(2012.01)

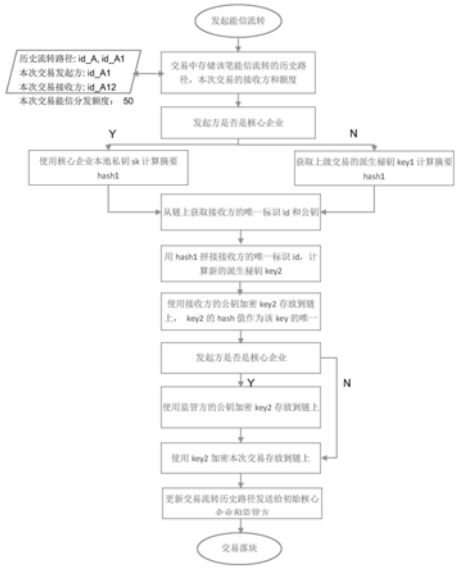
权利要求书1页 说明书6页 附图4页

(54)发明名称

区块链供应链金融场景下的交易隐私保护和分层监管

(57)摘要

本发明公开了一种区块链供应链金融场景下的交易隐私保护和分层监管方法，主要是通过交易发起方生成的派生密匙来加密交易内容，因为交易的顺序是从高层顺序向下流转，该方法可做到上级根据自己的对称密钥信息计算出下级的对称密钥信息，而下级不可反向计算出上级的对称密钥信息，但可在自己上链的数据中查看到能信流转的直线信息。



CN 111461712 A

1.区块链供应链金融场景下的交易隐私保护和分层监管方法,其特征在于:按照如下步骤进行:

步骤1:确立身份信息,供应链各层级在系统中创建身份标识的公、私钥对,公钥的hash值作为该层级的身份id号,将公钥和身份id号配对存储并提交到区块链上;

步骤2:发起交易,交易发起方发起交易请求,根据交易发起方的对称秘钥和交易接收方的身份id号生成派生秘钥,用派生秘钥加密交易信息并提交到区块链上,用交易双方的公钥加密派生秘钥并提交到区块链上;

步骤3:接收交易,交易接收方获取加密的交易信息,交易接收方获取公钥加密的派生秘钥,用本地的私钥解密获取派生秘钥,用派生秘钥解密获取本次交易信息。

2.根据权利要求1所述的区块链供应链金融场景下的交易隐私保护和分层监管方法,其特征在于:还包括步骤4:第三方监管交易,交易的监管方针对要监管的交易,获取交易双方的身份信息,使用秘钥派生规则获取或推演出派生秘钥,链上获取加密的交易消息,使用派生秘钥解密获取交易的明文信息。

3.根据权利要求1所述的区块链供应链金融场景下的交易隐私保护和分层监管方法,其特征在于:步骤2中,如果交易发起方是第一层,则用第三方监管的公钥加密派生秘钥并提交到区块链上,交易发起方的层级高于交易接收方。

4.根据权利要求2所述的区块链供应链金融场景下的交易隐私保护和分层监管方法,其特征在于:所有第一层企业需要将对下一级企业交易流转的对称密钥上交给监管方。

5.根据权利要求1所述的区块链供应链金融场景下的交易隐私保护和分层监管方法,其特征在于:步骤2中,每个节点在为下游交易生成对称秘钥的时候,秘钥的生成种子seed的生成规则为:

第一层企业用自身特有的私钥和交易的接收方id号的摘要值,作为参数生成本次交易的加密对称秘钥,用于加密第一层企业和交易接收方即第二层企业的交易信息;

第二层企业向下之间的交易流转中, 交易对称加密秘钥的生成规则为,用上一层交易的对称秘钥和交易接收方的id号的摘要值,作为输入参数生成本次交易的对称加密秘钥。

6.区块链供应链金融场景下的交易隐私保护和分层监管系统,其特征在于:该系统同时运行在供应链各层级指定电脑上并相互关联,包括:

身份信息注册装置,供用户创建身份信息;

公私钥对生成装置,用于生成每个用户的公、私钥对;

交易秘钥派生装置,用于生成交易双方派生密钥。

区块链供应链金融场景下的交易隐私保护和分层监管

[0001] 技术领域：

本发明属于金融交易风险控制技术领域，特别涉及一种区块链供应链金融场景下的交易隐私保护和分层监管。

[0002] 背景技术：

传统供应链金融因其行业业务性质，在实践的过程遇到了诸多难题和痛点。第一，供应链上存在很多信息孤岛，同一供应链上企业之间的ERP系统、账务系统较难统一，导致企业间信息并不互通，信息孤岛开始涌现，制约了很多融资信息的验证。第二，核心企业信任并不能有效传递，根据合同法，核心企业是跟一级供应商签订合同，但是一级供应商和二级供应商签订合同时并没有核心企业参与，并不能传递相关的核心企业的信任到多级供应商。第三，银行缺乏可信业务场景，由于中小企业无法证实贸易关系的存在，在现存的银行风控体系下，难以获得银行资金。相对地，银行业无法渗透入供应链进行获客和放款。第四，融资难融资贵现象突出，在目前赊销模式盛行的市场背景下，供应链上游的供应商往往存在较大资金缺口，然而没有核心企业的背书，他们难以获得银行的优质贷款。第五，合同履约并不能自动完成，现在很多约定结算没有自动完成，涉及多级供应商结算时，不确定性因素较多。

[0003] 区块链是分布式数据存储、点对点传输、共识机制、加密算法等计算机技术的新型应用模式。基于区块链技术的供应链金融解决方案，可以以节点可控的方式建立一种联盟链网络，涵盖供应链核心企业、供应商、经销商、资金方等贸易融资参与主体及政府或企业监管审计机构，制定共同遵守的规则透明的智能合约，并结合大数据、物联网等技术，深度整合物流、商流、信息流、资金流等数据信息，将相关数据信息上链并实时共享，增强供应链金融参与各方之间的互信，解决融资困难问题，减少资方风控成本，提升融资放款效率，降低监管溯源难度，促进供应链金融行业的健康发展。

[0004] 基于区块链技术的供应链金融在落地实现中的挑战性的问题主要体现在一下几个方面。首先，上链数据的隐私性，例如应收账款凭证是属于负债表的。应收账款凭证属于融资相关的信息，授信的平台对数据的隐私保护要求非常高，交易过程中必须要有很强的防截获、防破解能力。其次，不仅在技术上、监管上要有所配套，很多时候也需要政府、供应链各参与方、提供方等利益相关方的共同参与，共同推进整个行业的发展。

[0005] 现有公开的技术方案为：使用公私钥结合对称密钥的安全机制，可对交易数据做隐私保护，使非该交易参与用户不可见，也可授权其他用户访问。

[0006] 加密及授权访问交易数据步骤：

a)为交易数据生成对称密钥

b)使用对称密钥加密交易数据

c)授权某一用户访问某一交易数据，可使用该用户的公钥加密对称密钥

被授权用户访问交易数据步骤：

a)使用用户自己的私钥解密与某交易数据对应的对称密钥的密文

b)使用对称密钥解密该交易数据，获取交易数据明文

该技术的缺点为:扁平化的基于区块链的交易秘钥生成和分发机制，即使用对称密钥加密交易数据,使用被授权访问交易数据的用户的公钥加密对称密钥。交易数据被授权给n个用户访问时,需要加密n份对称密钥,然后上链,密钥管理起来比较复杂。在层级化的交易管理中，不能实现交易隐私的分层保护和监管能力。

[0007] 公开于该背景技术部分的信息仅仅旨在增加对本发明的总体背景的理解,而不应当被视为承认或以任何形式暗示该信息构成已为本领域一般技术人员所公知的现有技术。

[0008] 发明内容:

本发明的目的在于提供一种同级之间不可见、上下层级间单向可见的区块链供应链金融场景下的交易隐私保护和分层监管方法,从而克服上述现有技术中的缺陷。

[0009] 为实现上述目的,本发明提供了一种区块链供应链金融场景下的交易隐私保护和分层监管方法,按照如下步骤进行:

步骤1:确立身份信息,供应链各层级在系统中创建身份标识的公、私钥对,公钥的hash值作为该层级的身份id号,将公钥和身份id号配对存储并提交到区块链上;

步骤2:发起交易,交易发起方发起交易请求,根据交易发起方的对称秘钥和交易接收方的身份id号生成派生秘钥,用派生秘钥加密交易信息并提交到区块链上,用交易双方的公钥加密派生秘钥并提交到区块链上;

步骤3:接收交易,交易接收方获取加密的交易信息,交易接收方获取公钥加密的派生秘钥,用本地的私钥解密获取派生秘钥,用派生秘钥解密获取本次交易信息。

[0010] 为了便于公众理解,我们对文中用到的专业名词解释如下:

从狭义来讲,区块链是一种按照时间顺序将数据区块以顺序相连的方式组合成的一种链式数据结构,并以密码学方式保证的不可篡改和不可伪造的分布式账本。广义来讲,区块链技术是利用块链式数据结构来验证和存储数据、利用分布式节点共识算法来生成和更新数据、利用密码学的方式保证数据传输和访问的安全性、利用由自动化脚本代码组成的智能合约来编程和操作数据的一种全新的分布式基础架构与计算范式。

[0011] 区块链:一种保存记录(数据)的范式

区块:每当有新的数据需要写入区块链,这些数据会汇总到一个区块中,添加在已有区块链的末端。每个区块在保存数据的同时,还要保存前一个区块中所有记录的数据唯一对应的一个数(往往是所有数据的Hash):如果有人试图单独修改前一块中的数据,那么后面这块中保存的这个数就会对不上(“链”不上)

链:所有区块就是通过这样保存前一个块中的信息,链在一起,形成区块链

区块链系统:由分布式网络上一组互相不完全信任的计算机共同参与,通过共识规则,一起维护一套可靠、可追溯、不可篡改的链式数据的系统。

[0012] 我公司涉及的大宗供应链金融场景主要为:首先核心企业与供应商签订货物供应合同,核心企业基于应付账款开立能信给一级供应商,一级供应商可基于与二级供应商的购销合同对能信进行拆分、转让和融资,平台目前可支持到7级流转,理论上可支持能信流转层级的无限制。

[0013] 传统的企业信贷主要存在的问题是信息壁垒,供应商单方面数据可信度低,履约风险高,核验成本高、时间长,供应链金融效率低。基于区块链系统的供应链金融方案,解决中小企业融资难,实现低成本、低风险金融服务。然而在区块链联盟多个参与方中,由于每

个参与节点都存储了交易的账本，这带来另外一个潜在的问题，即如何保护核心企业与供应商之间，多个层级供应商之间业务往来的机密性和隐私性。尤其是在这种多层级的核心企业和多级供应商之间，我们要求能够达到：

多个核心企业之间的能信流转，是互相互斥不可知的。如核心企业A1和A2之间签发的能信和后续的流转，A1和A2之间不可知。

[0014] 对于整个联盟的监管方，监管主体M可以监控到所有的交易流转情况，后续可以基于监管的信息，实现核心企业、供应商的风控分析。

[0015] 以上游核心企业A为初始节点签发的一笔能信，核心企业希望能看到该笔能信后续所有的分发流转的状况，如A可以获知A1与A11或A2与A21的能信分发情况。

[0016] 核心企业如A将一笔能信分发给两个一级供应商如A1和A2，出于商业隐私性保护，A1和A2的能信后续再如何转发，对于两个分支流转的状态，A1和A2是互斥不可见的。如A2不能感知并获取A1与A11的交易信息。

[0017] 对于下游的供应商而言，他可以获知该能信在该分支流的上游信息，但是不能感知其他所不在分支的能信流转信息。每一级供应商可根据自己持有的能信，依次查看到核心企业一直到上一级供应商的能信流转信息，但是仅限于从核心企业流转到它的直接路径信息，不可看到流转到其他供应商或资金方的路径信息。如A11可以获知能信的来源由A到A1，再由A1分发给A11；但是A11无权获取A1分发给A12的交易信息。

[0018] 优选地，上述技术方案中，还包括步骤4：第三方监管交易，交易的监管方针对要监管的交易，获取交易双方的身份信息，使用秘钥派生规则获取或推演出派生秘钥，链上获取加密的交易消息，使用派生秘钥解密获取交易的明文信息。

[0019] 优选地，上述技术方案中，步骤2中，如果交易发起方是第一层，则用第三方监管的公钥加密派生秘钥并提交到区块链上，交易发起方的层级高于交易接收方。

[0020] 优选地，上述技术方案中，所有第一层企业需要将对下一级企业交易流转的对称密钥上交给监管方。

[0021] 优选地，上述技术方案中，步骤2中，每个节点在为下游交易生成对称秘钥的时候，秘钥的生成种子seed的生成规则为：

第一层企业用自身特有的私钥和交易的接收方id号的摘要值，作为参数生成本次交易的加密对称秘钥，用于加密第一层企业和交易接收方即第二层企业的交易信息；

第二层企业向下之间的交易流转中，交易对称加密秘钥的生成规则为，用上一层交易的对称秘钥和交易接收方的id号的摘要值，作为输入参数生成本次交易的对称加密秘钥。

[0022] 区块链供应链金融场景下的交易隐私保护和分层监管系统，该系统同时运行在供应链各层级指定电脑上并相互关联，包括：

身份信息注册装置，供用户创建身份信息；

公私钥对生成装置，用于生成每个用户的公、私钥对；

交易秘钥派生装置，用于生成交易双方派生密钥。

[0023] 与现有技术相比，本发明具有如下有益效果：

在基于区块链实现的多层级的供应链金融场景，实现交易双方交易内容的隐私保护，不泄露用户的交易敏感信息。

[0024] 实现层级化的隐私保护监管能力，上级核心企业可以监控下级多层供应商的交易

信息，底层的供应商不能查看顶层的交易信息,同级别实体之间不能互相查看交易信息。

[0025] 监管方可以监控评估所有的交易信息,实现层级化的监控管理。

[0026] 交易秘钥派生模块集成于现有系统中,使用轻量的智能合约实现,不需要额外引入第三方复杂的秘钥管理和分发服务,降低系统开销。

[0027] 附图说明：

图1为秘钥生成和交易加密的主要实现流程；

图2为监管方的监管流程；

图3为密匙生成规则示意图；

图4为密匙分发流转示意图；

图5为我公司涉及的大宗供应链金融场景；

图6为总流程示意图。

[0028] 具体实施方式：

下面对本发明的具体实施方式进行详细描述,但应当理解本发明的保护 范围并不受具体实施方式的限制。

[0029] 除非另有其它明确表示,否则在整个说明书和权利要求书中,术语“包括”或其变换如“包含”或“包括有”等等将被理解为包括所陈述的元件或组成部分,而并未排除其它元件或其它组成部分。

[0030] 我公司涉及的大宗供应链金融场景主要如图5所示,首先核心企业与供应商签订货物供应合同,核心企业基于应付账款开立能信给一级供应商,一级供应商可基于与二级供应商的购销合同对能信进行拆分、转让和融资,平台目前可支持到7级流转,理论上可支持能信流转层级的无限制。

[0031] 传统的企业信贷主要存在的问题是信息壁垒,供应商单方面数据可信度低,履约风险高,核验成本高、时间长,供应链金融效率低。基于区块链系统的供应链金融方案,解决中小企业融资难,实现低成本、低风险金融服务。然而在区块链联盟多个参与方中,由于每个参与节点都存储了交易的账本,这带来另外一个潜在的问题,即如何保护核心企业与供应商之间,多个层级供应商之间业务往来的机密性和隐私性。尤其是在这种多层级的核心企业和多级供应商之间，我们要求能够达到：

多个核心企业之间的能信流转,是互相互斥不可知的。如核心企业A1和A2之间签发的能信和后续的流转，A1和A2之间不可知。

[0032] 对于整个联盟的监管方,监管主体M可以监控到所有的交易流转情况,后续可以基于监管的信息,实现核心企业、供应商的风控分析。

[0033] 以上游核心企业A为初始节点签发的一笔能信,核心企业希望能看到该笔能信后续所有的分发流转的状况,如A可以获知A1与A11或A2与A21的能信分发情况。

[0034] 核心企业如A将一笔能信分发给两个一级供应商如A1和A2，出于商业隐私性保护,A1和A2的能信后续再如何转发,对于两个分支流转的状态,A1和A2是互斥不可见的。如A2不能感知并获取A1与A11的交易信息。

[0035] 对于下游的供应商而言,他可以获知该能信在该分支流的上游信息,但是不能感知其他所不在分支的能信流转信息。每一级供应商可根据自己持有的能信,依次查看到核心企业一直到上一级供应商的能信流转信息,但是仅限于从核心企业流转到它的直接路径

信息,不可看到流转到其他供应商或资金方的路径信息。如A11可以获知能信的来源由A到A1,再由A1分发给A11;但是A11无权获取A1分发给A12的交易信息。

[0036] 本申请的主要流程:主要实现流程分为身份注册阶段,能信分发阶段和交易监管阶段,包括如图6的4个步骤:

步骤1:注册身份信息,核心企业、供应商、监管方等上线系统, 创建身份标识的公私钥对,并将hash(公钥):公钥作为key-value的身份信息提交到区块链上。

[0037] 步骤2:发起交易 ,交易发起方发起交易请求, 使用交易秘钥派生装置,根据交易的发起方和接收方的身份信息,生成派生秘钥;用派生秘钥加密交易信息并上链;用交易双方的公钥加密派生秘钥并上链;如果交易发起方是核心企业,用监管方的公钥加密派生秘钥并上链。

[0038] 步骤3: 接收交易,交易接收方获取加密的交易信息;交易接收方获取公钥加密的派生秘钥;用本地的私钥解密获取派生秘钥,再解密获取交易信息。

[0039] 步骤4: 监管交易,交易的监管方针对要监管的交易,获取交易双方的身份信息,使用秘钥派生规则获取或推演出派生秘钥。

[0040] 链上获取加密的交易消息,使用派生秘钥解密获取交易的明文信息。

[0041] 秘钥生成规则的基本原理:我们主要采用如下的秘钥分发方案,实现核心企业和多层级的供应商的秘钥分发能力。我们可以使得上级可见所有交易相关的下级密匙,同级别成员之间看不到对方在其上下游交易的秘钥信息。每个节点在为下游交易生成对称秘钥的时候,秘钥的生成种子seed的生成规则为:

每个参与者如核心企业或供应商,注册上线的时候生成代表自己的公钥pk和私钥sk,如核心企业A的公钥pk_A和私钥sk_A。

[0042] 每个参与方将公钥pk_A存储到区块链上, 公钥的hash值为该参与方的身份id号,如id_A=hash(pk_A)。链上存储的键值kv对为 id_A: pk_A。

[0043] 核心企业用自身特有的”私钥”和交易的接收方id号的摘要值,作为参数生成本次交易的加密对称秘钥,用于加密核心企业和交易接收方即一级供应商的交易信息。

[0044] 供应商之间的交易流转中,交易对称加密秘钥的生成规则为,用上一层交易的对称秘钥(s_A_A1)和交易接收方的id号的摘要值,作为输入参数生成本次交易的对称加密秘钥,即s_A1_A11= AES_Gen (s_A_A1 || id_A11)。

[0045] 采用如上的秘钥生成规则,我们可以使得上级对所有下级的交易可见,同级别非相关的交易互相不可见。

[0046] 秘钥分发流转示例:在多层级的能信流转分发的场景中,具体的秘钥派生规则示例如图4所示:

a)核心企业A基于应付账款开立能信时,先对自己的私钥文件sk_A进行哈希,生成私钥的派生文件sk_Ah,sk_Ah : hash(sk_A);

b)核心企业A将开立的能信流转给一级供应商A1时,使用自己的私钥派生文件sk_Ah拼接一级供应商A1的能信账号(id_A1,全局唯一),再使用sha256进行hash,将该值作为一级供应商的对称密钥s_A_A1,s_A_A1: AES_Gen (sk_Ah || id_A1);

c)核心企业使用如上的对称密钥将受让的能信流转信息进行AES-256-CBC加密上链,并用接收方和监管方的公钥加密s_A_A1存储上链;

d)一级供应商查看该笔流转信息时,可以使用自己私钥解密获取对称派生秘钥s_A_A1,再用s_A_A1解密获得交易内容;

e)能信再往下流转时如由A1流转到A11,A1使用上级流转的对称秘钥s_A_A1作为秘钥派生材料,生成本次交易的对称秘钥,s_A1_A11: AES_Gen (s_A_A1 || id_A11)。

[0047] 采用如上的方案,可做到上级根据自己的对称密钥信息计算出下级的对称密钥信息,而下级不可反向计算出上级的对称密钥信息,但可在自己上链的数据中查看到能信流转的直线信息。

[0048] 为使监管方可以看到平台所有能信的流转信息,所有核心企业需要将对一级供应商交易流转的对称密钥上交给监管方,这样监管方可以推导出每个参与方的对称密钥,将加密上链的能信流转信息进行解密查看。

[0049] 监管具体流程为:监管方针对要监管的交易双方主体从链上获取交易的历史路径,从链上获取历史路径中核心企业发送的一级派生密钥,使用监管方的本地私钥获得派生密钥的明文,根据交易历史路径递归计算该路径上的各层级的派生密钥,使用计算出的交易双方的交易加密派生密钥解密交易明文、监管交易信息,最后将监管行为记录上链。

[0050] 基于区块链上存储的可信不可篡改的能信流转信息,核心企业对能信到期兑付的情况,每一级供应商受让能信的情况(认可度)及融资情况,资金方对供应商申请融资放款的效率,植入信誉计算分析模型,进行数据分析,对供应链金融各参与方做出信誉评估,予以奖惩,达到对供应链金融治理优化的目的,推进供应链金融的健康发展。

[0051] 秘钥派生模块的具体实现流程图参见图1和图2,秘钥派生模块主要负责为交易双方主体生成交易加密秘钥,实现层级化的交易监管能力。图1是秘钥生成和交易加密的主要实现流程,图2是监管方的监管流程。

[0052] 技术方案带来的有益效果:

在基于区块链实现的多层级的供应链金融场景,实现交易双方交易内容的隐私保护,不泄露用户的交易敏感信息。

[0053] 实现层级化的隐私保护监管能力,上级核心企业可以监控下级多层供应商的交易信息,底层的供应商不能查看顶层的交易信息,同级别实体之间不能互相查看交易信息。

[0054] 监管方可以监控评估所有的交易信息,实现层级化的监控管理。

[0055] 交易秘钥派生模块集成于现有系统中,使用轻量的智能合约实现,不需要额外引入第三方复杂的秘钥管理和分发服务,降低系统开销。

[0056] 前述对本发明的具体示例性实施方案的描述是为了说明和例证的目的。这些描述并非想将本发明限定为所公开的精确形式,并且很显然,根据上述 教导,可以进行很多改变和变化。对示例性实施例进行选择和描述的目的在 于解释本发明的特定原理及其实际应用,从而使得本领域的技术人员能够实 现并利用本发明的各种不同的示例性实施方案以及各种不同的选择和改变。本发明的范围意在由权利要求书及其等同形式所限定。

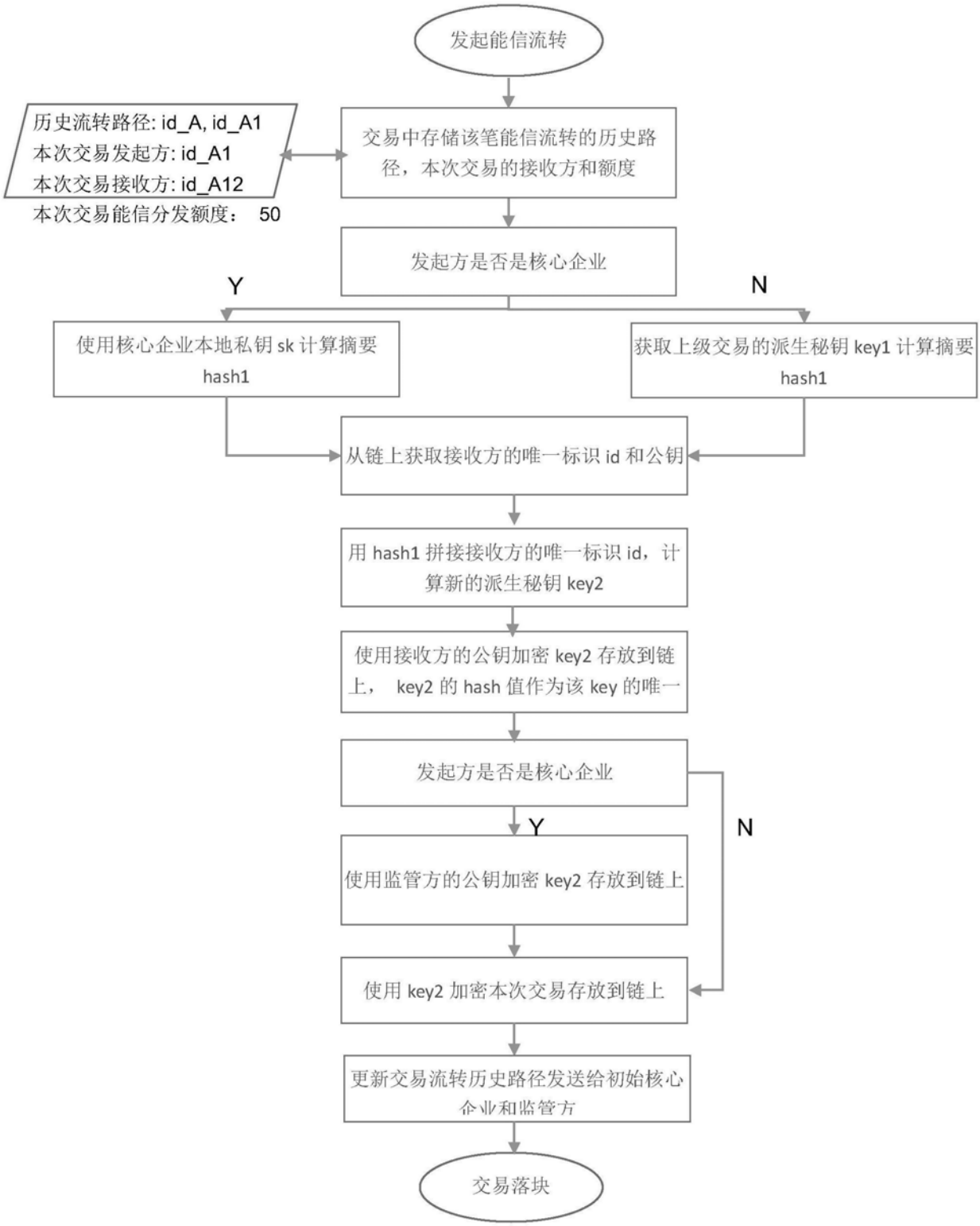

发起能信流转
历史流转路径: id_A, id_A1
本次交易发起方: id_A1
本次交易接收方: id_A12
本次交易能信分发额度： 50
交易中存储该笔能信流转的历史路径，本次交易的接收方和额度
发起方是否是核心企业
Y
N
使用核心企业本地私钥 sk 计算摘要 hash1
获取上级交易的派生秘钥 key1 计算摘要 hash1
从链上获取接收方的唯一标识 id 和公钥
用 hash1 拼接接收方的唯一标识 id，计算新的派生秘钥 key2
使用接收方的公钥加密 key2 存放到链上， key2 的 hash 值作为该 key 的唯一
发起方是否是核心企业
Y
N
使用监管方的公钥加密 key2 存放到链上
使用 key2 加密本次交易存放到链上
更新交易流转历史路径发送给初始核心企业和监管方
交易落块

图1

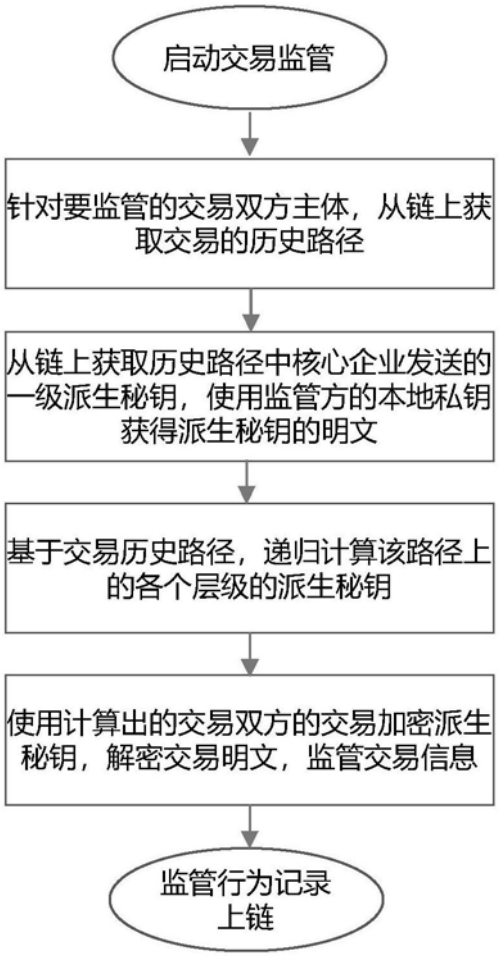

启动交易监管
针对要监管的交易双方主体，从链上获取交易的历史路径
从链上获取历史路径中核心企业发送的一级派生秘钥，使用监管方的本地私钥获得派生秘钥的明文
基于交易历史路径，递归计算该路径上的各个层级的派生秘钥
使用计算出的交易双方的交易加密派生秘钥，解密交易明文，监管交易信息
监管行为记录上链

图2

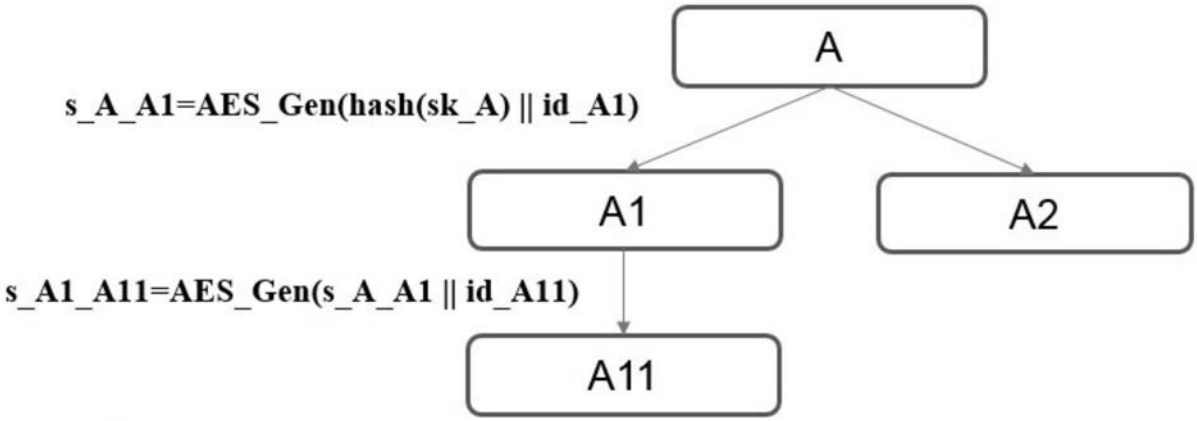

A
s_A_A1=AES_Gen(hash(sk_A) || id_A1)
A1
A2
s_A1_A11=AES_Gen(s_A_A1 || id_A11)
A11

图3

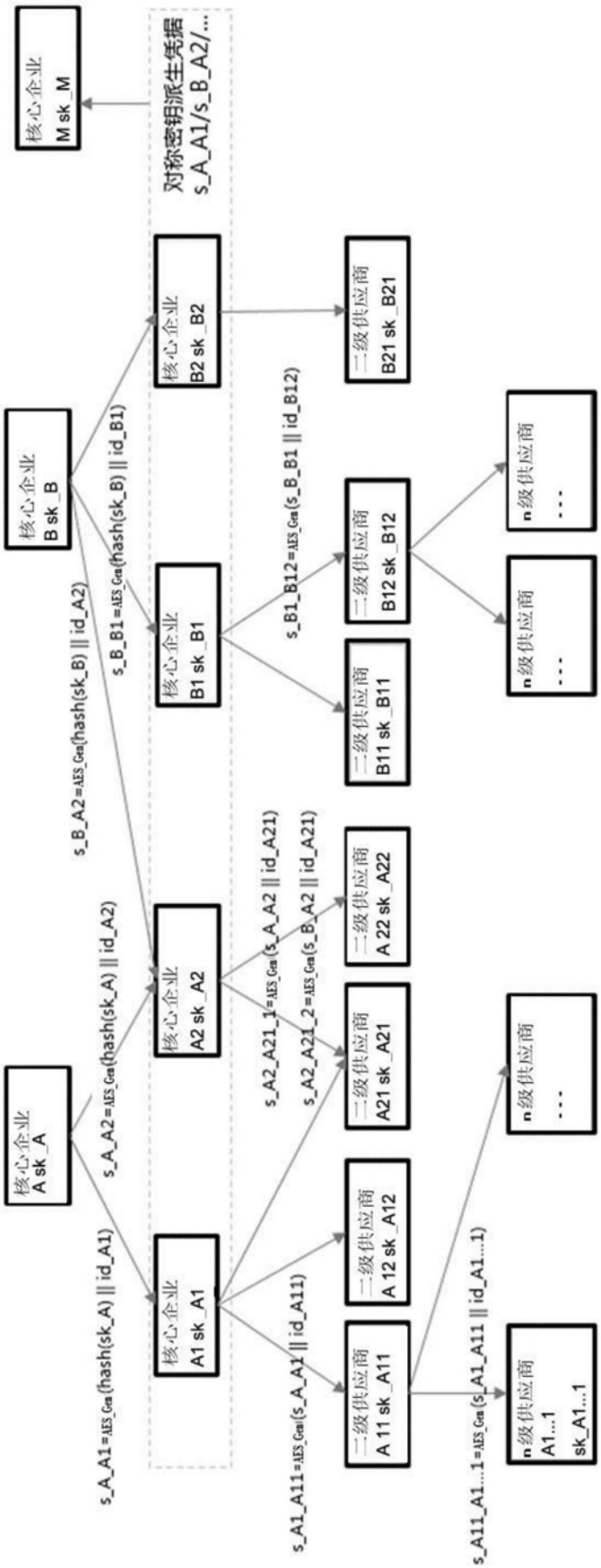

核心企业
M sk_M
对称密钥派生凭据
s_A_A1/s_B_A2/...
核心企业
B sk_B
核心企业
A sk_A
核心企业
A1 sk_A1
核心企业
A2 sk_A2
核心企业
B1 sk_B1
核心企业
B2 sk_B2
二级供应商
A 11 sk_A11
二级供应商
A 12 sk_A12
二级供应商
A21 sk_A21
二级供应商
A 22 sk_A22
二级供应商
B11 sk_B11
二级供应商
B12 sk_B12
二级供应商
B21 sk_B21
n级供应商
A1...1
sk_A1...1
n级供应商
...
n级供应商
...
n级供应商
...
s_A_A1=AES_Gen(hash(sk_A) || id_A1)
s_A_A2=AES_Gen(hash(sk_A) || id_A2)
s_B_A2=AES_Gen(hash(sk_B) || id_A2)
s_B_B1=AES_Gen(hash(sk_B) || id_B1)
s_A1_A11=AES_Gen(s_A_A1 || id_A11)
s_A2_A21_1=AES_Gen(s_A_A2 || id_A21)
s_A2_A21_2=AES_Gen(s_B_A2 || id_A21)
s_B1_B12=AES_Gen(s_B_B1 || id_B12)
s_A11_A1...1=AES_Gen(s_A1_A11 || id_A1...1)

图4

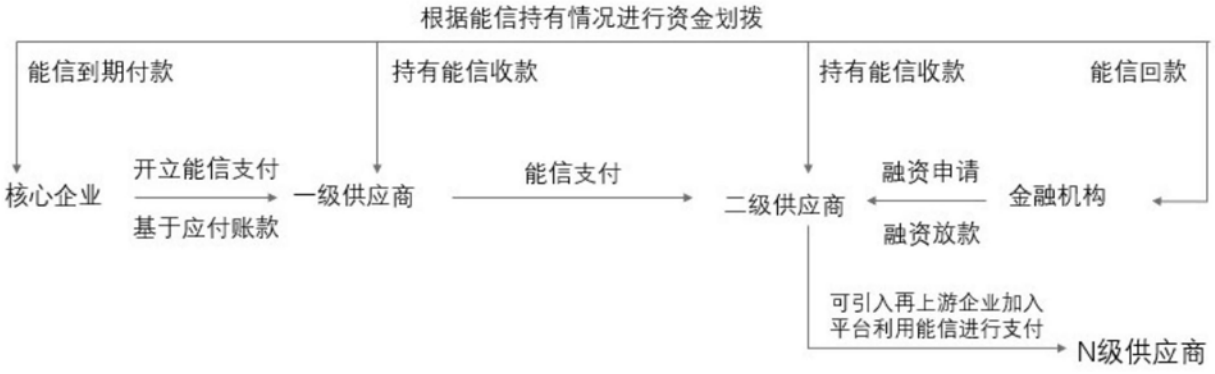

根据能信持有情况进行资金划拨
能信到期付款
持有能信收款
持有能信收款
能信回款
核心企业
开立能信支付
基于应付账款
一级供应商
能信支付
二级供应商
融资申请
融资放款
金融机构
可引入再上游企业加入
平台利用能信进行支付
N级供应商

图5

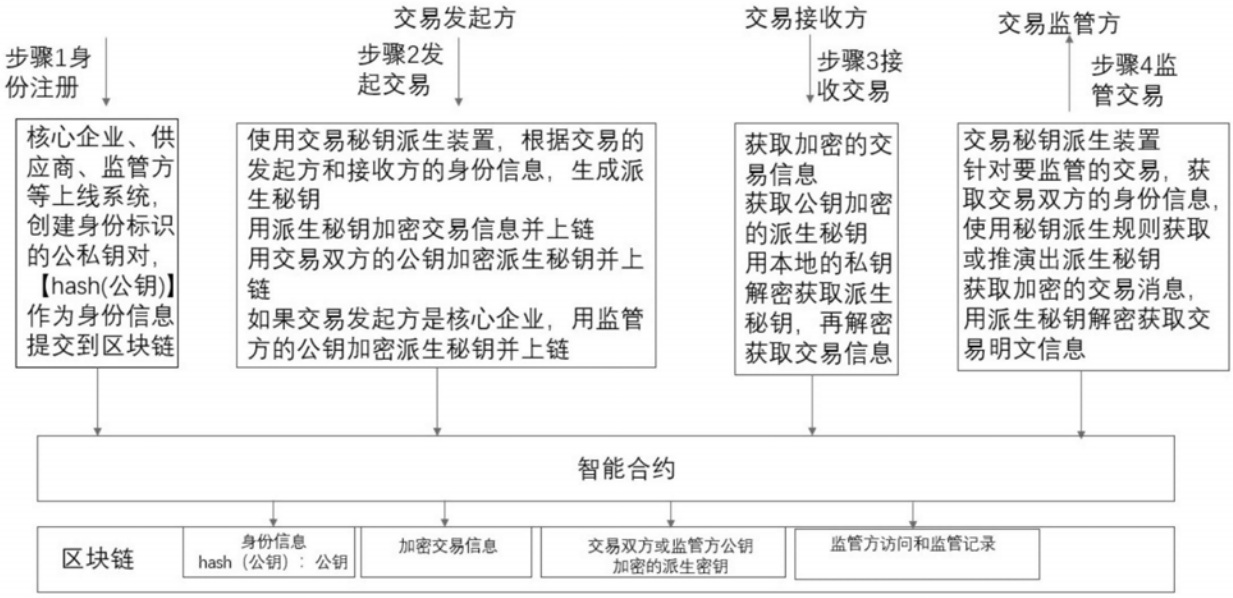

交易发起方
交易接收方
交易监管方
步骤1身份注册
步骤2发起交易
步骤3接收交易
步骤4监管交易
核心企业、供应商、监管方等上线系统，创建身份标识的公私钥对，【hash(公钥)】作为身份信息提交到区块链
使用交易秘钥派生装置，根据交易的发起方和接收方的身份信息，生成派生秘钥
用派生秘钥加密交易信息并上链
用交易双方的公钥加密派生秘钥并上链
如果交易发起方是核心企业，用监管方的公钥加密派生秘钥并上链
获取加密的交易信息
获取公钥加密的派生秘钥
用本地的私钥解密获取派生秘钥，再解密获取交易信息
交易秘钥派生装置
针对要监管的交易，获取交易双方的身份信息，使用秘钥派生规则获取或推演出派生秘钥
获取加密的交易消息，用派生秘钥解密获取交易明文信息
智能合约
区块链
身份信息
hash（公钥）：公钥
加密交易信息
交易双方或监管方公钥加密的派生密钥
监管方访问和监管记录

图6