



(12) 发明专利申请

(10) 申请公布号 CN 116109410 A

(43) 申请公布日 2023. 05. 12

(21) 申请号 202211390716.8

(22) 申请日 2022.11.08

(30) 优先权数据

102021212599.9 2021.11.09 DE

(71) 申请人 罗伯特·博世有限公司

地址 德国斯图加特

(72) 发明人 A·波代

(74) 专利代理机构 中国专利代理(香港)有限公

司 72001

专利代理师 刘艺诗 吕传奇

(51) Int.Cl.

G06Q 40/04 (2012.01)

G06Q 20/36 (2012.01)

G06Q 20/38 (2012.01)

G06Q 20/40 (2012.01)

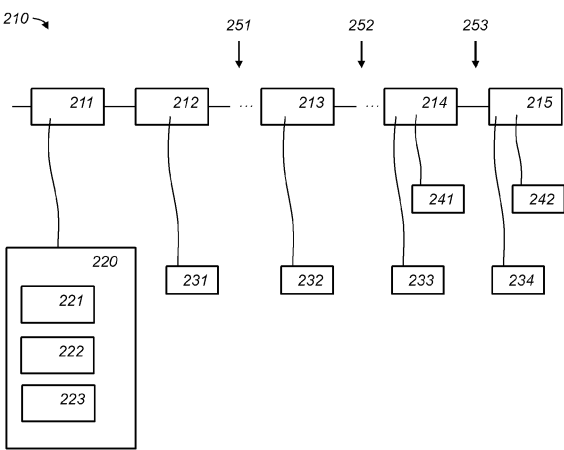
权利要求书2页 说明书17页 附图5页

(54) 发明名称

防御分布式分类账中的抢先交易攻击

(57) 摘要

防御分布式分类账中的抢先交易攻击。一些实施例针对一种用于由第一矿工维护分布式分类账的计算机实现的方法。可以从多个交易请求中选择一组交易,并将其包括在分布式分类账的新生成的区块中。可以通过评估对一个或多个选择规则的合规性来计算优度分数。可以向矿工分配与第一优度分数成比例的加密代币的金额。



1. 一种用于由第一矿工维护分布式分类账的计算机实现的方法(500),
 - 接收(510)多个交易请求以包括在分布式分类账中,
 - 从所述多个交易请求中选择(520)一组交易,
 - 生成(530)包括一组所选交易的分布式分类账的新区块,
 - 通过评估第一矿工对一个或多个选择规则的合规性来计算(540)第一优度分数,所述一个或多个选择规则指示用于为分布式分类账的新区块选择交易的规则,
 - 敲定(550)新区块并将所述区块转移到一个或多个另外的矿工,以及
 - 向第一矿工分配(560)与第一优度分数成比例的加密代币的金额。
2. 根据权利要求1所述的用于由第一矿工维护分布式分类账的计算机实现的方法,
 - 从第二矿工接收分布式分类账的区块,
 - 通过评估第二矿工对所述一个或多个选择规则的合规性来计算第二矿工的第二个优度分数,
 - 第一,对照分布式分类账认证所述区块中的交易,
 - 第二,认证分配给第二矿工的加密代币的金额与第二优度分数成比例,以及
 - 如果第一和第二认证中的任何一个失败,则拒绝所述区块。
3. 根据前述权利要求中任一项所述的用于由第一矿工维护分布式分类账的计算机实现的方法,其中
 - 交易请求具有年限,并且其中如果没有选择具有旧年限的交易请求,则合规性被评估为较低。
4. 根据前述权利要求中任一项所述的用于由第一矿工维护分布式分类账的计算机实现的方法,其中,所分配的加密代币从以下获得
 - 随着新区块的创建而铸造的新加密代币,
 - 和/或从以下获得
 - 与所选交易相关联的交易费用。
5. 根据前述权利要求中任一项所述的用于由第一矿工维护分布式分类账的计算机实现的方法,包括将包含在分布式分类账中的交易请求与第二矿工同步。
6. 根据前述权利要求中任一项所述的用于由第一矿工维护分布式分类账的计算机实现的方法,包括利用一组矿工生成包括在分布式分类账中的商定交易请求列表,以及从商定交易请求中选择所述一组交易。
7. 根据权利要求6所述的用于由第一矿工维护分布式分类账的计算机实现的方法,如果没有选择在商定列表中具有较旧年限的交易请求,则合规性被评估为较低。
8. 根据前述权利要求中任一项所述的用于由第一矿工维护分布式分类账的计算机实现的方法,包括将所述商定列表输出给用户。
9. 根据前述权利要求中任一项所述的用于由第一矿工维护分布式分类账的计算机实现的方法,包括当接收到交易请求和/或将交易请求包括在商定交易列表中时,向用户发送签名收据。
10. 根据前述权利要求中任一项所述的用于由第一矿工维护分布式分类账的计算机实现的方法(500),包括
 - 将第二矿工的所计算的第二个优度分数与确定的标准、例如阈值进行比较,并且如果所

述比较失败,则触发惩罚例程。

11. 一种用于将分布式分类账维护为第一矿工的服务器设备,包括
 - 通信接口,被配置为接收多个交易请求以包括在分布式分类账中,
 - 处理器系统,被配置用于
 - 从所述多个交易请求中选择一组交易,
 - 生成包括一组所选交易的分布式分类账的新区块,
 - 通过评估第一矿工对一个或多个选择规则的合规性来计算第一优度分数,所述一个或多个选择规则指示用于为分布式分类账的新区块选择交易的规则,
 - 敲定新区块并将所述区块转移到一个或多个另外的矿工,以及
 - 向第一矿工分配与第一优度分数成比例的加密代币的金额。
12. 一种用于使用分布式分类账的客户端设备,所述客户端设备包括
 - 通信接口,被配置为向服务器设备发送交易请求,以及
 - 处理器系统,被配置为
 - 维护具有加密代币的第一钱包,
 - 向服务器设备发送交易请求,从而请求将加密代币的金额从第一钱包转移到第二钱包,其中服务器设备被配置为从多个交易请求中选择交易请求,生成包括所选交易的分布式分类账的新区块,通过评估矿工对一个或多个选择规则的合规性来计算第一优度分数,敲定新区块并将所述区块转移到一个或多个另外的矿工,以及向第一矿工分配与第一优度分数成比例的加密代币的金额。
13. 一种暂时性或非暂时性计算机可读介质(1000),包括表示指令的数据(1020),当由处理器系统执行时,所述指令使得处理器系统执行根据权利要求1-10中任一项的方法。

防御分布式分类账中的抢先交易攻击

技术领域

[0001] 当前公开的主题涉及用于维护分布式分类账的计算机实现的方法、服务器设备、客户端设备和计算机可读介质。

背景技术

[0002] 分散式交易系统、交易数据库或分布式分类账是计算机网络中带来关于其交易及其顺序的共识的任何协议。这样的系统的常见形式基于区块链,并形成许多所谓的加密货币的基础。在加密货币中,加密代币跨多个客户端上分布。客户可以在彼此之间转移代币,或者向做市商转移代币以及从做市商转移代币。加密术和分布式分类账系统确保转移不能容易地被伪造或否认。

[0003] 国际专利申请W0 2019/043668 A1公开了一种已知的区块链,在这种情况下,用于跟踪加密货币代币。与代币相关的交易(诸如代币创建或销毁)在区块链上是可见的。

[0004] 诸如区块链的分布式分类账提供了一种安全的转移系统。这允许用例如第一类型代币兑换第二类型代币。通俗地说,第一类型代币被买入,并且具有作为第二类型代币的金额的价格。高级加密货币使用一种称为“曲线联合(curved bonding)”的机制,根据该机制,一种称为联合曲线的函数通过算法定义,它取决于当前的代币供应影响货币单位(代币)的价格。价格在这里被不严格地用来指示被兑换的代币,这些代币不一定具有货币价值。代币可以表示任何有限的资源,例如对计算资源等的访问,并且加密货币可以用于管制访问。

[0005] 该已知系统公开了利用曲线联合来管理加密货币。在已知方法中,向多个用户提供市场内钱包,该市场内钱包适合于存储在价值上链接到加密货币代币并且需要在数字市场平台上交易的链接数字代币。提供了适合于存储多个加密货币代币的加密货币储备。响应于用户从市场商店购买链接数字代币,链接数字代币被转移到用户的市场内钱包,并且加密货币代币的等值被转移到加密货币储备。响应于用户从用户的市场内钱包中提取多个链接数字代币,从用户的市场内钱包中移除期望数量的链接数字代币,并且将加密货币代币的等值从加密货币储备转移到用户的市场外钱包,市场外钱包适合于在市场平台之外存储加密货币代币。

发明内容

[0006] 已知的系统容易受到抢先交易攻击。抢先交易攻击利用系统的技术属性来达到其自己的目的。

[0007] 当抢先交易进行买入或卖出交易时,矿工和其他活动者可能从正常参与者提取价值。可以区分两类抢先交易:一方面,存在短期到中期或高频抢先交易(hfrr),其中正常交易不被显著延迟,但是攻击交易被下单在执行队列中(一个或多个)正常交易之前以及正好在(一个或多个)正常交易之后。例如,矿工可能共谋并且将交易下单在队列的前面。例如,知道即将到来的大型交易的用户可以将高交易费用与他抢先交易的交易相关联,以诱导矿工优先考虑他的交易。矿工是一种电子设备,其通常采用被配置成矿工的服务器设备的形

式。

[0008] 各分区矿工之间的共谋可能使某些交易延迟更长时间帧,这被称为主动审查(censorship)。对应的攻击被称为基于审查的抢先交易(cfr)。示例将是下单买入交易,然后阻止所有卖出交易,并且仅允许买入交易,最后卖出,并且因此在处理延迟的卖出交易之前提取价值。

[0009] 在分布式分类账中,通常接受矿工和客户端均可以影响交易的次序,主要是通过交易请求相关联的交易费用的高低——客户可以通过关联较高的费用来优先化他们的交易请求,而矿工将有可能选择具有较高交易费用的交易请求。这种灵活性允许用户影响交易的处理——为一杯咖啡付款不需要快速处理,而对于大型交易,所涉及的各方可能偏向于交易快速敲定。

[0010] 不幸的是,允许对支付处理次序进行影响的灵活性使得有时交易可能不得不比通常更久的排队等待变得可接受和预期。这给予攻击的机会。矿工、并且尤其是一组共谋的矿工可以首先发出并处理买入交易,并且然后抑制卖出交易一段时间,接着是攻击者的卖出交易。因此,买入和卖出操作囊括了审查交易时段。

[0011] 抢先交易攻击落入与加密攻击、拒绝服务等类似的类别。系统的技术属性被利用来为攻击者的目的服务。这样的审查攻击可以通过非技术措施来抑制,例如,法律或合同可能规定矿工不参与审查等。尽管可以设想到非技术解决方案,但是例如对于问题的技术解决方案是优选的。发明人意识到技术措施确实有可能减轻这些类型的攻击。

[0012] 如果审查攻击在进展中,则某些交易将在一段时间内不被处理。通过降低不进展旧交易的服务器收取的费用,参与审查攻击可能变得不太有吸引力。

[0013] 例如,用于分布式分类账的新区块可以包括从在设备(例如服务器设备,例如矿工)处接收的多个交易请求中选择的一组交易。例如,它们可能接收自客户端或其他矿工。

[0014] 敲定区块(例如在区块中包括共识代币)的矿工也可以从与新区块相关的可用资金(例如,新铸造的代币和交易费用的总和)中为自己分配一定金额的加密代币;一部分可能被转移到该区块的矿工,一部分可能被分配到别处。例如,未分配给矿工的部分可以存放在池中,例如钱包中。例如,这样的池可以由管理者(例如分布式分类账的管理员)访问。当新的区块被挖掘时,有多少代币变得可用(例如被铸造)可以由链逻辑来确定,但是也可以由智能合同来确定。

[0015] 在实施例中,当敲定新区块时,可用于分配的代币部分是从第一优度分数计算的。

[0016] 优度分数反映了这个矿工有多么好地遵循一组选择规则。其他矿工可以不仅基于交易的有效性或该区块的密码一致性,而且还基于分配给该矿工的代币金额来接受或拒绝该区块。

[0017] 特别地,如果不选择较旧的交易请求;尤其是如果不选择具有高交易费用的较旧交易请求,则优度分数可能较低。例如,可以通过对具有年限(age)和费用的特定组合(例如,如紧急度函数所指示的)的未选择交易请求进行计数来计算优度。在某种意义上,接收到新区块并且知道存在合理地应该已经被选择的旧交易(例如,作为选择规则中的目标,例如,使用紧急度函数)的矿工知道另一个矿工——出于不论何种原因——正在操控超出灵活系统合理需要的交易次序。通过拒绝该区块,提议该区块的矿工不会接收到在该区块中分配给它的相关联费用。

[0018] 交易请求可能在矿工之间的任何一点都不完全同步,例如,如果交易请求以对等方式分布的话。然而,较旧的交易请求通常是同步的,因此这将不可能过度影响优度分数的计算。然而,该问题可以通过引入交易请求的同步(例如,建立商定的交易请求列表)来减轻。这可以通过在矿工之间周期性地运行同步协议来实现。然后,可以仅从商定的交易请求中为新区块选择交易。同步可以包括交换交易请求的到达时间,使得所有矿工可以认证交易的年限。

[0019] 可以在分布式分类账上维护商定的交易请求列表,该分类账可以是同一分类账或另外的分类账。可以导出所商定的交易请求列表,例如,使得客户端设备可以认证其交易请求是否包括在其中。

[0020] 以矿工的行为为条件向其转移代币减轻了审查。例如,如果交易链接到与随着买入/卖出操作体量等改变的价格,那么这一点是重要的。例如,在实施例中,例如在创建程序和取消程序中,加密货币用第一种类代币兑换第二种类代币,并且反之亦然。在这样的实施例中,汇率可以例如作为联合曲线在系统中建立,或者例如通过引入买入/卖出差价从联合曲线导出。代币的价格也可能在分布式分类账系统的直接控制之外波动。无论汇率变化的原因如何,可以减轻基于审查的攻击都是合期望的。

[0021] 引入优度分数可以与使抢先交易不那么有吸引力的其他措施相结合。例如,可能存在买入/卖出差价,使得代币的买入价格高于代币的卖出价格。这使得抢先交易攻击甚至效率更低。

[0022] 优度分数与买入-卖出差价的组合尤其有益,因为它一般致使任何人持有的短期和/或高频抢先交易变得低效。同时,对于基于审查的攻击,它强制必要的时间帧,以便使攻击在经济上对攻击者有益。该时间帧通过买入-卖出差价变大,但这给了优度分数时间来发现矿工的异常行为并介入。换句话说,买入-卖出差价让诸如审查攻击之类的攻击变得更加“可见”,并且从而可惩罚。

[0023] 优度分数可以用于经由交易费用来强制良好行为。在实施例中,如果优度落到阈值以下,则可以触发另外的措施。例如,这样的另外的措施可以包括例如减少股份,监禁矿工特定量时间。

[0024] 当矿工被监禁时,他将在一定量时间内排除为活跃的矿工。因此,在该时间期间,他不能挖掘新区块,也不能获得新代币。

[0025] 例如,如果优度分数下降到阈值以下,或者不再满足(例如,如智能合同中或区块中规定的)确定标准,则除了(或代替)拒绝由缺少的矿工挖掘的区块之外,还可以触发另外的惩罚例程。惩罚例程可以在链逻辑、分类账协议、智能合同等中定义。

[0026] 以可计算的优度分数为基础进行惩罚具有如下优点,即可被缺少的矿工本身容易地和客观地验证,而且可被对例如系统的正确管理感兴趣的任何其他方认证。这也避免了部分矿工可能共谋起来惩罚不应受惩罚例程的矿工。

[0027] 比只拒绝区块更严格的措施可能有必要。例如,考虑获得很大价值的抢先交易攻击。这种价值收益可能比通常的交易费用大得多,并且因此,与抢先交易攻击所得的收益相比,经由交易费用比例的惩罚可以忽略不计。例如自动地、或手动地、或作为混合而触发惩罚例程,可以避免该行为。

[0028] 除了延迟或不处理旧的交易请求之外,可以录入优度分数中的其他元素可以包括

例如不够频繁地验证区块、离线太频繁、计算区块中的错误值,诸如加密值。这些都是重要的指标;例如,如果矿工过于频繁地离线,这意味着更容易找到大多数剩余矿工的共谋,从而降低整个系统的安全性。

[0029] 例如,在实施例中,矿工可以计算另一个矿工的优度分数,并将该优度分数与确定的标准(例如阈值)进行比较。如果比较失败,则可以触发惩罚例程。例如,在实施例中,确定数量的其他矿工也需要触发惩罚例程。

[0030] 例如,触发惩罚例程和可选地导致它的优度分数和/或优度分数计算可以在分布式分类账的区块中公布。如果足够数量的其他矿工也这样,则智能合同可能触发惩罚例程。尽管如此,没有其他矿工是必要的,例如,智能合同可以自己重新计算优度分数,并与自己的标准进行比较,以达到触发或不触发惩罚例程。

[0031] 优度分数可以是数字分数。优度分数可以包括多个数值。优度评估的标准可以是一个或多个数值必须高于或低于相应的阈值。例如,不同的值可以表示不同方面的优度,例如离线时间、旧交易的积压等等。

[0032] 买入-卖出差价的组合,例如,买入和卖出交易的不同价格与基于优度分数的惩罚触发的组合使得短期和审查抢先交易都是困难的。

[0033] 在实施例中,第一类型加密代币由智能合同维护。智能合同是在支持智能合同的分布式分类账上创建新的加密货币的有利方式。尽管如此,智能合同并不是必需的。例如,实现与智能合同相同的程序的做市商可以是链逻辑的一部分,例如链应用层的一部分。用户可以调用所述程序,就好像是分类账上定义的智能合同一样,即使智能合同是在别处实现的。通过将智能合同的功能并入链逻辑、例如运行分布式分类账的软件,使用智能合同的实施例可以被转换成没有智能合同的实施例。智能合同可以实现用于创建第一类型加密代币以兑换第二类型加密代币的创建程序。例如,智能合同可以实现用于取消第一类型加密代币以兑换第二类型加密代币的取消程序。第二类型代币可以是已建立的加密货币,例如比特币、以太等。智能合同还可以维护与关系到第一类型代币相关的信息,特别是指示第一类型加密代币的当前数量的当前供应大小和定义函数的联合曲线。

[0034] 例如,用于兑换的第二类型加密代币的金额可以通过对函数从当前供应大小到新供应大小进行积分来计算。该函数是联合曲线和多个另外项的总和,对于创建和取消程序中的至少一个,所述另外项包括费用项,该费用项包括在第一类型加密代币的金额之上移位的联合曲线的倍数。

[0035] 例如,在创建程序被触发的情况下,积分可以在创建函数之上完成,而对于取消,可以使用取消函数。创建函数可以高于取消函数。例如,创建函数可以高于联合曲线,而取消函数可以低于联合曲线。联合曲线是递增函数。

[0036] 本发明的一个方面是用于维护分布式分类账的服务器设备。例如,服务器设备可以是矿工。本发明的一个方面是客户端设备。例如,用户可以使用客户端设备来例如使用分布式分类账,例如发送交易请求。如果可能使用智能合同在分布式分类账上创建另外的加密货币,则交易请求可以在智能合同中发起创建或取消请求。

[0037] 在允许智能合同的分布式分类账上,预防审查尤为重要,因为任何数量的加密货币都可以在分布式分类账上创建。本文的实施例继续允许选择请求的灵活性,同时减轻滥用。

[0038] 另外的方面是一种用于维护分布式分类账的方法。该方法的实施例可以作为计算机实现的方法在计算机上实现,或者在专用硬件中实现,或者在两者的组合中实现。用于该方法的实施例的可执行代码可以存储在计算机程序产品上。计算机程序产品的示例包括存储器设备、光存储设备、集成电路、服务器、在线软件等。优选地,计算机程序产品包括存储在计算机可读介质上的非暂时性程序代码,用于当所述程序产品在计算机上执行时执行该方法的实施例。

[0039] 在实施例中,计算机程序包括计算机程序代码,当计算机程序在计算机上运行时,该计算机程序代码适于执行该方法的实施例的所有或部分步骤。优选地,计算机程序体现在计算机可读介质上。

[0040] 当前公开主题的另一方面是一种使计算机程序可供下载的方法。

附图说明

[0041] 将参考附图仅以示例的方式描述另外的细节、方面和实施例。各图中的元件是为了简单性和清楚而图示的,并且不一定是按比例绘制的。在各图中,与已经描述的元件相对应的元件可以具有相同的附图标记。在附图中,

图1a示意性地示出了客户端设备的实施例的示例,

图1b示意性地示出了服务器设备的实施例的示例,

图1c示意性地示出了分布式分类账系统的实施例的示例,

图2示意性地示出了区块链的实施例的示例,

图3a示意性地示出了分布式分类账系统的实施例的示例,

图3b示意性地示出了分布式分类账系统的实施例的示例,

图4示意性地示出了用于维护第一类型加密代币的方法的实施例的示例,

图5a示意性地示出了根据实施例的具有包括计算机程序的可写部分的计算机可读介质,

图5b示意性地示出了根据实施例的处理器系统的表示。

[0042] 参考符号列表

以下参考和缩写的列表对应于图1a-3b、5a、5b,并且被提供用于促进附图的解释,并且不应被解释为限制权利要求。

100 分布式分类账系统

110、110.1、110.2 客户端设备

130 处理器系统

140 存储装置

150 通信接口

160、160.1、160.2 服务器设备

162 数据库

170 处理器系统

180 存储装置

190 通信接口

172 计算机网络

210 区块链
211-215 区块
220 智能合同
221 创建程序
222 取消程序
223 更新程序
231-234 状态
241-242 加密代币转移
251-253 时间点
300 分布式分类账系统
301-303 服务器设备
311、312 客户端设备
320 对等链路
316 客户端到服务器链路
331 交易聚合器
1000、1001 计算机可读介质
1010 可写部分
1020 计算机程序
1110 (一个或多个)集成电路
1120 处理单元
1122 存储器
1124 专用集成电路
1126 通信元件
1130 互连
1140 处理器系统。

具体实施方式

[0043] 虽然当前公开的主题容许以许多不同形式的实施例,但是在附图中示出了并且将在本文详细描述一个或多个具体实施例,其具有如下理解:本公开将被认为是当前公开的主题的原理的例示,并且不旨在将其限制于所示出和描述的具体实施例。

[0044] 在下文中,为了便于理解,在操作中描述实施例的元件。然而,将清楚的是,相应元件被布置成执行被描述为由它们执行的功能,例如程序。

[0045] 此外,当前公开的主题不仅仅限于实施例,而且还包括在本文描述的或在相互不同的从属权利要求中记载的特征的每个其他组合。

[0046] 图1a示意性地示出了客户端设备110的实施例的示例。图1b示意性地示出了服务器设备160的实施例的示例。

[0047] 例如,服务器设备160可以被配置为维护分布式分类账。服务器设备被配置成矿工,并且有时被称为矿工或挖掘设备,或称为铸造机或铸造设备。例如,服务器160可以被配置为生成包括一组所选交易的分布式分类账的新区块。服务器设备可以从其接收的交易中

选择交易。某一金额的加密代币被分配给矿工。例如,代币可以是加密货币。例如,加密货币可以与分布式分类账相关联。例如,加密货币可以是比特币、以太等。

[0048] 尽管服务器设备——即矿工设备——有自由从服务器设备已知的交易请求中选择交易,但是有兴趣将选择保持在一定界限内。特别是,优选的是不让交易太久处于未处理。例如,服务器可以被配置为依据优度分数来计算将代币分配给自己的优度分数。本文给出了示例。

[0049] 例如,客户端设备110可以被配置为维护钱包。例如,客户端设备110可以被配置为向服务器设备160发送交易请求,例如,将代币从钱包转移到另外的钱包。交易在被处理时将反映在分布式分类账上的区块中。服务器设备160也可以访问钱包,这可能是通过执行智能合同的程序。

[0050] 客户端设备110可以包括处理器系统130、存储装置140和通信接口150。服务器设备160可以包括处理器系统160、存储装置180和通信接口190。存储装置140和180可以是电子存储装置。存储装置可以包括本地存储装置,例如本地硬盘驱动器或电子存储器。存储装置140和180可以包括非本地存储装置,例如云存储装置。在后一种情况下,存储装置140和180可以包括到非本地存储装置的存储接口。

[0051] 客户端设备110和服务器设备160可以是分布式分类账系统的一部分。客户端设备110和服务器设备160可以通过计算机网络与其他系统、外部存储装置、输入设备、输出设备和/或一个或多个传感器进行内部通信。计算机网络可以是互联网、内联网、LAN、WLAN等。计算机网络可以是互联网。该系统包括连接接口,该连接接口被布置成根据需要在系统内或系统外部进行通信。例如,连接接口可以包括:连接器,例如有线连接器,例如以太网连接器、光学连接器等;或者无线连接器,例如天线,例如Wi-Fi、4G或5G天线。

[0052] 通信接口150可以用于发送或接收数字数据,例如,转移加密代币(例如,表示加密货币)的交易请求,以及执行加密货币的创建或取消程序的请求;所述程序可以是智能合同的一部分。通信接口190可以用于发送或接收数字数据,例如转移加密代币的交易请求。通信接口190可以用于与其他服务器设备通信,例如,分发区块链的新区块,或者同步交易请求。

[0053] 设备110和160的执行可以在处理器系统中实现,例如一个或多个处理器电路,例如微处理器,其示例在本文示出。处理器系统可以包括一个或多个GPU和/或CPU。系统100的设备110和160可以包括可以分布在不同位置之上的多个处理器。例如,设备110和160可以使用云计算。

[0054] 设备110和160可以包括功能单元,所述功能单元可以是处理器系统的功能单元。例如,所示的功能单元可以全部或部分地以存储在设备处(例如存储在设备的电子存储器中)的计算机指令来实现,并且可由设备的微处理器来执行。在混合实施例中,功能单元部分地在硬件中实现(例如作为协处理器,例如加密协处理器),并且部分地在设备上存储和执行的软件中实现。

[0055] 图1c示意性地示出了分布式分类账系统的实施例的示例。系统100包括多个客户端设备;示出了客户端设备110.1和110.2。系统100包括多个服务器设备;示出了服务器设备160.1和160.2。这些设备通过计算机网络172,例如互联网连接。客户端和服务器设备可以根据实施例。客户端设备可以相互之间协助来转移加密代币。客户端设备可以与服务器

设备交互,以将加密代币从第一钱包转移到第二钱包。客户端设备可以请求服务器设备执行创建程序来创建一类型加密货币的新代币,这可能是为了兑换另一类型加密货币的代币。客户端设备可以请求服务器设备执行取消程序以取消该类型的加密货币的代币,这可能是为了兑换另一类型的加密货币的代币。创造有时也被称为买入,而取消有时被称为销毁或卖出。

[0056] 存储装置可以实现为电子存储器(比如闪速存储器),或者磁存储器(比如硬盘)等等。存储装置可以包括一起构成存储装置140、180的多个分立的存储器。存储装置可以包括临时存储器,比如RAM。存储装置可以是云存储装置。

[0057] 通常,客户端设备110和服务器设备160各自包括执行存储在系统处的适当软件的微处理器;例如,该软件可能已经被下载和/或存储在对应的存储器中,例如诸如RAM的易失性存储器或者诸如闪存的非易失性存储器。替代地,系统可以全部或部分地在可编程逻辑中实现,例如,作为现场可编程门阵列(FPGA)。所述系统可以全部或部分地实现为所谓的专用集成电路(ASIC),例如为其特定用途定制的集成电路(IC)。例如,电路可以用CMOS实现,例如使用诸如Verilog、VHDL等之类的硬件描述语言。特别地,客户端设备110和服务器设备160可以包括用于加密处理和/或算术处理的电路。

[0058] 处理器电路可以以分布式方式实现,例如作为多个子处理器电路。存储装置可以分布在多个分布式子存储装置之上。部分或全部存储器可以是电子存储器、磁存储器等。例如,存储装置可以具有易失性和非易失性部分。存储装置的部分可能是只读的。

[0059] 图2示意性地示出了区块链210的实施例的示例。区块链是分布式分类账的特定示例,其在实施例中被示出工作良好。也可以使用分布式分类账的其他示例。例如,在实施例中,分布式分类账可以是散列图、缠结或网格。分布式分类账包括彼此链接的多个区块。所述区块可以包括交易数据和元数据。元数据可以包括链接信息和共识机制。主要参考区块链描述了实施例,但是这样的实施例可以被改变以使用另一种类型的分布式分类账,特别是基于图的分布式分类账。

[0060] 区块链210包括多个区块,所述多个区块在序列中彼此链接。例如,该链接可以包括共识机制。例如,这样的机制可以是例如作为在比特币中的工作证明。该机制可能是利害关系的证明。共识机制允许分布式分类账中的分布式信任。在实施例中,可以使用例如如在本领域中已知的其他共识机制。

[0061] 为了帮助讨论,图2示出了区块链中的三个点:对应于三个时刻的点251、252和253。在点251,已经创建了直到区块213的区块,但是还没有创建区块213。在点252,已经创建了直到区块214的区块,但是还没有创建区块214。在点253,已经创建了直到区块215的区块,但是还没有创建区块215。

[0062] 在区块链210中示出了多个区块,在这种情况下是5个区块:区块211、212、213、214和215。可以存在更多或更少的区块。区块可以包括与分布式分类账机制相关的数据,例如共识数据,但也包括其他信息。特别地,区块可以包括交易,其中代币被绑定到例如与客户端的公钥相关的地址,例如如被并入客户端设备中。区块还可以包括其他信息。

[0063] 分布式分类账中的区块由具有创建共识信息能力的矿工创建,无论该共识信息是利害关系证明还是工作证明等。通常,矿工(例如服务器设备)接收多个交易,例如直接从用户或者从彼此共享他们接收的交易的其他矿工接收。从接收到的交易中进行选择,该选择

又被包括在分布式区块链的新区块中。与新区块相关联的加密货币代币总金额的一部分（例如，通过区块本身的创建而铸造的代币）以及与所包括的交易相关联的交易费用可以被转移到矿工，例如，在刚刚挖掘的那个区块中。

[0064] 分布式分类账可以实现加密货币。例如，新区块的创建也可以创建加密货币的新加密货币。矿工通常接收到全部或部分新铸造的加密货币。加密货币被链接到特定的加密身份，例如地址或加密密钥。

[0065] 有趣的是，一旦分布式分类账存在，就可以使用它（例如，通过使用智能合同）来创建另外的加密货币。例如，分布式分类账中的区块可以包括智能合同。区块211以智能合同220的形式示出了示例。智能合同通常用计算机语言编写。为智能合同优化的计算机语言的示例是实体(solidity)。例如，在实施例中，区块链210可以是以太坊区块链，并且智能合同可以以实体形式编写。尽管如此，不要求限制到特定的语言或区块链。例如，以太坊区块链可以如在G. Wood的论文“Ethereum: a secure decentralised generalised transaction ledger”（例如2021-07-11的伊斯坦布尔版本80085f7）中所描述的那样使用。

[0066] 例如，在实施例中，被配置为维护第一类型加密货币的服务器可以被配置为从分布式分类账获得智能合同。例如，智能合同可以存储在分布式分类账的区块中。智能合同可以实现所需的程序，例如，用于创建第一类型加密货币的创建程序和用于取消第一类型加密货币的取消程序。智能合同可以被配置为维持当前的供应大小。智能合同可以定义联合曲线。

[0067] 在实施例中，区块链210用于创建和取消第一类型加密货币。通俗地说，创建新的加密货币有时被称为“买入”代币；取消加密货币有时被称为“卖出”代币。

[0068] 智能合同实现多个程序，所述多个程序至少包括创建程序221和取消222（也称为卖出程序）。可选地，合同可以实现更新程序223。通俗地说，创建程序也被称为买入程序，并且取消程序222被称为卖出程序。这并不完全准确，因为通常代币一旦被取消它们就不再存在。在取消动作之后，代币的总供应减少。取消程序也称为销毁程序。

[0069] 服务器执行创建程序，并作为结果获得新状态。例如，新状态可以反映现在存在的第一类型加密货币的增加了的数量（称为供应）。服务器还可以获得指示新加密货币被转移到第一用户的交易，和/或指示第二类型的现有加密货币被从第一用户转移到与智能合同相关联的钱包的交易。智能合同被称为做市商。做市商可以将第二类型代币的金额保持在储备中，例如在钱包中。钱包的该部分被称为池或池余额。同一个钱包可以用于持有不是池的部分的代币。人们也可以仅针对池保持该钱包的使用。

[0070] 服务器客户端在区块链上写入，例如，在区块中包括新状态和第一类型的新加密货币，转移的第二类型加密货币被写入该区块链或另一个区块链上。第一类型代币和状态也可以放在单独的区块链上。

[0071] 假设第一用户想要买入多个第一类型加密货币。他/她通过客户端设备向服务器设备发送请求。该请求可以被发送到多个服务器设备。该请求可以包括，例如，

- 所请求的第一类型加密货币的金额 x
- 转移 y 个第二类型加密货币的指令
- 将第一类型加密货币绑定到的地址。

[0072] 例如，考虑正好在创建时钟214之前，在点252发送请求。

[0073] 服务器设备从区块链检索智能合约220。智能合约使用可以更新的状态。服务器设备从区块链检索当前状态。区块链210示出了点252之前的状态231和232,使得服务器设备检索状态232。

[0074] 为了确定与第一类型加密代币的金额(x)兑换的第二类型加密代币的金额(y),通俗地称为价格,智能合约使用联合曲线。智能合约可以包括联合曲线的定义。联合曲线的定义也可能处于一种状态。联合曲线的定义可以是智能合约,直到书面状态中的新定义覆盖它。注意,联合曲线通常是递增的或者至少是非递减的。

[0075] 在实施例中,智能合约不存储在区块中,而是通过其他手段对于服务器可访问;例如,智能合约可以在执行所述程序之前获得。使用智能合约可以具有如下优点:可以将例如任何特定程序的执行证明下单在分布式分类账上。注意,即使智能合约没有下单在链上,它也仍然可以作为一个被执行,只要其他矿工具有对其代码的访问权。

[0076] 事实上,所述程序甚至不需要在智能合约中实现,而是可以在常规软件中实现。例如,这样的软件可以在执行之前由服务器获得。该软件可以是定义挖掘操作的链逻辑软件的一部分。

[0077] 在实施例中,做市商——例如智能合约或其他软件——可以是链应用层的一部分。用户可以像在智能合约中一样调用所述程序。

[0078] 如果没有使用智能合约,则与智能合约相关联的钱包或池可以用与做市商相关联的钱包或池来替换,例如,用实现加密货币的软件来替换。

[0079] 注意,加密货币可以在有或没有智能合约的情况下创建。不需要创建或取消程序。例如,加密货币可以由链逻辑(例如定义分布式分类账的软件)来维护。然而,如果分布式分类账是为智能合约配置的,那么交易的公平处理就变得甚至更加重要。在这样的分布式分类账上可以定义潜在的无限数量的加密货币,并且它们中的每一种都依赖于交易的公平处理,并且潜在地易受攻击。

[0080] 还注意,链上的交易可能涉及加密货币的转移,无论是否由智能合约定义,但也可能涉及其他交易。分布式分类账可以用于安全地存储各种信息。

[0081] 为了完整性,一种用于在分布式分类账上维护第一类型加密代币的计算机实现的方法可以包括

-创建第一类型加密代币以兑换第二类型加密代币,以及取消第一类型加密代币以兑换第二类型加密代币,在分布式分类账上维护指示第一类型加密代币的当前数量的当前供应大小。创建、取消等可以在链逻辑中定义,或者可以在智能合约中定义,例如,存储在分布式分类账的区块中。如果使用联合曲线,则用于兑换的第二类型加密代币的金额可以通过对函数从当前供应大小到新供应大小进行积分来计算。该函数可以是联合曲线或从其导出的,例如联合曲线和费用项。例如,对于(例如,如创建程序中所定义的)创建,服务器设备可以将第二类型加密代币的金额转移到池中,并且将第一类型加密代币的所述金额转移到例如钱包中,并且使当前供应大小增加第一类型加密代币的所述金额。例如,对于(例如,如在取消程序中所定义的)取消,服务器设备可以从池中转移第二类型加密代币的金额,并且使第一类型加密代币的所述金额无效,并且使当前供应大小减少第一类型加密代币的所述金额,并且使第一类型加密代币的所述金额无效。

[0082] 图3a示意性地示出了分布式分类账系统300的实施例的示例。分布式分类账系统

300包括多个服务器设备。服务器设备被配置成用于分布式分类账系统的矿工；服务器设备被配置为有效地生成分布式分类账的新区块。图3a中示出了三个服务器设备：服务器设备301、302和303。可能存在两个服务器设备；可能存在多于三个服务器设备。

[0083] 分布式分类账系统300包括多个客户端设备。客户端设备被配置成分布式分类账系统的客户端；客户端设备被配置为向服务器设备发送交易请求。交易请求可以请求将加密代币（例如加密货币代币）从一个钱包转移到另一个钱包，例如将代币从一个地址关联到另一个地址，例如将其从一个加密密钥关联到另一个。图3a中示出了两个客户端设备：客户端设备311和312。可能存在多于两个客户端设备。

[0084] 服务器设备和客户端设备是电子设备，例如，它们可以包括计算机。

[0085] 服务器设备彼此之间互连。例如，这可以使用对等网络来完成。图3a示出了对等链路320。在这种情况下是服务器设备301和302之间以及服务器设备302和303之间。可以存在其间没有直接连接的服务器设备，例如服务器设备301和303之间。

[0086] 客户端设备用客户端到服务器链路311连接到服务器设备。例如，图3a中所示，客户端设备311连接到服务器设备301，并且客户端设备312连接到服务器设备302。客户端到服务器链路和对等链路都可以使用计算机网络（例如互联网）来实现。

[0087] 客户端设备可以被配置为向服务器设备发送交易请求。服务器设备被配置为接收多个交易以包括在分布式分类账中。服务器设备可以直接从客户端接收交易请求；例如，服务器设备301可以例如通过链路316直接从客户端设备311接收交易请求。然而，服务器设备也可以实现对等同步协议。例如，第一服务器设备可以将他从客户端设备接收的交易发送到第二服务器设备。

[0088] 例如，服务器设备301可以从客户端设备311接收的交易请求可以由服务器设备301转发到服务器设备302，并进而转发到服务器设备303。注意，尽管服务器设备301和303没有直接链路，它们仍然以对等方式交换交易请求。在实施例中，以分散的方式接收交易请求。这种方法的缺点是，要包括在区块中的潜在交易池对于所有矿工来说并不总是相同的。下面呈现了该问题的解决方案。

[0089] 对等联网的优点是不需要预先确定网络的拓扑。只要每个服务器设备知道（例如存储）其他服务器设备的一个或多个计算机地址，并且当网络保持连接时，完全的连接性仍然是可能的。可以使用替代的通信技术来代替对等网络。例如，网络可以是完全连接的，其中每个服务器设备与每个其他服务器设备通信。例如，网络可以是集中式的。例如，为了分发交易请求或新区块等，它可以被发送到中央服务器设备，中央服务器设备又将它分发给其他服务器设备。

[0090] 服务器设备被配置为生成分布式分类账的新区块。为此，服务器设备从其接收的多个交易请求中选择一组交易。这组交易被包括在区块中，可能在一些重新格式化或重写之后。交易和交易请求可以包括要将哪个代币从哪个地址转移到哪个其他地址。交易也可以与智能合同相关。例如，交易请求可以触发智能合同的创建程序或取消程序。对于通过智能合同创建的加密货币，抢先交易攻击也是一种威胁。

[0091] 服务器设备进一步在该区块中包括共识代币。共识代币取决于分布式分类账的特定类型，例如，它可以是对密码问题的解决方案，例如在工作证明系统（PoW）中，或者它可以是示出利害关系证明（PoS）或授权证明（PoA）的共识代币。该区块可以进一步指示创建该区

块的服务器设备(例如矿工)例如包括服务器设备的数字签名。

[0092] 矿工还将为自己分配某一金额的加密代币。这些代币可能来自何处存在各种选项,这也取决于分布式分类账的特定类型。例如,通过挖掘分布式分类账(例如区块链)的新区块,可以创建某一金额的加密货币,例如如在比特币中。该金额的加密货币的全部或部分可以被分配给创建该区块的服务器设备,例如矿工。加密货币的第二来源可能来自交易本身。交易请求可以将它与交易费用相关联。可以将全部或部分费用分配给挖掘新区块的服务器设备。交易也可能是智能合同执行的一部分。智能合同执行还伴随有交易费用,交易费用的全部或部分可以被分配给实行该执行并在新生成的区块中提供其证明的服务器设备。

[0093] 通常,服务器设备有自由选择要包括在区块中的交易。例如,如果不是所有的服务器设备都具有对同一交易的访问,那么这可能是有益的。在这样的情况下,一交易可能没有被选择仅仅是因为服务器设备不知道该交易。服务器设备还可以优先化承载较高费用的交易。对于其本身这并不一定是坏事。如果交易应该快速执行,则用户可以将它与高交易费用相关联,使得它将被快速拾取。如果交易的执行不是特别紧迫,则可以分配较低的交易费用。这可能意味着在服务器设备拾取它之前将要花上一段时间,但是成本更低。

[0094] 不幸的是,完全自由的交易选择使分布式分类账系统暴露于一类被称为基于审查的抢先交易的攻击。在抢先交易中,攻击使买入和卖出交易囊括在一串买入交易周围。这一串买入交易将驱使加密货币的价格上涨,使得攻击者后续的卖出交易将获得比囊括成本中攻击者买入交易更高的价格。为了执行攻击,攻击者需要知道一串买入交易正在到来,或者至少是一串主要是买入的交易。如果服务器设备或者甚至多个服务器设备非法地商定暂时不选择卖出交易,那么这是可以实现的。当处理了囊括的卖出交易时,处置卖出交易的积压。

[0095] 换句话说,服务器设备可以利用它们的能力来选择包括在新区块中的交易,以实现分布式分类账系统的攻击。这些攻击拥有多种类型的加密货币,只要代币的价格随着需求上升,就可以执行审查抢先交易攻击。攻击特别可能针对基于联合曲线的加密货币(例如在智能合同或链逻辑中实现的)。链接到联合曲线的加密货币的价格链接到现有代币的体量,因此一串买入交易(或创建交易)将因此具有更高的价格。

[0096] 可以通过使得对于服务器设备而言参与这样的攻击没那么有吸引力来减轻基于审查的抢先交易。例如,在实施例中,为成功完成新区块而分配给服务器设备的加密代币可以取决于优度分数。可以由服务器设备通过评估其对于一个或多个选择规则的合规性来计算优度分数。选择规则指示应该如何选择分布式分类账的新区块的交易,或者给出应选择什么交易的界限。

[0097] 当区块被敲定时,服务器设备基于该矿工的优度将该区块的可用费用的一部分分配给它自己。剩余代币可以隐式或显式地分配到别处。例如,分布式分类账可以被配置为所有未分配的代币被自动收集在池(例如钱包)中。例如,矿工可以显式地将剩余代币分配到别处(例如池、钱包),将它们返回给交易的发起者。

[0098] 当区块被敲定时,新区块可以被转移到一个或多个另外的矿工。例如,比如服务器设备301敲定一个区块,则它可以将该区块发送给服务器设备302,服务器设备302将最终将其发送给服务器设备303。直接或集中式通信也是可能的。

[0099] 在实施例中,服务器设备可以将可用费用的较大部分分配给它自己,但是这可能

被其他服务器设备捕捉并纠正。

[0100] 例如,假设第一矿工(比如服务器设备301)计算新区块,包括向其自身分配代币。当其他服务器设备接收到该区块时,它们将认证该区块中的交易,例如,该交易是否表示代币的有效转移(例如,从第一钱包到第二钱包),或者表示智能合同的有效执行,或者有效执行的一部分。接收声称的新区块的服务器设备(比如服务器设备302)也将认证由它的矿工(例如服务器设备301)分配的代币是否合理,特别是通过它的优度分数是否合理。如果例如交易有效性或分配的代币的认证失败,则拒绝该区块。

[0101] 可以由生成新区块的矿工(例如,服务器设备)以及认证新区块的矿工来计算优度分数。优度分数指示生成新区块的矿工对选择规则的合规性。选择规则指示要如何从可供矿工包含的交易请求中选择新区块的交易。例如,选择规则可能要求应当选择比第一阈值旧并且具有的交易费用高于第二阈值的交易请求。例如,选择规则可以要求应当选择比第一阈值旧并且具有的交易费用至少与任何未被选择的更近交易请求一样高的交易请求。违反规则的次数可能计入惩罚。例如,惩罚的数量可以是减少分配的代币的百分比等。

[0102] 除了选择规则之外,还可以存在其他规则来指示对矿工可用的代币部分。例如,规则可以设置期望的正常运行时间、服务质量、生成新区块的最大等待时间。这样的规则可以被称为优度规则,其中选择规则是特别重要的示例。

[0103] 可以在管控服务器设备的软件中(例如在链逻辑中)设置优度规则。原则上,优度规则可以是固定的,尽管它们可以通过更新服务器设备的软件来改变。优度规则可以被公布,并且可用于服务器设备。特别地,优度规则可以在分布式分类账的区块中公布。例如,优度规则可以由智能合同来设置。例如,可以通过系统的管控者或智能合同来改变优度规则。例如,可以在分布式分类账的新区块中发布新的优度规则。智能合同可以自动发布新规则。例如,可以触发智能合同来调整现有规则。例如,如果与智能合同相关联的池中的增长(例如,其中存放与新区块相关联的代币的一部分)落后于目标。新规则也可以手动发布,例如在区块中发布。如果交易请求的积压增长,那么不选择旧交易的惩罚可能增加。这样的规则改变可以自动引入,例如通过智能合同。例如,如果智能合同由条件触发,则可以实现规则改变。

[0104] 选择规则是优度规则的重要应用,因为它们有助于使基于审查的抢先交易无利可图。如果一组共谋服务器设备因参与审查而丢失的代币(由于相关联的违反选择规则)多于审查攻击所获得的代币,则该攻击不再有利可图,或者至少其盈利能力已经降低。该措施使得服务器设备不太可能会试图参与审查,因为这类型对系统的攻击不再起作用。

[0105] 例如,在实施例中,交易请求具有年限,并且其中如果没有选择具有旧年限的交易请求,则合规性被评估为较低。例如,交易请求的年限可以是当前时间和日期与交易请求第一次被发送到服务器设备的时间和日期之间的差。

[0106] 选择规则可以是挑选最旧的可用交易。选择规则可以计算交易适合度,例如作为年限和交易费用的函数,并挑选最高的一个。基础一方面是附加到交易请求的交易费用,并且另一方面是年限。

[0107] 例如,函数可以指示交易的紧急度,作为附加到交易请求的交易费用 t 和交易年限 a 的函数。例如,紧急度函数可以是乘积 at 或总和 $a+t$ 。例如,年限和费用可以在总和或乘积中加权,例如 γat ,或比如 $a^{\gamma_1} t^{\gamma_2}$ 或 $\gamma_1 a + \gamma_2 t$ 等。例如,紧急度函数可以是总和或乘

积中和/或它们的加权变量等方面的多项式。一般来说,紧急度函数可以是两个变量方面均增加的二元函数。

[0108] 如果交易请求的紧急度函数超过阈值,则该交易请求可以被视为紧急的。如果紧急交易请求没有被处理,则服务器设备可能受到惩罚,例如,接收减少部分的交易费用。

[0109] 在实施例中,交易的交易费用的金额(例如百分比)被转移到池中。百分比可能随着年限而降低。因此,对于较旧的交易请求,矿工有效取回的费用变得更大,并且池中收集的代币可以被转移到处理旧请求的服务器设备,以另外激励对较旧交易请求的挖掘。

[0110] 例如,当第一矿工(例如,服务器设备,例如,服务器设备301)从另一矿工(例如,服务器设备302)接收到声称的分布式分类账的新区块时,则第一矿工(例如,服务器设备301)将参与多次检查,以查看该区块是否可以被接受为有效。服务器设备将认证常规检查。例如,如果该区块包含从第一钱包到第二钱包的代币转移,则服务器设备可以认证该代币是否实际绑定到第一钱包,或者第一钱包是否有足够的资金,等等。如果交易涉及智能合同的执行,则服务器设备可以认证正确执行对应于交易。例如,创建和取消交易作为示出智能合同执行的交易可能在分类账上是可见的。

[0111] 服务器还将认证分配给第二服务器设备自身的代币是否正确。例如,第一服务器设备可以例如通过再次评估第二矿工对一个或多个选择规则的合规性来再次计算优度分数。根据优度分数,可以计算出可以分配的费用金额。

[0112] 如果任何检查失败,则该区块被拒绝。这意味着第二矿工实际上将不会接收到资金,因为新区块将不会成为分布式分类账的一部分。

[0113] 因此,在实施例中,一个矿工提议,其他矿工认证——并且从而形成关于区块的激励/优度和有效性的共识。例如,在实施例中,矿工委员会可以根据用于提议区块的特定协议一起工作。然后,一个矿工提议该区块。例如,根据矿工选择协议或规则,可以从成员中选择哪个矿工提议下一个区块。然后,矿工验证该区块。在验证中,他们还可以确定优度分数等,并就挖掘奖励形成共识。该实施例在PoS或PoA系统中工作良好。

[0114] 在实施例中,一组多个服务器设备被配置为从它们之中选择一个服务器设备来提议新区块,所选服务器设备生成新区块,并且剩余的服务器设备验证该新区块。在实施例中,选择一个服务器设备与创建商定的交易请求列表相结合。

[0115] 对每个服务器设备可见的交易请求可能不总是相同的。尤其是当使用对等协议来分发交易请求时,每个服务器设备对交易请求具有的看法可能不同。服务器设备甚至可能有动机不分发一些请求,例如作为审查攻击的一部分,或者避免具有特别高的交易费用的交易请求被竞争的服务器设备处理。

[0116] 这些问题可以通过首先构建商定的交易请求列表来减轻,必须从该列表中为新区块选择交易。如果交易被包括在不在商定的交易请求列表上的新区块中,则该新区块可能被其他服务器设备拒绝。

[0117] 例如,在实施例中,服务器设备可以被配置用于同步协议,在该同步协议中,包括在分布式分类账中的交易请求被同步。例如,服务器设备可以继续向彼此转发交易请求,但是有时服务器设备创建其未决交易请求列表的快照,并将其转发给其他服务器设备。其他服务器设备可以接受该列表为有效的,例如,因为服务器设备的特殊状态。可以使用协议来为新的商定的交易请求列表选择服务器设备。

[0118] 商定的交易请求列表的一个优点是可以在每个服务器设备处确定性地计算优度分数。另一个优点是,从这样的列表中可以看出服务器设备是否正在篡改选择过程,例如通过审查卖出或买入交易。这样的服务器设备可以通过其优度分数来惩罚,但也可能通过越界机制来惩罚,例如将服务器设备从分布式分类账系统中排除。

[0119] 例如,矿工可以将交易请求放在全局交易请求列表上。不选择旧交易请求的矿工可能受到惩罚。例如,认证矿工可以通过将区块中的交易与交易请求列表中交易的时间戳进行比较来计算新区块中交易的年限。

[0120] 在实施例中,服务器设备被配置为生成用于包括在具有一组矿工的分布式分类账中的商定交易列表,并从商定交易中选择该组交易。

[0121] 例如,矿工可以在池中生成商定的交易请求列表,并且每个矿工签署散列的交易请求池列表或类似物。

[0122] 例如,如下面讨论的,可以通过集中式设备来完成对交易请求列表的商定。也可以通过多方计算来完成对交易请求列表的商定。例如,为了达成协定,服务器设备可以被配置用于可检测的广播协议。可检测的广播令一方向所有方(例如所有服务器设备)发送消息,使得所有方接收相同的消息,或者所有方商定广播失败。与完全广播不同,可检测广播可以通过专用信道(诸如对等网络)实现。例如,参见M. Fitzi, N. Gisin, U. M. Maurer和O. von Rotz的论文“Unconditional Byzantine agreement and multi-party computation secure against dishonest minorities from scratch”。

[0123] 例如,服务器设备可以通过它们中的每一个向彼此发送它们的本地交易请求列表来同步它们的列表。商定列表可以是所接收列表中请求的并集。

[0124] 在实施例中,任何一个或所有服务器设备可以向用户输出商定列表。例如,服务器设备的网页或API等可以被配置用于访问商定列表。这可以被用户用来认证服务器设备是诚实的。此外,用户可以检查他提交的交易请求是否成功到列表上。

[0125] 在实施例中,用户(例如客户端设备)向服务器设备提交交易请求。服务器设备发回包括时间戳或区块号的签名收据。以这种方式,用户可以在以后证明他的交易请求已经提交,但是没有成功到列表,或者没有被处理。

[0126] 图3b示意性地示出了分布式分类账系统的实施例的示例。图3b示出了交易请求聚合器331。系统300中可以采用或不采用聚合器331。

[0127] 例如,所有服务器设备可以将它们接收到的任何交易请求转发给聚合器331。聚合器331可以将交易请求编译成单个聚合列表,例如剔除重复的请求,例如提交给多个服务器的请求。聚合器331可以周期性地向服务器设备发送聚合列表。新区块中的交易可以从聚合列表中选择,事实上它们甚至可能被要求从聚合列表中选择。

[0128] 在实施例中,聚合器331可以被配置为向分布式分类账系统提交新交易列表。分布式分类账系统可以是不同的系统,但甚至可以是同一分布式分类账系统。

[0129] 被示为客户端设备311的客户端设备可以联系聚合器331,以获得当前商定的交易请求列表。如果聚合器331在分布式分类账中看到新区块,则已处理的交易(例如新区块中的交易)可以从商定列表中移除。交易可以继续从聚合器331可获得,例如,以认证它们的年限。

[0130] 图4示意性地示出了用于由第一矿工维护分布式分类账的方法500的实施例的示

例。方法500包括

- 接收 (510) 多个交易请求以包括在分布式分类账中,
- 从所述多个交易请求中选择 (520) 一组交易,
- 生成 (530) 包括一组所选交易的分布式分类账的新区块,
- 通过评估第一矿工对一个或多个选择规则的合规性来计算 (540) 第一优度分数, 所述一个或多个选择规则指示用于为分布式分类账的新区块选择交易的规则,
- 敲定 (550) 新区块并将所述区块转移到一个或多个另外的矿工, 以及
- 向第一矿工分配 (560) 与第一优度分数成比例的加密代币的金额。

[0131] 例如, 所述方法可以是计算机实现的方法。例如, 从分布式分类账获得智能合同可以包括例如通过计算机网络或在本地数据库中从分布式分类账检索区块。执行智能合同可以在微处理器上完成。例如, 智能合同可以用解释语言编写, 该解释语言可以由解释器、虚拟机等执行。对曲线进行积分可以包括执行计算, 例如, 在联合曲线的基元或反导数(封闭形式的组成部分)中插入当前供应和新供应。基元可以是以封闭形式的, 并且可以包括多个基元段。接收创建或取消请求可以通过计算机网络进行。转移第一类型代币或第二类型代币可以包括将转移写入区块中以包含在分布式分类账的区块中。该区块可以包括共识机制, 例如工作证明或利害关系证明。

[0132] 如将对本领域技术人员而言清楚的是, 执行所述方法的许多不同方式是可能的。例如, 步骤的次序可以按照所示的次序来执行, 但是步骤的次序可以变化或者一些步骤可以并行执行。此外, 在步骤之间中可以插入其他方法步骤。插入的步骤可以表示诸如本文描述的方法的改善, 或者可以与该方法无关。例如, 一些步骤可以至少部分地并行执行。此外, 在下一个步骤开始之前, 给定的步骤可能还没有完全完成。

[0133] 该方法的实施例可以使用软件来执行, 该软件包括用于使得处理器系统执行方法500的指令。软件可能仅包括由系统的特定子实体采取的那些步骤。软件可以存储在合适的存储介质中, 合适的存储介质诸如是硬盘、软盘、存储器、光盘等。该软件可以作为信号沿着有线或无线或使用数据网络(例如互联网)发送。可以使软件可用于下载和/或在服务器上远程使用。该方法的实施例可以使用比特流来执行, 该比特流被布置为配置可编程逻辑(例如现场可编程门阵列(FPGA)), 以执行该方法。

[0134] 将领会, 当前公开的主题还扩展到适于将当前公开的主题付诸实践的计算机程序, 特别是载体上或载体中的计算机程序。该程序可以是以源代码、目标代码、代码中间源和目标代码的形式, 诸如部分编译的形式, 或者是以适合用于实现该方法的实施例的任何其他形式。涉及计算机程序产品的实施例包括对应于所阐述方法中至少一种方法的每个处理步骤的计算机可执行指令。这些指令可以细分为子例程和/或存储在可以静态或动态链接的一个或多个文件中。涉及计算机程序产品的另一个实施例包括与所阐述的系统和/或产品中至少一个的每个设备、单元和/或部分相对应的计算机可执行指令。

[0135] 图5a示出了具有可写部分1010的计算机可读介质1000, 以及也具有可写部分的计算机可读介质1001。计算机可读介质1000以光学可读介质的形式示出。计算机可读介质1001以电子存储器的形式示出, 在这种情况下是存储卡。计算机可读介质1000和1001可以存储数据1020, 其中该数据可以指示指令, 该指令当由处理器系统执行时, 使得处理器系统执行根据实施例的维护分布式分类账的方法的实施例。计算机程序1020可以作为物理标记

或通过计算机可读介质1000的磁化在计算机可读介质1000上体现。然而,也可设想到任何其他合适的实施例。此外,将领会,尽管计算机可读介质1000在这里被示出为光盘,但是计算机可读介质1000可以是任何合适的计算机可读介质,诸如硬盘、固态存储器、闪速存储器等,并且可以是不可记录的或可记录的。计算机程序1020包括用于使得处理器系统执行所述方法的指令。

[0136] 图5b示出了根据用于维护分布式分类账的设备的实施例的处理器系统1140的示意性表示。处理器系统包括一个或多个集成电路1110。图5b中示意性地示出了一个或多个集成电路1110的架构。电路1110包括处理单元1120,例如CPU,用于运行计算机程序组件来执行根据实施例的方法和/或实现其模块或单元。电路1110包括用于存储程序代码、数据等的存储器1122。存储器1122的一部分可以是只读的。电路1110可以包括通信元件1126,例如天线、连接器或两者,等等。电路1110可以包括专用集成电路1124,用于执行该方法中定义的部分或全部处理。处理器1120、存储器1122、专用IC 1124和通信元件1126可以经由互连1130(比如总线)彼此连接。处理器系统1110可以被布置用于分别使用天线和/或连接器进行接触和/或无接触通信。

[0137] 例如,在实施例中,处理器系统1140(例如,用于分布式分类账的设备)可以包括处理器电路和存储器电路,该处理器被布置为执行存储在存储器电路中的软件。例如,处理器电路可以是Intel Core i7处理器、ARM Cortex-R8等。在实施例中,处理器电路可以是ARM Cortex M0。存储器电路可以是ROM电路或者非易失性存储器,例如闪速存储器。存储器电路可以是易失性存储器,例如SRAM存储器。在后一种情况下,该设备可以包括被布置用于提供软件的非易失性软件接口,例如硬盘驱动器、网络接口等。

[0138] 应当注意,上面提及的实施例说明而不是限制当前公开的主题,并且本领域技术人员将能够设计许多替代实施例。

[0139] 在权利要求中,置于括号之间的任何附图标记都不应被解释为限制权利要求。动词“包括”及其变形的使用不排除权利要求中所陈述元件或步骤之外的元件或步骤的存在。元件前面的冠词“一”或“一个”不排除多个这样的元件的存在。诸如“至少一个”之类的表达在元件列表之前时表示从列表中选择所有元件或元件的任何子集。例如,表达“A、B和C中的至少一个”应当理解为仅包括A、仅包括B、仅包括C、A和B两者、A和C两者、B和C两者、或者A、B和C全部。当前公开的主题可以通过包括若干不同元件的硬件以及通过适当编程的计算机来实现。在列举了几个部分的设备权利要求中,这些部分中的几个可以由同一个硬件项目来体现。在相互不同的从属权利要求中引用某些措施的仅有事实并不指示这些措施的组合不能被有利地使用。

[0140] 在权利要求中,括号中的参考标记指代示例性实施例的附图中的参考标记或实施例的公式,因此增加了权利要求的可理解性。这些参考标记不应被解释为限制权利要求。

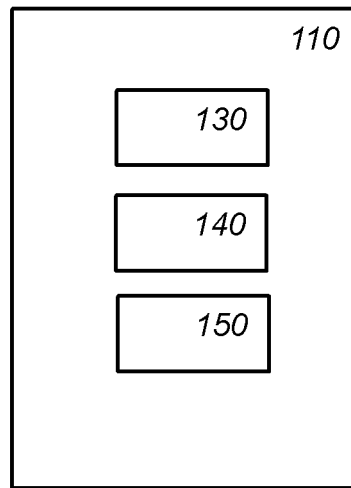


图 1a

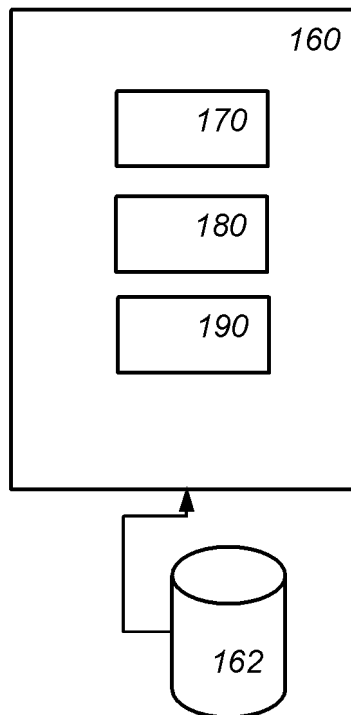


图 1b

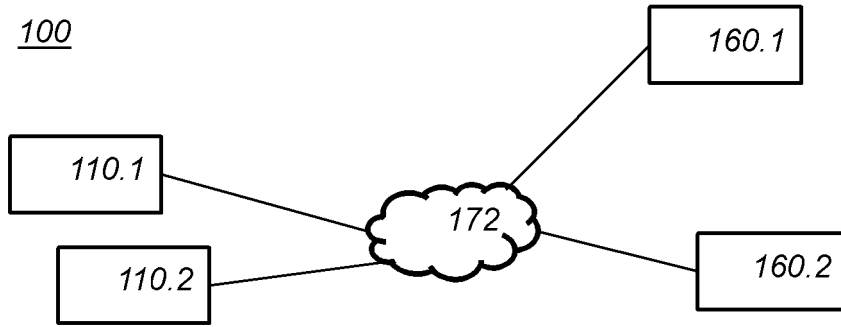


图 1c

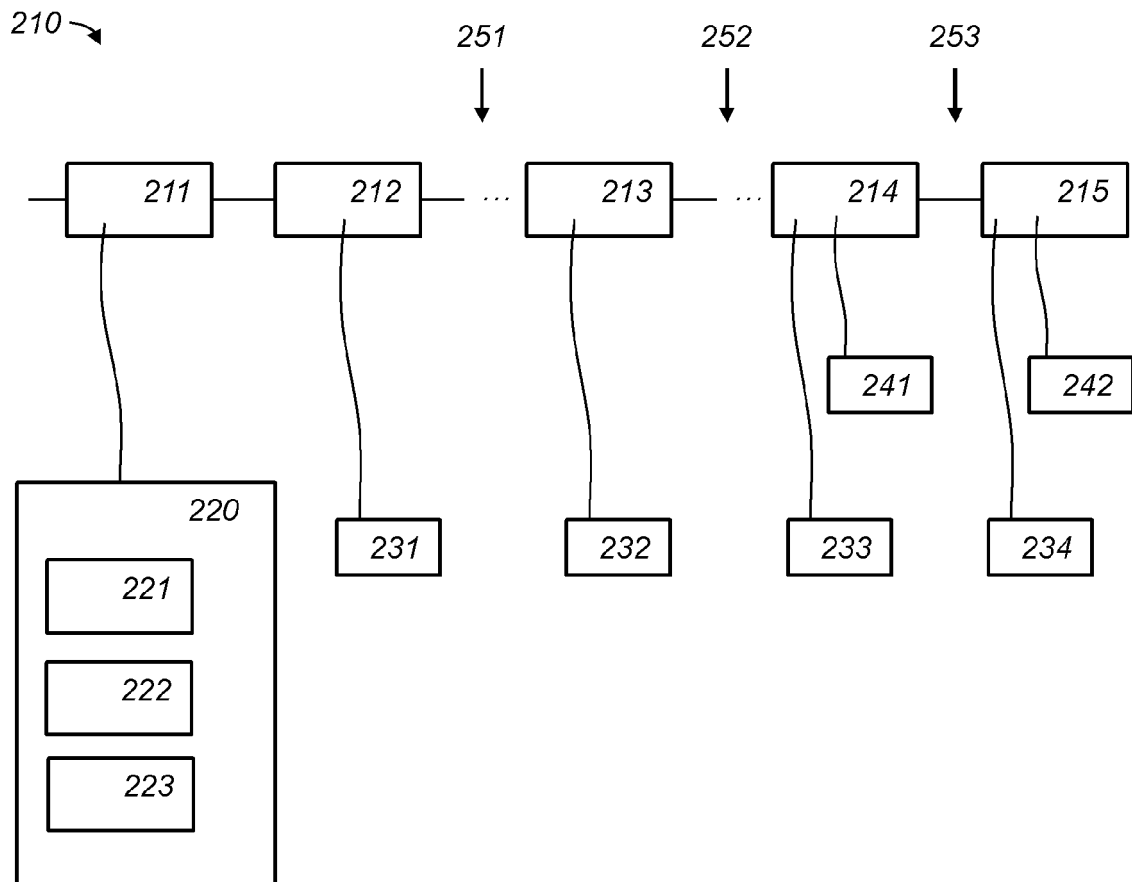


图 2

300 ↗

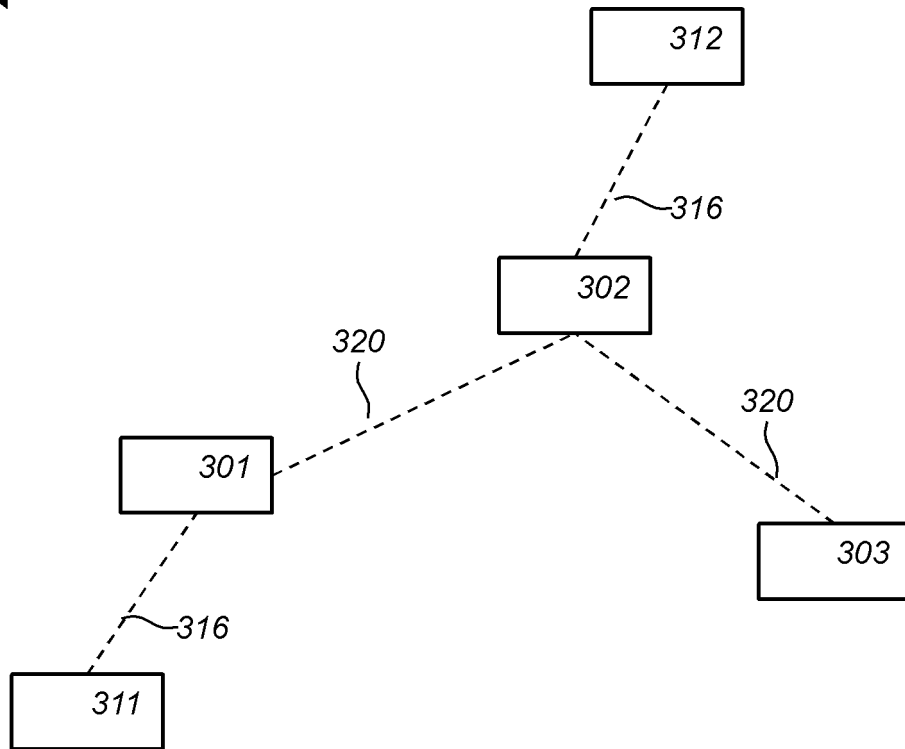


图 3a

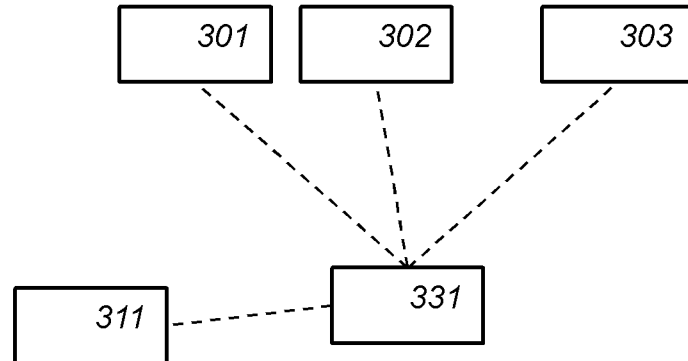


图 3b

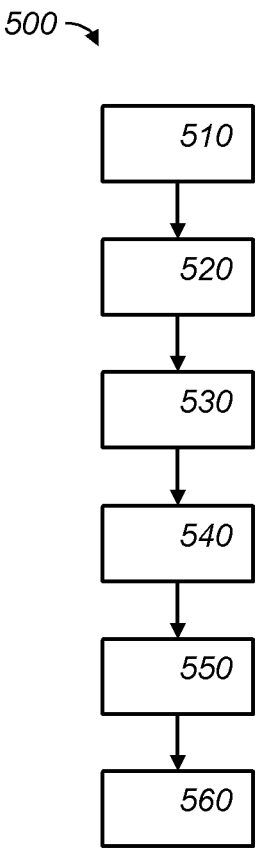


图 4

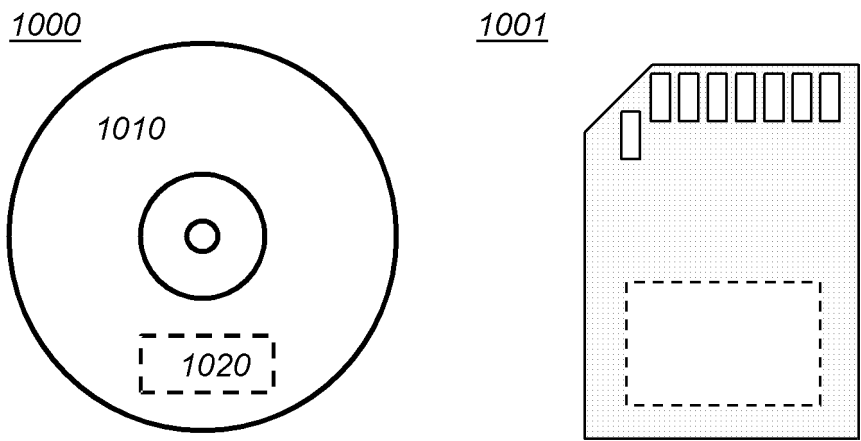


图 5a

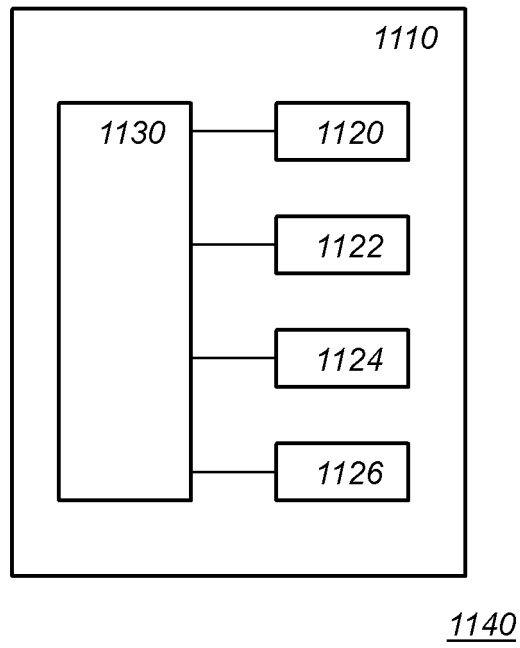


图 5b