ISSN 1673-9418 CODEN JKYTA8
Journal of Frontiers of Computer Science and Technology
1673-9418/2018/12(04)-0525-11
doi: 10.3778/j.issn.1673-9418.1709032

E-mail: fcst@vip.163.com
http://www.ceaj.org
Tel: +86-10-89056056

区块链的存储容量可扩展模型*

贾大宇[1],信俊昌[1+],王之琼[2],郭 薇[3],王国仁[1]
1. 东北大学 计算机科学与工程学院,沈阳 110819
2. 东北大学 中荷生物医学与信息工程学院,沈阳 110819
3. 沈阳航空航天大学 计算机学院,沈阳 110136

Storage Capacity Scalable Model for Blockchain*

JIA Dayu[1], XIN Junchang[1+], WANG Zhiqiong[2], GUO Wei[3], WANG Guoren[1]
1. School of Computer Science and Engineering, Northeastern University, Shenyang 110819, China
2. School of Sino-Dutch Biomedical and Information Engineering, Northeastern University, Shenyang 110819, China
3. School of Computer, Shenyang Aerospace University, Shenyang 110136, China
+ Corresponding author: E-mail: xinjunchang@mail.neu.edu.cn

JIA Dayu, XIN Junchang, WANG Zhiqiong, et al. Storage capacity scalable model for blockchain. Journal of Frontiers of Computer Science and Technology, 2018, 12(4): 525-535.

Abstract: Nowadays, the maximum storage capacity of blockchain is limited to the node with the minimum storage capacity in the entire network. This paper presents a scalable model for storage capacity of blockchain, which fragments a blockchian replica and stores the fragments in a part of nodes. This model adds verification nodes to blockchian system. These nodes can detect and update the storage nodes stability by using the POR (proofs of retrievability) method in real time. Thus, the model records the stability values and chooses the high stability nodes to store the copies of the blocks. Finally, under the conditions of normal running, node failure and malicious attack on multiple nodes, the experimental results on real datasets show that the scalable model not only has stability, fault tolerance and safety, but also reduces the amount of storage space.

Key words: blockchains; storage scalability; data replication; verification nodes; proofs of retrievability

* The National Natural Science Foundation of China under Grant Nos. 61472069, 61402089, 61402298 (国家自然科学基金); the Fundamental Research Funds for the Central Universities of China under Grant No. 161602003 (中央高校基本科研业务费专项资金); the Natural Science Foundation of Liaoning Province under Grant No. 2015020553 (辽宁省自然科学基金).
Received 2017-07, Accepted 2017-09.
CNKI网络出版: 2017-09-28, http://kns.cnki.net/kcms/detail/11.5602.TP.20170928.1555.008.html

摘 要:目前区块链的容量受到网络里存储空间最小的节点的限制,提出了区块链存储容量可扩展模型,该模型将一条完整的区块链副本进行分片处理,并将分片数据保存在一定比例的节点中。同时,模型增加了验证节点,对存储数据的节点进行基于数据可检索性证明(proofs of retrievability,POR)方法的实时检测,并记录更新存储节点稳定性值,依此选择高稳定性节点来储存新产生的数据副本,提高了数据存储的稳定性。最后,模型在多节点中正常运行、节点故障和有恶意攻击时的实验表明,区块链存储容量可扩展模型在具有稳定性、容错性和安全性的同时,有效地增加了区块链的存储扩展性。

关键词:区块链;储存扩展性;数据副本;验证节点;可检索性证明

文献标志码:A **中图分类号:**TP311

1 引言

区块链技术随着比特币等数字加密货币的日益普及而越来越受关注。区块链技术是一种新型的去中心化协议,能安全存储数字货币、股权债权等数字资产。区块链技术通过运用数据加密[1]、时间戳、分布式共识[2]和经济激励等手段,有效地解决了拜占庭将军问题[3]中的共识问题,实现了在节点无需互相信任的分布式系统中去中心化的点对点交易,从而有效降低了现实经济的信任成本,重新定义了互联网时代的产权制度。

虽然区块链技术显著提高了数据的安全性与可靠性,但是目前区块链技术的储存扩展性较差。以比特币为例,截至2017年5月8日,共产生465 402个区块,总容量为107.89 GB,链上已认证地址9 892 723个[4]。因为区块链技术要求比特币的网络中每个完全节点都保存着完整的区块链信息,所以目前有近1 000万个节点贡献了100 GB以上的磁盘空间来储存区块链数据。也就是说,目前的比特币系统用了近1 000 PB的存储空间仅保存了100 GB左右的数据,这极大地浪费了存储空间。并且比特币的容量和参与的节点数量会随着时间的推移迅猛增加,区块链技术就会越来越多地占用海量节点的大量存储空间。这也极大地限制了以区块链技术为基础的数据库系统的发展与应用。

为了增加区块链技术的储存扩展性,本文提出了一种区块链存储容量可扩展模型,并采用一种数据副本分配策略对模型进行了优化。

本文的主要贡献如下:

(1)提出了一种区块链存储容量可扩展模型。模型将区块链中各个区块保存在一定比例的节点中,而不是所有节点。同时,增加了节点可靠性验证,在保证数据安全的同时,减少了区块链的储存空间。

(2)提出了一种区块链数据副本分配策略,对容量可扩展模型中副本数的计算过程进行了优化。

(3)通过实验证明,区块链存储容量可扩展模型具有一定的稳定性、容错性和安全性,同时减少了海量节点的大量存储空间,有效地增加了区块链的储存扩展性。

2 相关工作

区块链系统基于P2P技术[5]提供了一个只可以写入的全公开日志。参与区块链网络的节点都遵循POW(proof of work)协议[6],即工作量证明。协议通过运算,得出一个满足规则的随机数,最先计算出结果的节点即获得本次记账权,发出本轮需要记录的数据,全网其他节点验证后一起存储。存储框架如图1所示,网络中的每个节点都保存着完整的数据副本。

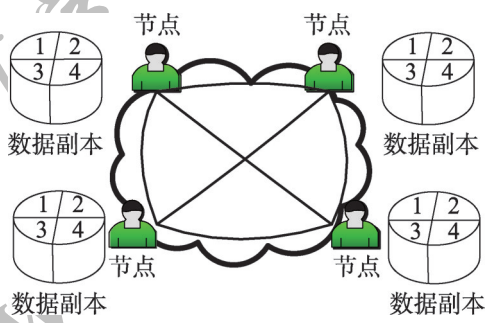


Fig.1 Storage framework of traditional blockchain

图1 传统区块链技术存储框架

近年来,学者对区块链进行了大量研究。Boyd

等人[7]提出了一种基于区块链的用户登录方法，使每个用户都可以公平地登录和使用服务器。Gervais等人[8]提出了一种框架来量化地分析区块链在各种共识和网络参数下的安全性。Herbert等人[9]提出了一种基于区块链技术的软件验证方法，改善了软件被盗版使用的问题。Karame[10]详细分析了比特币和其他基础区块链系统的安全性，并找出了其中潜在的安全隐患。Ali等人[11]提出了Blockstake命名存储系统，系统设计了四层架构，充分利用了区块链的去中心化特点，保证了数据的高安全性。King[12]和Bentov[13]等人实现了POS（proof of stake）权益证明机制，相对于POW机制，一定程度减少了数学运算带来的资源消耗，提升了区块链系统的性能。

3 区块链存储容量可扩展模型

本文利用分布式存储方法[14-15]，提出了区块链存储容量可扩展模型。其核心思想是将一条完整的区块链分成若干部分，分布存储在系统中，如图2所示。

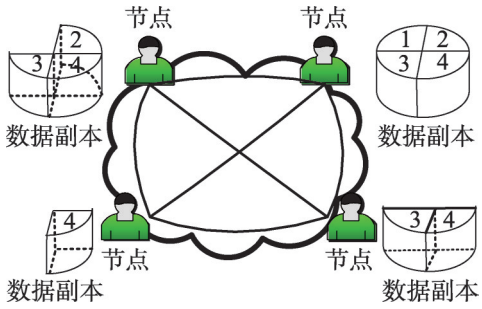


Fig.2 Storage framework of scalable model

图2 可扩展模型存储框架

在现有的区块链技术中，一个攻击者想要篡改数据，需要控制网络中50%以上的节点。在区块链分布式存储后，网络中区块链的副本数减少，攻击者就可以在控制少于50%节点数的情况下修改区块链数据，这在一定程度上降低了区块链的安全性。但是随着区块链技术的广泛应用，海量节点正源源不断地加入到区块链系统中。攻击者想要控制区块链系统中的很少一部分节点也几乎是不可能的。尽管如此，针对区块链容量可扩展模型还提出了节点可靠性验证的方法，增加了区块链的安全性。区块链存储容量可扩展模型框架如图3所示。

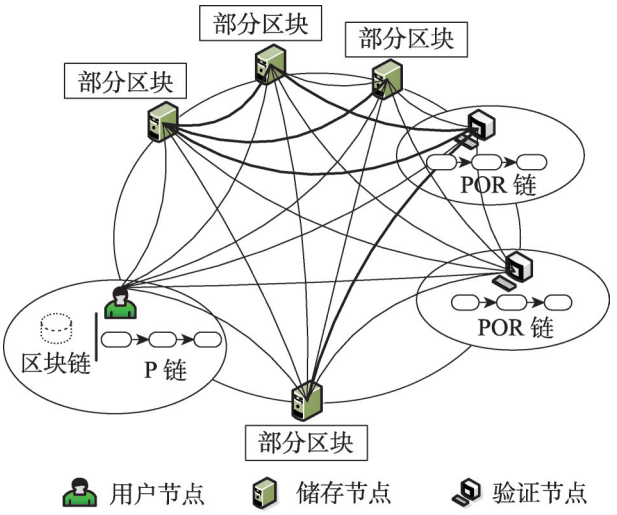


Fig.3 Scalable model for storage capacity of blockchain

图3 区块链存储容量可扩展模型

区块链存储容量可扩展模型中的节点包含3个角色：用户节点、储存节点和验证节点。用户节点是原始数据拥有者，储存节点是副本的保存者，而验证节点是储存节点稳定性的验证者。一个节点可以同时具备两种或者三种角色。同时，模型建立了两条新的区块链：P（position）链和POR（proofs of retrievability）链。P链保存在用户节点中，记录数据各个副本被保存在存储节点的位置。POR链保存在验证节点中，记录各个储存节点的可靠性评价。将储存节点位置信息和储存节点的可靠性评价写入基于区块链技术的P链和POR链中，也是利用了区块链不可被篡改的特点，保证数据的安全性。

3.1 数据存储

在区块链存储容量可扩展模型进行数据存储时，模型采用了POR数据可检索性证明[16-17]方法对用户节点区块链中的区块进行加密处理，得到相应的密文和密钥。POR方法是保存在外地服务器上数据的可检索性的加密证明。其实现的具体过程是：用户节点将密文交由储存节点保存后，可以随时查询储存节点中数据的完整性；储存节点会在被查询时，随机选择一部分密文数据发送给用户节点；用户节点通过密钥与接收密文的计算结果进行比对，得出储存节点中的数据是否完整。因此，利用POR方法可以在少量文件传输的通信成本下，实时验证出系统中数据的完整性。

在模型进行数据存储过程中，首先采用POR方法对用户节点中的每个区块进行加密，得到相应的密文和密钥。然后，用户节点计算出每个区块需要保存的副本数。接着，模型将POR方法生成的密钥保存到本地存储器中，并发给验证节点保存；将加密后的区块数据保存到储存节点中。此时，模型将访问验证节点中保存的储存节点可靠性信息，从中找出可靠值较高的储存节点来保存各个区块数据。验证节点为了保证储存节点可靠性信息不会被恶意篡改，将其保存在POR链中。之后，将每个区块按照所需要的副本数保存在相应数量的选出的储存节点中。当数据副本被保存后，为了保证用户节点进行数据读取，模型将储存节点的地址返回给用户节点，并将其保存在P链中，保证储存节点地址数据的安全性。

区块链存储容量可扩展模型的数据存储过程如图4、图5所示。

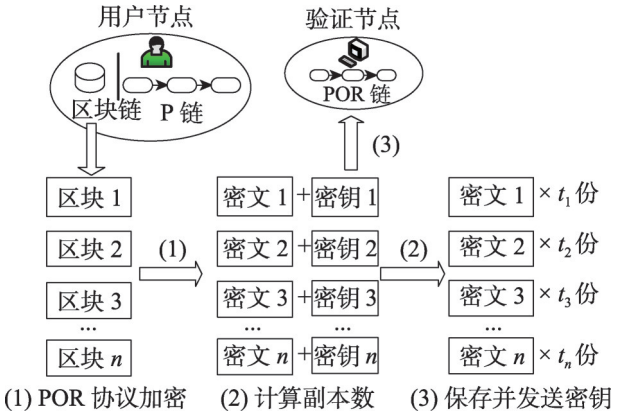


Fig.4 Step (1)~(3) of stored procedure

图4 存储过程步骤(1)~(3)

过程1 存储容量可扩展模型数据存储过程。

(1)采用POR方法对每个区块进行加密；

(2)用户节点计算出每个区块所需保存副本数；

(3)将POR方法生成的密钥保存到本地存储器中，并发给验证节点，保存到POR链中；

(4)用户节点向模型发送存储数据的请求；

(5)模型访问验证节点POR链中各个储存节点的可靠性信息，选出可靠性最高的作为本次操作的储存节点；

(6)将选出的储存节点返回给用户节点；

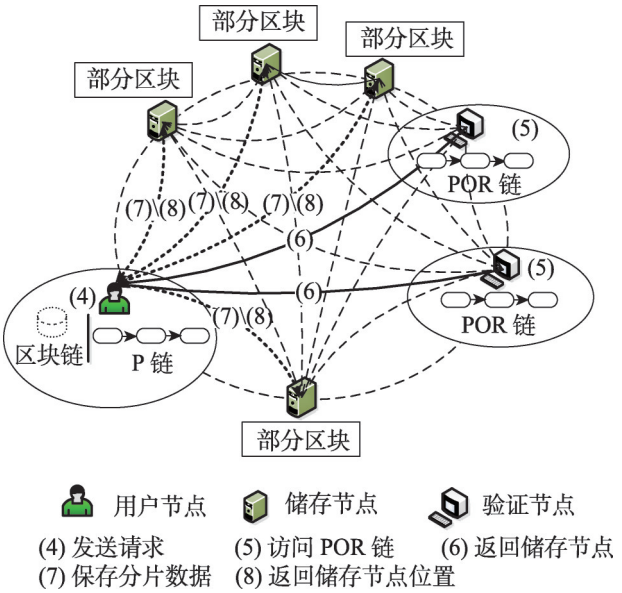


Fig.5 Step (4)~(8) of stored procedure

图5 存储过程步骤(4)~(8)

(7)用户节点按照所需要的副本数保存在相应数量的选出的储存节点中；

(8)将保存各个区块的储存节点的地址返回给用户节点，保存在P链里。

3.2 数据读取

在区块链存储容量可扩展模型进行数据读取时，首先用户节点访问本地磁盘中的P链，得到各个区块储存的位置信息，根据位置信息找到相应的储存节点。然后，储存节点将保存的数据返回给用户节点。用户节点根据本地保存的POR方法生成的密钥，对接收密文数据进行恢复，得到原始数据。

区块链存储容量可扩展模型的数据读取过程如图6所示。

过程2 存储容量可扩展模型数据读取过程。

(1)用户节点访问P链信息，找到保存每个区块的各个储存节点；

(2)储存节点将保存的数据返回给用户节点；

(3)用户节点根据完整返回的副本数据，利用本地保存的密钥对数据进行解密，恢复出原始数据。

3.3 储存节点可靠性验证

在区块链存储容量可扩展模型中，储存节点保存着区块数据。但是由于一些特殊状况，储存节点

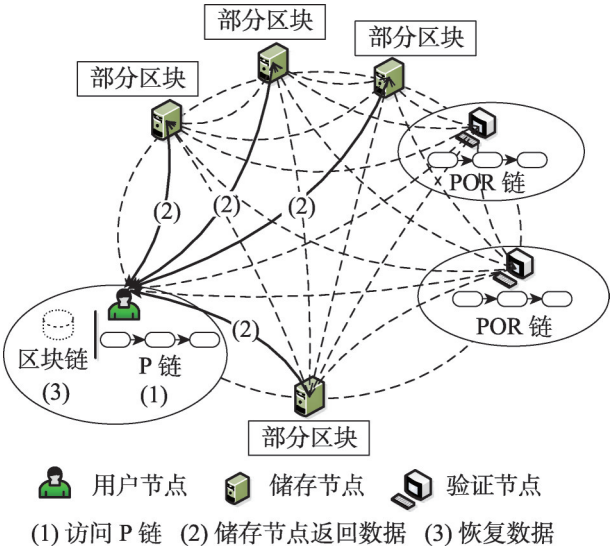


Fig.6 Data reading procedure

图6 数据读取过程

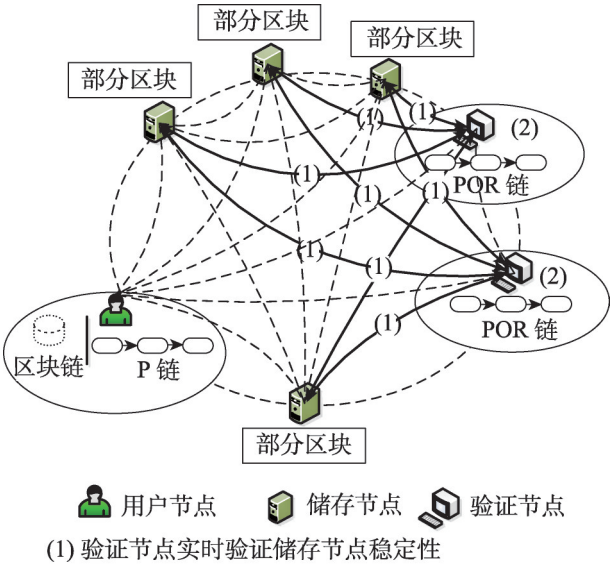


Fig.7 Reliability verification of storage nodes

图7 储存节点可靠性验证过程

可能出现将数据修改或将数据丢失等故障。为了减小由于储存节点故障导致的区块数据的不稳定性，验证节点会根据POR方法生成的密钥，随时验证存储节点随机发回的部分密文数据，实时检测储存节点数据存储情况。然后，验证节点将实时的检测情况写入POR链中，当用户节点再次申请储存数据时，提供最新的储存节点可靠性值，使用户节点选出此时最稳定的存储节点保存区块数据。

区块链存储容量可扩展模型中储存节点可靠性验证过程如图7所示。在实际应用中，模型对于储存节点可靠性的评价标准可以采取如下方法。首先，模型会给每个储存节点分配相同的可靠性值。然后，验证节点每隔相同的一段时间检测储存节点数据的可靠性，相隔时间根据对数据安全需求的具体情况来制定。当储存节点中数据完整时，其可靠性值不变。当储存节点数据被修改或者丢失时，则减少其可靠性值，并保存到POR链中。最后，当模型选择高可靠性的储存节点时，以POR链中的各个储存节点可靠性值作为衡量标准。

3.4 系统激励机制

在比特币的应用中，矿工通过计算得出下一个区块的哈希值。正是矿工们的大量计算，保证了比特币的安全性。因此，比特币系统会对每个挖矿成功者奖励一定数量的比特币。这也激励了成百上千的矿工消耗自身CPU的计算能力和大量电力去挖矿。而在区块链存储容量可扩展模型中，储存节点和验证节点提供了自己的大量磁盘空间，保证了用户节点的数据安全。本文对于储存节点和验证节点也提出一种激励机制，可以令他们自身作为用户节点，在模型中安全存储一定空间的数据。

4 数据副本分配策略

在区块链存储容量可扩展模型的数据存储过程的第二个步骤中，用户节点首先计算每个区块保存的副本数。但区块链的每个新区块都是在上一个区块基础上计算来的，不同的区块安全性不同。因此，本文根据每个区块的安全性，提出了一种区块链的数据副本分配策略，优化了模型的存储过程。

数据副本分配策略，首先根据系统节点总数得出保存每个区块的最少副本数。然后根据系统安全性需求，确定出一定数量连续的区块保存相同的副本数。最后根据区块链的难度设定，计算出每个区块需要保存的副本数。

区块链技术的创始人Nakamoto[18]在论文中假设了一个双重支付的攻击场景，攻击者试图比诚实节点更快地产生一条平行链条代替区块链。攻击者是

否能够成功赶超诚实链，可以近似地看成赌徒破产问题。此时，假设 p 为诚实节点制造出下一节点的概率，q 为攻击节点制造出下一节点的概率，那么攻击者在区块增加了第 z 块时，攻击者取得的进展服从泊松分布，分布期望为：

$$\lambda = z \times \frac{q}{p} \tag{1}$$

追赶上诚实链条的概率 P_z 为：

$$P_z = \sum_{k=0}^{\infty} \frac{\lambda^k e^{-\lambda}}{k!} \times \begin{cases} \left(\frac{q}{p}\right)^{(z-k)}, & \text{if } k \leqslant z \\ 1, & \text{if } k > z \end{cases} \tag{2}$$

为了避免对无限数列求和，将式(2)转换为：

$$P_z = 1 - \sum_{k=0}^{z} \frac{\lambda^k e^{-\lambda}}{k!} \times \left(1 - \left(\frac{q}{p}\right)^{(z-k)}\right) \tag{3}$$

本文利用Java编写代码，计算出在 $q=0.1$ 时，z 取0到30概率 P_z 的大小。并用Matlab将函数 $f(z,P_z)$ 画出图像，如图8所示。

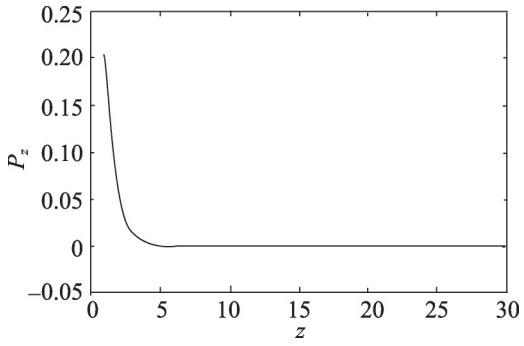


Fig.8 Image of $f(z, P_z)$

图8 函数 $f(z,P_z)$ 图像

由于随着 z 的增加，P_z 减小速率很快，当 z 取值较大时，图8不能明显表示出 P_z 的值。因此，当 z 取10到15时，画出了 $f(z, P_z)$ 的图像，如图9所示。

可以看出，随着区块的增加，攻击者越来越难赶超诚实链。越原始的区块中数据被篡改的可能性就越低，安全性也就越高。因此，在数据副本分配策略中，每个区块的副本数由区块所在位置决定，将区块链中较原始的区块保存少量份数，而较新的区块保存足够多的份数，二者函数关系如式(4)所示。设 M 为区块链中节点总数，i 为区块链中区块的编号，n

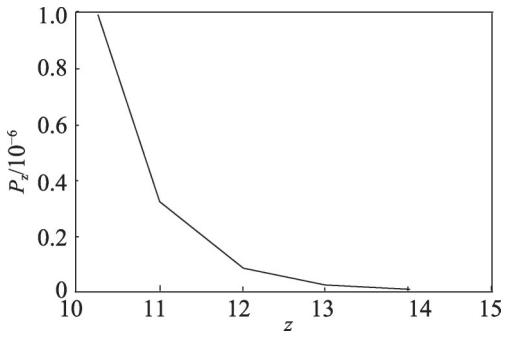


Fig.9 Image of $f(z, P_z)$ when z is selected from 10 to 15

图9 当 z 取10到15时函数 $f(z,P_z)$ 图像

为区块链目前的总区块数，m_i 为区块 i 需要保存的份数，P_{n-i} 为第 i 个区块被攻击者追赶上的概率，也可以看作为第 i 个区块的安全性系数。

$$m_i = \lceil P_{n-i} \times M \rceil \tag{4}$$

但是，在区块链机制中，如果50%以上节点保存了相同的数据，则这个数据被视作真实数据。从而，控制了网络中一半数量以上的节点，就会控制整个网络的数据。因此，也不能令每个区块的副本数特别小，而是要根据不同区块链系统安全性需要，规定出每个区块保存的最小副本数 k。

同时，Borel定律[19]定义了任何低于 $1/10^{50}$ 的概率都是不可能的。因此，根据式(3)可以计算出，当 z 增加到一定数值时，P_z 的概率会达到 10^{-50} 以下。此时，攻击节点想要赶上诚实节点变为不可能事件。因此，将每 z 个区块作为一组数据分片，保存相同的副本数量。

最后，得出每个区块的副本数。每 $z_{\min}$ 个区块被分割成一个分片，第 i 个分片保存 m_i 份副本，但副本数最小为 k。

因此，数据副本分配策略过程如下所示。

过程3 数据副本分配策略过程。

(1)根据区块链网络的计算能力，预估出攻击节点制造出下一节点的概率 q；

(2)将 q 带入式(3)，计算当 $P_z \leqslant 10^{-50}$ 时，z 的最小取值 $z_{\min}$；

(3)根据区块链的用户总量和区块总数，确定出在保证数据安全前提下，每个区块保存副本数的最小值 k；

(4)将区块链中节点总数 M 和区块链目前的区块数 n 带入式(4)，计算出每个位置的分片保存的副本数 m_i；

(5)对完整的区块链进行分片处理，每 $z_{\min}$ 个区块被分割成一个分片，第 i 个分片保存 m_i 份副本，当 $m_i<k$ 时，将 m_i 取值为 k。

此处，本文给出了当 $q=0.1$ 时，数据副本分配策略中每个区块的副本数。

首先，根据式(3)进行计算，为了简化分组过程，z 的取值为10的整数倍。当 $z\geqslant 100$ 时，P 的概率已达到 10^{-50} 以下。因此，将每100个区块作为一组数据分片，保存相同的副本数量。

然后，利用式(4)计算每组分片保存的副本数。此时，为了方便计算，对式(3)的计算结果利用Matlab对函数 $f(z,P_z)$ 做了weibull拟合，拟合结果为式(5)。

$$f(x)=a*b*x\hat{}(b-1)*\exp(-a*x\hat{}b) \tag{5}$$

其中，$a=1.905\,(1.886,\ 1.924)$，$b=0.723\,(0.715\,4,\ 0.730\,7)$，拟合方差(SSE)为1.215E−05，确定系数(R-square)为0.999 7。

从拟合结果可以看出，z 与 P_z 呈负指数关系。因此，为了简化分片过程，将式(3)化简为式(6)来计算分片保存副本数，分片结果如图10所示。

$$m=2^{-\left\lfloor\frac{n-i}{100}\right\rfloor}\times M \tag{6}$$

当 n 增加时，每新增100个区块组成一个分片，该分片由此时全网中所有节点保存。而对于之前分片的副本数，由式(6)根据此时网络中的节点总数重新计算。如果在新增100个区块的时间里，全网的节点数激增，计算出的所需副本数比网络中已存副本数多，则将之前分片副本数增加至式(6)计算数量；如果网络中已存副本数比计算出的所需副本数量大，则可以令部分存储节点释放其储存空间，但保证网络中已存副本量大于等于所需副本数量。

区块链存储容量可扩展模型利用此副本分配策略会在保证数据可靠性和安全性的前提下，增加区块链的存储容量。

假设：当可扩展模型采用基于式(6)的副本分配策略进行数据存储时，模型中共有节点数 M，其中存在不稳定节点数量为 $d(d\leqslant M)$，不稳定节点会有 $e(e\leqslant 1)$ 的概率出现数据丢失情况。则新产生的区块分片保存副本数 $m_{n/100}=M$，每一个分片的副本数 m_j 为式(7)所示，j 为分片序号。

$$m_j=\begin{cases}\dfrac{M}{2^{j-1}}, & \text{if } \dfrac{M}{2^{j-1}}\geqslant k\\ k, & \text{if } \dfrac{M}{2^{j-1}}<k\end{cases},\ j=1,2,\cdots,\frac{n}{100} \tag{7}$$

此时，当所有不稳定节点第一次出现数据丢失时，数据可以被完全恢复的概率为：

$$P_r=1-\sum_{j=1}^{\frac{n}{100}}\frac{C_d^{m_j}}{C_M^{m_j}}\times m_j^{\,e} \tag{8}$$

在式(8)中要求：

(1)当 $d<m_j$ 时，停止求和计算。因为当 $d<m_j$ 时，不稳定节点数量小于保存副本数，不存在数据丢失的情况。

(2)当 $d<k$ 时，数据可以被完全恢复的概率为100%，不用式(8)计算。因为当 $d<k$ 时，不稳定节点数量小于每个区块保存副本数的最少值，不可能出现数据丢失的情况。

当不稳定节点出现多次数据丢失时，由于在区块链存储容量可扩展模型的POR链中记录了每次的数据丢失情况，并每次将该节点的可靠性值随即减少。可靠值被减少后，不稳定节点被选作储存节点的概率就会降低。数据会被保存在较稳定的节点中，可以被恢复的概率就会提高。

Fig.10 Allocation scheme of copies

图10 区块副本数分配方案

5 实验结果

实验的开发环境为Intel Core i5-6500 3.20 GHz CPU和16 GB内存的PC机上。利用VMware Workstation 12.5.2建立了16个节点，每个节点为内存1 GB，硬盘大小为60 GB的ubuntu16.04系统。借助IBM开发的开源Hyperledge Fabric v0.6版本，构建起P链和POR链区块链项目。

首先，测试基于区块链存储容量可扩展模型系统的稳定性。实验分别建立了4个、8个、12个和16个节点，所有节点均为储存节点，且其中3个节点同时为用户节点和验证节点。实验运行调用chaincode_example02.go交易代码，每完成一次交易，生成5.39 KB的广播消息。

在所有节点都正常运行且不被攻击的情况下，在数据分片时，以500 KB为一个组进行分片，每个分片的最小副本数为2份，副本数与分片位置的函数根据式(4)计算得出。当实验完成交易186次、930次和1 860次，生成广播数据1 MB、5 MB和10 MB时，区块链容量可扩展模型与基于Hyperledge Fabric v0.6的区块链系统中所有节点储存总容量如图11所示。

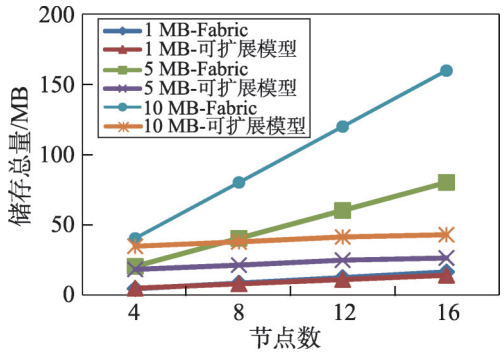


Fig.11 Storage space occupied by scalable model and Hyperledge Fabric

图11 可扩展模型与Hyperledge Fabric占用的存储空间

通过分析图11的实验结果，可以得到以下结论。

(1)在节点数较少的情况下，存储容量可扩展模型所有节点储存总量与Fabric区块链相比相差不大。但当节点数增多时，容量可扩展模型所占用的存储空间与Fabric区块链系统相比明显减少。

(2)当存储数据量较小时，存储容量可扩展模型所有节点储存总量与Fabric区块链相比相差不大。这是由于储存容量可扩展模型在存储交易数据的同时，在P链中保存了储存节点位置信息，在POR链中保存了储存节点的可靠性评价信息。并且在P链与POR链中的每条数据大小都为固定值，因此当存储数据量不断增加时，容量可扩展模型所占用的存储空间与Fabric区块链系统相比明显减少。

(3)当存储数据量不断增加时，区块链容量可扩展模型所需的储存空间的增量趋于平缓。

因此，容量可扩展模型在多节点、大数据的应用上，具有良好的存储扩展性。

同时，区块链存储容量可扩展模型与Fabric区块链系统的处理时间如图12和图13所示。容量可扩展模型的处理时间要略多于Fabric区块链系统，且随

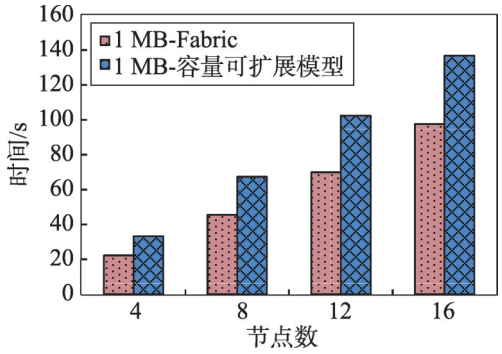


Fig.12 Time to process 1 MB data by scalable model and Hyperledge Fabric

图12 可扩展模型与Hyperledge Fabric处理1 MB数据时间

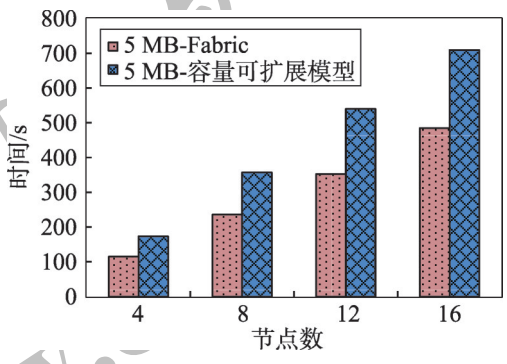


Fig.13 Time to process 5 MB data by scalable model and Hyperledge Fabric

图13 可扩展模型与Hyperledge Fabric处理5 MB数据时间

着节点数量和存储数据大小增加，可扩展模型的处理时间基本呈线性增加。

然后，测试系统的容错性。假设在8个、12个和16个储存节点中存在不稳定节点，不稳定节点会丢失本地的部分储存数据。为了符合实际应用情况，实验设置了4个不稳定节点，且这4个不稳定节点均不是验证节点，它们出现不稳定概率分别为0.8、0.6、0.4和0.2。当实验完成交易930次，得到数据5 MB，分片方法与上个实验相同时，区块链容量可扩展模型、仅基于数据副本分配策略的区块链系统与基于Hyperledge Fabric v0.6的区块链系统各自恢复的数据总量的百分比如图14所示。

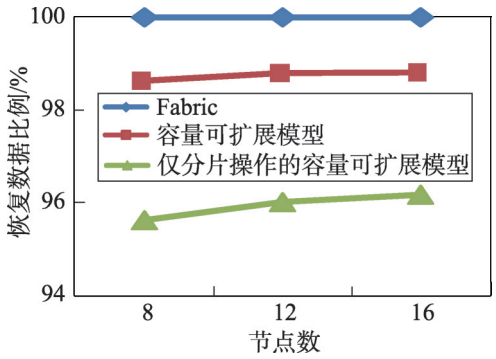


Fig.14 Fault tolerance of scalable model

图14 可扩展模型容错性测试

当不稳定节点出现时，Fabric基本不受影响，仅基于数据副本分配策略的区块链系统受影响最大，区块链容量可扩展模型所受影响较小。这是由于容量可扩展模型和仅基于数据副本分配策略的区块链系统相比，利用POR链中对各个节点的可靠性评价，选出了稳定性更好的节点存储数据。并且从实验中可以看出，当节点数增加，也就是系统中副本数增加时，容量可扩展模型数据恢复比例有所增加，系统的容错性增强。

最后，测试区块链容量可扩展模型的安全性。本文借助了Blockbench[20]对区块链安全测试方法：当有攻击者故意修改储存节点中的存储数据时，区块链会产生分叉，此时系统的安全性可以根据分叉链产生的区块数量来判断，区块数量越少，系统越安全。在实验中，建立了16个节点，运行Hyperledge Fabric与区块链容量可扩展模型，攻击出现在系统运行第100秒，在第250秒时结束。两个系统正常运行和被攻击时的实验结果如图15所示。

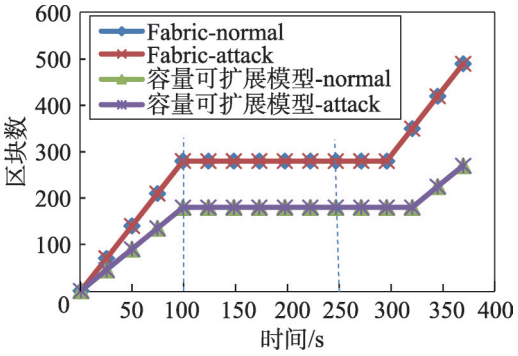


Fig.15 Security of scalable model

图15 可扩展模型安全性测试

从实验中可以看出，Hyperledge Fabric和区块链存储容量可扩展模型被攻击时，并没有产生分叉链，这是因为实验中容量可扩展模型也是基于Hyperledger Fabric技术构建的。Hyperledger的一致性协议保证了区块的安全性，让被攻击的链不产生分叉。但是在攻击停止后，Hyperledger和容量可扩展模型都用了一段时间才从攻击中恢复，并且容量可扩展模型比Hyperledger需要的恢复时间更长。

通过实验证明，基于Hyperledger Fabric的区块链存储容量可扩展模型在被攻击时，虽然需要更多的处理时间，但具有良好的安全性。

6 结束语

区块链的协议要求全网中每个节点都保存着同一条完整的区块链信息，这导致了区块链的容量受到网络里存储空间最小的节点的限制。本文提出了一个区块链存储容量可扩展模型。模型将区块链中各个区块保存在一定比例的节点中，而不是所有节点中。并且模型增加了节点可靠性验证，保证了数据的安全性。模型中用户节点根据数据副本分配策略将每个区块保存相应的副本数，并基于POR数据可检索性证明方法对副本数据进行加密，并将密钥发送个验证节点。验证节点利用POR方法实时更新储存节点的稳定性值，依此选择高稳定性节点来储

存用户节点的数据副本。最后,经实验证明,区块链存储容量可扩展模型在具有一定的稳定性、容错性和安全性的同时,有效地增加了区块链的储存扩展性。

未来可以进一步研究数据副本分配策略,提出更准确的计算数据副本方法,在保证数据安全性的前提下,减少更多储存空间。同时,也可以将区块链存储容量可扩展模型应用于Ethereum和Parity等不同的区块链系统中,提高不同区块链系统的存储扩展性。

References:

[1] Bonneau J, Miller A, Clark J, et al. SoK: research perspectives and challenges for Bitcoin and cryptocurrencies[C]// Proceedings of the 2015 IEEE Symposium on Security and Privacy, San Jose, May 17-21, 2015. Washington: IEEE Computer Society, 2015: 104-121.

[2] Yuan Yong, Wang Feiyue. Blockchain: the state of the art and future trends[J]. Acta Automatica Sinica, 2016, 42(4): 481-494.

[3] Eyal I, Gencer A E, Sirer E G, et al. Bitcoin-NG: a scalable blockchain protocol[C]//Proceedings of the 13th USENIX Symposium on Networked Systems Design and Implementation, Santa Clara, Mar 16-18, 2016. Berkeley: USENIX Association, 2016: 45-59.

[4] Blockmeta. The blockchain data of Bitcion[EB/OL]. [2017-05-07]. https://blockmeta.com/btc-stat.

[5] Amalarethinam D I G, Balakrishnan C, Charles A. An improved methodology for fragment re-allocation in peer-to-peer distributed databases[C]//Proceedings of the 4th International Conference on Advances in Recent Technologies in Communication and Computing, Bangalore, Oct 19-20, 2012. Piscataway: IEEE, 2012: 78-81.

[6] Li Jingrui, Wolf T. A one-way proof-of-work protocol to protect controllers in software-defined networks[C]//Proceedings of the 2016 Symposium on Architectures for Networking and Communications Systems, Santa Clara, Mar 17-18, 2016. New York: ACM, 2016: 123-124.

[7] Boyd C, Carr C. Fair client puzzles from the Bitcoin blockchain[C]//LNCS 9722: Proceedings of the 21st Australasian Conference on Information Security and Privacy, Melbourne, Jul 4-6, 2016. Berlin, Heidelberg: Springer, 2016: 161-177.

[8] Gervais A, Karame G O, Wüst K, et al. On the security and performance of proof of work blockchains[C]//Proceedings of the 2016 ACM SIGSAC Conference on Computer and Communications Security, Vienna, Oct 24-28, 2016. New York: ACM, 2016: 3-16.

[9] Herbert J, Litchfield A. A novel method for decentralised peer-to-peer software license validation using cryptocurrency blockchain technology[C]//Proceedings of the 38th Australasian Computer Science Conference, Jan 27-30, 2015. Sydney: Australian Computer Society, 2015: 27-35.

[10] Karame G. On the security and scalability of Bitcoin's blockchain[C]//Proceedings of the 2016 ACM SIGSAC Conference on Computer and Communications Security, Vienna, Oct 24-28, 2016. New York: ACM, 2016: 1861-1862.

[11] Ali M, Nelson J C, Shea R, et al. Blockstack: a global naming and storage system secured by blockchains[C]//Proceedings of the 2016 USENIX Annual Technical Conference, Jun 22-24, 2016. Berkeley: USENIX Association, 2016: 181-194.

[12] King S, Nadal S. PPCoin: peer-to-peer crypto-currency with proof-of-stake[EB/OL]. [2017-04-02]. http://www.peercoin.net/bin/peercoinpaper.pdf.

[13] Bentov I, Lee C, Mizrahi A, et al. Proof of activity: extending Bitcoin's proof of work via proof of stake[J/OL]. Cryptology ePrint Archive, 2014: 452.

[14] Tung Y C, Lin K C J, Chou F C. Bandwidth-aware replica placement for peer-to-peer storage systems[C]//Proceedings of the 2011 Global Communications Conference, Houston, Dec 5-9, 2011. Piscataway: IEEE, 2011: 1-5.

[15] Ng W S, Ooi B C, Tan K L, et al. PeerDB: a P2P-based system for distributed data sharing[C]//Proceedings of the 19th International Conference on Data Engineering, Bangalore, Mar 5-8, 2003. Washington: IEEE Computer Society, 2003: 633-644.

[16] Juels A, Kaliski B S. PORs: proofs of retrievability for large files[C]//Proceedings of the 2007 ACM Conference on Computer and Communications Security, Alexandria, Oct 28-31, 2007. New York: ACM, 2007: 584-597.

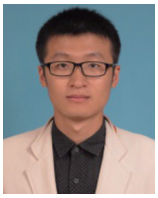
[17] Armknecht F, Bohli J M, Karame G O, et al. Outsourced proofs of retrievability[C]//Proceedings of the 2014 ACM SIGSAC Conference on Computer and Communications Security, Scottsdale, Nov 3-7, 2014. New York: ACM, 2014: 831-843.

[18] Nakamoto S. Bitcoin: a peer-to-peer electronic cash system

[EB/OL]. [2017-05-07]. http://www.bitcoin.org/bitcoin.pdf.
[19] Borel E. Probabilities and life[M]. New York: Dover Publications Inc, 1962.
[20] Dinh T T A, Wang Ji, Chen Gang, et al. BLOCKBENCH: a framework for analyzing private blockchains[C]//Proceedings of the 2017 ACM International Conference on Management of Data, Chicago, May 14-19, 2017. New York: ACM, 2017: 1085-1100.

附中文参考文献:

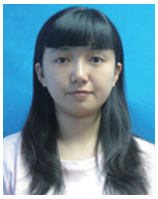
[2] 袁勇, 王飞跃. 区块链技术发展现状与展望[J]. 自动化学报, 2016, 42(4): 481-494.



JIA Dayu was born in 1990. He is a Ph.D. candidate at Northeastern University. His research interests include distributed systems and big data management, etc.
贾大宇(1990—),男,辽宁沈阳人,东北大学博士研究生,主要研究领域为分布式系统,大数据管理等。

XIN Junchang was born in 1977. He received the M.S. and Ph.D. degrees in computer science and technology from Northeastern University in 2005 and 2008 respectively. Now he is a full professor at School of Computer Science and Engineering, Northeastern University, and the member of CCF. His research interests include big data management, sensory data management, uncertain data management, cloud computing and machine learning, etc.
信俊昌(1977—),男,辽宁辽阳人,2005年和2008年于东北大学分别获得硕士和博士学位,现为东北大学计算机科学与工程学院教授,CCF会员,主要研究领域为大数据管理,感知数据管理,不确定数据管理,云计算,机器学习等。

WANG Zhiqiong was born in 1980. She received the Ph.D. degree in computer software and theory from Northeastern University in 2014. Now she is an associate professor and M.S. supervisor at Northeastern University. Her research interests include data processing, computer image processing and big data analytics, etc.
王之琼(1980—),女,黑龙江哈尔滨人,2014年于东北大学计算机软件与理论专业获得博士学位,现为东北大学副教授、硕士生导师,主要研究领域为数据处理,计算机图像处理,大数据分析等。发表学术论文40余篇,作为负责人承担了国家自然科学基金、辽宁省自然科学基金和中国博士后科学基金等课题5项。



GUO Wei was born in 1983. She received the Ph.D. degree from Northeastern University in 2012. Now she is an associate professor at Shenyang Aerospace University. Her research interests include medical image processing, pattern recognition, computer-aided diagnosis and big data management, etc.
郭薇(1983—),女,辽宁沈阳人,2012年于东北大学获得博士学位,现为沈阳航空航天大学副教授,主要研究领域为医学图像处理,模式识别,计算机辅助诊断,大数据管理等。

WANG Guoren was born in 1966. He received the M.S. and Ph.D. degrees from Northeastern University in 1991 and 1996 respectively. Now he is a full professor and Ph.D. supervisor at School of Computer Science and Engineering, Northeastern University, and the member of CCF. His research interests include cloud computing, XML data management, data stream analysis, high-dimensional indexing and P2P data management, et al.
王国仁(1966—),男,湖北崇阳人,1991年和1996年于东北大学分别获得硕士和博士学位,现为东北大学计算机科学与工程学院教授、博士生导师,CCF会员,主要研究领域为云计算,XML数据管理,数据流分析,高维索引,P2P数据管理等。