计算机科学
COMPUTER SCIENCE

基于区块链的双分支结构扩展模型

王俊陆, 刘强, 张冉, 纪婉婷, 宋宝燕

引用本文

王俊陆, 刘强, 张冉, 纪婉婷, 宋宝燕基于区块链的双分支结构扩展模型[J]. 计算机科学, 2023, 50(8): 365-371.

WANG Junlu, LIU Qiang, ZHANG Ran, JI Wanting, SONG Baoyan. Blockchain-based Dual-branch Structure Expansion Model [J]. Computer Science, 2023, 50(8): 365-371.

计算机科学 COMPUTER SCIENCE
http://www.jsjkx.com
DOI:10.11896/jsjkx.220900049

基于区块链的双分支结构扩展模型

王俊陆　刘　强　张　冉　纪婉婷　宋宝燕
辽宁大学信息学院　沈阳 110036
(wangjunlu@lnu.edu.cn)

摘　要　随着区块链技术的迅速发展,区块链面临着存储开销和数据吞吐率方面的可扩展性挑战。受全体一致性共识原则影响,区块链节点需存储整个区块链的全局账本,数据存储开销大;同时,为维持区块内交易一致和可信,区块链网络中所有节点均需参与到交易验证同步中,导致网络中区块同步延迟高,带宽征用受阻,进一步降低了数据吞吐量。针对这些问题,提出了一种基于区块链的双分支结构扩展模型。首先,建立区块链三元存储扩展结构,节点对存储任务进行精准划分,分别存储区块链的单一、部分、全局账本,有效降低节点存储负担。其次,提出双分支结构模型,将主链进行信息分流,通过多通道子链并行存储数据,显著提升数据存储速率。针对分流后子链存在的兼容问题,引入双向轮换机制实现链式结构间融合过渡;针对分流后子链安全问题,提出赌徒扩展-F、赌徒扩展-S策略,对两种链式结构进行模拟安全攻击,并对攻击过程进行数学建模。最后,构建两个模型的安全性约束,验证双分支模型的安全性。实验结果表明,所提双分支结构扩展模型能有效抵御恶意双花攻击,且在存储开销、数据吞吐率方面有很大优势。

关键词:区块链扩容;二度分支链;三元存储扩展;双向轮换机制;赌徒扩展模式
中图法分类号　TP311

Blockchain-based Dual-branch Structure Expansion Model

WANG Junlu,LIU Qiang,ZHANG Ran,JI Wanting and SONG Baoyan
School of Information,Liaoning University,Shenyang 110036,China

Abstract　With the rapid development of blockchain technology,blockchain faces scalability challenges in terms of storage overhead and data throughput. The blockchain is affected by the consensus principle of overall consensus,and the global ledger of the entire blockchain needs to be stored between nodes,and the data storage overhead is high. At the same time,in order to maintain the consistency and credibility of transactions within the block,all nodes participate in the process of transaction verification and synchronization,the block synchronization delay in the peer-to-peer network is high. And the bandwidth requisition is blocked,which further reduces the data throughput. In response to these problems,this paper proposes a blockchain-based dual-branch structure expansion model. First,a ternary storage expansion structure of the blockchain is established. The nodes accurately divide the storage tasks and store the single,partial,and global ledger of the blockchain,which effectively reduces the storage burden of the nodes. Secondly,a dual-branch structure model is proposed,the main chain is divided into multi-channel sub-chains. And data is stored in parallel through multi-channel sub-chains,which significantly improves the data storage rate. Aiming at the compatibility problem of sub-chains after shunting,a two-way rotation mechanism is introduced to realize the fusion transition between chain structures. For the security problem of sub-chains after shunting,the gambler extension-F and gambler extension-S strategies are proposed to simulate the security attack of the two chain structures,and the mathematical modeling of the attack process is carried out. Finally,constructing the security constraints of the two models to verify the security of the dual-branch model. Experiments show that the dual-branch structure expansion model proposed in this paper can effectively resist malicious double-spending attacks,and has great advantages in storage overhead and data throughput.

Keywords　Blockchain expansion,Two-degree branch chain,Ternary storage expansion,Two-way rotation mechanism,Gambler expansion mode

到稿日期:2022-09-06　返修日期:2023-03-10
基金项目:辽宁省应用基础研究计划(2022JH2/101300250);数字辽宁智造强省(数字经济方向)(13031307053000568);国家重点研发计划(2021YFF0901004);辽宁省中央引导地方科技发展资金计划项目(2022JH6/100100032);辽宁省自然基金资助计划(2022-KF-13-06)
This work was supported by the Applied Basic Research Program of Liaoning Province(2022JH2/101300250),Digital Liaoning Smart Building Strong Province(Direction of Digital Economy)(13031307053000568),National Key R&D Program of China(2021YFF0901004),Central Government Guides Local Science and Technology Development Foundation Project of Liaoning Province(2022JH6/100100032) and Natural Science Foundation of Liaoning Province(2022-KF-13-06).
通信作者:宋宝燕(bysong@lnu.edu.cn)

1 引言

区块链存储采用哈希散列、非对称加密等高效密码学原理[1-2]确保可靠性，通过点到点连接[3]进行分散式存储[4-5]。区块链账本由所有节点共同维护，基于可信化共识机制[6]存储数据。近年来，区块链在数字货币、企业经营、营商环境等方面[7-8]应用广泛，如采用算力证明[9]的比特币、莱特币等。但随着区块链应用规模不断增大[10]，普通节点难以承受日趋加剧的存储负担，且需抵御愈加复杂的恶意攻击[11]，例如截至2022年5月，比特币区块链的全局账本已经达到500 GB。此外，账本记账速率越来越滞后于数据实时产生速率，例如，尽管以太坊已经采用了多种扩容方案来提升数据存储速率，但直到2022年第二季度，仍有提升数据吞吐率的需求。因此，区块链在存储负担和数据吞吐率方面的问题愈加突出。

现有的扩容机制多以单链为主，主要在区块大小和区块创建速率方向进行扩展。如BitcoinXT[12]扩展方案直接将区块体积增长为8 M，显著增加了区块体交易量；此外，相对于比特币区块链每10 min产生一个区块，ETH区块链每13 s产生一个块，交易速率得到明显提升。但这些扩容方案限制了区块链的数据吞吐上限。同时，现阶段区块链多采用分散式存储方式，每个节点存储区块链的全局账本，数据存储开销大。因此，如何进一步降低区块链存储开销，提升区块链数据吞吐率，成为当前区块链研究的难点。针对这些问题，本文提出了一种基于区块链的双分支结构扩展模型，主要贡献如下：

(1)针对区块链巨大的存储开销，设计了一种三元存储扩展结构，节点根据不同存储需求，采用单一、部分、全局账本进行存储，显著降低了存储开销。

(2)提出了双分支结构模型，包括自由竞争链和串行集中链。将主链进行数据分流，划分为多条子链，进一步拓展了数据存储通道，显著提升了数据吞吐量。

(3)在此基础上，针对子链分流后因结构性差异导致的不兼容情况，提出了一种双向轮换机制，通过二度链融合过渡平稳轮换链式结构。

(4)针对子链分流后结构的安全性问题，通过赌徒扩展-F、赌徒扩展-S策略，模拟攻击两种链式结构，并分别构建两种链式结构的安全性约束，验证了模型的有效性。

2 相关工作

目前，许多学者对区块链扩展技术展开了深入研究，取得了很多研究成果。文献[13]提出了许可链多中心动态共识机制，通过少数节点构建区块链共识网络，优化网络拓扑结构，减少区块确认延迟，提升数据存储速率。文献[14]提出了一种可扩展区块链模型，通过优化区块链存储结构来降低网络负载实现扩展。文献[15]提出了超级节点(BCBSN)协议，超级节点维护区块链网络的正常事务，以合理的比例减少事务传播时延，进一步提升区块链吞吐率。但上述方案对少数节点依赖性强，不利于区块链系统的稳定。

文献[16]提出了一种基于残数系统的存储优化机制，使用CRT-II的恢复过程来检测来自恶魔节点的乱码数据，减少了每个节点的存储量。文献[17]设计了一种分层次代理模型，代理节点和普通节点分工精确，极大地提升了区块存储量，但系统设计较为复杂，稳定性不足。

本文在现有研究的基础上，在区块链存储负担以及数据吞吐率方面进一步研究，提出了基于区块链的双分支结构扩展模型。

3 双分支扩展模型

在数据存储方面，本文设计了一种三元存储扩展结构。该结构存储方式分为全复制存储、多单元存储和全分割存储。链上节点按需选择对应方式存储，然后构建双分支多通道扩容结构，并通过双向轮换机制进行差异性结构链融合过渡。

3.1 三元存储扩展结构

在双分支区块链中，一条主链可扩展为多条子链，节点存储每条子链上的数据时，至少需存储一条完整的存储单元。

节点在单链上能根据任一区块头部哈希值回溯到区块链创世区块，则单链上所有区块形成一条存储单元。

三元存储扩展结构中有以下3种记账方式：

(1)全复制存储：每个节点记录整个区块链所有存储单元账本。此结构获得整个区块链全局视图，该类型节点多为区块链的全局管理和服务节点，用于动态监视区块链整体运行情况，以及提供区块链后续的维护、更新。

(2)多单元存储：每个节点记录有限个存储单元，并对其进行动态更新存储。此结构获得区块链局部视图，该类型节点为区块链的局部管理和服务节点，用于动态监视、管理区块链的局部运行情况，以及持续向区块链全局管理服务节点汇报当前存储单元的运行状况，也作为区块链的数据存储节点，如下文中采用串行集中链作为存储结构的区块链。

(3)全分割存储：每个节点记录自己所运行的单一存储单元。该模式下节点只负责单元子链的区块存储。此类型节点为区块链的数据存储节点，如下文中采用自由竞争链作为存储结构的区块链。三元存储扩展结构如图1所示。

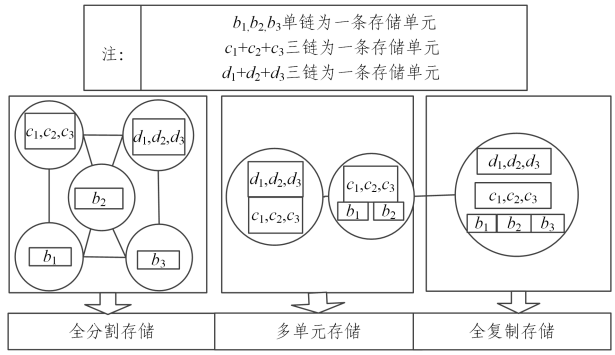


图1 三元存储扩展结构

Fig. 1 Ternary storage expansion structure

3.2 双分支链式结构构建

双分支链式结构包括自由竞争链和串行集中链两种子链结构。在这两种链式结构中，结构主链被分流为多条子链后，原主链信息被有序分配到各子链间存储，可显著提升数据流量。双分支链式结构主链分流为多条子链，子链对不同的

数据流进行并行存储，可显著提升数据吞吐量。

3.2.1 自由竞争链式结构

在自由竞争链中，区块链经分支后形成多条子链，子链间相互独立。存储节点必须存储一条完整的存储单元，体现了区块链良好的回溯性和完整性。子链只在本链条上打包信息，不与其他子链进行交互，子链间的算力竞争会导致算力资源分配不均，威胁区块链的算力安全，因此引入均衡分配机制来平衡算力差距。

各子链间算力分配不同导致存储速率差距明显，为防止恶意算力攻击引起安全问题，系统将新加入的记账节点分配到算力薄弱的区块子链记账，这一过程为均衡分配。

自由竞争链式结构示意图如图 2 所示，其中“Free-competition”代表自由竞争链式结构，每条单链由上至下依序创建区块，子区块 PreHash 值等于父区块 Hash 值，单链间互不影响。算力薄弱的单链由系统默认分配补充算力，使整体区块链算力趋于一致，其中(x,y)形式坐标唯一标识了区块在自由竞争链中的位置。

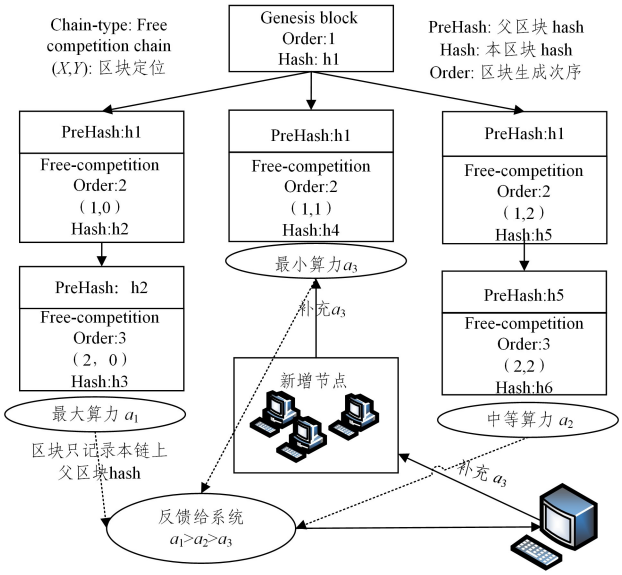


图 2 自由竞争链式结构示意图

Fig. 2 Schematic diagram of free competition chain structure

自由竞争链式结构中，存储区块的节点下载一条存储单元后运行本地事务。在双分支两种链式结构中，自由竞争链存储开销最小，且可以任意选择符合需求的链条进行存储，自由度更高。区块头部信息的链条类型 Construct 字段为“Free-competition”。新增 Location 字段。

由二维坐标$[Xline,Yrow]$进行标志定位，$Xline$ 表示自由竞争链开始分叉后的行标，$Xrow$ 表示自由竞争链开始分叉后的列标，通过区块链的 Location 字段，子链区块得到伪哈希所在的区块。

3.2.2 串行集中链式结构

串行集中链式结构经过分支后，同一层次高度的子链上区块，生成顺序为从左到右；同一层高度的区块经过算力汇聚全部生成后，开始进行区块链下一层高度区块创建，下一层区块创建顺序为从左到右。

区块链分流会带来算力安全问题。系统为聚合各分流子链算力，将区块创建顺序设置为由左到右、由上到下，集中所有支链算力依序创建区块。

串行集中链式结构示意图如图 3 所示，串行集中链将诚实算力集中起来进行区块有序创建。串行集中链式结构经过主链分流后，系统强制子链的同一高度区块打包顺序从左到右，待当前高度所有子链打包完毕后进入下一高度进行打包。物理层每条子链相互独立，逻辑层各子链相互联系。

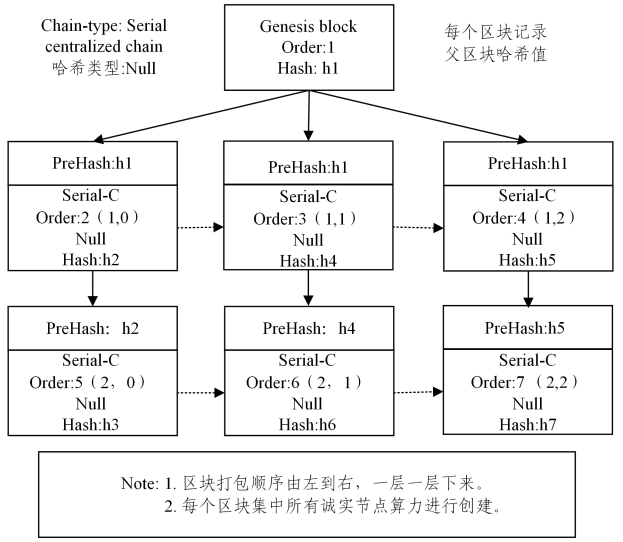


图 3 串行集中链式结构示意图

Fig. 3 Schematic diagram of serial centralized chain structure

在双分支两种链式结构中，串行集中链存储开销较大，但链式结构一方面将诚实算力集中起来抵御恶意双花攻击，安全度更高；另一方面，监管者可通过延迟攻击建立防御优势。该结构头部信息 Construct 字段为“Serial-concentration”。子区块 PreHash 值等于父区块 Hash 值。

3.3 双向轮换机制

双分支区块链中，一种链式结构扩展后可以转换成另一种链式结构，两种链式结构在状态切换时会导致兼容性问题。基于此，本文提出了一种双向轮换机制，使区块链在不同链式结构间平稳过渡。存在以下链式结构的双向轮换：自由竞争链和串行集中链间双向轮换。

自由竞争链向串行集中链轮换时，自由链待数据有序分配到串行链各子链，串行集中子链上的节点不能只存储本节点所在子链的存储单元，因为同一层次高度区块的创建次序由左到右，每条子链并非相互独立，所以还需存储分流后所有子链的存储单元，相应的 Construct 字段由“Free-competition”变成“Serial-concentration”；串行集中链向自由竞争链轮换时，串行集中链存储的数据有序分配到自由竞争各子链，自由竞争链上的节点只需存储子链所在的一条存储单元即可（不受其他子链干扰），相应的 Construct 字段由“Serial-concentration”变成“Free-competition”。

表 1 列出了两种链式结构融合过渡的状态变化。伴随着链式结构的变化，相应的区块关键属性字段也发生了变化（省略原有区块时间戳、随机数、MerkleRoot 等字段），进而改变了子链的记账规则，达到了链式结构间平稳过渡的目的。

表 1 双链融合过渡

Table 1 Two-chain integration transition

头部参数	创世区块头部	自由竞争链 0 区根块	自由竞争链 1 根区块	自由竞争链 区块	自由竞争链 0 尾区块	自由竞争链 1 尾区块
Prehash	Null	√	√	√	√	√
Construct	Null	Free-competition	Free-competition	Free-competition	Free-competition	Free-competition
Location	Null	(1,0)	(1,1)	(Xfree,Yfree)	(Xend-F0,0)	(Xend-F1,1)
头部参数	串行集中链 1 根区块	串行集中链 1 区块	串行集中链 1 尾区块	串行集中链 4 根区块	串行集中链 4 区块	串行集中链 4 尾区块
Prehash	√	√	√	√	√	√
Construct	Serial-concentration	Serial-concentration	Serial-concentration	Serial-concentration	Serial-concentration	Serial-concentration
Location	(1,1)	(Xserial1,1)	(Xend-S1,1)	(1,4)	(Xserial4,4)	(Xend-S4,4)

4 模型安全性分析与约束

在双分支扩展结构中，数据经分流形成多条子通道后，会面临区块链安全攻击。基于此，提出赌徒扩展-F、赌徒扩展-S 攻击模式，并对两种模式进行安全性分析。在此基础上，分别构建两种模型的安全性约束。

4.1 赌徒扩展-F

赌徒破产模型：假定一个赌徒每局能赌赢的概率固定，此时他已经输了若干局，若规定他能进行无数次赌博，试图把亏空的那些赌局补回来，即为最后填补亏空成功的概率。

自由竞争链式结构各子链独立运行，均衡分配机制均衡子链间算力分配，使其趋于一致，恶意节点对单链进行恶意攻击时，如图 4 所示，对自由链进行安全性分析。

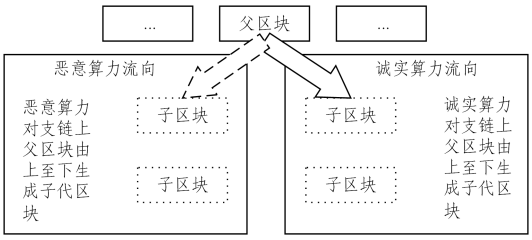


图 4 自由链攻击模式

Fig. 4 Free chain attack mode

赌徒扩展-F：在赌徒破产模型基础上，对链式结构中数学关联参数加以改进，求出自由竞争链间双花攻击安全性作用规律。设整个区块链模型的总算力为 1，恶意节点算力占比为 q，主链分流为 n 条子链，恶意节点和一条子链的诚实节点进行竞争，z 代表恶意节点追赶诚实节点 z 个区块的概率。此时被恶意节点攻击的诚实节点的算力为 $\frac{(1-q)}{n}$，所以恶意节点算力所占的比例 $q_1=\frac{q}{\left\{\frac{(1-q)}{n}+q\right\}}$，诚实节点算力所占的比例 $p_1=1-q_1$。

在赌徒扩展－F 策略中，求攻击者赶上诚实链条的概率，如式(1)所示：

$$\begin{cases} p(1)=q_1+p_1*p(2) \\ p(2)=p(1)^2 \\ p(z)=p(1)^z \end{cases} \xrightarrow{\text{解得}} p(1)=\frac{q}{n(1-q)} \tag{1}$$

恶意节点填补 z 个区块的成功概率如式(2)所示：

$$p(z)=\begin{cases} 1, & q_1\geqslant p_1 \\ \left(\frac{q_1}{p_1}\right)^z, & q_1<p_1 \end{cases} \tag{2}$$

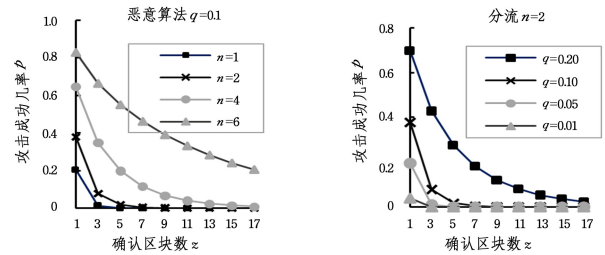
其中，$q_1=\frac{q}{\left\{q+\frac{(1-q)}{n}\right\}}$，$p_1=1-q_1$。采用转账确认追击模型，得到恶意节点攻击成功率如式(3)所示：

$$p=\sum_{k=0}^{k=+\infty}\frac{\lambda^k*e^{-\lambda}}{k!}*\begin{cases} 1, & q_1\geqslant p_1 \\ \left(\frac{q_1}{p_1}\right)^z, & q_1<p_1 \end{cases} \tag{3}$$

因为 $\lambda=\left(\frac{q_1}{p_1}\right)*z$，式(3)整理后得式(4)：

$$p=1-\sum_{k=0}^{k=z}\frac{\lambda^k*e^{-\lambda}}{k!}*\left(1-\left(\frac{q_1}{p_1}\right)^{z-k}\right) \tag{4}$$

自由链式结构函数关系描述如图 5 所示。图 5(a)中，链式结构的恶意算力占比为恒定的 0.1(即 10%)，得到两个变量 z 和 n 与恶意节点攻击成功概率 p 的关系。将诚实节点已确认的区块数 z 设置为 1,3,5,7,9,11,13,15,17，链中分叉数 n 设置为 1,2,4,6。当恶意算力 q 恒定时，每条函数线均向下递减，且上层函数线 p 总是高于下层函数线。图 5(b)中，设该链式结构分叉数恒定为 2，研究两个不同变量 q 和 z 与恶意节点攻击成功概率 p 的关系。将诚实节点已经确认的块数 z 设置为 1,3,5,7,9,11,13,15,17，该链式结构的恶意节点算力占比取 0.2,0.1,0.05,0.01，图中每条函数线向下递减，且上层函数线 p 总是高于下层函数线。



(a) q constant function (b) n constant function

图 5 自由链式结构函数关系中 q 和 n 常量关系函数

Fig. 5 q and n constant relation functions in the free chain structure function relation

综合分析，可得出如下规律：

(1)恶意算力占比 q、分叉数 n 不变，恶意节点攻击成功概率 p 随诚实链确认的区块 z 单调递减。

(2)算力占比 q、诚实链确认的区块 z 不变，恶意节点攻击成功概率 p 随分叉数 n 单调递增。

(3)分叉数 n、诚实链确认的区块 z 不变，恶意节点攻击成功概率 p 随恶意占比算力 q 单调递增。

结合推论，为保证区块链的安全可靠，可采取的措施是

减少区块链的分叉、增大诚实算力的占比，以及在交易中等待尽可能多的区块确认。

4.2 赌徒扩展-S

串行集中链式结构区块打包顺序为从左到右、从上到下，若脱离系统强制打包机制的恶意节点只针对某一条区块上的支链进行从上到下哈希计算，由于诚实节点算力集中在一整个层次区块上消耗，那么恶意攻击者会产生延迟优势。如图 6 所示，该情况下对子链进行安全性分析。

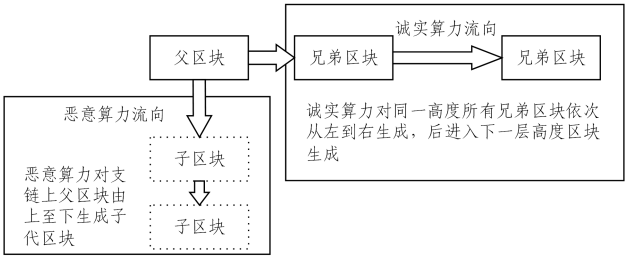


图 6 串行集中链攻击模式

Fig. 6 Serial centralized chain attack mode

赌徒扩展-S：在赌徒破产模型基础上，对链式结构中的数学关联参数进行设计和改进，求出串行集中链的双花攻击安全性作用规律。设区块链总算力为 1，恶意节点算力占比为 q，主链分流为 n 条子链，恶意节点和链上诚实节点竞争，z 代表恶意节点追赶诚实节点 z 个区块的概率。此时被恶意节点攻击的诚实节点的算力为 p，$p=1-q$，在赌徒扩展-S 策略中，恶意节点追击诚实节点区块的概率如式(5)所示：

$$\begin{cases} p(1)<p(1\text{ 真})=q+p*q+\cdots+p^{z-1}*q+p^{z}*p(2\text{ 真}) \\ p(2\text{ 真})<p(1)^2 \\ p(z\text{ 真})=p(1)^z \end{cases} \xrightarrow{\text{解得}} p(1\text{ 真})<p(1)<\frac{1-p^n}{p^n} \tag{5}$$

通过转账来确认追击模型的恶意节点以弥补 z 个区块的成功概率如式(6)所示：

$$p=\sum_{k=0}^{k=+\infty}\frac{\lambda^k*\mathrm{e}^{-\lambda}}{k!}*\begin{cases}1, & p^n\leqslant\frac{1}{2}\\ \left(\frac{1-p^n}{p^n}\right)^z, & p^n>\frac{1}{2}\end{cases} \tag{6}$$

其中，$\lambda=q*\frac{z}{p}$，$\left[\frac{(z+1-n)}{n}\right]^{\&}$ 表示取大于 $\left[\frac{(z+1-n)}{n}\right]$ 的最小整数。整理式(6)得到式(7)：

$$p=1-\sum_{k=0}^{k=\left[\frac{z+1-n}{n}\right]^{\&}}\frac{\lambda^k*\mathrm{e}^{-\lambda}}{k!}*\left(1-\left(\frac{1-p^n}{p^n}\right)^{\left[\frac{z+1-n}{n}\right]^{\&}-k}\right) \tag{7}$$

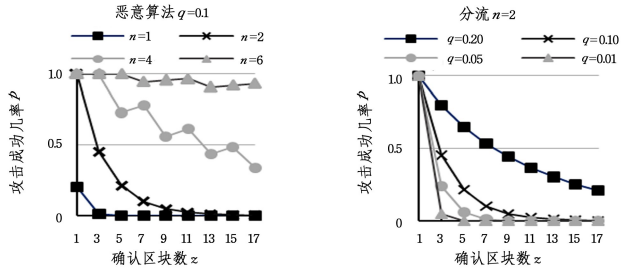
图 7 为串行集中链式结构中函数式关系图。由图 7(a)得，当恶意算力 q 恒定时，每条单独线条呈现出起伏的特征，且总体趋势为向下递减，处在上面的线条成功率 p 总是高于下层的线条。图 7(b)中，每条单独的线条均向下递减，且上面的线条成功概率 p 总是大于下层的线条成功概率。综合分析，得出如下规律：

(1)算力占比 q、分叉数 n 不变，引入两个自然数 t_1 和 t_2，设 $t_2>t_1$。即 z 处于 $[n*t_1, n-1+n*t_2]$ 区间的恶意节点攻击成功几率 p 小于 z 处于 $[n*t_2, n-1+n*t_2]$ 区间的恶意节点攻击成功几率 p。

(2)算力占比 q、诚实链确认的区块 z 不变，恶意节点攻击成功概率 p 随分叉数 n 单调递增。

(3)分叉数 n、诚实链确认的区块 z 不变，恶意节点攻击成功概率 p 随恶意占比算力 q 单调递增。

结合推论得到，链式结构的安全性与分叉子链数无关。为防止恶意攻击，可采取的措施是增大诚实算力占比以及在交易中等待尽可能多的区块确认。



(a) q constant function (b) n constant function

图 7 串行集中链式结构中 q 和 n 常量关系函数

Fig. 7 q and n constant relation function in serial centralized chain structure

4.3 模型安全性约束

双花攻击严重威胁区块链的数据安全，为验证本文提出的模型安全可靠，分别构建两种分支结构的安全性约束。

(1)自由竞争链安全性约束：自由链中，区块链双花攻击成功率与恶意算力占比、诚实区块确认数、自由链分叉数有关。实际上，少有恶意算力大于总算力 1%的节点(默认大型矿池是诚实节点)。如果算力占比不高于 1%的算力对区块链发起攻击，那么成功概率少于 1%的情况默认是安全状态，则确认区块数 z 与分叉子链数 n 安全性约束关系如图 8 所示。

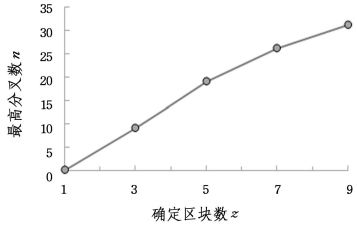


图 8 自由竞争链安全性约束

Fig. 8 Security constraints of free competition chain

图 8 中，随着确认区块数量的增加，链式结构最高分叉数单调增加。实际应用中，区块链分叉前应考虑分叉后子链数与确认区块数间的安全性约束。例如，区块链准备分叉为 5 条子链，为防止恶意双花攻击，则分叉后子链应等待至少两个区块确认后，才能确保该笔交易不被双花。

(2)串行集中链安全性约束：在少有恶意算力大于总算力 1%的节点情况下(默认大型矿池是诚实节点)，如果恶意节点算力在不高于 1%算力的情况下发起攻击，当成功概率少于 1%时默认为安全状态，节点的确认区块数 z 与链的分叉数 n 满足的关系如图 9 所示。图 9 中，随着确认区块数的增加，链式结构最高分叉数也线性增加。实际应用中，区块链应考虑

分叉后子链数与确认区块数之间的安全性约束。例如，当区块确认的区块数量不少于 5 时，为防止恶意双花攻击，串行集中链分叉数应不多于 2 条，才能确保该笔交易不会被双花。

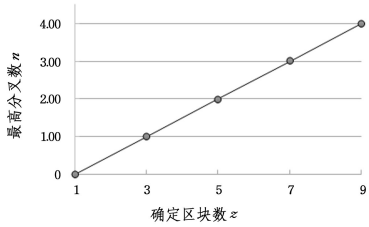


图 9 串行集中争链安全性约束

Fig. 9 Security constraints of serial centralized chain

5 实验分析

实验主要分为两方面：1)在模型性能方面，通过编程设计各模型内部运行机制，将本文提出的双分支结构扩展模型(简称 FDBC，包括自由竞争链式结构(简称 FDBC-F)和串行集中链式结构(简称 FDBC-S))与经典区块链模型隔离见证扩容(简称 SWE)机制以及 DAG 扩容机制)在存储速率(TPS)、有效数据率、确认延迟方面进行对比分析；2)在模型安全性方面，通过编程实现不同参数下的模拟攻击，对模型的安全性进行一致性验证。图 10 为实验设计方案。

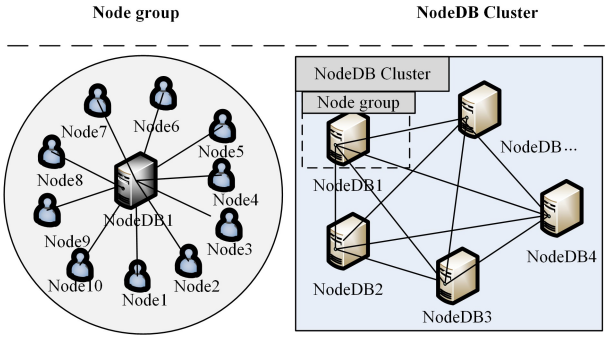


图 10 实验架构设计图

Fig. 10 Design diagram of experimental architecture

5.1 存储速率

在双分支链 TDBC 中，每个主体向全网广播区块创建信息，且通过对数据进行有效分流，将任务分配到各子链并行存储。实验在部署了 20 个主节点的环境中进行，以检测不同时期 3 种扩容机制下单位时间的数据吞吐量，实验结果如图 11 所示。

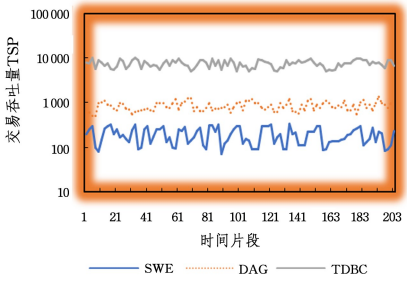


图 11 交易吞吐速率

Fig. 11 Transaction throughput rate

分析图 11 可得，由于 TDBC 中区块的并行高效创建，采用 TDBC 的区块链数据存储速率在高峰时交易达近万笔每秒，远高于 SWE 的百笔每秒和 DAG 的近千笔每秒，TDBC 在数据存储速率上的优势明显。

5.2 有效数据率

区块链中产生的交易信息经全网节点有效验证后即为有效数据。交易数据从产出到入链不可避免产生了数据损耗，如网络不稳定导致数据丢包，网络阻塞导致数据缓存被清除等。本实验分别部署了 5，10，20 个主体节点的区块链环境，通过在 3 种机制下入链的有效数据量占全部有效数据量的比值来反映有效数据率，结果如图 12 所示。

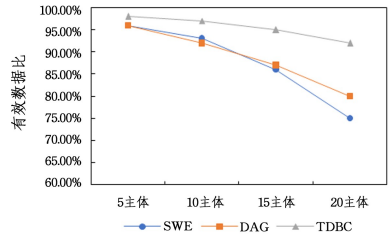


图 12 数据有效率

Fig. 12 Data efficiency

分析图 12 可知，TDBC 机制的数据有效率明显优于其他两种机制，且随着区块链网络的增大，其数据有效率始终比较稳定。DAG 机制的数据有效率优于 SWE 机制的数据有效率，SWE 机制的数据有效率在前期较高，随着区块链网络的扩展，数据有效性明显下降。

5.3 确定延迟

在区块链中，交易信息经有效性验证后写入区块体中，并得到全网其他节点验证的区块才能被确认，这个过程称为确认延迟。本实验为确定不同区块链网络规模对确定延迟的影响，分别部署了 5，10，20 个主体节点的实验环境，横坐标为不同时期，纵坐标为该阶段统计的确认时延范围，最终得到 3 种机制下区块的平均确认时延，如图 13 所示。

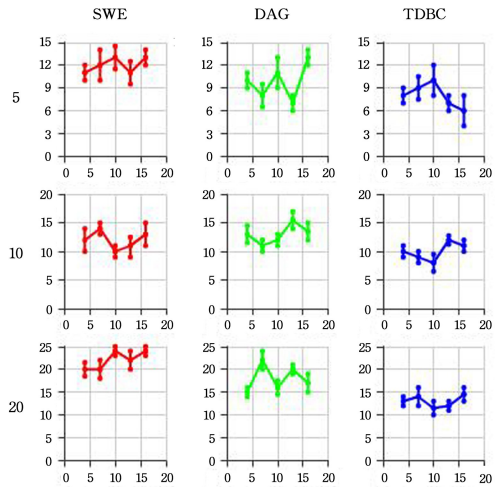


图 13 确定延迟

Fig. 13 Determine delay

分析图 13 可知，TDBC 的平均确定时延约为(8 s，10 s，13 s)，SWE 的平均确定时延约为(10 s，14 s，20 s)，DAG 的平均确定时延约为(9 s，12 s，16 s)，3 种区块链链式结构的区块确定延迟均稳定在一定范围内。经过分析可知，采用数据

分流的 TDBC 区块链确认延迟均小于其他两种机制，且随着网络规模的增大(通信主节点倍增)，采用 TDBC 机制的区块链确定延迟的增长幅度略小于 DAG 和 SWE 机制。

5.4 安全一致性评估

当恶意节点双花攻击双分支链时，模型通过诚实算力进行抵御，其中攻击的成功概率与恶意算力占比、区块确认数量以及分叉数量有关。本文对这些参数进行数学建模，得到理论数据预估值。之后在不同环境下对双分支链进行攻击，将攻击结果数据统计后转化得到如表 2 所列的实验数据集。

表 2 预估实验对比数据集

Table 2 Estimated experimental comparison datasets

		$(q=0.1\|n=8)$		$(q=0.2\|n=3)$		$(q=0.25\|n=2)$	
		$Z=2$	$Z=2$	$Z=2$	$Z=5$	$Z=1$	$Z=6$
FDBC-F	Theo	0.931	0.897	0.819	0.621	0.829	0.504
	Expe	0.905	0.883	0.808	0.512	0.911	0.551
FDBC-S	Theo	1.000	1.000	1.000	0.970	1.000	0.761
	Expe	1.000	1.000	1.000	0.950	1.000	0.714

可以看出，数据预估值和实验数据统计值在一定范围内波动，如 FDBC-F 在$(q=0.1,n=8)$，$(q=0.2,n=3)$条件下的理论实验数据组为{0.931，0.905}，{0.897，0.883}，{0.819，0.808}，{0.621，0.512}，数据组整体偏离较小，在有效波动范围内。实验分析结果展示了模型建模预估值和实验统计值不失真，验证了双分支结构扩展模型在模型安全性方面的一致性。

结束语 针对区块链在存储开销和数据吞吐率方面面临的可扩展性问题，本文构建了一种满足不同存储需求的双分支链模型，即自由竞争链式和串行集中链。通过主链分流拓展数据存储通道，显著提升数据吞吐率。此外，针对分流后子链安全问题，提出赌徒扩展-F 和赌徒扩展-S 策略。在此基础上，构建了双分支扩展模型的安全约束。实验结果表明，本文提出的双分支结构扩展模型能有效抵御恶意双花攻击，且在存储开销、数据吞吐率方面有很大优势。本文的研究工作基于 POW 共识机制，未来将研究将双分支扩展模型进一步拓展到其他主流共识机制的区块链中。

参 考 文 献

[1] KUZNETSOV A，LUTSENKO M，KUZNETSOVA K，et al. Statistical Testing of Blockchain Hash Algorithms[C]// CMiGIN. 2019：67-79.

[2] WANG J S，LI L L，YAN Y，et al. Security Incidents and Solutions of Blockchain Technology Application [J]. Computer Science，2018，45(6A)：352-355.

[3] NERURKAR P，PATEL D，BUSNEL Y，et al. Dissectingbitcoin blockchain：Empirical analysis of bitcoin network[J]. Journal of Network and Computer Applications，2021，177：102940.

[4] RAMAN R K，VARSHNEY L R. Distributed storage meets secret sharing on the blockchain[C]// 2018 Information Theory and Applications Workshop(ITA). IEEE，2018：1-6.

[5] BACH L M，MIHALJEVIC B，ZAGAR M. Comparative analysis of blockchain consensus algorithms[C]// 2018 41st International Convention on Information and Communication Technology，Electronics and Microelectronics (MIPRO). 2018：1545-1550.

[6] LEPORE C，CERIA M，VISCONTI A，et al. A survey on blockchain consensus with a performance comparison of PoW，PoS and pure PoS[J]. Mathematics，2020，8(10)：1782.

[7] XIE M，LIAO Z，HUANG L. Data Security Based on Blockchain Digital Currency[C]// 2020 3rd International Conference on Smart BlockChain(SmartBlock). IEEE，2020：5-10.

[8] SCHÄR F. Decentralized finance：On blockchain-and smart contract-based financial markets[J]. FRB of St. Louis Review，2021，103(2)：153-174.

[9] DIALLO E，DIB O，ZEMA N R，et al. When Proof-of-Work (PoW) based blockchain meets VANET environments[C]// 2021 12th International Conference on Information and Communication Systems(ICICS). IEEE，2021：336-343.

[10] ALDRIGHETTI A，CANAVARI M，HINGLEY M K. A Delphi Study on Blockchain Application to Food Traceability[J]. International Journal on Food System Dynamics，2021，12(1)：6-18.

[11] LIU Q，SONG B Y，JI W T，et al. Research on malicious attack model of blockchain multi-mining pools [J]. Journal of Frontiers of Computer Science & Technology，2021：1-11.

[12] YIU N C K. An Overview of Forks and Coordination in Blockchain Development[J]. arXiv：2102. 10006，2021.

[13] MIN X P，LI Q Z，KONG L J，et al. License chain multi-center dynamic consensus mechanism[J]. Chinese Journal of Computers，2018，41(5)：1005-1020.

[14] JIA D Y，XIN J C，WANG Z Q，et al. Blockchain storage capacity scalable model[J]. Journal of Frontiers of Computer Science & Technology，2018，12(4)：525-535.

[15] FADHIL M，OWENSON G，ADDA M. A bitcoin model for evaluation of clustering to improve propagation delay in bitcoin network[C]// 2016 IEEE International Conference on Computational Science and Engineering(CSE). IEEE，2016：468-475.

[16] MEI H，GAO Z，GUO Z，et al. Storage mechanism optimization in blockchain system based on residual number system[J]. IEEE Access，2019，7：114539-114546.

[17] WANG J L，LIU Q，SONG B Y. Research on the Optimization Model of Blockchain Hierarchical Proxy[J]. IEEE Access，2021，9：144327-144340.

WANG Junlu，born in 1988，Ph.D candidate，lecturer，is a member of China Computer Federation. His main research interests include large scale map processing techniques and big data processing techniques.

SONG Baoyan，born in 1965，Ph.D，professor，is a member of China Computer Federation. Her main research interests include large scale map processing techniques and big data processing techniques.

(责任编辑：何杨)