HQIOTA: 基于IOTA的高质量共识机制

胡　倩[1]，陈杨杨[1,2†]

(1. 东南大学 网络空间安全学院, 江苏 南京 210096; 2. 东南大学 自动化学院, 江苏 南京 210096)

摘要: 物联网应用(IOTA)作为一种经典的基于有向无环图而非链式结构的区块链系统, 由于采用置信度共识方式导致交易确认依赖中心节点, 并且难以及时发现交易冲突. 为此, 本文提出一种基于时间切片的设计方法, 通过规定在每个时间片结束时由内部节点检查并同步当前交易子图, 设计了一种high quality IOTA(HQIOTA)共识机制. 在交易确认中, 通过设计内部节点自适应调节控制替代了原有的外部规定阈值的转变. 进而能及时发现并删除矛盾交易, 解决了交易冲突不敏感的问题. 本文基于概率分布模拟的网络环境进行实验, 结果表明HQIOTA能比IOTA更快发现交易冲突并且更灵活地进行交易确认.

关键词: 区块链; 共识机制; 有向无环图; IOTA

引用格式: 胡倩, 陈杨杨. HQIOTA: 基于IOTA的高质量共识机制. 控制理论与应用, 2024, 41(8): 1335 – 1340

DOI: 10.7641/CTA.2023.20411

HQIOTA: High quality IOTA consensus mechanism

HU Qian[1], CHEN Yang-yang[1,2†]

(1. School of Cyber Science and Engineering, Southeast University, Nanjing Jiangsu 210096, China;
2. School of Automation, Southeast University, Nanjing Jiangsu 210096, China)

Abstract: Internet of things application (IOTA) is a classic blockchain system based on the directed acyclic graph rather than chain structure. Due to the adoption of confidence consensus, transaction confirmation depends on the central node and it is difficult to find conflicting transactions in time. Therefore, this paper proposes a design method based on time slice. It is specified that the current transaction subgraph is checked and synchronized by the internal node at the end of each time slice. A high quality IOTA (HQIOTA) consensus mechanism is designed. In the transaction confirmation, the adaptive control of internal nodes is designed to replace the transformation of the original external specified threshold. Then the contradictory transactions can be found and deleted in time, and the problem of being insensitive to conflicting transactions can be solved. In this paper, experiments are carried out in the network environment based on the probability distribution simulation. The results show that the HQIOTA can find transaction conflicts faster and confirm transactions more flexibly than IOTA.

Key words: blockchain; consensus mechanism; directed acyclic graph; IOTA

Citation: HU Qian, CHEN Yangyang. HQIOTA: High quality IOTA consensus mechanism. *Control Theory & Applications*, 2024, 41(8): 1335 – 1340

1　引言

自从2008年比特币[1]诞生, 其背后的区块链技术凭借独特创新的去中心化思维受到广泛关注. 近年来, 随着区块链在数字金融[2]、物联网[3]、医疗[4]、供应链[5]等各领域的广泛应用, 区块链的核心技术共识机制也成为研究热点. 经典的基于链式结构的共识机制有工作量证明(proof of work, PoW)[1]、权益证明(proof of stake, PoS)[6] 等, 但链式账本始终会受到由其串行结构所带来的可拓展性瓶颈限制, 而图的结构天然支持并发操作.

近年来, 用图结构来表示区块链账本的新思路被提了出来. 若区块链中允许某个区块指向两个或两个以上父节点, 即能容纳分叉, 则该区块链是有向无环图式结构. 链式结构每次只能新加入一个交易, 而图结构可以同时在多个叶子节点后添加多个交易, 其允许分叉、支持并发操作的特性, 使得系统的可扩展性和交易确认速度大大提高. 作为区块链从2.0时代迈向3.0时代的关键技术, 基于有向无环图结构的共识机

收稿日期: 2022−05−19; 录用日期: 2023−10−18.

†通信作者. E-mail: yychen@seu.edu.cn.

本文责任编委: 崔巍.

国家自然科学基金项目(62373097)资助.

Supported by the National Natural Science Foundation of China (62373097).

制成为近几年区块链领域的热门研究话题. 文献[7]提出了一种基于置信度共识的物联网应用 (internet of things application, IOTA) 机制, 即通过设置置信度阈值实现新交易被系统完全确认. 需要指出的是, 为了避免全局无序带来的交易冲突, 该机制通过设置一个中心化协调节点定期进行交易确认. 这也在一定程度上削弱了区块链去中心化的特性. 文献[8]提出了一种Conflux 共识机制结合GHOST协议[9]共识的主链, 实现有向无环图拓扑交易的全局有序. 需要指出的是, 由于GHOST协议是挑选子树权重最大的交易来选择主链, 因此存在一定的延迟, 进而导致主链不一致. 与此同时, 注意到账本虽然是树形结构但最终只有主链上的区块合法, 主链之外孤块的资源浪费不可避免. 为此, 文献[10]提出一种GHOST改进型协议, 即Inclusive Blockchain Protocol, 使得主链之外的区块也能合法存在并获得奖励, 但这种方式也会造成双花攻击的代价减小. 文献[11]提出了另一种IOTA改进型协议, 即ByteBall. 该协议通过在拓扑图中选出富集权威见证人交易最多的一条链作为主链确定全局顺序. 但是, 由于主链选择方法复杂, 很容易出现主链不一致问题. 不同于通过共识主链实现全局有序的设计, 基于平行链的有向无环图共识机制, 例如 Hashgraph[12]和 Nano[13]被提出用于解决主链不一致的问题. 网络中的每个节点分别维护一条链并且各链之间通过相互引用的关系构成区块点阵, 但是其链数量过多且结构复杂, 不易同步.

由以上调研可知, 在基于有向无环图的IOTA共识机制中, 交易确认严重依赖中心节点, 并且网络中相互冲突的交易无法及时被发现. 目前的改进算法大多为在有向无环图中选出一条主链来为全局交易进行排序, 然而引入主链后的节点结构在本质上仍趋向于链式结构, 削弱了图结构的高并发性. 本文通过规定在每个时间片结束时检查并同步当前交易子图, 提出了一种HQIOTA共识机制. 对于交易确认问题, 实现了从原来的外部规定阈值到现在由内部节点自适应调节控制的转变; 对于交易冲突问题, 实现了从原来的对交易冲突不敏感到现在能及时发现并删除矛盾交易的转变. 实验设置上, 为充分考虑现实情景中节点网络通讯存在的不确定性, 首先采用泊松分布、正态分布等概率分布来模拟网络状态, 在此基础上对比吞吐量随时间和节点个数变化的情况, 对HQIOTA的运行效率进行测试. 仿真结果表明, 本文所提出的HQIOTA不依靠中心节点就可以从内部自适应进行交易确认, 并且能比IOTA更快地发现系统中的交易冲突.

2 问题描述

IOTA作为第1个也是最为经典的基于有向无环图结构的共识算法, 从本质上直接取消了区块的概念, 直接以每一笔交易作为基本单位进行记账. 由于没有了打包多个交易到一个区块的过程, 因而节点之间也无需竞争出块权, 所有产生交易的节点均可以向缠结图中添加交易. 值得注意的是各节点本地的缠结图可能不一致, 所以应考虑到通信的异步性. 由于IOTA规定在添加新交易前需要花费少量算力验证前面已有的两笔交易, 因此每一笔交易都可以不断向前追溯到创世区块, 即第1笔交易的位置, 图中交易局部有序.

如果攻击者想要篡改某一个交易则必须欺骗所有直接或者间接与该顶点单元相关的交易. 随着有向无环图总体不断向后扩展, 相关交易会越来越多, 此时攻击难度也会越来越大. 累积权重越大的交易说明该交易被越多的后来交易引用过, 其可靠性也越高. 因此累积权重的本质是系统中所有节点对这笔交易的信任度, 需要系统中节点保持活跃, 即通过不断添加新交易来增大之前交易的累积权重, 这也是IOTA共识机制维持其安全性的重要手段.

实际上, 累积权重并不能真正决定缠结图中的交易确认时间. 在链式结构例如比特币中采用的是最长链标准, 随着时间越久会有越多后来区块支持前面的区块, 这种线性结构使得前面发布的区块确定性很强, 即被回滚的概率很小. 与比特币不同, 在分支较多的缠结图中, 理论上无论前面交易的累积权重有多高、等待时间有多长, 都不严格代表该交易确定性的概率越高. 一方面是因为IOTA共识机制局部有序、全局无序的性质使得交易确认时间不可控. 由于靠相加得到累积权重的难度是线性的, 所以比较容易被一个权重大的交易抵消, 例如攻击者可以通过构造大权重的交易来追上诚实交易的累积权重, 此时还用累积权重来判断交易的可信度就行不通了; 另一方面是因为IOTA全局无序会导致缠结图的不同分支上可能出现两笔冲突的交易而一直不被发现, 即双花攻击.

图1为各节点本地的缠结图, 绿色顶点代表被当前所有尖端交易验证过的高确定性交易, 蓝色顶点表示被部分确认的交易, 黄色代表尾部没有被任何人确认过的尖端交易. 从图中可以看出, 每个新交易只需选择并验证两个已有交易即可完成整个缠结图的协同验证. 假设一个恶意用户在图结构的不同位置分别加入了内容相互冲突的w交易和y交易. 之后的新交易在选择两个父交易进行验证时, 如果只包含了w和y中的一个, 则新交易发现不了冲突, 例如图中的1和2均会验证通过, 此时交易冲突w和y就分别得到了一次确认, 随着交易继续向后发展, w和y还会得到更多的确认; 如果选择的交易直接或者间接地包含w和y这两个交易冲突, 例如新交易5, 则此时就能够发现冲突, 对1和2的验证就无法通过, 交易5会重新选择其他尖端交易(比如选择1和4)进行验证以保证自己成为被添加进缠结图的有效交易.

通过以上分析可以看出, IOTA共识机制的瓶颈一方面在于难以衡量其交易何时得到确认. 目前的IOTA

系统是通过引入一个由基金会运行的中心化协调节点定期进行交易确认, 从外部人为规定阈值来进行确认. 这种方式削弱了区块链去中心化的特性, 使得系统的安全性严重依赖于中心化协调节点的运行情况. IOTA共识机制的瓶颈另一方面在于交易冲突得不到及时有效的处理, 因为新交易为保证自身能被添加进缠结图往往倾向于选择验证不冲突的交易. 本文提出一种HQIOTA共识机制, 在IOTA的基础上增加合理的排序机制, 保证系统的稳定性和安全性.

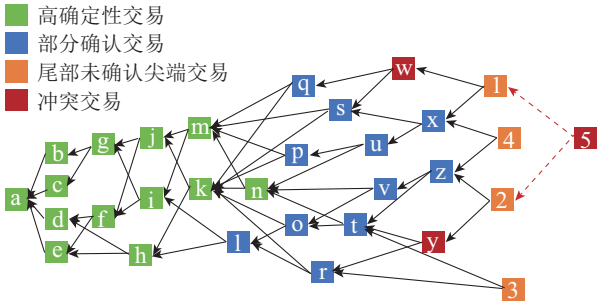

图 1　缠结图

Fig. 1　Tangle

3　算法设计

3.1　HQIOTA 结构

HQIOTA账本结构如图2所示, 图中黑色顶点为有向无环图中各节点发布的交易, 蓝色顶点为各时间片内当前缠结图视图的尖端交易状态. 假设一共有n个节点, 给所有节点从1到n进行编号, 自创始交易开始, 每隔一个固定的时间片, 由各节点轮流检查当前缠结图视图内的交易有无冲突, 若没有冲突则打包当前视图的所有尖端交易.

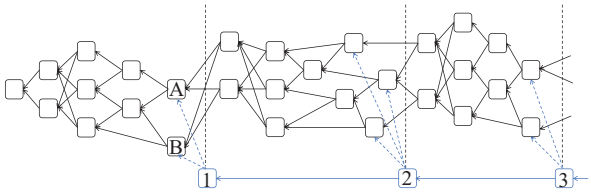

图 2　HQIOTA账本结构

Fig. 2　HQIOTA ledger structure

例如, 图2中共有3个时间片, 第1个时间片结束时1号节点将当前缠结图视图尖端交易状态(A, B)打包成图中蓝色的1号交易状态; 第2个时间片结束时则由2号节点打包当前尖端交易为2号交易状态, 往后依次类推. 叶子顶点又称为终端节点, 是指当前出度为0, 即没有子节点的节点. 由于IOTA中每一个交易都是对前面交易引用而来, 因此, 如果当前所有的叶子顶点相同, 则一定能向前推出相同的交易, 从而保证该缠结图子视图的一致性.

3.2　HQIOTA 算法流程

首先, 在一个时间片的周期内, 节点如果产生了新交易, 则通过IOTA的马尔可夫蒙特卡洛随机游走算法选择一个或者两个没有被验证过的尖端交易进行验证. 若验证通过则将新交易以引用父交易的形式添加到缠结图中. 若没有通过则重新选择节点再次验证.

算法中, 同步状态为时间, 异步状态为交易确认状态. 将节点根据加入网络的先后顺序编号, 从序号为1的节点开始, 依次往后. 各节点轮流检查当前时间片内交易是否有冲突, 例如是否出现同一笔资金同时支付给两位收款方等, 然后就当前尖端交易状态进行共识, 容错率为50%[1]. 具体地, 在当前时间片结束后的一小段时间空隙里, 由序号为i(初始值为1, 依次递增)的节点检查自己本地的缠结图上所有交易是否有冲突. 如果有冲突则应删除与交易冲突直接或间接相关的交易, 并将本次删除操作进行广播. 如果没有冲突则直接打包并广播当前缠结图的尖端交易状态. 上述过程由所有节点轮流进行以保证公平性. 除了负责打包当前交易状态的节点, 其他节点对比本地的缠结图和接收到的尖端交易状态是否一致. 如果一致, 则将系统全局变量m(在每个时间片初始时置为0)加1. 如果全局变量累计超过总节点个数的一半, 则认可当前的尖端状态. 否则就有理由怀疑负责打包当前尖端状态的节点由于传输延迟还没有更新到最新状态, 此时则顺延下一序号的节点重新打包当前的尖端交易状态. 重复以上过程, 直到能够确定当前的尖端状态. 此处对于尖端状态的共识采用的是少数服从多数的方法, 这种方式快捷高效, 是基于假设系统节点由于距离远近和网络传输所造成的不同步错误率不超过50%. 从实验结果可知, 此种假设已覆盖了多次仿真的最坏情况, 具有普遍性. 通常的最极端情况为顺延节点打包的尖端交易状态都不能获得一半以上节点认同. 节点同步尖端交易状态会有一个最长时间限制, 此时以该时间内获得节点认可量最高的尖端交易状态为准. 节点越靠后, 交易数量不会越多. 因为每个节点都会在本地监听新交易并将其添加到自己的交易子图中, 顺延节点只是打包并广播自己本地尖端的几个交易. 图结构是由该段时间的新交易数量决定, 与节点并无直接关系.

最后, 在确定尖端交易状态后, 所有与该状态不一致的节点主动向打包节点请求完整的系统交易子图来更新本地视图. 当每个节点当前的缠结图视图达成一致后, 对该缠结图视图的所有交易进行线性排序. 先对有直接或间接引用关系的交易确定局部顺序, 然后根据交易的时间戳确定彼此无关联的交易, 排序完

[1]文献[1]描述了经典案例–比特币网络受到51%算力攻击的情况. 之所以设置为总节点个数的一半, 是因为如果有超过一半节点的交易子图都能达成一致, 则可以认为该交易子图的权威性超过其他子图. 经典的共识算法PoW等[1,6]通常以节点个数一半作为达成共识的指标.

成后进入下一个时间周期. 由于每个时间周期内都能将交易线性化, 因此可以实现全局有序, 且不影响多个节点向图中加入新交易的并发性.

一个时间周期的HQIOTA算法伪代码流程如表1所示.

表 1 算法1 HQIOTA

Table 1 Algorithm 1 HQIOTA

输入: 时间片长度
输出: 当前时间片内线性化后的交易子图

```
timeSlice: 时间片
newTransaction: 是否有新交易到达
nt: 新交易
parent1: 欲验证的父交易1
parent2: 欲验证的父交易2
result: 当前缠结子图有无冲突
m = 0
i = 1
while time < timeSlice do
    if newTransaction == true then
        nt = newTransaction.get()
        parent1, parent2 = nt.MCMC()
        result1 = nt.verify(parent1)
        result2 = nt.verify(parent2)
        if result1 == true, result2 == true then
            tangle.append(nt, parents)
        end if
    end if
end while
当前时间片结束后, 节点i检查当前交易子图有无冲突
result = node[i].conflict(tangle)
若无冲突则广播当前尖端交易状态并对相同状态节点计数
if result == false then
    node[i].broadcast(tips)
    if node[j].tips == receive.tips then
        m++
    end if
end if
若有冲突则删除交易冲突并广播该操作
if result == true then
    node[i].delete(conflictTrans)
    goto node[i].broadcast(tips)
end if
若有超过一半节点当前交易状态与节点i一致, 则所有节点同步节点i的交易子图
if m ⩾ n/2 then
    node[j].update(tangle);
end if
node[j].linearization(tangle)
i++
end
```

4 实验结果

4.1 实验设计

为了充分考虑到现实通信中网络节点收发消息存在的不确定性, 即假设节点发送的消息只能以一定概率成功被接收者收到, 而非一定被准确无误地接收. 实验设计中采用二项分布、泊松分布、均匀分布、正态分布共4种概率分布来模拟通信网络的状态. 然后选用其中更符合的一种分布来进行后续实验. 本次实验设计的参数有总交易个数、交易到达率、蒙特卡洛随机游走算法中的膨胀系数以及网络错误率. 在进行算法性能测试和对比实验之前, 调参是十分关键的, 合适的参数才能更好地模拟实际情况. 以交易到达率为例, 在实验具体设置上, 采用概率论中经典的泊松分布来模拟一段时间内节点产生交易个数的随机性, 其中的参数为交易到达率, 控制着系统运行过程中交易速率的大小. 当交易到达率取为极小时, 意味着交易产生的速度很缓慢, 新交易往往只能验证一个尖端交易, 此时的缠结图结构如图3所示.

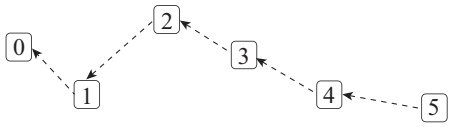

图 3 交易到达率取极小的缠结图

Fig. 3 Tangle with minimal transaction arrival rate

当交易速率取极大值时, 此时节点产生的新交易数量很多, 导致初始时都容易选择各节点本地缠结图中唯一可见的初始交易来验证, 此时的缠结图结构如图4所示. 因此, 在具体实验时, 将交易速率调整为合适值再测试是十分必要的.

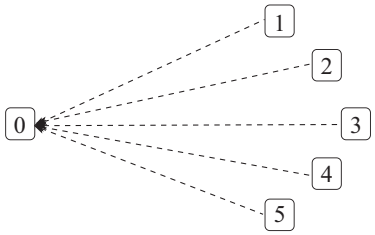

图 4 交易到达率取极大的缠结图

Fig. 4 Tangle with maximum transaction arrival rate

4.2 模拟网络状态的4种分布对比分析

此次实验为能更加模拟真实的网络情况, 即除了正确传输还考虑到网络拥塞、消息传输出错等现实原因, 利用二项分布、泊松分布、均匀分布、正态分布这4种概率分布来模拟信息传输的情况.

具体而言, 对每一次信息发送都先通过概率分布来得到其传输正确、错误、延迟等情况的概率, 以此来模拟网络通信的不确定性. 该模拟贯穿尖端交易状态验证、交易子图线性化等所有涉及消息传输的过程. 由于尖端交易状态确认过程中涉及大量信息传输, 因

此以每一个时间片结束后当前缠结子图确认时间作为衡量不同概率分布下算法性能的指标, 如图5所示, 在每种分布下分别统计前6个时间片中, 每段时间结束后的交易确认时间. 可以看出, 在正态分布模拟的网络通信状况下, 交易确认时间最短且波动幅度最小, 整体表现最佳. 而其他3种分布的交易确认时间更久, 而且更加不稳定. 实验结果也符合对于概率论各种分布在实际应用中的直观认知, 正态分布中信息传输正确的随机事件会以更大概率落在其分布图的中间位置, 这比均匀分布中信息传输正确的概率总是一个确定不变的值更能模拟实际网络的不确定性.

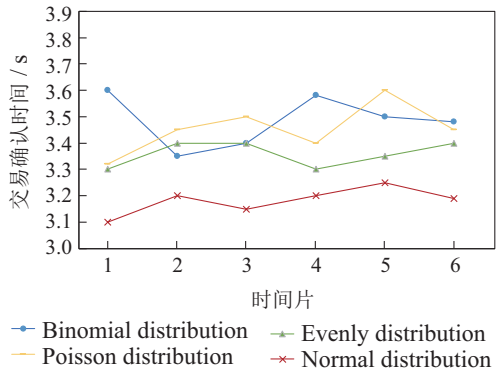

图 5　不同分布下的交易子图确认时间

Fig. 5　Confirmation time of transaction subgraph under different distributions

4.3　吞吐量对比分析

吞吐量是指每秒钟的交易数量. 注意到算法设计过程中时间片和节点个数是制约系统性能的主要自变量. 其他自变量, 如新交易到达速率等, 对算法性能的影响相对较弱, 因此在实验中相关参数均设为一致. 吞吐量是共识算法实验中最为常见的性能指标. 其他因变量, 如达成共识所需时间等, 不适合作为对比实验的因变量指标, 这是因为HQIOTA达成共识所需时间与时间片长度十分相关, 而IOTA达成共识时间取决于中心化协调节点的设置, 因此, 本小节主要研究HQIOTA共识机制随时间片增加和节点个数增多的吞吐量变化情况. 选取大小合适的时间片非常重要. 如果时间片太长会导致本时间段内缠结图中新连接的交易太多, 而且不同节点间交易子图不一致的概率会变大, 给后续确认尖端交易带来不便. 如果时间片太短, 则尖端交易状态确认的时间在一个时间周期的占比就会变大, 造成资源浪费.

本次实验中时间片设定为 20 s, 节点数目设定为30个. 时间片长度之所以设置为20 s是根据之前大量的实验测试 (50 s, 40 s, 30 s, 20 s), 20 s时其交易确认时间和吞吐量表现均较好. 实际上时间片太长会导致交易数量过多, 难以对尖端交易状态达成50%以上的共识. 太短会导致交易数不多时就频繁共识, 吞吐量较低. 图6为HQIOTA吞吐量随时间片推移的变化曲线. 从图中可以看出, IOTA系统的吞吐量约维持在80到90之间的水平, 略高于HQIOTA. 原因在于以下两点. 一方面, 针对交易何时确认的问题, IOTA通过中心化的协调节点定期从外部直接指定阈值来进行交易确认, 而本文的HQIOTA通过分时让内部节点自适应调节控制确认程度, 即将时间分片, 各节点轮流在分片间隙共识交易子图; 另一方面, 对于有矛盾的交易, IOTA不能及时发现(被认为完全确认的交易也可能存在矛盾), 所有交易都被认为产生有效的吞吐量; 而HQIOTA在每个时间片都能及时处理矛盾交易, 节点一旦发现矛盾交易则及时将其删除并广播该操作, 发现的矛盾交易越多会使得相应的吞吐量越少. IOTA的中心化协调节点每分钟会发布一条确认状态的特殊交易, 因此其发现冲突的时间为1 min. HQIOTA在本次实验中时间片选取为20 s, 因此发现交易冲突的时间为20 s, 比IOTA更快. HQIOTA的吞吐量降低主要是因为其能在更短的时间内发现交易冲突, 而这些交易并不被算在吞吐量内. 因此, 虽然HQIOTA相比于IOTA的吞吐量略有下降, 但是HQIOTA解决了以上两方面的问题, 具有更强的实用性.

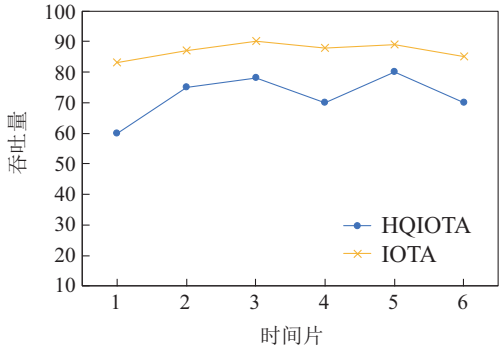

图 6　HQIOTA吞吐量随时间片变化曲线

Fig. 6　HQIOTA throughput versus time slice

图7是 HQIOTA 共识机制吞吐量随节点个数增加的变化曲线, 其中吞吐量为指定数目节点下, 多个时间片的均值水平. 从图中可以看出IOTA的吞吐量基本平稳保持在高吞吐量水平, 而HQIOTA相对而言波动较大. 原因仍然同前述两方面. 具体地, HQIOTA能动态发现每段时间内的交易冲突, 并将它们及时删除, 而IOTA无法及时发现交易冲突, 因此其吞吐量容易呈现出平稳的虚高状态.

实验测试中, 通过把IOTA和HQIOTA某一时刻的本地交易分别打印出来, 人工确认后发现IOTA比HQ-

[2]由于有的矛盾交易并未及时被共识机制发现, 因此有必要对IOTA比HQIOTA多出的交易进行人工确认, 即人工根据打印的交易地址找到交易数据, 再判断是否与已有交易冲突. 实验中选取了多个时刻的交易进行评估, 只是在文中具体选取了一个时刻以便于描述.

IOTA 多出的交易确实是矛盾交易[2], 因此说明 HQIOTA在处理矛盾交易方面更加及时和准确. 某一时刻HQIOTA和IOTA的本地交易如图 8 所示, 括号中第1个数字代表当前交易的高度, 第2个数字代表交易地址的前几位字符, 第3个数字代表生成该交易的节点编号. 检查HQIOTA本地交易发现没有冲突. 检查IOTA 算法中节点本地记录(11:319800:2)和(11: ab5663:9)对应的交易内容分别为将一笔资金转给两个不同用户, 产生冲突. 但由于IOTA中心化协调节点每分钟才进行一次交易确认, 因此, 这两笔交易将一直存在于图中直到中心节点确认交易. 而在HQIOTA中, 节点每20 s进行一次交易共识, 会更快地发现并删除矛盾交易, 由于被删除的交易不被计入吞吐量, 因此HQIOTA吞吐量低于IOTA.

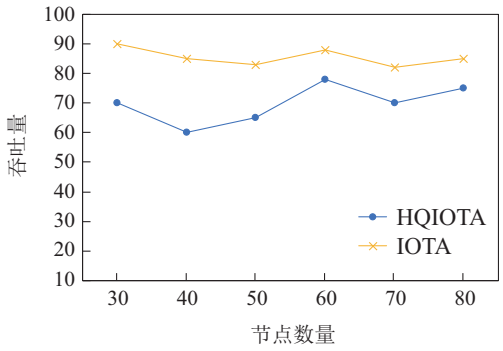

图 7 HQIOTA吞吐量随节点个数变化曲线

Fig. 7 HQIOTA throughput versus the number of nodes

HQIOTA:
(0:56a102:3)−>(1:8909a1:8)(1:29880b:5)−>(2:a15306:1)(2:715301:9)−>(3:623301:2)(3:754233:4)−>(4:a56433:6)−>···−>(12:b30045:18)(12:53c602:10)

IOTA:
(0:527706:8)−>(1:c85409:1)(1:8156b3:2)−>(2:319472:7)(2:41cb65:4)(2:675490:7)−>(3:3189a6:2)(3:cb76ad:10)−>···−>(10:67368a:8)(10:6244ab:13)(10:81a633:15)−>(11:319800:2)(11:ab5663:9)

图 8 某一时刻HQIOTA和IOTA的本地交易

Fig. 8 Local transactions of HQIOTA and IOTA at a certain moment

5 结语

本文主要研究了基于有向无环图结构的IOTA共识机制, 针对其存在的交易确认依赖外部节点、无法及时发现交易冲突的缺点, 本文引入时间切片的概念, 通过规定在每个时间片结束时由内部节点检查并同步当前交易子图, 提出了一种HQIOTA共识机制. 对于交易确认问题, 实现了从原来的外部规定阈值到现在由内部节点自适应调节控制的转变; 对于交易冲突问题, 实现了从原来的对交易冲突不敏感到现在能及时发现并删除矛盾交易的转变. 此外, 为了充分考虑现实情景中网络节点收发消息存在的不确定性, 实验设计中首先采用了4种概率分布来模拟网络状态. 然后通过多组实验验证了所提出的HQIOTA比IOTA能更快发现交易冲突并且不需要依赖中心节点就可以确认交易.

参考文献:

[1] NAKAMOTO S. Bitcoin: A peer-to-peer electronic cash system. *Decentralized Bus. Rev.*, 2008, 4: 21260.

[2] ZHAO Y. Research on personal credit evaluation of internet finance based on blockchain and decision tree algorithm. *Journal on Wireless Communications and Networking*, 2020, 1, 213.

[3] NARTEY C, TCHAO E T, GADZE J D, et al. Blockchain-IoT peer device storage optimization using an advanced time-variant multiobjective particle swarm optimization algorithm. *Journal on Wireless Communications and Networking*, 2022, DOI: 10.1186/s13638-021-02074-3.

[4] CHEEMA M A, ANSARI R I, ASHRAF N, et al. Blockchain-based secure delivery of medical supplies using drones. *Computer Networks*, 2022, 204: 108706.

[5] ZHENG K, ZHANG Z, GAUTHIER J. Blockchain-based intelligent contract for factoring business in supply chains. *Annals of Operations Research*. 2022, 308(1/2): 777 – 797.

[6] DAIAN P, PASS R, SHI E. Snow white: Robustly reconfigurable consensus and applications to provably secure proof of stake. *Financial Cryptography and Data Security: 23rd International Conference*. St Kitts & Nevis: Res Inst, 2019, 11598: 23 – 41.

[7] ALSHAIKHLI M, ELFOULY T, ELHARROUSS O, et al. Evolution of internet of things from blockchain to IOTA: A survey. *IEEE Access*, 2022, 10: 844 – 866.

[8] LI C, LI P, XU W, et al. Scaling nakamoto consensus to thousands of transactions per second. *ArXiv Preprint*, 2018, arXiv: 1805.03870.

[9] MATTHEWS R, LOVELL K, SORELL M. Ghost protocol-snapchat as a method of surveillance. *Forensic Science International: Digital Investigation*, 2021, 36(S): 301112.

[10] ZAMYATIN A, STIFTER N, JUDMAYER A, et al. A wild velvet fork appears! Inclusive blockchain protocol changes in practice. *In Financial Cryptography and Data Security: FC 2018 International Workshops, BITCOIN, VOTING, and WTSC*. Nieuwpoort, Curacao: Springer Berlin Heidelberg, 2018: 87 – 98.

[11] CHURYUMOV A. *Byteball: A decentralized system for storage and transfer of value.* (2016-05-08) [2024-03-13]. https://obyte.org/Byteball.pdf.

[12] WU J, CUI X, HU W, et al. A new sustainable interchain design on transport layer for blockchain. *Smart Blockchain*, 2018, 11373: 12 – 21.

[13] NELSON J, ALI M, SHEA R. Extending existing blockchains with virtualchain. *Distributed Cryptocurrencies and Consensus (DCCL)*. Chicago, lL USA: Microsoft Reasearch-Inria Joint Center, 2016: 77 – 84.

作者简介:

胡 倩 硕士, 主要研究方向为区块链、共识机制等, E-mail: 1209645709@qq.com;

陈杨杨 教授, 主要研究方向包括差分隐私、共识算法、博弈对抗、强化学习等, E-mail: ychen@seu.edu.cn.