(19)国家知识产权局

(12)发明专利

(10)授权公告号 CN 110751468 B
(45)授权公告日 2023.04.28

(21)申请号 201910906584.1

(22)申请日 2019.09.24

(65)同一申请的已公布的文献号
申请公布号 CN 110751468 A

(43)申请公布日 2020.02.04

(73)专利权人 上海交通大学
地址 200240 上海市闵行区东川路800号

(72)发明人 周琪武 龙宇 刘志强 刘振 谷大武

(74)专利代理机构 上海汉声知识产权代理有限公司 31236
专利代理师 胡晶

(51)Int.Cl.
G06Q 20/06(2012.01)
G06Q 20/38(2012.01)
G06Q 20/40(2012.01)
G06Q 40/04(2012.01)

(56)对比文件
CN 107330787 A,2017.11.07
CN 109345714 A,2019.02.15
CN 109583868 A,2019.04.05
CN 110223066 A,2019.09.10
CN 110223067 A,2019.09.10
Andrew Miller et al..Sprites and State Channels: Payment Networks that Go Faster than Lightning.《arXiv》.2017,第1-24页.
潘晨 等.区块链可扩展性研究:问题与方法.《计算机研究与发展》.2018,第55卷(第10期),2099-2110.

审查员 张红云

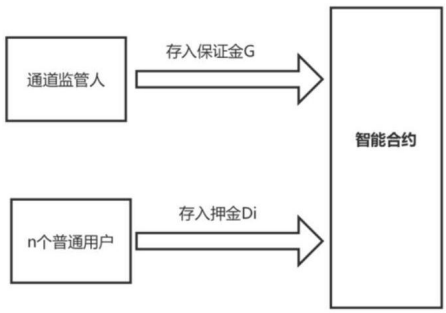
权利要求书4页 说明书16页 附图2页

(54)发明名称

用于区块链扩展的多向状态通道方法、系统及介质

(57)摘要

本发明提供了一种用于区块链扩展的多向状态通道方法、系统及介质，包括：通道建立步骤：通过通道监管人S和多个普通用户合作建立一个多向支付的链下通道；通道支付步骤：在建立的多向支付的链下通道内，普通用户之间进行交易，监管人S根据普通用户之间的交易信息，向多个普通用户发送通道状态更新信息。本发明提出了一种高效的支持并行的多向状态通道方案，有效解决了多个用户之间存在高频的双向支付的应用场景。在跨通道支付的路由方面，相比于基于双向支付通道构建的闪电网络和雷电网络，具有更好的性能。



通道建立阶段，n个普通用户节点和一个通道监管人S合作建立一个多向支付的链下通道。

CN 110751468 B

1.一种用于区块链扩展的多向状态通道支付方法,其特征在于,包括:

通道建立步骤:通过通道监管人S和多个普通用户合作建立一个多向支付的链下通道;

通道支付步骤:在建立的多向支付的链下通道内,普通用户之间进行交易,监管人S根据普通用户之间的交易信息,向多个普通用户发送通道状态更新信息;

通道关闭步骤:任意用户赎回押金,则关闭该用户的支付通道,同时作恶检测合约检测通道监管人S是否存在作恶行为:若是,则关闭所有通道;否则,则继续检测通道监管人S是否作恶;

所述通道建立步骤:

n个普通用户节点和一个通道监管人S合作建立一个多向支付的链下通道,任意普通用户可以通过在智能合约中冻结足够的保证金成为通道监管人;

在通道建立阶段时,通道内的所有普通用户均需要认可监管人S的身份并获知S的公钥,S获知通道内普通用户节点的公钥;

所有普通用户节点需要向通道中存入自己的押金D_i(1≤i≤n),而通道监管人S需要在通道中存入自己的保证金G并将其冻结至通道关闭,保证金G用来防止通道监管人的作恶行为,一旦普通用户节点中的任意节点将通道监管人作恶的证据提交到链上的作恶检测合约V_f,并且验证通过,保证金将作为罚金平均转入到通道内的所有普通节点账户中;

为了保证通道内普通用户节点不会受到损失,通道监管人的保证金金额需要满足以下等式:

$$G=n\times\sum_{i=1}^{n}D_i$$

当监管人作恶时,每个普通用户节点将会收到数目为$\sum_{i=1}^{n}D_i$的金额作为赔偿金;

所述通道支付步骤:

当通道内的多个普通用户想产生一笔转账交易时,首先多个普通用户之间沟通转账交易的金额,由收款方生成转账交易信息TxMsg=(sender,receiver,amount,r,TxID)sig_{sender},$sig_{receiver}$,其中,sender表示交易发送者,receiver表示交易接收者,amount表示转账金额,r表示当前交易所在的轮数,是根据交易双方已经获知的最新状态更新信息的轮数加一计算得出;TxID,一个8bit的数,用于唯一标记sender和receiver在其认为的第r轮中的某一次交易,TxID的引入是为了方便用户可以在一轮中进行多次交易,sigsender表示该消息需要转账发送者的签名,sigrecevier表示该消息需要转账接收者的签名;

收款方在签名后,将该转账交易信息发送至付款方,付款方核实转账金额是否符合预期,收款人和付款人是否为目标用户,核实正确后签名该信息,并将其发送给通道监管人S;通道监管人S收集每一轮中收到的转账交易信息,验证转账交易信息的合法性,发出当前轮的状态更新信息StateMsg;

当进行交易的多个普通用户收到由通道监管人S广播的新一轮状态更新信息StateMsg时,验证状态更新信息StateMsg的合法性:核实收到的r至r+Δ轮状态更新信息是否包含当前用户已发出的第r轮转账交易信息,如果存在,则表明当前转账交易完成;如果不存在则表明转账交易信息已经失效,需要重新生成一笔新的转账交易信息发送至通道监管人S,或者取消此次交易;

其中,Δ为系统选定参数,用于指定转账交易消息被状态更新信息延迟包含的最大轮

数。

2.根据权利要求1所述的用于区块链扩展的多向状态通道支付方法,其特征在于,所述通道支付步骤:

所述转账交易信息TxMsg是由发生交易的收款方进行生成,发送给付款方,付款方确认无误并签名后发送给通道监管人S,该消息用于让通道监管人获知交易双方想要达成的交易内容及交易意愿,由于附有交易双方的签名,因此可以作为通道余额状态更新时的凭据;

$TxMsg = (sender,receiver,amount,r,TxID)sig_{sender},sig_{receiver}$

所述通道状态更新信息StateMsg是由通道监管人签名发布,用于表示在该轮中通道内部的各用户账户余额信息,该通道状态更新信息包含本轮由通道监管人S认可的转账交易信息列表;

每个用户可以根据附在通道状态更新信息内的转账交易信息列表,核实转账交易信息的签名是否正确,本轮的各账户余额是否与预期相符,根据转账交易信息所表示的转账,以及上一轮的各账户余额,可以推算出当前轮的各账户余额;

一旦用户发现通道状态更新信息与预期不符,即可向链上的作恶检测合约提起申诉并提交监管人作恶证据,保证自身资金的安全性;

$StateMsg=(Amountarray[n],TxMsgList,r)sig_S$

其中,Amountarray[n]表示当前轮通道内n个人的账户余额,TxMsgList表示在该轮由通道监管人认可的转账交易消息TxMsg列表,r表示当前通道状态更新的轮数,sig_S表示通道监管人S的签名。

3.根据权利要求2所述的用于区块链扩展的多向状态通道支付方法,其特征在于,所述通道支付步骤:

所述验证转账交易信息的合法性指:

核实转账交易信息是否有付款方和收款方的签名认可;

检验转账交易信息中的轮数是否合法,即核实转账交易信息中的轮数是否在$r-\Delta$到r之间,r表示当前通道状态更新的轮数,Δ为系统选定参数,如果轮数不在此范围内,认为该转账交易信息已失效,拒绝该转账交易信息;

检查TxID值是否合法,即校验TxID值是否在相应的交易用户第r轮转账交易信息中存在,如果已经存在,则拒绝该转账交易信息;

根据上一轮状态更新信息中的各账户余额,以及当前轮已经认可的转账交易信息,计算出当前各用户的余额情况,检验交易的付款方余额是否大于等于转账金额,如果余额不足以支持该笔转账,则拒绝该转账交易信息。

4.根据权利要求3所述的用于区块链扩展的多向状态通道支付方法,其特征在于,所述通道关闭步骤:

所述作恶检测合约检测通道监管人S是否存在作恶行为:

所述作恶行为包括:

发布失效信息行为:发布包含失效转账交易信息的通道状态更新信息,导致用户的余额与实际余额不符;

发送错误信息行为:发布用户余额计算错误的通道状态更新信息;

对于发布失效信息行为,用户在通道建立后至通道关闭前,可以向作恶检测合约提交

一轮错误的通道状态更新信息StateMsg=(Amountarray[n],TxMsgList,r)sig_S,作恶检测合约进行如下验证:

验证状态更新信息通道监管人签名是否合法;

验证转账交易信息列表TxMsgList中所有转账交易信息的所在轮数r′是否在r-Δ到r之间,如果不在,则表明通道监管人作恶,将通道内的保证金分配给通道内的所有节点并关闭通道;

对于发送错误信息行为,用户在通道建立后至通道关闭前,向作恶检测合约提交连续两轮通道状态更新信息$StateMsg_{r1}$=(Amountarray[n]r1,TxMsgList,r1)sig_S与$StateMsg_{r1+1}$=(Amountarray[n]r1+1,TxmsgList,r1+1)sig_S作为证据,作恶检测合约进行如下验证:

验证两轮的状态更新信息通道监管人签名是否合法;

基于r1轮的用户余额列表Amountarray[n]r1,结合第r1+1轮的转账交易信息列表TxMsgList,计算得出第r1+1轮的用户余额列表A_1,与$Amountarray[n]_{r1+1}$进行比较,如果二者不相等,则表明通道监管人作恶,将通道内的保证金分配给通道内的所有节点并关闭通道。

5.根据权利要求4所述的用于区块链扩展的多向状态通道支付方法,其特征在于,所述通道关闭步骤:

用户赎回步骤:

若普通用户节点P_i想要赎回自己在支付通道内的押金,则需要在区块链中公布自己认为的最新状态更新信息StateMsg=(Amountarray[n],TxMsgList,r)sig_S,即通知所有人核实赎回人节点P_i的状态:若核实无误,则普通用户节点P_i成功赎回押金,关闭普通用户节点P_i的支付通道;若有误,则系统判定为用户作恶而被罚没所有押金,关闭普通用户节点P_i的支付通道;

在普通用户节点P_i赎回押金时,判断节点P_i是否存在待监管人处理的转账交易信息:如果存在待处理的转账交易信息,则需要等待至交易被处理或者该转账交易信息被判断为失效后,才能发起押金赎回申请,否则会由于在发起押金赎回操作后,状态更新信息中的个人用户余额仍在发生变化,被系统判定为用户作恶而被罚没所有押金;

作恶检测步骤:

通过将赎回押金的操作在区块链上打开一个时间窗口,防止P_i公布之前已作废的通道状态和监督监管人的作恶行为,在打开的时间窗口这段时间内P_i的押金将被冻结在通道中,并且所有通道内的节点可以向作恶检测合约提交节点认为的正确状态,一旦发现通道监管人作恶或P_i试图赎回不是自己实际余额的金额,作恶检测合约可以通过作恶证据自动惩罚作恶方。

6.根据权利要求5所述的用于区块链扩展的多向状态通道支付方法,其特征在于,所述作恶检测步骤:

节点P_i将其认可的最新通道状态信息StateMsg1=(Amountarray[n],TxMsgList,r1)sig_S和作恶证据StateMsg2=(Amountarray[n],TxMsgList,r2)sig_S的状态更新信息提交给作恶检测合约V_f的处理,作恶检测合约V_f的处理流程如下:

验证状态更新消息StateMsg1中通道监管人S的签名;

验证状态更新消息StateMsg1的正确性，确保转账交易信息列表的所有交易轮数均在有效轮数范围内；

打开仲裁时间窗口，在这段时间内通道内的节点可以提交作恶证据；

验证状态更新消息StateMsg2中S的签名；

验证状态更新消息StateMsg2的正确性，确保转账交易信息列表的所有交易轮数均在有效轮数范围内；

如果r1=r2，且StateMsg2≠StateMsg1，则认为监管人作恶，将通道内的保证金分配给通道内的所有节点并关闭通道；

如果r2>r1，且P_i的余额D_i发生了变化，向P_i发出信息告知其赎回申请无效，并附上状态更新消息StateMsg2，开启用户申诉时间窗口，等待P_i发起申诉，如果申述时间窗口关闭前，P_i申述失败，即认为节点P_i作恶，将P_i的余额分配给通道内的其他人；

向节点P_i的链上地址中转入D_i并更新通道状态；

所述等待P_i发起申诉指：

如果是由于通道监管人的恶意提交，P_i可以使用StateMsg2和另一合法状态更新信息向作恶检测合约提交作恶证据，合约验证通道监管人作恶后罚没其保证金并关闭通道，从而达到申诉成功的目的。

7.一种存储有计算机程序的计算机可读存储介质，其特征在于，所述计算机程序被处理器执行时实现权利要求1至6中任一项所述的用于区块链扩展的多向状态通道支付方法的步骤。

用于区块链扩展的多向状态通道方法、系统及介质

技术领域

[0001] 本发明涉及线下区块链技术领域，具体地，涉及用于区块链扩展的多向状态通道方法、系统及介质。

背景技术

[0002] 区块链是一种利用分布式账本技术解决多方信任问题的创新性解决方案。通过区块 链技术，可以在不依赖于任何第三方可信机构的前提下，建立可信分布式系统。去中心化的特性使得区块链技术拥有广泛的应用前景。当前的区块链系统性能存在严重不足，以比特币为例，由于比特币采用基于PoW(Proof of Work)的共识机制，全网完成一轮 共识的期望时间为10分钟，因此，比特币系统的交易吞吐量最高只能达到7笔/秒(假定 区块大小为1MB)。而主流的商业数字支付系统如visa，每秒的交易处理数量能达到上 千笔。当前区块链系统的性能与传统基于第三方的分布式系统存在较大的差距，无法满 足现实业务的需求。这使得区块链的发展受到了大大的限制。

[0003] 区块链扩容是提升区块链有限处理能力的一个重要途径。目前有两种类型的扩容方 案，一种是链上扩容方式，也称为Layer1扩容，即通过直接修改区块链的基础规则来 改进区块链自身，包括区块大小、共识机制等。具体的扩容方案有SegWit(隔离见证)、扩大区块容量、Sharding(分片)、DAG(有向无环图)等。经过业界实践，目前大家通 常认为链上扩容方式在性能上会存在难以逾越的天花板。另一种是链下扩容方式，也称 为Layer2扩容，目的是把计算转移到链下进行，这种扩容方式不直接改动区块链本身 的规则(区块大小、共识机制等)，而是在其之上再架设一层来处理具体的事务，只在需 要共识参与时(如数据存证、纠纷仲裁等)才与区块链进行信息交互与传播。具体的扩 容方案有状态通道、侧链等。在链下扩容方案中，大量的事务通常只在参与节点间进行， 不会进行全网传播，效率直接取决于节点间的网络性能，显然效率更高。而且因为没有 全网广播，信息不能公开可查，通常隐私性也更高。因此，链下交易性能可以不受原有 区块链性能的影响，具有更大的潜力，存在无限扩展的可能性。

[0004] 闪电网络是链下扩容方案的代表，闪电网络实现了通道内的双向支付功能和跨通道 支付功能。使得用户能够在链下进行交易，只在通道关闭时才需要在链上进行交易，从而使区块链支持高频小额交易成为可能。闪电网络的本质是使用哈希时间锁定智能合约来安全地进行0确认交易(没有被区块链网络节点确认的交易)。通过巧妙设置智能合 约，完善链下通道，使得用户可以在闪电网络上进行0确认的交易。其中主要包含了两 种类型的合约，RSMC(Recoverable Sequence Maturity Contract)和HTLC(Hashed Timelock Contract)。RSMC保障了两个用户之间的直接交易可以在链下完成，HTLC保 障了任意两个用户之间的转账都可以通过一条支付通道来完成。这两种类型的交易组合 构成了闪电网络，从而实现了加入到闪电网络中的任意两个用户都可以在链下完成交易。 但是，闪电网络存在一定的缺陷。由于比特币原有的脚本系统无法存储交易的中间状态，为了防止双向通道中某一方的恶意行为，通道双方都需要在本地存储每一轮通道状态更 新时产生的惩

罚交易。惩罚交易所需要的存储代价随着通道内支付次数的增加而不断累 加,将会给用户带来极大的存储开销。雷电网络是由以太坊社区提出的针对以太坊平台 的链下微支付通道解决方案,其原理与闪电网络的原理基本相同,但由于其构建在以太 坊平台上,利用以太坊平台灵活而强大的智能合约以及能够存储合约执行状态的特性, 解决了闪电网络中存储开销不断累积的缺陷。但是,由于在闪电网络和雷电网络中每一 个状态通道都仅仅与两个用户相关,致使它们的网络拓扑复杂,导致跨通道支付的路由 寻路困难、算法复杂低效。针对具体的应用场景,如多个用户之间存在高频的双向支付, 而闪电网络和雷电网络的每一个状态通道都只适用于两个用户之间的价值转移,致使多 数的交易都需要进行跨通道支付或者任意两个用户之间都建立双向支付通道,这将导致 其交易性能过低。

发明内容

[0005] 针对现有技术中的缺陷,本发明的目的是提供一种用于区块链扩展的多向状态通道方法、系统及介质。

[0006] 根据本发明提供的一种用于区块链扩展的多向状态通道方法,包括:

[0007] 通道建立步骤:通过通道监管人S和多个普通用户合作建立一个多向支付的链下通 道;

[0008] 通道支付步骤:在建立的多向支付的链下通道内,普通用户之间进行交易,监管人S根据普通用户之间的交易信息,向多个普通用户发送通道状态更新信息;

[0009] 通道关闭步骤:任意用户赎回押金,则关闭该用户的支付通道,同时作恶检测合约检测通道监管人S是否存在作恶行为:若是,则关闭所有通道;否则,则继续检测通道 监管人S是否作恶。

[0010] 优选地,所述通道建立步骤:

[0011] n个普通用户节点和一个通道监管人S合作建立一个多向支付的链下通道,任意普通用户可以通过在智能合约中冻结足够的保证金成为通道监管人;

[0012] 在通道建立阶段时,通道内的所有普通用户均需要认可监管人S的身份并获知S的公钥,S获知通道内普通用户节点的公钥;

[0013] 所有普通用户节点需要向通道中存入自己的押金D_i(1≤i≤n),而通道监管人S需要在通道中存入自己的保证金G并将其冻结至通道关闭,保证金G用来防止通道监管人 的作恶行为,一旦普通用户节点中的任意节点将通道监管人作恶的证据提交到链上的作 恶检测合约V_f,并且验证通过,保证金将作为罚金平均转入到通道内的所有普通节点账 户中;

[0014] 为了保证通道内普通用户节点不会受到损失,通道监管人的保证金金额需要满足以 下等式:

[0015] $G=n\times\sum_{i=1}^{n}D_i$

[0016] 当监管人作恶时,每个普通用户节点将会收到数目为$\sum_{i=1}^{n}D_i$的金额作为赔偿金。

[0017] 优选地,所述通道支付步骤:

[0018] 当通道内的多个普通用户想产生一笔转账交易时,首先多个普通用户之间沟通转账 交易的金额,由收款方生成转账交易信息 TxMsg=(sender,receiver,amount,r,TxID) sig_{sender},$sig_{receiver}$,其中r表示当前交易所在 轮数,是根据交易双方已经获知的最新状态

更新信息的轮数加一计算得出；

[0019] 收款方在签名后，将该转账交易信息发送至付款方，付款方核实转账金额是否符合 预期，收款人和付款人是否为目标用户，核实正确后签名该信息，并将其发送给通道监管人S；通道监管人S收集每一轮中收到的转账交易信息，验证转账交易信息的合法性， 发出当前轮的状态更新信息StateMsg；

[0020] 当进行交易的多个普通用户收到由通道监管人S广播的新一轮状态更新信息StateMsg时，验证状态更新信息StateMsg的合法性：核实收到的r至r+Δ轮状态更新 信息是否包含当前用户已发出的第r轮转账交易信息，如果存在，则表明当前转账交易 完成；如果不存在则表明转账交易信息已经失效，需要重新生成一笔新的转账交易信息 发送至通道监管人S，或者取消此次交易；

[0021] 其中，Δ为系统选定参数，用于指定转账交易消息被状态更新信息延迟包含的最大 轮数。

[0022] 优选地，所述通道支付步骤：

[0023] 所述转账交易信息TxMsg是由发生交易的收款方进行生成，发送给付款方，付款方确认无误并签名后发送给通道监管人S，该消息用于让通道监管人获知交易双方想要达 成的交易内容及交易意愿，由于附有交易双方的签名，因此可以作为通道余额状态更新 时的凭据；

[0024] $TxMsg=(sender,receiver,amount,r,TxID)sig_{sender},sig_{receiver}$

[0025] 其中，sender表示交易发送者，receiver表示交易接收者，amount表示转账金额，r表示当前交易所在的轮数，是指整个多人通道的状态更新轮数，TxID，一个8bit的 数，用于唯一标记sender和receiver在其认为的第r轮中的某一次交易，TxID的引入 是为了方便用户可以在一轮中进行多次交易，sig_{sender}表示该消息需要转账发送者的签名， $sig_{recevier}$表示该消息需要转账接受者的签名；

[0026] 所述通道状态更新信息StateMsg是由通道监管人签名发布，用于表示在该轮中通道内部的各用户账户余额信息，该通道状态更新信息包含本轮由通道监管人S认可的转 账交易信息列表；

[0027] 每个用户可以根据附在通道状态更新信息内的转账交易信息列表，核实转账交易信 息的签名是否正确，本轮的各账户余额是否与预期相符，根据转账交易信息所表示的转账，以及上一轮的各账户余额，可以推算出当前轮的各账户余额；

[0028] 一旦用户发现通道状态更新信息与预期不符，即可向链上的作恶检测合约提起申诉 并提交监管人作恶证据，保证自身资金的安全性；

[0029] $StateMsg=(Amountarray[n],TxMsgList,r)sig_S$

[0030] 其中，Amountarray[n]表示当前轮通道内n个人的账户余额，TxMsgList表示在该轮由通道监管人认可的转账交易消息TxMsg列表，r表示当前通道状态更新的轮数，sig_S表示通道监管人S的签名。

[0031] 优选地，所述通道支付步骤：

[0032] 所述验证转账交易信息的合法性指：

[0033] 核实转账交易信息是否有付款方和收款方的签名认可；

[0034] 检验转账交易信息中的轮数是否合法，即核实转账交易信息中的轮数是否在r-Δ

到r之间,r表示当前通道状态更新的轮数,Δ为系统选定参数,如果轮数不在此范围 内,认为该转账交易信息已失效,拒绝该转账交易信息;

[0035] 检查TxID值是否合法,即校验TxID值是否在相应的交易用户第r轮转账交易信息中存在,如果已经存在,则拒绝该转账交易信息;

[0036] 根据上一轮状态更新信息中的各账户余额,以及当前轮已经认可的转账交易信息, 计算出当前各用户的余额情况,检验交易的付款方余额是否大于等于转账金额,如果余 额不足以支持该笔转账,则拒绝该转账交易信息。

[0037] 优选地,所述通道关闭步骤:

[0038] 所述作恶检测合约检测通道监管人S是否存在作恶行为:

[0039] 所述作恶行为包括:

[0040] 发布失效信息行为:发布包含失效转账交易信息的通道状态更新信息,导致用户的 余额与实际余额不符;

[0041] 发送错误信息行为:发布用户余额计算错误的通道状态更新信息;

[0042] 对于发布失效信息行为,用户在通道建立后至通道关闭前,可以向作恶检测合约提 交一轮错误的通道状态更新信息StateMsg=(Amountarray[n],TxMsgList,r)sig_S,作恶 检测合约进行如下验证:

[0043] 验证状态更新信息通道监管人签名是否合法;

[0044] 验证转账交易信息列表TxMsgList中所有转账交易信息的所在轮数r′是否在r-Δ到r之间,如果不在,则表明通道监管人作恶,将通道内的保证金分配给通道内的所有 节点并关闭通道;

[0045] 对于发送错误信息行为,用户在通道建立后至通道关闭前,向作恶检测合约提交连 续两轮通道状态更新信息$StateMsg_{r1}$=(Amountarray[n]r1,TxMsgList,r1)sig_S与$StateMsg_{r1+1}$=(Amountarray[n]r1+1,TxmsgList,r1+1)sig_S作为证据,作恶检测合约进行如下验证:

[0046] 验证两轮的状态更新信息通道监管人签名是否合法;

[0047] 基于r1轮的用户余额列表Amountarray[n]r1,结合第r1+1轮的转账交易信息列表TxMsgList,计算得出第r1+1轮的用户余额列表A_1,与$Amountarray[n]_{r1+1}$进行比较, 如果二者不相等,则表明通道监管人作恶,将通道内的保证金分配给通道内的所有节点 并关闭通道。

[0048] 优选地,所述通道关闭步骤:

[0049] 用户赎回步骤:

[0050] 若普通用户节点P_i想要赎回自己在支付通道内的押金,则需要在区块链中公布自己 认为的最新状态更新信息StateMsg=(Amountarray[n],TxMsgList,r)sig_S,即通知所有 人核实赎回人节点P_i的状态:若核实无误,则普通用户节点P_i成功赎回押金,关闭普通用户节点P_i的支付通道;若有误,则系统判定为用户作恶而被罚没所有押金,关闭普通 用户节点P_i的支付通道;

[0051] 在普通用户节点P_i赎回押金时,判断节点P_i是否存在待监管人处理的转账交易信息:如果存在待处理的转账交易信息,则需要等待至交易被处理或者该转账交易信息被 判断为失效后,才能发起押金赎回申请,否则会由于在发起押金赎回操作后,状态更新 信息

中的个人用户余额仍在发生变化，被系统判定为用户作恶而被罚没所有押金；

[0052] 作恶检测步骤：

[0053] 通过将赎回押金的操作在区块链上打开一个时间窗口，防止P_i公布之前已作废的通 道状态和监督监管人的作恶行为，在打开的时间窗口这段时间内P_i的押金将被冻结在通 道中，并且所有通道内的节点可以向作恶检测合约提交节点认为的正确状态，一旦发现通道监管人作恶或P_i试图赎回不是自己实际余额的金额，作恶检测合约可以通过作恶证据自动惩罚作恶方。

[0054] 优选地，所述作恶检测步骤：

[0055] 节点P_i将其认可的最新通道状态信息 StateMsg1＝(Amountarray[n],TxMsgList,r1)sig_S和作恶证据 StateMsg2＝(Amountarray[n],TxMsgList,r2)sig_S的状态更新信息提交给作恶检测合约 V_f的处理，作恶检测合约V_f的处理流程如下：

[0056] 验证状态更新消息StateMsg1中通道监管人S的签名；

[0057] 验证状态更新消息StateMsg1的正确性，确保转账交易信息列表的所有交易轮数均 在有效轮数范围内；

[0058] 打开仲裁时间窗口，在这段时间内通道内的节点可以提交作恶证据；

[0059] 验证状态更新消息StateMsg2中S的签名；

[0060] 验证状态更新消息StateMsg2的正确性，确保转账交易信息列表的所有交易轮数均 在有效轮数范围内；

[0061] 如果r1＝r2，且StateMsg2≠StateMsg1，则认为监管人作恶，将通道内的保证金分配给通道内的所有节点并关闭通道；

[0062] 如果r2>r1，且P_i的余额D_i发生了变化，向P_i发出信息告知其赎回申请无效，并附上状态更新消息StateMsg2，开启用户申诉时间窗口，等待P_i发起申诉，如果申述时间 窗口关闭前，P_i申述失败，即认为节点P_i作恶，将P_i的余额分配给通道内的其他人；

[0063] 向节点P_i的链上地址中转入D_i并更新通道状态；

[0064] 所述等待P_i发起申诉指：

[0065] 如果是由于通道监管人的恶意提交，P_i可以使用StateMsg2和另一合法状态更新信 息向作恶检测合约提交作恶证据，合约验证通道监管人作恶后罚没其保证金并关闭通道，从而达到申诉成功的目的。

[0066] 根据本发明提供的一种存储有计算机程序的计算机可读存储介质，其特征在于，所 述计算机程序被处理器执行时实现上述中任一项所述的用于区块链扩展的多向状态通道方法的步骤。

[0067] 与现有技术相比，本发明具有如下的有益效果：

[0068] 本发明提出了一种高效的支持并行的多向状态通道方案，有效解决了多个用户之间 存在高频的双向支付的应用场景。在跨通道支付的路由方面，相比于基于双向支付通道构建的闪电网络和雷电网络，具有更好的性能。

附图说明

[0069] 通过阅读参照以下附图对非限制性实施例所作的详细描述，本发明的其它特征、目 的和优点将会变得更明显：

[0070] 图1为本发明提供的通道建立阶段流程示意图。

[0071] 图2为本发明提供的通道支付阶段流程示意图。

[0072] 图3为本发明提供的通道状态更新信息发布示意图。

[0073] 图4为本发明提供的通道监管人的工作流程示意图。

具体实施方式

[0074] 下面结合具体实施例对本发明进行详细说明。以下实施例将有助于本领域的技术人 员进一步理解本发明，但不以任何形式限制本发明。应当指出的是，对本领域的普通技术人员来说，在不脱离本发明构思的前提下，还可以做出若干变化和改进。这些都属于 本发明的保护范围。

[0075] 根据本发明提供的一种用于区块链扩展的多向状态通道方法，包括：

[0076] 通道建立步骤：通过通道监管人S和多个普通用户合作建立一个多向支付的链下通 道；

[0077] 通道支付步骤：在建立的多向支付的链下通道内，普通用户之间进行交易，监管人S根据普通用户之间的交易信息，向多个普通用户发送通道状态更新信息；

[0078] 通道关闭步骤：任意用户赎回押金，则关闭该用户的支付通道，同时作恶检测合约检测通道监管人S是否存在作恶行为：若是，则关闭所有通道；否则，则继续检测通道 监管人S是否作恶。

[0079] 优选地，所述通道建立步骤：

[0080] n个普通用户节点和一个通道监管人S合作建立一个多向支付的链下通道，任意普通用户可以通过在智能合约中冻结足够的保证金成为通道监管人；

[0081] 在通道建立阶段时，通道内的所有普通用户均需要认可监管人S的身份并获知S的公钥，S获知通道内普通用户节点的公钥；

[0082] 所有普通用户节点需要向通道中存入自己的押金D_i(1≤i≤n)，而通道监管人S需要在通道中存入自己的保证金G并将其冻结至通道关闭，保证金G用来防止通道监管人 的作恶行为，一旦普通用户节点中的任意节点将通道监管人作恶的证据提交到链上的作 恶检测合约V_f，并且验证通过，保证金将作为罚金平均转入到通道内的所有普通节点账 户中；

[0083] 为了保证通道内普通用户节点不会受到损失，通道监管人的保证金金额需要满足以 下等式：

[0084] $G=n\times\sum_{i=1}^{n}D_i$

[0085] 当监管人作恶时，每个普通用户节点将会收到数目为$\sum_{i=1}^{n}D_i$的金额作为赔偿金。

[0086] 优选地，所述通道支付步骤：

[0087] 当通道内的多个普通用户想产生一笔转账交易时，首先多个普通用户之间沟通转账 交易的金额，由收款方生成转账交易信息 TxMsg＝(sender,receiver,amount,r,TxID) sig_{sender},$sig_{receiver}$，其中r表示当前交易所在 轮数，是根据交易双方已经获知的最新状态更新信息的轮数加一计算得出；

[0088] 收款方在签名后，将该转账交易信息发送至付款方，付款方核实转账金额是否符合 预期，收款人和付款人是否为目标用户，核实正确后签名该信息，并将其发送给通道监

管人S;通道监管人S收集每一轮中收到的转账交易信息,验证转账交易信息的合法性，发出当前轮的状态更新信息StateMsg;

[0089] 当进行交易的多个普通用户收到由通道监管人S广播的新一轮状态更新信息StateMsg时,验证状态更新信息StateMsg的合法性:核实收到的r至r+Δ轮状态更新 信息是否包含当前用户已发出的第r轮转账交易信息,如果存在,则表明当前转账交易 完成;如果不存在则表明转账交易信息已经失效,需要重新生成一笔新的转账交易信息 发送至通道监管人S,或者取消此次交易;

[0090] 其中,Δ为系统选定参数,用于指定转账交易消息被状态更新信息延迟包含的最大 轮数。

[0091] 优选地,所述通道支付步骤:

[0092] 所述转账交易信息TxMsg是由发生交易的收款方进行生成,发送给付款方,付款方确认无误并签名后发送给通道监管人S,该消息用于让通道监管人获知交易双方想要达 成的交易内容及交易意愿,由于附有交易双方的签名,因此可以作为通道余额状态更新 时的凭据;

[0093] $TxMsg=(sender,receiver,amount,r,TxID)\,sig_{sender},sig_{receiver}$

[0094] 其中,sender表示交易发送者,receiver表示交易接收者,amount表示转账金额,r表示当前交易所在的轮数,是指整个多人通道的状态更新轮数,TxID,一个8bit的 数,用于唯一标记sender和receiver在其认为的第r轮中的某一次交易,TxID的引入 是为了方便用户可以在一轮中进行多次交易,sig_{sender}表示该消息需要转账发送者的签名，$sig_{recevier}$表示该消息需要转账接受者的签名;

[0095] 所述通道状态更新信息StateMsg是由通道监管人签名发布,用于表示在该轮中通道内部的各用户账户余额信息,该通道状态更新信息包含本轮由通道监管人S认可的转 账交易信息列表;

[0096] 每个用户可以根据附在通道状态更新信息内的转账交易信息列表,核实转账交易信 息的签名是否正确,本轮的各账户余额是否与预期相符,根据转账交易信息所表示的转账,以及上一轮的各账户余额,可以推算出当前轮的各账户余额;

[0097] 一旦用户发现通道状态更新信息与预期不符,即可向链上的作恶检测合约提起申诉 并提交监管人作恶证据,保证自身资金的安全性;

[0098] $StateMsg=(Amountarray[n],TxMsgList,r)\,sig_S$

[0099] 其中,Amountarray[n]表示当前轮通道内n个人的账户余额,TxMsgList表示在该轮由通道监管人认可的转账交易消息TxMsg列表,r表示当前通道状态更新的轮数,sig_S表示通道监管人S的签名。

[0100] 优选地,所述通道支付步骤:

[0101] 所述验证转账交易信息的合法性指:

[0102] 核实转账交易信息是否有付款方和收款方的签名认可;

[0103] 检验转账交易信息中的轮数是否合法,即核实转账交易信息中的轮数是否在r-Δ到r之间,r表示当前通道状态更新的轮数,Δ为系统选定参数,如果轮数不在此范围 内,认为该转账交易信息已失效,拒绝该转账交易信息;

[0104] 检查TxID值是否合法,即校验TxID值是否在相应的交易用户第r轮转账交易信息

中存在,如果已经存在,则拒绝该转账交易信息;

[0105] 根据上一轮状态更新信息中的各账户余额,以及当前轮已经认可的转账交易信息,计算出当前各用户的余额情况,检验交易的付款方余额是否大于等于转账金额,如果余 额不足以支持该笔转账,则拒绝该转账交易信息。

[0106] 优选地,所述通道关闭步骤:

[0107] 所述作恶检测合约检测通道监管人S是否存在作恶行为:

[0108] 所述作恶行为包括:

[0109] 发布失效信息行为:发布包含失效转账交易信息的通道状态更新信息,导致用户的 余额与实际余额不符;

[0110] 发送错误信息行为:发布用户余额计算错误的通道状态更新信息;

[0111] 对于发布失效信息行为,用户在通道建立后至通道关闭前,可以向作恶检测合约提 交一轮错误的通道状态更新信息StateMsg=(Amountarray[n],TxMsgList,r)sig_S,作恶 检测合约进行如下验证:

[0112] 验证状态更新信息通道监管人签名是否合法;

[0113] 验证转账交易信息列表TxMsgList中所有转账交易信息的所在轮数r′是否在r-Δ到r之间,如果不在,则表明通道监管人作恶,将通道内的保证金分配给通道内的所有 节点并关闭通道;

[0114] 对于发送错误信息行为,用户在通道建立后至通道关闭前,向作恶检测合约提交连 续两轮通道状态更新信息$StateMsg_{r1}$=(Amountarray[n]r1,TxMsgList,r1)sig_S与$StateMsg_{r1+1}$=(Amountarray[n]r1+1,TxmsgList,r1+1)sig_S作为证据,作恶检测合约进行如下验证:

[0115] 验证两轮的状态更新信息通道监管人签名是否合法;

[0116] 基于r1轮的用户余额列表Amountarray[n]r1,结合第r1+1轮的转账交易信息列表TxMsgList,计算得出第r1+1轮的用户余额列表A_1,与$Amountarray[n]_{r1+1}$进行比较, 如果二者不相等,则表明通道监管人作恶,将通道内的保证金分配给通道内的所有节点 并关闭通道。

[0117] 优选地,所述通道关闭步骤:

[0118] 用户赎回步骤:

[0119] 若普通用户节点P_i想要赎回自己在支付通道内的押金,则需要在区块链中公布自己 认为的最新状态更新信息StateMsg=(Amountarray[n],TxMsgList,r)sig_S,即通知所有 人核实赎回人节点P_i的状态:若核实无误,则普通用户节点P_i成功赎回押金,关闭普通用户节点P_i的支付通道;若有误,则系统判定为用户作恶而被罚没所有押金,关闭普通 用户节点P_i的支付通道;

[0120] 在普通用户节点P_i赎回押金时,判断节点P_i是否存在待监管人处理的转账交易信息:如果存在待处理的转账交易信息,则需要等待至交易被处理或者该转账交易信息被 判断为失效后,才能发起押金赎回申请,否则会由于在发起押金赎回操作后,状态更新 信息中的个人用户余额仍在发生变化,被系统判定为用户作恶而被罚没所有押金;

[0121] 作恶检测步骤:

[0122] 通过将赎回押金的操作在区块链上打开一个时间窗口,防止P_i公布之前已作废的

通 道状态和监督监管人的作恶行为,在打开的时间窗口这段时间内P_i的押金将被冻结在通 道中,并且所有通道内的节点可以向作恶检测合约提交节点认为的正确状态,一旦发现通道监管人作恶或P_i试图赎回不是自己实际余额的金额,作恶检测合约可以通过作恶证据自动惩罚作恶方。

[0123] 优选地,所述作恶检测步骤:

[0124] 节点P_i将其认可的最新通道状态信息 StateMsg1＝(Amountarray[n],TxMsgList,r1)sig_S和作恶证据 StateMsg2＝(Amountarray[n],TxMsgList,r2)sig_S的状态更新信息提交给作恶检测合约 V_f的处理,作恶检测合约V_f的处理流程如下:

[0125] 验证状态更新消息StateMsg1中通道监管人S的签名;

[0126] 验证状态更新消息StateMsg1的正确性,确保转账交易信息列表的所有交易轮数均 在有效轮数范围内;

[0127] 打开仲裁时间窗口,在这段时间内通道内的节点可以提交作恶证据;

[0128] 验证状态更新消息StateMsg2中S的签名;

[0129] 验证状态更新消息StateMsg2的正确性,确保转账交易信息列表的所有交易轮数均 在有效轮数范围内;

[0130] 如果r1＝r2,且StateMsg2≠StateMsg1,则认为监管人作恶,将通道内的保证金分配给通道内的所有节点并关闭通道;

[0131] 如果r2>r1,且P_i的余额D_i发生了变化,向P_i发出信息告知其赎回申请无效,并附上状态更新消息StateMsg2,开启用户申诉时间窗口,等待P_i发起申诉,如果申述时间 窗口关闭前,P_i申述失败,即认为节点P_i作恶,将P_i的余额分配给通道内的其他人;

[0132] 向节点P_i的链上地址中转入D_i并更新通道状态;

[0133] 所述等待P_i发起申诉指:

[0134] 如果是由于通道监管人的恶意提交,P_i可以使用StateMsg2和另一合法状态更新信 息向作恶检测合约提交作恶证据,合约验证通道监管人作恶后罚没其保证金并关闭通道, 从而达到申诉成功的目的。

[0135] 根据本发明提供的一种存储有计算机程序的计算机可读存储介质,其特征在于,所 述计算机程序被处理器执行时实现上述中任一项所述的用于区块链扩展的多向状态通道方法的步骤。

[0136] 下面通过优选例,对本发明进行更为具体地说明。

[0137] 优选例1:

[0138] 支持并行的多向支付通道方案,是一种新型状态通道方案,它允许多个节点构成一 个状态通道,并且支持多个节点同时在状态通道内进行链下支付。为了解决多向通道内的状态更新问题,方案引入了第三方监管人角色S,对通道内的所有交易进行确认和排 序,在每一轮中发布状态余额更新信息。通过通道监管人进行通道内的状态更新,既可 以降低链下支付过程中的交互开销,又保证了通道内未进行交易的节点不在线时支付通 道的可用性。另外,为了防止监管人作恶,设计了作恶检测合约V_f,用来自动检测通道 内可能存在的攻击行为,对监管人或普通用户的恶意行为进行惩罚。通过引入通道轮数 延迟参数Δ,使得通道监管人可以对通道内并行发生的多笔交易进行确认,从而达到交 易并行的效果。通道监管人的存在使得通道状态的更新不需要通道内所有节点的参与, 这解决了用户离

线时通道不可用的问题。同时，在每轮通道状态更新的过程中，仅需要 当前进行链下交易的双方和通道监管人交互协作即可，这使得更新过程中的通信复杂度 与参与人数无关。另外，我们的方案需要图灵完备的智能合约平台支持。

[0139] 图灵完备的智能合约平台：

[0140] 我们的方案需要图灵完备的智能合约平台来执行合约并存储合约执行的状态和结 果，比如以太坊提供的智能合约。我们假定一旦智能合约被部署在区块链中，在合约执行过程中任何用户都无法改变或影响合约的执行状态和结果。

[0141] 多向支付通道协议：

[0142] 在多向支付通道网络中，链下支付的流程大致可以分为三个阶段：多向支付通道的 建立，链下支付，通道的关闭。

[0143] (1)通道建立阶段

[0144] 如图1所示，在该阶段中，n个普通用户节点和一个通道监管人S合作建立一个多向支付的链下通道。任意普通用户可以通过在智能合约中冻结足够的保证金成为通道监管人。在通道建立阶段初期，通道内的所有普通用户均需要认可监管人S的身份并获知 S的公钥，S获知通道内普通用户节点的公钥。所有普通用户节点需要向通道中存入自 己的押金D_i($1\leqslant i\leqslant n$)，而通道监管人S需要在通道中存入自己的保证金G并将其冻结 至通道关闭。这笔保证金用来防止通道监管人的作恶行为，一旦任意节点将通道监管人 作恶的证据提交到链上的作恶检测合约V_f，并且验证通过，保证金将作为罚金平均转入 到通道内的所有普通节点账户中。

[0145] 为了保证通道内普通用户节点不会受到损失，通道监管人的保证金金额需要满足以 下等式：

[0146] $G=n\times\sum_{i=1}^{n}D_i$

[0147] 当监管人作恶时，每个节点将会收到数目为$\sum_{i=1}^{n}D_i$的金额作为他们的赔偿金。这个 金额是一个用户在通道内可能拥有的余额最大值。一旦监管人的作恶行为被发现，所有通道内的用户都可以获得该数额的赔偿金，这就从根本上保证了用户资产的安全性，因 为无论何种情况下赔偿金都足以抵消掉用户的资金损失，使得用户可以放心使用该多向 支付通道，而不用担心由于通道监管人的作恶行为造成个人资产损失。

[0148] (2)通道支付阶段

[0149] 在链下支付的过程中，为了保证系统的正常运行，需要定义两种不同的消息类型，如图2所示。一种消息类型，我们将其称之为转账交易信息TxMsg，是由发生交易的收 款方进行生成，发送给付款方，付款方确认无误并签名后发送给通道监管人S。该消息 用于让通道监管人获知交易双方想要达成的交易内容及交易意愿，由于附有交易双方的 签名，因此可以作为通道余额状态更新时的凭据。

[0150] $TxMsg=(sender,receiver,amount,r,TxID)\,sig_{sender},sig_{receiver}$

[0151] 其中，sender表示交易发送者，receiver表示交易接收者，amount表示转账金额，r表示当前交易所在的轮数，是指整个多人通道的状态更新轮数，TxID，一个8bit的 数，用于唯一标记sender和receiver在其认为的第r轮中的某一次交易，TxID的引入 是为了方便用户可以在一轮中进行多次交易，sig_{sender}表示该消息需要转账发送者的签名，$sig_{recevier}$表

示该消息需要转账接受者的签名。

[0152] 如图3所示，另外一种消息，我们将其称之为通道状态更新信息StateMsg，是由通道监管人签名发布，用于表示在该轮中通道内部的各用户账户余额信息，该通道状态更 新消息会包含本轮由通道监管人S认可的转账交易信息列表。每个用户可以根据附在通 道状态更新信息内的转账交易信息列表，核实转账交易信息的签名是否正确，本轮的各 账户余额是否与预期相符，根据转账交易信息所表示的转账，以及上一轮的各账户余额， 可以推算出当前轮的各账户余额。一旦用户发现通道状态更新信息与预期不符，即可向 链上的作恶检测合约提起申诉并提交监管人作恶证据，从而保证自身资金的安全性。

[0153] 消息格式为

[0154] $StateMsg=(Amountarray[n],TxMsgList,r)sig_S$

[0155] 其中，Amountarray[n]表示当前轮通道内n个人的账户余额，TxMsgList表示在该轮由通道监管人认可的转账交易消息TxMsg列表，r表示当前通道状态更新的轮数。sigS 表示通道监管人S的签名。

[0156] 通道监管人的工作流程：

[0157] 如图4所示，在通道监管人S发布了第r-1轮的通道状态更新信息以后，通道监管人等待新转账交易信息的到达。当通道监管人S收到一条新的合法的转账交易信息时， 开始筹备新一轮的状态更新信息，此时，开启一个状态更新定时器。在状态更新定时器 开启期间，通道监管人接收通道内发送至自己的转账交易信息，验证其合法性，验证合 法后将其放入新一轮的状态更新信息中。当状态更新定时器终止时，根据认可的新的转 账交易信息，计算出通道各用户的最新余额，生成新一轮的状态更新信息，签名后，广 播给通道的所有用户。

[0158] 通道监管人对一笔新转账交易信息的验证流程如下：

[0159] 当通道监管人在筹备新一轮(第r轮)状态更新信息的过程中，接收到一笔通道内产生的转账交易信息，将根据以下步骤验证其合法性：

[0160] 1)核实转账交易信息是否有付款方和收款方的签名认可；

[0161] 2)检验转账交易信息中的轮数是否合法，具体为，核实转账交易信息中的轮数是否 在r-Δ到r之间，Δ为系统选定参数，如果轮数不在此范围内，认为该转账交易信息 已失效，拒绝该转账交易信息；

[0162] 3)检查TxID值是否合法，即校验TxID值是否在相应的交易用户第r轮转账交易 信息中存在，如果已经存在，则拒绝该转账交易信息；

[0163] 4)根据上一轮状态更新信息中的各账户余额，以及当前轮已经认可的转账交易信息，计算出当前各用户的余额情况，检验交易的付款方余额是否大于等于转账金额，如 果余额不足以支持该笔转账，则拒绝该转账交易信息。

[0164] 通道用户的交易流程：

[0165] 当通道内的两个用户想产生一笔转账交易时，双方首先沟通转账交易的金额，由收 款方生成转账交易信息$TxMsg=(sender,receiver,amount,r,TxID)___,sig_{receiver}$，其中r 表示当前交易所在轮数，是根据交易双方已经获知的最新状态更新信息的轮数加一计算 得出。收款方在签名后，将该转账交易信息发送至付款方，付款方核实转账金额是否符合预期，收款人和付款人是否为目标用户，核实正确后签名该信息，并将其发送给通道 监

管人S。

[0166] 当进行交易的两个用户收到由通道监管人S广播的新一轮状态更新信息时，核实其 正确性，若在其中发现该笔转账交易，即可视为该笔转账交易完成。另一方面，如果付款人发送至通道监管人S的转账交易信息，没有被包含在第r轮至第r+Δ轮的状态更 新消息内，表明发送至监管人S处的转账交易信息已经失效，需要重新生成一笔新的转 账交易信息发送至通道监管人S，或者取消此次交易。

[0167] 在此我们只描述了一笔转账交易中包含一个付款方和一个收款方的情况，但是我们 的方案并不局限于此，一笔转账交易可以包含多个付款方和多个收款方。只要该笔转账交易信息拥有参与方的签名，表明参与方认可了该笔交易，就可以作为一个合法的转账 交易信息发送给通道监管人S等待处理。

[0168] 通道监管人作恶行为检测：

[0169] 通道监管人存在两种明显的作恶行为，一种为发布包含失效转账交易信息的通道状 态更新信息，导致用户的余额与实际余额不符。另一种为发布用户余额计算错误的通道状态更新信息。即上一轮通道状态更新信息是正确的，下一轮的通道状态更新信息内包 含的转账交易信息均合法有效，但在计算通道内各用户余额时，通道监管人故意计算错 误，导致用户的金额与实际发生转账交易后的余额不符。

[0170] 为了有效避免通道监管人进行这两种作恶行为，用户在任何时刻都可以向作恶检测 合约V_f提交作恶证据，作恶检测合约核实通道监管人作恶后，将通道内的保证金分配给通道内的所有节点并关闭通道。

[0171] 对于第一种作恶行为，用户在通道建立后至通道关闭前，可以向作恶检测合约提交 一轮错误的通道状态更新信息StateMsg＝(Amountarray[n],TxMsgList,r)sig_S，作恶检 测合约进行如下验证:

[0172] 1)验证状态更新信息通道监管人签名是否合法；

[0173] 2)验证转账交易信息列表TxMsgList中所有转账交易信息的所在轮数r′是否在r-Δ到r之间，如果不在，则表明通道监管人作恶，将通道内的保证金分配给通道内 的所有节点并关闭通道。

[0174] 对于第二种作恶行为，用户在通道建立后至通道关闭前，向作恶检测合约提交连续 两轮通道状态更新信息$StateMsg_{r1}$＝(Amountarray[n]r1,TxMsgList,r1)sig_S与$StateMsg_{r1+1}$＝(Amountarray[n]r1+1,TxmsgList,r1+1)sig_S作为证据，作恶检测合约进行如下验证：

[0175] 1)验证两轮的状态更新信息通道监管人签名是否合法；

[0176] 2)基于r_1轮的用户余额列表$Amountarray[n]_r1$，结合第r1+1轮的转账交易信息列表TxMsgList，计算得出第r1+1轮的用户余额列表A_1，与$Amountarray[n]_{r1+1}$进行比较， 如果二者不相等，则表明通道监管人作恶，将通道内的保证金分配给通道内的所有节点 并关闭通道。

[0177] (3)通道关闭阶段

[0178] 若节点P_i想要赎回自己在支付通道内的押金，他需要在区块链中公布自己认为的最 新状态更新信息StateMsg＝(Amountarray[n],TxMsgList,r)sig_S。

[0179] 由于在我们的方案中，引入了通道轮数延迟参数Δ用于处理通道内并行的转账交

易。在赎回押金时，节点P_i需要保证自己没有待监管人处理的转账交易信息。如果存在 待处理的转账交易信息，需要等待至交易被处理或者该转账交易信息被判断为失效后，才能发起押金赎回申请，否则会由于在他发起押金赎回操作后，状态更新信息中的个人 用户余额仍在发生变化，被系统判定为用户作恶而被罚没所有押金。

[0180] 为了防止P_i公布之前已作废的通道状态和监督监管人的作恶行为，赎回押金的操作 会在区块链上打开一个时间窗口，在这段时间内P_i的押金将被冻结在通道中，并且所有通道内的节点可以向作恶检测合约提交自己认为正确的状态，来惩罚P_i或通道监管人的可能作恶行为。一旦发现通道监管人作恶或P_i试图赎回不是自己实际余额的金额(通过 公布已作废的通道状态更新信息)，作恶检测合约可以通过作恶证据自动惩罚作恶方。

[0181] 输入：节点P_i认可的最新通道状态信息， StateMsg1＝(Amountarray[n], TxMsgList,r1)sig_S和可能的作恶证据 StateMsg2＝(Amountarray[n],TxMsgList,r2)sig_S的状态更新信息。作恶检测合约V_f的 处理流程如下：

[0182] 验证状态更新消息StateMsg1中通道监管人S的签名；

[0183] 验证状态更新消息StateMsg1的正确性，确保转账交易信息列表的所有交易轮数均 在有效轮数范围内；

[0184] 打开仲裁时间窗口，在这段时间内通道内的节点可以提交作恶证据；

[0185] 验证状态更新消息StateMsg2中S的签名；

[0186] 验证状态更新消息StateMsg2的正确性，确保转账交易信息列表的所有交易轮数均 在有效轮数范围内；

[0187] 如果r1＝r2，且StateMsg2≠StateMsg1，将通道内的保证金分配给通道内的所有节 点并关闭通道(监管人作恶)；

[0188] 如果r2>r1，且P_i的余额D_i发生了变化，向P_i发出信息告知其赎回申请无效，并附上状态更新消息StateMsg2，开启用户申诉时间窗口，等待P_i发起申诉。如果申述时间 窗口关闭前，P_i申述失败，将P_i的余额分配给通道内的其他人(节点P_i作恶)；

[0189] 向节点P_i的链上地址中转入D_i并更新通道状态.

[0190] 值得强调的是，在上述作恶检测合约V_f的处理流程倒数第二步，如果r2>r1，且P_i的余额D_i发生变化时，会开启用户申诉时间窗口，这是因为存在通道监管人恶意提交用 户余额计算错误的通道状态更新信息作为作恶证据的可能性。在这种情况下，由于作恶 检测合约V_f无法确保StateMsg2中的各账户余额是否为合法有效值，因此，需要P_i个人 根据StateMsg2进行申诉反驳。如果是由于通道监管人的恶意提交，P_i可以使用 StateMsg2和另一合法状态更新信息向作恶检测合约提交作恶证据，合约验证通道监管 人作恶后罚没其保证金并关闭通道，从而达到申诉成功的目的。由于使用了申诉机制， 保证了通道监管人在用户押金赎回时，不会恶意提交用户余额计算错误的通道状态更新 信息作为作恶证据，因为监管人作恶会得不偿失，致使其保证金被罚没。

[0191] 优选例2：

[0192] 下面通过一个实例来说明该多向支付通道方案。以用户Alice和Bob想要使用多向通道完成一笔链下支付为例，具体为Alice向Bob支付10代币购买一个服务，大致 的支付流程如下：

[0193] 1)Bob生成转账交易消息TxMsg，具体为

[0194] (Alice,Bob,10,r,00000001)___,sigBob。将其发送给Alice。

[0195] 2)Alice确认转账的金额正确,交易的接收者是目标地址后,附上自己的签名。此时TxMsg消息为:(Alice,Bob,10,r,00000001)sigAlice,sigBob,将该交易消息发送 给通道监管人S。

[0196] 3)通道监管人S接收到该笔转账交易信息后,验证其合法性:

[0197] 通道监管人S核实由Alice发送的TxMsg是否有交易收款方和付款者的签名;

[0198] 检验转账交易信息中的轮数是否在r-Δ到r之间,Δ为系统选定参数,如果轮 数不在此范围内,则拒绝该笔转账交易信息;

[0199] 校验相应用户在第r轮是否存在TxID为00000001的转账交易,如果存在,则拒 绝该转账交易信息;

[0200] 确认Alice的账户中是否有足够的金额,如果当前Alice的账户余额不足,不足 以支付该笔转账,则拒绝该笔转账交易信息;

[0201] 确认上述无误后,将其放入新一轮的状态更新信息中;

[0202] 开启一个定时器,接收在定时器终止之前通道内发送至监管人的转账交易信息,如果收到转账交易,验证其合法性。当定时器时间截止时,生成一个状态更新消息 msg=(Amountarray[n],TxMsg,r)sigS,,并将其广播给通道内的所有人。

[0203] 4)通道内的所有人接收到该消息,核实所有签名无误后认可该结果。参与该轮交易的用户Alice和Bob,此时即可认为支付完成,Bob在收到转账后即可提供服务。

[0204] 提示:

[0205] 通道建立合约负责通道建立阶段用户和监管人向合约中转入押金和保证金,验证金 额;

[0206] 作恶检测合约负责在通道运行期间任意的作恶行为,如果发现作恶行为对相应的用 户进行惩罚,如果是通道监管人作恶,则会导致通道关闭。其他普通用户作恶只会导致该用户的押金被罚没,均分到其他用户的余额中。

[0207] 押金赎回合约负责任意用户的押金赎回行为,在押金赎回验证通过时,负责将用户 的押金打入到用户的区块链账户中。

[0208] 通道建立合约、作恶检测合约、押金赎回合约这三个合约是一个称为多向支付通道 智能合约的子合约,三个合约负责不同的事情,其实质还是多向支付通道智能合约的一个子模块,负责不同的功能。就好比在一个程序中,有不同的进程负责不同的事情一样。

[0209] 多向支付通道的建立,链下支付,通道的关闭这三个步骤的关系是,

[0210] 首先需要用户和通道监管人向通道建立合约打入押金和保证金,合约验证金额合法 以后,通道建立。通道建立以后,用户可以在多向支付通道内部,向其他任意的多向支付通道内的用户进行转账。任何用户可以在任何时刻退出这个多向支付通道,在退出时,需要向押金赎回合约提交赎回申请和证据,如果在一定时间窗口内作恶检测合约没有收到任何与赎回押金的用户相关的作恶证据,押金赎回合约便会向押金赎回的用户地址转入的相应的赎回金额。

[0211] 在通道的使用过程中,任意的作恶行为,用户都可以向作恶检测合约提交通道内任 意用户的作恶证据,如果由合约判断某用户确实作恶,如果该用户是普通用户,那么他在通道内的押金被罚没,均分给通道内的其他人(这里的均分,是指将该押金均分为剩 余

人数的份数后，加在每个用户的押金里，作为通道内可以使用的金额，在这里不存在 实际的区块链转账行为)；如果该用户是监管人，那么他在通道内的保证金被罚没，合约 会将保证金均分给通道内其他人(这里的保证金均分，先是保证金均分后加在每个人的 余额上，接着多向支付通道合约将合约中所有人的余额在区块链上转账至每个人区块链 的账户中。)。

[0212] 步骤1：n个普通用户节点和一个通道监管人S合作建立一个多向支付的链下通道。

[0213] 所述步骤1包括如下步骤：

[0214] 步骤1.1：通道建立前，欲建立多向通道的所有普通用户认可监管人S的身份并获知S的公钥，S获知通道内普通用户节点的公钥；

[0215] 步骤1.2：n个普通用户节点向多向支付通道智能合约的子合约---通道建立合约中打入资金的押金D_i，通道监管人S向智能合约中打入保证金G，G和Di满足的式子为$G=n\times \sum_{i=1}^{n} D_i$。通道建立合约当验证押金和保证金满足条件以后，该多向支付通道成功建 立。

[0216] 步骤2：多向支付通道内的任意用户之间可以使用多向支付通道进行转账。具 体见“通道支付阶段”的内容。这里需要注意的是A和B进行转账时，C和D仍然 可以进行转账。在步骤2中，有三种不同的角色，做不一样的事情。一种是交易的 付款方，一种是交易的收款方，另一种是通道监管人。

[0217] 所述步骤2包括如下步骤：

[0218] 步骤2.1：交易收款方发送转账交易信息TxMsg给交易付款方；

[0219] 步骤2.2：交易付款方验证转账交易信息TxMsg合法后，签名后发送给通道监 管人；

[0220] 步骤2.3：通道监管人收到新一轮的第一个转账交易信息TxMsg后，开启新一轮的工作流程，具体详见交底书中“通道监管人的工作流程部分”。

[0221] 步骤2.4：通道监管人发送新一轮的状态更新信息，收款方和付款方收到新一轮的状态更新消息后，验证他们的转账交易信息TxMsg被包含在内，表明转账交易成功。

[0222] 步骤2.5：在上述2.4中，如果通道监管人发布错误的状态更新信息，通道内的普通用户可以向作恶检测合约提交作恶证据。

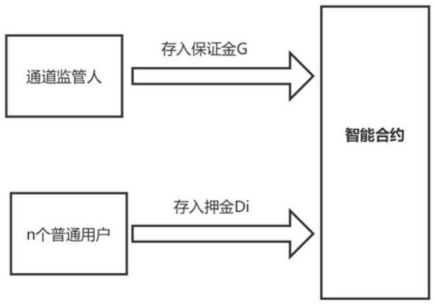
[0223] 步骤3：任意用户赎回押金。这里分为两种情况，一种是单个用户将其押金赎回，由押金赎回合约将钱打入其区块链的账户中，另一种情况时，用户在押金赎回时，作恶 检测合约发现通道监管人S作恶，这将导致S的保证金被罚没均分给通道内的普通用 户，由多向支付通道合约将每个用户的余额打入到其区块链的账户中，通道关闭。具体 内容请参考“通道关闭阶段”。

[0224] 在本申请的描述中，需要理解的是，术语“上”、“下”、“前”、“后”、“左”、“右”、 “竖直”、“水平”、“顶”、“底”、“内”、“外”等指示的方位或位置关系为基于附图所示 的方位或位置关系，仅是为了便于描述本申请和简化描述，而不是指示或暗示所指的装 置或元件必须具有特定的方位、以特定的方位构造和操作，因此不能理解为对本申请的 限制。

[0225] 本领域技术人员知道，除了以纯计算机可读程序代码方式实现本发明提供的系统、装置及其各个模块以外，完全可以通过将方法步骤进行逻辑编程来使得本发明提供的系 统、装置及其各个模块以逻辑门、开关、专用集成电路、可编程逻辑控制器以及嵌入式微控制器等的形式来实现相同程序。所以，本发明提供的系统、装置及其各个模块可以 被

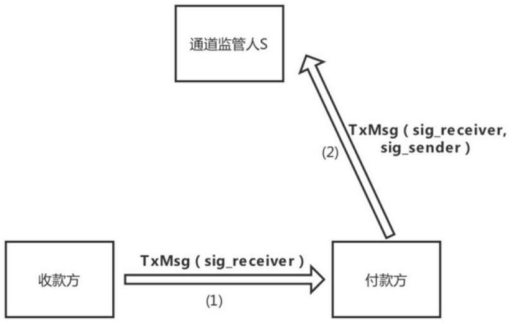
认为是一种硬件部件,而对其内包括的用于实现各种程序的模块也可以视为硬件部件 内的结构;也可以将用于实现各种功能的模块视为既可以是实现方法的软件程序又可以 是硬件部件内的结构。

[0226] 以上对本发明的具体实施例进行了描述。需要理解的是,本发明并不局限于上述特 定实施方式,本领域技术人员可以在权利要求的范围内做出各种变化或修改,这并不影响本发明的实质内容。在不冲突的情况下,本申请的实施例和实施例中的特征可以任意 相互组合。



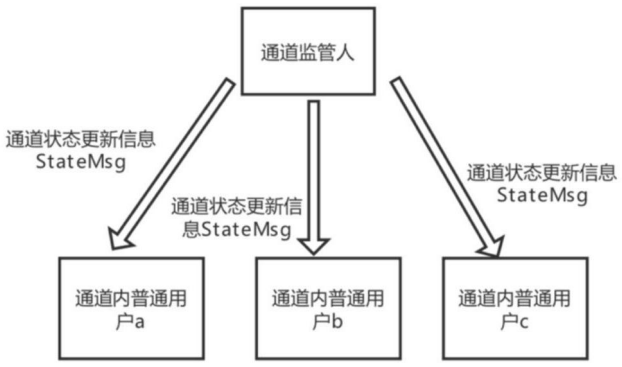
通道建立阶段，n个普通用户节点和一个通道监管人S合作
建立一个多向支付的链下通道。

图1



转账交易信息TxMsg传递流程
由发生交易的收款方进行生成，发送给付款方，
付款方确认无误并签名后发送给通道监管人S。

图2



通道状态更新信息StateMsg传递流程
由通道监管人签名发布，广播给通道内
所有普通用户。

图3

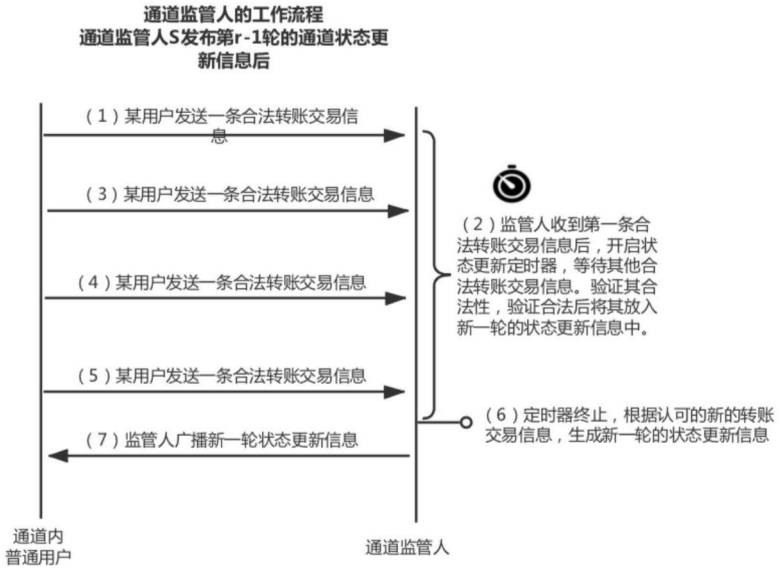

通道监管人的工作流程
通道监管人S发布第r-1轮的通道状态更新信息后
（1）某用户发送一条合法转账交易信息
（3）某用户发送一条合法转账交易信息
（4）某用户发送一条合法转账交易信息
（5）某用户发送一条合法转账交易信息
（7）监管人广播新一轮状态更新信息
（2）监管人收到第一条合法转账交易信息后，开启状态更新定时器，等待其他合法转账交易信息。验证其合法性，验证合法后将其放入新一轮的状态更新信息中。
（6）定时器终止，根据认可的新的转账交易信息，生成新一轮的状态更新信息
通道内普通用户
通道监管人

图4