(12) 按照专利合作条约所公布的国际申请

(19) 世界知识产权组织
国 际 局

(43) 国际公布日
2020 年 4 月 30 日 (30.04.2020)

WIPO | PCT

(10) 国际公布号
WO 2020/082889 A1

(51) 国际专利分类号:
G06Q 40/04 (2012.01) *G06Q 50/26* (2012.01)

(21) 国际申请号: PCT/CN2019/103093

(22) 国际申请日: 2019 年 8 月 28 日 (28.08.2019)

(25) 申请语言: 中文

(26) 公布语言: 中文

(30) 优先权:
201811260940.9 2018年10月26日 (26.10.2018) CN

(71) 申请人: 阿里巴巴集团控股有限公司 (**ALIBABA GROUP HOLDING LIMITED**) [—/CN]; 开曼群岛大开曼资本大厦一座四层 847 号邮箱, Grand Cayman (KY)。

(72) 发明人: 崔嘉辉 (**CUI, Jiahui**); 中国浙江省杭州市余杭区文一西路 969 号 3 号楼 5 楼阿里巴巴集团法务部, Zhejiang 311121 (CN)。 刘正 (**LIU, Zheng**); 中国浙江省杭州市余杭区文一西路 969 号 3 号楼 5 楼阿里巴巴集团法务部, Zhejiang 311121 (CN)。 殷山 (**YIN, Shan**); 中国浙江省杭州市余杭区文一西路 969 号 3 号楼 5 楼阿里巴巴集团法务部, Zhejiang 311121 (CN)。

(74) 代理人: 北京博思佳知识产权代理有限公司 (**BEIJING BESTIPR INTELLECTUAL PROPERTY LAW CORPORATION**); 中国北京市海淀区上地三街 9 号嘉华大厦 B 座 409, Beijing 100085 (CN)。

(81) 指定国 (除另有指明, 要求每一种可提供的国家保护): AE, AG, AL, AM, AO, AT, AU, AZ, BA, BB, BG, BH, BN, BR, BW, BY, BZ, CA, CH, CL, CN, CO, CR, CU, CZ, DE, DJ, DK, DM, DO, DZ, EC, EE, EG, ES, FI, GB, GD, GE, GH, GM, GT, HN, HR, HU, ID, IL, IN, IR, IS,

(54) **Title:** CREDIT REPORTING EVALUATION METHOD AND APPARATUS, AND ELECTRONIC DEVICE

(54) 发明名称: 征信评估方法及装置、电子设备

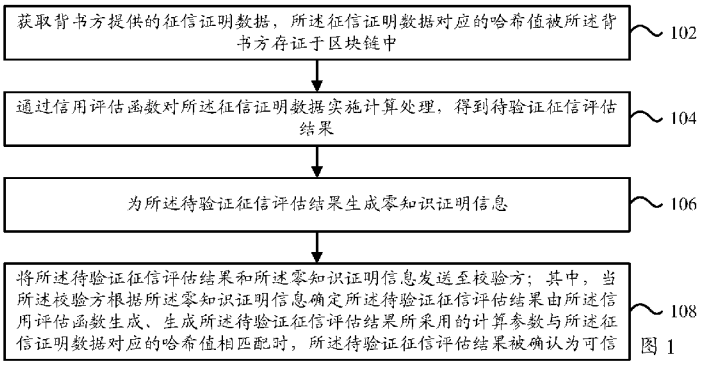

图 1

102 Acquire credit reporting proof data provided by an endorser, wherein a hash value corresponding to the credit reporting proof data is stored in a blockchain by the endorser for proofing
104 Implement calculation processing on the credit reporting proof data by means of a credit evaluation function, so as to obtain a credit reporting evaluation result to be verified
106 Generate zero-knowledge proof information for the credit reporting evaluation result to be verified
108 Send the credit reporting evaluation result to be verified and the zero-knowledge proof information to a checker, wherein when the checker determines, according to the zero-knowledge proof information, that the credit reporting evaluation result to be verified is generated by means of the credit evaluation function and that a calculation parameter used for generating the credit reporting evaluation result to be verified matches the hash value corresponding to the credit reporting proof data, the credit reporting evaluation result to be verified is confirmed to be credible

(57) **Abstract:** Provided are a credit reporting evaluation method and apparatus, and an electronic device. The method comprises: acquiring credit reporting proof data provided by an endorser, wherein a hash value corresponding to the credit reporting proof data is stored in a blockchain by the endorser for proofing; implementing calculation processing on the credit reporting proof data by means of a credit evaluation function, so as to obtain a credit reporting evaluation result to be verified; generating zero-knowledge proof information for the credit reporting evaluation result to be verified; and sending the credit reporting evaluation result to be verified and the zero-knowledge proof information to a checker, wherein when the checker determines, according to the zero-knowledge proof information, that the credit reporting evaluation result to be verified is generated by means of the credit evaluation function and that a calculation parameter used for generating the credit reporting evaluation result to be verified matches the hash value corresponding to the credit reporting proof data, the credit reporting evaluation result to be verified is confirmed to be credible.

WO 2020/082889 A1

[见续页]

JO, JP, KE, KG, KH, KN, KP, KR, KW, KZ, LA, LC, LK, LR, LS, LU, LY, MA, MD, ME, MG, MK, MN, MW, MX, MY, MZ, NA, NG, NI, NO, NZ, OM, PA, PE, PG, PH, PL, PT, QA, RO, RS, RU, RW, SA, SC, SD, SE, SG, SK, SL, SM, ST, SV, SY, TH, TJ, TM, TN, TR, TT, TZ, UA, UG, US, UZ, VC, VN, ZA, ZM, ZW。

(84) 指定国(除另有指明，要求每一种可提供的地区保护)：ARIPO (BW, GH, GM, KE, LR, LS, MW, MZ, NA, RW, SD, SL, ST, SZ, TZ, UG, ZM, ZW), 欧亚 (AM, AZ, BY, KG, KZ, RU, TJ, TM), 欧洲 (AL, AT, BE, BG, CH, CY, CZ, DE, DK, EE, ES, FI, FR, GB, GR, HR, HU, IE, IS, IT, LT, LU, LV, MC, MK, MT, NL, NO, PL, PT, RO, RS, SE, SI, SK, SM, TR), OAPI (BF, BJ, CF, CG, CI, CM, GA, GN, GQ, GW, KM, ML, MR, NE, SN, TD, TG)。

本国际公布:

— 包括国际检索报告(条约第21条(3))。

(57) 摘要：本说明书一个或多个实施例提供一种征信评估方法及装置、电子设备，该方法包括：获取背书方提供的征信证明数据，所述征信证明数据对应的哈希值被所述背书方存证于区块链中；通过信用评估函数对所述征信证明数据实施计算处理，得到待验证征信评估结果；为所述待验证征信评估结果生成零知识证明信息；将所述待验证征信评估结果和所述零知识证明信息发送至校验方；其中，当所述校验方根据所述零知识证明信息确定所述待验证征信评估结果由所述信用评估函数生成、生成所述待验证征信评估结果所采用的计算参数与所述征信证明数据对应的哈希值相匹配时，所述待验证征信评估结果被确认为可信。

征信评估方法及装置、电子设备

技术领域

[01]本说明书一个或多个实施例涉及区块链技术领域，尤其涉及一种征信评估方法及装置、电子设备。

背景技术

[02]在征信评估的过程中，存在证明方、校验方和背书方三种角色，其中校验方需要对证明方的征信状况进行评估，而评估所需的数据存储于背书方处。背书方基于隐私方面的考虑而不会公开证明方的相关数据，可由证明方授权从背书方处获取相关数据后，提供至校验方进行征信评估。

发明内容

[03]有鉴于此，本说明书一个或多个实施例提供一种征信评估方法及装置、电子设备。

[04]为实现上述目的，本说明书一个或多个实施例提供技术方案如下:

[05]根据本说明书一个或多个实施例的第一方面，提出了一种征信评估方法，应用于证明方，所述方法包括:

[06]获取背书方提供的征信证明数据，所述征信证明数据对应的哈希值被所述背书方存证于区块链中;

[07]通过信用评估函数对所述征信证明数据实施计算处理，得到待验证征信评估结果;

[08]为所述待验证征信评估结果生成零知识证明信息;

[09]将所述待验证征信评估结果和所述零知识证明信息发送至校验方；其中，当所述校验方根据所述零知识证明信息确定所述待验证征信评估结果由所述信用评估函数生成、生成所述待验证征信评估结果所采用的计算参数与所述征信证明数据对应的哈希值相匹配时，所述待验证征信评估结果被确认为可信。

[10]根据本说明书一个或多个实施例的第二方面，提出了一种征信评估方法，应用于校验方，所述方法包括:

[11]接收证明方提供的待验证征信评估结果和零知识证明信息;

[12]根据所述零知识证明信息验证是否满足下述条件：所述待验证征信评估结果由信用评估函数生成、生成所述待验证征信评估结果所采用的计算参数与背书方存证于区块链中的哈希值相匹配，其中所述哈希值对应于所述背书方记录的所述证明方的征信证明数据；

[13]当所述零知识证明信息满足上述条件时，确认所述待验证征信评估结果可信。

[14]根据本说明书一个或多个实施例的第三方面，提出了一种征信评估装置，应用于证明方，所述装置包括：

[15]数据获取单元，获取背书方提供的征信证明数据，所述征信证明数据对应的哈希值被所述背书方存证于区块链中；

[16]计算单元，通过信用评估函数对所述征信证明数据实施计算处理，得到待验证征信评估结果；

[17]生成单元，为所述待验证征信评估结果生成零知识证明信息；

[18]发送单元，将所述待验证征信评估结果和所述零知识证明信息发送至校验方；其中，当所述校验方根据所述零知识证明信息确定所述待验证征信评估结果由所述信用评估函数生成、生成所述待验证征信评估结果所采用的计算参数与所述征信证明数据对应的哈希值相匹配时，所述待验证征信评估结果被确认为可信。

[19]根据本说明书一个或多个实施例的第四方面，提出了一种征信评估装置，应用于校验方，所述装置包括：

[20]第一接收单元，接收证明方提供的待验证征信评估结果和零知识证明信息；

[21]验证单元，根据所述零知识证明信息验证是否满足下述条件：所述待验证征信评估结果由信用评估函数生成、生成所述待验证征信评估结果所采用的计算参数与背书方存证于区块链中的哈希值相匹配，其中所述哈希值对应于所述背书方记录的所述证明方的征信证明数据；

[22]确认单元，当所述零知识证明信息满足上述条件时，确认所述待验证征信评估结果可信。

[23]根据本说明书一个或多个实施例的第五方面，提出了一种电子设备，包括：

[24]处理器；

[25]用于存储处理器可执行指令的存储器；

[26]其中，所述处理器通过运行所述可执行指令以实现如第一方面中任一实施例所述的方法。

[27]根据本说明书一个或多个实施例的第六方面，提出了一种电子设备，包括：

[28]处理器；

[29]用于存储处理器可执行指令的存储器；

[30]其中，所述处理器通过运行所述可执行指令以实现如第二方面中任一实施例所述的方法。

附图说明

[31]图 1 是一示例性实施例提供的一种征信评估方法的流程图。

[32]图 2 是一示例性实施例提供的另一种征信评估方法的流程图。

[33]图 3 是一示例性实施例提供的一种评估用户征信状况的交互示意图。

[34]图 4 是一示例性实施例提供的一种设备的结构示意图。

[35]图 5 是一示例性实施例提供的一种装置的框图。

[36]图 6 是一示例性实施例提供的另一种设备的结构示意图。

[37]图 7 是一示例性实施例提供的另一种装置的框图。

具体实施方式

[38]这里将详细地对示例性实施例进行说明，其示例表示在附图中。下面的描述涉及附图时，除非另有表示，不同附图中的相同数字表示相同或相似的要素。以下示例性实施例中所描述的实施方式并不代表与本说明书一个或多个实施例相一致的所有实施方式。相反，它们仅是与如所附权利要求书中所详述的、本说明书一个或多个实施例的一些方面相一致的装置和方法的例子。

[39]需要说明的是：在其他实施例中并不一定按照本说明书示出和描述的顺序来执行相应方法的步骤。在一些其他实施例中，其方法所包括的步骤可以比本说明书所描述的更多或更少。此外，本说明书中所描述的单个步骤，在其他实施例中可能被分解为多个步骤进行描述；而本说明书中所描述的多个步骤，在其他实施例中也可能被合并为单个步骤进行描述。

[40]图 1 是一示例性实施例提供的一种征信评估方法的流程图。如图 1 所示，该方法应用于证明方，可以包括以下步骤:

[41]步骤 102，获取背书方提供的征信证明数据，所述征信证明数据对应的哈希值被所述背书方存证于区块链中。

[42]在一实施例中，背书方用于对证明方的征信证明数据进行存储、保护和背书，该征信证明用户可以用于证明该证明方的征信状况。征信证明数据具有一定的隐私性，背书方不会直接将该征信证明数据提供至诸如校验方等，以避免隐私数据发生泄露。

[43]在一实施例中，背书方可以通过向区块链中发布交易，以使得哈希值被存证于区块链中。在本说明书中所描述的交易（transfer），是指用户通过区块链的客户端创建，并需要最终发布至区块链的分布式数据库中的一笔数据。其中，区块链中的交易，存在狭义的交易以及广义的交易之分。狭义的交易是指用户向区块链发布的一笔价值转移；例如，在传统的比特币区块链网络中，交易可以是用户在区块链中发起的一笔转账。而广义的交易是指用户向区块链发布的一笔具有业务意图的业务数据；例如，运营方可以基于实际的业务需求搭建一个联盟链，依托于联盟链部署一些与价值转移无关的其它类型的在线业务（比如，征信评估业务、租房业务、车辆调度业务、保险理赔业务、信用服务、医疗服务等），而在这类联盟链中，交易可以是用户在联盟链中发布的一笔具有业务意图的业务消息或者业务请求。

[44]在一实施例中，所述哈希值可以由所述背书方对所述征信证明数据和随机数进行哈希计算得到，从而防止取值空间太小而导致的穷举攻击，从而有助于提升可靠性。而证明方可以获取所述背书方提供的对应于所述哈希值的随机数，从而验证所述征信证明数据、所述随机数和所述哈希值之间的对应关系，防止诸如背书方对征信证明数据进行更新但未及时更新哈希值等问题，避免校验方实施的校验操作失败。

[45]在一实施例中，背书方可以通过自身的私钥对存证于区块链账本中的哈希值进行签名，背书方在向证明方提供征信证明数据、存证凭证等时也可以添加签名，以确保相关数据的可靠性，表明相关数据未被篡改。

[46]步骤 104，通过信用评估函数对所述征信证明数据实施计算处理，得到待验证征信评估结果。

[47]在一实施例中，信用评估函数可以为默认函数，而信用评估函数所采用的计算参数为默认参数，证明方可以基于默认设定而获知该默认函数和默认参数，而校验方同样了

解该默认函数，可以基于该默认函数对待验证征信评估结果进行验证。

[48]在一实施例中，校验方可以将希望采用的信用评估函数及其计算参数发送至证明方，使得证明方基于该信用评估函数对相关计算参数进行处理而得到待验证征信评估结果，因而校验方能够便于针对所采用的信用评估函数及其计算参数进行调整（比如针对不同证明方采用不同版本的函数）、升级等处理。同时，由于证明方针对待验证征信评估结果的计算、校验方将信用评估函数及其计算参数发送至证明方等操作均在链下完成，并不需要公布和记录在区块链账本中，因而不会对诸如信用评估函数造成公开，校验方不需要担心对信用评估函数所采用的计算方式造成泄露。

[49]步骤 106，为所述待验证征信评估结果生成零知识证明信息。

[50]在一实施例中，证明方可以基于相关技术中的零知识证明（Zero—Knowledge Proof）技术，为待验证征信评估结果生成相应的零知识证明信息，使得校验方即便不需要获知征信证明数据的情况下，也可以对待验证征信评估结果进行验证，从而既可以避免征信证明数据的泄露，又能够满足其验证需求。例如，本说明书可以采用相关技术中的zkSNARK（Zero-Knowledge Succinct Non-Interactive Argument of Knowledge，零知识下简明的非交互知识论证）等任意类型的零知识证明技术，本说明书并不对此进行限制。

[51]步骤 108，将所述待验证征信评估结果和所述零知识证明信息发送至校验方；其中，当所述校验方根据所述零知识证明信息确定所述待验证征信评估结果由所述信用评估函数生成、生成所述待验证征信评估结果所采用的计算参数与所述征信证明数据对应的哈希值相匹配时，所述待验证征信评估结果被确认为可信。

[52]在一实施例中，背书方只需将证明方的征信证明数据的哈希值存证于区块链中，而无需向外界（除证明方之外）提供征信证明数据的明文内容，即可通过本说明书的技术方案而确保校验方可以对证明方提供的待验证征信评估结果进行验证，既可以避免对征信证明数据造成泄露，又可以避免证明方对征信证明数据进行篡改造假，还可以确保校验方的验证过程不出现违规情况。

[53]在一实施例中，证明方可以获取所述背书方提供的所述哈希值对应的存证凭证，比如该存证凭证可以包括哈希值在区块链账本中的位置（比如哈希值所处的区块、哈希值所在交易的流水号等）、哈希值的取值等，而证明方可以将所述存证凭证发送至所述校验方，以使所述校验方根据所述存证凭证从区块链中查找到所述哈希值，从而针对待验证征信评估结果进行验证。当然，校验方还可以通过其他方式从区块链中查找到哈希值，

比如校验方直接向背书方索要等，本说明书并不对此进行限制。

[54]图 2 是一示例性实施例提供的另一种征信评估方法的流程图。如图 2 所示，该方法应用于校验方，可以包括以下步骤：

[55]步骤 202，接收证明方提供的待验证征信评估结果和零知识证明信息。

[56]步骤 204，根据所述零知识证明信息验证是否满足下述条件：所述待验证征信评估结果由信用评估函数生成、生成所述待验证征信评估结果所采用的计算参数与背书方存证于区块链中的哈希值相匹配，其中所述哈希值对应于所述背书方记录的所述证明方的征信证明数据。

[57]在一实施例中，背书方用于对证明方的征信证明数据进行存储、保护和背书，该征信证明用户可以用于证明该证明方的征信状况。征信证明数据具有一定的隐私性，背书方不会直接将该征信证明数据提供至诸如校验方等，以避免隐私数据发生泄露。

[58]在一实施例中，背书方可以通过向区块链中发布交易，以使得哈希值被存证于区块链中。在本说明书中所描述的交易，是指用户通过区块链的客户端创建，并需要最终发布至区块链的分布式数据库中的一笔数据。其中，区块链中的交易，存在狭义的交易以及广义的交易之分。狭义的交易是指用户向区块链发布的一笔价值转移；例如，在传统的比特币区块链网络中，交易可以是用户在区块链中发起的一笔转账。而广义的交易是指用户向区块链发布的一笔具有业务意图的业务数据；例如，运营方可以基于实际的业务需求搭建一个联盟链，依托于联盟链部署一些与价值转移无关的其它类型的在线业务（比如，征信评估业务、租房业务、车辆调度业务、保险理赔业务、信用服务、医疗服务等），而在这类联盟链中，交易可以是用户在联盟链中发布的一笔具有业务意图的业务消息或者业务请求。

[59]在一实施例中，所述哈希值可以由所述背书方对所述征信证明数据和随机数进行哈希计算得到，从而防止取值空间太小而导致的穷举攻击，从而有助于提升可靠性。而证明方可以获取所述背书方提供的对应于所述哈希值的随机数，从而验证所述征信证明数据、所述随机数和所述哈希值之间的对应关系，防止诸如背书方对征信证明数据进行更新但未及时更新哈希值等问题，避免校验方实施的校验操作失败。

[60]在一实施例中，背书方可以通过自身的私钥对存证于区块链账本中的哈希值进行签名，背书方在向证明方提供征信证明数据、存证凭证等时也可以添加签名，以确保相关数据的可靠性，表明相关数据未被篡改。

[61]在一实施例中，信用评估函数可以为默认函数，而信用评估函数所采用的计算参数为默认参数，证明方可以基于默认设定而获知该默认函数和默认参数，而校验方同样了解该默认函数，可以基于该默认函数对待验证征信评估结果进行验证。

[62]在一实施例中，校验方可以将希望采用的信用评估函数及其计算参数发送至证明方，使得证明方基于该信用评估函数对相关计算参数进行处理而得到待验证征信评估结果，因而校验方能够便于针对所采用的信用评估函数及其计算参数进行调整（比如针对不同证明方采用不同版本的函数）、升级等处理。同时，由于证明方针对待验证征信评估结果的计算、校验方将信用评估函数及其计算参数发送至证明方等操作均在链下完成，并不需要公布和记录在区块链账本中，因而不会对诸如信用评估函数造成公开，校验方不需要担心对信用评估函数所采用的计算方式造成泄露。

[63]在一实施例中，证明方可以基于相关技术中的零知识证明技术，为待验证征信评估结果生成相应的零知识证明信息，使得校验方即便不需要获知征信证明数据的情况下，也可以对待验证征信评估结果进行验证，从而既可以避免征信证明数据的泄露，又能够满足其验证需求。例如，本说明书可以采用相关技术中的 zkSNARK 等任意类型的零知识证明技术，本说明书并不对此进行限制。

[64]步骤 206，当所述零知识证明信息满足上述条件时，确认所述待验证征信评估结果可信。

[65]在一实施例中，背书方只需将证明方的征信证明数据的哈希值存证于区块链中，而无需向外界（除证明方之外）提供征信证明数据的明文内容，即可通过本说明书的技术方案而确保校验方可以对证明方提供的待验证征信评估结果进行验证，既可以避免对征信证明数据造成泄露，又可以避免证明方对征信证明数据进行篡改造假，还可以确保校验方的验证过程不出现违规情况。

[66]在一实施例中，证明方可以获取所述背书方提供的所述哈希值对应的存证凭证，比如该存证凭证可以包括哈希值在区块链账本中的位置（比如哈希值所处的区块、哈希值所在交易的流水号等）、哈希值的取值等，而证明方可以将所述存证凭证发送至所述校验方，以使所述校验方根据所述存证凭证从区块链中查找到所述哈希值，从而针对待验证征信评估结果进行验证。当然，校验方还可以通过其他方式从区块链中查找到哈希值，比如校验方直接向背书方索要等，本说明书并不对此进行限制。

[67]图 3 是一示例性实施例提供的一种评估用户征信状况的交互示意图。假定由政府机

构对各个用户的征信证明数据进行保存，为该征信证明数据的有效性、可靠性等进行背书，比如该征信证明数据可以包括纳税数据等，本说明书并不对此进行限制；而征信机构需要对用户的征信情况进行计算，该过程中需要应用到政府机构记录的纳税数据等征信证明数据；如图 3 所示，通过在征信结构、用户、政府机构之间的交互过程，并结合对区块链的应用，可以在有效评估出用户的征信状况的同时，确保征信证明数据不会发生泄露或篡改等异常，该交互过程可以包括以下步骤：

[68] 步骤 301，政府机构记录用户的纳税数据。

[69] 在一实施例中，政府机构可以根据用户在税务部门的纳税记录，生成相应的纳税数据，该纳税数据的真实、可靠性已经通过了政府机构的检验，由政府部门对该纳税数据进行背书。

[70] 步骤 302，政府机构生成纳税数据对应的哈希值 h，并对该哈希值 h 签名后提交至区块链中，以存证于区块链中。

[71] 在一实施例中，政府机构可以通过预定义的哈希函数 H()对纳税数据进行计算，得到相应的哈希值 h。由于哈希算法的特性，使得纳税数据与哈希值 h 之间能够保证可靠的对应关系，并且哈希值 h 不会暴露纳税数据的内容，即无法由哈希值 h 反推出纳税数据。

[72] 在一实施例中，为了防止取值空间太小而受到穷举攻击，政府机构在计算上述哈希值 h 时，可以添加一随机数 r，使得哈希函数 H()被应用于同时针对纳税数据和随机数 r 进行计算，以得到上述的哈希值 h，可以进一步确保哈希值 h 不会暴露纳税数据的内容，可以提升安全性。

[73] 在一实施例中，政府机构可以通过对应于自身数字身份的私钥，对哈希值 h 进行签名；而政府机构的公钥处于公开状态，使得诸如征信结构、用户等均可以通过公钥对该签名进行验证，从而确保哈希值 h 由政府结构发布且未经篡改。

[74] 在一实施例中，政府机构可以被配置为区块链中的一区块链节点，比如该区块链可以为联盟链，使得政府机构可以通过向区块链发布一笔交易，将哈希值 h 存证于区块链中，即存证于区块链账本中。由于区块链的分布式特性，使得哈希值 h 被提交至区块链、存证于区块链账本时，该哈希值 h 无法被不法分子进行篡改，具有极高的安全性和可靠度。

[75] 步骤 303a，政府机构向用户提供纳税数据及存证凭证。

[76]在一实施例中，当用户需要生成或更新征信数据时，可以向政府机构提出数据获取请求，使得政府机构在验证该用户的身份无误后，可以向该用户提供纳税数据、对应于该纳税数据的哈希值 h 的存证凭证等，以用于后续处理。

[77]在一实施例中，除了纳税数据之外，还可能存在其他类型的征信证明数据，这些征信证明数据可以由不同的政府机构分别用于管理，这些政府机构可以分别通过诸如上述的步骤 301-302、对自身维护的征信证明数据进行管理和存证，而用户可以在步骤 303a 中分别从各个政府机构处分别获取所需的纳税数据及其存证凭证，此处不再赘述。下面均以用户获取纳税数据及其存证凭证为例进行说明

[78]步骤 303b，征信机构向用户提供信用评估函数 f()。

[79]在一实施例中，当用户需要生成或更新征信数据时，可以向征信机构提出生成请求或更新请求，使得征信机构可以将信用评估函数 f()提供至该用户。当然，征信机构也可以在其他时机下，将信用评估函数 f()提供至用户，本说明书并不对此进行限制。

[80]在一实施例中，征信机构与用户之间对于信用评估函数 f()的传输操作可以在链下实施，而并不需要发布至区块链，使得该信用评估函数 f()所采用的计算方式等不会发生泄露，并且征信机构可以根据实际情况对传输的信用评估函数 f()进行版本调整、版本更新等，操作灵活。

[81]在一实施例中，征信机构在提供信用评估函数 f()的同时，如需必要还应当指明该信用评估函数 f()所需采用的计算参数，以使得用户可以基于该计算参数确定针对该信用评估函数 f()的输入数据。例如，用户可以首先从征信机构处获得信用评估函数 f()，然后基于该信用评估函数 f()所需采用的计算参数，向对应的政府机构获得相应的征信证明数据等；当然，用户也可以向所有政府机构获得所有的征信证明数据，然后针对该信用评估函数 f()所需采用的计算参数，选择相应的输入数据。

[82]在一实施例中，政府机构向用户提供的存证凭证可以包括：哈希值 h、计算哈希值 h 所采用的随机数 r、哈希值 h 在区块链账本中的位置、政府机构对哈希值 h 的签名等，本说明书并不对此进行限制。用户可以验证哈希值 h 的签名，以确定其未被篡改；用户可以根据哈希值 h 在区块链账本中的位置，从而区块链账本中查询到相应的存证内容，以验证该存证内容与纳税数据、随机数 r 等之间的一致性，以确定哈希值 h 对应于纳税数据。

[83]步骤 304，用户计算待验证结果 s。

[84]在一实施例中，用户通过征信机构提供的信用评估函数 f()，对纳税数据等进行计算，得到相应的待验证结果 s。事实上，如果纳税数据真实可靠，该待验证结果 s 就是对应于该用户的征信状况的计算结果，但由于尚未经过校验方的校验，因而此处称之为待验证结果 s，以避免用户通过对信用评估函数 f()进行调换、对纳税数据进行篡改等方式而生成伪造结果。

[85]步骤 305，用户生成零知识证明 p。

[86]在一实施例中，用户可以利用相关技术中的零知识证明技术，生成针对待验证结果 s 的零知识证明 p，使得征信机构可以基于该零知识证明 p 实现相关证明，确定待验证结果 s 的有效性。

[87]步骤 306，用户向征信机构发送待验证结果 s、零知识证明 p、存证凭证。

[88]步骤 307，征信机构根据存证凭证从区块链中获取相应的哈希值 h。

[89]在一实施例中，用户向征信机构提供的存证凭证可以包括哈希值 h、哈希值 h 在区块链账本中的位置、政府机构对哈希值 h 的签名等，但不能包含上述的随机数 r 等信息，以避免不法分子根据该随机数 r 实施穷举攻击。征信机构可以被配置为区块链中的一区块链节点，比如该区块链可以为联盟链，使得征信机构可以根据存证凭证从区块链账本中获取对应于该用户的纳税数据的哈希值 h。

[90]当然，除了用户提供的存证凭证之外，征信机构还可以通过其他方式从区块链中获得哈希值 h，本说明书并不对此进行限制。

[91]步骤 308，征信机构验证待验证结果 s。

[92]在一实施例中，征信机构可以根据获得的零知识证明 p，验证是否满足下述条件：

[93]①证明方在通过信用评估函数 f()计算出待验证结果 s 的过程中，输入的计算参数是否对应于上述的哈希值 h;

[94]②证明方是否忠实地执行了信用评估函数 f()而得到待验证结果 s，而未采用其他函数进行替代。

[95]其中，当上述的条件①和条件②均被满足时，征信机构可以确认待验证结果 s 可信，从而据此确定用户的征信状况；否则，征信机构可以认为待验证结果 s 不可信。

[96]图 4 是一示例性实施例提供的一种设备的示意结构图。请参考图 4，在硬件层面，该设备包括处理器 402、内部总线 404、网络接口 406、内存 408 以及非易失性存储器

410，当然还可能包括其他业务所需要的硬件。处理器 402 从非易失性存储器 410 中读取对应的计算机程序到内存 408 中然后运行，在逻辑层面上形成征信评估装置。当然，除了软件实现方式之外，本说明书一个或多个实施例并不排除其他实现方式，比如逻辑器件抑或软硬件结合的方式等等，也就是说以下处理流程的执行主体并不限定于各个逻辑单元，也可以是硬件或逻辑器件。

[97]请参考图 5，在软件实施方式中，该征信评估装置应用于证明方，该装置可以包括：

[98]数据获取单元 51，获取背书方提供的征信证明数据，所述征信证明数据对应的哈希值被所述背书方存证于区块链中；

[99]计算单元 52，通过信用评估函数对所述征信证明数据实施计算处理，得到待验证征信评估结果；

[100] 生成单元 53，为所述待验证征信评估结果生成零知识证明信息；

[101] 发送单元 54，将所述待验证征信评估结果和所述零知识证明信息发送至校验方；其中，当所述校验方根据所述零知识证明信息确定所述待验证征信评估结果由所述信用评估函数生成、生成所述待验证征信评估结果所采用的计算参数与所述征信证明数据对应的哈希值相匹配时，所述待验证征信评估结果被确认为可信。

[102] 可选的，

[103] 所述信用评估函数为默认函数，所述信用评估函数所采用的计算参数为默认参数；

[104] 或者，所述装置还包括：确定单元 55，根据所述校验方发送的指示信息，确定所采用的信用评估函数及其计算参数。

[105] 可选的，还包括：

[106] 凭证获取单元 56，获取所述背书方提供的所述哈希值对应的存证凭证；

[107] 凭证发送单元 57，将所述存证凭证发送至所述校验方，以使所述校验方根据所述存证凭证从区块链中查找到所述哈希值。

[108] 可选的，所述存证凭证包括以下至少之一：所述哈希值、所述哈希值在区块链上的记录位置。

[109] 可选的，所述哈希值由所述背书方对所述征信证明数据和随机数进行哈希计算得到；所述装置还包括：

[110] 随机数获取单元 58，获取所述背书方提供的对应于所述哈希值的随机数；

[111] 验证单元 59，验证所述征信证明数据、所述随机数和所述哈希值之间的对应关系。

[112] 图 6 是一示例性实施例提供的一种设备的示意结构图。请参考图 6，在硬件层面，该设备包括处理器 602、内部总线 604、网络接口 606、内存 608 以及非易失性存储器 610，当然还可能包括其他业务所需要的硬件。处理器 602 从非易失性存储器 610 中读取对应的计算机程序到内存 608 中然后运行，在逻辑层面上形成征信评估装置。当然，除了软件实现方式之外，本说明书一个或多个实施例并不排除其他实现方式，比如逻辑器件抑或软硬件结合的方式等等，也就是说以下处理流程的执行主体并不限定于各个逻辑单元，也可以是硬件或逻辑器件。

[113] 请参考图 7，在软件实施方式中，该征信评估装置应用于校验方，该装置可以包括：

[114] 第一接收单元 71，接收证明方提供的待验证征信评估结果和零知识证明信息；

[115] 验证单元 72，根据所述零知识证明信息验证是否满足下述条件：所述待验证征信评估结果由信用评估函数生成、生成所述待验证征信评估结果所采用的计算参数与背书方存证于区块链中的哈希值相匹配，其中所述哈希值对应于所述背书方记录的所述证明方的征信证明数据；

[116] 确认单元 73，当所述零知识证明信息满足上述条件时，确认所述待验证征信评估结果可信。

[117] 可选的，

[118] 所述信用评估函数为默认函数，所述信用评估函数所采用的计算参数为默认参数；

[119] 或者，所述装置还包括：发送单元 74，向所述证明方发送指示信息，以指示所述证明方所采用的信用评估函数及其计算参数。

[120] 可选的，还包括：

[121] 第二接收单元 75，接收所述证明方提供的所述哈希值对应的存证凭证，所述存证凭证由所述背书方提供至所述证明方；

[122] 查找单元 76，根据所述存证凭证从区块链中查找到所述哈希值。

[123] 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，计算机的具体形式可以是个人计算机、膝上型计算机、蜂窝电话、相机电话、智能电话、个人数字助理、媒体播放器、导航设备、电子邮件收发设备、游戏控制台、平板计算机、可穿戴设备或者这些设备中的任意几种设备的组合。

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

[125] 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。

[126] 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)、数字多功能光盘 (DVD) 或其他光学存储、磁盒式磁带、磁盘存储、量子存储器、基于石墨烯的存储介质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。

[127] 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。

[128] 上述对本说明书特定实施例进行了描述。其它实施例在所附权利要求书的范围内。在一些情况下，在权利要求书中记载的动作或步骤可以按照不同于实施例中的顺序来执行并且仍然可以实现期望的结果。另外，在附图中描绘的过程不一定要求示出的特定顺序或者连续顺序才能实现期望的结果。在某些实施方式中，多任务处理和并行处理也是可以的或者可能是有利的。

[129] 在本说明书一个或多个实施例使用的术语是仅仅出于描述特定实施例的目的，而非旨在限制本说明书一个或多个实施例。在本说明书一个或多个实施例和所附权利要求书中所使用的单数形式的“一种”、“所述”和“该”也旨在包括多数形式，除非上下文清楚地表示其他含义。还应当理解，本文中使用的术语“和/或”是指并包含一个或多个相关联的列出项目的任何或所有可能组合。

[130] 应当理解，尽管在本说明书一个或多个实施例可能采用术语第一、第二、第三等来描述各种信息，但这些信息不应限于这些术语。这些术语仅用来将同一类型的信息彼此区分开。例如，在不脱离本说明书一个或多个实施例范围的情况下，第一信息也可以被称为第二信息，类似地，第二信息也可以被称为第一信息。取决于语境，如在此所使用的词语“如果”可以被解释成为“在……时”或“当……时”或“响应于确定”。

[131] 以上所述仅为本说明书一个或多个实施例的较佳实施例而已，并不用以限制本说明书一个或多个实施例，凡在本说明书一个或多个实施例的精神和原则之内，所做的任何修改、等同替换、改进等，均应包含在本说明书一个或多个实施例保护的范围之内。

权利要求书

1. 一种征信评估方法，应用于证明方，所述方法包括:

获取背书方提供的征信证明数据，所述征信证明数据对应的哈希值被所述背书方存证于区块链中;

通过信用评估函数对所述征信证明数据实施计算处理，得到待验证征信评估结果;

为所述待验证征信评估结果生成零知识证明信息;

将所述待验证征信评估结果和所述零知识证明信息发送至校验方；其中，当所述校验方根据所述零知识证明信息确定所述待验证征信评估结果由所述信用评估函数生成、生成所述待验证征信评估结果所采用的计算参数与所述征信证明数据对应的哈希值相匹配时，所述待验证征信评估结果被确认为可信。

2. 根据权利要求 1 所述的方法，

所述信用评估函数为默认函数，所述信用评估函数所采用的计算参数为默认参数;

或者，所述方法还包括: 根据所述校验方发送的指示信息，确定所采用的信用评估函数及其计算参数。

3. 根据权利要求 1 所述的方法，还包括:

获取所述背书方提供的所述哈希值对应的存证凭证;

将所述存证凭证发送至所述校验方，以使所述校验方根据所述存证凭证从区块链中查找到所述哈希值。

4. 根据权利要求 3 所述的方法，所述存证凭证包括以下至少之一: 所述哈希值、所述哈希值在区块链上的记录位置。

5. 根据权利要求 1 所述的方法，所述哈希值由所述背书方对所述征信证明数据和随机数进行哈希计算得到；所述方法还包括:

获取所述背书方提供的对应于所述哈希值的随机数;

验证所述征信证明数据、所述随机数和所述哈希值之间的对应关系。

6. 一种征信评估方法，应用于校验方，所述方法包括:

接收证明方提供的待验证征信评估结果和零知识证明信息;

根据所述零知识证明信息验证是否满足下述条件: 所述待验证征信评估结果由信用评估函数生成、生成所述待验证征信评估结果所采用的计算参数与背书方存证于区块链中的哈希值相匹配，其中所述哈希值对应于所述背书方记录的所述证明方的征信证明数据;

当所述零知识证明信息满足上述条件时，确认所述待验证征信评估结果可信。

7. 根据权利要求 6 所述的方法，

所述信用评估函数为默认函数，所述信用评估函数所采用的计算参数为默认参数；

或者，所述方法还包括：向所述证明方发送指示信息，以指示所述证明方所采用的信用评估函数及其计算参数。

8. 根据权利要求 6 所述的方法，还包括：

接收所述证明方提供的所述哈希值对应的存证凭证，所述存证凭证由所述背书方提供至所述证明方；

根据所述存证凭证从区块链中查找到所述哈希值。

9. 一种征信评估装置，应用于证明方，所述装置包括：

数据获取单元，获取背书方提供的征信证明数据，所述征信证明数据对应的哈希值被所述背书方存证于区块链中；

计算单元，通过信用评估函数对所述征信证明数据实施计算处理，得到待验证征信评估结果；

生成单元，为所述待验证征信评估结果生成零知识证明信息；

发送单元，将所述待验证征信评估结果和所述零知识证明信息发送至校验方；其中，当所述校验方根据所述零知识证明信息确定所述待验证征信评估结果由所述信用评估函数生成、生成所述待验证征信评估结果所采用的计算参数与所述征信证明数据对应的哈希值相匹配时，所述待验证征信评估结果被确认为可信。

10. 根据权利要求 9 所述的装置，

所述信用评估函数为默认函数，所述信用评估函数所采用的计算参数为默认参数；

或者，所述装置还包括：确定单元，根据所述校验方发送的指示信息，确定所采用的信用评估函数及其计算参数。

11. 根据权利要求 9 所述的装置，还包括：

凭证获取单元，获取所述背书方提供的所述哈希值对应的存证凭证；

凭证发送单元，将所述存证凭证发送至所述校验方，以使所述校验方根据所述存证凭证从区块链中查找到所述哈希值。

12. 根据权利要求 11 所述的装置，所述存证凭证包括以下至少之一：所述哈希值、所述哈希值在区块链上的记录位置。

13. 根据权利要求 9 所述的装置，所述哈希值由所述背书方对所述征信证明数据和随机数进行哈希计算得到；所述装置还包括：

随机数获取单元，获取所述背书方提供的对应于所述哈希值的随机数；

验证单元，验证所述征信证明数据、所述随机数和所述哈希值之间的对应关系。

14. 一种征信评估装置，应用于校验方，所述装置包括:

第一接收单元，接收证明方提供的待验证征信评估结果和零知识证明信息;

验证单元，根据所述零知识证明信息验证是否满足下述条件：所述待验证征信评估结果由信用评估函数生成、生成所述待验证征信评估结果所采用的计算参数与背书方存证于区块链中的哈希值相匹配，其中所述哈希值对应于所述背书方记录的所述证明方的征信证明数据;

确认单元，当所述零知识证明信息满足上述条件时，确认所述待验证征信评估结果可信。

15. 根据权利要求 14 所述的装置，

所述信用评估函数为默认函数，所述信用评估函数所采用的计算参数为默认参数;

或者，所述装置还包括：发送单元，向所述证明方发送指示信息，以指示所述证明方所采用的信用评估函数及其计算参数。

16. 根据权利要求 14 所述的装置，还包括:

第二接收单元，接收所述证明方提供的所述哈希值对应的存证凭证，所述存证凭证由所述背书方提供至所述证明方;

查找单元，根据所述存证凭证从区块链中查找到所述哈希值。

17. 一种电子设备，包括:

处理器;

用于存储处理器可执行指令的存储器;

其中，所述处理器通过运行所述可执行指令以实现如权利要求 1-5 中任一项所述的方法。

18. 一种电子设备，包括:

处理器;

用于存储处理器可执行指令的存储器;

其中，所述处理器通过运行所述可执行指令以实现如权利要求 6-8 中任一项所述的方法。

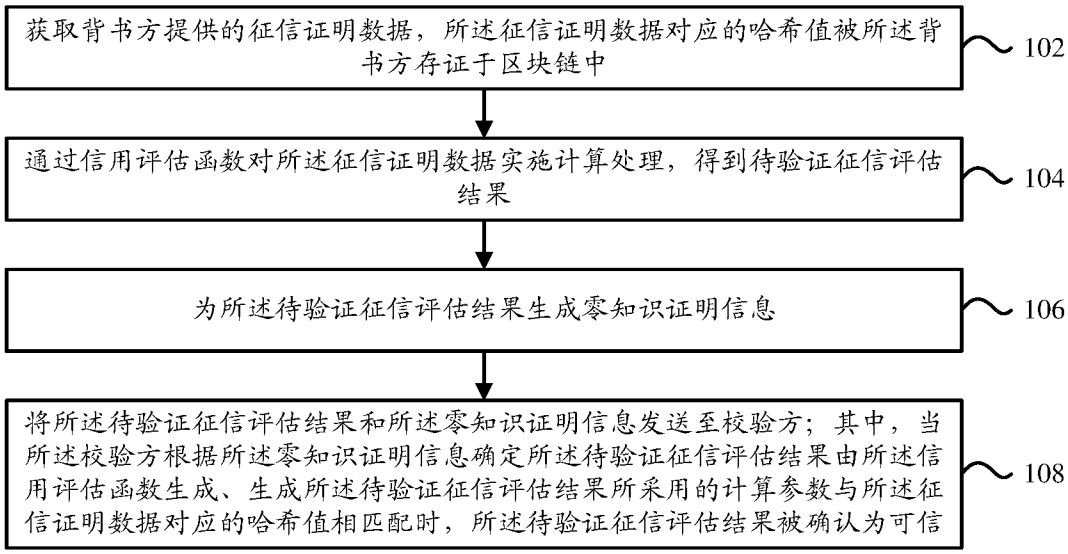
获取背书方提供的征信证明数据，所述征信证明数据对应的哈希值被所述背书方存证于区块链中
102
通过信用评估函数对所述征信证明数据实施计算处理，得到待验证征信评估结果
104
为所述待验证征信评估结果生成零知识证明信息
106
将所述待验证征信评估结果和所述零知识证明信息发送至校验方；其中，当所述校验方根据所述零知识证明信息确定所述待验证征信评估结果由所述信用评估函数生成、生成所述待验证征信评估结果所采用的计算参数与所述征信证明数据对应的哈希值相匹配时，所述待验证征信评估结果被确认为可信
108

图 1

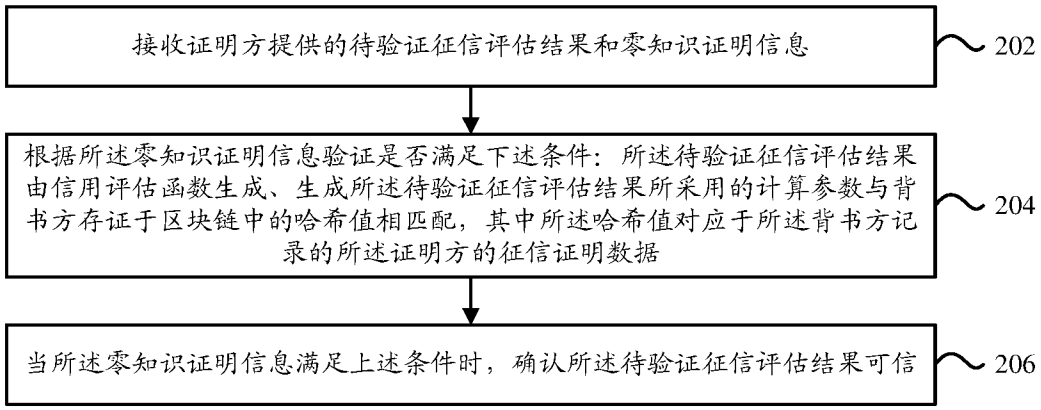
接收证明方提供的待验证征信评估结果和零知识证明信息
202
根据所述零知识证明信息验证是否满足下述条件：所述待验证征信评估结果由信用评估函数生成、生成所述待验证征信评估结果所采用的计算参数与背书方存证于区块链中的哈希值相匹配，其中所述哈希值对应于所述背书方记录的所述证明方的征信证明数据
204
当所述零知识证明信息满足上述条件时，确认所述待验证征信评估结果可信
206

图 2

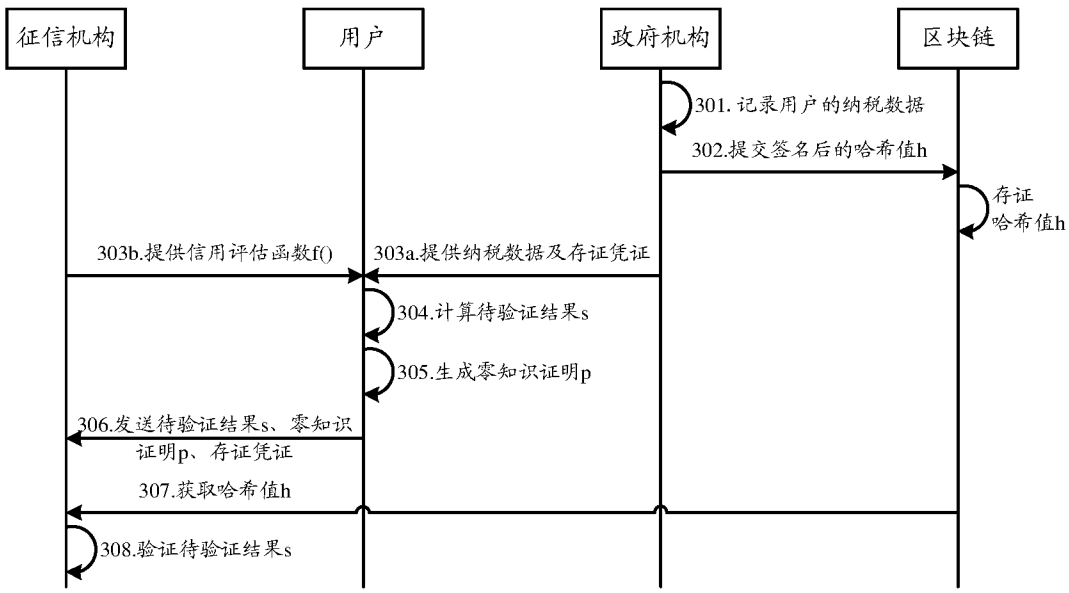
征信机构
用户
政府机构
区块链
301. 记录用户的纳税数据
302.提交签名后的哈希值h
存证
哈希值h
303b.提供信用评估函数f()
303a.提供纳税数据及存证凭证
304.计算待验证结果s
305.生成零知识证明p
306.发送待验证结果s、零知识证明p、存证凭证
307.获取哈希值h
308.验证待验证结果s

图 3

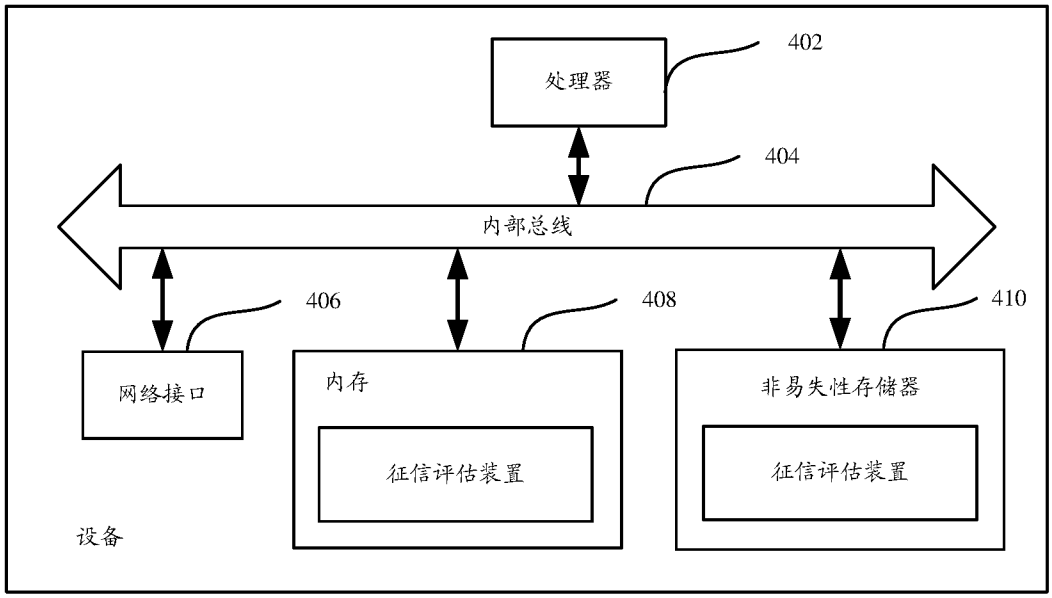
处理器
402
404
内部总线
406
408
410
网络接口
内存
征信评估装置
非易失性存储器
征信评估装置
设备

图 4

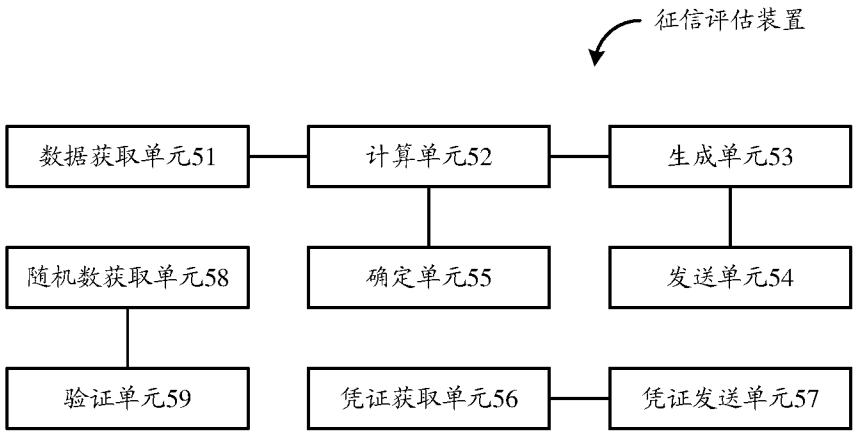
征信评估装置
数据获取单元51
计算单元52
生成单元53
随机数获取单元58
确定单元55
发送单元54
验证单元59
凭证获取单元56
凭证发送单元57

图 5

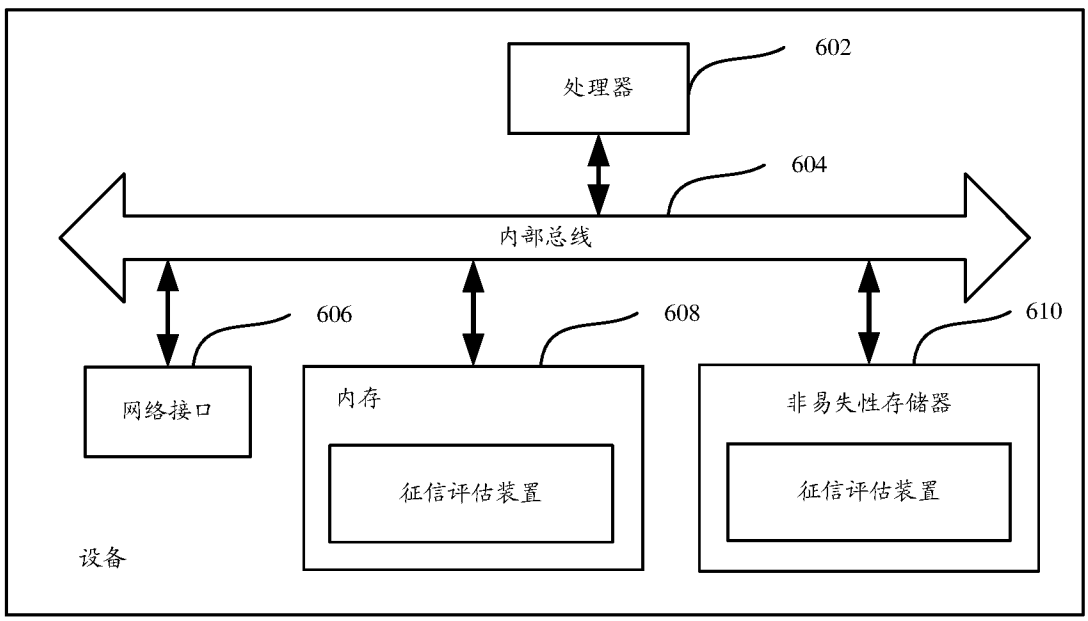
处理器
602
604
内部总线
606
608
610
网络接口
内存
征信评估装置
非易失性存储器
征信评估装置
设备

图 6

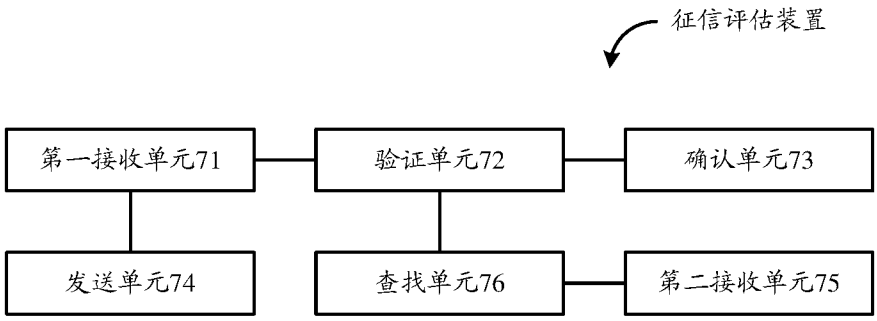

图 7

INTERNATIONAL SEARCH REPORT

International application No.
PCT/CN2019/103093

A. CLASSIFICATION OF SUBJECT MATTER

G06Q 40/04(2012.01)i; G06Q 50/26(2012.01)i

According to International Patent Classification (IPC) or to both national classification and IPC

B. FIELDS SEARCHED

Minimum documentation searched (classification system followed by classification symbols)

G06Q; G06F

Documentation searched other than minimum documentation to the extent that such documents are included in the fields searched

Electronic data base consulted during the international search (name of data base and, where practicable, search terms used)

CNPAT; CNKI; WPI; EPODOC; IEEE: 阿里巴巴, 崔嘉辉, 刘正, 殷山, 区块链, 零知识, 哈希, 证明, 验证, 征信, 信用, blockchain?, block, chain?, zero, knowledge, zero-knowledge, zkSNARK, zk-SNARK, hash, proof+, verif+, credit

C. DOCUMENTS CONSIDERED TO BE RELEVANT

Category*	Citation of document, with indication, where appropriate, of the relevant passages	Relevant to claim No.
PX	CN 109559224 A (ALIBABA GROUP HOLDING LIMITED) 02 April 2019 (2019-04-02) claims 1-18	1-18
Y	CN 108681583 A (BEIJING QIHOO TECHNOLOGY CO., LTD.) 19 October 2018 (2018-10-19) description, paragraphs 0035-0090	1-18
Y	CN 107274184 A (SHANGHAI DIANRONG INFORMATION TECHNOLOGY CO., LTD.) 20 October 2017 (2017-10-20) description, paragraphs 0027-0032	1-18
A	CN 108364218 A (BANK OF CHINA CO., LTD.) 03 August 2018 (2018-08-03) entire document	1-18
A	US 2018211332 A1 (INTERNATIONAL BUSINESS MACHINES CORPORATION) 26 July 2018 (2018-07-26) entire document	1-18

☐ Further documents are listed in the continuation of Box C. ☑ See patent family annex.

* Special categories of cited documents:
"A" document defining the general state of the art which is not considered to be of particular relevance
"D" document cited by the applicant in the international application
"E" earlier application or patent but published on or after the international filing date
"L" document which may throw doubts on priority claim(s) or which is cited to establish the publication date of another citation or other special reason (as specified)
"O" document referring to an oral disclosure, use, exhibition or other means
"P" document published prior to the international filing date but later than the priority date claimed
"T" later document published after the international filing date or priority date and not in conflict with the application but cited to understand the principle or theory underlying the invention
"X" document of particular relevance; the claimed invention cannot be considered novel or cannot be considered to involve an inventive step when the document is taken alone
"Y" document of particular relevance; the claimed invention cannot be considered to involve an inventive step when the document is combined with one or more other such documents, such combination being obvious to a person skilled in the art
"&" document member of the same patent family

Date of the actual completion of the international search	Date of mailing of the international search report
30 October 2019	**27 November 2019**

Name and mailing address of the ISA/CN	Authorized officer
China National Intellectual Property Administration (ISA/CN) **No. 6, Xitucheng Road, Jimenqiao Haidian District, Beijing 100088** **China**	
Facsimile No. **(86-10)62019451**	Telephone No.

INTERNATIONAL SEARCH REPORT
Information on patent family members

International application No.
PCT/CN2019/103093

Patent document cited in search report	Publication date (day/month/year)	Patent family member(s)	Publication date (day/month/year)
CN 109559224 A	02 April 2019	None	
CN 108681583 A	19 October 2018	None	
CN 107274184 A	20 October 2017	WO 2018205729 A1	15 November 2018
CN 108364218 A	03 August 2018	None	
US 2018211332 A1	26 July 2018	None	

国际检索报告

国际申请号
PCT/CN2019/103093

A. 主题的分类

G06Q 40/04(2012.01)i; G06Q 50/26(2012.01)i

按照国际专利分类(IPC)或者同时按照国家分类和IPC两种分类

B. 检索领域

检索的最低限度文献(标明分类系统和分类号)

G06Q; G06F

包含在检索领域中的除最低限度文献以外的检索文献

在国际检索时查阅的电子数据库(数据库的名称，和使用的检索词（如使用））

CNPAT;CNKI;WPI;EPODOC;IEEE：阿里巴巴，崔嘉辉，刘正，殷山，区块链，零知识，哈希，证明，验证，征信，信用，blockchain?，block，chain?，zero，knowledge，zero-knowledge，zkSNARK，zk-SNARK，hash，proof+，verif+，credit

C. 相关文件

类 型*	引用文件，必要时，指明相关段落	相关的权利要求
PX	CN 109559224 A (阿里巴巴集团控股有限公司) 2019年 4月 2日 (2019-04-02) 权利要求1-18	1-18
Y	CN 108681583 A (北京奇虎科技有限公司) 2018年 10月 19日 (2018-10-19) 说明书第0035-0090段	1-18
Y	CN 107274184 A (上海点融信息科技有限责任公司) 2017年 10月 20日 (2017-10-20) 说明书第0027-0032段	1-18
A	CN 108364218 A (中国银行股份有限公司) 2018年 8月 3日 (2018-08-03) 全文	1-18
A	US 2018211332 A1 (INTERNATIONAL BUSINESS MACHINES CORPORATION) 2018年 7月 26日 (2018-07-26) 全文	1-18

☐ 其余文件在C栏的续页中列出。

☑ 见同族专利附件。

* 引用文件的具体类型：

“A” 认为不特别相关的表示了现有技术一般状态的文件

“E” 在国际申请日的当天或之后公布的在先申请或专利

“L” 可能对优先权要求构成怀疑的文件，或为确定另一篇引用文件的公布日而引用的或者因其他特殊理由而引用的文件（如具体说明的）

“O” 涉及口头公开、使用、展览或其他方式公开的文件

“P” 公布日先于国际申请日但迟于所要求的优先权日的文件

“T” 在申请日或优先权日之后公布，与申请不相抵触，但为了理解发明之理论或原理的在后文件

“X” 特别相关的文件，单独考虑该文件，认定要求保护的发明不是新颖的或不具有创造性

“Y” 特别相关的文件，当该文件与另一篇或者多篇该类文件结合并且这种结合对于本领域技术人员为显而易见时，要求保护的发明不具有创造性

“&” 同族专利的文件

国际检索实际完成的日期	国际检索报告邮寄日期
2019年 10月 30日	2019年 11月 27日
ISA/CN的名称和邮寄地址 中国国家知识产权局(ISA/CN) 中国北京市海淀区蓟门桥西土城路6号 100088 传真号 (86-10)62019451	受权官员 王兴 电话号码 86-(10)-53961701

国际检索报告
关于同族专利的信息

国际申请号
PCT/CN2019/103093

检索报告引用的专利文件	公布日 (年/月/日)	同族专利	公布日 (年/月/日)
CN 109559224 A	2019年 4月 2日	无	
CN 108681583 A	2018年 10月 19日	无	
CN 107274184 A	2017年 10月 20日	WO 2018205729 A1	2018年 11月 15日
CN 108364218 A	2018年 8月 3日	无	
US 2018211332 A1	2018年 7月 26日	无	