



(12)发明专利申请

(10)申请公布号 CN 111108732 A

(43)申请公布日 2020.05.05

(21)申请号 201880043164.9

(22)申请日 2018.07.02

(30)优先权数据

62/527,519 2017.06.30 US

62/690,389 2018.06.27 US

(85)PCT国际申请进入国家阶段日

2019.12.26

(86)PCT国际申请的申请数据

PCT/US2018/040553 2018.07.02

(87)PCT国际申请的公布数据

W02019/006446 EN 2019.01.03

(71)申请人 维萨国际服务协会

地址 美国加利福尼亚州

(72)发明人 裴曼·莫沙塞尔 沙亚·加内什

沙闪克·阿格拉瓦尔

(74)专利代理机构 北京天昊联合知识产权代理有限公司 11112

代理人 张娜 顾丽波

(51)Int.Cl.

H04L 29/06(2006.01)

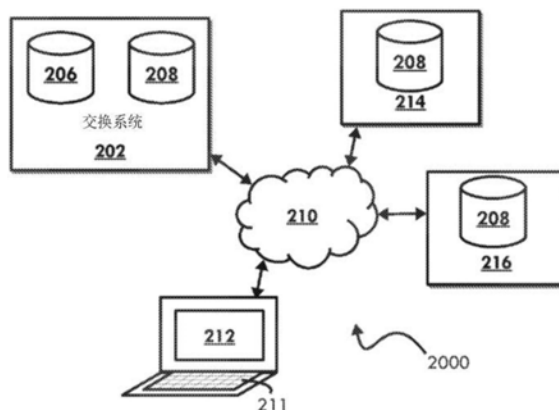
权利要求书4页 说明书18页 附图6页

(54)发明名称

用于确定数字资产交易所的偿付能力的方法、系统和计算机程序产品

(57)摘要

公开了一种用于确定数字资产交换系统的偿付能力的系统、方法和计算机程序产品。所述方法包括：标识与所述数字资产交换系统的多个用户相对应的多个区块链地址；生成对与所述多个区块链地址相对应的数字资产数量的第一承诺；生成对所述多个用户中的每个用户的余额的第二承诺；生成零知识算法的第一组成部分，所述第一组成部分被配置为接收所述第一承诺作为输入，并且输出基于与每个区块链地址相对应的每个公共密钥生成的值；生成所述零知识算法的第二组成部分，所述第二组成部分被配置为接收所述第二承诺作为输入，并且输出基于每个用户余额生成的值；以及基于所述零知识算法用至少一个处理器确定所述数字资产交换系统是具有偿付能力的。



1. 一种用于确定数字资产交换系统的偿付能力的计算机实现的方法,包括:

用至少一个处理器来标识与所述数字资产交换系统的多个用户相对应的多个区块链地址,所述多个区块链地址中的每个区块链地址包括通过对与所述数字资产交换系统所控制的私有秘钥相对应的公共秘钥进行哈希处理而生成的值,使得所述公共秘钥和所述私有秘钥不暴露在区块链网络上;

用至少一个处理器生成对与所述多个区块链地址相对应的数字资产数量的第一承诺;

用至少一个处理器生成对所述多个用户中的每个用户的余额的第二承诺;

用至少一个处理器生成零知识算法的第一组成部分,所述第一组成部分被配置为接收所述第一承诺作为输入,并且输出基于与每个区块链地址相对应的每个公共秘钥生成的值,使得所述零知识算法的所述第一组成部分向验证系统证明所述数字资产交换系统能够访问与每个区块链地址相对应的每个公共秘钥;

用至少一个处理器生成所述零知识算法的第二组成部分,所述第二组成部分被配置为接收所述第二承诺作为输入,并且输出基于每个用户余额生成的值,使得所述零知识算法的所述第二组成部分向验证系统证明每个用户余额都包括在所述数字资产的数量中;以及

基于所述零知识算法,用至少一个处理器确定所述数字资产交换系统是具有偿付能力的。

2. 如权利要求1所述的计算机实现的方法,其中所述零知识算法的所述第一组成部分包括zkSNARK协议,并且其中所述零知识算法的所述第二组成部分包括西格玛协议。

3. 如权利要求1所述的计算机实现的方法,其中所述零知识算法的所述第一组成部分是布尔函数。

4. 如权利要求3所述的计算机实现的方法,其中所述零知识算法的所述第二组成部分是代数函数。

5. 如权利要求4所述的计算机实现的方法,其中确定所述数字资产交换系统具有偿付能力包括确定所述代数函数的输出是否为所述布尔函数的输入。

6. 如权利要求1所述的计算机实现的方法,其中所述区块链网络包括比特币公共区块链网络。

7. 如权利要求1所述的计算机实现的方法,其中所述第一承诺包括沿着椭圆曲线的第一点,并且其中所述第二承诺包括沿着椭圆曲线的第二点。

8. 一种用于确定数字资产交换系统的偿付能力的系统,包括:

安全数据存储设备,所述安全数据存储设备包括用于所述数字资产交换系统的多个用户的多个公共/私有密钥对;和

至少一个处理器,所述至少一个处理器与区块链网络通信,所述至少一个处理器被编程或配置为:

标识与所述数字资产交换系统的所述多个用户相对应的多个区块链地址,所述多个区块链地址中的每个区块链地址包括通过对与所述数字资产交换系统所控制的私有秘钥相对应的公共秘钥进行哈希处理而生成并且存储在所述安全数据存储设备上的值,使得所述公共秘钥和所述私有秘钥不暴露在所述区块链网络上;

生成对与所述多个区块链地址相对应的数字资产的数量第一承诺;

生成对所述多个用户中的每个用户的余额的第二承诺;

生成零知识算法的第一组成部分,所述第一组成部分被配置为接收所述第一承诺作为输入,并且输出基于与每个区块链地址相对应的每个公共密钥生成的值,使得所述零知识算法的所述第一组成部分向验证系统证明所述数字资产交换系统能够访问与每个区块链地址相对应的每个公共密钥;

生成所述零知识算法的第二组成部分,所述第二组成部分被配置为接收所述第二承诺作为输入,并且输出基于每个用户余额生成的值,使得所述零知识算法的所述第二组成部分向验证系统证明每个用户余额都包括在所述数字资产的数量中;以及

基于所述零知识算法确定所述数字资产交换系统是具有偿付能力的。

9.如权利要求8所述的系统,其中所述零知识算法的所述第一组成部分包括zkSNARK协议,并且其中所述零知识算法的所述第二组成部分包括西格玛协议。

10.如权利要求8所述的系统,其中所述零知识算法的所述第一组成部分是布尔函数。

11.如权利要求10所述的系统,其中所述零知识算法的所述第二组成部分是代数函数。

12.如权利要求11所述的系统,其中确定所述数字资产交换系统具有偿付能力包括确定所述代数函数的输出是否为所述布尔函数的输入。

13.如权利要求8所述的系统,其中所述区块链网络包括比特币公共区块链网络。

14.如权利要求8所述的系统,其中所述第一承诺包括沿着椭圆曲线的第一点,并且其中所述第二承诺包括沿着椭圆曲线的第二点。

15.一种用于确定数字资产交换系统的偿付能力的计算机程序产品,包括至少一个非暂时性计算机可读介质,所述至少一个非暂时性计算机可读介质包括程序指令,当由至少一个处理器执行时,所述程序指令使所述至少一个处理器执行以下操作:

标识与所述数字资产交换系统的多个用户相对应的区块链网络的多个区块链地址,所述多个区块链地址中的每个区块链地址包括通过对与所述数字资产交换系统所控制的私有密钥相对应的公共密钥进行哈希处理而生成并且存储在所述安全数据存储设备上的值,使得所述公共密钥和所述私有密钥不暴露在所述区块链网络上;

生成对与所述多个区块链地址相对应的数字资产的数量数的第一承诺;

生成对所述多个用户中的每个用户的余额的第二承诺;

生成零知识算法的第一组成部分,所述第一组成部分被配置为接收所述第一承诺作为输入,并且输出基于与每个区块链地址相对应的每个公共密钥生成的值,使得所述零知识算法的所述第一组成部分向验证系统证明所述数字资产交换系统能够访问与每个区块链地址相对应的每个公共密钥;

生成所述零知识算法的第二组成部分,所述第二组成部分被配置为接收所述第二承诺作为输入,并且输出基于每个用户余额生成的值,使得所述零知识算法的所述第二组成部分向验证系统证明每个用户余额都包括在所述数字资产的数量中;以及

基于所述零知识算法确定所述数字资产交换系统是具有偿付能力的。

16.如权利要求15所述的计算机程序产品,其中所述零知识算法的所述第一组成部分包括zkSNARK协议,并且其中所述零知识算法的所述第二组成部分包括西格玛协议。

17.如权利要求15所述的计算机程序产品,其中所述零知识算法的所述第一组成部分是布尔函数。

18.如权利要求17所述的计算机程序产品,其中所述零知识算法的所述第二组成部分

是代数函数。

19. 如权利要求18所述的计算机程序产品,其中确定所述数字资产交换系统具有偿付能力包括确定所述代数函数的输出是否为所述布尔函数的输入。

20. 如权利要求15所述的计算机程序产品,其中所述区块链网络包括比特币公共区块链网络。

21. 如权利要求15所述的计算机程序产品,其中所述第一承诺包括沿着椭圆曲线的第一点,并且其中所述第二承诺包括沿着椭圆曲线的第二点。

22. 一种用于生成和验证匿名数字证书的计算机实现的方法,包括:

用证明系统的至少一个处理器,通过基于非对称加密算法用私有密钥对哈希消息进行加密,来生成数字签名;

用所述至少一个处理器将所述数字签名传递到验证系统;

用所述至少一个处理器生成对被用于生成所述哈希消息的消息的承诺;

用所述至少一个处理器生成零知识算法的第一组成部分,所述第一组成部分被配置为接收所述承诺作为输入,并且基于被用于生成所述哈希消息的所述消息来输出值;

用所述至少一个处理器生成所述零知识算法的第二组成部分,所述第二组成部分被配置为接收所述承诺作为输入,并且基于被用于生成所述数字签名的所述私有密钥来输出值;以及

基于所述第一组成部分和所述第二组成部分用所述至少一个处理器来生成所述零知识算法。

23. 如权利要求22所述的计算机实现的方法,其中对所述消息的所述承诺包括沿着椭圆曲线的点。

24. 如权利要求22所述的计算机实现的方法,进一步包括基于所述承诺和所述零知识算法由所述验证系统的至少一个处理器来验证所述数字签名。

25. 如权利要求22所述的计算机实现的方法,其中所述零知识算法的所述第一组成部分包括zkSNARK协议,并且其中所述零知识算法的所述第二组成部分包括西格玛协议。

26. 如权利要求22所述的计算机实现的方法,其中所述零知识算法的所述第一组成部分是布尔函数。

27. 如权利要求25所述的计算机实现的方法,其中所述零知识算法的所述第二组成部分是代数函数。

28. 如权利要求27所述的计算机实现的方法,进一步包括通过确定所述代数函数的输出是所述布尔函数的输入,基于所述零知识算法来验证所述数字签名。

29. 一种用于生成和验证匿名数字证书的系统,包括:

安全数据存储设备,所述安全数据存储设备包括公共密钥/私有密钥对的私有密钥和消息;以及

证明计算机,所述证明计算机包括至少一个处理器,所述至少一个处理器被编程或配置为:

通过基于非对称加密算法用所述私有密钥对所述消息的哈希进行加密来生成数字签名;

将所述数字签名传递到验证计算机;

生成对所述消息的承诺；

生成零知识算法的第一组成部分，所述第一组成部分被配置为接收所述承诺作为输入，并且基于被用于生成所述哈希消息的所述消息来输出值；

生成所述零知识算法的第二组成部分，所述第二组成部分被配置为接收所述承诺作为输入，并且基于被用于生成所述数字签名的所述私有密钥来输出值；

基于所述第一组成部分和所述第二组成部分来生成所述零知识算法；以及

将所述零知识算法传递到所述验证计算机。

30. 如权利要求29所述的系统，其中对所述消息的所述承诺包括沿着椭圆曲线的点。

31. 如权利要求29所述的系统，进一步包括所述验证计算机，所述验证计算机包括至少一个处理器，所述至少一个处理器被编程或配置为基于所述承诺和所述零知识算法来验证所述数字签名。

32. 如权利要求29所述的系统，其中所述零知识算法的所述第一组成部分包括zkSNARK协议，并且其中所述零知识算法的所述第二组成部分包括西格玛协议。

33. 如权利要求29所述的系统，其中所述零知识算法的所述第一组成部分是布尔函数。

34. 如权利要求33所述的系统，其中所述零知识算法的所述第二组成部分是代数函数。

35. 如权利要求34所述的系统，进一步包括通过确定所述代数函数的输出是所述布尔函数的输入，基于所述零知识算法来验证所述数字签名。

36. 一种用于生成和验证匿名数字证书的计算机程序产品，包括至少一个非暂时性计算机可读介质，所述至少一个非暂时性计算机可读介质包括程序指令，当由至少一个处理器执行时，所述程序指令使所述至少一个处理器执行以下操作：

通过基于非对称加密算法用私有密钥对所述消息的哈希进行加密来生成数字签名；

将所述数字签名传递到验证计算机；

生成对所述消息的承诺；

生成零知识算法的第一组成部分，所述第一组成部分被配置为接收所述承诺作为输入，并且基于被用于生成所述哈希消息的所述消息来输出值；

生成所述零知识算法的第二组成部分，所述第二组成部分被配置为接收所述承诺作为输入，并且基于被用于生成所述数字签名的所述私有密钥来输出值；

基于所述第一组成部分和所述第二组成部分来生成所述零知识算法；以及

将所述零知识算法传递到所述验证计算机。

37. 如权利要求36所述的计算机程序产品，其中对所述消息的所述承诺包括沿着椭圆曲线的点。

38. 如权利要求36所述的计算机程序产品，其中所述零知识算法的所述第一组成部分包括zkSNARK协议，并且其中所述零知识算法的所述第二组成部分包括西格玛协议。

39. 如权利要求36所述的计算机程序产品，其中所述零知识算法的所述第一组成部分是布尔函数。

40. 如权利要求39所述的计算机程序产品，其中所述零知识算法的所述第二组成部分是代数函数。

41. 如权利要求40所述的计算机程序产品，进一步包括通过确定所述代数函数的输出是所述布尔函数的输入，基于所述零知识算法来验证所述数字签名。

用于确定数字资产交易所的偿付能力的方法、系统和计算机程序产品

[0001] 相关申请的交叉引用

[0002] 本申请要求2017年6月30日提交的第62/527 519号美国临时专利申请和2018年6月27日提交的第62/690 389号美国临时专利申请的优先权,所述两个美国临时专利申请都通过引用整体并入本文中。

背景技术

1. 技术领域

[0003] 公开的实施方案通常涉及复合语句的零知识证明,并且在优选和非限制性实施方案或方面中,涉及一种用于确定数字资产交易所的偿付能力和/或验证匿名数字证书的系统、方法和计算机程序产品。

[0004] 2. 技术注意事项

[0005] 零知识证明 (ZKP) 允许一个人在不揭露秘密内容的情况下证明关于一条秘密信息的语句。ZKP通常满足至少三个属性:完整性、可靠性和零知识。一个ZKP通常至少满足三个属性:完整性、可靠性和零知识。关于完整性,如果语句是真的,那么诚实的验证者将会被诚实的证明者说服语句是真的。关于可靠性,如果语句是假的,那么不诚实的证明者可以说服诚实的验证者语句是真的可能性为零或非常小。关于零知识,如果语句是真的,那么对语句的知识不会传达对秘密的了解。举例来说,令 R 为可有效计算的二元关系,它由 (s, w) 形式的对组成,其中, s 是语句,并且 w 是见证。令 L 为与 R 相关联的语言,即 $L = \{s \mid \exists w \text{ s.t. } R(s, w) = 1\}$ 。 L 的零知识证明让证明者 P 在不揭露 w 的情况下说服验证者 V ,针对公共输入 $s, s \in L$ 。知识的证明不仅抓住了语句 $s \in L$ 的真实性,而且证明者“拥有”这个事实的见证 w 。非交互式证明是其中 P 仅向 V 发送一条消息,并且 V 基于其输入、消息和任何公共参数来决定是否接受。

[0006] 需要ZKP的语句的性质可以变化,例如布尔语句(即,真或假)、代数语句(例如., 两个量的总和等于第三个量)和/或诸如此类。因为基础语句变化,所以ZKP的类型也变化。用于不同类型语句的不同ZKP通常彼此不兼容,从而迫使研究人员当需要几种证明的组合时,只能使用一种证明。当要证明一个以上的语句时,特别是当语句函数分层使得一个函数的输出是另一个函数的输入时,生成了复杂的复合语句,而对于这些复杂的复合语句,不存在有效的ZKP。举例来说,两层复合语句可以是代数上的算术、算术上的代数、算术上的算术或代数上的代数的组合。复合语句的其他配置是可能的。

[0007] 举例来说,考虑通过加密货币(例如., 比特币)交易所的证明来证明他们是具有偿付能力的,即., 证明交易所控制着足以覆盖所有用户账户的加密货币。偿付能力的证明包含两个部分:负债证明,即., 即欠交易所用户的总加密货币;和资产证明,即由交易所控制的总加密货币。如果资产等于或超过负债,那么交易所完全具有偿付能力。如果公共分类账提供所有交易的全部细节,包含转移的价值和发送者/接收者账户的身份,那么偿付能力的

证明通常是简单明了的。然而,如果要维护用户和账户的隐私,那么证明偿付能力变得具有挑战性。

[0008] 偿付能力的ZKP将允许加密货币交易所向其用户验证其控制了足够的资金,而不揭露所述资金和负债的数额或分布。在没有加密的偿付能力证明的情况下,交易所可能会被降级为寻求第三方审计员来验证资金,这要求用户信任第三方审计员,并且审计员维护数据的隐私。因此,在本领域中需要偿付能力语句的有效ZKP。

[0009] 交易所将需要证明的基础语句大多是代数的(即资产超过或等于负债),但语句的关键部分是布尔的(例如,哈希函数的等价性检查)——尽管用户钱包的公共密钥是以代数方式从秘密密钥导出的,但是只有通过布尔电路计算出的公共密钥的哈希被放在区块链上以节省带宽。西格玛协议ZKP(例如,Provisions系统所采用的ZKP)擅长证明代数语句,例如,私有价值的知识 x ,使得 $g^x=y$ 。参见Dagher、Gaby G.等人的规定:比特币交易所偿付能力的隐私保护证明,计算机协会(ACM)计算机和通信安全(CCS)会议,2015年。然而,规定与将哈希公共密钥(即, $H(g^x)=h$)存储在区块链中的加密货币(例如比特币)不兼容。另一方面,zkSNARK(例如,Zerocash系统所采用的zkSNARK)擅长证明复杂、非代数性语句,例如,私有价值 x 的知识,使得 $SHA256(x)=y$ 。参见Ben-Sasson、Eli等人的Zerocash:来自比特币的分散式匿名支付,IEEE安全与隐私研讨会,2014年。还不知道如何有效地组合这两种技术。这样做将需要证明一个私有 x 的知识,使得 $H(g^x)=y$,其含有代数和非代数语句,用现有方法证明所述语句极其困难并且效率低下。

[0010] 对复合语句的ZKP的需要延伸到加密货币交易所对偿付能力的证明之外。举例来说,数字证书被用于标识因特网上的实体,其中消息是用数字签名发送和签名的。用于这样的消息的数字证书的匿名凭证要求消息和签名保持秘密,同时仍证明签名是有效的。在这个应用程序中,消息在被代数签名之前被哈希。因此,要证明的ZKP语句是代数函数和布尔函数的复合语句,对此还没有已知的有效的ZKP技术。在又一个示例中,当前的加密货币系统(例如,ZCash)作为匿名分散式数字货币运行,并且使用zkSNARK在一个大语句中证明许多较小的组成部分。用于证明语句的公共引用字符串可能会变得非常大(例如,在ZCash的情况下,千兆字节)。具有ZKP的系统来证明较小的个别复合语句将是有益的,其中,一个语句的输出是另一个语句的输入,并且其中减少了公共引用字符串的大小。

[0011] 因此,在本领域中需要为复合语句提供一种有效的零知识证明系统。在本领域中还需要提供一种用于使用零知识算法来确定数字资产交易所的偿付能力的系统以及一种用于使用零知识算法来验证数字签名的系统。

发明内容

[0012] 因此,并且总体上,提供了一种用于生成复合语句的零知识算法的系统、计算机实现的方法和计算机程序产品,用于确定数字资产交易所的偿付能力的系统、方法和计算机程序产品以及用于验证匿名数字证书的系统、方法和计算机程序产品。

[0013] 根据非限制性实施方案,提供了一种用于确定数字资产交换系统的偿付能力的计算机实现的方法,包括:用至少一个处理器来标识与所述数字资产交换系统的多个用户相对应的多个区块链地址,所述多个区块链地址中的每个区块链地址包括通过对与所述数字资产交换系统所控制的私有秘钥相对应的公共秘钥进行哈希处理而生成的值,使得所述公

共密钥和所述私有密钥不暴露在区块链网络上；用至少一个处理器生成对与所述多个区块链地址相对应的数字资产数量的第一承诺；用至少一个处理器生成对所述多个用户中的每个用户的余额的第二承诺；用至少一个处理器生成零知识算法的第一组成部分，所述第一组成部分被配置为接收所述第一承诺作为输入，并且输出基于与每个区块链地址相对应的每个公共密钥生成的值，使得所述零知识算法的所述第一组成部分向验证系统证明所述数字资产交换系统能够访问与每个区块链地址相对应的每个公共密钥；用至少一个处理器生成所述零知识算法的第二组成部分，所述第二组成部分被配置为接收所述第二承诺作为输入，并且输出基于每个用户余额生成的值，使得所述零知识算法的所述第二组成部分向验证系统证明每个用户余额都包括在所述数字资产的数量中；以及基于所述零知识算法，用至少一个处理器确定所述数字资产交换系统是具有偿付能力的。

[0014] 在非限制性实施方案中，所述零知识算法的所述第一组成部分包括zkSNARK协议，并且其中所述零知识算法的所述第二组成部分包括西格玛协议。在非限制性实施方案中，所述零知识算法的所述第一组成部分是布尔函数。在非限制性实施方案中，所述零知识算法的所述第二组成部分是代数函数。

[0015] 在非限制性实施方案中，确定所述数字资产交换系统是具有偿付能力的包括确定所述代数函数的输出是否是所述布尔函数的输入。在非限制性实施方案中，所述区块链网络包括比特币公共区块链网络。在非限制性实施方案中，所述第一承诺包括沿着椭圆曲线的第一点，并且其中所述第二承诺包括沿着椭圆曲线的第二点。

[0016] 根据另一个非限制性实施方案，提供了一种用于确定数字资产交换系统的偿付能力的系统，包括：安全数据存储设备，所述安全数据存储设备包括用于所述数字资产交换系统的多个用户的多个公共/私有密钥对；和至少一个处理器，所述至少一个处理器与区块链网络通信，所述至少一个处理器被编程或配置为：标识与所述数字资产交换系统的所述多个用户相对应的多个区块链地址，所述多个区块链地址中的每个区块链地址包括通过对与所述数字资产交换系统所控制的私有密钥相对应的公共密钥进行哈希处理而生成并且存储在所述安全数据存储设备上的值，使得所述公共密钥和所述私有密钥不暴露在所述区块链网络上；生成对与所述多个区块链地址相对应的数字资产的数量第一承诺；生成对所述多个用户中的每个用户的余额的第二承诺；生成零知识算法的第一组成部分，所述第一组成部分被配置为接收所述第一承诺作为输入，并且输出基于与每个区块链地址相对应的每个公共密钥生成的值，使得所述零知识算法的所述第一组成部分向验证系统证明所述数字资产交换系统能够访问与每个区块链地址相对应的每个公共密钥；生成所述零知识算法的第二组成部分，所述第二组成部分被配置为接收所述第二承诺作为输入，并且输出基于每个用户余额生成的值，使得所述零知识算法的所述第二组成部分向验证系统证明每个用户余额都包括在所述数字资产的数量中；以及基于所述零知识算法确定所述数字资产交换系统是具有偿付能力的。

[0017] 在非限制性实施方案中，所述零知识算法的所述第一组成部分包括zkSNARK协议，并且其中所述零知识算法的所述第二组成部分包括西格玛协议。在非限制性实施方案中，所述零知识算法的所述第一组成部分是布尔函数。在非限制性实施方案中，所述零知识算法的所述第二组成部分是代数函数。在非限制性实施方案中，确定所述数字资产交换系统是具有偿付能力的包括确定所述代数函数的输出是否是所述布尔函数的输入。

[0018] 在非限制性实施方案中,所述区块链网络包括比特币公共区块链网络。在非限制性实施方案中,所述第一承诺包括沿着椭圆曲线的第一点,并且其中所述第二承诺包括沿着椭圆曲线的第二点。

[0019] 根据另一非限制性实施方案,提供了一种用于确定数字资产交换系统的偿付能力的计算机程序产品,包括至少一个非暂时性计算机可读介质,所述至少一个非暂时性计算机可读介质包括程序指令,当由至少一个处理器执行时,所述程序指令使所述至少一个处理器执行以下操作:标识与所述数字资产交换系统的多个用户相对应的区块链网络的多个区块链地址,所述多个区块链地址中的每个区块链地址包括通过对与所述数字资产交换系统所控制的私有秘钥相对应的公共秘钥进行哈希处理而生成并且存储在所述安全数据存储设备上的值,使得所述公共秘钥和所述私有秘钥不暴露在所述区块链网络上;生成对与所述多个区块链地址相对应的数字资产的数量数的第一承诺;生成对所述多个用户中的每个用户的余额的第二承诺;生成零知识算法的第一组成部分,所述第一组成部分被配置为接收所述第一承诺作为输入,并且输出基于与每个区块链地址相对应的每个公共秘钥生成的值,使得所述零知识算法的所述第一组成部分向验证系统证明所述数字资产交换系统能够访问与每个区块链地址相对应的每个公共秘钥;生成所述零知识算法的第二组成部分,所述第二组成部分被配置为接收所述第二承诺作为输入,并且输出基于每个用户余额生成的值,使得所述零知识算法的所述第二组成部分向验证系统证明每个用户余额都包括在所述数字资产的数量中;以及基于所述零知识算法确定所述数字资产交换系统是具有偿付能力的。

[0020] 在非限制性实施方案中,所述零知识算法的所述第一组成部分包括zkSNARK协议,并且其中所述零知识算法的所述第二组成部分包括西格玛协议。在非限制性实施方案中,所述零知识算法的所述第一组成部分是布尔函数。在非限制性实施方案中,所述零知识算法的所述第二组成部分是代数函数。在非限制性实施方案中,确定所述数字资产交换系统是具有偿付能力的包括确定所述代数函数的输出是否是所述布尔函数的输入。

[0021] 在非限制性实施方案中,所述区块链网络包括比特币公共区块链网络。在非限制性实施方案中,所述第一承诺包括沿着椭圆曲线的第一点,并且其中所述第二承诺包括沿着椭圆曲线的第二点。

[0022] 根据另一非限制性实施方案,提供了一种用于生成和验证匿名数字证书的计算机实现的方法,包括:用证明系统的至少一个处理器,通过基于非对称加密算法用私有密钥对哈希消息进行加密,来生成数字签名;用所述至少一个处理器将所述数字签名传递到验证系统;用所述至少一个处理器生成对被用于生成所述哈希消息的消息的承诺;用所述至少一个处理器生成零知识算法的第一组成部分,所述第一组成部分被配置为接收所述承诺作为输入,并且基于被用于生成所述哈希消息的所述消息来输出值;用所述至少一个处理器生成所述零知识算法的第二组成部分,所述第二组成部分被配置为接收所述承诺作为输入,并且基于被用于生成所述数字签名的所述私有密钥来输出值;以及基于所述第一组成部分和所述第二组成部分用所述至少一个处理器来生成所述零知识算法。

[0023] 在非限制性实施方案中,对所述消息的所述承诺包括沿着椭圆曲线的点。在非限制性实施方案中,所述方法包括基于所述承诺和所述零知识算法由所述验证系统的至少一个处理器来验证所述数字签名。

[0024] 在非限制性实施方案中,所述零知识算法的所述第一组成部分包括zkSNARK协议,并且其中所述零知识算法的所述第二组成部分包括西格玛协议。在非限制性实施方案中,所述零知识算法的所述第一组成部分是布尔函数。在非限制性实施方案中,所述零知识算法的所述第二组成部分是代数函数。在非限制性实施方案中,确定所述数字资产交换系统是具有偿付能力的包括确定所述代数函数的输出是否是所述布尔函数的输入。

[0025] 根据又一个非限制性实施方案,提供了一种用于生成和验证匿名数字证书的系统,包括:安全数据存储设备,所述安全数据存储设备包括公共密钥/私有密钥对的私有密钥和消息;以及证明计算机,所述证明计算机包括至少一个处理器,所述至少一个处理器被编程或配置为:通过基于非对称加密算法用所述私有密钥对所述消息的哈希进行加密来生成数字签名;将所述数字签名传递到验证计算机;生成对所述消息的承诺;生成零知识算法的第一组成部分,所述第一组成部分被配置为接收所述承诺作为输入,并且基于被用于生成所述哈希消息的所述消息来输出值;生成所述零知识算法的第二组成部分,所述第二组成部分被配置为接收所述承诺作为输入,并且基于被用于生成所述数字签名的所述私有密钥来输出值;基于所述第一组成部分和所述第二组成部分来生成所述零知识算法;以及将所述零知识算法传递到所述验证计算机。

[0026] 在非限制性实施方案中,对所述消息的所述承诺包括沿着椭圆曲线的点。在非限制性实施方案中,所述系统包括所述验证计算机,所述验证计算机包括至少一个处理器,所述至少一个处理器被编程或配置为基于所述承诺和所述零知识算法来验证所述数字签名。在非限制性实施方案中,所述零知识算法的所述第一组成部分包括zkSNARK协议,并且其中所述零知识算法的所述第二组成部分包括西格玛协议。在非限制性实施方案中,所述零知识算法的所述第一组成部分是布尔函数。在非限制性实施方案中,所述零知识算法的所述第二组成部分是代数函数。在非限制性实施方案中,所述至少一个处理器进一步被编程为通过确定所述代数函数的输出是所述布尔函数的输入来基于所述零知识算法来验证所述数字签名。

[0027] 根据另一个非限制性实施方案,提供了一种用于生成和验证匿名数字证书的计算机程序产品,包括至少一个非暂时性计算机可读介质,所述至少一个非暂时性计算机可读介质包括程序指令,当由至少一个处理器执行时,所述程序指令使所述至少一个处理器执行以下操作:通过基于非对称加密算法用私有密钥对所述消息的哈希进行加密来生成数字签名;将所述数字签名传递到验证计算机;生成对所述消息的承诺;生成零知识算法的第一组成部分,所述第一组成部分被配置为接收所述承诺作为输入,并且基于被用于生成所述哈希消息的所述消息来输出值;生成所述零知识算法的第二组成部分,所述第二组成部分被配置为接收所述承诺作为输入,并且基于被用于生成所述数字签名的所述私有密钥来输出值;基于所述第一组成部分和所述第二组成部分来生成所述零知识算法;以及将所述零知识算法传递到所述验证计算机。

[0028] 在非限制性实施方案中,对所述消息的所述承诺包括沿着椭圆曲线的点。在非限制性实施方案中,所述零知识算法的所述第一组成部分包括zkSNARK协议,并且其中所述零知识算法的所述第二组成部分包括西格玛协议。在非限制性实施方案中,所述零知识算法的所述第一组成部分是布尔函数。在非限制性实施方案中,所述零知识算法的所述第二组成部分是代数函数。在非限制性实施方案中,所述至少一个处理器进一步促使通过确定所

述代数函数的输出是所述布尔函数的输入,基于所述零知识算法来验证所述数字签名。

[0029] 根据又一个非限制性实施方案,通过有效地组合zkSNARK和西格玛协议,提供了一种用于含有代数和非代数函数的复合语句的ZKP证明的新框架。所述组合允许x的知识的证明,使得 $AES(x) = y_1$ 和 $g^x = y_2$,同时保持x私有。此外,本发明提供证明双离散对数的知识,即, $y = g^{g^x}$ 的知识,其中g是用于椭圆曲线(EC)组(特别是用于比特币的EC secp256k1)的生成器。用于这样的证明的先前技术仅对基于RSA的组有效,并且因此不适用于比特币。

[0030] 将在以下编号的条款中陈述本发明的其他优选和非限制性实施方案或方面:

[0031] 条款1:一种用于确定数字资产交换系统的偿付能力的计算机实现的方法,包括:用至少一个处理器来标识与所述数字资产交换系统的多个用户相对应的多个区块链地址,所述多个区块链地址中的每个区块链地址包括通过对与所述数字资产交换系统所控制的私有密钥相对应的公共密钥进行哈希处理而生成的值,使得所述公共密钥和所述私有密钥不暴露在区块链网络上;用至少一个处理器生成对与所述多个区块链地址相对应的数字资产数量的第一承诺;用至少一个处理器生成对所述多个用户中的每个用户的余额的第二承诺;用至少一个处理器生成零知识算法的第一组成部分,所述第一组成部分被配置为接收所述第一承诺作为输入,并且输出基于与每个区块链地址相对应的每个公共密钥生成的值,使得所述零知识算法的所述第一组成部分向验证系统证明所述数字资产交换系统能够访问与每个区块链地址相对应的每个公共密钥;用至少一个处理器生成所述零知识算法的第二组成部分,所述第二组成部分被配置为接收所述第二承诺作为输入,并且输出基于每个用户余额生成的值,使得所述零知识算法的所述第二组成部分向验证系统证明每个用户余额都包括在所述数字资产的数量中;以及基于所述零知识算法,用至少一个处理器确定所述数字资产交换系统是具有偿付能力的。

[0032] 条款2:如条款1所述的计算机实现的方法,其中所述零知识算法的所述第一组成部分包括zkSNARK协议,并且其中所述零知识算法的所述第二组成部分包括西格玛协议。

[0033] 条款3:如条款1或2所述的计算机实现的方法,其中所述零知识算法的所述第一组成部分是布尔函数。

[0034] 条款4:如条款1-3中任一项所述的计算机实现的方法,其中所述零知识算法的所述第二组成部分是代数函数。

[0035] 条款5:如条款1-4中任一项所述的计算机实现的方法,其中确定所述数字资产交换系统具有偿付能力包括确定所述代数函数的输出是否为所述布尔函数的输入。

[0036] 条款6:如条款1-5中任一项所述的计算机实现的方法,其中所述区块链网络包括比特币公共区块链网络。

[0037] 条款7:如条款1-6中任一项所述的计算机实现的方法,其中所述第一承诺包括沿着椭圆曲线的第一点,并且其中所述第二承诺包括沿着椭圆曲线的第二点。

[0038] 条款8:一种用于确定数字资产交换系统的偿付能力的系统,包括:安全数据存储设备,所述安全数据存储设备包括用于所述数字资产交换系统的多个用户的多个公共/私有密钥对;和至少一个处理器,所述至少一个处理器与区块链网络通信,所述至少一个处理器被编程或配置为:标识与所述数字资产交换系统的所述多个用户相对应的多个区块链地址,所述多个区块链地址中的每个区块链地址包括通过对与所述数字资产交换系统所控制的私有密钥相对应的公共密钥进行哈希处理而生成并且存储在所述安全数据存储设备上

的值,使得所述公共秘钥和所述私有秘钥不暴露在所述区块链网络上;生成对与所述多个区块链地址相对应的数字资产的数量数的第一承诺;生成对所述多个用户中的每个用户的余额的第二承诺;生成零知识算法的第一组成部分,所述第一组成部分被配置为接收所述第一承诺作为输入,并且输出基于与每个区块链地址相对应的每个公共秘钥生成的值,使得所述零知识算法的所述第一组成部分向验证系统证明所述数字资产交换系统能够访问与每个区块链地址相对应的每个公共秘钥;生成所述零知识算法的第二组成部分,所述第二组成部分被配置为接收所述第二承诺作为输入,并且输出基于每个用户余额生成的值,使得所述零知识算法的所述第二组成部分向验证系统证明每个用户余额都包括在所述数字资产的数量中;以及基于所述零知识算法确定所述数字资产交换系统是具有偿付能力的。

[0039] 条款9:如条款8所述的系统,其中所述零知识算法的所述第一组成部分包括zkSNARK协议,并且其中所述零知识算法的所述第二组成部分包括西格玛协议。

[0040] 条款10:如条款8或9所述的系统,其中所述零知识算法的所述第一组成部分是布尔函数。

[0041] 条款11:如条款8-10中任一项所述的系统,其中所述零知识算法的所述第二组成部分是代数函数。

[0042] 条款12:如条款8-11中任一项所述的系统,其中确定所述数字资产交换系统具有偿付能力包括确定所述代数函数的输出是否为所述布尔函数的输入。

[0043] 第13条:如条款8-12中任一项所述的系统,其中所述区块链网络包括比特币公共区块链网络。

[0044] 第14条:如条款8-13中任一项所述的系统,其中所述第一承诺包括沿着椭圆曲线的第一点,并且其中所述第二承诺包括沿着椭圆曲线的第二点。

[0045] 条款15:一种用于确定数字资产交换系统的偿付能力的计算机程序产品,包括至少一个非暂时性计算机可读介质,所述介质包括程序指令,当由至少一个处理器执行时,所述程序指令使所述至少一个处理器执行以下操作:标识与所述数字资产交换系统的多个用户相对应的区块链网络的多个区块链地址,所述多个区块链地址中的每个区块链地址包括通过对与所述数字资产交换系统所控制的私有秘钥相对应的公共秘钥进行哈希处理而生成并且存储在所述安全数据存储设备上的值,使得所述公共秘钥和所述私有秘钥不暴露在所述区块链网络上;生成对与所述多个区块链地址相对应的数字资产的数量数的第一承诺;生成对所述多个用户中的每个用户的余额的第二承诺;生成零知识算法的第一组成部分,所述第一组成部分被配置为接收所述第一承诺作为输入,并且输出基于与每个区块链地址相对应的每个公共秘钥生成的值,使得所述零知识算法的所述第一组成部分向验证系统证明所述数字资产交换系统能够访问与每个区块链地址相对应的每个公共秘钥;生成所述零知识算法的第二组成部分,所述第二组成部分被配置为接收所述第二承诺作为输入,并且输出基于每个用户余额生成的值,使得所述零知识算法的所述第二组成部分向验证系统证明每个用户余额都包括在所述数字资产的数量中;以及基于所述零知识算法确定所述数字资产交换系统是具有偿付能力的。

[0046] 条款16:如条款15所述的计算机程序产品,其中所述零知识算法的所述第一组成部分包括zkSNARK协议,并且其中所述零知识算法的所述第二组成部分包括西格玛协议。

[0047] 条款17:如条款15或16所述的计算机程序产品,其中所述零知识算法的所述第一

组成部分是布尔函数。

[0048] 条款18:如条款15-17中任一项所述的计算机程序产品,其中所述零知识算法的所述第二组成部分是代数函数。

[0049] 条款19:如条款15-18中任一项所述的计算机程序产品,其中确定所述数字资产交换系统具有偿付能力包括确定所述代数函数的输出是否为所述布尔函数的输入。

[0050] 条款20:如条款15-19中任一项所述的计算机程序产品,其中所述区块链网络包括比特币公共区块链网络。

[0051] 条款21:如条款15-20中任一项所述的计算机程序产品,其中所述第一承诺包括沿着椭圆曲线的第一点,并且其中所述第二承诺包括沿着椭圆曲线的第二点。

[0052] 条款22:一种用于生成和验证匿名数字证书的计算机实现的方法,包括:用证明系统的至少一个处理器,通过基于非对称加密算法用私有密钥对哈希消息进行加密,来生成数字签名;用所述至少一个处理器将所述数字签名传递到验证系统;用所述至少一个处理器生成对被用于生成所述哈希消息的消息的承诺;用所述至少一个处理器生成零知识算法的第一组成部分,所述第一组成部分被配置为接收所述承诺作为输入,并且基于被用于生成所述哈希消息的所述消息来输出值;用所述至少一个处理器生成所述零知识算法的第二组成部分,所述第二组成部分被配置为接收所述承诺作为输入,并且基于被用于生成所述数字签名的所述私有密钥来输出值;以及基于所述第一组成部分和所述第二组成部分用所述至少一个处理器来生成所述零知识算法。

[0053] 条款23:如条款22所述的计算机实现的方法,其中对所述消息的所述承诺包括沿着椭圆曲线的点。

[0054] 条款24:如条款22或23所述的计算机实现的方法,进一步包括基于所述承诺和所述零知识算法由所述验证系统的至少一个处理器来验证所述数字签名。

[0055] 条款25:如条款22-24中任一项所述的计算机实现的方法,其中所述零知识算法的所述第一组成部分包括zkSNARK协议,并且其中所述零知识算法的所述第二组成部分包括西格玛协议。

[0056] 条款26:如条款22-25中任一项所述的计算机实现的方法,其中所述零知识算法的所述第一组成部分是布尔函数。

[0057] 条款27:如条款25-26中任一项所述的计算机实现的方法,其中所述零知识算法的所述第二组成部分是代数函数。

[0058] 条款28:如条款22-27中任一项所述的计算机实现的方法,进一步包括通过确定所述代数函数的输出是所述布尔函数的输入,基于所述零知识算法来验证所述数字签名。

[0059] 条款29:一种用于生成和验证匿名数字证书的系统,包括:安全数据存储设备,所述安全数据存储设备包括公共密钥/私有密钥对的私有密钥和消息;以及证明计算机,所述证明计算机包括至少一个处理器,所述至少一个处理器被编程或配置为:通过基于非对称加密算法用所述私有密钥对所述消息的哈希进行加密来生成数字签名;将所述数字签名传递到验证计算机;生成对所述消息的承诺;生成零知识算法的第一组成部分,所述第一组成部分被配置为接收所述承诺作为输入,并且基于被用于生成所述哈希消息的所述消息来输出值;生成所述零知识算法的第二组成部分,所述第二组成部分被配置为接收所述承诺作为输入,并且基于被用于生成所述数字签名的所述私有密钥来输出值;基于所述第一组成

部分和所述第二组成部分来生成所述零知识算法;以及将所述零知识算法传递到所述验证计算机。

[0060] 条款30:如条款29所述的系统,其中,对所述消息的承诺包括沿着椭圆曲线的点。

[0061] 条款31:如条款29或30所述的系统,进一步包括所述验证计算机,所述验证计算机包括至少一个处理器,所述至少一个处理器被编程或配置为基于所述承诺和所述零知识算法来验证所述数字签名。

[0062] 条款32:如条款29-31中任一项所述的系统,其中所述零知识算法的所述第一组成部分包括zkSNARK协议,并且其中所述零知识算法的所述第二组成部分包括西格玛协议。

[0063] 条款33:如条款29-32中任一项所述的系统,其中所述零知识算法的所述第一组成部分是布尔函数。

[0064] 条款34:如条款29-33中任一项所述的系统,其中所述零知识算法的所述第二组成部分是代数函数。

[0065] 条款35:如条款29-34中任一项所述的系统,进一步包括通过确定所述代数函数的输出是所述布尔函数的输入,基于所述零知识算法来验证所述数字签名。

[0066] 条款36:一种用于生成和验证匿名数字证书的计算机程序产品,包括至少一个非暂时性计算机可读介质,所述至少一个非暂时性计算机可读介质包括程序指令,当由至少一个处理器执行时,所述程序指令使所述至少一个处理器执行以下操作:通过基于非对称加密算法用私有密钥对所述消息的哈希进行加密来生成数字签名;将所述数字签名传递到验证计算机;生成对所述消息的承诺;生成零知识算法的第一组成部分,所述第一组成部分被配置为接收所述承诺作为输入,并且基于被用于生成所述哈希消息的所述消息来输出值;生成所述零知识算法的第二组成部分,所述第二组成部分被配置为接收所述承诺作为输入,并且基于被用于生成所述数字签名的所述私有密钥来输出值;基于所述第一组成部分和所述第二组成部分来生成所述零知识算法;以及将所述零知识算法传递到所述验证计算机。

[0067] 条款37:如条款36所述的计算机程序产品,其中对所述消息的所述承诺包括沿着椭圆曲线的点。

[0068] 条款38:如条款36或37所述的计算机程序产品,其中所述零知识算法的所述第一组成部分包括zkSNARK协议,并且其中所述零知识算法的所述第二组成部分包括西格玛协议。

[0069] 条款39:如条款36-38中任一项所述的计算机程序产品,其中所述零知识算法的所述第一组成部分是布尔函数。

[0070] 条款40:如条款36-39中任一项所述的计算机程序产品,其中所述零知识算法的所述第二组成部分是代数函数。

[0071] 条款41:如条款36-40中任一项所述的计算机程序产品,进一步包括通过确定所述代数函数的输出是所述布尔函数的输入,基于所述零知识算法来验证所述数字签名。

[0072] 在参考附图考虑到下面的描述、附录和所附的权利要求书之后,本发明的这些和其它特点和特性以及结构的相关元件和部件组合的操作方法和功能以及制造的经济性将变得更加显而易见,所有的这些描述、附录以及权利要求书和附图形成本说明书的一部分,其中,类似的附图标记指定各个附图中的对应部分。然而,要明确理解的是,附图仅出于图

示和描述的目的,并且并不意在作为对本发明的限制的定义。除非上下文另有明确说明,否则在说明书和权利要求书中使用的单数形式“一(a)”、“一(an)”和“所述”包括复数指代。

[0073] 附图的简要说明

[0074] 下面参考在附图中图示的示例性实施方案更详细地解释本发明的额外优点和细节,其中:

[0075] 图1是用于生成复合语句的零知识算法并且特别是代数和布尔语句的組合的零知识算法的系统和方法的一个实施方案或方面的示意图;

[0076] 图2是根据非限制性实施方案或方面的用于确定数字资产交易所的偿付能力的系统的示意图;

[0077] 图3是根据非限制性实施方案或方面的用于确定数字资产交易所的偿付能力的方法的流程图;

[0078] 图4是根据非限制性实施方案或方面的用于生成和验证匿名数字签名的方法的流程图;

[0079] 图5是根据非限制性实施方案或方面的用于生成和验证匿名数字签名的系统的示意图;并且

[0080] 图6是根据非限制性实施方案或方面的用于生成零知识算法的方法的流程图,所述零知识算法用于证明对值的知识或对值的访问。

具体实施方式

[0081] 在下文中出于描述的目的,术语“上部”、“下部”、“右侧”、“左侧”、“垂直”、“水平”、“顶部”、“底部”、“横向”、“纵向”及其派生词应与本发明相关,如它在附图中定向的。然而,应当理解,除非明确相反地说明,否则本发明可以采取各种替代变型和步骤顺序。还应当理解,附图中示出的以及以下说明书中描述的特定设备和过程仅仅是本发明的示例性实施方案。因此,与本文中所公开的实施方案有关的特定尺寸和其他物理特性不应被视为限制性。同样,应当理解,本文中列举的任何数值范围意在包括其中包含的所有子范围。举例来说,“1至10”的范围意在包括在(并且包括)所列举的最小值1和所列举的最大值10之间的所有子范围,即,具有等于或大于1的最小值和等于或小于10的最大值。

[0082] 如本文中所使用的,术语“通信(communication)”和“通信(communicate)”是指一个或多个信号、消息、命令或其他类型的数据的接收或转移。对于一个单元(例如,任何设备、系统或其部件)要与另一个单元进行通信意味着所述一个单元能够直接地或间接地从另一个单元接收数据和/或将数据传输到另一个单元。这可以是指本质上是有线和/或无线的直接或间接连接。另外,即使可以在第一单元与第二单元之间修改、处理、中继和/或路由所传输的数据,两个单元也可以彼此通信。举例来说,即使第一单元被动地接收数据并且没有主动地将数据传输到第二单元,第一单元也可以与第二单元通信。作为另一示例,如果中间单元处理来自一个单元的数据并且将所处理的数据传输到第二单元,那么第一单元可以与第二单元通信。将了解到,许多其他布置是可能的。

[0083] 如本文中所使用的,术语“数字资产”是指以电子数字形式存在的价值单位,例如但不限于加密货币单位、许可证密钥、智能合约和/或诸如此类。“数字资产交易所”和“数字资产交换系统”是指被配置为管理和控制数字资产的一个或多个计算设备。

[0084] 如本文中所使用的,术语“加密货币”是指其中使用加密技术来创建和调节其分配的数字货币。在一些非限制性示例中,在没有中央权威(例如,金融机构)充当中介的情况下,在去中心化的区块链网络中维护、转移和创建加密货币。加密货币可以包括比特币、以太坊、XRP、比特币现金、莱特币、大零币和/或其他数字货币。

[0085] 如本文中所使用的,术语“zkSNARK”(零知识简洁的非交互式知识论证)是指具有简洁性属性的关系R的知识的非交互式零知识论证,这意味着对于任何s和w,证明的长度 π 由 $|\pi| = \text{多项式}(\kappa) \text{多对数函数}(|s| + |w|)$ 给出。

[0086] 如本文中所使用的,术语“西格玛协议”是指具有以下结构的两方交互式协议。让P(证明者)和V(验证者)是具有共同输入s和用于P的私有输入w的两方。在西格玛协议中,P发送消息a,V回复随机的 κ 位字符串r,P然后发送消息e,并且V基于抄本(a,r,e)而决定接受或拒绝。如果满足以下属性,那么证明者P和验证者V之间的西格玛协议是关系R的 Σ 协议:(1)它是三步公共硬币协议;(2)完整性:如果P和V遵循协议,那么每当 $(s,w) \in R$ 时, $\Pr[\langle P(w), V \rangle(s) = 1] = 1$;(3)特殊可靠性:存在被称为提取器的多项式时间算法,当给定s以及接受s的两个抄本(a,r,e)和(a,r',e')时,其中 $r \neq r'$,所述多项式时间算法输出w',使得 $(s,w') \in R$;和(4)特殊诚实验证者零知识:存在多项式时间模拟器,所述多项式时间模拟器在输入s和随机r上输出抄本(a,r,e),具有与在(共同)输入s上由P与V之间的诚实交互所生成的概率分布相同的概率分布。

[0087] 如本文中所使用的,术语“承诺”是指基于一个或多个输入而生成的值,使得可以在不揭露一个或多个输入的情况下发布所述值。举例来说,基于输入生成承诺可以涉及用一个或多个哈希或椭圆曲线算法处理该输入。在一些示例中,承诺可以由如由x和y坐标标识的沿着曲线的点表示。如本文中所使用的,函数“Com(x)”被用于标示对变量x的承诺。

[0088] 如本文中所使用的,术语“零知识算法”是指被配置为验证系统或实体具有对一个或多个值的知识或对其进行访问的一个或多个函数、过程和/或计算,例如但不限于与非对称密码学中的公共密钥相对应的私有密钥。零知识算法可以包括验证系统可以用两侧上的给定输入进行计算的证明。

[0089] 本发明的非限制性实施方案可以在包括至少一个处理器的一个或多个计算设备(例如但不限于一个或多个服务器、计算机、移动设备和/或诸如此类)上实现。如本文中所使用的,术语“证明系统”和“证明计算机”是指由用户或实体操作的试图证明其有权访问秘密密钥或秘密信息的一个或多个计算设备。术语“验证系统”和“验证计算机”指的是由用户或实体操作的试图验证证明系统具有秘密密钥或秘密信息而自身无权访问它的一个或多个计算设备。将了解到,各种其他实施方式是可能的。

[0090] 非限制性实施方案减少了执行用于复合计算语句的零知识算法所需的计算资源。通过生成对秘密值的承诺并且生成零知识算法的第一和第二组成部分,系统的非限制性实施方案提供了零知识算法,所述零知识算法可以由验证系统在给定承诺作为输入/输出的情况下以有效方式并且使用比其他零知识算法少的处理周期执行,所述其他零知识算法没有用第一组成部分和第二组成部分构建并且被配置为使用承诺。举例来说,在用于确定数字资产交易所的偿付能力的系统的非限制性实施方案中,改进的零知识算法允许用户使用标准计算机作为验证系统以有效地验证数字资产交易所的偿付能力,并且用户余额包括在数字资产的总数量中。作为另一个示例,在用于生成和验证匿名数字签名的系统的非限制

性实施方案中,改进的零知识算法允许用户使用标准计算机作为验证系统来有效地验证数字签名,而无需访问私有密钥或基础消息。

[0091] 具体参考图1,并且在一个优选并且非限制性实施方案或方面中,提供了一种用于生成复合语句的零知识算法的系统和方法100。特别地,描绘了是代数函数($g^x=y$)和布尔函数($H(y)=h$)的混合的复合语句,所述复合语句可以被用于证明数字资产交易所的偿付能力。如图所示,存在私有密钥102“x”,其对应一个或多个公共密钥104“ g^x ”或“y”。在比特币的上下文中,私有密钥102可以是256位数字(尽管一些实施方式可以在128与512位之间使用)。通常通过椭圆曲线转换从私有密钥102导出公共密钥104。在比特币的上下文中,公共密钥104可以是65个字节的数字,包括对应于椭圆曲线的“X”坐标整数的32个字节和对应于椭圆曲线的“Y”坐标整数的32个字节。西格玛协议ZKP 106可以被用于证明加密货币交易所知道(并且大概控制)与公共密钥104相对应的私有密钥102。西格玛协议ZKP 106函数的输出可以用作哈希算法110的输入108。在比特币的上下文中,公共密钥104可以至少经历SHA-256哈希以生成哈希输出114。zkSNARK ZKP 112可以被用于证明加密货币交易所知道(并且大概控制)与哈希输出114相对应的公共密钥104。本发明提供了单独的ZKP,以显示出代数ZKP 106的输出是布尔ZKP 112的输入108。以这种方式,两个ZKP可以通过有效的ZKP进行分层,所述ZKP不会揭露将函数互连的基础值。复合语句可以是函数的任何合适的组合或混合,例如,代数-代数、算术-代数、代数-算术、算术-算术和/或诸如此类。将了解到,ZKP的其他配置是可能的。

[0092] 系统的非限制性实施方案提供了计算语句的生成,所述计算语句包括AND、OR以及代数和算术组成部分的混合的函数组合物。非限制性实施方案提供新的NIZK以用于 x 、 x_1 、 x_2 、 y_1 、 y_2 的知识的证明,使得:

[0093] • $f_1(x_1, f_2(x_2)) = z$

[0094] • $f_1(x, y_1) = z_1$ 并且 $f_2(x, y_2) = z_2$

[0095] • $f_1(x, y_1) = z_1$ 或 $f_2(x, y_2) = z_2$

[0096] 对于公共值 z , z_1 , z_2 , 并且其中 f_1 和 f_2 可以是代数或算术的。对这些组合物使用根据非限制性实施方案的NIZK技术允许系统处理任意复合语句。

[0097] 非限制性实施方案提供了证明系统以证实在西格玛协议中用于代数语句的输入/输出与由代数承诺方案(例如,“Com”)承诺的输入/输出相同。这使得能够将代数语句的输出用作复合语句中的中间输出。举例来说,证明系统可以示出它有权访问 h 、 x_1 、 x_2 ,使得 $h = g_1 x_1 - g_2 x_2^2$ 给定 g_1 、 g_2 、 $\text{Com}(h)$ 、 $\text{Com}(x_1)$ 、 $\text{Com}(x_2)$ 。为了做到这一点,证明系统通过承诺其坐标(即, $\text{Com}(P) = (\text{Com}_q(P_x), \text{Com}_q(P_y))$)来生成对椭圆曲线 $E(F_t)$ 上的点 P 的承诺,其中 $P = (P_x, P_y)$ 并且 $q > t$ 。

[0098] 在非限制性实施方案中,系统证明访问(例如,知道)两个确定的椭圆曲线点 P 、 Q ,使得对于公共点 T 而言 $T = P + Q$ 。为了做到这一点,系统扩展椭圆曲线加/减运算 $P + Q - T$,使得如果并且仅如果维持形式为 $L(\cdot) = R(\cdot)$ 的两组方程式,那么 $T = P + Q$,其中 L 和 R 在坐标中是3次多元多项式。给定对坐标值的承诺以及多项式 L 和 R 的输出,系统使用西格玛协议证明所承诺值之间的相对对应关系。然而,在椭圆曲线点上的加法运算是在 F_t 上定义的,而承诺方案可以在大小为 q 的不同组上定义。虽然可以通过在不同顺序的组中使用两个不同的承诺方案来解决这个差异,但其将需要执行复乘方法来选择特定顺序的椭圆曲线组,这效率低

下并且浪费计算资源。这种方法还可以适用于其中T也是私有并且被承诺的情况。

[0099] 证明系统的非限制性实施方案利用椭圆曲线组的双离散对数证明。举例来说,证明系统生成对组元素gx的承诺,其中g是椭圆曲线组的生成器,并且证明对x的访问,使得 $\text{Com}(gx) = y$ 给定公共y。这样的方法不仅限于RSA组,所述RSA组将不适用于比特币,因为比特币协议利用椭圆曲线组。证明系统的非限制性实施方案证明了在不同椭圆曲线组上的所承诺值的相等性,使得系统可以证明对x的访问,使得针对公共值y、z, $\text{Com}_p(x) = y$ 并且 $\text{Com}_q(x) = z$, 其中 Com_p 标示大小为p的椭圆曲线组的代数承诺(类似地, Com_q)。通过承诺两个组中的共享值并且调用证明,这种方法使得证明系统能够有效地将一个组中的证明系统转移到另一组,借此避免处理密集型指数运算。

[0100] 现在参考图2,示出了根据非限制性实施方案的数字资产交换偿付能力系统2000。系统2000包括交换系统202,交换系统202可以包括持有与多个用户的区块链地址相对应的私有密钥的加密货币交换。在这个示例中,交换系统202充当证明系统,并且包括一个或多个处理器、用于存储用户的私有密钥的安全数据存储设备206和分布式分类账208。系统2000还包括各自托管分布式分类账208的多个分布式节点214、216。将了解到,在一些实施方案中,许多节点214、216可以托管分布式分类账208,并且交换系统202可以不托管分布式分类账208。在图2中所示的示例中,交换系统202和节点214、216是区块链网络的节点。在比特币区块链或其他公共区块链的示例中,可能存在大量节点。安全数据存储设备206可以利用各种形式的加密和安全存储机制来保护存储在其中的敏感私有密钥不被访问或破坏。

[0101] 继续参考图2,用户设备211充当验证系统,并且访问交换系统202以检查用户的余额,交易数字资产,以法定货币或加密货币存款,提取数字资产和/或诸如此类。用户设备211可以经由网络210(例如,因特网)访问交换系统202,并且通过在用户设备211上显示的一个或多个图形用户界面(GUI) 212与一个或多个数字资产交互。通过GUI 212,用户可以请求交换系统202验证其自身的偿付能力,并且确认交换系统202持有与其总数字资产相对应的私有密钥。在管理和调节比特币加密货币和其他加密货币(例如,比特币现金,通过比特币区块链网络中的分支)的比特币区块链网络的情况下,交换系统202持有与唯一地对应于用户的公共密钥相对应的私有密钥。用户的公共密钥可以由用户保守秘密。然而,因为分布式分类账208用用户的公共密钥的哈希而不是公共密钥本身来标识用户的区块链地址。

[0102] 交换系统202证明,它控制着足够的准备金以结算每个客户的账户,使得如果交换在一次攻击中损失了大量数字资产,那么交换将不能够提供证明其偿付能力的计算语句。因此,客户将迅速发现有关攻击并且采取必要的措施。在比特币的交换的示例中,比特币地址是公共/私有ECDSA密钥对的公共部分的160位哈希,其中公共部分是通过通过对secp256k1曲线进行幂运算从私有密钥导出的。因为比特币地址不揭露公共密钥/私有密钥对的公共密钥,而是仅揭露哈希,所以比特币地址可以保持匿名。因此,为了证明其偿付能力,交易所想要证实其知道与一些哈希公共密钥相对应的私有密钥在区块链上可用,并且匿名这样做,必须这样做,而不揭露客户的公共/私有密钥对的私有密钥或公共密钥。通过将公共密钥保密,对手或潜在的加密货币小偷无法追踪交易所资金的动向。

[0103] 为了证明其偿付能力,交换系统202需要向其客户和/或监管者(例如,验证系统211)证明其知道秘密x,使得 $H(gx) = y$,其中H是哈希函数,例如,SHA-256。语句具有代数(gx)和布尔(哈希函数H)组成部分,其中代数组成部分与私有密钥和公共密钥相关,并且布

尔组成部分与公共密钥和哈希公共密钥相关。交换系统202被配置为执行三个主要任务以证明其偿付能力：(1) 允许客户(验证系统211) 验证他们的账户被包括在总数中的负债证明；(2) 所述资产证明示出交易所具有一定量的准备金的资产证明；和(3) 准备金在可接受的程度上覆盖负债的证明。

[0104] 在交易所正在证明比特币准备金的偿付能力的非限制性示例中，将示出交换系统202如何可以执行这三个主要任务中的每一个的示例，但是将了解，针对其他密码货币和数字资产，可以利用类似的方法。在下面的示例中，让 g, h 是顺序 q 的组 G 的固定公共生成器。对于比特币公共密钥 y ， $x \in Z_q$ 是相对应的秘密密钥，使得 $y = gx$ 。在被配置为提供资产证明的零知识算法的第一组成部分中，对于组元素 $k = (k_x; k_y)$ ， $\text{Com}(k)$ 表示对坐标 k 的生成承诺，即， $\text{Com}(k) = (\text{Com}(k_x), \text{Com}(k_y))$ 。相对应于密钥 y 的比特币地址由 $h = H(y)$ 给出，其中 H 将 y 哈希处理为更紧凑的表示形式。与比特币地址 h 相关联的余额由 $\text{bal}(h)$ 表示。

[0105] 交换系统202生成零知识算法的组成部分，所述组成部分被配置为通过首先生成对其总资产的承诺连同交易所知道其总值等于所承诺值的一组比特币地址的私有密钥的零知识证明一起来证明交换系统202具有足够的资产。为了做到这一点，交易所创建了一组哈希PK以用作匿名组：来自区块链上可用的公共数据的 $\text{PK} = \{h_1, \dots, h_n\}$ 。在这个示例中， $x_1, \dots, x_n$ 是指相对应的秘密密钥，使得 $h_i = H(gx_i)$ ， s_i 指示交易所是否知道第 i 个秘密密钥。总资产可以表达为 $\text{资产} = \sum_{i=1}^n s_i \cdot \text{bal}(h_i)$ 。对于所有 $i \in [1, n]$ ，区块链上可用的公数据是 $h_i = H(y_i)$ ， $p_i = g \cdot \text{bal}(h_i)$ 。

[0106] 由一个或多个处理器生成并且用作零知识算法的组成部分的以下计算语句证明交换系统202控制着足够的资产：

[0107] (1) 交换系统202生成承诺。对于 $i \in [1, n]$ ，交换系统通过发布 $\alpha_i = \text{Com}_q(x_i) = gx_i$ 和 r_i 对 x_i 作出承诺，并且通过发布 $\beta_i = \text{Com}_q(y_i)$ 对 y_i 作出承诺。

[0108] (2) 交换系统202通过发布 $u_i = \text{Com}_q(s_i \cdot \text{bal}(h_i)) = gs_i \cdot \text{bal}(h_i) \cdot ht_i$ ， $s_i \in \{0, 1\}$ ，对它控制的公共密钥的每个地址中的余额和以其他方式对0作出承诺，其中，如果交换系统知道 x_i ，那么 $s_i = 1$ ，使得 $y_i = gx_i$ 。

[0109] (3) 交换系统202分别使用协议 ddlog 、 comIOSnark 以及用于函数组合物和OR组合物、组合物和复合OR的建构，以针对每个 i 证明以下内容：

$$[0110] \quad \pi_i : PK \left\{ (x_i, y_i, s_i, r_i, a_i, b_i, t_i) : \begin{pmatrix} \alpha_i = \text{Com}_q(x_i) \wedge \beta_i = \text{Com}_q(y_i) \wedge \\ u_i = \text{Com}_q(s_i \cdot \text{bal}(h_i)) \wedge f_1(f_2(x_i), h_i) = s_i \wedge s_i = 1 \end{pmatrix} \vee (s_i = 0) \right\}$$

[0111] 其中 $f_2(x) = g^x$ ，并且

$$[0112] \quad \underline{f_1(y, h) = \begin{cases} 1 & \text{if } H(y) = h \\ 0 & \text{otherwise.} \end{cases}}$$

[0113] (4) 交换系统202生成并且发布 $Z_{\text{资产}} = \prod_{i=1}^n u_i$ 。

[0114] 交换系统202还生成零知识算法的组成部分，所述组成部分被配置为证明交换系统已经对其总负债作出承诺，并且每个客户的相应余额包括在该总承诺中。交易所可以将每个客户映射到表示交易所系统的负债(例如，负债列表)的数据结构中的条目(例如，标识符)。举例来说，可以为每个客户提供标识符，例如，账号、用户名、电子邮件地址和/或诸如

此类,并且交换系统利用基于哈希承诺方案来对那些客户标识符作出承诺。

[0115] 为了确保任何被包括的用户只能加到交易系统的总负债,交易系统202生成零知识算法,以证明每个所承诺余额落在0与最大 $=2^{51}$ 之间的区间内。关于所承诺的输入由zk-SNARK的非限制性实施方案提供的协议允许在不使用按位承诺(这促成大的证明大小)的情况下使用电路来检查范围。零知识算法的以下组成部分(所述组成部分包括由交易系统202生成的计算语句)允许交易系统202对其总负债ZLiab可验证地作出承诺,并且说服客户其余额包括在ZLiab中。对于这个示例,让C是电路,所述电路将m个位整数 $x_1, \dots, x_n$ 看作输入,并且如果对于所有i, $x_i < \text{最大值}$,则输出1,并且否则输出0:

[0116] (1) 交换系统202通过发布 $c_i = \text{Com}_q(x_i) = g^{x_i} h^{r_i}$ 对每个客户 C_i 的余额 x_i 作出承诺。

[0117] (2) 交换系统202使用协议 comInSnark 来证明,对于所有客户, $x_i < \text{最大值}$ 。 $\pi: \text{PK} \{ (x_i, r_i) : C(x_1, \dots, x_n) = 1 \wedge c_i = \text{Com}_q(x_i) \}$ 。

[0118] (3) 交换系统202通过选择随机随机数并且计算 $\text{CID}_i = H(\text{用户}_i || n_i)$ 来计算每个客户的客户标识符,其中 $n_i \in \{0, 1\}^{512}$, 用户_i 是第i个客户的用户名,并且H是抗碰撞哈希函数。

[0119] (4) 交换系统202发布所有客户元组的负债列表: $\text{ListLiab} = (\text{CID}_1, \dots, \text{CID}_n, c_1, \dots, c_n, \pi)$ 。

[0120] 每个验证系统211被私有地给出 (r_i, n_i) ,并且验证系统计算CID并且验证包括在负债列表中;客户检查其自己的余额,并且通过计算 $c_i = g^{x_i} h^{r_i}$ 包括在内;验证系统验证证明 π ;并且每个验证系统计算 $Z_{\text{Liab}} = \prod_{i=1}^n c_i$ 。

[0121] 一旦交换系统202生成零知识算法的组成部分,所述组成部分被配置为证明交换系统的总资产和总负债,交换系统202就生成零知识算法,所述零知识算法被配置为通过证明 $Z_{\text{资产}}/Z_{\text{Liab}}$ 是对0的承诺来证明交换系统是具有偿付能力的。举例来说,计算语句可以是:

$\pi: \text{PK} \{ (R) : Z = hR \}$, 其中 $Z = Z_{\text{资产}} Z_{\text{Liab}}^{-1}$ 。

[0122] 现在参考图3,示出了根据非限制性实施方案的用于确定数字资产交易所的偿付能力的方法。作为第一步骤300,交换系统标识其控制的多个区块链地址。作为示例,交换系统可以标识与由交换系统202维护的多个公共/私有密钥对中的每一个相对应的多个公共区块链地址。作为示例,区块链地址可以包括哈希公共密钥,以维护公共密钥和私有密钥两者的保密性。此外,在步骤300中,交换系统可以为其控制相对应的密钥的每个公共区块链地址生成哈希集。哈希集用作来自区块链网络上可用的公共数据(例如,对于所有 $i \in [1, n]$, $h_i = H(y_i)$, $p_i = g^{h_i}$)的匿名集($\text{PK} = \{h_1, \dots, h_n\}$)。

[0123] 继续参考图3,在下一步骤302处,交换系统确定与多个区块链地址相关联的数字资产的总量。可以依据区块链网络中的公共分布式分类账确定数字资产的总量。在步骤304处,交换系统生成对数字资产的总量的承诺。在步骤306处,交换系统为交换系统的每个用户生成对每个个别用户余额的承诺。如本文中所解释的,交换系统可以生成承诺作为沿着椭圆曲线或通过哈希承诺协议的点。在步骤308处,交换系统生成零知识算法的第一组成部分,所述第一组成部分被配置为证明交换系统具有对与每个区块链地址相对应的每个公共密钥的控制。因为区块链地址可以是公共密钥的哈希,所以这样的编程函数涉及布尔函数。

在非限制性实施方案中,零知识算法的第一组成部分包括zkSNARK语句,所述zkSNARK语句接收总资产的承诺作为输入。

[0124] 在步骤310处,交换系统生成零知识算法的第二组成部分,所述第二组成部分被配置为证明每个用户余额包括在与交换系统控制的多个区块链地址相对应的资产总量中。因为余额可归因于通过椭圆曲线密码学致使匿名的个别用户,所以这样的编程函数涉及代数函数。在非限制性实施方案中,零知识算法的第二组成部分是西格玛协议语句,所述西格玛协议语句接收至少对用户余额的承诺作为输入。

[0125] 仍然参考图3,在步骤312处,交换系统基于零知识算法确定其偿付能力。交换系统还可以向验证系统提供零知识算法,使得验证系统能够确定交换系统是具有偿付能力的。这样的确定可以涉及确定总资产和总负债均等于对零(0)的承诺。零知识算法被配置为通过证明 π 来证明交换系统的偿付能力: $PK\{(R): Z=hR\}$,其中 $Z=Z_{资产}/Z_{Liab}$ 。在这个示例证明中, $Z_{资产}$ 是对数字资产交易所的总资产的承诺,并且 Z_{Liab} 是对数字资产交易所的总负债(例如,用户余额)的承诺。

[0126] 在非限制性实施方案中,可以匿名地生成和使用数字证书,使得可以使用零知识算法来验证匿名证书。举例来说,用户可以从组织或证书颁发机构获得凭证,并且稍后向验证系统证明已经给了她适当的凭证。用户的凭证可以含有一组属性,并且验证系统可以要求用户证明她凭证中的属性满足特定策略。特别地,数字证书(例如但不限于X.509证书)可以包括消息 m ,所述消息可以含有关于用户或机器的各种标识信息以及消息上证明其真实性的数字签名(由证书颁发机构)。然后,持有与被用于生成数字签名的私有密钥相对应的公共验证密钥的任何人都可以验证数字签名。在现有的系统和方法中,数字证书揭露消息 m ,并且因此揭露所有者的身份。

[0127] 为了提供匿名凭证,不能揭露消息。使用匿名凭证依赖于消息 m 的知识的ZKP和签名 σ ,其中 σ 是消息 m 相对于验证密钥 vk 的有效签名。在这样的实施方案中,消息 m 在被代数签名之前被哈希(例如,RSA或椭圆曲线运算)。为了避免对仅使用zkSNARK并且因此对于代数组成部分效率低下或者是交互式的(例如,要求证明系统和验证系统交换多个消息)的这种混合语句的证明,zkSNARK和西格玛协议两者的使用产生计算资源的效率。非限制性实施方案通过避免代数语句的资源密集型电路表示提供了与现有技术相比少了八(8)倍的组幂运算。

[0128] 在非限制性实施方案中,匿名数字证书系统包括一个或多个处理器,所述一个或多个处理器被配置为生成零知识算法,所述零知识算法涉及代数关系(用于幂运算)和基于电路的语句(用于哈希函数)。以这种方式,幂运算不需要基于电路的语句,在这个示例中,所述幂运算是使用RSA算法加密的数字签名。因此,在给定消息 m 的哈希摘要(例如,SHA哈希摘要)、候选RSA签名 σ 和RSA模数 N 的情况下,验证涉及检查是否 $\sigma^e \bmod n = h$,其中, h =填充(SHA(m)))。由一个或多个处理器生成的以下计算语句基于RSA签名而实现凭证的隐私保护验证:

[0129] (1) 对于 $p < n$,证明系统通过计算 $c_1 = \text{Comp}_p(m)$, $c_2 = \text{Comp}_p(h)$, $c_3 = \text{Comp}_n(\sigma)$, $c_4 = \text{Comp}_n(h)$ 对消息 m 、摘要 h 和签名 σ 作出承诺。

[0130] (2) 给定 c_1 和 c_2 ,证明系统使用zk-comIOSnark给出哈希摘要正确的证明:

[0131] $PK\{(m, h, r_1, r_2): \text{填充}(\text{SHA}(m)) = h \wedge c_1 = \text{Comp}_p(m) \wedge c_2 = \text{Comp}_p(h)\}$ 。

[0132] (3) 证明系统使用西格玛协议来证明对所承诺值第 e 个根的知识:

[0133] $PK\{(h, \sigma, r_2, r_3) : \sigma e \bmod n = h \wedge c_2 = \text{Com}_n(h) \wedge c_3 = \text{Com}_n(\sigma)\}$ 。

[0134] (4) 证明系统使用协议 E_q 来证明承诺 c_2 和 c_4 是相同值:

[0135] $PK\{(h, h', r_2, r_4) : c_2 = \text{Com}_p(h) \wedge c_4 = \text{Com}_n(h') \wedge h = h' \bmod p\}$ 。

[0136] 利用上面的处理技术的验证过程基于现有基础结构(如标准RDA-PSS、RSA-PKCS和/或诸如此类)提供了有效的隐私保护验证。本领域技术人员将了解,也可以使用其他数字签名算法和模式。

[0137] 现在参考图5,示出了根据非限制性实施方案的匿名数字证书系统5000。验证系统502与验证系统504通信。将了解,证明系统502和验证系统504可以是任何类型的计算设备中的一个或多个,例如,服务器计算机、移动设备和/或诸如此类。证明系统502有权访问存储在安全数据存储设备506中的秘密私有密钥和消息。证明系统通过根据散列函数对消息进行哈希处理并且通过应用一个或多个密码运算(例如,RSA或椭圆曲线算法)用私有密钥对哈希消息进行签名来生成匿名数字签名510。证明系统502将匿名数字签名510传递给验证系统504。验证系统可以有权访问哈希消息,或者在一些示例中,证明系统502可以将哈希消息传递给验证系统。

[0138] 继续参考图5,证明系统502通过至少一个网络环境500与验证系统通信。将了解到,证明系统502可以以安全的方式通信以便保持匿名。在一些示例中,证明系统502可以通过中间系统(图5中未示出)与验证系统504仅间接地通信以保持匿名性。证明系统502生成对消息和私有密钥的承诺,将承诺传递给验证系统504,并且生成零知识算法,所述零知识算法被配置为便于验证系统504在没有访问消息或私有密钥的情况下验证匿名数字签名510。验证系统504接收该数据并且执行零知识算法,以在给定承诺和公共密钥的情况下验证匿名数字签名510。

[0139] 现在参考图4,示出了根据非限制性实施方案的用于生成和验证匿名数字签名的方法。在第一步骤400处,证明系统生成消息 m 的哈希。消息 m 可以标识用户或用户可能想要保密的其他可标识信息,同时仍然能够验证用户拥有与公共密钥相对应的私有密钥。在下一步骤402处,证明系统通过使用非对称加密算法用私有密钥对哈希消息进行数字签名来生成匿名数字签名。在步骤404处,证明系统生成对消息 m 的承诺。如本文中所解释的,交换系统可以生成承诺作为沿着椭圆曲线或通过哈希承诺协议的点。在步骤406处,证明系统将匿名数字签名传递给验证系统,但是将了解,数字签名可以在其生成之后的任何时间传递。

[0140] 在步骤408处,证明系统生成零知识算法的第一组成部分,所述第一组成部分被配置为证明证明系统具有消息的知识。因为已知变量是哈希消息,所以这样的编程函数涉及布尔函数。在非限制性实施方案中,零知识算法的第一组成部分包括zkSNARK语句,所述zkSNARK语句接收消息的承诺作为输入。在步骤410处,证明系统生成零知识算法的第二组成部分,所述第二组成部分被配置为证明证明系统具有对私有密钥的知识并且有权访问私有密钥。因为哈希消息是使用椭圆曲线密码学技术进行数字签名的,所以这样的编程函数涉及代数函数。在非限制性实施方案中,零知识算法的第二组成部分是西格玛协议语句,所述西格玛协议语句接收至少对私有密钥的承诺作为输入。

[0141] 仍然参考图4,在步骤412处,证明系统生成零知识算法以传递给验证系统,使得验证系统可以验证证明系统有权访问私有密钥和消息。zkSNARK和西格玛协议语句的组合允

许生成复合计算语句作为零知识算法的一部分,所述零知识算法对资源有效并且使用承诺作为输入。

[0142] 现在参考图6,示出了根据非限制性实施方案的用于验证对秘密值的访问或知识的方法。可以在其中证明系统试图证明对值的访问或知识,同时保持值和任何标识信息秘密的任何数量的用例和场景中使用图6中所示的方法。在第一步600处,证明系统生成对秘密价值的承诺。在第二步骤602处,用布尔函数处理值。举例来说,可以用哈希函数处理值。在步骤604处,通过代数函数(例如,椭圆曲线函数)来处理哈希值。在步骤606处,将最终结果(对哈希值执行代数函数的乘积)连同承诺一起传递到验证系统。

[0143] 继续参考图6,在步骤608处,证明系统生成零知识算法的第一组成部分,所述第一组成部分与在步骤602处应用的布尔函数相对应。作为示例,第一组成部分可以包括zkSNARK语句。在步骤610处,证明系统生成零知识算法的第二组成部分,所述第二组成部分与在步骤604处应用的代数函数相对应。作为示例,第二组成部分可以包括西格玛协议语句。给定在步骤600处生成的承诺,零知识算法的第一组成部分和第二组成部分被用于建构零知识算法。在步骤612处,由验证系统执行零知识算法,以确定在步骤604处使用的椭圆曲线函数的输出是否等于在步骤602处使用的布尔函数的输入。零知识算法允许这由具有生成的承诺的验证系统来执行。如果验证系统在步骤612处执行零知识算法并且确定证明完成,那么方法继续进行到步骤614,在步骤614中验证系统验证结果。如果验证系统在步骤612处执行零知识算法并且确定证明没有完成,那么方法继续进行到步骤616,在步骤616中验证系统拒绝验证。

[0144] 尽管出于图示的目的基于目前认为最实用和最优选并且非限制性实施方案对本发明已经进行了详细描述,但将会理解,这样的细节仅仅是为了该目的,且本发明并不限于所公开的实施方案,而是相反,本发明意在涵盖在所附的权利要求书的精神和范围内的修改和等同布置。举例来说,将会理解,本发明预期在可能程度上任何实施方案的一个或多个特征可以与任何其它实施方案的一个或多个特征组合。

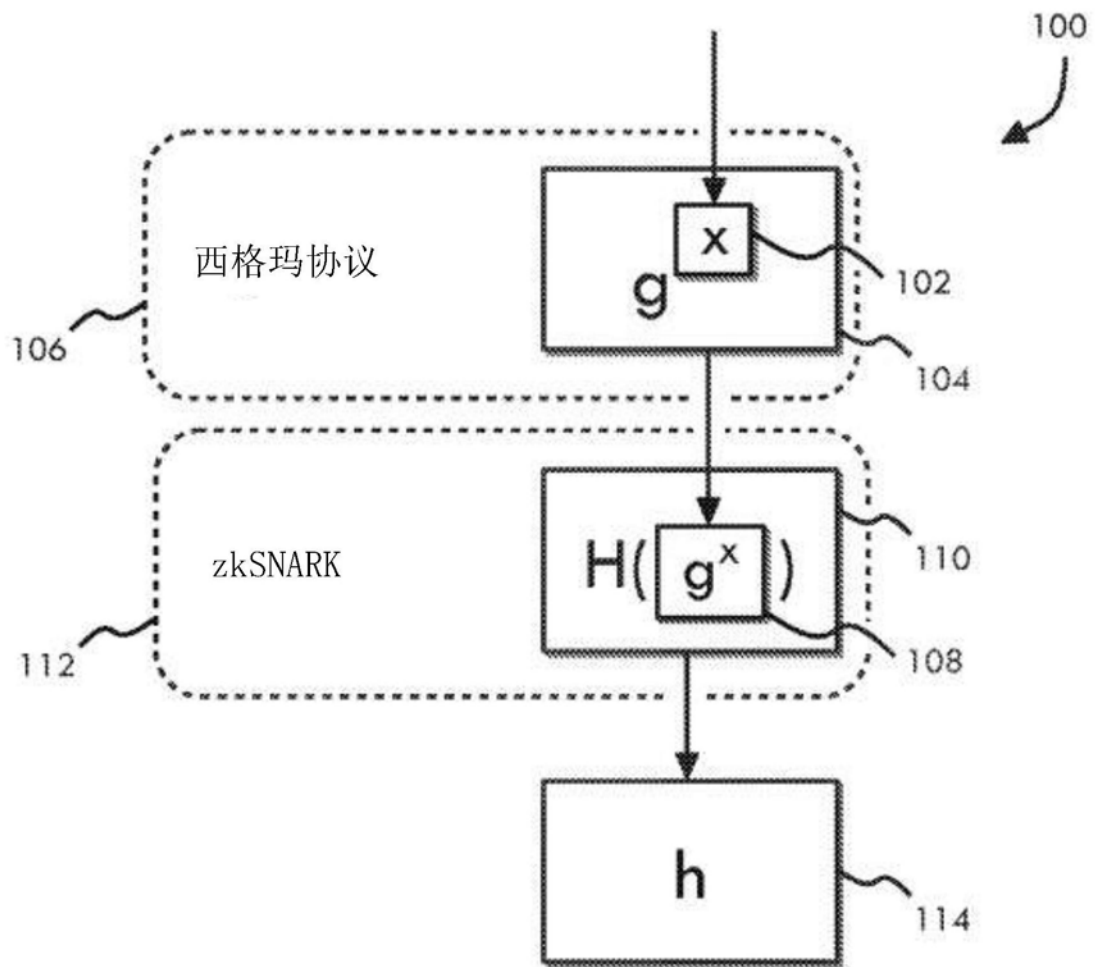


图1

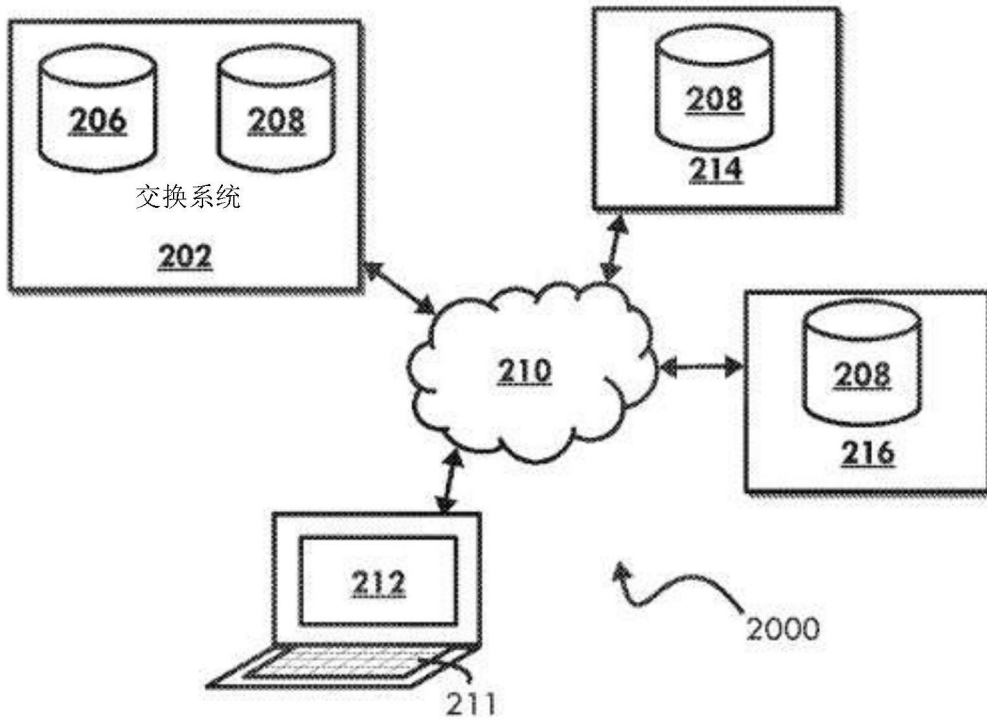


图2

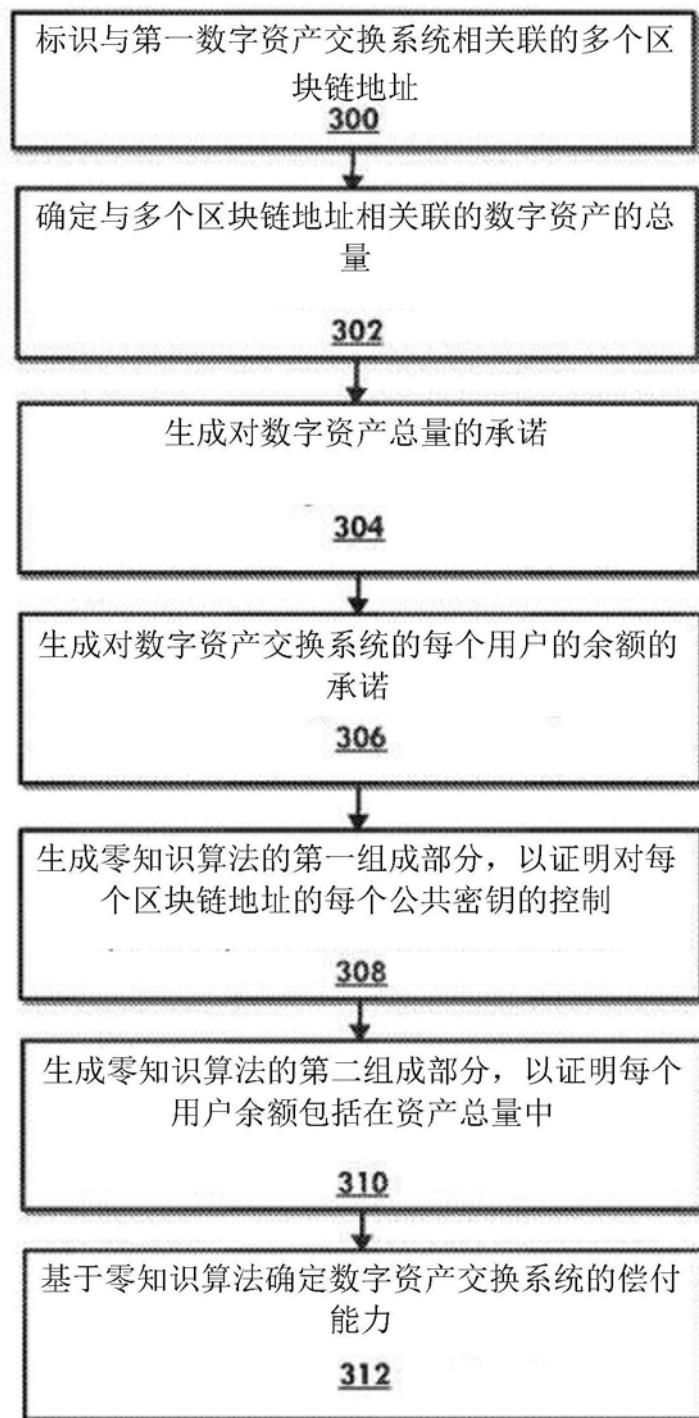


图3

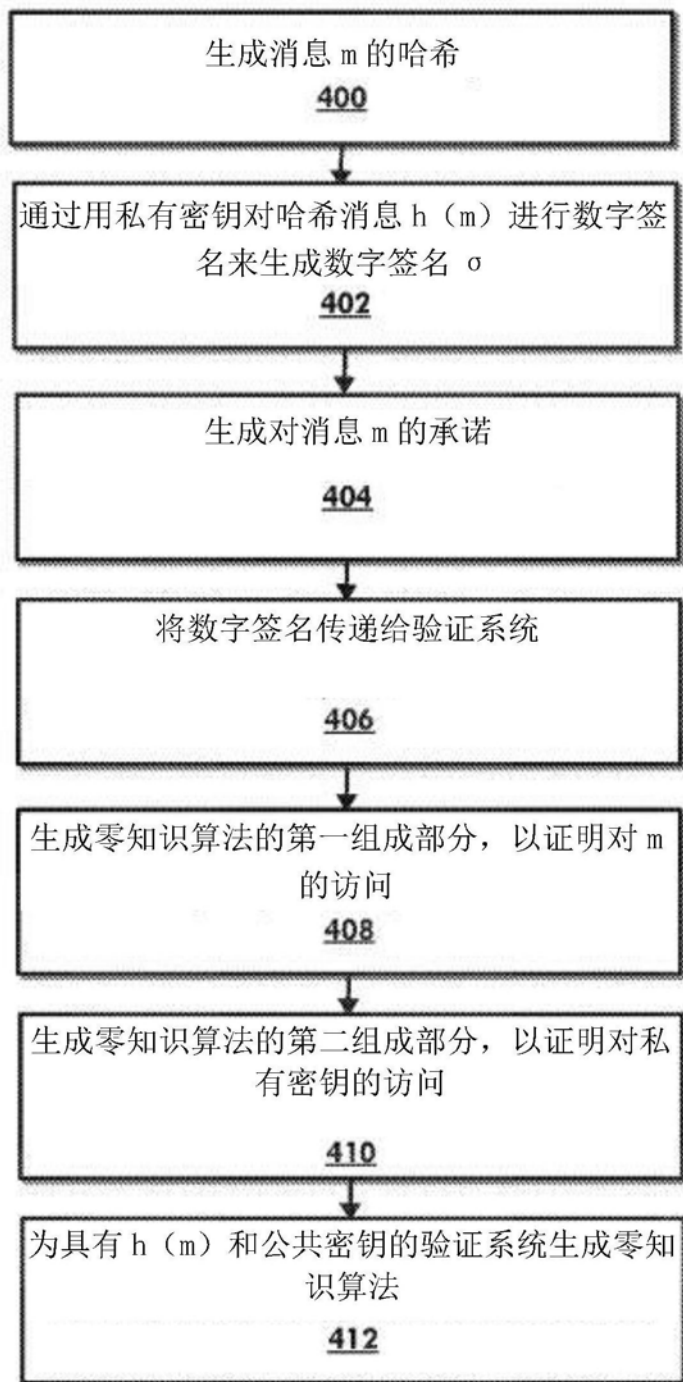


图4

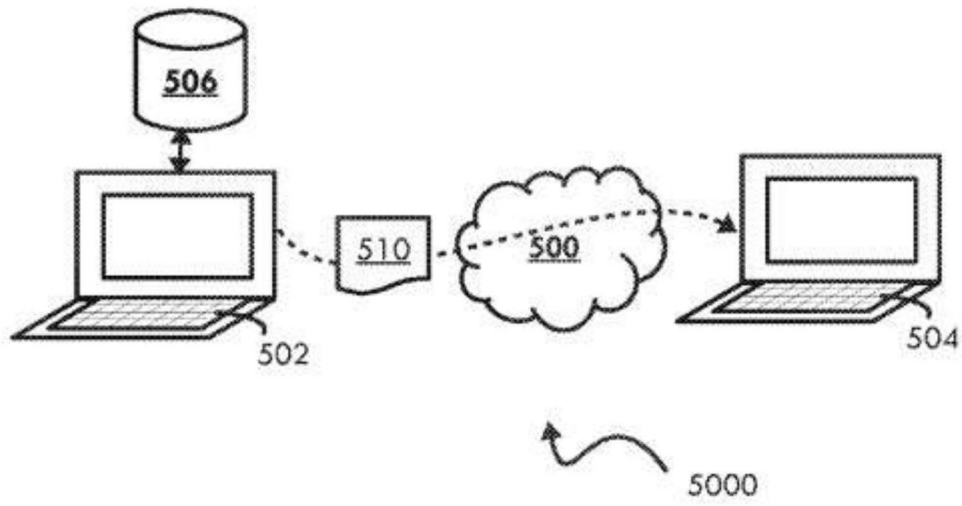


图5

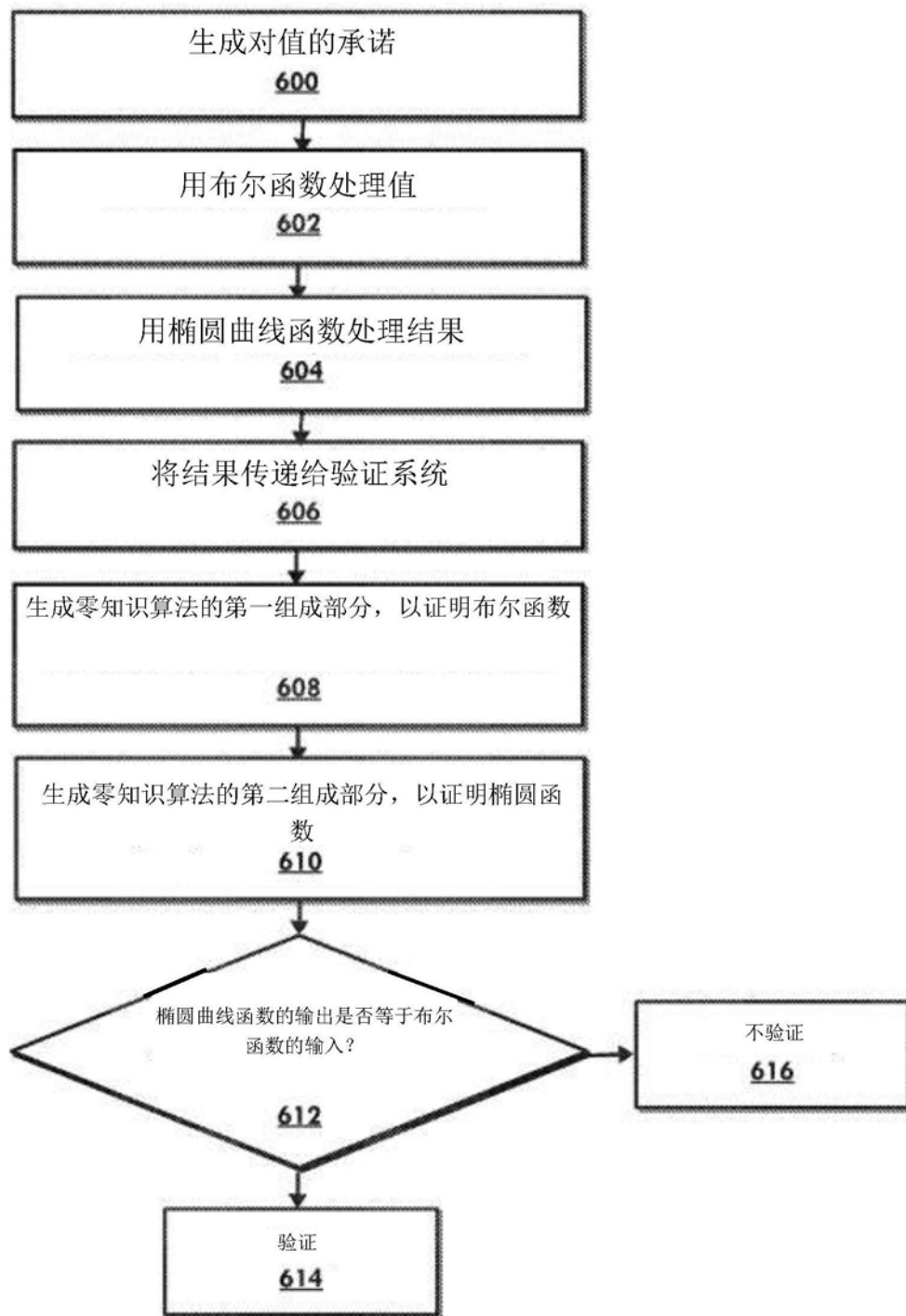


图6