



(12)发明专利申请

(10)申请公布号 CN 108985760 A

(43)申请公布日 2018.12.11

(21)申请号 201810621647.4

(22)申请日 2018.06.15

(71)申请人 杭州复杂美科技有限公司

地址 310000 浙江省杭州市西湖区文三路
90号东部软件园6号楼6层

(72)发明人 吴思进 王志文

(51)Int.Cl.

G06Q 20/38(2012.01)

G06Q 20/06(2012.01)

G06Q 20/40(2012.01)

G06Q 40/04(2012.01)

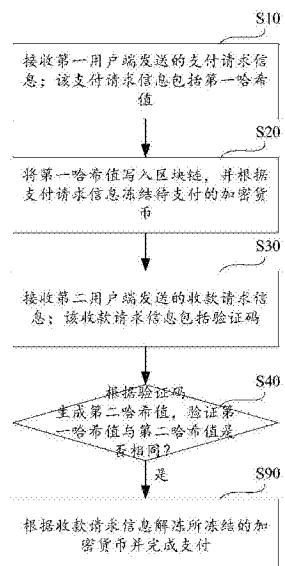
权利要求书2页 说明书8页 附图9页

(54)发明名称

支付方法及系统、设备和存储介质

(57)摘要

本发明提供一种支付方法及系统、设备和存储介质，该方法包括：接收第一用户端发送的支付请求信息；该支付请求信息包括第一哈希值；将第一哈希值写入区块链，并根据支付请求信息冻结待支付的加密货币；接收第二用户端发送的收款请求信息；该收款请求信息包括验证码；根据该验证码生成第二哈希值，验证第一哈希值与第二哈希值是否相同；是，则根据收款请求信息解冻所冻结的加密货币并完成支付。本发明通过将由付款方提交的第一哈希值写入区块链，再根据收款方提交的（由付款方告知的）验证码进行验证，并在验证通过时完成支付，从而保证了只有在收款方通过验证的情况下才进行支付，避免了用户因误转账等问题而承受损失。



1.一种支付方法,其特征在于,包括:

接收第一用户端发送的支付请求信息;所述支付请求信息包括第一哈希值;

将所述第一哈希值写入区块链,并根据所述支付请求信息冻结待支付的加密货币;

接收第二用户端发送的收款请求信息;所述收款请求信息包括验证码;

根据所述验证码生成第二哈希值,验证所述第一哈希值与所述第二哈希值是否相同:是,则根据所述收款请求信息解冻所冻结的加密货币并完成支付。

2.根据权利要求1所述的方法,其特征在于,还包括:

获取记录在区块链上的第三哈希值,根据所述验证码验证所述第三哈希值;

其中,所述第三哈希值由所述第二用户端通过约定的加密方式对所述验证码处理生成并写入区块链。

3.根据权利要求2所述的方法,其特征在于,还包括:

在接收到多项收款请求信息,且存在至少两项收款请求信息通过所有验证时,将其中最早写入区块链的若干第三哈希值所对应的用户确定为收款方。

4.根据权利要求1所述的方法,其特征在于,所述支付请求信息还包括第四哈希值,所述收款请求信息还包括第一地址;

所述方法还包括:

验证所述第一地址的哈希值和所述第四哈希值是否相同:否,则停止进行支付。

5.根据权利要求1所述的方法,其特征在于,所述收款请求信息还包括第一地址;

所述根据所述验证码生成第二哈希值包括:根据所述验证码和所述第一地址生成第二哈希值。

6.根据权利要求1-5任一项所述的方法,其特征在于,所述根据所述收款请求信息解冻所冻结的加密货币并完成支付包括:

在度过预定或动态配置的区块高度时长的冻结期后,根据所述收款请求信息解冻所冻结的加密货币并完成支付。

7.根据权利要求6所述的方法,其特征在于,还包括:

在所述冻结期内接收所述第一用户端发送的撤销支付请求信息;

根据所述撤销支付请求信息解冻所冻结的加密货币,并停止支付。

8.根据权利要求6所述的方法,其特征在于,还包括:

在所述冻结期内接收所述第一用户端发送的确认支付信息;

根据所述确认支付信息解冻所冻结的加密货币并完成支付。

9.一种支付系统,其特征在于,包括:

通信单元,配置用于接收第一用户端发送的支付请求信息,以及,接收第二用户端发送的收款请求信息;所述支付请求信息包括第一哈希值,所述收款请求信息包括验证码;

冻结单元,配置用于将所述第一哈希值写入区块链,并根据所述支付请求信息冻结待支付的加密货币;

第一验证单元,配置用于根据所述验证码生成第二哈希值,验证所述第一哈希值与所述第二哈希值是否相同;

支付单元,配置用于在所述验证结果为是时根据所述收款请求信息解冻所冻结的加密货币并完成支付。

10. 根据权利要求9所述的系统，其特征在于，还包括：

第二验证单元，配置用于获取记录在区块链上的第三哈希值，根据所述验证码验证所述第三哈希值；

其中，所述第三哈希值由所述第二用户端通过约定的加密方式对所述验证码处理生成并写入区块链。

11. 根据权利要求10所述的系统，其特征在于，所述支付单元进一步配置用于在所述通信单元接收到多项收款请求信息，且存在至少两项收款请求信息通过所有验证时，将其中最早写入区块链的若干第三哈希值所对应的用户确定为收款方。

12. 根据权利要求9所述的系统，其特征在于，所述支付请求信息还包括第四哈希值，所述收款请求信息还包括第一地址；

所述系统还包括：

第三验证单元，配置用于验证所述第一地址的哈希值和所述第四哈希值是否相同；

所述支付单元进一步配置用于在所述第三验证单元的验证结果为否时停止进行支付。

13. 根据权利要求9所述的系统，其特征在于，所述收款请求信息还包括第一地址；

所述第一验证单元进一步配置用于根据所述验证码和所述第一地址生成第二哈希值。

14. 根据权利要求9-13任一项所述的系统，其特征在于，所述冻结单元进一步配置用于在预定或动态配置的区块高度时长的冻结期内持续冻结所述加密货币；

所述支付单元进一步配置用于在度过所述冻结期后，根据所述收款请求信息解冻所冻结的加密货币并完成支付。

15. 根据权利要求14所述的系统，其特征在于，所述通信单元进一步配置用于在所述冻结期内接收所述第一用户端发送的撤销支付请求信息；

所述支付单元进一步配置用于根据所述撤销支付请求信息解冻所冻结的加密货币，并停止支付。

16. 根据权利要求14所述的系统，其特征在于，所述通信单元进一步配置用于在所述冻结期内接收所述第一用户端发送的确认支付信息；

所述支付单元进一步配置用于根据所述确认支付信息解冻所冻结的加密货币并完成支付。

17. 一种设备，其特征在于，所述设备包括：

一个或多个处理器；

存储器，用于存储一个或多个程序，

当所述一个或多个程序被所述一个或多个处理器执行时，使得所述一个或多个处理器执行如权利要求1-8中任一项所述的方法。

18. 一种存储有计算机程序的存储介质，其特征在于，该程序被处理器执行时实现如权利要求1-8中任一项所述的方法。

支付方法及系统、设备和存储介质

技术领域

[0001] 本申请涉及互联网金融技术领域，具体涉及一种支付方法及系统、设备和存储介质。

背景技术

[0002] 在现有的法币支付解决方案中，针对转账转错对象一类的问题，通常采用延迟到账的方式来解决问题，以供用户在到账前进行申诉或报警等操作，依仗于中心化的系统来进行撤销转账或冻结误转账对象账户等操作。

[0003] 然而在去中心化的区块链系统中，同样存在误转账的问题，例如，用户A要给用户B的地址转一笔加密货币，但可能不小心误转到了用户C的地址，此时，由于不存在中心化的系统，用户A无法通过申诉或报警等方式追回这笔加密货币，上述解决方案不适用于在去中心化的区块链系统中解决加密货币误转账一类的问题。

发明内容

[0004] 鉴于现有技术中的上述缺陷或不足，期望提供一种在去中心化系统中避免用户因误转账而造成损失的支付方法及系统、设备和存储介质。

[0005] 第一方面，本发明提供一种支付方法，包括：

[0006] 接收第一用户端发送的支付请求信息；该支付请求信息包括第一哈希值；

[0007] 将第一哈希值写入区块链，并根据支付请求信息冻结待支付的加密货币；

[0008] 接收第二用户端发送的收款请求信息；该收款请求信息包括验证码；

[0009] 根据该验证码生成第二哈希值，验证第一哈希值与第二哈希值是否相同：是，则根据收款请求信息解冻所冻结的加密货币并完成支付。

[0010] 第二方面，本发明提供一种支付系统，包括通信单元、冻结单元、第一验证单元和支付单元。

[0011] 通信单元配置用于接收第一用户端发送的支付请求信息，以及，接收第二用户端发送的收款请求信息；支付请求信息包括第一哈希值，收款请求信息包括验证码；

[0012] 冻结单元配置用于将第一哈希值写入区块链，并根据支付请求信息冻结待支付的加密货币；

[0013] 第一验证单元配置用于根据验证码生成第二哈希值，验证第一哈希值与第二哈希值是否相同；

[0014] 支付单元配置用于在验证结果为是时根据收款请求信息解冻所冻结的加密货币并完成支付。

[0015] 第三方面，本发明还提供一种设备，包括一个或多个处理器和存储器，其中存储器包含可由该一个或多个处理器执行的指令以使得该一个或多个处理器执行根据本发明各实施例提供的支付方法。

[0016] 第四方面，本发明还提供一种存储有计算机程序的存储介质，该计算机程序使计

算机执行根据本发明各实施例提供的支付方法。

[0017] 本发明诸多实施例提供的支付方法及系统、设备和存储介质通过将由付款方提交的第一哈希值写入区块链，再根据收款方提交的（由付款方告知的）验证码进行验证，并在验证通过时完成支付，从而保证了只有在收款方通过验证的情况下才进行支付，避免了用户因误转账等问题而承受损失；

[0018] 本发明一些实施例提供的支付方法及系统、设备和存储介质进一步通过同时根据验证码和地址进行验证，使得第三方在盗取验证码时仍无法完成支付，而只有付款方指定的收款方可以根据验证码完成支付；

[0019] 本发明一些实施例提供的支付方法及系统、设备和存储介质进一步通过由收款方在提交收款请求前在区块链上记录可验证的加密证明，以证明持有验证码的时间，并将所有通过验证的收款请求者中持有验证码最早的确定为收款方，使不法分子无法通过截取验证码抢先骗取支付的款项；

[0020] 本发明一些实施例提供的支付方法及系统、设备和存储介质进一步通过配置一定区块高度时长的冻结期，使得付款方在发生误转账时可以及时撤销支付请求；

[0021] 本发明一些实施例提供的支付方法及系统、设备和存储介质进一步通过在上述冻结期中根据付款方的确认信息提前完成支付，避免了收款方在每笔交易中的长时间等待，进一步优化了用户体验。

附图说明

[0022] 通过阅读参照以下附图所作的对非限制性实施例所作的详细描述，本申请的其它特征、目的和优点将会变得更明显：

[0023] 图1为本发明一实施例提供的一种支付方法的流程图。

[0024] 图2为图1所示方法的一种优选实施方式的流程图。

[0025] 图3为图1所示方法的一种优选实施方式的流程图。

[0026] 图4为图3所示方法的一种优选实施方式的流程图。

[0027] 图5为图1所示方法的一种优选实施方式的流程图。

[0028] 图6为图5所示方法的一种优选实施方式的流程图。

[0029] 图7为图5所示方法的一种优选实施方式的流程图。

[0030] 图8为本发明一实施例提供的一种支付系统的结构示意图。

[0031] 图9为图8所示系统的一种优选实施方式的结构示意图。

[0032] 图10为图8所示系统的一种优选实施方式的结构示意图。

[0033] 图11为本发明一实施例提供的一种设备的结构示意图。

具体实施方式

[0034] 下面结合附图和实施例对本申请作进一步的详细说明。可以理解的是，此处所描述的具体实施例仅仅用于解释相关发明，而非对该发明的限定。另外还需要说明的是，为了便于描述，附图中仅示出了与发明相关的部分。

[0035] 需要说明的是，在不冲突的情况下，本申请中的实施例及实施例中的特征可以相互组合。下面将参考附图并结合实施例来详细说明本申请。

[0036] 图1为本发明一实施例提供的一种支付方法的流程图。

[0037] 如图1所示,在本实施例中,本发明提供一种支付方法,包括:

[0038] S10:接收第一用户端发送的支付请求信息;该支付请求信息包括第一哈希值;

[0039] S20:将第一哈希值写入区块链,并根据支付请求信息冻结待支付的加密货币;

[0040] S30:接收第二用户端发送的收款请求信息;该收款请求信息包括验证码;

[0041] S40:根据该验证码生成第二哈希值,验证第一哈希值与第二哈希值是否相同:

[0042] 是,则执行步骤S90:根据收款请求信息解冻所冻结的加密货币并完成支付。

[0043] 具体地,在本实施例中,以智能合约的方式在区块链系统中实现上述方法,在更多实施例中,还可以以其它本领域常用的区块链技术实现上述方法,可实现相同的技术效果。

[0044] 以下将以用户甲向乙进行加密货币转账为例对上述方法进行详细阐述,在更多实施例中,本发明提供的解决方案还可以应用于发红包、付款等不同支付场景,可实现相同的技术效果。

[0045] 当用户甲要向用户乙转账一笔加密货币时,用户甲的第一用户端生成一项验证码r,并根据该验证码r生成第一哈希值H₁,再生成包括该第一哈希值H₁的支付请求信息。

[0046] 其中,在本实施例中,该验证码r具体配置为一随机数,第一哈希值H₁的生成方式为生成该随机数r的哈希值:H₁=hash(r),支付请求信息还包括私钥签名信息、用户甲的地址、支付的数额信息等信息,并可以进一步包括用户乙的地址等信息。在更多实施例中,还可以将验证码配置为非随机数,为第一哈希值配置基于该随机数的不同生成方式,将支付请求信息配置为包括本领域技术人员可以理解的不同信息,可实现相同或相似的技术效果。

[0047] 在步骤S20中,将该第一哈希值H₁写入区块链,并根据支付请求信息在用户甲的地址上冻结待支付的加密货币。

[0048] 当用户甲通过即时通讯软件、邮件、短信、口头告知等任意一种非公开的方式将上述验证码告知用户乙之后,用户乙的第二用户端根据该验证码生成收款请求信息并提交。

[0049] 在步骤S40中,根据步骤S30所接收的收款请求信息中的验证码生成第二哈希值H₂,并验证H₁和H₂是否相同:

[0050] 若不相同,则说明该收款请求信息的提交者并非用户甲指定的收款方,继续等待真实的收款方提交收款请求信息,或,在超过预定时长后撤销该笔转账;

[0051] 若相同,则验证通过,执行步骤S90,解冻所冻结的加密货币并转到用户乙的地址上,完成支付。

[0052] 对于转账、支付、一对一发红包等应用场景,上述方法还可以进一步增加对支付对象地址的验证,以下将进行具体介绍;而对于抢红包等应用场景,由于支付对象是不确定的,因此无法增加对支付对象地址的验证。

[0053] 上述实施例通过将由付款方提交的第一哈希值写入区块链,再根据收款方提交的(由付款方告知的)验证码进行验证,并在验证通过时完成支付,从而保证了只有在收款方通过验证的情况下才进行支付,避免了用户因误转账等问题而承受损失。

[0054] 在一优选实施例中,作为转账对象的用户乙的第二用户端提前通过即时通讯软件、邮件、短信、口头告知等任意一种非公开的方式将第一地址add₁告知用户甲的第一客户端,第一哈希值的生成方式为H₁=hash(r+add₁);

- [0055] 步骤S30所接收的收款请求信息还包括该第一地址add₁；
- [0056] 在步骤S40中，根据验证码r和第一地址add₁生成第二哈希值H₂=hash (r+add₁)，并验证H₁和H₂是否相同。
- [0057] 该优选实施例进一步保障了，即便第三方丙通过非法手段盗取了验证码r，根据丙所提交的验证码r和第二地址add₂也无法通过上述验证；如果丙试图用验证码r和用户乙的第一地址add₁通过验证，则步骤S90中也只会将加密货币支付到用户乙的第一地址add₁上。
- [0058] 图2为图1所示方法的一种优选实施方式的流程图。如图2所示，在另一优选实施例中，支付请求信息还包括第四哈希值，收款请求信息还包括第一地址，上述方法还包括：
- [0059] S41：验证第一地址的哈希值和第四哈希值是否相同；否，则停止进行支付。
- [0060] 具体地，与上述优选实施例相似地，作为转账对象的用户乙的第二用户端提前通过即时通讯软件、邮件、短信、口头告知等任意一种非公开的方式将第一地址add₁告知用户甲的第一客户端，步骤S10所接收的支付请求信息还包括根据该第一地址add₁生成的第四哈希值H₄=hash (add₁)；
- [0061] 步骤S30所接收的收款请求信息还包括该第一地址add₁；
- [0062] 在步骤S41中，根据第一地址add₁生成第五哈希值H₅=hash (add₁)，并验证H₄和H₅是否相同；只有在步骤S40和S41的验证同时通过时，才进行步骤S90的支付，若其中一项验证未通过，则不进行支付。
- [0063] 图2所示的方法同样保障了第三方在盗取验证码时无法通过验证骗取支付。
- [0064] 上述优选实施例进一步通过同时根据验证码和地址进行验证，使得第三方在盗取验证码时仍无法完成支付，而只有付款方指定的收款方可以根据验证码完成支付。
- [0065] 图3为图1所示方法的一种优选实施方式的流程图。如图3所示，在一优选实施例中，上述方法还包括：
- [0066] S50：获取记录在区块链上的第三哈希值，根据验证码验证第三哈希值。
- [0067] 其中，第三哈希值由第二用户端通过约定的加密方式对验证码处理生成并写入区块链。
- [0068] 具体地，在上述图1-2所示的方法中，对于作为收款方的用户乙，还存在提交收款请求信息时，被他人非法获取并抢先提交收款请求信息的风险。针对该问题，在图3所示的方法中，用户乙的第二用户端先以智能合约所约定的加密方式对验证码进行加密处理，生成第三哈希值，例如H₃=hash (r+1)，或，H₃=hash (r+add)，等，并将第三哈希值H₃写入区块链。此处应当说明的是，该约定的加密方式应与第一用户端公开的用于供验证的任一哈希值的加密方式不同，例如，当第一用户端公开了H₂=hash (r+add₁)，则不能再将第三哈希值的加密方式约定为H₃=hash (r+add)，而应约定不同的加密方式。
- [0069] 当第二用户端提交收款请求信息后，根据该收款请求信息获取区块链中记录的第三哈希值H₃，根据约定的加密方式和验证码r验证第三哈希值H₃是否正确；若不正确，则未通过验证，停止支付；若正确，则可以证明用户乙在将第三哈希值H₃写入区块链时已持有验证码r。
- [0070] 图4为图3所示方法的一种优选实施方式的流程图。如图4所示，进一步优选地，上述方法还包括：
- [0071] S51：在接收到多项收款请求信息，且存在至少两项收款请求信息通过所有验证

时,将其中最早写入区块链的若干第三哈希值所对应的用户确定为收款方。

[0072] 具体地,根据上述图3所示方法的分析可知,当第三哈希值H₃通过验证时,第三哈希值H₃写入区块链的时间即可被视为对应用户持有验证码的时间证明。

[0073] 假设用户丙在用户乙的第二用户端上传收款请求信息时截取验证码r,同样生成哈希值H₃'并写入区块链,并抢先提交收款请求信息,则H₃'写入区块链的时间必然晚于H₃写入区块链的时间,步骤S51仍会将用户乙确定为收款方,用户丙无法窃取该笔加密货币。

[0074] 其中,当图4所示方法应用于转账或支付等场景时,将写入区块链时间最早的一项第三哈希值所对应的用户确定为收款方;而当图4所示方法应用于抢红包等场景时,根据付款方指定的收款方数量,例如红包个数,将写入区块链时间最早的多项第三哈希值所对应的用户确定为收款方。

[0075] 上述实施例进一步通过由收款方在提交收款请求前在区块链上记录可验证的加密证明,以证明持有验证码的时间,并将所有通过验证的收款请求者中持有验证码最早的确定为收款方,使不法分子无法通过截取验证码抢先骗取支付的款项。

[0076] 图5为图1所示方法的一种优选实施方式的流程图。如图5所示在一优选实施例中,上述方法的步骤S90具体包括:

[0077] S91:在度过预定或动态配置的区块高度时长的冻结期后,根据收款请求信息解冻所冻结的加密货币并完成支付。

[0078] 具体地,在图5所示方法中,在通过所配置的所有验证后,在默认状态下仍需要等待度过冻结期,才执行支付操作。通过配置该冻结期,可以进一步在该冻结期中配置各种保障性策略,例如以下图6所示的方法中作为付款方的用户甲可以在冻结期撤回支付请求,又例如作为支付对象的用户乙也可以在冻结期撤回收款请求,等等。

[0079] 在本实施例中,冻结期的时长配置为预定或动态配置的区块高度时长,在更多实施例中,也可以根据不同的实际需求配置为固定时长等不同时长。

[0080] 图6为图5所示方法的一种优选实施方式的流程图。如图6所示,在一优选实施例中,上述方法还包括:

[0081] S60:在冻结期内接收第一用户端发送的撤销支付请求信息;

[0082] S70:根据撤销支付请求信息解冻所冻结的加密货币,并停止支付。

[0083] 具体地,在图6所示方法中,用户甲可以在冻结期内提交撤销支付请求,区块链网络的节点收到该请求后撤销支付请求,并解冻步骤S20所冻结的加密货币。

[0084] 上述优选实施例进一步通过配置一定区块高度时长的冻结期,使得付款方在发生误转账时可以及时撤销支付请求。

[0085] 图7为图5所示方法的一种优选实施方式的流程图。如图7所示,在一优选实施例中,上述方法还包括:

[0086] S80:在冻结期内接收第一用户端发送的确认支付信息;

[0087] S81:根据确认支付信息解冻所冻结的加密货币并完成支付。

[0088] 具体地,在为支付配置冻结期后,在每一笔支付中,收款方在通过验证后都需要等待度过冻结期才能收到支付的加密货币,导致用户体验不佳,通过付款方确认后进行提前解冻并完成支付可以解决这一问题,提升收款方的用户体验。

[0089] 上述优选实施例进一步通过在上述冻结期中根据付款方的确认信息提前完成支

付,避免了收款方在每笔交易中的长时间等待,进一步优化了用户体验。

[0090] 图8为本发明一实施例提供的一种支付系统的结构示意图。图8所示的系统可对应执行图1、5-7所示的任一方法。

[0091] 如图8所示,在本实施例中,本发明提供一种支付系统10,包括通信单元101、冻结单元102、第一验证单元103和支付单元104。

[0092] 通信单元101配置用于接收第一用户端20发送的支付请求信息,以及,接收第二用户端30发送的收款请求信息;支付请求信息包括第一哈希值,收款请求信息包括验证码;

[0093] 冻结单元102配置用于将第一哈希值写入区块链,并根据支付请求信息冻结待支付的加密货币;

[0094] 第一验证单元103配置用于根据验证码生成第二哈希值,验证第一哈希值与第二哈希值是否相同;

[0095] 支付单元104配置用于在验证结果为是时根据收款请求信息解冻所冻结的加密货币并完成支付。

[0096] 在本实施例中,上述支付系统10以智能合约的方式部署在区块链网络中的各节点上,在更多实施例中,还可以根据不同的实际需求将上述支付系统10以本领域技术人员可以理解的不同方式部署在区块链网络中,可实现相同的技术效果。

[0097] 在一优选实施例中,收款请求信息还包括第一地址;第一验证单元103进一步配置用于根据验证码和第一地址生成第二哈希值。

[0098] 在一优选实施例中,冻结单元102进一步配置用于在预定或动态配置的区块高度时长的冻结期内持续冻结待支付的加密货币;支付单元104进一步配置用于在度过冻结期后,根据收款请求信息解冻所冻结的加密货币并完成支付。

[0099] 在一优选实施例中,通信单元101进一步配置用于在冻结期内接收第一用户端20发送的撤销支付请求信息;支付单元104进一步配置用于根据撤销支付请求信息解冻所冻结的加密货币,并停止支付。

[0100] 在一优选实施例中,通信单元101进一步配置用于在冻结期内接收第一用户端发送的确认支付信息;

[0101] 支付单元104进一步配置用于根据确认支付信息解冻所冻结的加密货币并完成支付。

[0102] 上述各实施例提供的系统的支付原理可参照图1、3-5所示的任一方法,此处不再赘述。

[0103] 图9为图8所示系统的一种优选实施方式的结构示意图。图9所示的系统可对应执行图3-4所示的方法。

[0104] 如图9所示,在一优选实施例中,支付系统10还包括第二验证单元105,配置用于获取记录在区块链上的第三哈希值,根据验证码验证第三哈希值;

[0105] 其中,第三哈希值由第二用户端通过约定的加密方式对验证码处理生成并写入区块链。

[0106] 进一步优选地,支付单元104进一步配置用于在通信单元101接收到多项收款请求信息,且存在至少两项收款请求信息通过所有验证时,将其中最早写入区块链的若干第三哈希值所对应的用户确定为收款方。

- [0107] 图9所示的系统的支付原理可参照图3-4所示的方法,此处不再赘述。
- [0108] 图10为图8所示系统的一种优选实施方式的结构示意图。图10所示的系统可对应执行图2所示的方法。
- [0109] 如图10所示,在一优选实施例中,支付请求信息还包括第四哈希值,收款请求信息还包括第一地址;
- [0110] 支付系统10还包括第三验证单元106,配置用于验证第一地址的哈希值和第四哈希值是否相同;
- [0111] 支付单元104进一步配置用于在第三验证单元106的验证结果为否时停止进行支付。
- [0112] 图10所示的系统的支付原理可参照图2所示的方法,此处不再赘述。
- [0113] 图11为本发明一实施例提供的一种设备的结构示意图。
- [0114] 如图11所示,作为另一方面,本申请还提供了一种设备1100,包括一个或多个中央处理单元(CPU)1101,其可以根据存储在只读存储器(ROM)1102中的程序或者从存储部分1108加载到随机访问存储器(RAM)1103中的程序而执行各种适当的动作和处理。在RAM1103中,还存储有设备1100操作所需的各种程序和数据。CPU1101、ROM1102以及RAM1103通过总线1104彼此相连。输入/输出(I/O)接口1105也连接至总线1104。
- [0115] 以下部件连接至I/O接口1105:包括键盘、鼠标等的输入部分1106;包括诸如阴极射线管(CRT)、液晶显示器(LCD)等以及扬声器等的输出部分1107;包括硬盘等的存储部分1108;以及包括诸如LAN卡、调制解调器等的网络接口卡的通信部分1109。通信部分1109经由诸如因特网的网络执行通信处理。驱动器1110也根据需要连接至I/O接口1105。可拆卸介质1111,诸如磁盘、光盘、磁光盘、半导体存储器等等,根据需要安装在驱动器1110上,以便于从其上读出的计算机程序根据需要被安装入存储部分1108。
- [0116] 特别地,根据本公开的实施例,上述任一实施例描述的支付方法可以被实现为计算机软件程序。例如,本公开的实施例包括一种计算机程序产品,其包括有形地包含在机器可读介质上的计算机程序,所述计算机程序包含用于执行支付方法的程序代码。在这样的实施例中,该计算机程序可以通过通信部分1109从网络上被下载和安装,和/或从可拆卸介质1111被安装。
- [0117] 作为另一方面,本申请还提供了一种计算机可读存储介质,该计算机可读存储介质可以是上述实施例的装置中所包含的计算机可读存储介质;也可以是单独存在,未装配入设备中的计算机可读存储介质。计算机可读存储介质存储有一个或者一个以上程序,该程序被一个或者一个以上的处理器用来执行描述于本申请的支付方法。
- [0118] 附图中的流程图和框图,图示了按照本发明各种实施例的系统、方法和计算机程序产品的可能实现的体系架构、功能和操作。在这点上,流程图或框图中的每个方框可以代表一个模块、程序段、或代码的一部分,该模块、程序段、或代码的一部分包含一个或多个用于实现规定的逻辑功能的可执行指令。也应当注意,在有些作为替换的实现中,方框中所标注的功能也可以以不同于附图中所标注的顺序发生。例如,两个接连地表示的方框实际上可以基本并行地执行,它们有时也可以按相反的顺序执行,这根据所涉及的功能而定。也要注意的是,框图和/或流程图中的每个方框、以及框图和/或流程图中的方框的组合,可以通过执行规定的功能或操作的专用的基于硬件的系统来实现,或者可以通过专用硬件与计算

机指令的组合来实现。

[0119] 描述于本申请实施例中所涉及到的单元或模块可以通过软件的方式实现,也可以通过硬件的方式来实现。所描述的单元或模块也可以设置在处理器中,例如,各所述单元可以是设置在计算机或移动智能设备中的软件程序,也可以是单独配置的硬件装置。其中,这些单元或模块的名称在某种情况下并不构成对该单元或模块本身的限定。

[0120] 以上描述仅为本申请的较佳实施例以及对所运用技术原理的说明。本领域技术人员应当理解,本申请中所涉及的发明范围,并不限于上述技术特征的特定组合而成的技术方案,同时也应涵盖在不脱离本申请构思的情况下,由上述技术特征或其等同特征进行任意组合而形成的其它技术方案。例如上述特征与本申请中公开的(但不限于)具有类似功能的技术特征进行互相替换而形成的技术方案。

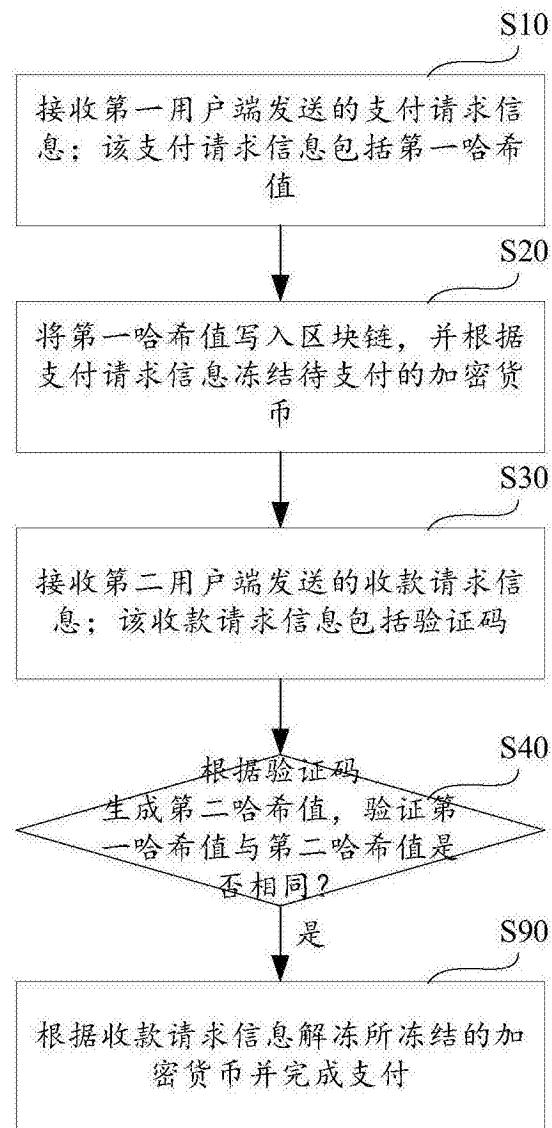


图1

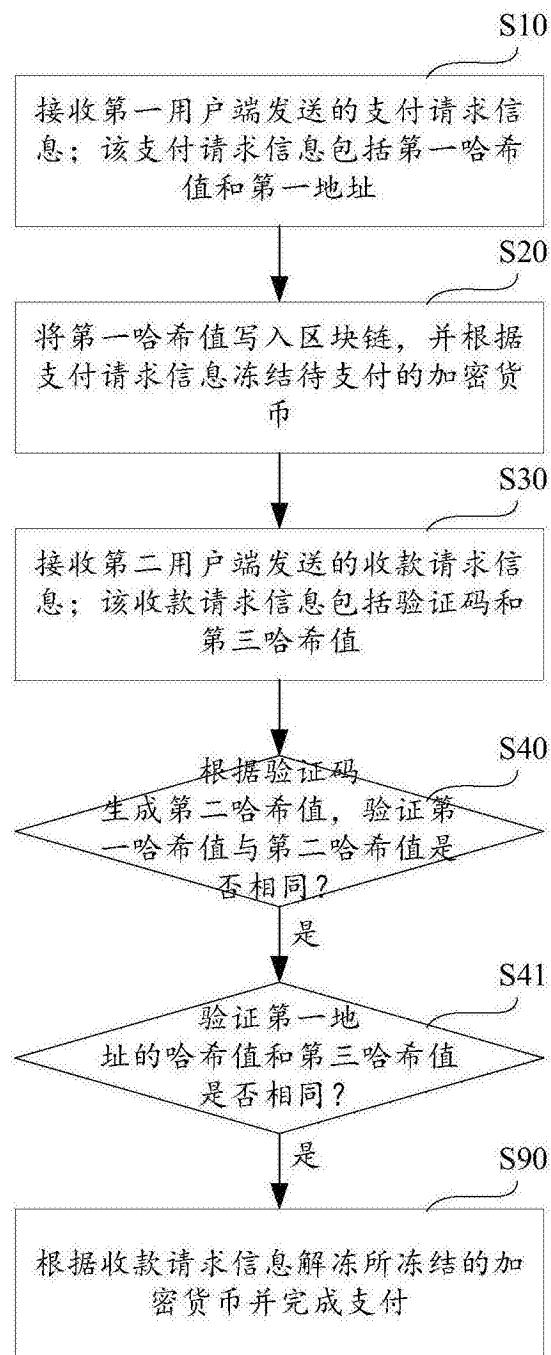


图2

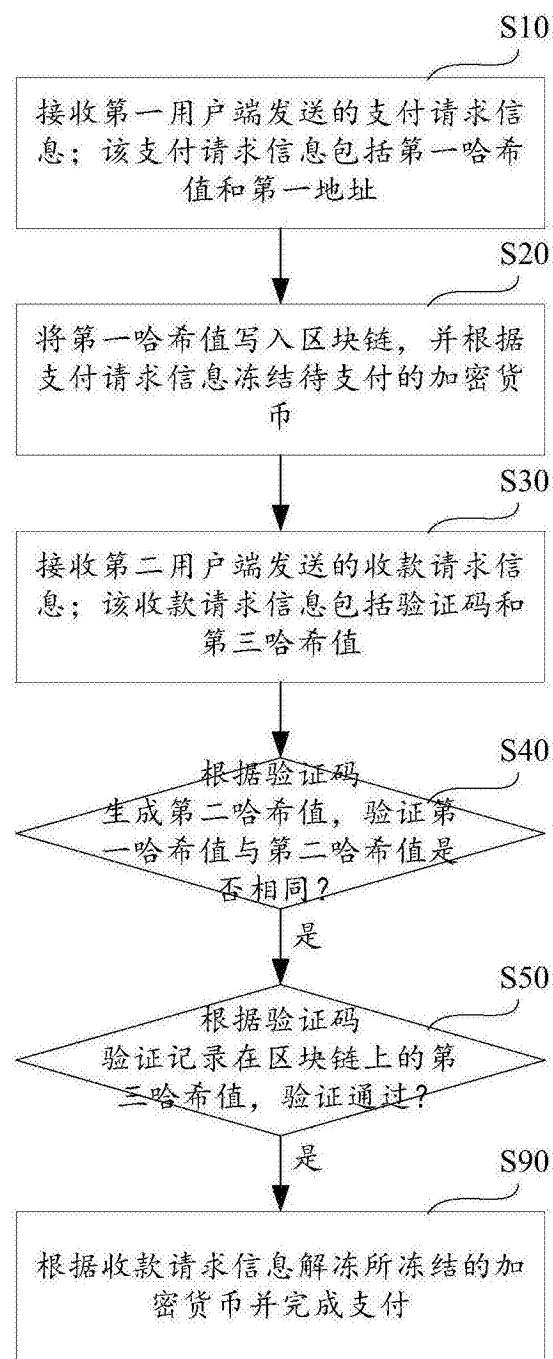


图3

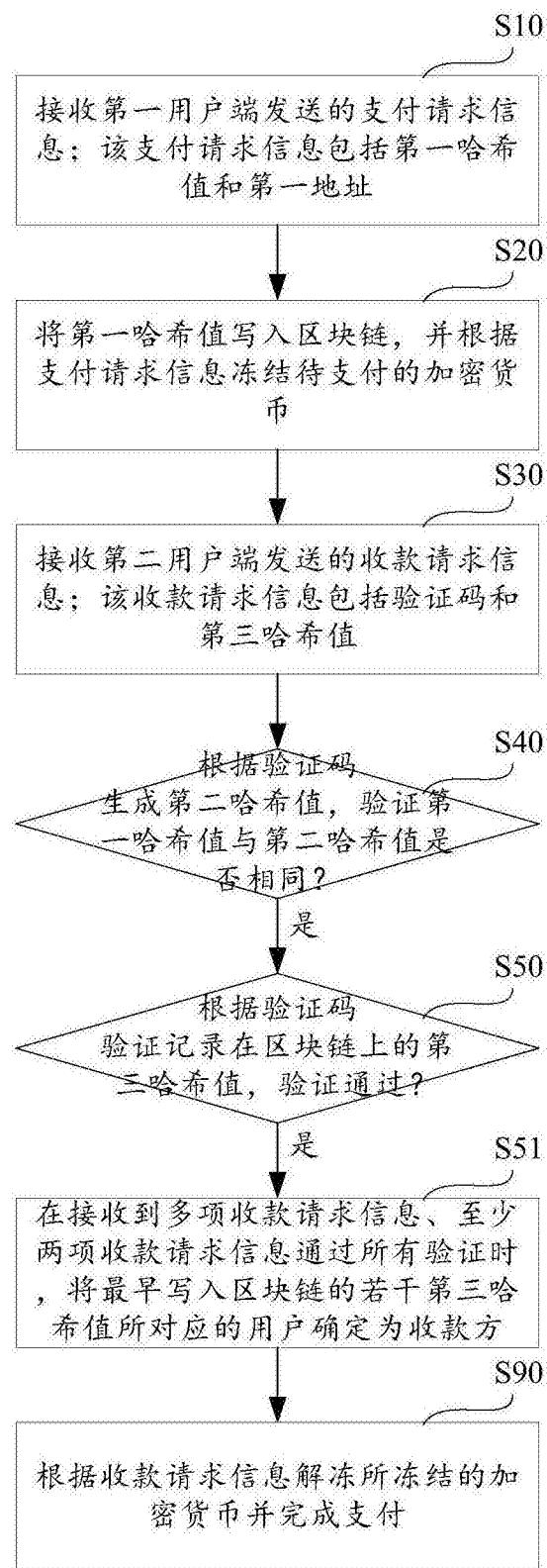


图4

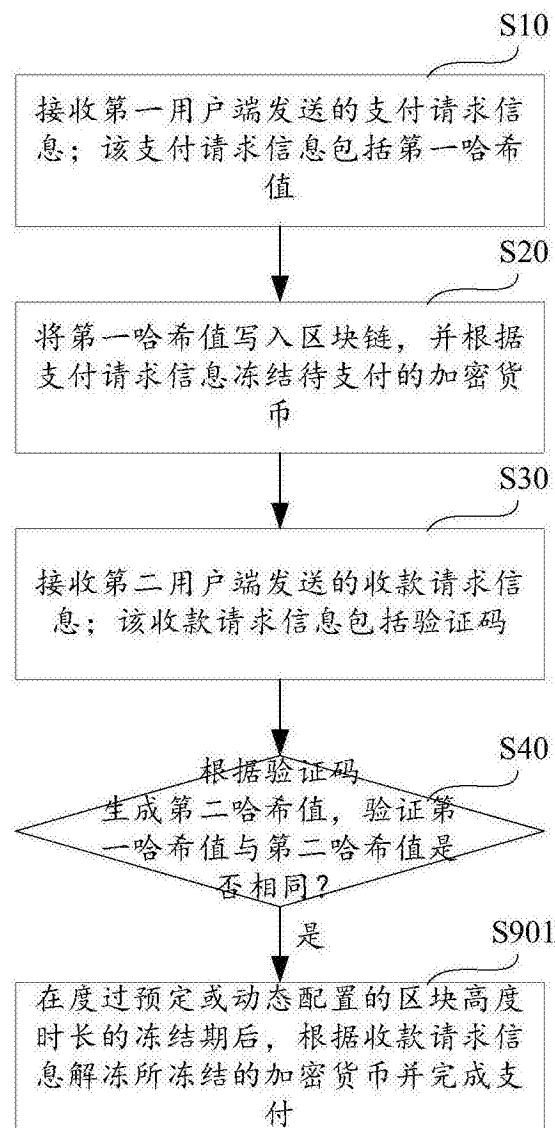


图5

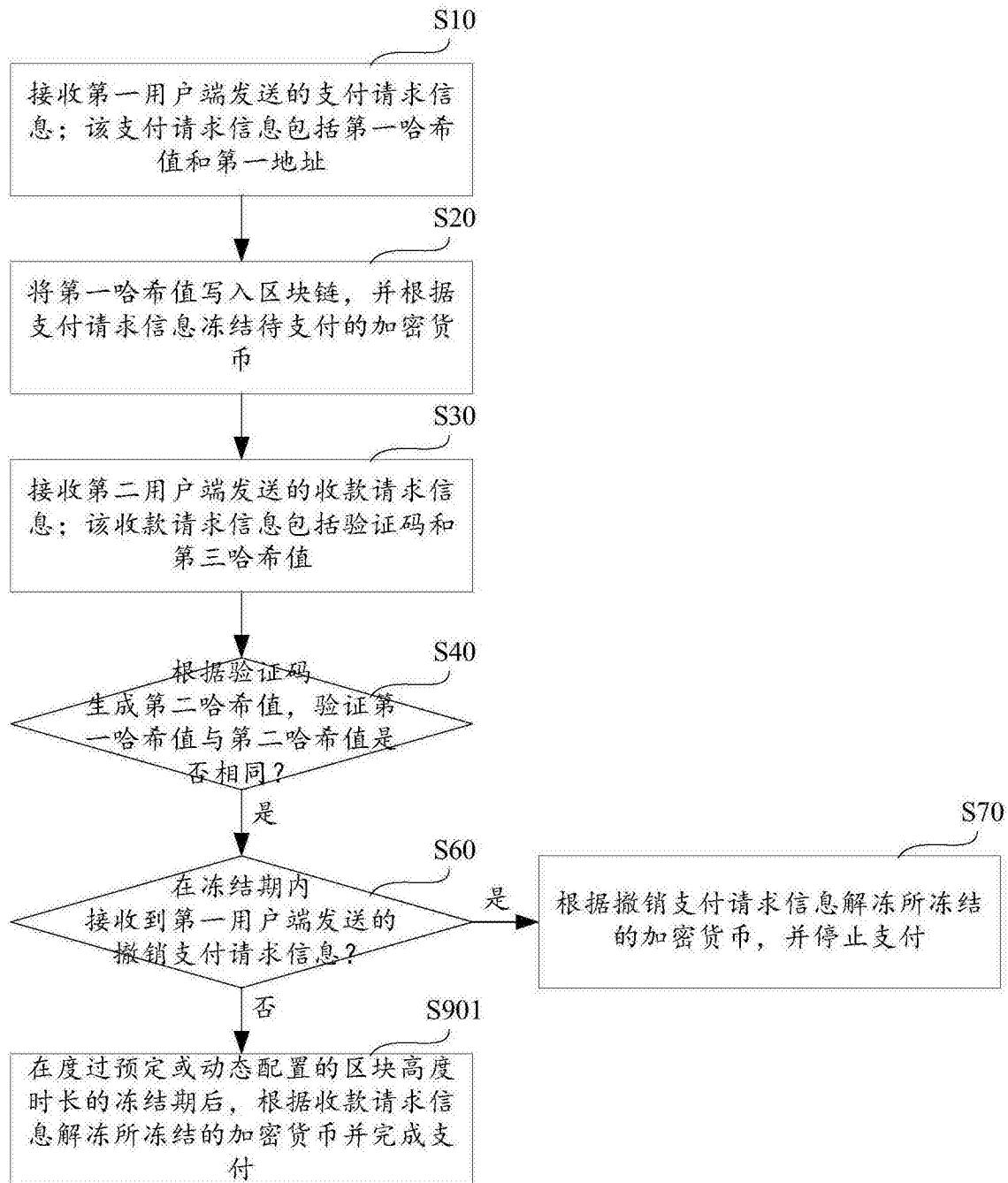


图6

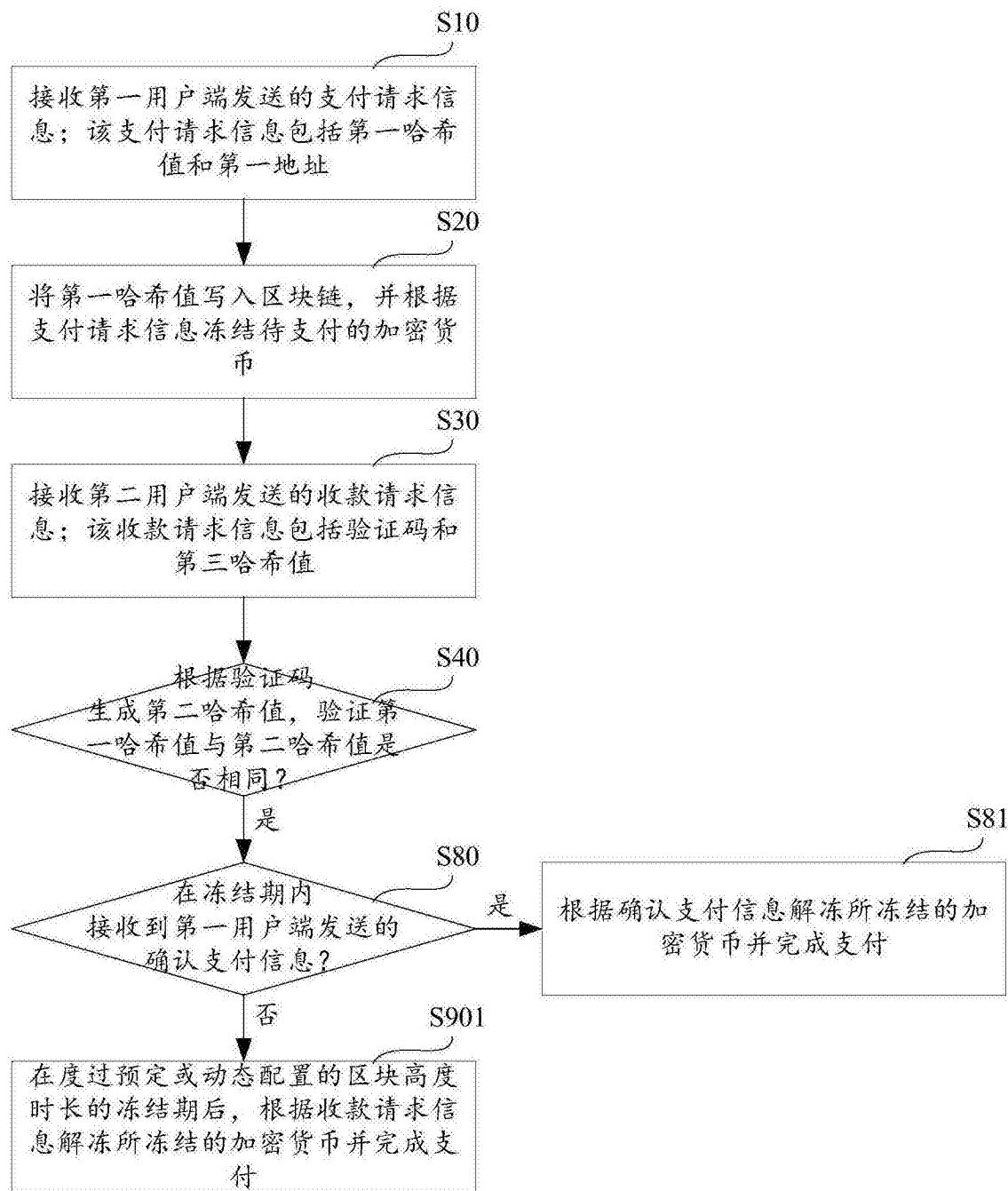


图7

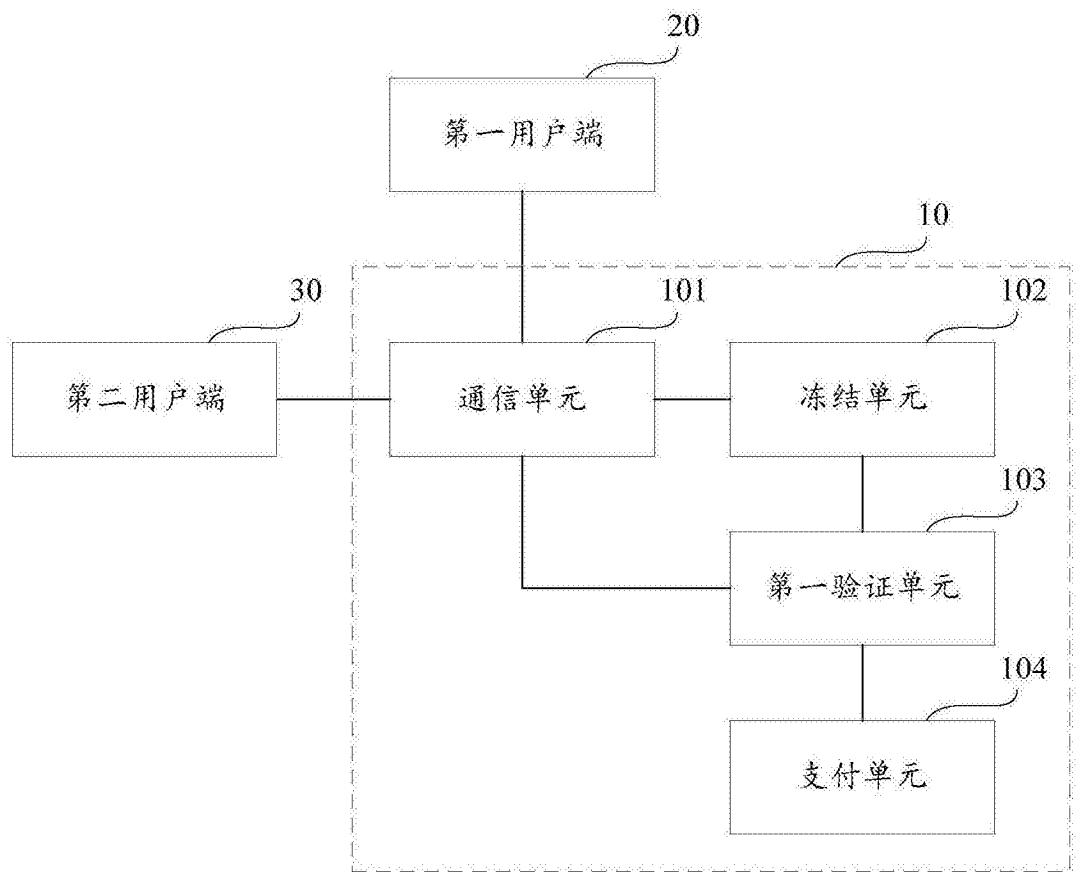


图8

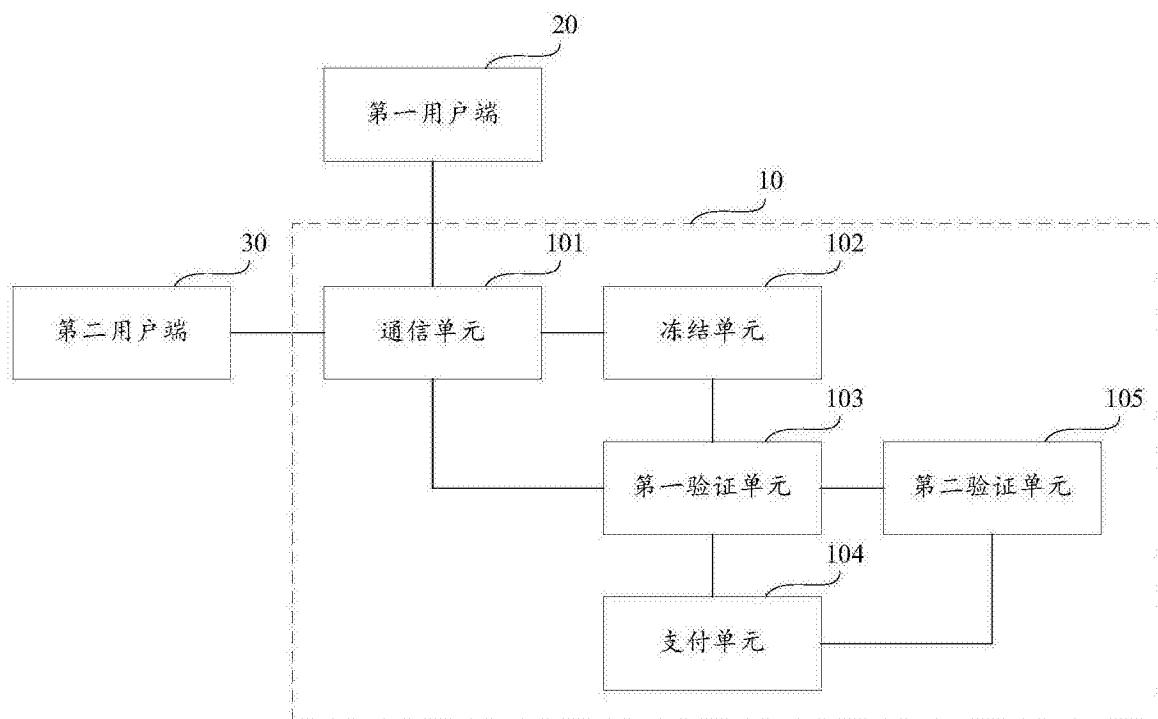


图9

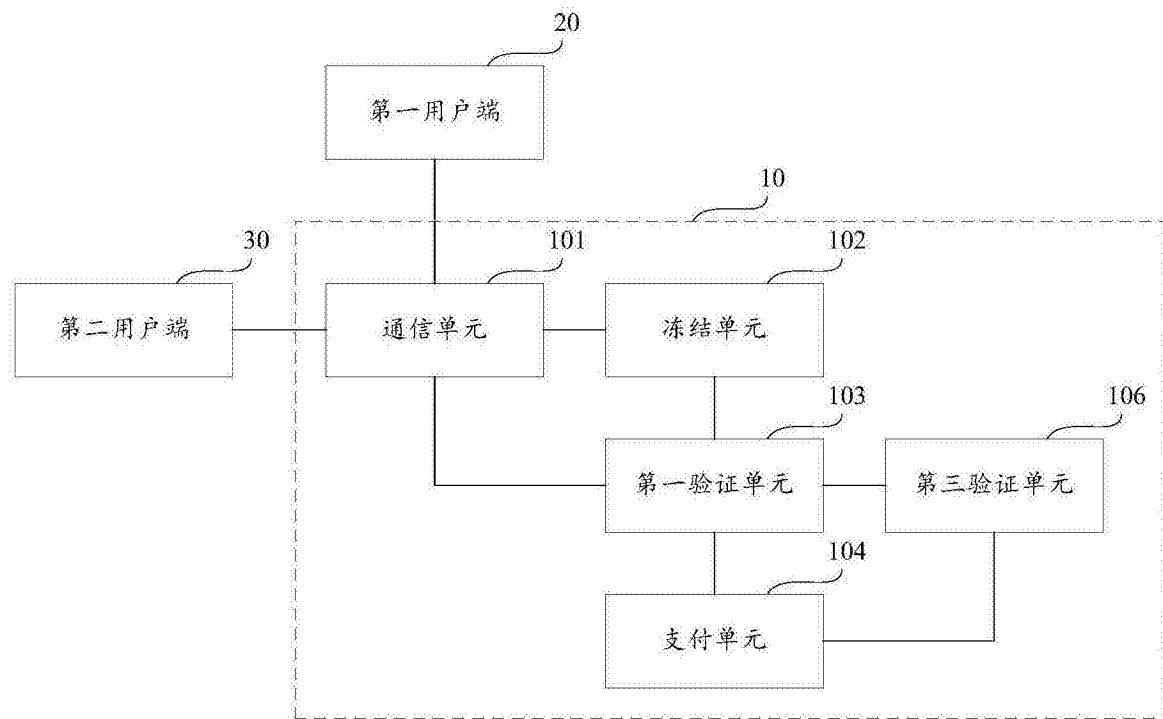


图10

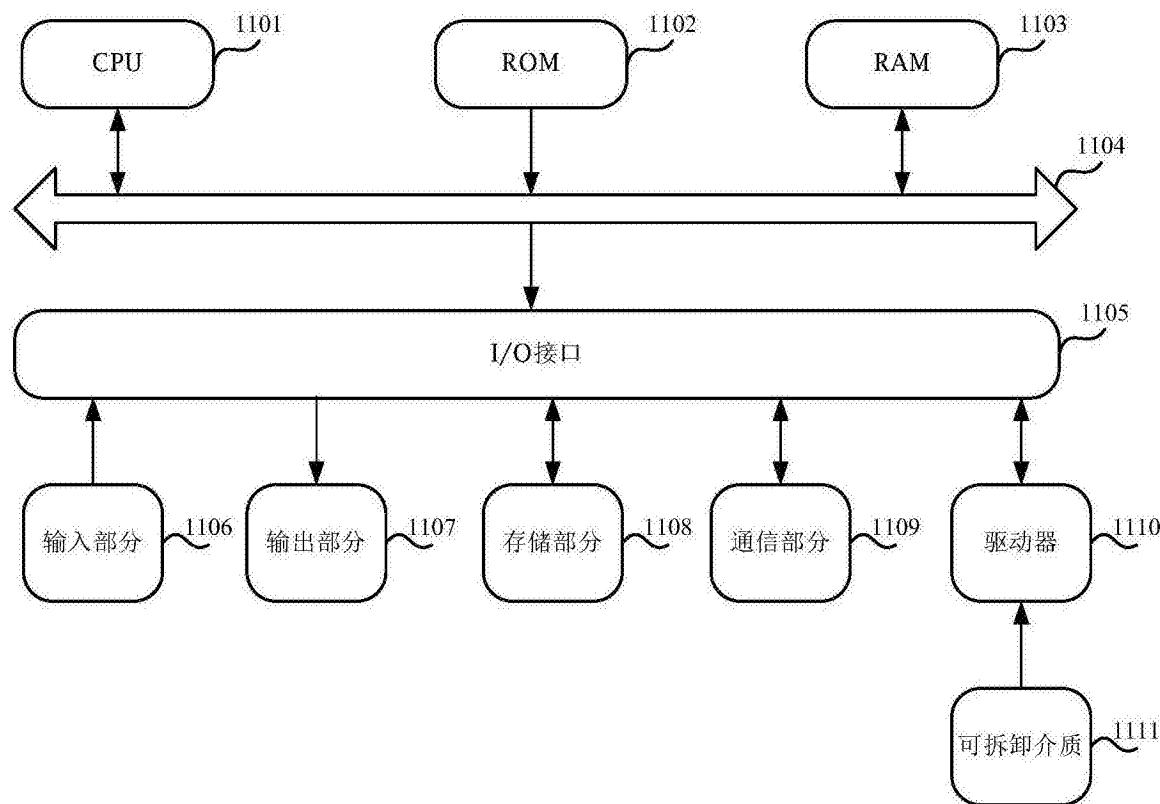


图11