计算机科学 COMPUTER SCIENCE
http://www.jsjkx.com
DOI:10.11896/jsjkx.241000174

P-DAG:基于并行链结构的高效安全区块链系统

蒋凌云　刘关浩　杨京霖　徐　佳
南京邮电大学计算机学院、软件学院、网络空间安全学院　南京 210003
(jianglingyun@njupt.edu.cn)

摘　要　基于树图结构的区块链系统利用树图结构具有并发性的特点可以显著提高吞吐量,但是其在安全性方面仍存在很多问题需要解决。针对基于树图结构的区块链系统易遭受活性攻击导致账本状态无法收敛的问题,提出了一个具有高吞吐量和低确认时延的可扩展的高安全性区块链系统 P-DAG(Parallel-Directed Acyclic Graph)。该系统采用多条并行链作为账本结构,将区块创建与上链进行解耦,从而分散恶意节点的算力,增强整个系统的安全性;利用哈希值具有随机性且服从均匀分布的特点,设计基于哈希值的随机权重赋值机制,减少每条链的收敛时间和区块的确认时延。理论分析和仿真实验表明,P-DAG 与 Conflux 具有相近的吞吐量,但所需要的账本收敛时间与 Conflux 相比降低了约 50%,区块确认时延与 Conflux 相比降低了约 30%。

关键词:区块链;并行链;有向无环图;活性攻击;账本收敛
中图分类号　TP309

P-DAG:An Efficient and Secure Blockchain System Based on Parallel Chain

JIANG Lingyun,LIU Guanhao,YANG Jinglin and XU Jia
School of Computer Science,Nanjing University of Posts and Telecommunications,Nanjing 210003,China

Abstract　Although blockchain systems based on tree structures leverage the concurrency of tree graphs to significantly improve throughput,they still face numerous security challenges that need to be addressed. In response to the issue where such tree-based blockchain systems are vulnerable to liveness attacks,leading to a failure in ledger state convergence,a scalable and highly secure blockchain system called P-DAG(Parallel-Directed Acyclic Graph) is proposed,featuring high throughput and low confirmation latency. This system adopts a ledger structure with multiple parallel chains and decouples block creation from the process of adding blocks to the chain,thus distributing the computational power of malicious nodes to enhance the overall security of the system. By utilizing the randomness and uniform distribution properties of hash values,a hash-based random weight assignment mechanism is designed to reduce the convergence time of each chain and the block confirmation latency. Theoretical analysis and simulation experiments show that P-DAG achieves throughput similar to Conflux,but reduces ledger convergence time by approximately 50% and block confirmation latency by about 30% compared to Conflux.

Keywords　Blockchain,Parallel chain,Directed acyclic graph,Liveness attack,Ledger convergence

1　引言

针对区块链系统可扩展性不足的问题,目前主流的解决方案有 3 种。1)链下支付技术,将小额交易转移到链下进行,只有当用户需要关闭通道或一方出现恶意行为的时候才需要进行链上仲裁,将仲裁结果上链。但链下支付技术存在通道双方资金不平衡问题,针对该问题,PnP[1]从初始资金分配的角度出发,将资金规划问题建模为机会约束优化问题,在满足支付需求的同时实现资金分配效率的最大化;APCN[2]提出了一种基于共享资金模式的新型支付通道模型。2)分片技术,借鉴传统分布式数据库中的分片思想,将全网的节点划分到多个集合,通过并行处理交易实现链上扩容。但是分片方案易出现交易负载不均衡的问题,为了解决该问题,BrokerChain[3]通过对用户状态进行细粒度的分割,引入 Broker 账户专门处理跨片交易;TxAllo[4]设计了一种动态交易分配方案,通过将交易分配问题转化为图上的社区检测问题,优化账户及其关联交易的分配。3)基于有向无环图(DAG,Directed Acyclic Graph)的分布式账本技术,从账本形态上对区块链进行改造,利用有向无环图结构支持并发操作的优势提升区块链性能。DAG 因其高并发的特性,被认为是解决区块链可扩展性最具前景的方向之一。

GHOST[5]协议首次提出使用树的结构来存储区块,采用最重子树原则进行账本构建,虽然有效地提高了系统吞吐量,但是 GHOST 容易被恶意节点实施活性攻击。Conflux[6]针对该问题,提出了自适应权重调节机制,虽解决了活性攻击问题,但是需要节点实时检测系统状态,容易造成不必要的资源浪费。Conflux 需要进行更高难度的挖矿,降低了出块速率,影响系统吞吐量。Teegraph[7]提出了一种结合受信任执行环

基金项目:国家自然科学基金(62372250);江苏省 333 高层次人才培养工程项目(BRA2020065)
This work was supported by the National Natural Science Foundation of China(62372250) and Research Foundation of Jiangsu for 333 High Level Talents Training Project(BRA2020065).
通信作者:徐佳(xujia@njupt.edu.cn)

境(TEE)和 DAG 的共识算法,将传统拜占庭容错的节点容错比例从 $3f+1$ 降低到了 $2f+1$,但是在实际中这种受信执行环境并不总能得到保证。OHIE[8]首次采用并行链结构进行账本构建,每条链运行比特币协议,很大程度上提高了系统吞吐量,但是由于其链内仍采用单链结构,易遭受双花攻击且存在资源浪费情况。TIPS[9]通过引入布隆过滤器解决基于 DAG 的区块链中存在的交易打包冲突问题,提高了系统吞吐量,但在布隆过滤器假阳率较高的情况下,系统性能并不理想且安全性也会受到影响。JHDAG[10]设计了一种新的 DAG 结构,用小区块代替传统的大区块,用最长链原则来进行共识,但是 JHDAG 由于采用最长链原则进行共识,容易遭受恶意节点的双花攻击。

因此,为了解决现有的基于 DAG 的区块链系统易遭受活性攻击和双花攻击的问题,本文设计了 P-DAG 区块链系统,主要贡献如下:

1)账本采用并行链结构,将区块的创建与上链进行解耦,区块创建完成后根据哈希值映射到某个链上,利用哈希值具有随机性的特点,攻击者在区块创建完成之前无法确定区块会被添加到哪条链上,使得攻击者无法集中算力攻击账本中的某一条链。

2)账本中的每条链是一个树结构。通过基于哈希值的随机权重赋值机制以及最重子树原则,减少账本收敛时间和区块确认时延,避免系统遭受活性攻击。

2 系统设计

假设网络中存在诚实节点和受攻击者操纵的拜占庭节点,网络中所有节点是同质的,即网络中每个节点的算力相同。P-DAG 是一个基于半同步环境的分布式区块链系统,对于任一诚实节点在 t 时刻发送的消息,其他诚实节点最晚在 $t+\Delta$ 时刻会接收到该消息。攻击者可以控制消息到达不同的诚实节点的时间或者改变消息到达其他节点的顺序,但是不能改变消息的内容。根据半同步网络的假设,攻击者可以让网络中的消息最多经过 Δ 时间到达某个诚实节点。系统的结构如图 1 所示,本地账本由 k 条并行的树状结构链组成,每条链基于最重子树原则进行构建,通过共识机制将区块添加到账本中。

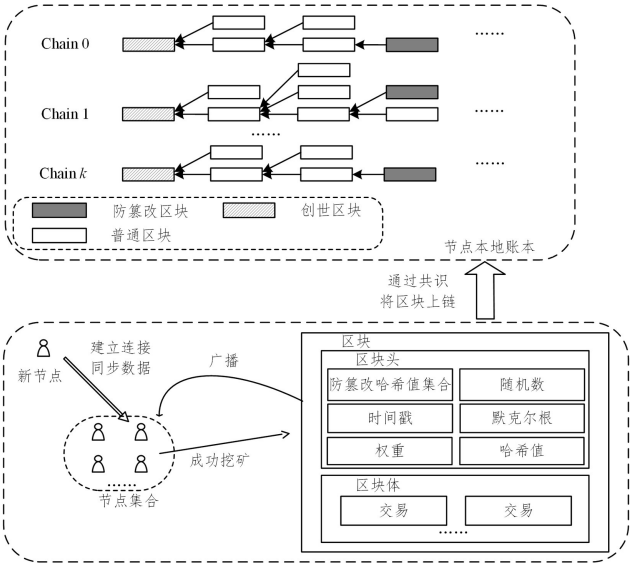

图 1 系统结构图

Fig. 1 System architecture diagram

节点无需注册身份,可以自由加入或退出网络。节点加入网络时,需要通过广播与其他节点建立连接,并通过网络中的其他节点进行数据同步,下载区块链系统的历史数据。为了避免遭受攻击者攻击,在同步数据的过程中,节点会进行数据验证,保证区块链系统的一致性。诚实节点的主要职责包括打包区块并广播、验证区块以及将区块上链。

2.1 基于哈希值的随机权重赋值机制

GHOST 协议首次提出了改变区块链底层数据结构的设计,在 GHOST 协议中所有区块的默认权重为 1,使用最重子树原则进行账本构建,虽然确实有效提高了系统吞吐量,但并没有给出严格的安全性证明。Conflux 中指出 GHOST 协议易遭受活性攻击的问题,对此提出了自适应权重赋值机制,该机制需要节点不停检测当前是否可能正在遭受活性攻击。当节点检测出自己可能正在遭受活性攻击时,需要自适应地调节自己下一个区块的权重,且该调节过程是比较耗时的。

为了解决上述问题,在每个区块创建后,根据其哈希值,为区块赋予一个权重,具体地,假设一个区块的哈希值包含 a 个前导 0,则该区块的权重为 a。被成功打包的区块,根据哈希值的末 $\log_2 k$ 位确定自己需要被添加到哪条链上。每个区块的权重由哈希值决定可能互不相同,且恶意节点不可伪造,后续引理分析表明通过引入随机性,当系统参数设置满足一定条件时,P-DAG 可以抵御攻击者的双花攻击且可以通过调整参数使得攻击者对 P-DAG 系统实施活性攻击无效。

2.2 节点挖矿和验证

P-DAG 采用基于 PoW 的工作量证明机制进行挖矿以抵御女巫攻击。采用最重子树算法进行账本构建,每次产生的区块会根据哈希值的后 $\log_2 k$ 位被添加到某一条链的最重子树上,为了方便计算,规定 k 是 2 的整数次幂。算法 1 展示了任意一条链上最重子树叶子节点的选择,即从创世区块出发,选择权重最大的子树进行继续遍历,直到遍历到叶子节点。如果一条链的最重子树上存在多个叶子节点,则需要从这些叶子节点中选出一个最终的节点用于区块的添加。具体选择规则如算法 1 所示,当最重子树上存在多个叶子节点时,选择权重值最大的叶子节点,如果有叶子节点权重相同的情况,再根据哈希值比较,选择哈希值最小的叶子节点。

算法 1 最重子树叶子节点选择算法

输入:节点本地账本的某一条链

输出:该链的最重子树的叶子节点

```
1. 定义一个空区块 leave
2. 定义该链的创世区块位 pre=leave
3. WHILEtrue
4.     IF pre. children=null
5.       RETURN pre
6.     FOR block IN pre. children THEN
7.      IF leave=null THEN
8.       leave=block
9.     ELSE IF block. weight > leave. weight
10.      leave=block
11.      ELSE IF leave. weight=block. weight
12.        IF block. hash < leave. hash
13.          leave=block
14.        END IF
15.      END IF
```

```
16.   END FOR
17.   pre=leave
18.   leave=null
19. END WHILE
20. RETURN leave
```

假设系统初始化时，会为每一条链创建创世区块。在传统的区块链系统中，节点在进行挖矿的时候，会将父区块的哈希值包含进自己的区块头中进行哈希运算，以此根据哈希值形成一条有向边，通过哈希值验证可以保证数据的防篡改特性。但是 P-DAG 中区块是在创建后才能明确自己被添加到哪条链中，因此，为了保证数据的防篡改特性，区块在进行打包的时候会从每条链的最重子树上选择一个区块作为防篡改区块，并将该区块的哈希值放到区块头中，形成防篡改哈希值集合，然后进行挖矿。

2.3 防篡改哈希值选择

区块结构如图 1 所示，随机数用来提供挖矿难度的证明，时间戳是区块成功创建的时间，默克尔树根是根据交易的哈希值所构造出的默克尔树的根节点的哈希值，用来保证交易内容不被修改。每个区块都有一个权重，一个区块的权重等于该区块自身的权重值与以该区块为根的子树的权重值之和，区块自身的权重在区块创建完成后通过基于哈希值的权重赋值机制确定。

算法 2 给出了如何选取防篡改哈希值集合，对 k 条链进行遍历，遍历每条链时，利用算法 1 从每条链上选取一个最重子树的叶子区块，将该区块的哈希值放入防篡改哈希值集合中。网络中的节点收到来自其他节点的区块时，需要对区块进行验证，对每条链进行层序遍历，找出该区块的所有父区块，并验证他们的哈希值的正确性，如果哈希值验证不正确，说明至少有一个区块中的内容被攻击者篡改。

算法 2 防篡改哈希值集合选择算法

```
输入：节点本地账本 ledger
输出：防篡改哈希值集合
1. 定义空的哈希值集合 ret
2. FOR chain IN ledger THEN
3.   获取 chain 的最重子树叶子节点 leave
4.   将 leave 添加到 ret 中
5. END FOR
6. RETURN ret
```

2.4 区块排序

区块链系统的一致性原则要求网络中的节点能够就账本状态达成一致，即网络中的节点要能够确定账本中的区块顺序。采用并行链结构，每条链中又是一个树结构。对于每条链中的树，根据最重子树原则层序遍历，每一层的区块再根据哈希值的大小进行排序，如果两个区块中存在交易冲突，则认为哈希值小区块中的交易是有效的，具体操作过程如算法 3 所示。当最重子树与所有其他子树的权重差值都超过确认阈值 D 时，最重子树的根区块可以被确认。D 值的计算详见引理 3。

算法 3 区块排序算法

```
输入：节点本地账本 ledger
输出：防篡改哈希值集合
1. 定义一个空列表 order
2. FOR chain IN ledger THEN
3.   定义一个空区块 P,Q
4.   FOR child IN chain THEN
5.     If P=null THEN
6.         Q=child
7.     ELSE IF P. weight <child. weight
8.         Q=P
9.         P =child
10.    ELSE IF P. weight =child. weight
11.      IF P. hash>child. hash THEN
12.        Q=P
13.        P=child
14.      ENDIF
15.    ENDIF
16.  ENDFOR
17.  IF P. weight−Q. weight>D THEN
18.    order. add(P)
19.  ENDIF
20. ENDFOR
21. RETURN order
```

3 系统分析

在 GHOST 协议中，节点根据挖矿难度，要成功创建一个区块，其哈希值至少包含 p 个前导 0，则可以设置挖矿难度使节点成功挖矿区块的哈希值至少包含 q 个前导 0，且满足 $q+\log_2 k=p$。每个区块的哈希值的末 $\log_2 k$ 位的取值范围是 $[0, 2^k-1]$，由于哈希值具有随机性，所以取到每个值的概率是相同的。因此，所设计的系统中，每条链的区块增长速率与 GHOST 协议中区块增长速率相同，所设计的系统的吞吐量较 GHOST 相比在理论上可以提高 k 倍。

为了对 P-DAG 系统进行分析，首先需要定义一些参数，假设网络中节点的数量为 n，网络中存在一个攻击者 A，A 可以控制网络中节点数量所占的比例为 ρ，被控制的节点称为拜占庭节点，则诚实节点所占比例为 $\mu=1-\rho$。假设系统中每个节点本地账本中链的数量为 k 条，将哈希函数建模为随机预言机，每个节点在任一时刻只能进行一次哈希运算，因此攻击者 A 在本系统中的任意时刻所能进行的哈希运算的次数为 $\rho \cdot n$ 次。假设节点的挖矿难度为 $h=\frac{1}{c \cdot \Delta n \cdot k}$，其中 Δ 表示最大网络时延，c 表示网络中一个新的区块产生所需要的预期时间。区块之间的距离表示两个区块之间路径上的边的条数。有如下引理：

引理 1 对于任意的 $\delta \in (0,1)$，在 $t=r$ 时，网络中诚实节点的本地账本的某条链中，对任意一个位于最重子树上的区块 b，当 $t=r+T$ 时，区块 b 以及区块 b 所指向的区块的预期权重的增加量大于等于 $T \cdot (1-\delta)\frac{\mu}{c \cdot k} \cdot avg$，其中 avg 为每个区块自身权重。

证明：区块的权重等于区块自身权重加上以该区块为根的子树上的区块的权重和，由于哈希值具有随机性，且服从均匀分布，因此根据基于哈希值的随机权重赋值机制可得，每个区块自身的权重值范围为 $[x,255]$，其中 x 表示一个有效区块的哈希值所需要包含的前导 0 的个数。为了简化分析，下面的分析中都假设每个区块的自身权重大小都为 $avg=\frac{x+255}{2}$。用 S 表示账本中任意一条链根据最重权重子树原

则选出的主链。每当节点打包出一个区块或者从网络中其他节点那儿接收一个区块 b'，则 b' 块要么在 S 上，要么沿根节点出发，在 S 上的某一个区块 b 处产生分叉，即区块 b' 是区块 b 的一个孩子区块。用随机变量 X 表示 S 长度增加 1 所需要的时间，如果一个诚实节点成功挖出区块，则最多过 Δ 时间，网络中所有诚实节点都会收到该区块。由于诚实节点挖出区块所需要的平均时间为 $\frac{c}{\mu}$，所以 $E[X]\leqslant\frac{ck}{\mu}+\Delta$。故想让某个区块的权重增加 avg 所需要的最大时间为 $\frac{ck}{\mu}+\Delta$。用随机变量 $N(T)$ 表示 T 时间段内区块增长数量，所以 $E[N(T)]=\frac{T\mu}{ck}$。根据 Chernoff-Hoeffding 不等式[11-12]，在时间 T 内账本中每条链根据最重子树原则选出的主链 S 权重增加 $T\cdot(1-\delta)\frac{\mu}{c\cdot k}\cdot avg$ 的概率为 $1-e^{-\frac{E[N(T)]}{2}}$。

引理 2 用 subTree 表示账本中某条链在 r 时刻的子树，该子树满足只有恶意节点在这个子树上挖矿，诚实节点在另一个子树上挖矿，且他们拥有相同的父节点。在 $r+T$ 时刻，网络中首次有诚实节点接收到了子树 *subTree* 中的区块。存在一个可忽略的函数 $\varepsilon(\cdot)$，满足当 $\frac{\mu}{(c+\Delta)}>\frac{\rho}{c}$ 时，*subTree* 与任何诚实节点的主链有交集的概率（即攻击者成功实施双花攻击的概率）小于等于 $\varepsilon(T)$。

证明：沿用引理 1 中的假设，每个区块自身权重为 avg。用区块 b 表示 *subTree* 的父区块，由于网络中的诚实节点并不知道 *subTree* 的存在，所以它们在区块 b 的其他孩子节点为根的子树上进行挖矿，假设该子树为 B。在 $r+T$ 时刻，诚实节点第一次收到了子树 *subTree* 中的区块，为了保证节点无法成功实施双花攻击，在时间 T 内，诚实节点挖出区块的数量需要大于攻击者挖出区块的数量，由引理 1 得，诚实节点挖矿的速率为 $\frac{\mu}{c}$，攻击者挖矿的速率为 $\frac{\rho}{c}$。攻击者可以利用网络延迟，使得部分节点本地账本不一致。因此，为了消除网络延迟带来的影响，如果 $\frac{\mu}{(c+\Delta)}>\frac{\rho}{c}$ 成立，则根据 Chernoff-Hoeffding 不等式可以保证攻击者使 *subTree* 成为最重子树的概率小于 $\varepsilon(T)=e^{-\Omega(T)}$。

引理 3 设账本中某条链的最重子树在 T 时间内权重的增加量为 $S(T)$，则存在阈值 $D=\mu_H-\mu_A-2.326\cdot\sqrt{\sigma_H^2-\sigma_A^2}$，使得当 $c\geqslant\left(\frac{(\mu-\rho)\cdot avg}{2.326\cdot\sqrt{(\sigma_W^2+avg^2)}}\right)^2\cdot\frac{T}{k}$ 时，攻击者无法利用网络延迟来进行活性攻击。

证明：引理 3 给出区块被确认的条件以及证明，每条链上的区块产生过程服从参数为 λ 的泊松分布，其中 $\lambda=\frac{1}{ck}$。用随机变量 W 表示区块自身权重大小，$S(t)$ 表示 t 时刻到达系统中某条链上的区块权重的总和。设满足挖矿条件的哈希值需要至少包含 x 个前导 0，由于哈希值服从均匀分布，所以 $E[W]=\frac{x+255}{2}$，$E[S(t)]=\lambda\cdot E[W]$。用随机变量 $N(T)$ 表示时间 T 内产生的区块数量，随机变量 W_i 表示区块权重，则在时间 T 中，系统中新增的区块的权重总和为 $Sum(T)=\sum_{i=1}^{N(T)}W_i$。由于 $N(T)$ 和 W_i 独立同分布且每个随机变量都有有限的期望和方差，所以根据中心极限定理，$S(T)$ 可以近似为正态分布，即 $S(T)\sim N(T\cdot\lambda\cdot E[W],T\cdot\lambda\cdot(\sigma^2(W)+E^2[w]))$，其中 $\sigma^2(W)$ 表示系统中所有区块的权重和的方差。

假设现在攻击者 A 想要对某条链实施攻击，A 需要至少维护该链上的一条子树的权重与最重子树的权重相近。从攻击者 A 攻击的时刻开始计时，用随机变量 $S_H(T)\sim N(\mu_H,\sigma_H^2)$ 和 $S_A(T)\sim N(\mu_A,\sigma_A^2)$ 分别表示诚实节点和攻击者在时间 T 内所维护的子树权重增加的量，$\mu_H=\frac{\mu}{ck}\cdot T\cdot E[W]$ 和 $\mu_A=\frac{\rho}{ck}\cdot T\cdot E[W]$ 分别表示诚实节点和攻击者在时间 T 内在某条链上产生的区块权重的均值，$\sigma_H^2=\mu\cdot T\cdot\lambda\cdot(\sigma^2(W)+E^2[w])$ 和 $\sigma_A^2=\rho\cdot T\cdot\lambda\cdot(\sigma^2(W)+E^2[w])$ 分别表示诚实节点和攻击者在时间段 T 内产生的区块权重总和的方差。令 $\Delta S=S_H(T)-S_A(T)$。因为 $S_H(T)$ 和 $S_A(T)$ 都是正态分布且相互独立，因此 ΔS 也服从正态分布，将 ΔS 转换成标准正态分布得 $Z=\frac{S_H(T)-S_A(T)-\left(T\cdot\frac{\mu-\rho}{ck}\cdot E[W]\right)}{\sqrt{T\cdot\frac{\mu+\rho}{ck}(\sigma^2+E^2[W])}}$。一个区块可以被安全地确认是指在确认该区块后，该区块所在主链未来被替换的概率非常小，即 $P(\Delta S<0)$ 的概率非常小，假设这个概率为 1%，所以 $P(\Delta S<0)\leqslant0.01$ 转换成 $P\left(Z<\frac{0-\left(T\cdot\frac{\mu-\rho}{ck}\Delta E[W]\right)}{\sqrt{T\cdot\frac{\mu+\rho}{ck}(\sigma^2+E^2[W])}}\right)\leqslant0.01$，设 z_τ 在标准正态分布下使得 $P(Z<-z_\tau)=\tau$，代入 $\tau=0.01$ 得 $z_{0.01}\approx2.326$，D 表示确认阈值，可得 $D=\left(T\cdot\frac{\mu-\rho}{ck}\cdot E[W]\right)-2.326\sqrt{T\cdot\frac{\mu+\rho}{ck}(\sigma^2+E^2[W])}$，化简得 $D=\mu_H-\mu_A-2.326\cdot\sqrt{\sigma_H^2-\sigma_A^2}$。满足当 $\Delta S\geqslant D$ 时，最重子树的根区块可以被确认，且随着 T 增加，该区块被攻击者取代的概率呈指数下降。因此，当最重子树的权重与其他任一子树的权重的差的值大于 D 时，可以在保证安全性的情况下对子树的根区块进行确认。

由引理 1 可得在时间 T 内，对于任意的 $\delta\in(0,1)$，诚实节点维护的子树的权重与攻击者维护的子树权重差值 $Diff=T\cdot(1-\delta)\frac{\mu-\rho}{c\cdot k}\cdot avg$，令 $Diffy\geqslant D$，可得 $c\geqslant\left(\frac{(\mu-\rho)\cdot avg}{2.326\cdot\sqrt{(\sigma_W^2+avg^2)}}\right)^2\cdot\frac{T}{k}$。因此，只要满足 $c\geqslant\left(\frac{(\mu-\rho)\cdot avg}{2.326\cdot\sqrt{(\sigma_W^2+avg^2)}}\right)^2\cdot\frac{T}{k}$，就可以保证系统免遭攻击者活性攻击。

由于本文的 k 条链是相互独立的，任意一条链都满足上述 3 个引理，所以整个系统也满足上述 3 个性质。

通过分析可以证明 P-DAG 满足几个特性：1）节点本地账本的主链上区块的数量随着网络中被挖出区块的增加而稳定增加；2）保证主链的安全性，即主链被恶意节点所维护的链所取代的可能性要尽可能低；3）系统活性，主链上的区块要能被及时确认，即网络中的节点根据共识算法输出的区块序列要能随着时间的推移而增长。

4 系统仿真

通过 Java 语言实现了 P-DAG 系统的出块、验证和排序过程，并在 CPU 为 Intel(R) Core(TM) i5-13500HX、16 GB 内存的主机上进行仿真实验。通过使用多线程并行处理和 Docker 容器技术，模拟区块链节点的挖矿、通信和共识等操作，验证 P-DAG 的吞吐量、确认时延等性能指标。为了使实验具有可比性和公平性，本文设置的系统参数与 GHOST 和 Conflux 相同，在 4.1－4.3 小节中恶意节点的比例为 30%，4.4 小节测试了恶意节点比例对系统性能的影响。

4.1 区块确认时延测试

区块确认时延影响着系统性能和用户体验，交易确认时延过高会导致系统性能下降并给用户带来不好的体验。Conflux 协议虽然在 GHOST 协议的基础上提出了自适应权重赋值机制以抵御攻击者的活性攻击，但是其自适应调节的时间过长，会给用户带来很不好的体验。首先假设攻击者在暂时不进行活性攻击的情况下测量系统的确认时延，比较 P-DAG 在不同的 k 值和不同区块产生速率下区块确认时延的大小，并将区块确认时延大小与 Conflux 和 GHOST 进行对比。实验结果如图 2 所示，对于 $k=8$，16 和 32，P-DAG 的确认时延都要优于 GHOST 和 Conflux。$k=16$ 时 P-DAG 的区块确认时延是最小的。

当 k 等于 16 时的区块确认时延低于 $k=8$ 和 $k=32$ 的原因如下：当链的条数比较多时，区块被分散到不同的链上，导致每条链上最重子树的权重与其他子树权重大小差不多。当链的条数比较少时，每条链上区块比较多，攻击者可以很好地利用网络时延进行活性攻击，导致最重子树上的区块无法被确认。

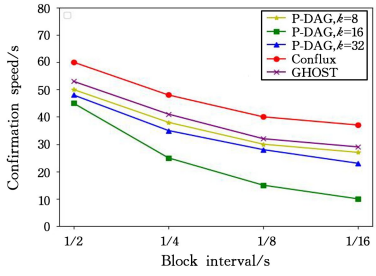

图 2 区块确认时延

Fig. 2 Block confirmation latency

4.2 账本收敛速度测试

在基于主干链的区块链系统中账本收敛速度就是网络中的节点就账本中的主干链达成一致所需要的时间，且在节点达成一致后，主干链被取代的概率应随着时间增加而呈指数级减小。根据之前的引理 3 可知，当最重子树的权重与其他子树之间的权重差值超过 $D=\mu_H-\mu_A-2.326\cdot\sqrt{\sigma_H^2-\sigma_A^2}$ 时，以该区块为根的子树可以被安全地确认。图 3 给出了在攻击者实施活性攻击的情况下不同区块链系统的账本的收敛时间，用 d 表示 P-DAG 中两个最重子树的权重差值。

如图 3 所示，从攻击者实施活性攻击开始，需要花 1 800 s 左右才能使最重子树的权重与其他子树的权重的差值 d 超过 D，最终使账本状态收敛，而 Conflux 的自适应调节机制需要 4000 s 才能使最重子树的权重与其他子树的权重产生明显的差异，使账本收敛。由此可见，在活性攻击下，P-DAG 的收敛速度相比 Conflux 提高了一倍以上。

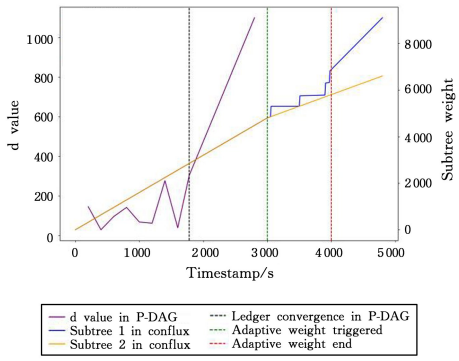

图 3 账本收敛时间

Fig. 3 Ledger convergence time

4.3 系统吞吐量测试

系统吞吐量反映了系统处理交易的速度和效率，是衡量一个区块链系统的重要指标。

选取前述实验中区块确认时间最短的 $k=16$，将 P-DAG 与 GHOST 和 Conflux 吞吐量进行了比较，实验结果如图 4 所示。

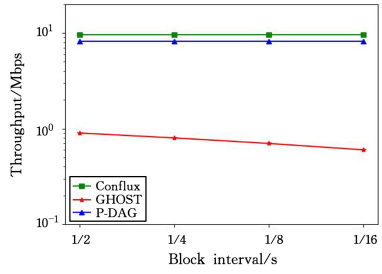

图 4 系统吞吐量

Fig. 4 System throughput

由图 4 可知，P-DAG 系统的吞吐量高于 GHSOT 系统的吞吐量，且与 Conflux 系统吞吐量接近。P-DAG 系统吞吐量理论上应是 GHOST 的 k 倍，但是并未能达到这一效果，主要是受网络带宽等物理因素影响。P-DAG 系统吞吐量略低于 Conflux，是因为 Conflux 是基于图结构的区块链系统，其并发性更高，所有账本中的区块都会被包含在算法 3 的区块输出序列中，而 P-DAG 是基于树形结构的区块链系统，虽然其账本收敛的速度要高于 Conflux，但在系统刚启动到账本收敛这段时间内，会有些区块不是在最终收敛的最重子树上的。为了系统安全性考虑，这些区块被直接丢弃，不计入系统吞吐量内。

4.4 恶意节点比例对系统性能的影响

本节研究了 P-DAG 在不同恶意节点比例的情况下系统抵御活性攻击的能力以及区块确认时延的变化。

图 5 展示了 P-DAG 在不同恶意节点比例下账本收敛时间，P-DAG 采用并行链结构，将区块创建与上链进行解耦，恶意节点无法控制区块的上链过程，只能通过不广播或延迟广播区块来影响账本中其他区块的确认和账本状态的收敛。因此，在系统中恶意节点所占比例高达 45% 的情况下，P-DAG 依然能够在 2100 s 左右使账本状态收敛，可见 P-DAG 具有较强的鲁棒性。

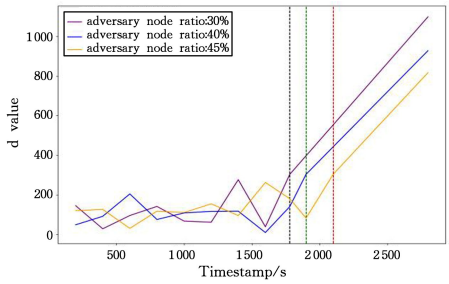

图 5 不同恶意节点比例下账本收敛时间

Fig. 5 convergence time under different adversary node ratios

图 6 展示了 P-DAG 在不同恶意节点比例下区块的确认时延变化情况，随着恶意节点比例增加，区块确认时延增加。

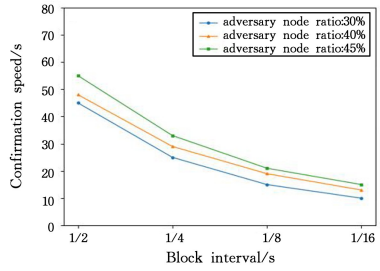

图 6 不同恶意节点比例下区块确认时延

Fig. 6 Confirmation latency under different adversary node ratios

结束语 本文提出了 P-DAG 区块链系统，通过并行链结构和基于哈希值的随机权重赋值机制，提高了系统安全性，降低了区块的确认时延。理论分析和仿真实验结果表明，P-DAG 系统相比现有的区块链系统，在账本收敛时间和区块确认时延方面具有显著优势，特别是在树图结构中能够有效避免活性攻击。

P-DAG 在系统吞吐量方面还有一定的优化空间，未来可以考虑结合支付通道网络进一步优化系统吞吐量。支付通道网络能够缓解链上交易的压力，通过链下交易处理提高系统的整体吞吐量，而 P-DAG 并行链结构仍可确保链上交易的安全性和快速确认。这种结合有望进一步优化系统性能。

参 考 文 献

[1] LI P, MIYAZAKI T, ZHOU W. Secure balance planning of off-blockchain payment channel networks[C]// IEEE INFOCOM 2020-IEEE Conference on Computer Communications. IEEE, 2020: 1728-1737.

[2] ZHANG X, QIAN C. Toward Aggregated Payment Channel Networks[J]. IEEE/ACM Transactions on Networking, 2024, 32(5): 4333-4348.

[3] HUANG H, PENG X, ZHAN J, et al. Brokerchain: A cross-shard blockchain protocol for account/balance-based state sharding[C]// IEEE INFOCOM 2022-IEEE Conference on Computer Communications. IEEE, 2022: 1968-1977.

[4] ZHANG Y, PAN S, YU J. Txallo: Dynamic transaction allocation in sharded blockchain systems[C]// 2023 IEEE 39th International Conference on Data Engineering (ICDE). IEEE, 2023: 721-733.

[5] YONATAN S, AVIV Z. Secure highrate transaction processing in bitcoin[C]// International Conference on Financial Cryptography and Data Security. Springer, 2015: 507-527.

[6] LI C, LI P, ZHOU D, et al. A decentralized blockchain with high throughput and fast confirmation[C]// 2020 {USENIX} Annual Technical Conference ({USENIX}{ATC} 20). 2020: 515-528.

[7] XIANG F U, WANG H, SHI P, et al. Teegraph: trusted execution environment and directed acyclic graph-based consensus algorithm for IoT blockchains [J]. Science China (Information Sciences), 2022, 65(3): 269-271.

[8] YU H, NIKOLIĆ I, HOU R, et al. Ohie: Blockchain scaling made simple[C]// 2020 IEEE Symposium on Security and Privacy (SP). IEEE, 2020: 90-105.

[9] CHEN C, CHEN X, FANG Z. Tips: Transaction inclusion protocol with signaling in dag-based blockchain[J]. IEEE Journal on Selected Areas in Communications, 2022, 40(12): 3685-3701.

[10] HE J, WANG G, ZHANG G, et al. Consensus mechanism design based on structured directed acyclic graphs[J]. Blockchain: Research and Applications, 2021, 2(1): 29-40.

[11] CHERNOFF H. A Measure of the Asymptotic Efficiency for Tests of a Hypothesis Based on the Sum of Observations[J]. Annals of Mathematical Statistics, 1952, 23: 493-509.

[12] HOEFFDING W. On the Distribution of the Number of Successes in Independent Trials[J]. Annals of Mathematical Statistics, 1956, 27: 713-721.

JIANG Lingyun, born in 1978, Ph.D, associate professor, is a member of CCF (No. P7835M). Her main research interests include blockchain, intelligent sensing and information processing.

XU Jia, born in 1980, Ph.D, professor. His main research interests include wireless charging networks, blockchain, and intelligent information processing.