(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 113545025 A
(43)申请公布日 2021.10.22

(21)申请号 202080018935.6

(22)申请日 2020.01.04

(30)优先权数据
102019000023.4 2019.01.07 DE

(85)PCT国际申请进入国家阶段日
2021.09.06

(86)PCT国际申请的申请数据
PCT/EP2020/050111 2020.01.04

(87)PCT国际申请的公布数据
WO2020/144123 DE 2020.07.16

(71)申请人 艾博希安环球股份有限公司
地址 德国美因茨市

(72)发明人 H·盖斯勒

(74)专利代理机构 南京苏创专利代理事务所(普通合伙) 32273
代理人 凤婷

(51)Int.Cl.
H04L 29/06(2006.01)
H04L 9/32(2006.01)

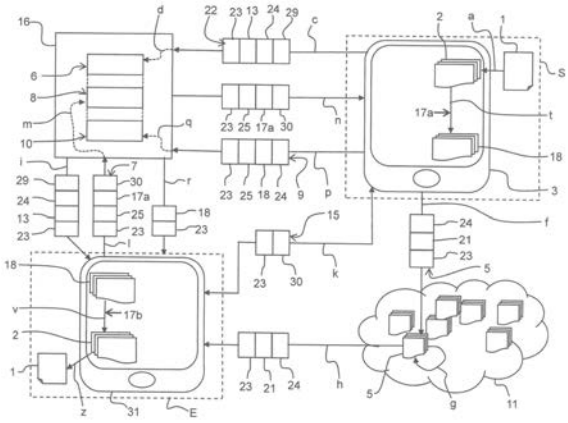
权利要求书3页 说明书12页 附图9页

(54)发明名称

用于信息传输的方法和系统

(57)摘要

本发明涉及一种用于信息传输的方法和系统,其中一条电子信息(2)从发送方(S)的发送端(3)传输到接收方(E)的接收端(31),包括以下步骤:-第一交易步骤(c),其中第一数据记录(22)由发送端(3)生成,所述数据记录具有至少一个散列值(13、14、20),且第一数据记录(22)被传输到区块链(16),-第一验证步骤(d),其中区块链(16)中的第一数据记录(22)被验证并存储为第一经验证数据记录(6),-第二交易步骤(I),其中第二数据记录(7)由接收端(31)生成,所述第二数据记录具有至少一个公共接收方密钥(17a)或接收方标识符(25),且第二数据记录(7)被传输到区块链(16),-第二验证步骤(m),其中区块链(16)中的第二数据记录(7)被验证并存储为第二经验证数据记录(8),-数据加密步骤(o、t、u),其中加密数据(18、19、26)由发送端(3)通过公共接收方密钥(17a)生成,-传输步骤,其中加密数据(18、19、26)被传输到接收端(31),以及-数据解密步骤(v、w、y),其中通过由接收端(31)利用私有接收方密钥(17b)对加密数据(18、19、26)进行解密,使接收方(E)能够访问电子信息(2)。



CN 113545025 A

1.一种用于信息传输的方法,其中电子信息(2)从发送方(S)的发送端(3)传输到接收方(E)的接收端(31),所述方法包括以下步骤:

-第一交易步骤(c),其中包括至少一个散列值(13、14、20)的第一数据记录(22)由发送端(3)生成且第一数据记录(22)被传输到区块链(16),

-第一验证步骤(d),其中,第一数据记录(22)在区块链(16)中被验证并且存储为第一经验证数据记录(6),

-第二交易步骤(I),其中包括至少公共接收方密钥(17a)或接收方标识符(25)的第二数据记录(7)由接收端(31)生成,且第二数据记录(7)被传输到区块链(16),

-第二验证步骤(m),其中,第二数据记录(7)在区块链(16)中被验证并且存储为第二经验证数据记录(8),

-数据加密步骤(o、t、u),其中通过公共接收方密钥(17a)加密的数据(18、19、26)由发送端(3)生成,

-传输步骤,其中加密数据(18、19、26)被传输到接收端(31),以及

-数据解密步骤(v、w、y),其中通过由接收端(31)利用私有接收方密钥(17b)对加密数据(18、19、26)进行解密,使接收方(E)能够访问电子信息(2)。

2.根据权利要求1所述的方法,其特征在于,所述方法包括以下步骤:

-第三交易步骤(p),其中第三数据记录(9)由发送端(3)生成并传输到区块链(16),以及

-第三验证步骤(q),其中所述第三数据记录(9)在区块链(16)中被验证并存储为第三经验证数据记录(10)。

3.根据权利要求2所述的方法,其特征在于,信息标识符(23)被分配给所述电子信息(2),

-其中所述信息标识符(23)由发送端(3)生成并传输到区块链(16)作为第一交易步骤(c)中的第一数据记录(22)的一部分,或者

-其中所述信息标识符(23)由区块链(16)生成并在传输步骤(e)中传输到发送端(3),

-其中至少第二数据记录(7)和第三数据记录(9)包括信息标识符(23),特别是

-其中信息标识符(23)为散列值(13、14、20)之一或散列值(13、14、20)的组合。

4.根据权利要求3所述的方法,其特征在于,执行通知步骤(f),其中通知数据记录(5)存储在数据库(11)中,特别是云中,接收方(E)经由接收端(31)访问数据库,通知数据记录(5)包括至少电子信息(2)的拟发布的描述(21)和信息标识符(23)。

5.根据权利要求4所述的方法,其特征在于,所述数据库(11)执行处理步骤(g),其中对信息(2)的描述(21)和信息标识符(23)进行技术处理。

6.根据前述权利要求中的一项所述的方法,其特征在于,所述方法包括协议步骤(k),其中在发送方(S)和接收方(E)之间交换用于信息传输的协议(30),特别是其中所述协议(30)或所述协议(30)的散列值存储为区块链(16)中第二数据记录(7)的一部分。

7.根据前述权利要求中的一项所述的方法,其特征在于,

-发送端(3)生成电子信息(2)的散列值(13)并且第一数据记录(22)包括所述散列值,

-在于所述方法包括第一数据加密步骤(t),其中信息(2)由发送端(3)利用公共接收方密钥(17a)加密,其中生成了第一加密数据(18),以及

-在于所述方法包括第一数据解密步骤(v),其中第一加密数据(18)由接收端(31)利用私有接收方密钥(17b)解密,其中获得了电子信息(2)。

8.根据权利要求7所述的方法,其特征在于,所述方法包括数据传输步骤(s),其中第一加密数据(18)直接从发送端(3)传输到接收端(31),且特别是其中,

-第三数据记录(9)具有第一加密数据(18)的散列值(27)。

(实施例2和4)

9.根据权利要求1-6中的一项所述的方法,其特征在于,所述方法包括以下步骤:

-信息加密步骤(b),其中,电子信息(2)通过发送方密钥(12)或公共发送方密钥(12a)由发送端(3)进行加密,其中生成了加密信息(4),

-第二数据加密步骤(u),其中由发送端(3)通过公共接收方密钥(17a)对发送方密钥(12)或私有发送方密钥(12b)进行加密,其中生成了第二加密数据(26),

-第二数据解密步骤(w),其中由接收端(31)通过私有接收方密钥(17b)解密第二加密数据(26),其中获得了发送方密钥(12)或私有发送方密钥(12b),以及

-信息解密步骤(x),其中加密信息(4)由接收端(31)通过发送方密钥(12)或私有发送方密钥(12b)进行解密,其中获得了电子信息(2)。

10.根据权利要求9所述的方法,其特征在于,发送端(3)生成加密信息(4)的散列值(20)和发送方密钥(12)或私有发送方密钥(12b)的散列值(14),其中第一数据记录(22)包括这两个散列值(14、20)。

11.根据权利要求9所述的方法,其特征在于,加密信息(4)为通知数据记录(5)的一部分,使得加密信息(4)可以由接收端(31)经由数据库(11)访问。

12.根据权利要求9所述的方法,其特征在于,加密信息(4)为第一数据记录(22)或第三数据记录(9)的一部分,使得加密信息(4)可以由接收端(31)经由区块链(16)访问。

13.根据权利要求9所述的方法,其特征在于,所述方法包括数据传输步骤(s),其中加密数据(4)直接从发送端(3)传输到接收端(31)。

14.根据权利要求9所述的方法,其特征在于,所述方法包括以下步骤:

-第三数据加密步骤(o),其中发送端(3)通过公共接收方密钥(17a)对加密信息(4)进行加密,其中生成了第三加密数据(19),

-数据传输步骤(s),其中第三加密数据(19)从发送方(S)的发送端(3)传输到接收端(31),以及

-第三数据解密步骤(y),其中第三加密数据(19)由接收端(31)通过私有接收方密钥(17b)解密,其中获得了加密信息(4)。

15.根据前述权利要求中的一项所述的方法,其特征在于,所述方法包括转换步骤(a),其中所述信息(1)被转换为电子信息(2),特别是其中所述信息(1)由测量设备生成或者为文档。

16.根据前述权利要求中的一项所述的方法,其特征在于,所述方法包括以下步骤:

-第三交易步骤(yyy),其中第三数据记录(bbb)由接收端(31)生成并传输到区块链(16),以及

-第三验证步骤(zzz),其中第三数据记录(bbb)被存储。

17.一种用于信息传输的系统,包括发送端(3)、接收端(31)和区块链(16),其中发送端

(3)、接收端(31)和区块链(16)设计为执行前述权利要求中的一项所述的方法,且特别地,所述系统另外包括数据库(11)。

用于信息传输的方法和系统

技术领域

[0001] 本发明涉及一种用于信息传输的方法，其中电子信息从发送方的发送端传输到接收方的接收端。此外，本发明涉及一种系统，该系统包括发送方的发送端、接收方的接收端和区块链，该系统旨在执行用于信息传输的方法。

背景技术

[0002] 用于保护信息的状态和交换的方法是已知的，在这些方法中信息的状态以加密的形式传输并存储在一个或多个数据库中。此处使用的加密是为了对第三方保密信息，并使篡改数据变得更加困难。在变型中，数据可以存储多次。此外，还有用于在外部数据库中存储信息的状态和交换的程序，例如在服务公司或在国家机构或诸如监管协会等的其他信用机构。然而，这些程序在数据保护法下有弊端，因为诸如身份证号码或出生日期等个人数据以及敏感信息的状态由第三方存储在服务提供商、信用国家机构或其他信用中心。此外，以诸如平台提供商等服务提供商对数据进行中心存储也带来了存储数据可能在一个地方被更改的风险。此外，在中心服务提供商的情况下，信息的所有者，或者不如说是发送方和接收方依赖于服务提供商提供的数据服务的可用性。这意味着，例如，如果服务提供商关闭数据服务，则信息的所有者和接收方将无法再访问信息的状态和信息交换。此外，由所有者、接收方或其他人自己验证数据是不可能的，相反，这种验证依赖于服务提供商的服务。在这方面，此类解决方案可能会受到国家边界、国家社区或经济领域的限制，这也很困难，因此在这种情况下，这些解决方案为了安全或验证不允许跨越此类边界。

发明内容

[0003] 本发明的目的是提供一种方法和系统，允许在发送方的发送端和接收方的接收端之间进行加密和防篡改的信息传输，其中发送方保持对信息的控制，发送方和接收方能够保持对谁在什么时间有什么信息、接收方在什么时间请求从发送方传输信息进行跟踪。在此过程开始时，对接收方来说信息是未知的。

[0004] 本发明要解决的问题通过具有权利要求1的特征的方法解决，本发明的优选变型由从属权利要求2至15描述。此外，本发明还通过具有权利要求16的特征的系统来实现。

[0005] 更具体地，根据本发明的方法包括以下步骤：

[0006] -第一交易步骤，其中具有至少一个散列值的第一数据记录由发送端生成，且所述第一数据记录被传输到区块链，

[0007] -第一验证步骤，其中在所述区块链中的所述第一数据记录被验证并存储为第一经验证数据记录，

[0008] -第二交易步骤，其中包括至少一个公共接收方密钥或接收方标识符的第二数据记录由接收端生成，且第二数据记录被传输到区块链，

[0009] -第二验证步骤，其中所述第二数据记录在区块链中被验证并存储为第二经验证数据记录，

[0010] -数据加密步骤,其中加密数据由发送端通过公共接收方密钥生成,

[0011] -传输步骤,其中加密数据被传输到接收端,以及

[0012] -数据解密步骤,其中通过由接收端利用私有接收方密钥对加密数据进行解密,使接收方能够访问电子信息。

[0013] 散列值被理解为意指数据记录的可以用于验证该数据记录的真实性的值。从数据记录生成散列值的方法有,例如,MD-2、MD-4、MD-5、SHA-1、SHA-256、LM-Hash、NTLM或Keccak。特别是,数据记录的校验和是数据记录的散列值。用于生成散列值的方法不允许公开有关基础数据记录的任何细节。

[0014] 区块链为分布式、去中心化的数据库,数据记录可以以防篡改的方式存储在其中。为此,数据记录被存储在一个区块中,在该区块中紧挨着数据记录存储前驱区块的前驱散列值。篡改保护是由区块链网络的多个可信赖节点创建的,这些节点执行区块的验证,或者所谓的区块的挖掘或确认,新区块优选为定期形成,最后一个可用区块的前驱散列值也被存储。在验证步骤中,对要存储在区块中的数据记录的有效性进行验证。此外,解决了所谓的密码难题,可信赖的节点必须为其提供计算能力,密码难题的解决也称为工作量证明验证。区块的链存储在多个节点中,特别是节点的同步,以便将有关交易的信息冗余地存储在网络中。由于所有的区块都是基于现有的区块通过将前驱区块的散列值插入到新区块中而形成的,因此形成了一条链。在区块链中验证的数据记录可以通过区块的链接追溯到初始区块,也称为创始区块。链中数据记录的不匹配或篡改可以追溯,因为例如数据记录的内容不再与以前的版本匹配。因此,传输的数据记录在每个经验证的区块链中存储为经验证的数据记录,以防止篡改。例如,可以通过对现有区块形成校验和来追溯对已验证数据记录的更改。

[0015] 经验证的数据记录具有其他数据,例如时间戳、数据记录的长度和/或传输的数据记录的校验和。特别是,区块链网络的区块中所有存储数据的校验和形成为散列值,特别是使用加密哈希函数。

[0016] 加密是将诸如清晰可读的文本等“明文”的数据记录转换为“密文”,即无法理解的字符串。术语“明文”和“密文”应被认为是象征性的。所有类型的数据或数据记录都可以加密,例如文本消息、语音消息、录制的图像或程序的源代码。解密时,从加密数据记录中重新获得明文。对不同的经典和现代对称加密方法和非对称加密方法进行区分。

[0017] 在对称加密方法中,发送方和接收方拥有相同的密钥。在本发明中,发送方密钥为对称加密方法的密钥。已知的方法为例如AES、DES、Triple-DES、Blowfish、Twofish、Cast-128、Cast-256、RC2、RC4、RC5或RC6。

[0018] 在非对称加密方法中,密钥由一对不同的共钥和私钥组成。公钥对应的私钥只有一个。公钥用于加密数据,私钥用于解密加密数据,反之亦然。非对称加密的常用方法为RSA、Diffie-Hellmann-Merkle、McElice或Elgamal。公钥是流通的,而私钥只有对用公钥加密的数据记录进行解密或以可验证的方式加密数据记录的人才能访问。在本发明中,公共发送方密钥、私有发送方密钥、公共接收方密钥和私有接收方密钥是非对称加密方法的密钥。

[0019] 传输到区块链的数据记录经过数字签名。为了进行数字签名,发送方使用非对称加密在私钥的帮助下计算数字数据记录的值,该值称为数字签名。该值允许任何人使用公

钥验证数据记录的来源和完整性。为了能够将使用私钥创建的签名分配给某人，必须将关联的公钥分配给这个人。特别是，对于数字签名，私钥通常应用于传输的数据记录的散列值。在已知公钥的情况下，由于公钥对应的私钥只有一个，因此可以对加密的散列值进行解密。通过将以此方式获得的散列值与传输的数据记录的重新计算的散列值进行比较，可以验证传输的数据记录的来源和完整性。这种散列方法和非对称加密方法的结合可以与诸如所谓的填充法等其他方法相结合，以改进数字签名。已知的数字签名方法为例如RSA、RSA-FDH、RSA-PSS、RSA-OAEP、DSA、El-Gamal、Schnorr签名、Pointcheval-Stern签名、XTR、Cramer-Shoup签名、McEliece-Niederreiter签名、Goldreich-Goldwasser-Halevi签名或NTRU。

[0020] 在底层方法中，发送端生成具有散列值的第一数据记录。特别是，这是发送方希望传输至接收方的电子信息的散列值。第一交易步骤和第一验证步骤的组合允许发送方证明它拥有要在第一交易步骤时传输的电子信息，因为散列值能够实现唯一分配，在所述第一交易步骤中，具有散列值的第一数据记录被传输到区块链，在所述第一验证步骤中，第一经验证数据记录被存储在区块链中。例如，发送方能够证明他在第一交易步骤时拥有某个发明。这种方法的优点是，在第一交易步骤时，信息不必为接收方所知和/或接收方不必为发送方所知。

[0021] 通过第二交易步骤和第二验证步骤，发送方经由区块链获得接收方的公共接收方密钥。一方面，发送方可以直接从第二经验证数据记录获取公共接收方密钥，或者可以使用接收方标识符从公共数据库获得公共接收方密钥。区块链中的第二验证步骤允许发送方和接收方保持追溯第二交易步骤已经执行以及接收方已经请求从发送方传输信息。

[0022] 通过公共接收方密钥，加密数据由发送端生成。特别是，电子信息是利用公共接收方密钥加密的。

[0023] 在将加密数据传输到接收端后，接收方可以通过使用私有接收方密钥解密加密数据来访问电子信息。具体地，接收方可以通过使用私有接收方密钥对利用公共接收方密钥加密的电子信息进行解密来访问电子数据。

[0024] 用于信息传输的所述方法的优点是，发送方仅以加密形式传递其电子信息，而不会公开。此外，只有接收方才能访问所述电子信息。特别地，有利的是，接收方能够通过验证区块链中的散列值来证明他具有在交易时的相应的信息。例如，发送方因此能够证明他在当时有某个想法，从而特别是接收方不能声称他之前有这个想法。通过这种方式，很容易在区块链中以防篡改的方式公开地验证谁具有什么信息，特别是电子信息，以及何时有。

[0025] 优选地，该方法的一个实施例包括以下步骤：

[0026] -第三交易步骤，其中第三数据记录由发送端生成并传输到区块链，以及

[0027] -第三验证步骤，其中所述第三数据记录在区块链中被验证并存储为第三经验证数据记录。

[0028] 有利地，第三交易步骤和第三验证步骤使得可以以防篡改的方式验证发送方何时将第三数据记录存储在区块链中。特别地，第三数据记录可以有利地用于以防篡改的方式向接收方传输数据，因为接收方可以通过接收端访问经验证的第三数据记录。

[0029] 优选地，该方法的一个实施例包括以下步骤：

[0030] -第四交易步骤，其中第四数据记录由接收端生成并传输到区块链，以及

[0031] -第四验证步骤，其中所述第四数据记录在区块链中被验证并存储为第四经验证数据记录。

[0032] 有利地，第四交易步骤和第四验证步骤使得可以以防篡改的方式验证接收方何时将第四数据记录存储在区块链中。特别地，第四数据记录可以有利地用于以防篡改的方式记录信息传输的成功完成，因为经验证的第四数据记录可以通过接收端和发送端访问。

[0033] 作为进一步的替代方案，提出有以下步骤：所述方法包括

[0034] -第三交易步骤，其中第三数据记录由接收端生成并传输到区块链，以及

[0035] -第三验证步骤，其中所述第三数据记录被存储。在该替代方案中，第三交易步骤和第三验证步骤使得可以以防篡改的方式验证接收方何时将第三数据记录存储在区块链中。特别地，第三数据记录可以有利地用于以防篡改的方式记录信息传输的成功完成，

[0036] 因为经验证的第三数据记录可以通过接收端和发送端访问。

[0037] 优选地，在本发明的进一步实施例中，信息标识符与电子信息相关联，

[0038] -其中信息标识符由发送端生成并传输到区块链作为第一交易步骤中的第一数据记录的一部分，或者

[0039] -其中信息标识符由区块链生成并在传输步骤中传输到发送端，

[0040] -其中至少第二数据记录和第三数据记录包括信息标识符。特别优选的是散列值之一或散列值的组合的信息标识符。

[0041] 有利地，因此可以理解，以防篡改的方式，交易步骤和验证步骤涉及什么电子信息。特别地，可以追溯接收方的第二数据记录指向特定信息片段，从而可以由接收方以及由发送方追溯接收方在特定时间向接收方请求特定信息片段。

[0042] 优选地，在本发明的另一实施例中，执行通知步骤，其中通知数据记录存储在数据库中，特别是云中，接收方经由接收端可以访问数据库，其中通知数据记录包括至少拟发布的电子信息的描述和信息标识符。

[0043] 有利地，发送方可以经由数据库、特别是云发布电子信息的描述，尽管该描述不一定对发布至关重要。例如，他可以在数据库中发布想法的粗略描述，而不披露该想法的基本细节。如果接收方基于对发布不重要的描述而对整个电子信息感兴趣，他可以通过第二交易步骤请求所述信息。此外，发送方可以有利地通过第一验证步骤跟踪并且接收方可以检查发送方在什么时间具有电子信息。

[0044] 优选地，在本发明的又一实施例中，数据库执行处理步骤，其中对电子信息的描述和信息标识符进行技术上的处理。例如，描述的关键字存储在数据库中。这具有以下优点：接收者可以更容易地在数据库中搜索和找到电子信息，特别是通过搜索特定关键字。

[0045] 优选地，在本发明的另一实施例中，该方法包括协议步骤，其中信息传输的协议在发送方和接收方之间交换。特别优选地，协议以明文形式存储，或者协议的散列值存储为区块链中的第二数据记录的一部分。

[0046] 有利地，协议步骤产生信息传输条件的交换。特别是，交换保密协议以确保将想法传输给接收方不会损害新颖性。通过将信息存储在区块链中，可以以防篡改的方式验证信息传输的条件是否存在，并且在存储明文的情况下，可以确保传输的条件是明确的。通过结合第二和第三经验证数据记录，很容易在区块链中以防篡改的方式公开地验证接收方和发送方是否知道条件。

[0047] 优选地，在进一步的实施例中，该方法的特征在于

[0048] -发送端生成电子信息的散列值并且第一数据记录具有所述散列值，

[0049] -在于该方法包括第一数据加密步骤，其中信息由发送端通过公共接收方密钥加密，其中生成了第一加密数据，以及

[0050] -在于该方法包括第一数据解密步骤，其中第一加密数据由接收端通过私有接收方密钥解密，其中获得了电子信息。

[0051] 通过电子信息的散列值的生成、第一交易步骤和第一验证步骤，发送方可以有利地验证他在第一交易步骤时拥有电子信息。电子信息通过公共接收方密钥进行加密，使得只有接收方能够从第一加密数据获得电子信息。因此，没有电子信息的公开。尤其是，如果发送方和接收方之前已经签订了保密协议，那么交换想法不会破坏新颖性。此外，所有交易都可以经由区块链以防篡改的方式进行追踪。

[0052] 优选地，在另一实施例中，该方法包括数据传输步骤，其中第一加密数据直接从发送端传输到接收端。特别优选地，第三数据记录具有第一加密数据的散列值。

[0053] 有利地，使用公共接收方密钥加密的电子信息直接在发送端和接收端之间直接传输，使得传输更快并且排除了公众。通过经由区块链传输第一加密数据的散列值，可以以防篡改的方式追踪到接收方已经从发送方接收到正确的第一加密数据。

[0054] 特别优选地，数据传输步骤经由至少一个单独的数据库进行，特别是其中加密的数据被拆分成多个部分序列并且仅在接收端中组合成加密数据。数据库优选地为云。特别优选地，各个部分序列经由不同的数据库传输。有利地，这改善了传输的安全性，因为为了获得电子信息，第三方需要加密数据的所有部分序列。尤其是由于加密数据的各个部分序列经由不同的数据库传输这一事实而变得更加困难。

[0055] 优选地，在另一变型中，该方法包括以下步骤：

[0056] -信息加密步骤，其中发送端通过发送方密钥或公共发送方密钥对电子信息进行加密，其中生成了加密信息，

[0057] -第二数据加密步骤，其中发送端通过公共接收方密钥对发送方密钥或私有发送方密钥进行加密，其中生成了第二加密数据，

[0058] -第二数据解密步骤，其中接收端通过私有接收方密钥解密第二加密数据，其中获得了发送方密钥或私有发送方密钥，以及

[0059] -信息解密步骤，其中接收端通过发射方密钥或私有发射方密钥对加密信息进行解密，其中获得了电子信息。

[0060] 有利地，这增加了传输的安全性，因为必须执行两个解密步骤才能获得电子信息。

[0061] 优选地，在本发明的另一实施例中，发送端生成加密信息的散列值和发送方密钥或私有发送方密钥的散列值，其中第一数据记录包括这两个散列值。有利地，因此可以经由区块链以防篡改的方式验证发送方在第一交易时具有电子信息，并且有利地，因此进一步增加了防止篡改的保护，因为2个散列值经由加密方法相关联，以经验证的方式存储。

[0062] 优选地，在本发明的另一实施例中，发送端生成信息的散列值、加密信息的散列值和发送方密钥或私有发送方密钥的散列值，其中第一数据记录包括这三个散列值。

[0063] 有利地，可以经由区块链以防篡改的方式验证发送方在第一交易时具有电子信息，并且有利地，因此进一步增加了防篡改保护，因为3个散列值通过加密方法相关联，以经

验证的方式存储。

[0064] 在本发明的优选实施例中，加密信息为通知数据记录的一部分，使得加密信息可以由接收端经由数据库访问。

[0065] 有利地，因此可以避免经由区块链传输加密信息，以保持区块链的区块的数据量尽可能小。

[0066] 在本发明的替代实施例中，加密信息为第一数据记录或第三数据记录的一部分，使得加密信息可以由接收端经由区块链访问。

[0067] 有利地，这使得可以以防篡改的方式验证加密信息已经从发送方传送到接收方。在本发明的替代实施例中，该方法包括数据传输步骤，其中加密信息直接从发送端传输到接收端。

[0068] 有利地，这避免了经由区块链传输加密信息，以便保持区块链的区块的数据量尽可能小。此外，可以私密地传输信息。此外，加密信息可以通过直接的方式更快地传输。

[0069] 优选地，本发明的另一实施例另外包括以下步骤：

[0070] -第三数据加密步骤，其中发送端通过公共接收方密钥对加密信息进行加密，其中产生了第三加密数据，

[0071] -数据传输步骤，其中第三加密数据直接从发送方的发送端传输到接收端，以及

[0072] -第三数据解密步骤，其中接收端利用私有接收方密钥解密第三加密数据，其中获得了所述加密信息。

[0073] 特别优选地，发送端生成第三加密数据的散列值，其中特别是第三数据记录包括该散列值。

[0074] 有利地，这实现了更安全的传输，因为需要三个解密才能获得电子信息。此外，第三加密数据的散列值，即通过公共接收者密钥加密的加密信息，可以以防篡改的方式验证发送方在第三交易步骤时具有电子信息，即在接收方可以获得信息之前，因为解密所需的第二加密数据，即利用公共接收方密钥加密的发送方密钥或私有发送方密钥，也可以经由第三交易步骤提供给接收方。

[0075] 优选地，在另一实施例中，该方法包括转换步骤，其中所述信息被转换为电子信息，特别是其中所述信息由测量设备生成或者为文档。在转换步骤中，信息、特别是文档或测量值，被收发器转换成电子信息。

[0076] 优选地，在本发明的另一实施例中，区块链的计算机位于数据库中。

[0077] 该方法可以用不同的区块链执行。优选地，该方法用一个区块链执行。

[0078] 本发明的另一主题为一种包括发送端、接收端和区块链的系统，其中这些被设计为执行上述方法。优选地，所述系统还包括数据库，特别是云。特别优选地，区块链的一台或多台计算机为数据库的一部分。

附图说明

[0079] 本发明的有利实施例在以下附图中通过示例的方式进行说明。附图示出了：

[0080] 图1：本发明的实施例的示意图，其中电子信息通过公共接收方密钥加密并通过私有接收方密钥解密，且其中第一加密数据从发送方至接收方通过区块链传输，

[0081] 图2：图1的实施例的变型的示意图，其中第一加密数据直接从发送方至接收方通

过数据传输步骤传输，

[0082] 图3:图2的实施例的变型的示意图,其中信息标识符从区块链生成，

[0083] 图4:本发明的另一实施例的示意图,其中电子信息用公共发送方密钥或发送方密钥进行加密,用私有发送方密钥或发送方密钥进行解密,且其中加密信息从发送方至接收方经由数据库进行传输，

[0084] 图5:图4中的实施例的变型的示意图,其中加密信息从发送方至接收方经由区块链通过第一交易步骤进行传输，

[0085] 图6:图4中的实施例的变型的示意图,其中加密信息从发送方至接收方经由区块链通过第三交易步骤进行传输，

[0086] 图7:图4中的实施例的变型的示意图,其中加密信息直接从发送方至接收方通过数据传输步骤传输，

[0087] 图8:图4的扩展实施例的示意图,其中,加密信息另外通过公共接收方密钥进行加密并通过私有接收方密钥进行解密,且其中第三加密数据直接从发送方至接收方通过数据传输步骤进行传输,以及

[0088] 图9:图8的实施例的变型的示意图,其中信息标识符通过区块链生成。

具体实施方式

[0089] 图1示出了本发明的一个实施例,其中信息1从发送方S至接收方E传输。发送方S具有发送端3,其具有电子信息2。电子信息2特别是通过转换步骤a生成,在转换步骤a中,例如,将文档形式的信息1转换为电子信息2。类似地,在接收方E的接收端31中执行再转换步骤z,以便从电子信息2获得信息1。除了发送端3和接收端31之外,根据本发明的系统包括区块链16和数据库11,其中数据库11为特别是云。

[0090] 为了将电子信息2从发送端3传输到接收端31,执行以下步骤。首先,执行第一交易步骤c,其中第一数据记录22由发送端3生成并传送到区块链16。数据记录22具有信息标识符23、电子信息2的闪存值13、发送方签名及发送方信息24以及附加数据29。在第一验证步骤d中,第一数据记录22在区块链16中进行验证并且存储为第一经验证数据记录6。第一经验证数据记录6使发送方S能够以防篡改的方式验证他具有在第一交易步骤c时的电子信息2,因为电子信息2的闪存值13允许唯一的赋值。

[0091] 在通知步骤f中,发送端3向数据库11发送通知数据记录5。通知数据记录5还包括信息标识符23。此外,通知数据记录5包括电子信息2的描述21和发送方签名及发送方信息24。描述21为对电子信息2的发布不重要的描述,使得通知数据记录5可以在不披露电子信息2的实质内容的情况下在数据库11中发布。优选地,处理步骤g在数据库11中执行,在该步骤中,对通知数据记录5进行处理以便更容易使用。例如,将描述21的关键字单独存储,以便更容易地找到通知数据记录5。

[0092] 发送端3和接收端31可以访问区块链16中的经验证数据记录。访问理解为发送端3或接收端31主动读取区块链16的经验证数据记录和/或经验证数据记录由区块链16发送到发送端3或接收端31。另外,发送端3和接收端31可以访问数据库11中的数据记录,其中对数据库11的访问也可以理解为由发送端3或接收端31主动读取数据记录和/或由数据库11向发送端3或接收端31发送数据记录。

[0093] 通过第一访问i，接收端31访问第一经验证数据记录6，其中特别地，其从第一经验证数据记录6获取电子信息2的信息标识符23和散列值13。

[0094] 通过云访问h，接收端31接收通知数据记录5的数据，即信息标识符23、描述21和发送方签名及发送方信息24。基于信息标识符23，接收端31可以将对应的第一经验证数据记录6与通知数据记录5相关联。

[0095] 如果接收方E对电子信息2感兴趣，还可以进行协议步骤k，其中，协议数据记录15在接收方E和发送方S之间通过接收端31和发送端3进行交换。协议数据记录15包括信息标识符23和协议30。协议30优选地为由接收方E和发送方S双方签署的保密协议。保密协议优选地确保接收方E和发送方S之间的信息交换不损害信息1或电子信息2的新颖性。

[0096] 如果接收方E对电子信息2感兴趣，并且如果可选地执行了与协议30的附加协议步骤k，则它执行第二交易步骤I，其中第二数据记录7被传输到区块链16。第二数据记录7包括信息标识符23、接收方签名及接收方信息25、公共接收方密钥17a和可选的协议30。在第二验证步骤m中，第二数据记录7在区块链中进行验证并且存储为第二经验证数据记录8。

[0097] 通过第二访问n，发送端3接收第二经验证数据记录8的数据，即信息标识符23、接收方签名及接收方信息25、公共接收方密钥17a和可选的协议30。通过第二验证步骤m，发送方S可以以防篡改的方式验证接收方E已经向发送方S发送了对带有信息标识符23的电子信息2的请求。

[0098] 在第一数据加密步骤t中，发送端3通过公共接收方密钥17a加密电子信息2，其中生成了第一加密数据18。在图1所示的情况下，发送端3直接通过第二访问n获得公共接收方密钥17a。可选地，发送端3可以通过基于接收方签名及接收方信息25搜索接收方E的公共接收方密钥17a的公共数据库来获得公共接收方密钥17a。在第一数据加密步骤t之后，执行第三交易步骤p，其中第三数据记录9被传送到区块链16。第三数据记录包括信息标识符23、接收方签名及接收方信息25、第一加密数据18和发送方签名及发送方信息24。在第三验证步骤q中，第三数据记录9在区块链16中进行验证并且存储为第三经验证数据记录10。

[0099] 通过第三访问r，接收方E通过接收端31从区块链16中提取信息标识符23和第一加密数据18。在接收端31中，第一加密数据18，即通过公共接收方密钥17a加密的电子信息2，在第一数据解密步骤v中通过接收方E的私有接收方密钥17b解密。因此，接收方E通过第一数据解密步骤v接收电子信息2。

[0100] 图2示出了图1中所示的本发明实施例的变型，其中第一加密数据18通过数据传输步骤s直接从发送端3传输至接收端31。以此方式，区块链16中的数据量保持在低水平并且实现第一加密数据18的快速传输。代替第一加密数据18，第三数据记录9包括第一加密数据18的闪存值27。闪存值27存储在区块链16中的第三经验证数据记录10中，其中接收端31可以经由第三访问r访问闪存值27。第一加密数据18的闪存值27使接收端31能够比较由数据传输步骤s传输的加密数据18是否与在区块链16中验证的数据匹配。

[0101] 图3示出了图2中所示的本发明实施例的变型，其中信息标识符23由区块链16生成并存储在第一经验证数据记录6中。由区块链16生成的信息标识符23通过传输步骤e传输到发送端3。因此，该方法的所有数据记录都包括信息标识符23。接收端31从区块链16的第一经验证数据记录6获取信息标识符23。

[0102] 图4示意性地示出了本发明的另一实施例，其中由于双重加密使得更安全的通信

成为可能。在发送端3中，电子信息2通过发送方密钥12或公共发送方密钥12a进行加密，其中生成了加密信息4。这是信息加密步骤b。此外，在第二数据加密步骤u中，发送方密钥12或私有发送方密钥12b通过公共接收方密钥17a进行加密，其中生成了第二加密数据26。在本发明的该实施例中，第一数据记录22包括发送方密钥12或私有发送方密钥12b的闪存值14和加密信息4的闪存值20。通过闪存值14和闪存值20的交易，可以由发送方S验证他具有在第一交易步骤c时的电子信息2，因为通过第一验证步骤d，第一数据记录22以防止修改的方式存储在区块链16中。

[0103] 第一访问i使接收方通过接收端31访问第一经验证数据记录6。加密信息4经由数据库11从发送端3传输至接收端31，其中加密信息4为通知数据记录5的一部分，接收端31可以通过云访问h访问通知数据记录。第二加密数据26经由区块链16从发送端3传输至接收端31，其中第二加密数据26为第三数据记录9的一部分，其在第三交易步骤p中传送到区块链16。接收端31经由第三访问r访问第三经验证数据记录10，其中第二加密数据26以防止修改的方式存储。

[0104] 通过首先执行第二数据解密步骤w，接收方E可以通过接收端31访问电子信息2，其中第二加密数据26使用私有接收方密钥17b解密。通过第二数据解密步骤w，接收方E因此达到发送方密钥12或私有发送方密钥12b。在信息解密步骤x中，加密信息4通过发送方密钥12或私有发送方密钥12b进行解密，其中生成了电子信息2，使得电子信息2存在于接收端31中。从电子信息2，接收方E可以通过再转换步骤z得出信息1。该变型的优点在于，第二加密数据26和加密信息4彼此分开传输，并且需要两个解密步骤才能获得电子信息2，从而实现电子信息2的安全传输。

[0105] 图5示出了图4实施例的变型，在该变型中，加密信息4和第二加密数据26经由区块链16从发送端3传输到接收端31。加密信息4为第一数据记录22的一部分，其在第一交易步骤c中被传送到区块链16。第一数据记录22通过第一验证步骤d被存储在区块链16中作为第一经验证数据记录6。接收方E有可能经由第一访问i通过接收端31获得加密信息4。在本发明的该变型中，加密信息4和第二加密数据26都通过区块链16传输。否则，执行与图4的实施例中相同的方法步骤。

[0106] 图6示出了图4的实施例的另一变型，其中，在该变型中，加密信息4和第二加密数据26经由区块链16从发送端3传输到接收端31。在该变型中，加密信息4和第二加密数据26为第三数据记录9的一部分并且通过第三交易步骤p被传输到区块链16中。第三数据记录9在第三验证步骤q中存储在区块链16中作为第三经验证数据记录10。接收端31然后有可能经由第三访问r从区块链16读取加密信息4和第二加密数据26。在接收端31中，通过第二数据解密步骤w从第二加密数据26获得发送方密钥12或私有发送方密钥12b。通过发送方密钥12或私有发送方密钥12b，执行信息解密步骤x，其中获得了电子信息2。该变型的优点是发送方S不将加密信息4存储在区块链16中，直到接收方E通过第二交易步骤I请求具有信息标识符23的电子信息2，使得发送方S保留对电子信息2或加密电子信息4的主权。

[0107] 图7示意性地示出了图4的实施例的进一步变型，在该变型中，加密信息4和第二加密数据26通过数据传输步骤s直接从发送端3传输到接收端31。在本发明的该实施例中，电子信息2在信息加密步骤b中通过传感器密钥12对称加密，其中生成了加密信息4。发送方密钥12通过公共接收方密钥17a加密，其中生成了第二加密数据26。这些数据然后在数据传输

步骤s中传输到接收方E。在图7的变型中，信息标识符23由区块链16生成，并通过传输步骤e从区块链16传输到发送端3。可选地，信息标识23也可以在发送端3中生成。图7的变型具有以下优点：信息可以通过数据传输步骤s在发送方S和接收方E之间快速交换，而区块链16中的数据量不会变得太大。

[0108] 本发明的另一实施例如图8所示，其中提高了信息传输的安全性，因为需要三个解密步骤才能得到电子信息2。在发送端3中，电子信息2由信息加密步骤b使用发送方密钥12或公共发送方密钥12a进行加密，其中生成了加密信息4。加密信息4另外在第三数据加密步骤o中通过公共接收方密钥17a加密，其中生成了第三加密数据19。此外，发送方密钥12或私有发送方密钥12b通过公共接收方密钥17a通过第二数据加密步骤u加密，其中生成了第二加密数据26。第二加密数据26为第三数据记录9的一部分并且通过第三交易步骤p被传送到区块链16。接收端31通过第三访问r读取第二加密数据26。另一方面，第三加密数据19通过数据传输步骤s直接从发送端3传输到接收端31。

[0109] 该方法还可以另外包括以下步骤：

[0110] -第三交易步骤yyy，其中第三数据记录bbb由接收端31生成并传输到区块链16，以及

[0111] -第三验证步骤zzz，其中对第三数据记录bbb进行存储。

[0112] 接收方E获得电子信息2，方式为，第二数据解密步骤w首先由接收端31执行，其中第二加密数据26通过私有接收方密钥17b解密，生成了发送方密钥12或私有发送方密钥12b。然后，解密第三加密数据19，其中首先执行第三数据解密步骤y，其中第三加密数据19通过私有接收方密钥17b解密，使得加密信息4存在于接收端31中。然后在信息解密步骤x中通过发送方密钥12或私有发送方密钥12b对加密信息4进行解密，其中生成了电子信息2。该实施例是特别安全的，因为需要三个解密步骤，且第三加密数据19和第二加密数据26独立地传输到接收端。此外，由于第三加密数据19的散列值28为第三数据记录9的一部分，所以可以确保发送方S具有在第三交易步骤p时的电子信息2。此外，第三加密数据19的散列值28使接收方E能够验证在数据传输步骤s中是否实际传输了正确的第三加密数据19。

[0113] 图9示出了图8的实施例的变型，其中信息标识符23由区块链16生成，且第一经验证数据记录6包括信息标识符23。由区块链16生成的信息标识符23通过传输步骤e传输到发送端3。该方法的所有数据记录都具有用于识别信息的信息标识符23。

[0114] 附图标记列表：

[0115] 1 信息

[0116] 2 电子信息

[0117] 3 发送端

[0118] 4 加密信息

[0119] 5 通知数据记录

[0120] 6 第一经验证数据记录

[0121] 7 第二数据记录

[0122] 8 第二经验证数据记录

[0123] 9 第三数据记录

[0124] 10 第三经验证数据记录

[0125] 11 数据库,云

[0126] 12 发送方密钥

[0127] 12a 公共发送方密钥

[0128] 12b 私有发送方密钥

[0129] 13 电子信息2的散列值

[0130] 14 发送方密钥12或私有发送方密钥12b的散列值

[0131] 15 协议数据记录

[0132] 16 区块链

[0133] 17a 公共接收方密钥

[0134] 17b 私有接收方密钥

[0135] 18 第一加密数据(利用公共接收方密钥17a加密的电子信息2)

[0136] 19 第三加密数据(利用公共接收方密钥17a加密的加密信息4)

[0137] 20 加密信息4的散列值

[0138] 21 电子信息2的描述

[0139] 22 第一数据记录

[0140] 23 信息标识符

[0141] 24 发送方签名及发送方信息

[0142] 25 接收方签名及接收方信息

[0143] 26 第二加密数据(利用公共接收方密钥17a或公共发送方密钥12a加密的发送方密钥12)

[0144] 27 第一加密数据18的散列值

[0145] 28 第三加密数据19的散列值

[0146] 29 附加数据

[0147] 30 协议

[0148] 31 接收端

[0149] E 接收方

[0150] S 发送方

[0151] a 转换步骤

[0152] b 信息加密步骤

[0153] c 第一交易步骤

[0154] d 第一验证步骤

[0155] e 传输步骤

[0156] f 通知步骤

[0157] g 处理步骤

[0158] h 云访问

[0159] i 第一访问

[0160] k 协议步骤

[0161] l 第二交易步骤

[0162] m 第二验证步骤

[0163] n 第二访问

[0164] o 第三数据加密步骤

[0165] p 第三交易步骤

[0166] q 第三验证步骤

[0167] r 第三访问

[0168] s 数据传输步骤

[0169] t 第一数据加密步骤

[0170] u 第二数据加密步骤

[0171] v 第一数据解密步骤

[0172] w 第二数据解密步骤

[0173] x 信息解密步骤

[0174] y 第三数据解密步骤

[0175] z 再转换步骤

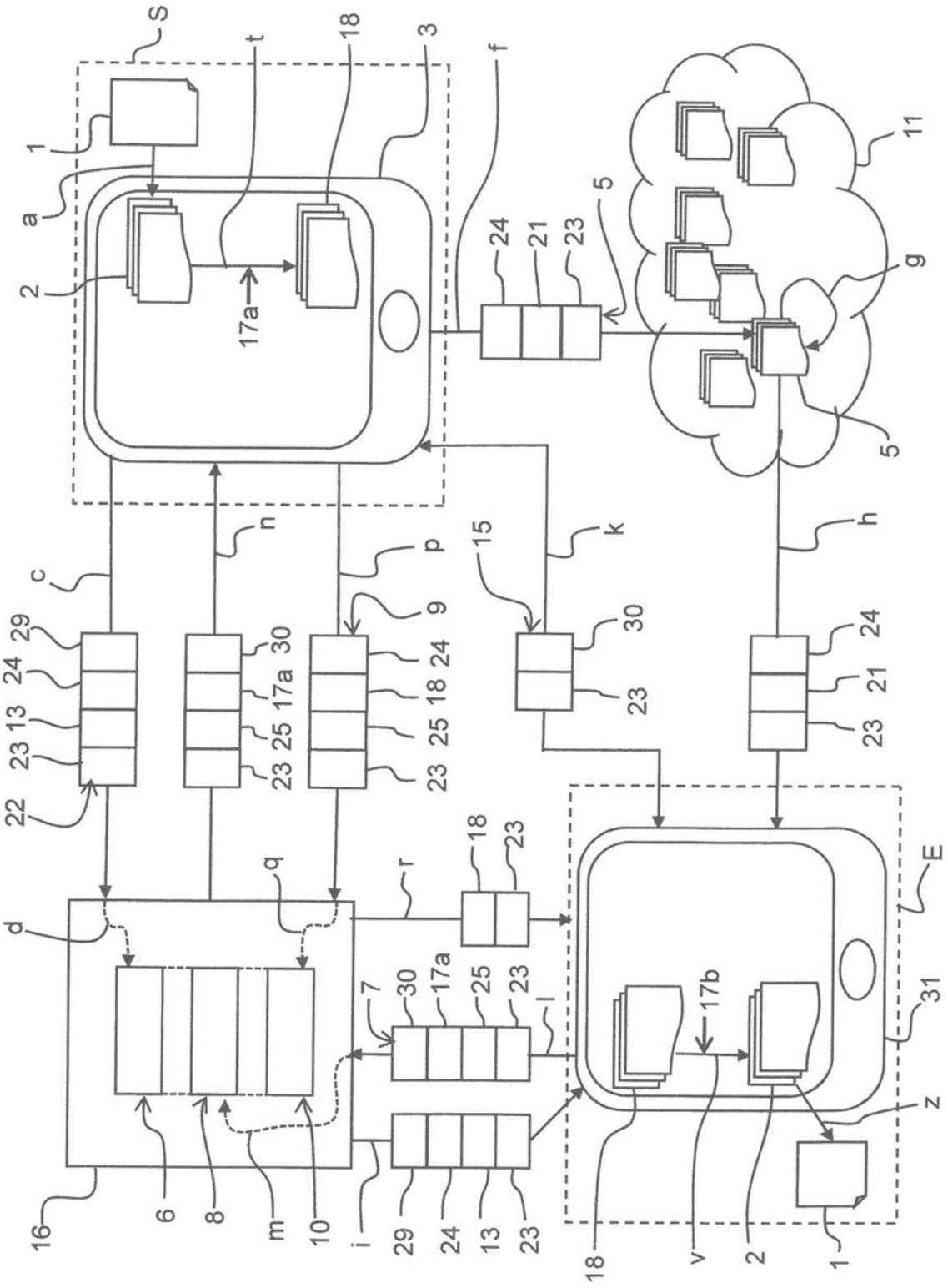

S
t
18
3
f
1
a
2
17a
11
5
24
21
23
g
5
n
p
15
k
h
c
29
24
13
23
22
30
17a
25
23
9
18
24
25
23
30
23
24
21
23
18
23
E
d
q
r
7
30
17a
25
23
l
17b
31
z
16
6
8
m
10
i
29
24
13
23
18
v
2
1

图1

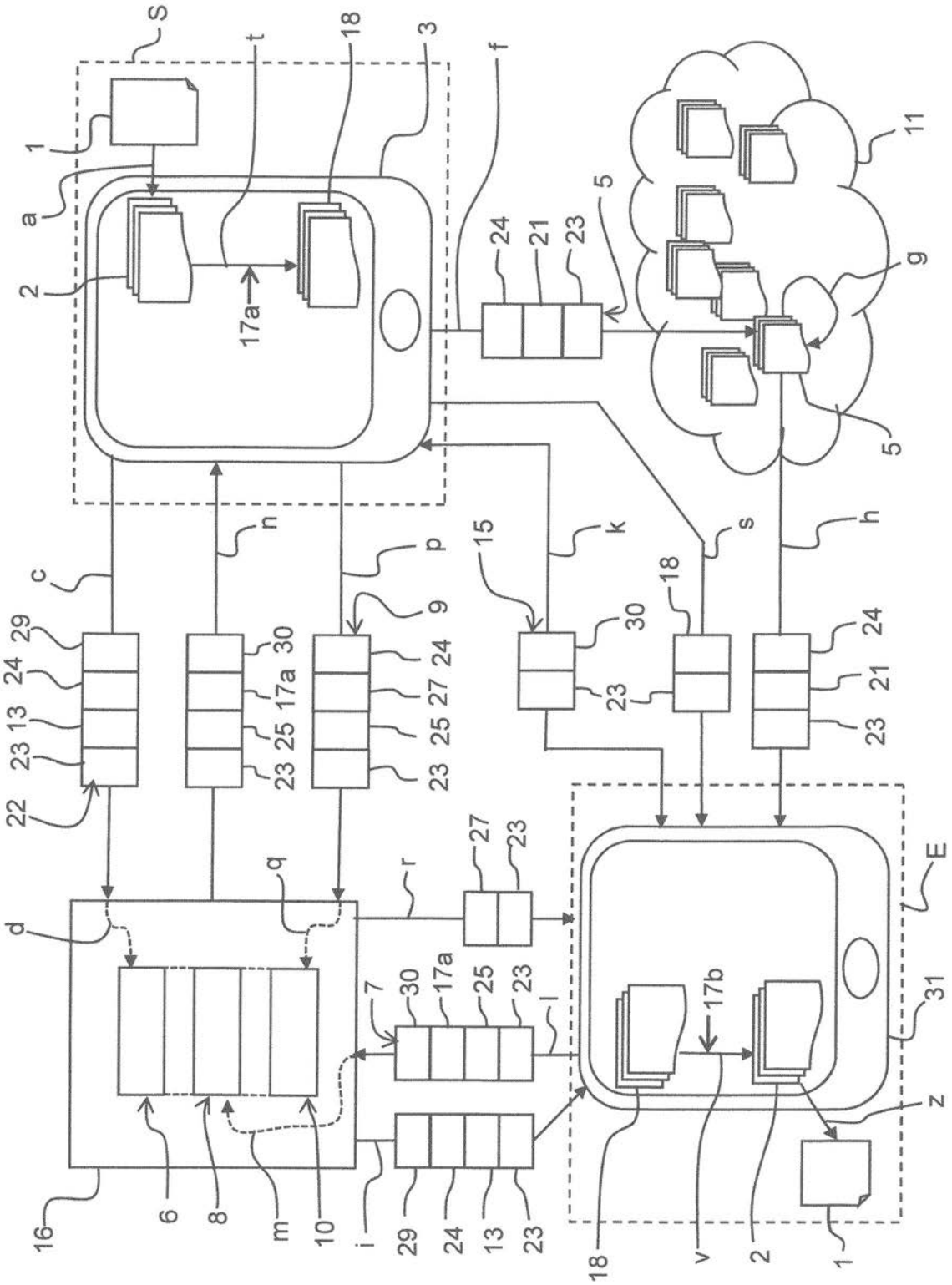

S
t
18
3
f
1
a
2
17a
11
5
24
21
23
g
5
n
p
15
k
s
h
c
9
18
29
24
13
23
22
30
17a
25
27
23
30
24
21
23
27
23
E
q
r
d
7
30
17a
25
23
l
17b
31
z
16
6
8
m
10
i
29
24
13
23
18
v
2
1

图2

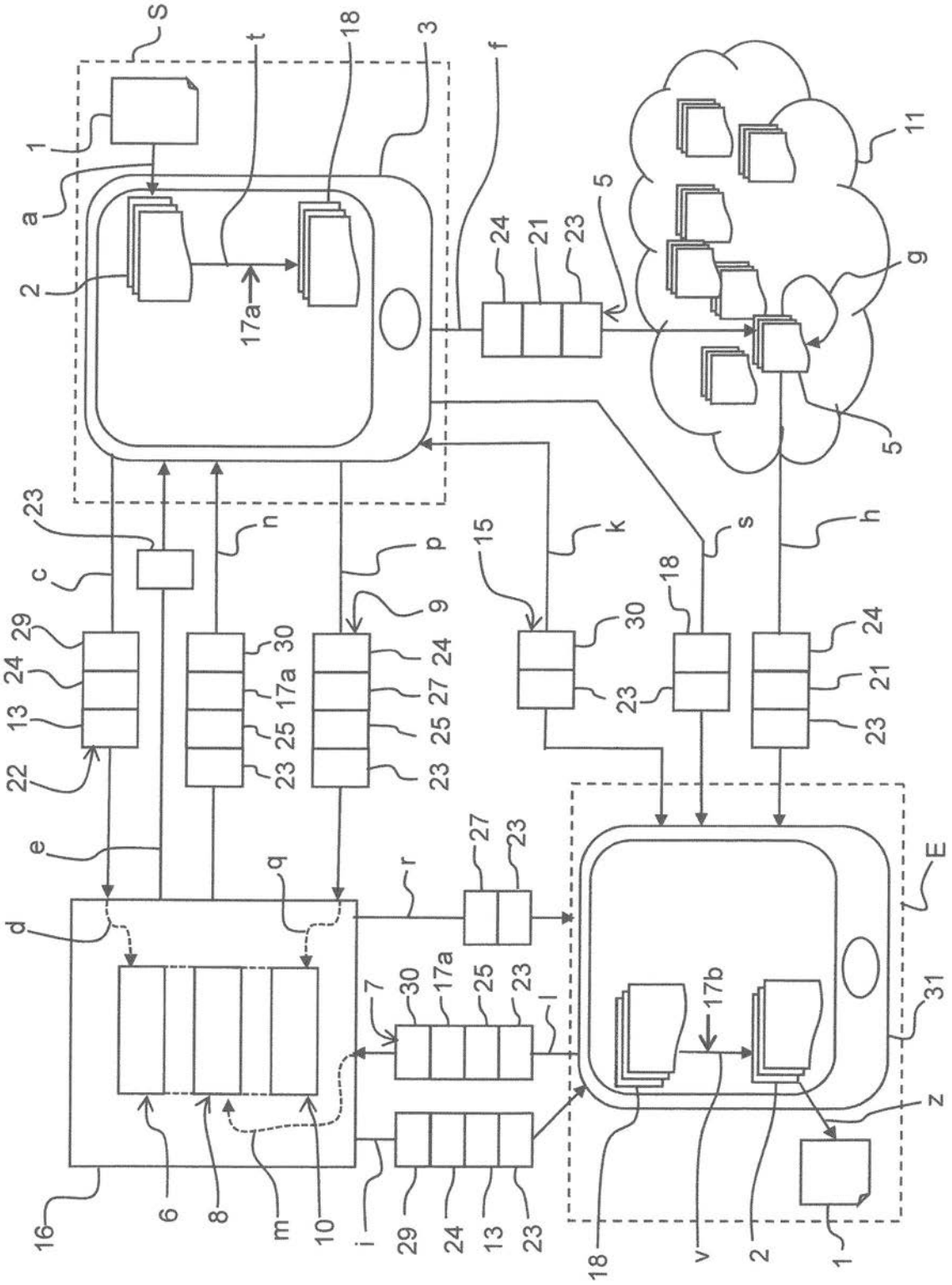

S
t
18
3
f
1
a
2
17a
11
5
24
21
23
g
23
n
p
15
k
s
h
c
9
18
29
30
24
24
21
13
17a
27
30
23
25
25
23
23
22
e
27
23
q
r
E
d
7
30
17a
25
23
l
17b
31
z
16
6
8
m
10
i
29
24
13
23
18
v
2
1

图3

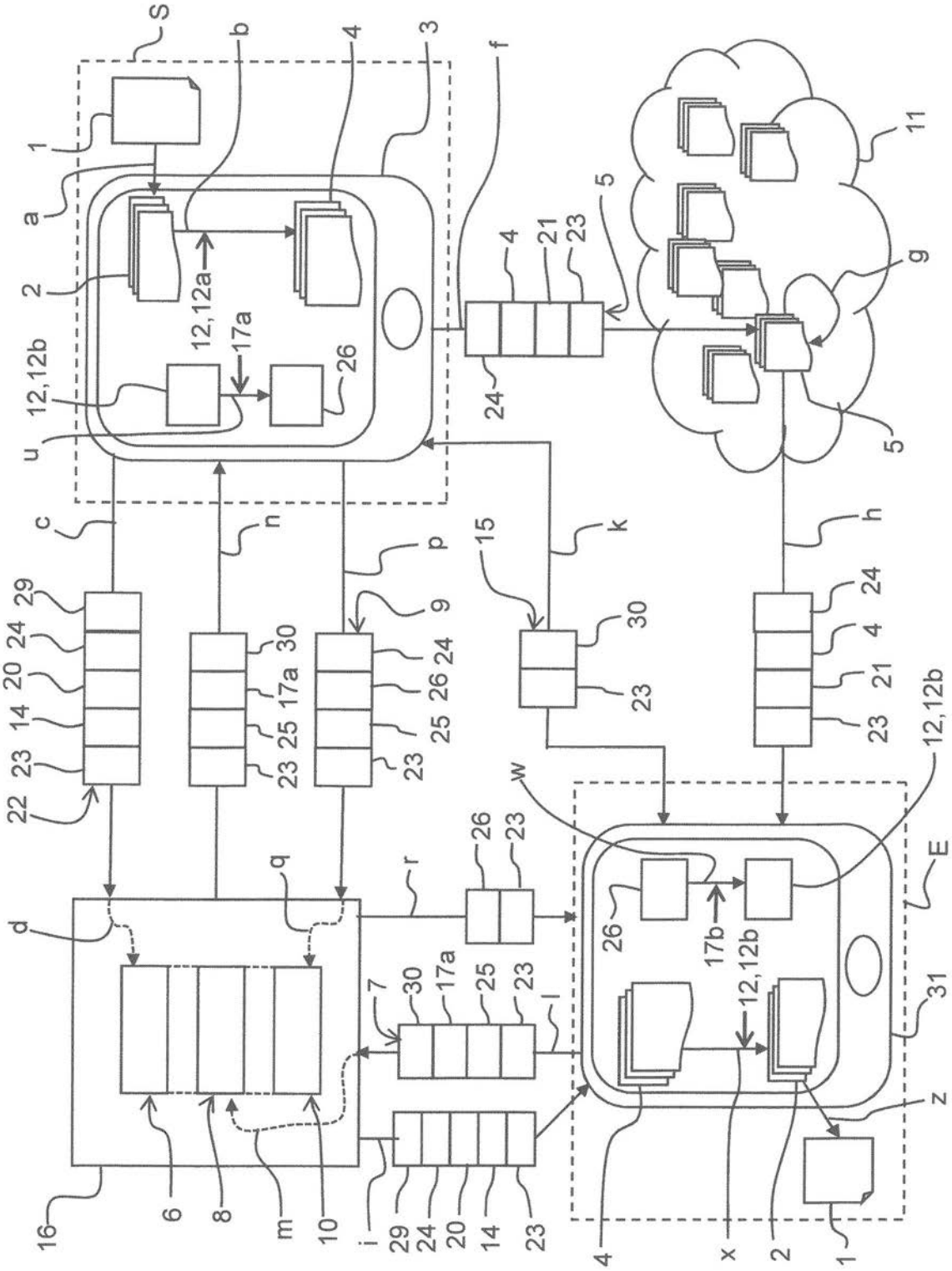

S
b
4
3
f
1
a
2
12,12a
17a
26
12,12b
u
11
5
4
21
23
g
24
5
c
n
p
15
k
h
29
24
20
14
23
22
30
17a
25
23
9
24
26
25
23
30
23
4
21
23
24
12,12b
w
26
23
E
q
r
d
26
17b
12,12b
7
30
17a
25
23
l
31
z
16
6
8
m
10
i
29
24
20
14
23
4
x
2
1

图4

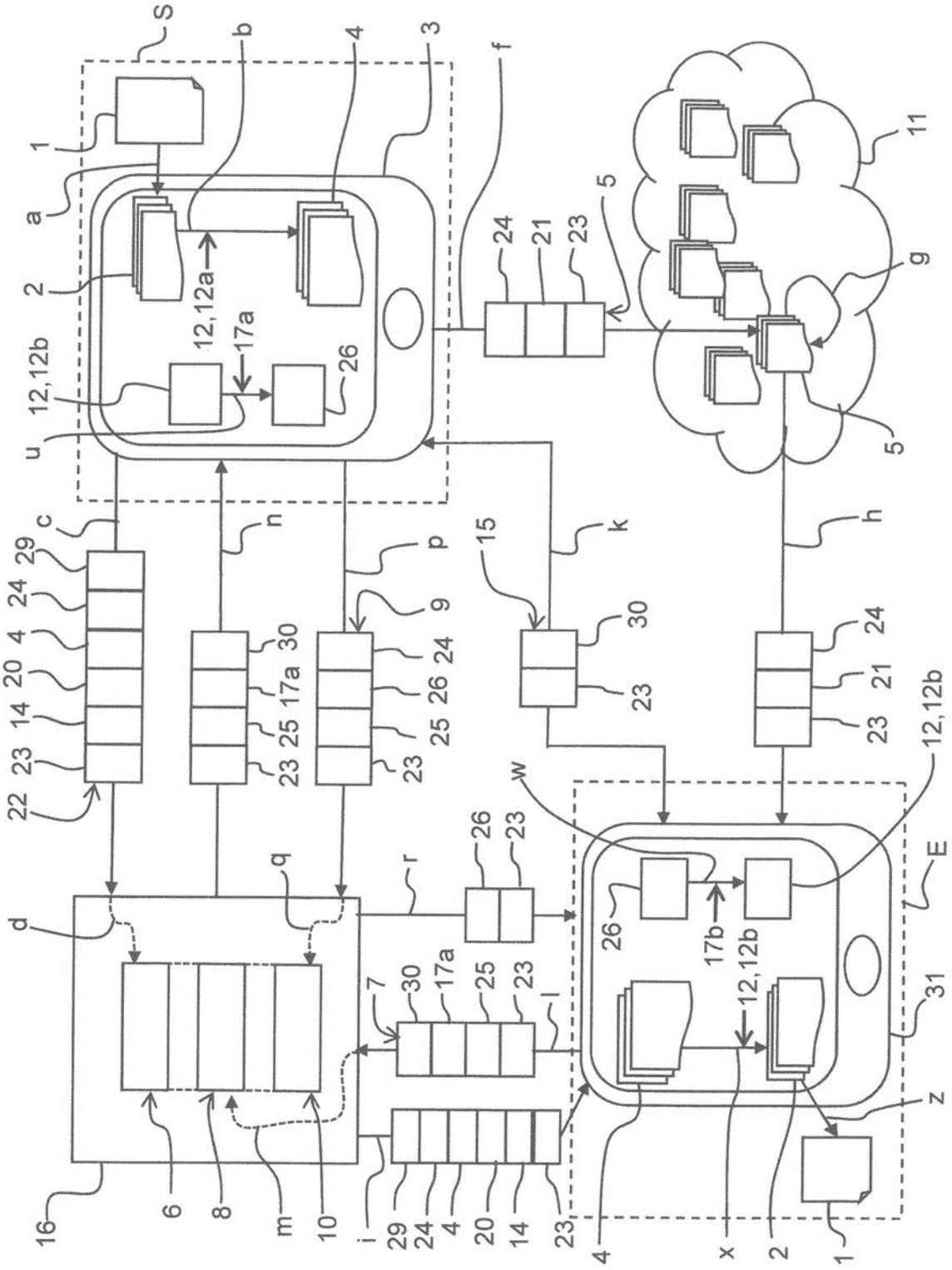

S
b
4
3
f
1
a
2
12,12a
17a
26
12,12b
u
11
5
24
21
23
g
c
29
24
4
20
14
23
22
n
30
17a
25
23
p
9
15
k
h
30
23
24
21
23
12,12b
w
E
26
17b
12,12b
31
z
d
q
r
26
23
7
30
17a
25
23
l
16
6
8
m
10
i
29
24
4
20
14
23
4
x
2
1

图5

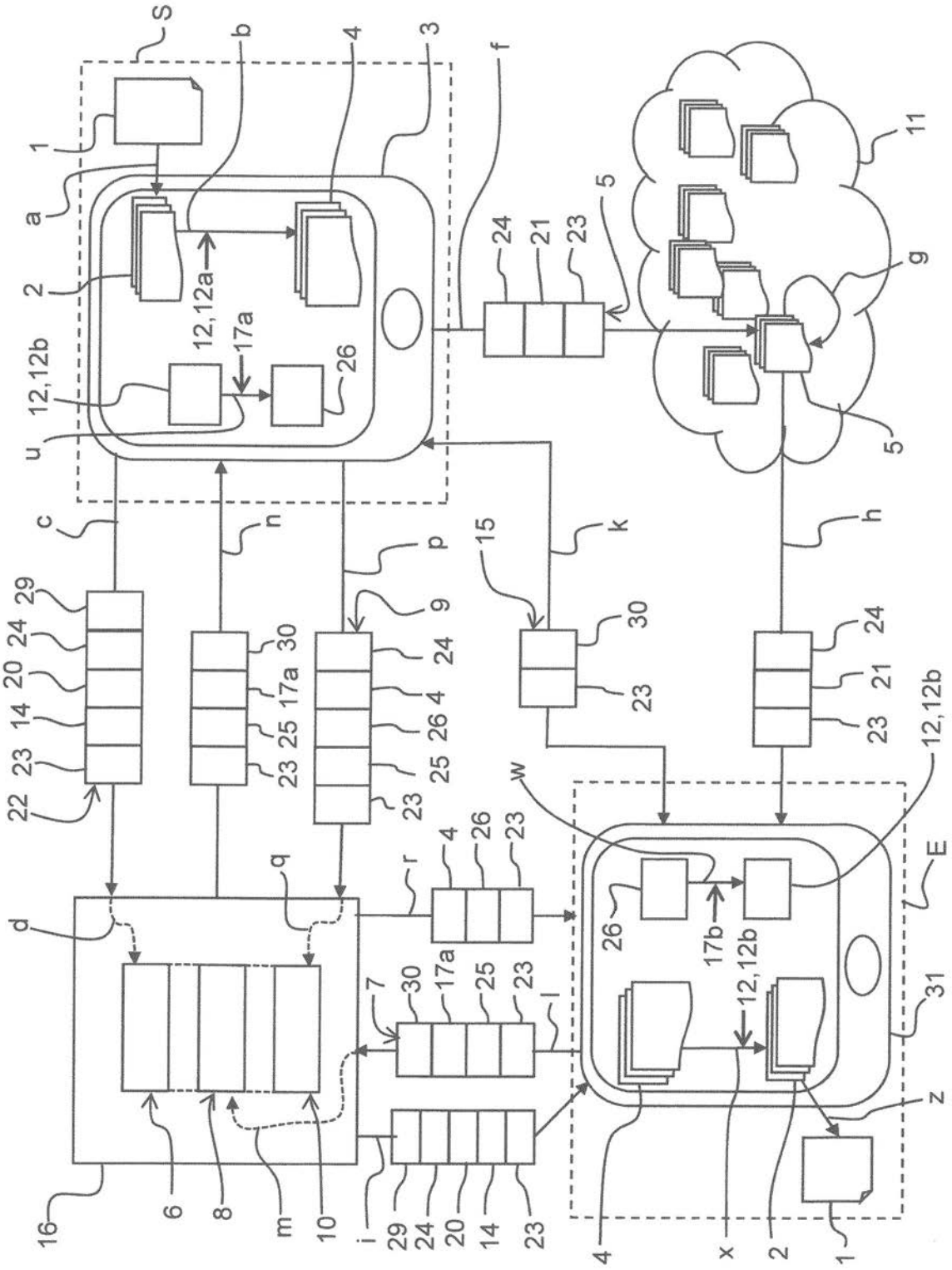

S
b
4
3
f
1
a
2
12,12a
17a
26
12,12b
u
24
21
23
5
11
g
5
c
n
p
15
k
h
29
24
20
14
23
22
30
17a
25
23
9
24
4
26
25
23
30
23
24
21
23
12,12b
w
E
4
26
23
r
q
d
26
17b
12,12b
31
7
30
17a
25
23
l
z
16
6
8
m
10
i
29
24
20
14
23
4
x
2
1

图6

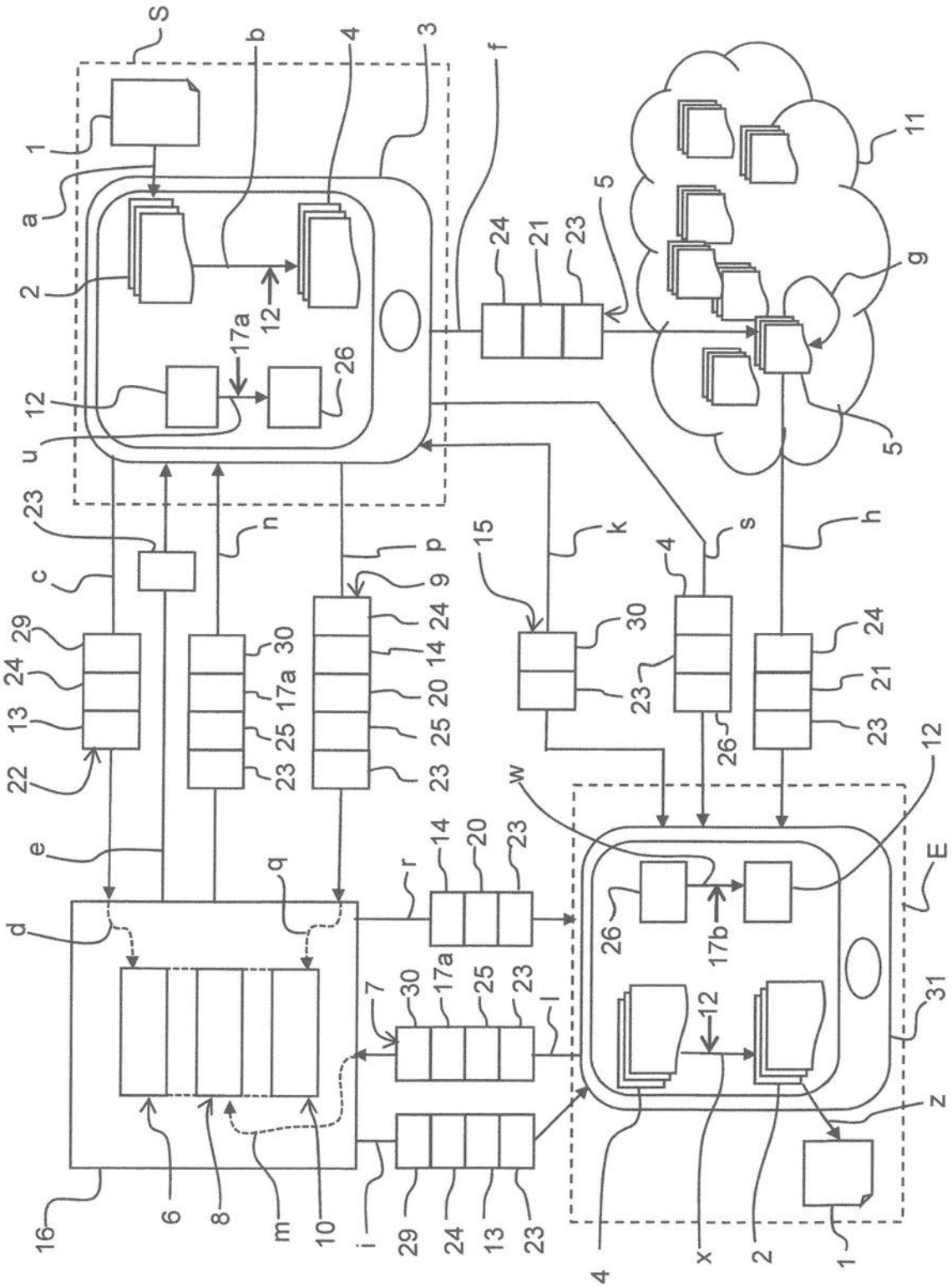

S
b
4
3
f
1
a
2
17a
12
26
12
u
24
21
23
5
11
g
5
23
c
n
p
15
k
4
s
h
29
24
13
22
30
17a
25
23
9
24
14
20
25
23
30
23
26
24
21
23
12
w
E
e
q
r
14
20
23
d
26
17b
7
30
17a
25
23
l
12
31
z
16
6
8
m
10
i
29
24
13
23
4
x
2
1

图7

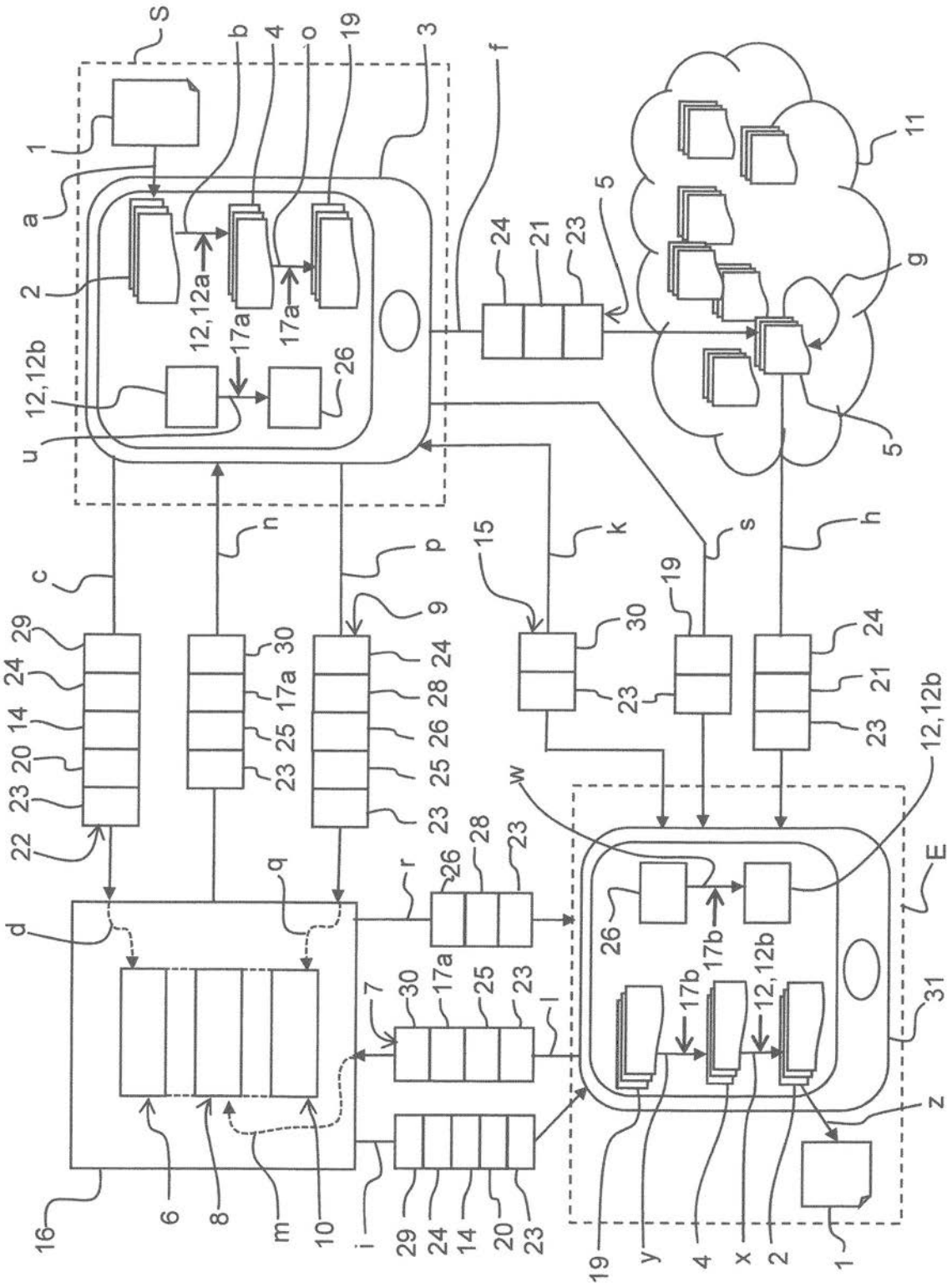

S
b
4
o
19
3
f
1
a
2
12,12a
17a
17a
26
12,12b
u
24
21
23
5
11
g
5
n
p
15
k
s
h
c
9
19
29
24
14
20
23
22
30
17a
25
23
24
28
26
25
23
30
19
23
24
21
23
12,12b
w
E
28
23
26
q
r
26
d
7
30
17a
25
23
l
26
17b
17b
12,12b
31
z
16
6
8
m
10
i
29
24
14
20
23
19
y
4
x
2
1

图8

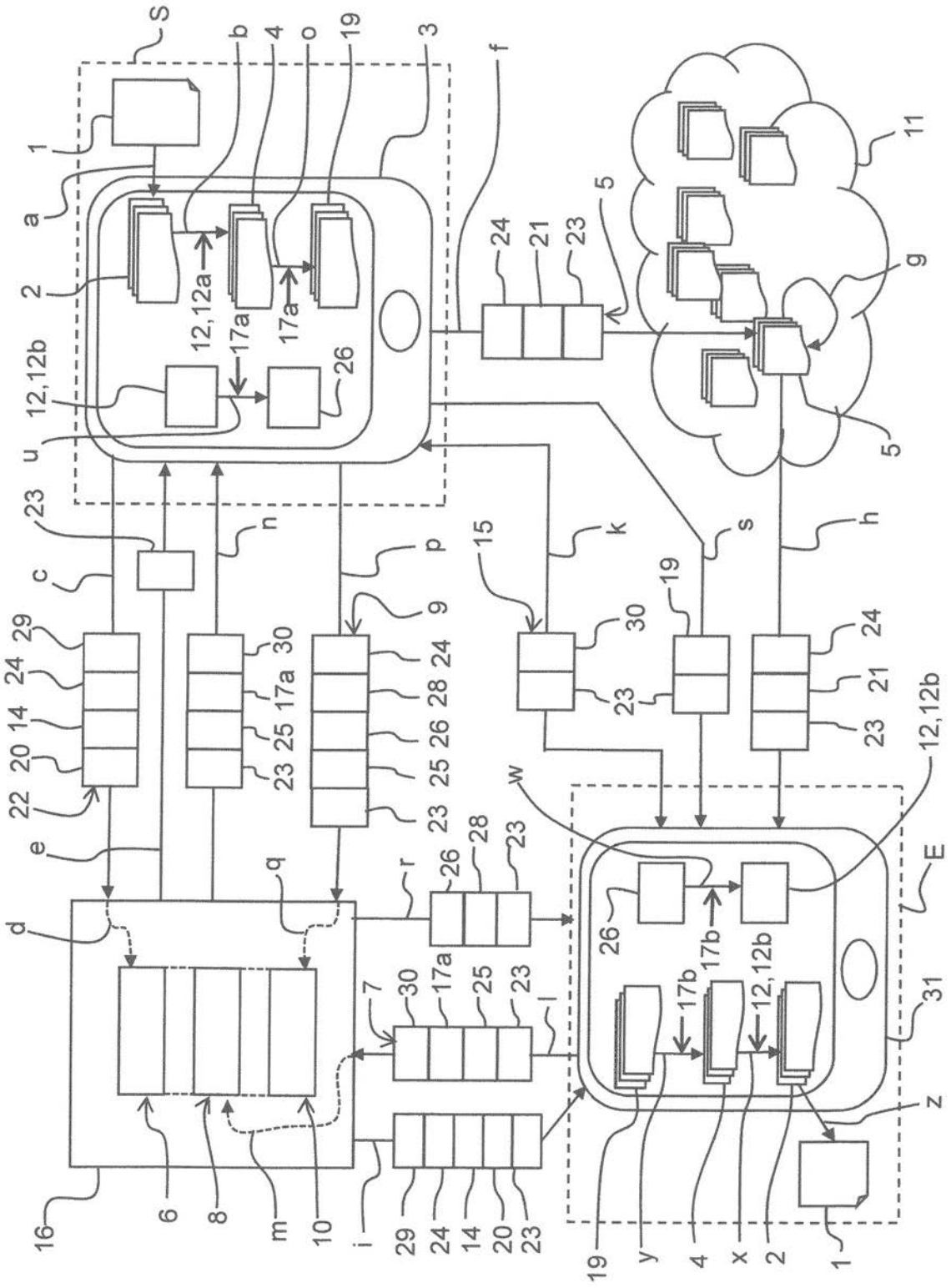

S
1
a
2
12,12b
u
12,12a
17a
26
b
4
o
19
3
f
24
21
23
5
11
g
c
n
p
9
15
k
s
h
29
24
14
20
22
e
30
17a
25
23
28
26
w
12,12b
E
d
q
r
7
l
31
z
6
8
m
10
i
16
y
x

图9