一种具有主从区块的区块链架构

谭朋柳，万里旭冉
（南昌航空大学软件学院，江西 南昌 330063）

摘　要：随着区块链技术的不断发展，不同的适应场景衍生出不同的链，每种链都各具特色，如比特币、以太坊等公有链、大量的私有链和联盟链。但就目前互联网的发展情况而言，许多应用场景在传统单链结构的区块链上的实现变得尤为不便。提出了一种具有主从区块（MSBC, master-slave blockchain）的区块链架构，主要由主区块、从属主块和从属微块三部分组成，主链由主区块组成，每一个主区块的侧链上都有一个从属主块和多个从属微块。另外，主区块与主区块之间直接通过前块哈希相连，主区块与从属主块之间通过唯一信息的哈希值连接，而从属微块与前一块（无论从属主块或从属微块）之间也通过前块哈希进行连接。这种结构可以将人才链中固定不变的简历信息放在主链上，而将不断更新的简历信息放在侧链上。MSBC 架构可扩展性更强，并且可以提高数据的查询效率。实验结果验证了此架构可以提高人才链等类似应用中的可行性以及查询效率。

关键词：区块链；主从区块；侧链
中图分类号：TP393
文献标识码：A
doi: 10.11959/j.issn.2096−3750.2021.00219

A blockchain architecture with master-slave blockchain

TAN Pengliu, WAN Lixuran
School of Software, Nanchang Hangkong University, Nanchang 330063, China

Abstract: With the continuous development of blockchain technology, different chains are derived due to different adaptation scenarios. Each chain has its own characteristics, such as public chains like bitcoin and ethereum, a large number of private chains and alliance chains. But as far as the current Internet is concerned, the implementation of many application scenarios on traditional blockchains has become particularly inconvenient. A master-slave blockchain (MSBC) architecture was proposed, which was mainly composed of a master block, a subordinate master block and a subordinate micro block. The master chain was composed of master blocks. Each master block has a slave master block and multiple slave micro block on its side chain. In addition, the master block and the master block were directly connected by the Hash of the previous block, the master block and the slave master block were connected by the Hash of the unique information, and the slave micro block and the previous block (whatever the slave master block or the slave micro block) was also connected by the Hash of the previous block. In talent chain, this kind of structure could put a person's fixed resume information on the master chain, but updated resume information constantly on the slave side chain. MSBC architecture was more scalable, and it could improve the efficiency of data query. The experimental results show that the framework in the similar applications such as talent chain is feasible and the query efficiency has been improved greatly.

Key words: blockchain, master-slave block, side chain

收稿日期：2020−08−28；**修回日期**：2021−01−25
通信作者：谭朋柳，pltan@nchu.edu.cn
基金项目：国家自然科学基金资助项目（No.61961029）；江西省科技厅重点研发计划项目（No.20171ACE50025）
Foundation Items: The National Natural Science Foundation of China (No.61961029), The Key Research and Development Plan in Jiangxi Province Department of Science and Technology (No.20171ACE50025)

1　引言

近几年，随着比特币技术的不断发展，区块链作为比特币底层很重要的一种技术，也逐渐成为人们关注的重点。同时，也引起了市场、各大机构的广泛关注。作为一种去中心化的分布式存储技术，区块链拥有巨大的发展前景，但仍面临着众多挑战[1-2]。其中一个突出问题就是可拓展性[3]，面对数量庞大的数据信息，单一的区块链很难存储如此多的信息，因此急需解决基于区块链的可扩展性问题。

就目前区块链的发展而言，越来越多的应用场景在区块链中的实现变得不方便，如人才链、房屋信息记录等。这些应用需要区块链可以存储大量的数据，每个事物的信息是不断更新的，并且如果把需要更新的信息重新上链，会导致同一事物的信息存储位置杂乱，这就造成了查询效率变低。但如果将需要更新的信息与历史信息一起重新上链，对于区块链的存储上限也是一个挑战，因此一个新型的底层区块链结构的创建迫在眉睫。

区块链作为一种账本技术[4-11]，以区块的形式存在，并且所有数据都存储在区块中。中本聪将区块容量上限设置为 1 MB[12-13]，每个区块都包含区块头和区块体两个部分。在区块头中，包含前一块区块的哈希、时间戳、默克尔根值、随机值等信息。而在区块体中则主要包含交易的信息，前块哈希字段为前一区块的摘要信息，可以防止前一区块被任意篡改，并唯一指向了前一区块，这样就将各个区块连接起来了。因此就产生了一系列问题，如仅凭借区块体存储数据，单个区块体存储数据的容量十分有限。随着比特币平均区块大小稳步上升，截至 2017 年比特币平均区块大小接近上限，根据区块链网的统计，截至 2019 年，比特币平均区块容量达到 1.305 MB，创下了新高。同时，比特币区块扩容问题也成为了关注的焦点，其中软分叉和硬分叉的观点备受关注，软分叉采用的是隔离见证的方案，单笔交易 100%使用的情况下，扩容最多也只能达到 1.6 MB，并且隔离见证的复杂性和巨大开发工作量使得其他应用难以及时更新，甚至不愿更新。而硬分叉则是直接将区块大小扩容至 2 MB，但这也会有巨大的风险。比特币扩容的呼声越来越高，一个公认的事实是，1 MB 的区块上限已经不能满足用户的交易需求，需要扩容比特币网络，以提高交易速度和使用率。

区块链特殊的数据结构组织形式，使区块链技术具有 4 个主要特点[14-15]：去中心化、透明化、合约执行自动化、可追溯性。同样，对于本文提出的框架，也具有相同的特点，没有一个强制性的控制中心，并且每一个节点都具有相同的义务和权利，因此任意节点的崩溃不会影响整个系统的运行，使得整体具有较高的鲁棒性和可靠性。在整个运作过程中，相互之间不能进行欺骗，每一个数据的记录都要其他节点的共同认证。最后，每个被记录的数据都是被永久保存的，并且不可以被篡改。

本文最主要的贡献是提出了一个新型底层区块链结构——MSBC，将传统单链结构改进成带侧链的区块链结构，每个区块的侧链上都包含一个从属主块（subordinate mainblock）和若干个从属微块（subordinate micoblock），且可以将同一事物需要不断添加的信息存放在侧链上。MSBC 适用于各种需要不断更新增加数据的信息资源管理系统，若运用传统单链结构的区块链，这些信息的存储分为两种：1) 每次都只将需要更新的信息上链；2) 每次都将全部信息上链，包含历史信息和需要更新的信息。针对第一种情况，相比于传统单链结构的区块链，本文结构区块链在查询的时候更加便捷，大幅度提高了查询效率。而针对第二种情况，传统单链结构的区块链就面临着每个区块的存储上限问题，MSBC 同样解决了这个问题，将需要更新的信息直接加在侧链上。

2　相关工作

一般说来，区块链平台整体上可划分为网络层、共识层、数据层、智能合约层和应用层 5 个层次[16]。其中，数据层封装了底层数据区块以及相关的数据加密、时间戳等基础数据和基本算法；网络层则包括分布式组网机制、数据传播机制和数据验证机制等；共识层主要封装网络节点的各类共识算法；智能合约层主要封装各类脚本、算法和智能合约，是区块链可编程特性的基础；应用层则封装了区块链的各种应用场景和案例。区块链系统中，基于时间戳的链式区块结构、分布式节点的共识机制、基于共识算力的经济激励和灵活可编程的智能合约是区块链技术最具代表性的创新点。区块链最核心的优势是其透明、去中心化等特点保证了不同主体之间能够相互信任，极大地降低了重塑或者维护信任的成本。区块链技术可以进一步拓展到货

币、经济和市场以外的领域，其潜在的应用领域包括选举、医疗、公证、版权网络安全、汽车租赁以及学历鉴定等。

从最早应用区块链技术的比特币到最先在区块链中引入智能合约的以太坊，再到应用最广的联盟链（Hyperledger Fabric），尽管它们在具体实现上各有不同，但在整体体系架构上存在着诸多共性。在数据结构的设计上，现有区块链平台借鉴了 Haber 等[17-19]的研究工作，设计了基于文档时间戳的数字公证服务证明各类电子文档的创建时间，时间戳服务器对新建文档、当前时间及指向之前文档签名的哈希指针进行签名，形成了一个基于时间戳的证书链，该链反映了文件创建的先后顺序，且链中的时间戳无法被篡改。Haber 等还提出将多个文档组成块并针对块进行签名，用默克尔树组织块内文档等方案[20]。至今，学术界大多从两方面理解区块链：1) 区块链是一种账本技术，它结合了数据库技术，将所有发生在区块链上的交易信息记录到数据库中，使区块链具有去中心化的特征。2) 区块链是一种链式数据结构，它遵循时间顺序连接，并结合密码学保证数据的不可篡改性。

比特币、以太坊和 Hyperledger Fabric 目前都采用全网节点共享一条区块链的单链方案，网络上的每个节点需要处理和存储全网的所有交易和全部数据，整个区块链系统的处理能力实际上受限于单个计算节点的处理能力。另外，受共识算法的影响，随着节点数的增加，系统整体处理能力不但未随之提升，甚至会降低。为了实现动态的可扩展性，以太坊应用了分片[21]的解决方案，从资源均衡的角度将整个区块链网络划分成大小相同的多个分片；Hyperledger Fabric 应用了多通道的解决方案，将整个区块链网络划分为多个逻辑上的通道，每个节点根据自身需要参与的交易选择加入相应的通道。

区块链系统在查询方面也暴露出许多不足。主要体现在查询效率低，大多数区块链系统底层的数据存储系统使用的是 LevelDB，它是一种针对写密集型应用而设计的数据存储系统，以牺牲数据读性能为代价换取写性能的提高。然而，在实际应用中，区块链系统单位时间内的数据写入量并不大。如以太坊系统的交易写入量为 7～10 笔/s，比特币系统目前的交易写入量为 1 笔/s 左右，LevelDB 的高速写入优势无法体现出来。随着区块链系统中数据的增加和应用的扩展，往往需要处理频繁的查询，其底层存储系统的写性能过剩但是读性能不足，这成为了限制查询性能的主要瓶颈。区块链在历史数据查询上都很不方便，更别说复杂的复合查询和统计了。目前，大多数区块链平台随着节点数的增加其系统整体性能反而下降。另外，若将人才资源系统放在区块链上进行实现，就会导致如前面所讲的两种情况出现，当只将需要更新的信息上链时，在区块链上的人才资源信息会非常杂乱，这就给查询带来了很多不便，也就降低了查询的效率；另一方面，若将所有信息重新上链，虽然查询的效率相比之前理论上会有所提高，但由于信息会越来越多，而区块的存储容量有限，因此随着之后的信息增多，这同样会造成不便。但 MSBC 架构优化了传统单链结构的区块链的逻辑结构，将更新的信息每次都放在每个用户的侧链上，这样就解决了查询效率低的问题；其次只上链每次需要更新的信息，同时解决了区块容量不够存储所有信息的问题。

综上所述，传统单链结构的区块链不但存在查询效率低的问题，同时当应用于类似人才链时，还存在诸如以上问题。本文提出的 MSBC 框架大体解决了上述问题，MSBC 是一个带侧链的结构，更好地解决了单链结构区块链区块存储不灵活。同时，一个带侧链的区块可以存储同一用户的信息，且同一用户不断更新的信息放在侧链上，在查询时，只要通过索引找到对应用户的区块，就可以直接查看用户侧链上的所有历史上链信息，理论上解决了查询效率低的问题。

3 主从区块结构

本文提出的 MSBC 结构，从区块主链上看，是传统的区块链单链结构；从侧链上看，也可以看成传统的单链结构。因此，安全性能不低于传统单链结构的区块链的安全性。针对传统单链结构的区块链结构，本文提出的结构优化了其逻辑结构，理论上提高了查询效率，同时也保证了与传统单链结构的区块链相同的安全性。

3.1 区块体结构

MSBC 结构属于链式结构，其中区块是指数据的集合，包括相关信息和记录，是形成区块链的基本单元。为了保证区块链的可追溯性，每个区块都会带有时间戳，作为独特的标记。具体地，区块由两部分组成：1) 区块头，包含该区块的哈希以及前

块区块的哈希，负责连接到前面的区块，并为区块链提供完整性。2) 区块主体，记录了网络中更新的数据信息[16]。基于块内交易数据哈希生成的默克尔根实现了块内交易数据的不可篡改性与简单支付验证；时间戳表明了该区块的生成时间。本文根据传统单链结构进行改进，得到区块体结构如图 1 所示。图 1 中，左、右两个区块是中间区块的前一块和后一块的简单表示，中间区块上部分为区块头，包含前块哈希（previousHash）、唯一信息哈希值（onlydataHash）和自身哈希值（Hash）。下部分为区块体，包含区块的数据信息。以人才链为例，data1 为姓名，data2 为性别，以此类推。其中 onlydata 为唯一性信息，对应为用户的身份证号码。与传统单链结构的区块链相比，MSBC 架构增加了一个唯一信息哈希值，用来进行侧链的连接。

3.2　从属主块结构

区块链单一的区块体结构对于现在很多市场资源信息的存储不太方便，因此，本文先设计了一个从属主块结构，即侧链上第一个从属区块，称为从属主块，通过唯一信息（以人才链为例，每个用户的唯一信息即该用户的身份证号码）的哈希值与区块体进行连接，每一个区块体除了下一区块与它连接，都有且只有唯一的一个从属主块在侧链上与之连接。从属主块上包含唯一信息哈希值（onlydataHash）、时间戳（timestamp）、数据信息（data information）、从属主块包含数据信息的哈希值（Hash of own content）、索引（index）、从属微块索引数组（microblock index array）等信息。从属主块结构如图 2 所示。

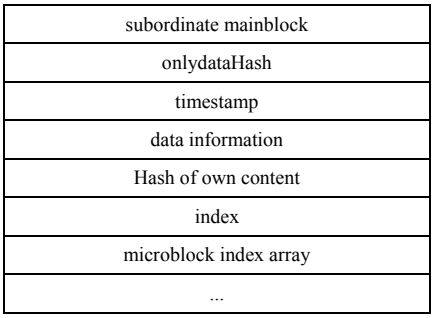

图 2　从属主块结构

3.3　从属微块结构

除了引入上述从属主块结构，本文还引入了从属微块结构，从属微块相对从属主块而言区别在于第一块从属微块是连接从属主块的，之后的都是从属微块之间相互连接，但无论是从属主块和从属微块连接，还是从属微块与从属微块之间连接，都通过前一块信息的默克尔根哈希值衔接。从属微块结构与从属主块结构相似，包含前块哈希（previousHash）、时间戳（timestamp）、数据信息（data information）、数据信息哈希值（Hash of own content）和索引（index）等信息。从属微块结构如图 3 所示。

4　带侧链结构工作原理

利用从属主块和从属微块，本文提出了 MSBC

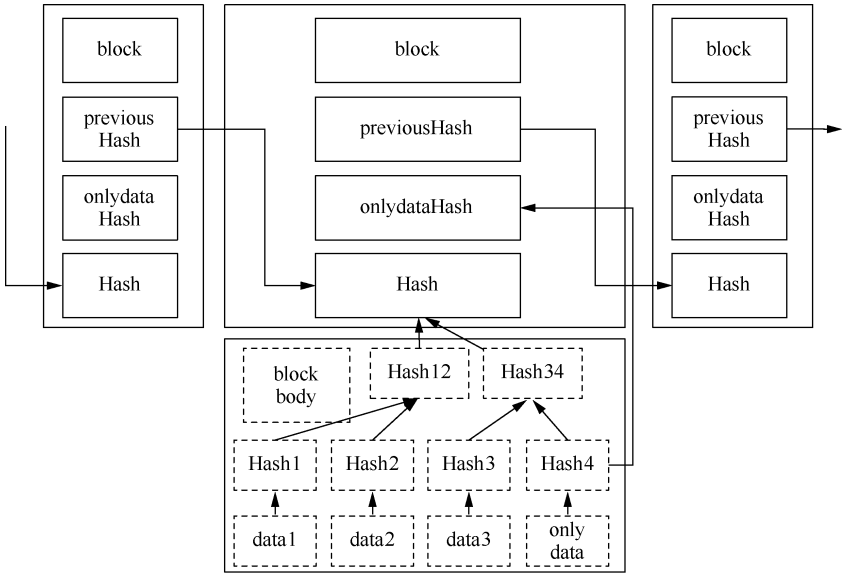

图 1　区块体结构

结构框架。主链上由多个传统区块组成，每一个区块都有自身的侧链，侧链包含一个从属主块和多个从属微块。MSBC 结构如图 4 所示。

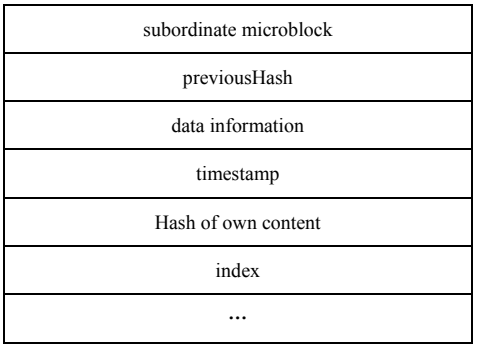

图 3　从属微块结构

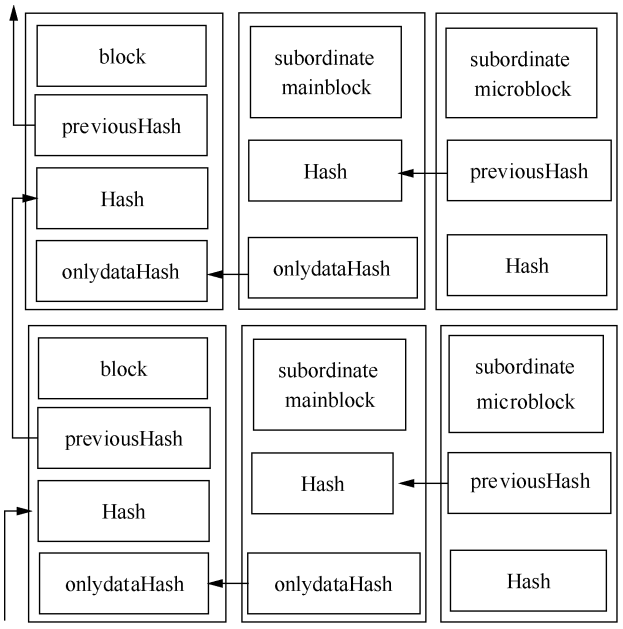

图 4　MSBC 结构

与传统单链结构的连接方法类似，MSBC 框架在单链的基础上加入了侧链的结构，将需要存储在主区块上的大量数据都放在侧链上，从侧链的角度看，也是一个传统的单链模式。

主区块与主区块之间的连接与传统的区块链连接相同，把主区块中的信息进行双重 SHA256 哈希运算，后一主区块根据前一主区块内容生成的哈希值将两者连接起来。在侧链上，将从属主块基于主区块的唯一性信息生成的哈希与主区块连接起来，将从属微块基于前一从属块（无论从属主块还是从属微块）的内容生成的哈希值与前一从属块连接起来。

以人才资源管理为例，因为统一为个人信息上链，每个人将自己的信息上链，不用通过矿工挖矿，则自己生成自己的主区块，所以就取消了矿工挖矿问题。这是跟传统单链结构的区块链不同的地方，直接计算出前块哈希就能连接上链，但是这也随之衍生出一个问题就是多个用户同时上链，因此，若有多个用户同时上链，则首先判断时间，根据时间先后选择最早的用户上链，其他用户需要重新根据新的哈希值形成自己的主区块。若时间完全相同，则随机选取一名用户上链。

5　实验与分析

本文提出的框架采用 Java 语言实现。

5.1　架构实现

MSBC 在传统单链结构的区块链的基础上进行改进，因此需要通过实验验证 MSBC 的可行性。

5.1.1　实验数据

本实验模拟了 4 个用户的上链，假设每个用户分别上链 3 次数据，实验数据如表 1 所示，分别为 No.1 data、No.2 data 和 No.3 data，3 次数据分别模拟 4 个用户的 3 次上链数据。

5.1.2　实验结果

实验中，根据给出数据逐个上链，得出所需要的哈希值，哈希表（哈希值为前 6 位）如表 2 所示，表 2 为每个区块以及从属链上的区块的哈希值。前块哈希表（哈希值为前 6 位）如表 3 所示，表 3 为各个区块的前一区块的哈希值以及每个从属块的前一从属块的哈希值。

5.1.3　实验分析

根据上面的实验结果，可以得到区块结构（哈

表 1　　**实验数据**

姓名	性别	ID	No.1 data	No.2 data	No.3 data
zhangsan	male	11111	zhangsanfirst	zhangsansecond	zhangsanthird
lisi	female	22222	lisifirst	lisisecond	lisithird
wangwu	male	33333	wangwufirst	wangwusecond	wangwuthird
zhaoliu	male	44444	zhaoliufirst	zhaoliusecond	zhaoliuthird

表 2　　**哈希表（哈希值为前 6 位）**

data	index	Hash	onlydataHash	mainblock Hash	microblock Hash 1	microblock Hash 2
Zhangsanmale11111	1	3b2b14	d17f25	2297ed	5cec7b	7de990
Lisifemale22222	2	b44371	cc393d	440cc5	d9246a	93b08c
Wangwumale33333	3	c5f43e	216e68	6e07b7	343711	038bdc
Zhaoliumale44444	4	a38a83	E11d8c	13d59b	cde48c	9cb70c

表 3　　**前块哈希表（哈希值为前 6 位）**

data	index	previou-sHash	onlydataHash	the previousHash of microblock Hash 1	the previousHash of microblock Hash 2
Zhangsanmale11111	1	79b2ea	d17f25	2297ed	5cec7b
Lisifemale22222	2	3b2b14	cc393d	440cc5	d9246a
Wangwumale33333	3	b44371	216e68	6e07b7	343711
Zhaoliumale44444	4	c5f43e	e11d8c	13d59b	cde48c

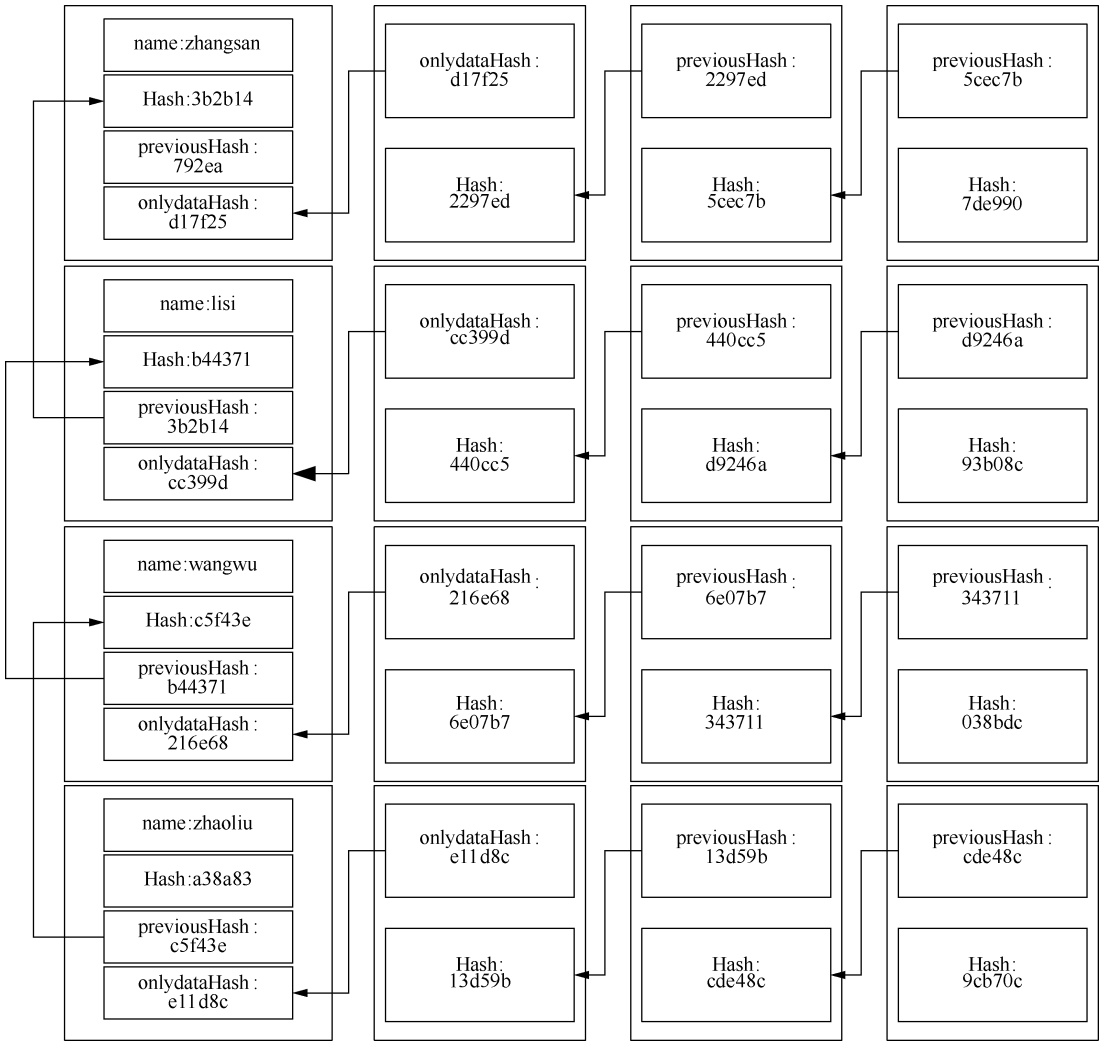

图 5　区块结构（哈希值为前 6 位）

希值为前 6 位）如图 5 所示，每个用户都是通过计算前一个用户的哈希值连接，并且每一个用户的从属链块（从属主块）是计算用户主区块的唯一信息哈希连接，从属微块则通过计算前一个从属块的哈希值连接。通过此方法，初步实现了本文所提出的框架结构。

5.2　查询效率

本实验在单机上进行，假设各组实验的网络开

销相同。

5.2.1　实验数据

本实验随机生成了 200 组用户数据，每个用户至少有 1 次简历信息，至多有 3 次简历信息。其中用户的姓名随机生成，身份证号由随机生成的 5 位数字表示且号码不重复，性别随机（用户的所有信息均为随机生成，且确保了姓名和身份证信息的唯一性），简历信息由姓名+resume 表示，如第一次简历信息为 xxx_resume1，以此类推。

实验对 MSBC 与传统单链结构的区块链进行对比，4 组实验分别在 10 组用户数据、50 组用户数据、100 组用户数据和 200 组用户数据情况下进行查询时间的统计。

5.2.2　实验结果

本文实验数据量有限，对上链时间的影响并不大，在本实验中着重对比查询时间。MSBC 和传统单链结构的区块链随用户量增多的查询时间如表 4 所示，表示了传统单链结构的区块链和 MSBC 根据索引值在用户数量不同时查询效率的变化。

表 4　MSBC 和传统单链结构的区块链随用户量增多的查询时间

用户量	MSBC/10^8ns	传统单链结构/10^8ns
10	0.017 382	0.749
50	0.022 777	1.438
100	0.023 745	2.823
200	0.025 356	3.29

由表 4 可以看出，MSBC 和传统单链结构的区块链在查询时间上随着用户数据量的增多而增长。但是也可以明显看出，相较于传统单链结构的区块链，MSBC 在查询时间上有着显著的提升。此外，在用户数量增加的情况下，传统单链结构的区块链的查询时间受较大影响，当用户量为 200 组时，其查询时间相较于用户量为 10 组时增加了 5 倍左右；相反，MSBC 在 10 组和 200 组时的查询时间只增加了 1.5 倍左右。MSBC 查询时间如图 6 所示，传统单链结构的区块链查询时间如图 7 所示，分别显示了 MSBC 和传统单链结构的区块链在查询时间上的变化情况，其中横坐标表示用户数据量，纵坐标表示时间，时间单位均为 10^8 ns。由图 6 和图 7 展示的实验数据可见，随着用户量的增多，MSBC 的查询时间的增长幅度较为平缓，而传统单链结构的区块链查询时间的增加幅度较为明显。由此可见，较传统单链结构的区块链而言，MSBC 在查询效率方面受用户增长的影响更小，查询效率更高。

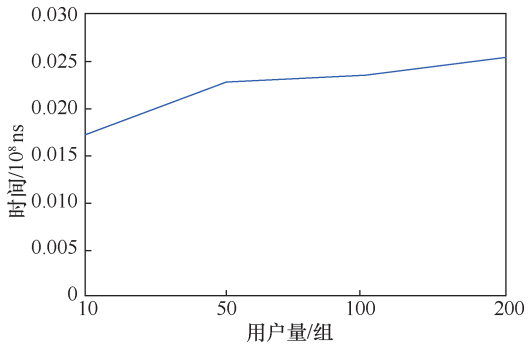

图 6　MSBC 查询时间

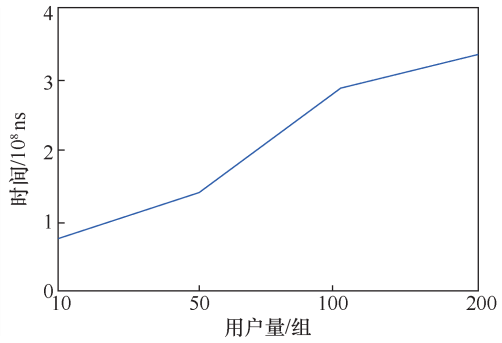

图 7　传统单链结构的区块链查询时间

6　应用举例

6.1　人才链

人才信息的管理是目前市场一个比较重要的环节，首先是信息量庞大问题，对于每个人的简历都是一个比较大的数据，存储起来简单，但是管理起来比较复杂，尤其是数据的真实性有待探讨，因此将人才信息放在 MSBC 框架上，可以有效地解决人才信息的管理问题。对于数据的真实性问题，当客户将数据放在区块上后就不能对数据进行修改，若数据有假，由于链的不可篡改性，虚假的信息会一直存在，当需要进行验证时，客户无法删除和修改已上链的信息。

若是将人才信息放上链，每个人将个人不变的信息（姓名、性别、身份证号等）上链，形成一个区块。在形成了自己的区块后，可以把个人简历第一次放入侧链中，即生成第一个从属块，也就是从属主块，此时根据区块中的身份证哈希值进行连接，此后简历的增加则是在从属主块后形成从属微块，从属微块根据前一块微块的个人简历信息、时间戳等全部内容的双重哈希值进行连接。

6.2　房产链

如今，随着房屋数量的不断增多、房价的上涨，租房的人也逐渐增多。由于租客的不断更改，租客信息的不断变更，因此对于房屋信息的管理也变得尤为重要。

房屋信息管理同样可以适用于本文提出的框架，存储每个房屋尤其是出租房屋的信息，对于每一个租客的信息都可以进行存储，并且上链后可以永久存储，不可被篡改。这样就可以清楚地了解每一任租客的信息。

以每一个房屋作为区块，区块上存储房屋的不变信息（地址、房间号、几室几厅）等主要信息，从属主块基于区块上的房产证号的双重哈希将其去区块连接起来，从属主块上会存储第一任租客的信息、时间戳等内容。而从属微块基于前一从属块（无论是从属主块还是从属微块）内容的哈希将其与从属主块进行连接，并存储相应租客的信息、时间戳等内容。

7　结束语

本文最主要的贡献在于从区块链的底层结构入手，加入了侧链，提出了 MSBC 架构，解决了传统单链结构的区块链存储不灵活、查询效率低问题，适用范围广。对于日益庞大的数据，MSBC 可以在保证同等安全性的情况下，更加便捷地存储更多数据，并且可以适应不断更新的数据，使得数据管理更为简洁明了。

其次本文提出的 MSBC 结构为区块链的可拓展性问题提出了一种解决方法，通过对传统单链结构区块链的改进，使得区块链中区块信息能够更加灵活地进行存储。传统单链结构的区块链需要等待一定量的交易才可以打包上链，而 MSBC 架构中区块大小不固定，存储更灵活。同时，相比于传统单链结构的区块链，进一步提高了链上数据的查询效率。实验验证了该结构的可行性。

以人才链为例，若是普通的单链区块链，人才链在实现起来就非常困难。首先每个人的简历信息数据量大是一个问题；其次，一个人可能存在更换多种工作的经历。因此，需要对上链的简历信息进行不断地更新。传统的区块链可以一次只将更新的个人简历信息上链，但这样会使一个人的简历信息太过分散，不容易实现，并且查询效率低。若将所有信息重新上链，虽然查询的效率相比之前会有所提高，但由于冗余信息会越来越多，不仅浪费空间，而且区块的存储容量有限，随着信息量的增多，可能会造成区块容量不够。本文提出的 MSBC 结构为人才链提供了一种很好的解决方法，每个人以固定不变的身份信息作为主区块，将不断更新的简历信息放在从属块上，可以解决数据存储的杂乱问题，并提高查询效率。

与传统单链结构的区块链相比，MSBC 架构无传统的竞争挖矿过程，没有挖矿中的随机数与难度系数，这使得上链更快、实时性更强，同时在理论及实验上提高了数据的上链效率。

本文为解决当前区块链可扩展性不强及查询效率较低问题，提出了一种新型区块链结构 MSBC，实验结果验证了 MSBC 在查询效率上优于传统单链结构的区块链。本文主要研究区块链架构，提出了 MSBC 架构，共识机制是区块链中主要的研究问题之一，将来会对此进行重点研究。下一步，考虑实际网络开销的不同，将在模型中加入 P2P 网络，进一步与目前主流的单链区块链结构在查询效率、存储性能、上链时间、共识时间等方面进行实验对比，验证 MSBC 架构综合性能的优越性。基于 MSBC 架构的人才链和房产链等应用正处于研发阶段，在未来，将以应用为基础，进一步研究区块链相关理论和技术。

参考文献：

[1] NAKAMOTO S. Bitcoin: a peer-to-peer electronic cash system[Z]. Consulted, 2008.

[2] 何蒲, 于戈, 张岩峰, 等. 区块链技术与应用前瞻综述[J]. 计算机科学, 2017, 44(4): 1-7, 15.
HE P, YU G, ZHANG Y F, et al. Survey on blockchain technology and its application prospect[J]. Computer Science, 2017, 44(4): 1-7, 15.

[3] SHEN X, PEI Q Q, LIU X F. Survey of block chain[J]. Chinese Journal of Network and Information Security, 2016, 2(11): 11-20.

[4] 李牧南. 区块链和比特币相关主题的知识结构分析: 共被引和耦合聚类分析视角[J]. 自动化学报, 2017, 43(9): 1509-1519.
LI M N. Analyzing intellectual structure of related topics to blockchain and bitcoin: from co-citation clustering and bibliographic coupling perspectives[J]. Acta Automatica Sinica, 2017, 43(9): 1509-1519.

[5] 贾大宇, 信俊昌, 王之琼, 等. 区块链的存储容量可扩展模型[J]. 计算机科学与探索, 2018, 12(4): 525-535.
JIA D Y, XIN J C, WANG Z Q, et al. Storage capacity scalable model for blockchain[J]. Journal of Frontiers of Computer Science and Technology, 2018, 12(4): 525-535.

[6] 张宁, 王毅, 康重庆, 等. 能源互联网中的区块链技术: 研究框架与典型应用初探[J]. 中国电机工程学报, 2016, 36(15): 4011-4023.
ZHANG N, WANG Y, KANG C Q, et al. Blockchain technique in the energy Internet: preliminary research framework and typical applica-

tions[J]. Proceedings of the CSEE, 2016, 36(15): 4011-4023.

[7] WOLRICH G M, YAP K S, GUIFORD J D, et al. Instruction set for message scheduling of SHA256 algorithm: US, 8838997B2[P]. 2012-09-28.

[8] SZYDLO M. Merkle tree traversal in log space and time[J]. Lecture Notes in Computer Science, 2004(3027): 541-554.

[9] MERKLE R C. Protocols for public key cryptosystems[C]//1980 IEEE Symposium on Security and Privacy. Piscataway: IEEE Press, 1980: 122-133.

[10] MERKLE R C. A digital signature based on a conventional encryption function[J]. Conference on Advances in Cryptologycrypto, 1987, 293(1): 369-378.

[11] HABER S, STORNETTA W S. How to time-stamp a digital document[J]. Journal of Cryptology, 1991, 3(2): 99-111.

[12] BAYER D, HABER D, STORNETTA W S. Improving the efficiency and reliability of digital time-stamping[M]. Beilin: Springer, 1993.

[13] BAYER D, HABER S, STORNETTA W S. Improving the efficiency and reliability of digital time-stamping[C]//Methods in Communication, Security and Computer Science. Berlin: Springer, 1993: 329-334.

[14] CROMAN K, DECKER C, EYAL I, et al. On scaling decentralized blockchains[J]. The Financial Cryptography and Data Security, 2016: 106-125.

[15] AZZI R, CHAMOUN R K, SOKHN M. The power of a blockchain-based supply chain[J]. Computers & Industrial Engineering, 2019(135): 582-592.

[16] 邵奇峰, 金澈清, 张召, 等. 区块链技术: 架构及进展[J]. 计算机学报, 2018, 41(5): 969-988.
SHAO Q F, JIN C Q, ZHANG Z, et al. Blockchain: architecture and research progress[J]. Chinese Journal of Computers, 2018, 41(5): 969-988.

[17] HABER S, STORNETTA W S. How to time-stamp a digital document[C]//Proceedings of the Advances in Cryptology-CRYPTO' 90(CRYPTO). [S.l.:s.n.], 1990: 437-455.

[18] HABER S, STORNETTA W S. Secure names for bit-strings[C]//Proceedings of the 4th ACM conference on Computer and Communications Security-CCS'97. New York: ACM Press, 1997: 28-35.

[19] 蔡维德, 郁莲, 王荣, 等. 基于区块链的应用系统开发方法研究[J]. 软件学报, 2017, 28(6): 1474-1487.
CAI W D, YU L, WANG R, et al. Research on application system development method based on blockchain[J]. Journal of Software, 2017, 28(6): 1474-1487.

[20] BUTERIN V. Ethereum 2.0 mauve paper[R]. White Paper, 2016.

[21] 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.
YUAN Y, WANG F Y. Blockchain: the state of the art and future trends[J]. Acta Automatica Sinica, 2016, 42(4): 481-494.

[作者简介]

谭朋柳（1975− ），男，南昌航空大学副教授，主要研究方向为区块链、信息物理融合系统、智能医疗等。

万里旭冉（1996− ），女，南昌航空大学软件学院硕士生，主要研究方向为区块链。