



# (12)发明专利申请

(10)申请公布号 CN 109934709 A

(43)申请公布日 2019.06.25

(21)申请号 201811308520.3

(22)申请日 2018.11.05

(71)申请人 阿里巴巴集团控股有限公司

地址 英属开曼群岛大开曼

(72)发明人 李漓春 张文彬

(74)专利代理机构 北京三友知识产权代理有限公司

11127

代理人 李辉

(51)Int.Cl.

G06Q 40/04(2012.01)

G06F 21/62(2013.01)

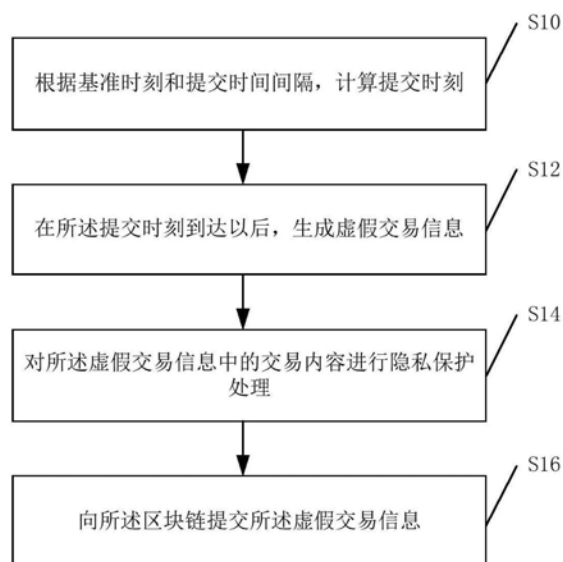
权利要求书2页 说明书9页 附图3页

## (54)发明名称

基于区块链的数据处理方法、装置和服务器

## (57)摘要

本说明书实施例提供一种基于区块链的数据处理方法、装置和服务器。所述方法包括：根据基准时刻和提交时间间隔，计算提交时刻；在所述提交时刻到达以后，生成虚假交易信息；对所述虚假交易信息中的交易内容进行隐私保护处理；向所述区块链提交所述虚假交易信息。



1. 一种基于区块链的数据处理方法,包括:  
根据基准时刻和提交时间间隔,计算提交时刻;  
在所述提交时刻到达以后,生成虚假交易信息;  
对所述虚假交易信息中的交易内容进行隐私保护处理;  
向所述区块链提交所述虚假交易信息。
2. 如权利要求1所述的方法,所述基准时刻包括以下至少一种:  
最近一次向所述区块链提交虚假交易信息的时刻;  
最近一次向所述区块链提交真实交易信息的时刻。
3. 如权利要求1所述的方法,所述生成虚假交易信息,包括:  
在不存在待提交的真实交易信息时,生成虚假交易信息。
4. 如权利要求1所述的方法,所述方法还包括:  
获取真实交易信息;  
对所述真实交易信息中的交易内容进行隐私保护处理;  
向所述区块链提交所述真实交易信息。
5. 如权利要求1所述的方法,所述提交时间间隔满足指数分布或爱尔郎分布。
6. 如权利要求1所述的方法,所述虚假交易信息中的交易内容包括以下至少一种:  
数值为0的交易金额;  
空白存证信息。
7. 如权利要求1所述的方法,在生成虚假交易信息的步骤中包括:  
获取账户标识作为所述虚假交易信息中的接收方账户标识。
8. 如权利要求7所述的方法,提供账户标识集合;所述账户标识集合包括至少一个接收方账户标识;每个接收方账户标识对应有基准交易比例;相应地,在获取账户标识的步骤中包括:  
获取发起方账户标识与所述账户标识集合中各个接收方账户标识之间的实际交易比例;  
从所述账户标识集合中选取实际交易比例小于或等于基准交易比例的接收方账户标识,作为所述虚假交易信息中的接收方账户标识。
9. 一种基于区块链的数据处理装置,包括:  
计算单元,用于根据基准时刻和提交时间间隔,计算提交时刻;  
生成单元,用于在所述提交时刻到达以后,生成虚假交易信息;  
加密单元,用于对所述虚假交易信息中的交易内容进行隐私保护处理;  
提交单元,用于向所述区块链提交所述虚假交易信息。
10. 一种服务器,包括:  
存储器,用于存储计算机指令;  
处理器,用于执行所述计算机指令实现以下步骤:根据基准时刻和提交时间间隔,计算提交时刻;在所述提交时刻到达以后,生成虚假交易信息;对所述虚假交易信息中的交易内容进行隐私保护处理;向区块链提交所述虚假交易信息。
11. 一种基于区块链的数据处理方法,包括:  
根据基准时刻和提交时间间隔,计算提交时刻;

在所述提交时刻到达以后,在不存在待被提交的真实交易信息时,生成虚假交易信息;对所述虚假交易信息中的交易内容进行隐私保护处理;向所述区块链提交所述虚假交易信息;

在存在待被提交的真实交易信息时,对所述真实交易信息中的交易内容进行隐私保护处理;向所述区块链提交所述真实交易信息。

12. 一种基于区块链的数据处理装置,包括:

计算单元,用于根据基准时刻和提交时间间隔,计算提交时刻;

第一提交单元,用于在所述提交时刻到达以后,在不存在待被提交的真实交易信息时,生成虚假交易信息;对所述虚假交易信息中的交易内容进行隐私保护处理;向所述区块链提交所述虚假交易信息;

第二提交单元,用于在存在待被提交的真实交易信息时,对所述真实交易信息中的交易内容进行隐私保护处理;向所述区块链提交所述真实交易信息。

13. 一种服务器,包括:

存储器,用于存储计算机指令;

处理器,用于执行所述计算机指令实现以下步骤:根据基准时刻和提交时间间隔,计算提交时刻;在所述提交时刻到达以后,在不存在待被提交的真实交易信息时,生成虚假交易信息;对所述虚假交易信息中的交易内容进行隐私保护处理;向所述区块链提交所述虚假交易信息;在存在待被提交的真实交易信息时,对所述真实交易信息中的交易内容进行隐私保护处理;向区块链提交所述真实交易信息。

## 基于区块链的数据处理方法、装置和服务

### 技术领域

[0001] 本说明书实施例涉及计算机技术领域,特别涉及一种基于区块链的数据处理方法、装置和服务。

### 背景技术

[0002] 区块链技术是一种分布式数据库技术,利用密码学和共识机制保证了数据的不可篡改和不可伪造。随着计算机和互联网技术的发展,区块链技术以其去中心化、公开透明、不可篡改、可信任等优点,备受青睐,在智能合约、证券交易、电子商务、物联网、社交通讯、文件存储、存在性证明、身份验证、股权众筹等众多场景得到广泛应用。

[0003] 目前,当将区块链技术应用于上述场景时,由于每笔交易的交易信息均需要发送到区块链进行验证、实施和上链,因而账户的交易笔数面临泄露给第三方的风险。

[0004] 出于保护隐私的考虑,业务亟需一种能够隐藏交易笔数的技术方案。

### 发明内容

[0005] 本说明书实施例的目的是提供一种基于区块链的数据处理方法、装置和服务,以隐藏账户在区块链上的交易笔数。

[0006] 为实现上述目的,本说明书实施例提供一种基于区块链的数据处理方法,包括:

[0007] 根据基准时刻和提交时间间隔,计算提交时刻;

[0008] 在所述提交时刻到达以后,生成虚假交易信息;

[0009] 对所述虚假交易信息中的交易内容进行隐私保护处理;

[0010] 向所述区块链提交所述虚假交易信息。

[0011] 为实现上述目的,本说明书实施例提供一种基于区块链的数据处理装置,包括:

[0012] 计算单元,用于根据基准时刻和提交时间间隔,计算提交时刻;

[0013] 生成单元,用于在所述提交时刻到达以后,生成虚假交易信息;

[0014] 加密单元,用于对所述虚假交易信息中的交易内容进行隐私保护处理;

[0015] 提交单元,用于向所述区块链提交所述虚假交易信息。

[0016] 为实现上述目的,本说明书实施例提供一种服务器,包括:

[0017] 存储器,用于存储计算机指令;

[0018] 处理器,用于执行所述计算机指令实现以下步骤:根据基准时刻和提交时间间隔,计算提交时刻;在所述提交时刻到达以后,生成虚假交易信息;对所述虚假交易信息中的交易内容进行隐私保护处理;向所述区块链提交所述虚假交易信息。

[0019] 为实现上述目的,本说明书实施例提供一种基于区块链的数据处理方法,包括:

[0020] 根据基准时刻和提交时间间隔,计算提交时刻;

[0021] 在所述提交时刻到达以后,在不存在待被提交的真实交易信息时,生成虚假交易信息;对所述虚假交易信息中的交易内容进行隐私保护处理;向所述区块链提交所述虚假交易信息;

[0022] 在存在待被提交的真实交易信息时,对所述真实交易信息中的交易内容进行隐私保护处理;向所述区块链提交所述真实交易信息。

[0023] 为实现上述目的,本说明书实施例提供一种基于区块链的数据处理装置,包括:

[0024] 计算单元,用于根据基准时刻和提交时间间隔,计算提交时刻;

[0025] 第一提交单元,用于在所述提交时刻到达以后,在不存在待被提交的真实交易信息时,生成虚假交易信息;对所述虚假交易信息中的交易内容进行隐私保护处理;向所述区块链提交所述虚假交易信息;

[0026] 第二提交单元,用于在存在待被提交的真实交易信息时,对所述真实交易信息中的交易内容进行隐私保护处理;向所述区块链提交所述真实交易信息。

[0027] 为实现上述目的,本说明书实施例提供一种服务器,包括:

[0028] 存储器,用于存储计算机指令;

[0029] 处理器,用于执行所述计算机指令实现以下步骤:根据基准时刻和提交时间间隔,计算提交时刻;在所述提交时刻到达以后,在不存在待被提交的真实交易信息时,生成虚假交易信息;对所述虚假交易信息中的交易内容进行隐私保护处理;向所述区块链提交所述虚假交易信息;在存在待被提交的真实交易信息时,对所述真实交易信息中的交易内容进行隐私保护处理;向所述区块链提交所述真实交易信息。

[0030] 由以上本说明书实施例提供的技术方案可见,本说明书实施例中,所述发起方服务器通过不时的向区块链提交交易内容经过隐私保护处理的虚假交易信息,使得第三方无法分辨向区块链提交的真实交易信息和虚假交易信息,从而能够实现隐藏向区块链提交真实交易信息的次数,进而能够实现隐藏发起方账户在区块链上的交易笔数。

## 附图说明

[0031] 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说明书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。

[0032] 图1为本说明书实施例一种数据处理方法的流程图;

[0033] 图2为本说明书实施例一种数据处理方法的流程图;

[0034] 图3为本说明书实施例一种数据处理装置的功能结构示意图;

[0035] 图4为本说明书实施例一种数据处理装置的功能结构示意图;

[0036] 图5为本说明书实施例一种服务器的功能结构示意图。

## 具体实施方式

[0037] 下面将结合本说明书实施例中的附图,对本说明书实施例中的技术方案进行清楚、完整地描述,显然,所描述的实施例仅仅是本说明书一部分实施例,而不是全部的实施例。基于本说明书中的实施例,本领域普通技术人员在没有作出创造性劳动前提下所获得的所有其他实施例,都应当属于本说明书保护的范围。

[0038] 请参阅图1。本说明书实施例提供一种基于区块链的数据处理方法。

[0039] 在本实施例中,所述区块链(Block Chain),可以是一种按照时间先后顺序,将多

个区块数据以链式结构进行组织,并以密码学算法保证安全、可追溯、且不可篡改的分布式账本。所述区块链可以包括公有区块链、联合区块链(也称为联盟区块链)、和私有区块链等。所述区块链可以基于区块链网络来实现。所述区块链网络可以包括P2P网络(peer-to-peer network)等。所述区块链网络可以包括多个区块链节点。各个区块链节点之间共同维护统一的区块链账本。

[0040] 在本实施例中,所述数据处理方法以发起方服务器为执行主体。所述发起方服务器可以作为一个区块链节点加入区块链网络。在所述发起方服务器中可以登录有发起方账户。所述发起方账户可以为发起方在所述区块链中的账户。所述发起方服务器能够与客户端进行通信。所述客户端例如可以为智能手机、平板电子设备、便携式计算机、个人数字助理(PDA)、或智能穿戴设备等。此外,需要说明的是,根据所述数据处理方法应用的业务场景的不同,所述发起方的类型可以相同或不同,所述发起方账户的类型可以相同或不同。例如,所述数据处理方法可以应用于转账业务场景。那么,所述发起方可以为汇出方;所述发起方账户可以为汇出方账户。另举一例,所述数据处理方法可以应用于存证业务场景。那么,所述发起方可以为存证信息的存放方;所述发起方账户可以为存放方账户。

[0041] 所述数据处理方法可以包括以下步骤。

[0042] 步骤S10:根据基准时刻和提交时间间隔,计算提交时刻。

[0043] 在本实施例中,所述基准时刻可以包括以下至少一种:最近一次向区块链提交虚假交易信息的时刻、最近一次向区块链提交真实交易信息的时刻。

[0044] 所述真实交易信息可以是所述客户端发来的。具体地,所述客户端可以向所述发起方服务器发送交易信息。所述发起方服务器可以接收交易信息作为真实交易信息。或者,所述真实交易信息还可以是用户输入的。具体地,用户可以在所述发起方服务器输入交易信息。所述发起方服务器可以接收用户输入的交易信息作为真实交易信息。当然,所述真实交易信息还可以是采用其它方式获得的,本实施例对此并不做具体限定。其中,所述真实交易信息可以包括交易内容和所述发起方账户的发起方账户标识。根据所述数据处理方法应用的业务场景的不同,所述真实交易信息中的交易内容可以相同或不同。例如,所述数据处理方法可以应用于转账业务场景。那么,所述真实交易信息中的交易内容可以包括交易金额。另举一例,所述数据处理方法可以应用于存证业务场景。那么,所述真实交易信息中的交易内容可以包括存证信息。所述发起方账户标识可以用于标识所述发起方账户,例如可以为所述发起方账户的名称或地址等。在本实施例的一个实施方式中,所述真实交易信息可以不包括接收方账户标识。例如,在一些存证业务场景中,发起方可以没有交易对手。因而所述真实交易信息可以不包括接收方账户标识。在本实施例的另一个实施方式中,所述真实交易信息可以包括接收方账户标识。例如,在一些转账业务场景中,发起方需要有交易对手。因而所述真实交易信息可以包括接收方账户标识。其中,所述接收方账户标识可以用于标识接收方账户,例如可以为接收方账户的名称或地址等。此外,需要说明的是,根据所述数据处理方法应用的业务场景的不同,所述接收方的类型可以相同或不同,所述接收方账户的类型可以相同或不同。例如,所述数据处理方法可以应用于转账业务场景。那么,所述接收方可以为汇入方;所述接收方账户可以为汇入方账户。

[0045] 所述虚假交易信息可以是所述发起方服务器虚构的交易信息。所述虚假交易信息可以包括交易内容和发起方账户标识。根据所述数据处理方法应用的业务场景的不同,所

述虚假交易信息中的交易内容可以相同或不同。例如,所述数据处理方法可以应用于转账业务场景。那么,所述虚假交易信息中的交易内容可以包括数值为零的交易金额。这样在后续过程中将所述虚假交易信息提交到区块链以后,发起方账户的余额和接收方账户的余额可以保持不变。另举一例,所述数据处理方法可以应用于存证业务场景。那么,所述虚假交易信息中的交易内容可以包括空白存证信息。与所述真实交易信息相对应,所述虚假交易信息可以不包括接收方账户标识,或者,也可以包括接收方账户标识。

[0046] 在本实施例中,所述提交时间间隔的取值可以根据业务需要灵活设定。具体地,所述提交时间间隔的取值可以为一固定值;或者,也可以依据业务实际需求分时间段,每一时间段内设定为一固定值;又或者,还可以为一随机值。例如,在交易高峰期提交时间间隔的取值可以设定为0.1秒钟(还可以依据业务需求设置更短或更长);在交易低谷期提交时间间隔的取值可以设定为1分钟(还可以依据业务需求设置更短或更长)。当然,还可以根据分布函数设定所述提交时间间隔的取值,使得所述提交时间间隔的取值满足所述分布函数。所述分布函数例如可以包括指数分布函数和爱尔朗分布(Erlang Distribution)函数。其中,

所述指数分布函数的表达式可以为  $f(x, \lambda) = \begin{cases} \lambda e^{-\lambda x}, & x \geq 0 \\ 0, & x < 0 \end{cases}$ ; 所述爱尔朗分布函数的表达式可以为  $f(x, k, \lambda) = \frac{\lambda^k x^{k-1} e^{-\lambda x}}{(k-1)!}$ 。这里x表示提交时间间隔的取值;λ表示到达率;k表示爱尔朗分布函数的阶数。其中,所述到达率可以表示单位时间内事件发生的数量。在一些场景示例中,所述到达率具体可以表示单位时间内的交易数量。在实际业务中,例如,可以设定提交时间间隔的期望交易(包括真实交易和虚假交易)到达率D;可以统计真实交易的实际到达率E。那么,在指数分布函数和爱尔朗分布函数中λ=D-E。当然,本领域技术人员应当能够理解,上述根据分布函数和爱尔朗分布函数设定提交时间间隔的取值的方式仅为示例,实际上根据分布函数和爱尔朗分布函数还可以采用任意其它适当方式来设定提交时间间隔的取值。

[0047] 在本实施例中,所述发起方服务器可以将基准时刻和提交时间间隔相加,得到提交时刻。具体地,所述发起方服务器可以将最近一次向所述区块链提交交易信息的时刻和提交时间间隔相加,得到提交时刻。这里最近一次向所述区块链提交交易信息的时刻可以为提交虚假交易信息的时刻,或者,也可以为提交真实交易信息的时刻。或者,这里最近一次向所述区块链提交交易信息的时刻也可以仅为提交虚假交易信息的时刻。

[0048] 步骤S12:在所述提交时刻到达以后,生成虚假交易信息。

[0049] 在本实施例中,所述发起方服务器可以获取所述发起方账户的发起方账户标识,作为所述虚假交易信息中的发起方账户标识;可以获取交易内容作为所述虚假交易信息中的交易内容。其中,所述交易内容可以是所述发起方服务器生成的。如此所述发起方服务器可以生成交易内容作为所述虚假交易信息中的交易内容。生成的交易内容例如可以包括数值为零的交易金额等。或者,所述交易内容也可以是用户输入的。如此所述发起方服务器可以接收用户输入的交易内容作为所述虚假交易信息中的交易内容。又或者,所述交易内容还可以是其它设备发来的。如此所述发起方服务器可以接收其它设备发来的交易内容作为所述虚假交易信息中的交易内容。又或者,所述交易内容还可以是预先存储在本地的。如此

所述发起方服务器可以从本地读取交易内容作为所述虚假交易信息中的交易内容。读取的交易内容例如可以包括空白存证信息等。当然,所述虚假交易信息中的交易内容还可以是采用其它方式获得的,本实施例对此并不做具体限定。

[0050] 在本实施例中,在所述提交时刻到达以后,所述发起方服务器可以直接生成虚假交易信息。或者,在所述提交时间间隔内,所述发起方服务器有可能获取到真实交易信息。所述发起方服务器获取真实交易信息的方式,可以参见步骤S10,在此不再赘述。在获取到真实交易信息以后,所述发起方服务器可以将获取的真实交易信息作为待被提交的真实交易信息。如此在所述提交时刻到达以后,所述发起方服务器可以判断是否存在待被提交的真实交易信息;在不存在待被提交的真实交易信息时,可以生成虚假交易信息。这样所述发起方服务器能够将在所述提交时间间隔内获得的真实交易信息延迟至在所述提交时刻进行提交。

[0051] 在本实施例的一个实施方式中,所述发起方服务器可以获取账户标识作为所述虚假交易信息中的接收方账户标识。所述发起方服务器可以采用任意方式获取账户标识。例如,所述发起方服务器可以随机选取区块链中的账户标识,作为所述虚假交易信息中的接收方账户标识。另举一例,所述发起方服务器可以提供有账户标识集合。所述账户标识集合可以是预先设定的,具体可以包括至少一个接收方账户标识。每个接收方账户标识可以对应基准交易比例。所述基准比例可以根据实际需要灵活设定。那么,所述发起方服务器可以获取与所述账户标识集合中各个接收方账户标识之间的实际交易比例;可以从所述账户标识集合中选取实际交易比例小于或等于基准交易比例的接收方账户标识,作为所述虚假交易信息中的接收方账户标识。

[0052] 步骤S14:对所述虚假交易信息中的交易内容进行隐私保护处理。

[0053] 在本实施例中,所述发起方服务器可以采用任意算法对所述虚假交易信息中的交易内容进行隐私保护处理。所述任意算法例如可以包括承诺算法、同态加密算法、哈希算法等。所述承诺算法例如可以包括Pedersen承诺算法等,所述同态加密算法例如可以包括Paillier算法、Okamoto-Uchiyama算法、Boneh-Goh-Nissim算法等。例如,所述虚假交易信息中的交易内容可以包括数值为零的交易金额。那么,所述发起方服务器可以使用同态加密算法对数值为零的交易金额进行隐私保护处理。另举一例,所述虚假交易信息中的交易内容可以包括空白存证信息。那么,所述发起方服务器可以使用哈希算法计算空白存证信息的哈希值。

[0054] 步骤S16:向所述区块链提交所述虚假交易信息。

[0055] 在本实施例中,所述发起方服务器可以向所述区块链提交所述虚假交易信息;以便所述区块链中的共识区块链节点能够根据所述虚假交易信息中的交易内容更新发起方账户的状态和/或接收方账户的状态。例如,所述虚假交易信息中的交易内容可以包括数值为零的交易金额。那么,所述区块链中的共识区块链节点能够根据数值为零的交易金额更新发起方账户的余额和接收方账户的余额。从而,发起方账户的余额和接收方账户的余额可以保持不变。

[0056] 在本实施例的一个实施方式中,在向所述区块链提交虚假交易信息之前,所述发起方服务器还可以根据所述虚假交易信息生成校验信息;可以在所述虚假交易信息中添加该校验信息。例如,所述校验信息可以包括所述虚假交易信息的签名信息。

[0057] 在本实施例的一个实施方式中,在所述提交时间间隔内,所述发起方服务器有可能获取到真实交易信息。所述发起方服务器获取真实交易信息的方式,可以参见步骤S10,在此不再赘述。在获取到真实交易信息以后,所述发起方服务器可以对所述真实交易信息中的交易内容进行隐私保护处理;可以向所述区块链提交所述真实交易信息;以便所述区块链中的共识区块链节点能够根据所述真实交易信息中的交易内容更新发起方账户的状态和/或接收方账户的状态。这样所述发起方服务器能够在获取到真实交易信息以后即时提交所述真实交易信息。

[0058] 在本实施例中,所述发起方服务器通过不时的向区块链提交交易内容经过隐私保护处理的虚假交易信息,使得第三方无法分辨向区块链提交的真实交易信息和虚假交易信息,从而能够实现隐藏向区块链提交真实交易信息的次数,进而能够实现隐藏发起方账户在区块链上的交易笔数。此外,鉴于第三方无法分辨向区块链提交的真实交易信息和虚假交易信息,本实施例也能够实现隐藏真实交易的时刻、真实交易的账户等。

[0059] 请参阅图2。本说明书实施例还提供另一种基于区块链的数据处理方法。所述数据处理方法以发起方服务器为执行主体。所述发起方服务器可以作为一个区块链节点加入区块链网络。在所述发起方服务器中可以登录有发起方账户。所述发起方账户可以为发起方在所述区块链中的账户。所述发起方服务器能够与客户端进行通信。所述数据处理方法可以包括以下步骤。

[0060] 步骤S20:根据基准时刻和提交时间间隔,计算提交时刻。

[0061] 在本实施例中,步骤S20可以与前述实施例中的步骤S10对照解释。

[0062] 步骤S22:在所述提交时刻到达以后,在不存在待被提交的真实交易信息时,生成虚假交易信息;对所述虚假交易信息中的交易内容进行隐私保护处理;向所述区块链提交所述虚假交易信息。

[0063] 在本实施例中,步骤S22可以与前述实施例中的步骤S12对照解释。

[0064] 步骤S24:在存在待被提交的真实交易信息时,对所述真实交易信息中的交易内容进行隐私保护处理;向所述区块链提交所述真实交易信息。

[0065] 在本实施例中,待被提交的真实交易信息的数量可以为一个或多个。具体地,在待被提交的真实交易信息的数量为一个时,所述发起方服务器可以对该真实交易信息中的交易内容进行隐私保护处理;可以向所述区块链提交该真实交易信息。在待被提交的真实交易信息的数量为多个时,所述发起方服务器可以从中选取一个真实交易信息;可以对该真实交易信息中的交易内容进行隐私保护处理;可以向所述区块链提交该真实交易信息。其中,所述发起方服务器可以采用任意方式选取真实交易信息。例如,所述发起方服务器可以随机选取真实交易信息。另举一例,所述发起方服务器可以选取获得时刻最早的真实交易信息。

[0066] 在本实施例中,所述发起方服务器通过不时的向区块链提交交易内容经过隐私保护处理的虚假交易信息,使得第三方无法分辨向区块链提交的真实交易信息和虚假交易信息,从而能够实现隐藏向区块链提交真实交易信息的次数,进而能够实现隐藏发起方账户在区块链上的交易笔数。此外,鉴于第三方无法分辨向区块链提交的真实交易信息和虚假交易信息,本实施例也能够实现隐藏真实交易的时刻、真实交易的账户等。

[0067] 以下介绍本说明书实施例的一个场景示例。

[0068] 发起方服务器可以将最近一次向区块链提交交易信息的时刻和提交时间间隔相加,得到提交时刻。这里最近一次向区块链提交交易信息的时刻可以为提交虚假交易信息的时刻,也可以为提交真实交易信息的时刻。所述发起方服务器可以在所述提交时刻到达以后,判断是否存在待被提交的真实交易信息;在不存在待被提交的真实交易信息时,可以生成虚假交易信息,可以对所述虚假交易信息中的交易内容进行隐私保护处理,可以向所述区块链提交所述虚假交易信息;在存在待被提交的真实交易信息时,可以对所述真实交易信息中的交易内容进行隐私保护处理,可以向所述区块链提交所述真实交易信息。

[0069] 以下介绍本说明书实施例的另一个场景示例。

[0070] 发起方服务器可以将最近一次向区块链提交交易信息的时刻和提交时间间隔相加,得到提交时刻。这里最近一次向区块链提交交易信息的时刻可以为提交虚假交易信息的时刻,也可以为提交真实交易信息的时刻。所述发起方服务器可以在所述提交时刻到达以后,生成虚假交易信息,可以对所述虚假交易信息中的交易内容进行隐私保护处理,可以向所述区块链提交所述虚假交易信息。此外,在获取到真实交易信息以后,所述发起方服务器可以对所述真实交易信息中的交易内容进行隐私保护处理,可以向所述区块链提交所述真实交易信息,从而能够实现即时向区块链提交真实交易信息。

[0071] 以下介绍本说明书实施例的另一个场景示例。

[0072] 发起方服务器可以将最近一次向区块链提交交易信息的时刻和提交时间间隔相加,得到提交时刻。这里最近一次向区块链提交交易信息的时刻可以仅为提交虚假交易信息的时刻。所述发起方服务器可以在所述提交时刻到达以后,生成虚假交易信息,可以对所述虚假交易信息中的交易内容进行隐私保护处理,可以向所述区块链提交所述虚假交易信息。此外,在获取到真实交易信息以后,所述发起方服务器可以对所述真实交易信息中的交易内容进行隐私保护处理,可以向所述区块链提交所述真实交易信息,从而能够实现即时向区块链提交真实交易信息。

[0073] 请参阅图3。本说明书实施例提供一种基于区块链的数据处理装置。所述装置可以包括以下单元。

[0074] 计算单元30,用于根据基准时刻和提交时间间隔,计算提交时刻;

[0075] 生成单元32,用于在所述提交时刻到达以后,生成虚假交易信息;

[0076] 加密单元34,用于对所述虚假交易信息中的交易内容进行隐私保护处理;

[0077] 提交单元36,用于向所述区块链提交所述虚假交易信息。

[0078] 请参阅图4。本说明书实施例提供一种基于区块链的数据处理装置。所述装置可以包括以下单元。

[0079] 计算单元40,用于根据基准时刻和提交时间间隔,计算提交时刻;

[0080] 第一提交单元42,用于在所述提交时刻到达以后,在不存在待被提交的真实交易信息时,生成虚假交易信息;对所述虚假交易信息中的交易内容进行隐私保护处理;向所述区块链提交所述虚假交易信息;

[0081] 第二提交单元44,用于在存在待被提交的真实交易信息时,对所述真实交易信息中的交易内容进行隐私保护处理;向所述区块链提交所述真实交易信息。

[0082] 请参阅图5。本说明书实施例还提供一种服务器。所述服务器可以包括存储器和处理器。

[0083] 在本实施例中,所述存储器可以按任何适当的方式实现。例如,所述存储器可以为只读存储器、机械硬盘、固态硬盘、或U盘等。所述存储器可以用于存储计算机指令。

[0084] 在本实施例中,所述处理器可以按任何适当的方式实现。例如,处理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等等。所述处理器可以执行所述计算机指令实现以下步骤:根据基准时刻和提交时间间隔,计算提交时刻;在所述提交时刻到达以后,在不存在待被提交的真实交易信息时,生成虚假交易信息;对所述虚假交易信息中的交易内容进行隐私保护处理;向所述区块链提交所述虚假交易信息;在存在待被提交的真实交易信息时,对所述真实交易信息中的交易内容进行隐私保护处理;向所述区块链提交所述真实交易信息。

[0085] 请参阅图5。本说明书实施例还提供一种服务器。所述服务器可以包括存储器和处理器。

[0086] 在本实施例中,所述存储器可以按任何适当的方式实现。例如,所述存储器可以为只读存储器、机械硬盘、固态硬盘、或U盘等。所述存储器可以用于存储计算机指令。

[0087] 在本实施例中,所述处理器可以按任何适当的方式实现。例如,处理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等等。所述处理器可以执行所述计算机指令实现以下步骤:根据基准时刻和提交时间间隔,计算提交时刻;在所述提交时刻到达以后,在不存在待被提交的真实交易信息时,生成虚假交易信息;对所述虚假交易信息中的交易内容进行隐私保护处理;向所述区块链提交所述虚假交易信息;在存在待被提交的真实交易信息时,对所述真实交易信息中的交易内容进行隐私保护处理;向所述区块链提交所述真实交易信息。

[0088] 需要说明的是,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或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它实施例的不同之处。尤其,对于装置实施例和服务器实施例而言,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。

[0089] 本领域技术人员在阅读本说明书文件之后,可以无需创造性劳动想到将本说明书列举的部分或全部实施例进行任意组合,这些组合也在本说明书公开和保护的范围之内。

[0090] 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<sup>2</sup>。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Verilog2。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。

[0091] 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。

[0092] 通过以上的实施方式的描述可知,本领域的技术人员可以清楚地了解到本说明书可借助软件加必需的通用硬件平台的方式来实现。基于这样的理解,本说明书的技术方案本质上或者说对现有技术做出贡献的部分可以以软件产品的形式体现出来,该计算机软件产品可以存储在存储介质中,如ROM/RAM、磁碟、光盘等,包括若干指令用以使得一台计算机设备(可以是个人计算机,服务器,或者网络设备)执行本说明书各个实施例或者实施例的某些部分所述的方法。

[0093] 本说明书可用于众多通用或专用的计算机系统环境或配置中。例如:个人计算机、服务器计算机、手持设备或便携式设备、平板型设备、多处理器系统、基于微处理器的系统、置顶盒、可编程的消费电子设备、网络PC、小型计算机、大型计算机、包括以上任何系统或设备的分布式计算环境等等。

[0094] 本说明书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说明书,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。

[0095] 虽然通过实施例描绘了本说明书,本领域普通技术人员知道,本说明书有许多变形和变化而不脱离本说明书的精神,希望所附的权利要求包括这些变形和变化而不脱离本说明书的精神。

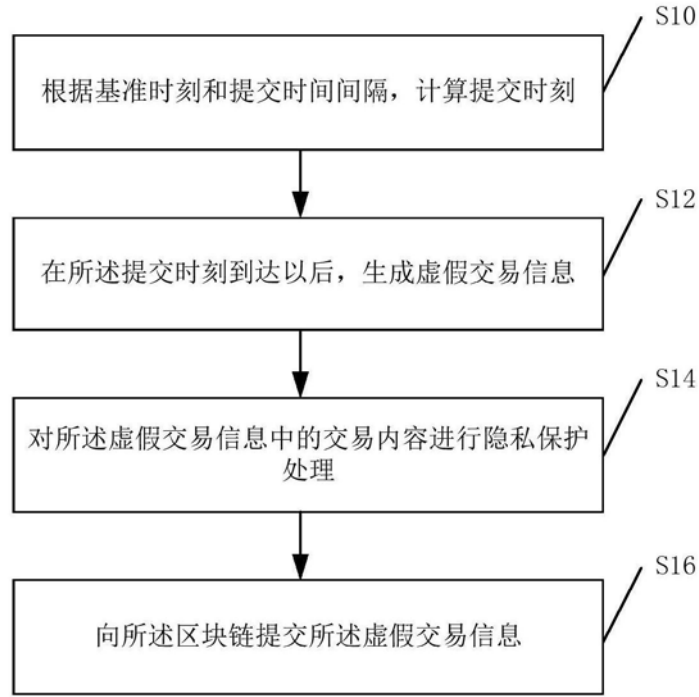


图1

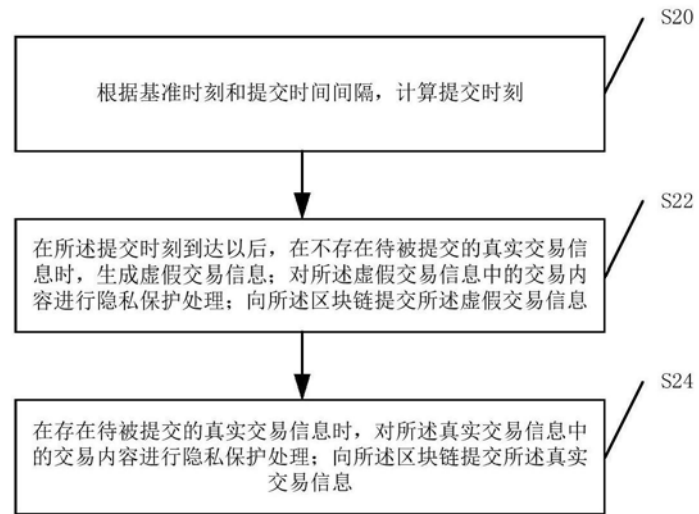


图2

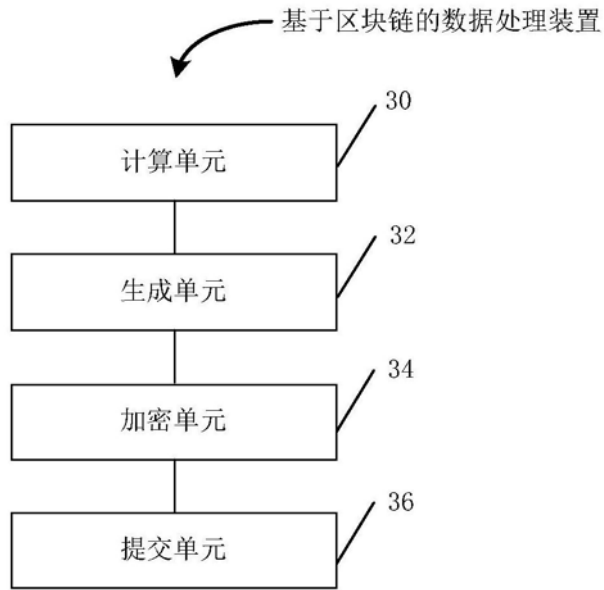


图3

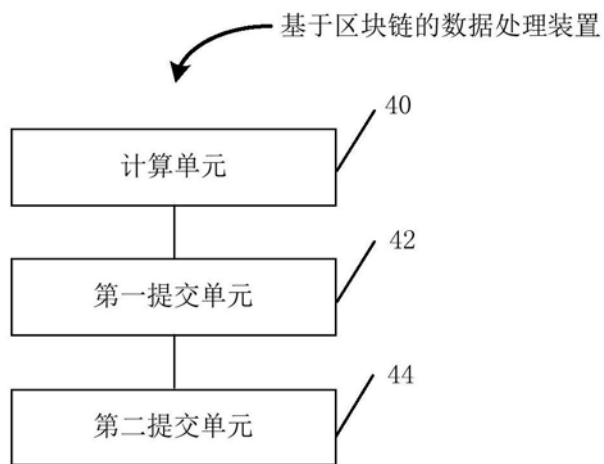


图4

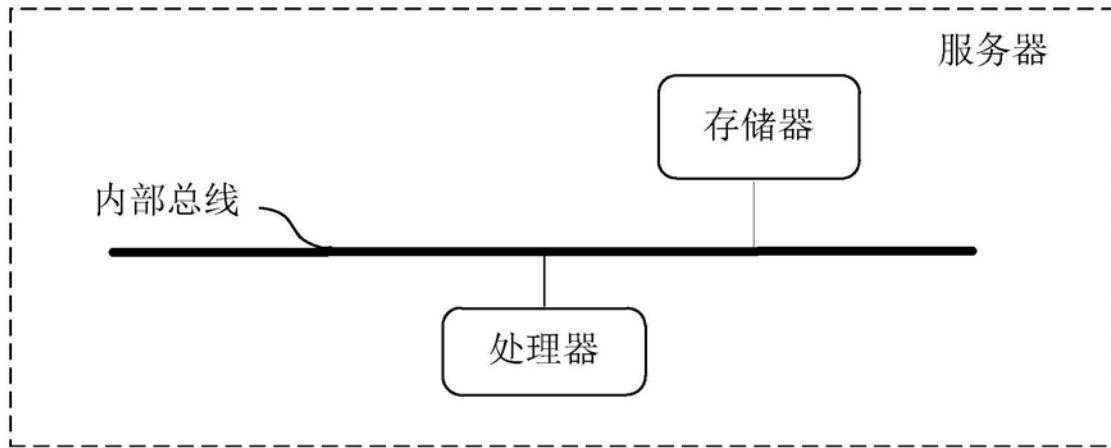


图5