(19)中华人民共和国国家知识产权局

(12)发明专利

(10)授权公告号 CN 111767578 B
(45)授权公告日 2021.06.04

(21)申请号 202010900858.9

(22)申请日 2020.08.31

(65)同一申请的已公布的文献号
申请公布号 CN 111767578 A

(43)申请公布日 2020.10.13

(73)专利权人 支付宝(杭州)信息技术有限公司
地址 310000 浙江省杭州市西湖区西溪路556号8层B段801-11

(72)发明人 杨仁慧 杨文玉 王辛民 陈远 郭倩婷 钱锋 李书博

(74)专利代理机构 北京晋德允升知识产权代理有限公司 11623
代理人 王戈

(51)Int.Cl.
G06F 21/62(2013.01)
G06F 21/60(2013.01)
G06F 21/64(2013.01)
G06Q 40/04(2012.01)
H04L 29/06(2006.01)

审查员 齐银凤

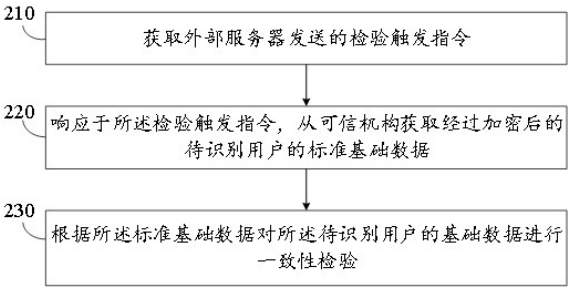
权利要求书6页 说明书17页 附图3页

(54)发明名称

一种数据检验方法、装置及设备

(57)摘要

本说明书实施例公开了一种数据检验方法、装置及设备，所述方法应用于隐私计算单元。该方法包括：通过获取外部服务器发送的检验触发指令；并响应于该检验触发指令，从可信机构获取经过加密后的待识别用户的标准基础数据；根据标准基础数据对待识别用户的基础数据进行一致性检验。



CN 111767578 B

1.一种数据检验方法,所述方法应用于隐私计算单元,所述方法包括:

获取外部服务器发送的检验触发指令;所述外部服务器中部署有定时触发逻辑;所述检验触发指令是由所述外部服务器在表示当前时刻的时间信息满足所述定时触发逻辑中的定时触发规则时发送的;若所述当前时刻的时间信息不满足所述定时触发逻辑中的定时触发规则时,获取云存储服务器中存储的待检验数据的数据量;当所述数据量达到预设数据量阈值时,所述外部服务器发送所述检验触发指令;

所述隐私计算单元向可信机构证明自身的身份;

所述隐私计算单元验证所述可信机构的身份信息;

当所述隐私计算单元的身份以及所述可信机构的身份可信时,响应于所述检验触发指令,从可信机构获取经过加密后的待识别用户的标准基础数据;

根据所述标准基础数据对所述待识别用户的基础数据进行一致性检验;所述待识别用户的基础数据是对第一机构上传的加密后的待识别用户的基础数据进行解密得到的。

2.根据权利要求1所述的方法,所述检验触发指令是所述外部服务器按照定时触发规则发送的。

3.根据权利要求2所述的方法,所述定时触发规则包括预设时长或预设启动时刻。

4.根据权利要求1所述的方法,所述第一机构上传的加密后的待识别用户的基础数据存储在云存储服务器中。

5.根据权利要求4所述的方法,所述根据所述标准基础数据对所述待识别用户的基础数据进行一致性检验之前,还包括:

根据所述待识别用户的用户标识信息,从所述云存储服务器中获取所述用户标识信息对应的加密后的待识别用户的基础数据。

6.根据权利要求5所述的方法,所述用户标识信息包括:

所述待识别用户在所述第一机构注册的账号;或,

所述待识别用户在所述第一机构发起交易操作时由所述第一机构的系统为所述待识别用户分配的账号。

7.根据权利要求6所述的方法,所述用户标识信息包括:

对所述待识别用户的一项或多项信息经哈希计算得到的摘要值。

8.根据权利要求7所述的方法,所述用户标识信息包括:

对所述待识别用户的一项或多项信息经加盐哈希计算得到的摘要值。

9.根据权利要求1所述的方法,所述隐私计算单元为部署在区块链系统上的隐私计算单元或部署在区块链系统之外的设备上的隐私计算单元。

10.根据权利要求1所述的方法,所述第一机构为代销机构。

11.根据权利要求1所述的方法,所述根据所述标准基础数据对所述待识别用户的基础数据进行一致性检验之前,还包括:

对从所述可信机构获取到的经过加密后的待识别用户的标准基础数据进行解密,得到所述标准基础数据。

12.根据权利要求11所述的方法,所述根据所述标准基础数据对所述待识别用户的基础数据进行一致性检验,具体包括:

将所述待识别用户的基础数据与所述标准基础数据进行比对,得到检验结果;

当所述检验结果表示所述待识别用户的基础数据与所述标准基础数据一致时，确定所述第一机构上传的所述待识别用户的基础数据为真实数据；

当所述检验结果表示所述待识别用户的基础数据与所述标准基础数据不一致时，确定所述第一机构上传的所述待识别用户的基础数据为虚假数据。

13.根据所述权利要求12所述的方法，所述将所述待识别用户的基础数据与所述标准基础数据进行比对，得到检验结果之后，还包括：

所述隐私计算单元接收第二机构发送的检验结果获取请求；所述检验结果获取请求用于请求获取根据所述标准基础数据对所述待识别用户的基础数据进行一致性检验得到的检验结果；

基于所述检验结果获取请求，将所述检验结果发送给所述第二机构。

14.根据权利要求13所述的方法，所述第二机构为金融机构。

15.根据权利要求13所述的方法，所述检验结果获取请求中包含所述待识别用户的用户标识信息。

16.根据权利要求1所述的方法，所述隐私计算单元部署有第一智能合约，所述第一智能合约用于接收所述外部服务器发送的检验触发指令，并响应于所述检验触发指令，执行根据所述标准基础数据对所述待识别用户的基础数据进行一致性检验的操作。

17.根据权利要求12所述的方法，所述确定所述第一机构上传的所述待识别用户的基础数据为真实数据之后，还包括：

所述隐私计算单元生成用于证明所述第一机构上传的所述待识别用户的基础数据为真实数据的可验证声明。

18.根据权利要求17所述的方法，所述可验证声明中包含所述第一机构的数字签名和/或所述隐私计算单元的数字签名。

19.根据权利要求17所述的方法，所述隐私计算单元生成用于证明所述第一机构上传的所述待识别用户的基础数据为真实数据的可验证声明之后，还包括：

将所述可验证声明发送至区块链系统中进行保存。

20.根据权利要求13所述的方法，所述隐私计算单元中还部署有第二智能合约；

所述将所述检验结果发送给所述第二机构，具体包括：

调用所述第二智能合约发送所述检验结果至所述第二机构。

21.根据权利要求5所述的方法，所述根据所述待识别用户的用户标识信息，从所述云存储服务器中获取所述用户标识信息对应的加密后的待识别用户的基础数据之前，还包括：

所述隐私计算单元向所述第一机构和/或所述云存储服务器证明所述隐私计算单元的身份。

22.一种数据检验的触发方法，所述方法包括：

外部服务器获取用于表示当前时刻的时间信息；所述外部服务器中部署有定时触发逻辑；

判断所述时间信息是否满足所述定时触发逻辑中的定时触发规则，得到判断结果；

若所述判断结果表示所述时间信息满足所述定时触发逻辑中的定时触发规则，向隐私计算单元发送检验触发指令；

若所述判断结果表示所述时间信息不满足所述定时触发逻辑中的定时触发规则;获取云存储服务器中存储的待检验数据的数据量;

判断所述数据量是否达到预设数据量阈值;

当所述数据量达到所述预设数据量阈值时,向隐私计算单元发送检验触发指令;

所述隐私计算单元向可信机构证明自身的身份;

所述隐私计算单元验证所述可信机构的身份信息;

当所述隐私计算单元的身份以及所述可信机构的身份可信时,所述检验触发指令用于触发所述隐私计算单元根据从可信机构获取的经过加密后的待识别用户的标准基础数据对所述待识别用户的基础数据进行一致性检验;所述待识别用户的基础数据是对第一机构上传的加密后的待识别用户的基础数据进行解密得到的。

23.根据权利要求22所述的方法,所述定时触发规则为计时时长达到预设时长则进行触发;

或者,所述定时触发规则为当前时刻达到预设启动时刻则进行触发。

24.一种数据检验装置,所述装置应用于隐私计算单元,所述装置包括:

检验触发指令获取模块,用于获取外部服务器发送的检验触发指令;所述外部服务器中部署有定时触发逻辑;所述检验触发指令是由所述外部服务器在表示当前时刻的时间信息满足所述定时触发逻辑中的定时触发规则时发送的;若所述当前时刻的时间信息不满足所述定时触发逻辑中的定时触发规则时,获取云存储服务器中存储的待检验数据的数据量;当所述数据量达到预设数据量阈值时,所述外部服务器发送所述检验触发指令;

第二隐私计算单元身份证明模块,用于所述隐私计算单元向可信机构证明自身的身份;

可信机构身份验证模块,所述隐私计算单元验证所述可信机构的身份信息;标准基础数据获取模块,用于当所述隐私计算单元的身份以及所述可信机构的身份可信时,

响应于所述检验触发指令,从可信机构获取经过加密后的待识别用户的标准基础数据;

检验模块,用于根据所述标准基础数据对所述待识别用户的基础数据进行一致性检验;所述待识别用户的基础数据是对第一机构上传的加密后的待识别用户的基础数据进行解密得到的。

25.根据权利要求24所述的装置,所述检验触发指令获取模块获取的所述检验触发指令是所述外部服务器按照定时触发规则发送的。

26.根据权利要求25所述的装置,所述定时触发规则包括预设时长或预设启动时刻。

27.根据权利要求24所述的装置,所述第一机构上传的加密后的待识别用户的基础数据存储在云存储服务器中。

28.根据权利要求27所述的装置,所述装置,还包括:

基础数据获取模块,用于根据所述待识别用户的用户标识信息,从所述云存储服务器中获取所述用户标识信息对应的加密后的待识别用户的基础数据。

29.根据权利要求24所述的装置,所述隐私计算单元为部署在区块链系统上的隐私计算单元或部署在区块链系统之外的设备上的隐私计算单元;所述第一机构为代销机构。

30.根据权利要求24所述的装置,所述装置,还包括:

解密模块，用于对从所述可信机构获取到的经过加密后的待识别用户的标准基础数据进行解密，得到所述标准基础数据。

31.根据权利要求30所述的装置，所述检验模块，具体包括：

比对单元，用于将所述待识别用户的基础数据与所述标准基础数据进行比对，得到检验结果；

真实数据确定单元，用于当所述检验结果表示所述待识别用户的基础数据与所述标准基础数据一致时，确定所述第一机构上传的所述待识别用户的基础数据为真实数据；

虚假数据确定单元，用于当所述检验结果表示所述待识别用户的基础数据与所述标准基础数据不一致时，确定所述第一机构上传的所述待识别用户的基础数据为虚假数据。

32.根据所述权利要求31所述的装置，所述检验模块，还包括：

检验结果获取请求接收单元，用于所述隐私计算单元接收第二机构发送的检验结果获取请求；所述检验结果获取请求用于请求获取根据所述标准基础数据对所述待识别用户的基础数据进行一致性检验得到的检验结果；所述检验结果获取请求中包含所述待识别用户的用户标识信息；

检验结果发送单元，用于基于所述检验结果获取请求，将所述检验结果发送给所述第二机构；所述第二机构为金融机构。

33.根据权利要求24所述的装置，所述隐私计算单元部署有第一智能合约，所述第一智能合约用于接收所述外部服务器发送的检验触发指令，并响应于所述检验触发指令，执行根据所述标准基础数据对所述待识别用户的基础数据进行一致性检验的操作。

34.根据权利要求31所述的装置，所述检验模块，还包括：

可验证声明生成单元，用于所述隐私计算单元生成用于证明所述第一机构上传的所述待识别用户的基础数据为真实数据的可验证声明；所述可验证声明中包含所述第一机构的数字签名和/或所述隐私计算单元的数字签名。

35.根据权利要求34所述的装置，所述检验模块，还包括：

可验证声明存储单元，用于将所述可验证声明发送至区块链系统中进行保存。

36.根据权利要求32所述的装置，所述隐私计算单元中还部署有第二智能合约；

所述检验结果发送单元，具体用于：

调用所述第二智能合约发送所述检验结果至所述第二机构。

37.根据权利要求28所述的装置，所述装置，还包括：

第一隐私计算单元身份证明模块，用于所述隐私计算单元向所述第一机构和/或所述云存储服务器证明所述隐私计算单元的身份。

38.一种数据检验的触发装置，所述装置包括：

时间信息获取模块，用于外部服务器获取用于表示当前时刻的时间信息；所述外部服务器中部署有定时触发逻辑；

判断模块，用于判断所述时间信息是否满足所述定时触发逻辑中的定时触发规则，得到判断结果；

检验触发指令发送模块，用于若所述判断结果表示所述时间信息满足所述定时触发逻辑中的定时触发规则，向隐私计算单元发送检验触发指令；

待检验数据的数据量获取模块，用于若所述判断结果表示所述时间信息不满足所述定

时触发逻辑中的定时触发规则;获取云存储服务器中存储的待检验数据的数据量;

数据量判断模块,用于判断所述数据量是否达到预设数据量阈值;

检验触发指令发送模块,用于当所述数据量达到所述预设数据量阈值时,向隐私计算单元发送检验触发指令;

所述隐私计算单元向可信机构证明自身的身份;

所述隐私计算单元验证所述可信机构的身份信息;

当所述隐私计算单元的身份以及所述可信机构的身份可信时,所述检验触发指令用于触发所述隐私计算单元根据从可信机构获取的经过加密后的待识别用户的标准基础数据对所述待识别用户的基础数据进行一致性检验;所述待识别用户的基础数据是对第一机构上传的加密后的待识别用户的基础数据进行解密得到的。

39.根据权利要求38所述的装置,所述定时触发规则为计时时长达到预设时长则进行触发;

或者,所述定时触发规则为当前时刻达到预设启动时刻则进行触发。

40.一种数据检验设备,应用于隐私计算单元,包括:

至少一个处理器;以及,

与所述至少一个处理器通信连接的存储器;其中,

所述存储器存储有可被所述至少一个处理器执行的指令,所述指令被所述至少一个处理器执行,以使所述至少一个处理器能够:

获取外部服务器发送的检验触发指令;所述外部服务器中部署有定时触发逻辑;所述检验触发指令是由所述外部服务器在表示当前时刻的时间信息满足所述定时触发逻辑中的定时触发规则时发送的;若所述当前时刻的时间信息不满足所述定时触发逻辑中的定时触发规则时,获取云存储服务器中存储的待检验数据的数据量;当所述数据量达到预设数据量阈值时,所述外部服务器发送所述检验触发指令;

所述隐私计算单元向可信机构证明自身的身份;

所述隐私计算单元验证所述可信机构的身份信息;

当所述隐私计算单元的身份以及所述可信机构的身份可信时,响应于所述检验触发指令,从可信机构获取经过加密后的待识别用户的标准基础数据;

根据所述标准基础数据对所述待识别用户的基础数据进行一致性检验;所述待识别用户的基础数据是对第一机构上传的加密后的待识别用户的基础数据进行解密得到的。

41.一种数据检验的触发设备,应用于隐私计算单元,包括:

至少一个处理器;以及,

与所述至少一个处理器通信连接的存储器;其中,

所述存储器存储有可被所述至少一个处理器执行的指令,所述指令被所述至少一个处理器执行,以使所述至少一个处理器能够:

获取用于表示当前时刻的时间信息;外部服务器中部署有定时触发逻辑;

判断所述时间信息是否满足所述定时触发逻辑中的定时触发规则,得到判断结果;

若所述判断结果表示所述时间信息满足所述定时触发逻辑中的定时触发规则,向隐私计算单元发送检验触发指令;若所述判断结果表示所述时间信息不满足所述定时触发逻辑中的定时触发规则;获取云存储服务器中存储的待检验数据的数据量;

判断所述数据量是否达到预设数据量阈值；

当所述数据量达到所述预设数据量阈值时，向隐私计算单元发送检验触发指令；

所述隐私计算单元向可信机构证明自身的身份；

所述隐私计算单元验证所述可信机构的身份信息；

当所述隐私计算单元的身份以及所述可信机构的身份可信时，所述检验触发指令用于触发所述隐私计算单元根据从可信机构获取的经过加密后的待识别用户的标准基础数据对所述待识别用户的基础数据进行一致性检验；所述待识别用户的基础数据是对第一机构上传的加密后的待识别用户的基础数据进行解密得到的。

一种数据检验方法、装置及设备

技术领域

[0001] 本申请涉及区块链技术领域，尤其涉及一种数据检验方法、装置及设备。

背景技术

[0002] KYC：是Know Your Customer的简称，当前行业相关法律规定要求自然人、法人和其他组织，要对自己的客户作出全面的了解，也就是了解客户原则。主要目标是通过对客户身份的核实和商业行为的了解，有效地发现和报告可疑行为，从而合理而有效地从客户日常的、习惯性的行为中发现不正常的、或许是可疑的行为。包括与客户建立业务关系时了解客户的身份、了解交易的目的、了解资金的来源和去向、以及了解客户的日常经营活动和金融交易情况等，是反洗钱的基础。

发明内容

[0003] 本发明的目的在于提供一种数据检验方法、装置及设备，包括：

[0004] 一种数据检验方法，所述方法应用于隐私计算单元，所述方法包括：

[0005] 获取外部服务器发送的检验触发指令；

[0006] 响应于所述检验触发指令，从可信机构获取经过加密后的待识别用户的标准基础数据；

[0007] 根据所述标准基础数据对所述待识别用户的基础数据进行一致性检验；所述待识别用户的基础数据是对第一机构上传的加密后的待识别用户的基础数据进行解密得到的。

[0008] 一种数据检验的触发方法，所述方法包括：

[0009] 外部服务器获取用于表示当前时刻的时间信息；所述外部服务器中部署有定时触发逻辑；

[0010] 判断所述时间信息是否满足所述定时触发逻辑中的定时触发规则，得到判断结果；

[0011] 若所述判断结果表示所述时间信息满足所述定时触发逻辑中的定时触发规则，向隐私计算单元发送检验触发指令；所述检验触发指令用于触发所述隐私计算单元根据从可信机构获取的经过加密后的待识别用户的标准基础数据对所述待识别用户的基础数据进行一致性检验；所述待识别用户的基础数据是对第一机构上传的加密后的待识别用户的基础数据进行解密得到的。

[0012] 一种数据检验装置，所述装置应用于隐私计算单元，所述装置包括：

[0013] 检验触发指令获取模块，用于获取外部服务器发送的检验触发指令；

[0014] 标准基础数据获取模块，用于响应于所述检验触发指令，从可信机构获取经过加密后的待识别用户的标准基础数据；

[0015] 检验模块，用于根据所述标准基础数据对所述待识别用户的基础数据进行一致性检验；所述待识别用户的基础数据是对第一机构上传的加密后的待识别用户的基础数据进行解密得到的。

[0016] 一种数据检验的触发装置,所述装置包括:

[0017] 时间信息获取模块,用于外部服务器获取用于表示当前时刻的时间信息;所述外部服务器中部署有定时触发逻辑;

[0018] 判断模块,用于判断所述时间信息是否满足所述定时触发逻辑中的定时触发规则,得到判断结果;

[0019] 检验触发指令发送模块,用于若所述判断结果表示所述时间信息满足所述定时触发逻辑中的定时触发规则,向隐私计算单元发送检验触发指令;所述检验触发指令用于触发所述隐私计算单元根据从可信机构获取的经过加密后的待识别用户的标准基础数据对所述待识别用户的基础数据进行一致性检验;所述待识别用户的基础数据是对第一机构上传的加密后的待识别用户的基础数据进行解密得到的。

[0020] 一种数据检验设备,包括:

[0021] 至少一个处理器;以及,

[0022] 与所述至少一个处理器通信连接的存储器;其中,

[0023] 所述存储器存储有可被所述至少一个处理器执行的指令,所述指令被所述至少一个处理器执行,以使所述至少一个处理器能够:

[0024] 获取外部服务器发送的检验触发指令;

[0025] 响应于所述检验触发指令,从可信机构获取经过加密后的待识别用户的标准基础数据;

[0026] 根据所述标准基础数据对所述待识别用户的基础数据进行一致性检验;所述待识别用户的基础数据是对第一机构上传的加密后的待识别用户的基础数据进行解密得到的。

[0027] 一种数据检验的触发设备,包括:

[0028] 至少一个处理器;以及,

[0029] 与所述至少一个处理器通信连接的存储器;其中,

[0030] 所述存储器存储有可被所述至少一个处理器执行的指令,所述指令被所述至少一个处理器执行,以使所述至少一个处理器能够:

[0031] 获取用于表示当前时刻的时间信息;所述外部服务器中部署有定时触发逻辑;

[0032] 判断所述时间信息是否满足所述定时触发逻辑中的定时触发规则,得到判断结果;

[0033] 若所述判断结果表示所述时间信息满足所述定时触发逻辑中的定时触发规则,向隐私计算单元发送检验触发指令;所述检验触发指令用于触发所述隐私计算单元根据从可信机构获取的经过加密后的待识别用户的标准基础数据对所述待识别用户的基础数据进行一致性检验;所述待识别用户的基础数据是对第一机构上传的加密后的待识别用户的基础数据进行解密得到的。

[0034] 本说明书实施例能够达到以下有益效果:通过获取外部服务器发送的检验触发指令;并响应于该检验触发指令,从可信机构获取经过加密后的待识别用户的标准基础数据;根据标准基础数据对待识别用户的基础数据进行一致性检验。通过该方法,可以通过外部服务器触发用户的身份检验过程,满足主动触发用户的KYC检验的需求。此外,结合可信机构提供的标准基础数据对用户进行KYC检验,能够保证KYC检验结果的准确性。

附图说明

[0035] 为了更清楚地说明本说明书实施例或现有技术中的技术方案，下面将对实施例或现有技术描述中所需要使用的附图作简单地介绍，显而易见地，下面描述中的附图仅仅是本申请中记载的一些实施例，对于本领域普通技术人员来讲，在不付出创造性劳动性的前提下，还可以根据这些附图获得其他的附图。

[0036] 图1是本说明书实施例提供的一种数据检验方法的系统架构示意图；

[0037] 图2是本说明书实施例提供的一种数据检验方法的流程图；

[0038] 图3为本说明书实施例提供的一种数据检验的触发方法的流程图；

[0039] 图4是本说明书实施例提供的一种数据检验装置的结构示意图；

[0040] 图5是本说明书实施例提供的一种数据检验的触发装置的结构示意图；

[0041] 图6是本说明书实施例提供的一种数据检验设备的结构示意图。

具体实施方式

[0042] 为使本说明书一个或多个实施例的目的、技术方案和优点更加清楚，下面将结合本说明书具体实施例及相应的附图对本说明书一个或多个实施例的技术方案进行清楚、完整地描述。显然，所描述的实施例仅是本说明书的一部分实施例，而不是全部的实施例。基于本说明中的实施例，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，都属于本说明书一个或多个实施例保护的范围。

[0043] 在互联网领域，用户通过互联网平台在各个机构注册身份信息，通过互联网平台实现各种业务。各个机构需要在确定用户身份的情况下，才能对用户的业务进行处理，因此，对用户身份的真实性进行检验是各个机构处理业务的需求。下面以反洗钱为例加以说明。

[0044] 反洗钱(Anti-Money Laundering，AML)是指预防通过各种方式掩饰、隐瞒毒品犯罪、黑社会性质的组织犯罪、恐怖活动犯罪、走私犯罪、贪污贿赂犯罪、破坏金融管理秩序犯罪等犯罪所得及其收益的来源和性质的洗钱活动的措施。常见的洗钱途径广泛涉及银行、保险、证券、房地产等各种领域。大多数反洗钱工作都包括三个核心的事项：

[0045] 1、客户身份识别制度。反洗钱义务主体在与客户建立业务关系或者与其进行交易时，应当根据真实有效地身份证件，核实和记录其客户的身份，并在业务关系存续期间及时更新客户的身份信息资料。

[0046] 2、大额和可疑交易报告(Suspicious Transaction Report，STR)制度。非法资金流动一般具有数额巨大、交易异常等特点，因此，法律规定了大额和可疑交易报告制度，要求金融机构对数额达到一定标准的交易和缺乏合法目的的异常交易应当及时向反洗钱行政主管部门报告，以作为追查违法犯罪行为的线索。

[0047] 3、客户身份资料和交易记录保存制度。客户身份资料和交易记录保存，是指金融机构依法采取必要措施将客户身份资料和交易信息保存一定期限，可以为追查违法犯罪行为提供证据支持。

[0048] 客户身份识别制度也就是通常所说的“了解你的客户”(Know Your Customer，KYC)，指的是获取客户相关识别信息，包括与客户建立业务关系时了解客户的身份、了解交易的目的、了解资金的来源和去向、以及了解客户的日常经营活动和金融交易情况等，是反

洗钱的基础。

[0049] 现有的实现中，根据监管要求，需要核查各个机构的KYC检验结果。而对于KYC的检验，只有通过机构发起交易的方式来触发智能合约执行KYC检验的操作。但是，在实际应用中，可能存在需要主动触发KYC检验的需求。

[0050] 为了解决上述问题，以下结合附图，详细说明本说明书各实施例提供的技术方案。

[0051] 图1是本说明书实施例提供的一种数据检验方法的系统架构示意图。如图1所示，本申请提供的一种数据检验方法实施例，可以包括图1中的角色：隐私计算平台110、外部服务器120、第一机构130、可信机构140、第二机构150以及云存储服务器160。

[0052] 其中，第一机构130可以是代销机构，第二机构150可以是金融机构，隐私计算平台110可以部署在区块链系统上，也可以部署在区块链系统外的设备上。第一机构130可以直接接收用户的信息，从而基于这些用户信息完成一定的处理工作，如KYC场景中提到的KYC检验。另一方面，第一机构130可以对外提供KYC检验结果，也可以对外提供KYC检验所需的基础数据，第一机构130可以将用户的基础数据存储在云存储服务器160中，当隐私计算平台110中的隐私计算单元需要对用户的基础数据进行一致性检验时，可以从云存储服务器160中获取用户的基础数据，当然，也可以直接从第一机构130处获取。隐私计算平台110，可以在可信的安全计算环境中执行KYC的检验。外部服务器120定时向隐私计算平台110发送检验触发指令，触发隐私计算平台110中的隐私计算单元执行KYC检验，隐私计算单元在进行KYC检验时，可以从可信机构140处获取经过加密后的用户的标准基础数据，并根据标准基础数据对用户的基础数据进行一致性检验。检验之后得到的检验结果，可以根据第二机构150的获取请求发送给第二机构150，在一些情况下，也可以主动将KYC检验结果发送给第二机构150。

[0053] 接下来，将针对说明书实施例提供的一种启动信息验证的方法结合附图进行具体说明：

[0054] 实施例1

[0055] 图2是本说明书实施例提供的一种数据检验方法的流程图。从程序角度而言，流程的执行主体可以为搭载于应用服务器的程序或应用客户端。本说明书实施例中的执行主体可以是一个负责隐私计算的应用服务集群。该服务器集群中可以包括一个或多个应用服务，这些应用服务可以与区块链网络具有数据交互，也可以部署在区块链上。在后面的实施例中，为了描述方便，负责隐私计算的应用服务器集群可以用“隐私计算单元”代替。

[0056] 如图2所示，该流程可以包括以下步骤：

[0057] 步骤210：获取外部服务器发送的检验触发指令。

[0058] 检验触发指令可以是一个请求对用户的身份进行真实性验证进行触发的操作指令，所述检验触发指令中至少可以包括请求验证的用户对应的用户标识信息。

[0059] 可选的，所述检验触发指令可以是由外部服务器按照定时触发规则发送的。其中，外部服务器可以是一个单独部署的、用于定时触发信息验证的定时服务器。在实际实现时，外部服务器中可以部署有定时触发规则，当外部服务器检测到当前事件信息满足定时触发规则时，向隐私计算单元发送检验触发指令。

[0060] 定时触发规则可以包括预设时长、预设启动时刻。例如：定时触发规则中可以是规定每间隔2个小时触发一次KYC检验，也可以是规定每天的上午8:00触发KYC检验。具体地，

外部服务器中可以部署有计时功能服务，该计时功能服务可以记录时间，当计时功能服务的计时时长达到预设时长或者计时功能服务记录的当前时刻到达预设启动时刻，则外部服务器可以向隐私计算单元发送检验触发指令，触发隐私计算单元进行KYC检验。

[0061] 在实际应用中，可能会存在虽然没有满足定时触发规则，可云存储服务器中已经存储了大量的待检验数据，造成该服务器负载压力过大，但是由于还未满足触发定时触发规则，导致无法将用户上传的待检验数据发送给隐私计算单元。为了解决这一技术问题，外部服务器还可以监控云存储服务器中待检验数据的数据量，即使没有满足定时触发规则，只要云存储服务器中的数据量达到预设数据量阈值，也可以触发隐私计算单元执行KYC检验，以减轻云存储服务器的负载压力。

[0062] 需要说明的是，云存储服务器可以是对象存储服务器(Object Storage Service，简称OSS)，也可以是其他云存储服务器，对此，本说明书实施例不作具体限定。

[0063] 步骤220：响应于所述检验触发指令，从可信机构获取经过加密后的待识别用户的标准基础数据。

[0064] 可信机构可以表示专门负责用户信息管理的机构。也可以是能够掌握用户身份信息的相关企业，比如：公安机关或保险公司等。

[0065] 待识别用户可以是个人用户，也可以是企业用户之类。对于个人用户，基础数据可以包括个人的姓名、性别、国籍、证件类型、证件号码、年龄、职业、手机号码、联系地址等信息中的部分或者全部。对于企业用户，基础数据可以包括企业的名称、营业执照编号、营业场所地址、法定代表人的姓名、证件类型、证件号码和有效期限等信息中的部分或者全部。这些信息大多是比较敏感的，因此，在传输时，需要对这些基础数据进行加密后再传输，以保证用户的基础数据的安全性。

[0066] 可选的，所述根据所述标准基础数据对所述待识别用户的基础数据进行一致性检验之前，还可以包括：

[0067] 对从所述可信机构获取到的经过加密后的待识别用户的标准基础数据进行解密，得到所述标准基础数据。

[0068] 步骤230：根据所述标准基础数据对所述待识别用户的基础数据进行一致性检验；所述待识别用户的基础数据是对第一机构上传的加密后的待识别用户的基础数据进行解密得到的。

[0069] 第一机构可以指的是代销机构。代销机构可以是代为销售金融产品的机构，在实际应用中，一些金融产品的金融机构和代销机构之间有合作关系，金融机构通过代销机构来代销金融机构的金融产品，例如网络平台代销基金公司的理财产品。

[0070] 在实际应用中，从可信机构获取的待识别用户的标准基础数据具有可信性，在对待识别用户的身份进行KYC检验时，可以理解为判断第一机构上传的待识别用户的基础数据是否是真实数据，具体地，如果待识别用户的基础数据与标准基础数据一致，可以确定第一机构上传的待识别用户的基础数据是真实数据。反之，则可以确定第一机构上传的待识别用户的基础数据是虚假数据。具体地，在根据所述标准基础数据对所述待识别用户的基础数据进行一致性检验，具体可以将所述待识别用户的基础数据与所述标准基础数据进行比对，得到检验结果；当所述检验结果表示所述待识别用户的基础数据与所述标准基础数据一致时，确定所述第一机构上传的所述待识别用户的基础数据为真实数据；当所述检验

结果表示所述待识别用户的基础数据与所述标准基础数据不一致时，确定所述第一机构上传的所述待识别用户的基础数据为虚假数据。

[0071] 隐私计算单元在进行KYC检验时，需要从云存储服务器中获取需要进行KYC检验的待识别用户的基础数据。所述云存储服务器用于存储各个机构上传的各个用户的基础数据。该步骤中的待识别用户的基础数据与步骤220中描述的“基础数据”一致，因此，在传输时，也需要对这些基础数据进行加密后再传输，以保证用户的基础数据的安全性。

[0072] 具体地，对于第一机构上传的待识别用户的加密后的基础数据，可以是由第一机构采用对称加密或非对称加密的方式将所述基础数据加密后上传至云存储服务器中进行保存，也可以是由第一机构将基础数据上传至云存储服务器中之后，由云存储服务器对该基础数据进行加密后发送给隐私计算单元。如果采用对称加密，即加密秘钥和解密秘钥是同一把秘钥的情形，可以由第一机构和隐私计算单元之间通过秘钥协商过程得到这把秘钥；对于采用非对称加密，即加密秘钥和解密秘钥是两把不同但是相对应的秘钥的情形，其中一把为公钥，用于加密，另一把为私钥，用于解密，一般第一机构可以采用隐私计算单元的公钥将基础数据加密后发送至隐私计算单元，进而由隐私计算单元采用对应的私钥解密，恢复得到待识别用户的基础数据。

[0073] 为了进一步提升数据传输的安全性，即尽管传输的是加密数据，也不希望错误的接收方接收到，因此，在将待识别用户的基础数据发送至隐私极端单元前，还可以先确认对方的身份。例如：在第一机构上传用户的基础数据至云存储服务器中时，第一机构和云存储服务器可以互相确认彼此的身份，云存储服务器在将用户的基础数据发送给隐私计算单元时，隐私计算单元与云存储服务器可以互相确认彼此的身份，第一机构与隐私计算单元也可以互相确认彼此的身份。确认对方身份的方式有若干种，这里列举一种采用结合了区块链的分布式数字身份技术的实现方式。区块链可以提供去中心化(或弱中心化)的、不可篡改(或难以篡改)的、可信的分布式账本，并可以提供安全、稳定、透明、可审计且高效的记录交易以及数据信息交互的方式。区块链网络可以包括多个节点。一般来说区块链的一个或多个节点归属于一个参与方。笼统的说，区块链网络的参与方越多，参与方越权威，区块链网络的可信程度越高。这里称多个参与方构成的区块链网络为区块链平台。借助区块链平台，可以帮助验证金融机构的身份。

[0074] 为了使用区块链平台提供的分布式数字身份服务，第一机构、第二机构、可信机构以及隐私计算单元可以将自身的身份在区块链平台中登记。例如，第一机构可以创建一对公钥和私钥，私钥保密存储，并可以创建一个分布式数字身份(也称为去中心化标识符，Decentralized Identitfiers,DID)。可以由第一机构自己创建DID，也可以请求分布式身份服务(Decentralized Identity Service,DIS)系统来创建DID。DIS是一种基于区块链的身份管理方案，可以提供数字身份的创建、验证和管理等功能，从而实现规范化地管理和保护实体数据，同时保证信息流转的真实性和效率，并可以解决跨机构的身份认证和数据合作等难题。DIS系统可以与区块链平台相连。通过DIS系统可以为第一机构创建一个DID，并将该DID和所述公钥发送至区块链平台保存，还将该创建的DID返回给第一机构。所述公钥可以包含到DIDdoc中，所述DIDdoc可以存储于区块链平台中。DIS为金融机构创建DID，可以基于第一机构发来的公钥创建，例如采用Hash函数对所述第一机构的公钥进行计算后创建，也可以根据第一机构的其它信息(可以包括所述公钥或不包括所述公钥)创建。后者可

能需要第一机构提供一些公钥之外的信息。

[0075] 其中，隐私计算单元可以是部署在区块链系统上的隐私计算单元，也可以是部署在区块链系统之外的设备上的隐私计算单元。所述隐私计算单元在被使用前，可以向使用者证明自身是可信的。证明自身可信的过程可能涉及远程证明报告。链上和链下的隐私计算单元证明自身可信的过程类似。以链下为例，远程证明报告产生于针对链下隐私计算单元上的链下TEE的远程证明过程。远程证明报告可以由权威的认证服务器对链下隐私计算单元产生的自荐信息进行验证后生成，该自荐信息与链下隐私计算单元上创建的链下TEE相关。链下隐私计算单元通过产生与链下TEE相关的自荐信息，并由所述权威认证服务器对该自荐信息进行验证后产生远程证明报告，使得远程证明报告可以用于表明链下隐私计算单元上的链下TEE可信任。

[0076] 例如，可信机构向区块链系统外的设备上的隐私计算单元发送用户的标准基础数据时，可以首先验证所述隐私计算单元是否可信。具体的，所述可信机构可以向链下隐私计算单元发起挑战，并接收链下隐私计算单元返回的远程证明报告。例如，所述可信机构可以向链下隐私计算单元发起链下挑战，即发起挑战的过程可以与区块链网络无关，这样可以跳过区块链节点之间的共识过程，并减少链上链下的交互操作，使得所述可信机构向链下隐私计算单元的挑战具有更高的操作效率。再例如，所述可信机构可以采用链上挑战的形式，比如所述可信机构可以向区块链节点提交挑战交易，该挑战交易所含的挑战信息可由区块链节点通过预言机机制传输至链下隐私计算单元，且该挑战信息用于向链下隐私计算单元发起挑战。无论上述链上挑战还是链下挑战的形式，挑战者(如所述可信机构)在获取远程证明报告后，可以根据权威认证服务器的公钥对该远程证明报告的签名进行验证，如果验证通过则可以确认链下隐私计算单元是可信的。

[0077] 链下隐私计算平台可以在TEE中存储一对公私钥。公钥可以在远程证明过程之类的过程中发送至对方，而私钥则妥善保管在TEE中。所述可信机构在根据所述远程证明报告确定所述链下隐私计算单元可信的情况下，可以将链下合约的字节码加密传输至所述链下隐私计算单元，由所述链下隐私计算单元在所述链下可信执行环境中解密得到所述字节码并部署。上述加密，即可以采用所述公钥加密。上述过程中，链下隐私计算单元部署合约后，可以存储该合约，并计算该合约的hash值。该合约的hash值可以反馈至合约的部署方，部署方对于部署的合约可以在本地产生一个hash值，从而部署方可以比对部署的合约的hash值与本地的合约hash值是否相同，如果相同则说明链下隐私计算单元上部署的合约是自己部署的合约。所述链下隐私计算单元传出的内容，可以用所述TEE内保存的私钥来签名，从而证明是由该TEE执行的结果。实际上，一个TEE内可以部署有多个智能合约，TEE可以为每个智能合约生成一个单独的公私钥对，从而，每个部署的智能合约可以具有一个ID(如该智能合约对应的公钥或基于该公钥生成的字符串)，且每个智能合约执行的结果也都可以用该智能合约对应的在TEE妥善保管的私钥来签名，这样，可以证明一个结果是由一个链下隐私计算单元中的特定的合约执行的结果。这样，不同合约的执行结果可以由不同的私钥来签名，只有对应的公钥才能验证该签名，或者说不能由对应公钥验证签名的无法证明该结果是对应合约的执行结果，因此相当于通过公私钥对为链下隐私计算单元中部署的合约赋予了身份。上述以链下隐私合约为例，链上隐私合约也是类似的，也可以具有身份，即具有公私钥对。

[0078] 后续,链下隐私计算单元可以提供对部署的所述链下合约的调用。具体的,链下部署的合约被调用时,所述链下可信执行环境中可以加载所述部署的合约的字节码并执行,且执行结果可反馈至所述合约的调用者,或者反馈至合约中指定的接收者或调用该合约的交易中指定的接收者,再或者通过所述预言机机制反馈至所述区块链节点。通过所述预言机机制反馈至所述区块链节点的,可以经由链上合约的设置,进一步反馈至链上合约中指定的接收者或调用链上合约的交易中指定的接收者。

[0079] 此外,所述链下隐私计算单元的执行结果,可以用秘钥进行加密后输出。例如采用非对称加密方式,加密所使用的公钥,可以是在上述挑战过程中协商的公私钥对中的公钥,也可以是挑战者通过前述的DIS服务生成之后发送至链下隐私计算单元的。这里的挑战者可以是本申请实施例中的可信机构,也可以是所述第一机构、第二机构或云存储服务器。从而,通过上述方式,可以保障出、入链下隐私计算单元的数据都是经过加密的,以确保数据传输过程中的安全。类似的,进入链下隐私计算单元的数据,可以由发送方用自身的秘钥签名。后续类似环节中的原理也相同。

[0080] 图2中的方法,通过获取外部服务器发送的检验触发指令;并响应于该检验触发指令,从可信机构获取经过加密后的待识别用户的标准基础数据;根据标准基础数据对待识别用户的基础数据进行一致性检验。通过该方法,可以通过外部服务器触发用户的身份检验过程,满足主动触发用户的KYC检验的需求。此外,结合可信机构提供的标准基础数据对用户进行KYC检验,能够保证KYC检验结果的准确性。

[0081] 基于图2的方法,本说明书实施例还提供了该方法的一些具体实施方案,下面进行说明。

[0082] 可选的,所述根据所述标准基础数据对所述待识别用户的基础数据进行一致性检验之前,还可以包括:

[0083] 根据所述待识别用户的用户标识信息,从所述云存储服务器中获取所述用户标识信息对应的加密后的待识别用户的基础数据。

[0084] 可选的,所述用户标识信息可以包括:

[0085] 所述待识别用户在所述第一机构注册的账号;或,

[0086] 所述待识别用户在所述第一机构发起交易操作时由所述第一机构的系统为所述待识别用户分配的账号。

[0087] 可选的,所述用户标识信息可以包括:

[0088] 对所述待识别用户的一项或多项信息经哈希计算得到的摘要值。

[0089] 可选的,所述用户标识信息可以包括:

[0090] 对所述待识别用户的一项或多项信息经加盐哈希计算得到的摘要值。

[0091] 需要说明的是,上述步骤中,用户标识信息可以表示用于唯一标识用户身份的信息,例如:用户标识信息可以是用户ID。其中,用户ID可以是用户在代销机构注册的账号,或者是用户在代销机构发起交易操作时由代销机构的系统为该用户分配的账号。这类账号例如可以是一串字符。用户ID应当可以唯一的标识一位用户。对应字段如上所述的个人用户或企业用户的信息。

[0092] 对于个人用户来说,如果证件类型统一采用身份证的话,用户ID也可以是身份证号码。但是身份证号码实际上也是属于个人的隐私数据,因此,考虑到避免泄露个人隐私数

据，可以对身份证号码进行hash处理。由于hash计算具有单向的特点和隐匿原始信息的特点，并且好的hash函数具有防碰撞能力，即不同的输入得到的hash值极大概率也不同，因此可以采用hash计算结果(或者称摘要值)作为用户ID。手机号码也是相同的原理。

[0093] 类似的，还可以是对一组用户的数据顺序拼接后进行hash计算，得到的摘要值作为用户ID，例如hash(姓名+证件类型+证件号码)所得到的摘要值作为用户ID，其中的“+”可以表示前后字符的顺序拼接。反洗钱KYC中对于数据的安全性一般具有较高的要求，为了进一步加强数据安全防护，还可以在hash计算中采取加盐操作，例如hash(姓名+证件类型+证件号码+salt)，salt为按照预定规则生成的一个值。

[0094] 代销机构可以是在用户注册时提示用户提供基础数据，也可以是用户在代销机构平台上发起交易操作时要求用户提供基础数据。代销机构在获取用户提供的基础数据之后，可以将用户提供的基础数据存储到云存储服务器当中。

[0095] 在实际应用中，单一机构往往无法获取足够的信息而无法处理业务，这就存在从其他机构获取信息的需求。例如，各国在反洗钱合规履职的要求中，很多都要求各个金融机构提供反洗钱审核结果。目前，很多国家央行、很多大的金融机构都有在反洗钱领域利用区块链来提升效率和准确性并满足监管的尝试。同时，数据作为一种资源，其流动性和可获取性是很多数据应用和产业发展的基础，但数据交换和共享过程中的隐私保护一直是产业发展的一大挑战。以前述的代销机构和金融机构为例，购买金融产品的客户往往直接是代销机构的客户。按照监管要求，销售金融产品需要具有对客户进行KYC的检验结果。如上所述，购买金融产品的客户直接是代销机构的客户，代销机构一般能直接获取用户的基本信息，从而具有KYC检验能力。根据数据隐私保护的要求，代销机构通常不能将KYC的基础数据和KYC结果直接转给金融机构。金融机构没有KYC的基础数据，无法进行独立的KYC，而根据监管要求，金融机构也需要具有KYC检验结果。这样，金融机构无法进行KYC，KYC履职不到位，不能满足监管的要求。因此，为了满足监管要求，除了代销机构需要具有对客户进行KYC的检验结果外，金融机构也需要具有对客户进行KYC的检验结果。

[0096] 检验结果可以用{用户ID，KYC检验结果}表示，其中KYC检验结果例如为通过、不通过，或者KYC检验结果可以是真实、虚假等。隐私计算平台将所述检验结果发送至所述金融机构，包括直接发送至所述金融机构，此外也可以包括发送至一个指定的存储服务介质中，后续由所述金融机构从该存储服务介质中拉取。

[0097] 因此，所述将所述待识别用户的基础数据与所述标准基础数据进行比对，得到检验结果之后，还可以包括：

[0098] 所述隐私计算单元接收第二机构发送的检验结果获取请求；所述检验结果获取请求用于请求获取根据所述标准基础数据对所述待识别用户的基础数据进行一致性检验得到的检验结果；

[0099] 基于所述检验结果获取请求，将所述检验结果发送给所述第二机构；所述第二机构可以为金融机构。

[0100] 其中，第二机构向隐私计算单元发送的所述检验结果获取请求中可以包含所述待识别用户的所述用户标识信息，例如：待识别用户的用户ID。

[0101] 可选的，所述隐私计算单元上可以部署有第一智能合约，所述第一智能合约用于接收所述外部服务器发送的检验触发指令，并响应于所述检验触发指令，执行根据所述标

准基础数据对所述待识别用户的基础数据进行一致性检验的操作。

[0102] 可选的，所述隐私计算单元中还部署有第二智能合约；所述将所述检验结果发送给所述第二机构，具体可以包括：

[0103] 调用所述第二智能合约发送所述检验结果至所述第二机构。

[0104] 需要说明的是，部署在隐私计算单元上的第二智能合约与第一智能合约可以是同一个合约，第一智能合约和第二智能合约的公私钥对可以相同，也可以在所述隐私计算单元仅包括该一个智能合约的情况下即等同于该隐私计算单元的公私钥对。第一智能合约接收所述外部服务器发送的检验触发指令，并响应于所述检验触发指令，执行根据所述标准基础数据对所述待识别用户的基础数据进行一致性检验的操作。得到检验结果后，调用所述第二智能合约发送所述检验结果至所述第二机构。

[0105] 可选的，所述确定所述第一机构上传的所述待识别用户的基础数据为真实数据之后，还可以包括：

[0106] 所述隐私计算单元生成用于证明所述第一机构上传的所述待识别用户的基础数据为真实数据的可验证声明。所述可验证声明中可以包含所述第一机构的数字签名和/或所述隐私计算单元的数字签名。可验证声明可以保存在区块链系统中。

[0107] 可验证声明(Verifiable Claim,VC)可以证明所述待识别用户的基础数据为真实数据，即可验证声明可以证明所述待识别用户的KYC检验结果是真实的。VC也是DID中的一项重要应用。所述VC可以存储于区块链平台。例如，VC的内容包括某个/某些用户ID对应的用户基础数据已经通过隐私计算单元的KYC检验，并由所述隐私计算单元签名；或者包括检验结果的hash值，并由所述隐私计算单元签名。当然，由于隐私计算单元检验的该基础数据是第一机构提供的，因此，该可验证声明中还可以包含所述第一机构的数字签名。

[0108] 监管机构在检查所述第二机构对用户的KYC的检验结果时，除了从第二机构获得所述匹配结果，还可以通过区块链来验证VC。具体的，监管机构可以从区块链上获取所述隐私计算单元的DIDdoc中的公钥，验证所述第二机构的所述用户ID的检验结果时，还采用所述隐私计算单元的公钥验证所述VC的签名，从而确认所述VC是由所述隐私计算单元颁发的，且是完整的，即没有经过篡改。这样，基于区块链平台的不可篡改特性以及签名机构的可信，可以提升对第二机构提供的KYC验证结果的真实性认可。所述签名机构的可信，即所述隐私计算单元/第二智能合约的可信，可以通过审计所述隐私计算单元的身份和其内部署的合约代码来实现。审计所述隐私计算单元的身份，具体例如前述所述的发起挑战的过程，可以验证其身份可信。

[0109] 通过上述方法，将KYC检验结果发送给第二机构，可以为本来没有能力做反洗钱工作的第二机构赋能，使得这样的机构能够具有购买其金融产品的用户的KYC检验结果，从而满足规定的反洗钱审核义务，提升行业整体的KYC检验能力。

[0110] 实施例2

[0111] 图3为本说明书实施例提供的一种数据检验的触发方法的流程图。从程序角度而言，流程的执行主体可以为搭载于应用服务器的程序或应用客户端。本实施例中的执行主体可以是部署在区块链以及隐私计算单元之外的一个外部服务器，该外部服务器可以用于定时触发隐私计算单元执行用户的KYC检验。该外部服务器也可以是一个服务器集群。该服务器集群中可以包括一个或多个服务器，这些服务器可以与区块链网络以及隐私计算单元

具有数据交互。

[0112] 如图3所示，该流程可以包括以下步骤：

[0113] 步骤310：外部服务器获取用于表示当前时刻的时间信息；所述外部服务器中部署有定时触发逻辑。

[0114] 具体而言，定时触发逻辑可用于确定隐私计算单元中的第一智能合约的启动时刻，并在当前时刻到达该启动时刻的情况下，启动第一智能合约。该智能合约中定义有用于完成用户的KYC检验的合约代码。

[0115] 时间信息可以是当前时刻的时刻信息，也可以是外部服务器中的计时功能的计时时长信息。外部服务器监控时间信息，定时向隐私计算单元发送检验触发指令，触发隐私计算单元执行KYC检验。

[0116] 步骤320：判断所述时间信息是否满足所述定时触发逻辑中的定时触发规则，得到判断结果。

[0117] 步骤330：若所述判断结果表示所述时间信息满足所述定时触发逻辑中的定时触发规则，向隐私计算单元发送检验触发指令；所述检验触发指令用于触发所述隐私计算单元根据从可信机构获取的经过加密后的待识别用户的标准基础数据对所述待识别用户的基础数据进行一致性检验；所述待识别用户的基础数据是对第一机构上传的加密后的待识别用户的基础数据进行解密得到的。

[0118] 该步骤与实施例1中的方法步骤对应，当外部服务器检测到时间信息满足所述定时触发逻辑中的定时触发规则，向隐私计算单元发送检验触发指令，触发隐私计算单元执行实施例1中的方法步骤，对待识别用户进行KYC检验。

[0119] 上述图3的步骤中，外部服务器向隐私计算单元发送检验触发指令时，可以通过以下方式进行触发：

[0120] 方式一、通过计时时长进行触发。具体可以包括以下步骤：

[0121] 判断所述计时时长是否达到所述预设时长；

[0122] 若所述计时时长达到所述预设时长，向所述隐私计算单元发送检验触发指令。例如：预设时长是3小时，即当外部服务器监测到计时时长达到3小时，就可以向隐私计算单元发送检验触发指令。

[0123] 方式二、通过时刻进行触发。具体可以包括以下步骤：

[0124] 判断所述当前时刻是否到达所述预设启动时刻；

[0125] 若所述当前时刻到达所述预设启动时刻，向所述隐私计算单元发送检验触发指令。例如：预设启动时刻是每天的8:00和18:00，那么在每天的8:00和18:00时，向隐私计算单元发送检验触发指令。

[0126] 方式三、结合时间信息和待检验数据的数据量共同触发。具体可以包括以下步骤：

[0127] 若所述计时时长未达到所述预设时长，或者，若所述当前时刻未到达所述预设启动时刻，获取云存储服务器中存储的待检验数据的数据量；

[0128] 判断所述数据量是否达到预设数据量阈值；

[0129] 若所述数据量达到所述预设数据量阈值，向隐私计算单元发送检验触发指令。

[0130] 需要说明的是，本说明书实施例中的方案通过外部服务器发送定时触发指令，主动触发隐私计算单元执行KYC检验(实际上是触发隐私计算单元中的第一智能合约执行KYC

检验)，但是，在实际应用中，也可以根据待检验数据的数据量来触发隐私计算单元执行KYC检验，因此，外部服务器向隐私计算单元发送检验触发指令可以通过以下方式触发：

[0131] 方式四、通过待检验数据的数据量进行触发。具体可以包括以下步骤：

[0132] 外部服务器获取云存储服务器中的待检测数据的数据量信息；所述数据量信息为所述待检测数据的数据量的具体数目；

[0133] 判断待检验数据的数据量是否达到预设数据量阈值；

[0134] 若所述待检验数据的数据量达到所述预设数据量阈值，向隐私计算单元发送检验触发指令。

[0135] 通过上述几种方式，可以触发外部服务器向隐私计算单元发送检验触发指令，触发隐私计算单元执行KYC检验，无需相关机构通过发起交易的方式来触发KYC检验，既可减少区块链节点处理调用目标智能合约的区块链交易的相关操作，也可减少相关机构发起交易的操作，有利于提升用户体验。

[0136] 图3中的方法，由外部服务器主动地向隐私计算单元发送检验触发指令，主动触发隐私计算单元中的第一智能合约完成KYC检验，使得相关机构无需定时通过发起交易的方式来调用智能合约。能减少隐私计算单元或区块链节点处理调用智能合约的交易的相关操作，可提高完成定时任务的效率。也可减少相关机构发起交易的操作，有利于提升用户体验。

[0137] 基于同样的思路，本说明书实施例还提供了上述实施例1中的方法对应的装置。图4是本说明书实施例提供的一种数据检验装置的结构示意图。如图4所示，该装置应用于隐私计算单元，该装置可以包括：

[0138] 检验触发指令获取模块410，用于获取外部服务器发送的检验触发指令；

[0139] 标准基础数据获取模块420，用于响应于所述检验触发指令，从可信机构获取经过加密后的待识别用户的标准基础数据；

[0140] 检验模块430，用于根据所述标准基础数据对所述待识别用户的基础数据进行一致性检验；所述待识别用户的基础数据是对第一机构上传的加密后的待识别用户的基础数据进行解密得到的。

[0141] 基于图4的装置，本说明书实施例还提供了该装置的一些具体实施方案，下面进行说明。

[0142] 可选的，所述检验触发指令获取模块410获取的所述检验触发指令是所述外部服务器按照定时触发规则发送的。

[0143] 可选的，所述定时触发规则可以包括预设时长或预设启动时刻。

[0144] 可选的，所述第一机构上传的加密后的待识别用户的基础数据可以存储在云存储服务器中。

[0145] 可选的，所述装置，还可以包括：

[0146] 基础数据获取模块，用于根据所述待识别用户的用户标识信息，从所述云存储服务器中获取所述用户标识信息对应的加密后的待识别用户的基础数据。

[0147] 可选的，所述用户标识信息可以包括：

[0148] 所述待识别用户在所述第一机构注册的账号；或，

[0149] 所述待识别用户在所述第一机构发起交易操作时由所述第一机构的系统为所述

待识别用户分配的账号。

[0150] 可选的，所述用户标识信息可以包括：

[0151] 对所述待识别用户的一项或多项信息经哈希计算得到的摘要值。

[0152] 可选的，所述用户标识信息可以包括：

[0153] 对所述待识别用户的一项或多项信息经加盐哈希计算得到的摘要值。

[0154] 可选的，所述隐私计算单元可以为部署在区块链系统上的隐私计算单元或部署在区块链系统之外的设备上的隐私计算单元；所述第一机构可以为代销机构。

[0155] 可选的，所述装置，还可以包括：

[0156] 解密模块，用于对从所述可信机构获取到的经过加密后的待识别用户的标准基础数据进行解密，得到所述标准基础数据。

[0157] 可选的，所述检验模块430，具体可以包括：

[0158] 比对单元，用于将所述待识别用户的基础数据与所述标准基础数据进行比对，得到检验结果；

[0159] 真实数据确定单元，用于当所述检验结果表示所述待识别用户的基础数据与所述标准基础数据一致时，确定所述第一机构上传的所述待识别用户的基础数据为真实数据；

[0160] 虚假数据确定单元，用于当所述检验结果表示所述待识别用户的基础数据与所述标准基础数据不一致时，确定所述第一机构上传的所述待识别用户的基础数据为虚假数据。

[0161] 可选的，所述检验模块430，还可以包括：

[0162] 检验结果获取请求接收单元，用于所述隐私计算单元接收第二机构发送的检验结果获取请求；所述检验结果获取请求用于请求获取根据所述标准基础数据对所述待识别用户的基础数据进行一致性检验得到的检验结果；所述检验结果获取请求中包含所述待识别用户的用户标识信息；

[0163] 检验结果发送单元，用于基于所述检验结果获取请求，将所述检验结果发送给所述第二机构；所述第二机构为金融机构。

[0164] 可选的，所述隐私计算单元可以部署有第一智能合约，所述第一智能合约用于接收所述外部服务器发送的检验触发指令，并响应于所述检验触发指令，执行根据所述标准基础数据对所述待识别用户的基础数据进行一致性检验的操作。

[0165] 可选的，所述检验模块430，还可以包括：

[0166] 可验证声明生成单元，用于所述隐私计算单元生成用于证明所述第一机构上传的所述待识别用户的基础数据为真实数据的可验证声明；所述可验证声明中包含所述第一机构的数字签名和/或所述隐私计算单元的数字签名。

[0167] 可选的，所述检验模块430，还可以包括：

[0168] 可验证声明存储单元，用于将所述可验证声明发送至区块链系统中进行保存。

[0169] 可选的，所述隐私计算单元中还可以部署有第二智能合约；

[0170] 可选的，所述检验结果发送单元，具体可以用于：

[0171] 调用所述第二智能合约发送所述检验结果至所述第二机构。

[0172] 可选的，所述装置，还可以包括：

[0173] 第一隐私计算单元身份证明模块，用于所述隐私计算单元向所述第一机构和/或

所述云存储服务器证明所述隐私计算单元的身份。

[0174] 可选的，所述装置，还可以包括：

[0175] 第二隐私计算单元身份证明模块，用于所述隐私计算单元向所述可信机构证明所述隐私计算单元的身份。

[0176] 可选的，所述装置，还可以包括：

[0177] 可信机构身份验证模块，用于隐私计算单元验证所述可信机构的身份信息。

[0178] 基于同样的思路，本说明书实施例还提供了上述实施例2中的方法对应的装置。图5是本说明书实施例提供的一种数据检验的触发装置的结构示意图。如图5所示，该装置可以包括：

[0179] 时间信息获取模块510，用于外部服务器获取用于表示当前时刻的时间信息；所述外部服务器中部署有定时触发逻辑；

[0180] 判断模块520，用于判断所述时间信息是否满足所述定时触发逻辑中的定时触发规则，得到判断结果；

[0181] 检验触发指令发送模块530，用于若所述判断结果表示所述时间信息满足所述定时触发逻辑中的定时触发规则，向隐私计算单元发送检验触发指令；所述检验触发指令用于触发所述隐私计算单元根据从可信机构获取的经过加密后的待识别用户的标准基础数据对所述待识别用户的基础数据进行一致性检验；所述待识别用户的基础数据是对第一机构上传的加密后的待识别用户的基础数据进行解密得到的。

[0182] 基于图5的装置，本说明书实施例还提供了该装置的一些具体实施方案，下面进行说明。

[0183] 可选的，所述定时触发规则可以为计时时长达到预设时长则进行触发；

[0184] 或者，所述定时触发规则可以为当前时刻达到预设时刻则进行触发。

[0185] 可选的，所述装置，还可以包括：

[0186] 待检验数据的数据量获取模块，用于若所述判断结果表示所述时间信息不满足所述定时触发逻辑中的定时触发规则，获取云存储服务器中存储的待检验数据的数据量；

[0187] 数据量判断模块，用于判断所述数据量是否达到预设数据量阈值；

[0188] 检验触发指令发送模块，用于若所述数据量达到所述预设数据量阈值，向隐私计算单元发送检验触发指令。

[0189] 基于同样的思路，本说明书实施例还提供了上述实施例中的方法对应的设备。

[0190] 图6是本说明书实施例提供的一种数据检验设备的结构示意图。如图6所示，设备600可以包括：

[0191] 至少一个处理器610；以及，

[0192] 与所述至少一个处理器通信连接的存储器630；其中，

[0193] 所述存储器630存储有可被所述至少一个处理器610执行的指令620，所述指令被所述至少一个处理器610执行。

[0194] 对应于实施例1，一种数据检验设备中，所述指令620可以使所述至少一个处理器610能够：

[0195] 获取外部服务器发送的检验触发指令；

[0196] 响应于所述检验触发指令，从可信机构获取经过加密后的待识别用户的标准基础

数据；

[0197] 根据所述标准基础数据对所述待识别用户的基础数据进行一致性检验；所述待识别用户的基础数据是对第一机构上传的加密后的待识别用户的基础数据进行解密得到的。

[0198] 对应于实施例2，一种数据检验的触发设备中，所述指令620可以使所述至少一个处理器610能够：

[0199] 获取用于表示当前时刻的时间信息；所述外部服务器中部署有定时触发逻辑；

[0200] 判断所述时间信息是否满足所述定时触发逻辑中的定时触发规则，得到判断结果；

[0201] 若所述判断结果表示所述时间信息满足所述定时触发逻辑中的定时触发规则，向隐私计算单元发送检验触发指令；所述检验触发指令用于触发所述隐私计算单元根据从可信机构获取的经过加密后的待识别用户的标准基础数据对所述待识别用户的基础数据进行一致性检验；所述待识别用户的基础数据是对第一机构上传的加密后的待识别用户的基础数据进行解密得到的。

[0202] 本说明书中的各个实施例均采用递进的方式描述，各个实施例之间相同相似的部分互相参见即可，每个实施例重点说明的都是与其他实施例的不同之处。尤其，对于图6所示的数据检验设备/数据检验触发设备而言，由于其基本相似于方法实施例，所以描述的比较简单，相关之处参见方法实施例的部分说明即可。

[0203] 在20世纪90年代，对于一个技术的改进可以很明显地区分是硬件上的改进(例如，对二极管、晶体管、开关等电路结构的改进)还是软件上的改进(对于方法流程的改进)。然而，随着技术的发展，当今的很多方法流程的改进已经可以视为硬件电路结构的直接改进。设计人员几乎都通过将改进的方法流程编程到硬件电路中来得到相应的硬件电路结构。因此，不能说一个方法流程的改进就不能用硬件实体模块来实现。例如，可编程逻辑器件(Programmable Logic Device, PLD)(例如现场可编程门阵列(Field Programmable Gate Array，FPGA))就是这样一种集成电路，其逻辑功能由用户对器件编程来确定。由设计人员自行编程来把一个数字符系统“集成”在一片PLD上，而不需要请芯片制造厂商来设计和制作专用的集成电路芯片。而且，如今，取代手工地制作集成电路芯片，这种编程也多半改用“逻辑编译器(logic compiler)”软件来实现，它与程序开发撰写时所用的软件编译器相类似，而要编译之前的原始代码也得用特定的编程语言来撰写，此称之为硬件描述语言(Hardware Description Language，HDL)，而HDL也并非仅有一种，而是有许多种，如ABEL(Advanced Boolean Expression Language)、AHDL(Altera Hardware Description Language)、Confluence、CUPL(Cornell University Programming Language)、HDCal、JHDL(Java Hardware Description Language)、Lava、Lola、MyHDL、PALASM、RHDL(Ruby Hardware Description Language)等，目前最普遍使用的是VHDL(Very-High-Speed Integrated Circuit Hardware Description Language)与Verilog。本领域技术人员也应该清楚，只需要将方法流程用上述几种硬件描述语言稍作逻辑编程并编程到集成电路中，就可以很容易得到实现该逻辑方法流程的硬件电路。

[0204] 控制器可以按任何适当的方式实现，例如，控制器可以采取例如微处理器或处理器以及存储可由该(微)处理器执行的计算机可读程序代码(例如软件或固件)的计算机可读介质、逻辑门、开关、专用集成电路(Application Specific Integrated Circuit，

ASIC)、可编程逻辑控制器和嵌入微控制器的形式，控制器的例子包括但不限于以下微控制器：ARC 625D、Atmel AT91SAM、Microchip PIC18F26K20 以及Silicone Labs C8051F320，存储器控制器还可以被实现为存储器的控制逻辑的一部分。本领域技术人员也知道，除了以纯计算机可读程序代码方式实现控制器以外，完全可以通过将方法步骤进行逻辑编程来使得控制器以逻辑门、开关、专用集成电路、可编程逻辑控制器和嵌入微控制器等的形式来实现相同功能。因此这种控制器可以被认为是一种硬件部件，而对其内包括的用于实现各种功能的装置也可以视为硬件部件内的结构。或者甚至，可以将用于实现各种功能的装置视为既可以是实现方法的软件模块又可以是硬件部件内的结构。

[0205] 上述实施例阐明的系统、装置、模块或单元，具体可以由计算机芯片或实体实现，或者由具有某种功能的产品来实现。一种典型的实现设备为计算机。具体的，计算机例如可以为个人计算机、膝上型计算机、蜂窝电话、相机电话、智能电话、个人数字符助理、媒体播放器、导航设备、电子邮件设备、游戏控制台、平板计算机、可穿戴设备或者这些设备中的任何设备的组合。

[0206] 虽然本说明书一个或多个实施例提供了如实施例或流程图所述的方法操作步骤，但基于常规或者无创造性的手段可以包括更多或者更少的操作步骤。实施例中列举的步骤顺序仅仅为众多步骤执行顺序中的一种方式，不代表唯一的执行顺序。在实际中的装置或终端产品执行时，可以按照实施例或者附图所示的方法顺序执行或者并行执行(例如并行处理器或者多线程处理的环境，甚至为分布式数据处理环境)。术语“包括”、“包含”或者其任何其他变体意在涵盖非排他性的包含，从而使得包括一系列要素的过程、方法、产品或者设备不仅包括那些要素，而且还包括没有明确列出的其他要素，或者是还包括为这种过程、方法、产品或者设备所固有的要素。在没有更多限制的情况下，并不排除在包括所述要素的过程、方法、产品或者设备中还存在另外的相同或等同要素。例如若使用到第一，第二等词语用来表示名称，而并不表示任何特定的顺序。

[0207] 为了描述的方便，描述以上装置时以功能分为各种单元分别描述。当然，在实施本申请时可以把各单元的功能在同一个或多个软件和/或硬件中实现。

[0208] 本领域内的技术人员应明白，本发明的实施例可提供为方法、系统、或计算机程序产品。因此，本发明可采用完全硬件实施例、完全软件实施例、或结合软件和硬件方面的实施例的形式。而且，本发明可采用在一个或多个其中包含有计算机可用程序代码的计算机可用存储介质(包括但不限于磁盘存储器、CD-ROM、光学存储器等)上实施的计算机程序产品的形式。

[0209] 本发明是参照根据本发明实施例的方法、设备(系统)、和计算机程序产品的流程图和/或方框图来描述的。应理解可由计算机程序指令实现流程图和/或方框图中的每一流程和/或方框、以及流程图和/或方框图中的流程和/或方框的结合。可提供这些计算机程序指令到通用计算机、专用计算机、嵌入式处理机或其他可编程数据处理设备的处理器以产生一个机器，使得通过计算机或其他可编程数据处理设备的处理器执行的指令产生用于实现在流程图一个流程或多个流程和/或方框图一个方框或多个方框中指定的功能的装置。

[0210] 这些计算机程序指令也可存储在能引导计算机或其他可编程数据处理设备以特定方式工作的计算机可读存储器中，使得存储在该计算机可读存储器中的指令产生包括指令装置的制造品，该指令装置实现在流程图一个流程或多个流程和/或方框图一个方框或

多个方框中指定的功能。

[0211] 这些计算机程序指令也可装载到计算机或其他可编程数据处理设备上，使得在计算机或其他可编程设备上执行一系列操作步骤以产生计算机实现的处理，从而在计算机或其他可编程设备上执行的指令提供用于实现在流程图一个流程或多个流程和/或方框图一个方框或多个方框中指定的功能的步骤。

[0212] 在一个典型的配置中，计算设备包括一个或多个处理器(CPU)、输入/输出接口、网络接口和内存。

[0213] 内存可能包括计算机可读介质中的非永久性存储器，随机存取存储器(RAM)和/或非易失性内存等形式，如只读存储器(ROM)或闪存(flash RAM)。内存是计算机可读介质的示例。

[0214] 计算机可读介质包括永久性和非永久性、可移动和非可移动媒体可以由任何方法或技术来实现信息存储。信息可以是计算机可读指令、数据结构、程序的模块或其他数据。计算机的存储介质的例子包括，但不限于相变内存(PRAM)、静态随机存取存储器(SRAM)、动态随机存取存储器(DRAM)、其他类型的随机存取存储器(RAM)、只读存储器(ROM)、电可擦除可编程只读存储器(EEPROM)、快闪记忆体或其他内存技术、只读光盘只读存储器(CD-ROM)、数字符多功能光盘(DVD)或其他光学存储、磁盒式磁带，磁带式磁盘存储或其他磁性存储设备或任何其他非传输介质，可用于存储可以被计算设备访问的信息。按照本文中的界定，计算机可读介质不包括暂存电脑可读媒体(transitory media)，如调制的数据信号和载波。

[0215] 还需要说明的是，术语“包括”、“包含”或者其任何其他变体意在涵盖非排他性的包含，从而使得包括一系列要素的过程、方法、商品或者设备不仅包括那些要素，而且还包括没有明确列出的其他要素，或者是还包括为这种过程、方法、商品或者设备所固有的要素。在没有更多限制的情况下，由语句“包括一个……”限定的要素，并不排除在包括所述要素的过程、方法、商品或者设备中还存在另外的相同要素。

[0216] 本领域技术人员应明白，本申请的实施例可提供为方法、系统或计算机程序产品。因此，本申请可采用完全硬件实施例、完全软件实施例或结合软件和硬件方面的实施例的形式。而且，本申请可采用在一个或多个其中包含有计算机可用程序代码的计算机可用存储介质(包括但不限于磁盘存储器、CD-ROM、光学存储器等)上实施的计算机程序产品的形式。

[0217] 本申请可以在由计算机执行的计算机可执行指令的一般上下文中描述，例如程序模块。一般地，程序模块包括执行特定任务或实现特定抽象数据类型的例程、程序、对象、组件、数据结构等等。也可以在分布式计算环境中实践本申请，在这些分布式计算环境中，由通过通信网络而被连接的远程处理设备来执行任务。在分布式计算环境中，程序模块可以位于包括存储设备在内的本地和远程计算机存储介质中。

[0218] 以上所述仅为本申请的实施例而已，并不用于限制本申请。对于本领域技术人员来说，本申请可以有各种更改和变化。凡在本申请的精神和原理之内所作的任何修改、等同替换、改进等，均应包含在本申请的权利要求范围之内。

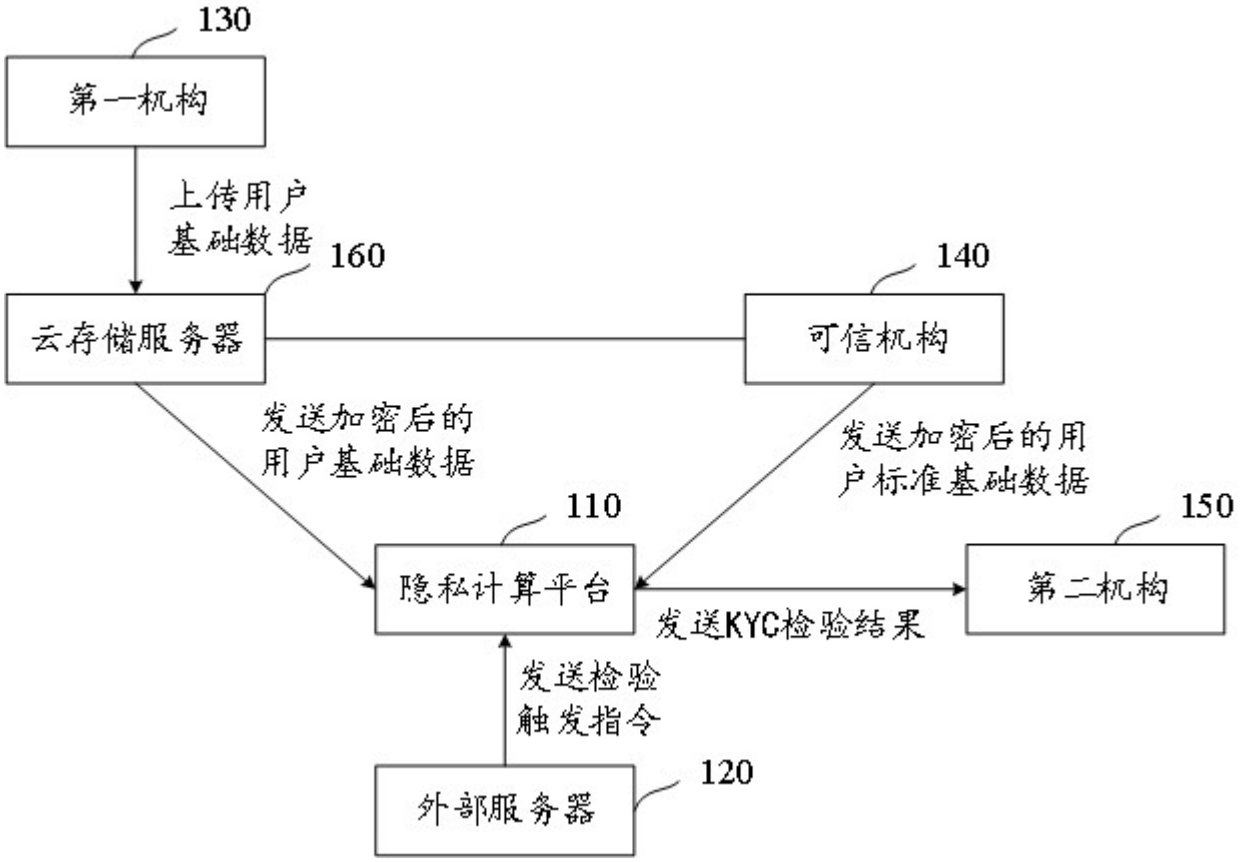

130
第一机构
上传用户
基础数据
160
云存储服务器
140
可信机构
发送加密后的
用户基础数据
发送加密后的用
户标准基础数据
110
隐私计算平台
150
第二机构
发送KYC检验结果
发送检验
触发指令
120
外部服务器

图1

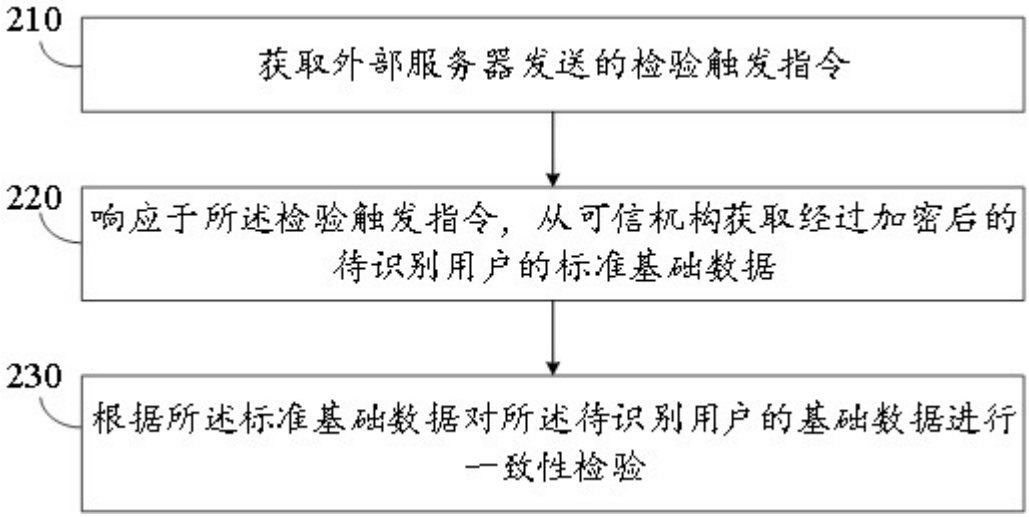

210
获取外部服务器发送的检验触发指令
220
响应于所述检验触发指令，从可信机构获取经过加密后的
待识别用户的标准基础数据
230
根据所述标准基础数据对所述待识别用户的基础数据进行
一致性检验

图2

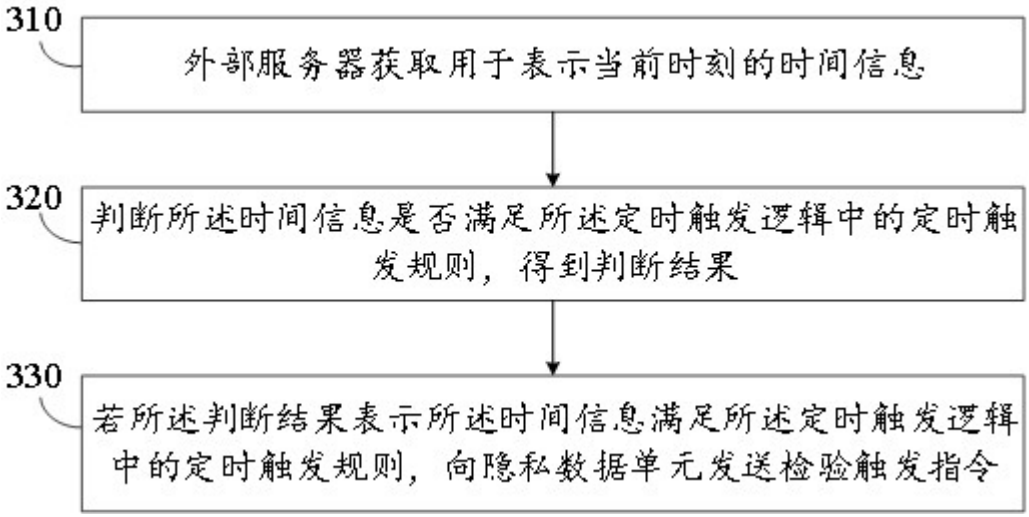

310
外部服务器获取用于表示当前时刻的时间信息
320
判断所述时间信息是否满足所述定时触发逻辑中的定时触发规则，得到判断结果
330
若所述判断结果表示所述时间信息满足所述定时触发逻辑中的定时触发规则，向隐私数据单元发送检验触发指令

图3

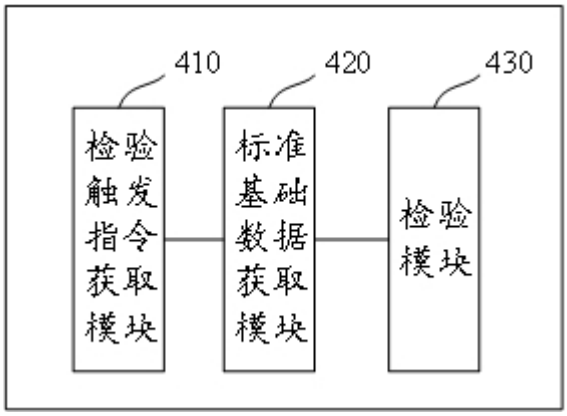

410
420
430
检验触发指令获取模块
标准基础数据获取模块
检验模块

图4

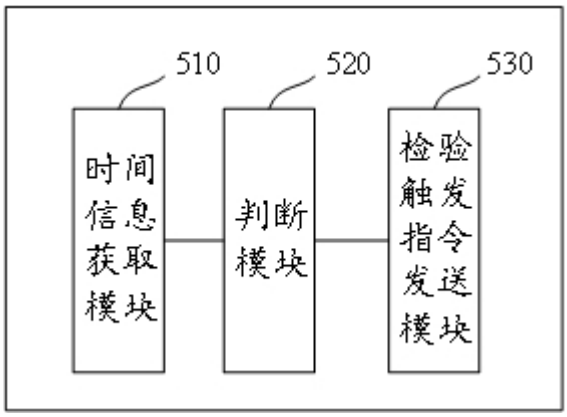

510
520
530
时间信息获取模块
判断模块
检验触发指令发送模块

图5

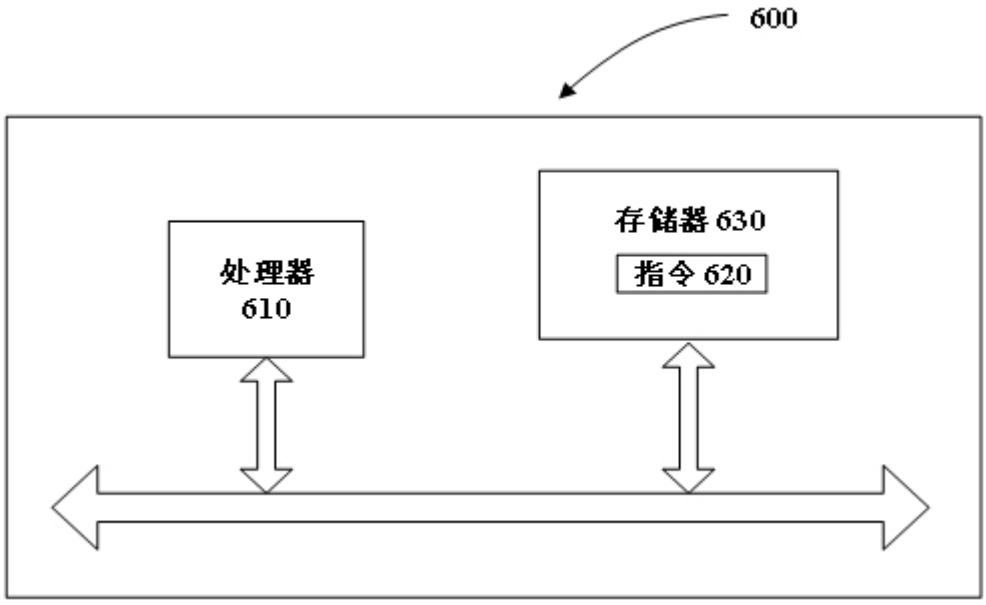


图6