孚衍(GOVM)技术白皮书

一个基于多链的高性能区块链系统

2019 年 10 月

V1.0.0

摘要

孚衍（GOVM）系统设计了一种全新的区块链架构，以高性能为目标的公有链。通过多链并行，可突破带宽、存储等单节点资源瓶颈，实现横向拓展的扩容方案，实现系统的高性能；通过单链前后区块的哈希锁定和父子链区块的哈希锁定，实现数据的不可篡改性；支持动态增加新链，实现系统的可扩展性，从而线性提升系统的整体性能；支持不同的链发布相同的智能合约，合约可以通过跨链读取信息实现跨链通信，从而实现智能合约的超高性能。

它的理论 TPS 性能极限可以超过 $83*2^{64}$，远远高于当前所有的区块链系统。

目录

1. 简介

1.1. 区块链市场

我国在“十三五”规划中明确指出要强化区块链等战略性前沿技术并进行超前布局。我国区块链企业数量不断增长，其中 2014 年单年度新增区块链企业数量最多。与全球区块链领域投资相比，中国区块链产业投融资起步稍晚，2016 年明显加速。

截止到 2017 年中国区块链市场支出规模仅为 0.83 亿美元。2018 年全年中国区块链市场支出规模将达 1.6 亿美元。并预测在 2019 年中国区块链市场支出规模将接近 3 亿美元。现阶段区块链的总体市场规模较小，这是因为市场上的区块链项目多处于尝试阶段，投入不大。另一方面，很多企业已经认识到了区块链的潜力，计划在未来增加预算，受此影响，中国区块链市场将迎来快速增长，预计到了 2023 年的市场支出规模预计达到 19.5 亿美元，2019－2023 年的年均复合增长率为 60.51%。[1]

根据 Adroit Market Research 发布报告显示，预计到 2025 年，全球区块链 DLT 市场规模将达 327. 6 亿美元，在 2018 年至 2025 年的预测期间，年复合增长率将保持两位数。

来自世界经济论坛调查报告的预测，7 年后全球 GDP 总量的 10%将基于区块链技术保存。

1.2. 政策背景

国家政策多次提及发展区块链产业

以区块链等为代表的新一代信息技术加速突破应用……融合机器人、数字化、新材料的先进制造技术正在加速推进制造业向智能化、服务化、绿色化转型。 ——2018 年 5 月习近平总书记在两院院士大会上的重要讲话

区块链技术首次被列入《国家信息化规划》。 ——2016 年 12 月国务院印发《“十三五”国家信息化规划》

提升信息技术服务能力，鼓励利用开源代码开发个性化软件，开展基于区块链、人工智能等新技术的试点应用。 ——2017 年 8 月国务院印发《关于进一步扩大和升级信息消费持续释放内幕潜力的指导意见》

研究利用区块链、人工智能等新兴技术，建立基于供应链的信用评价机制。 ——2017 年 10 月国务院办公厅发布《国务院办公厅关于积极推进供应链创新与应用的指导意见》

区块链领域成为创新创业的新热土，技术融合将拓展应用新空间，区块链未来三年将在实体经济中广泛落地，成为数字中国建设的重要支撑。 ——2018 年 5 月工信部发布《2018 中国区块链产业白皮书》

据互链脉搏不完全统计，截至 2019 年 5 月，全国共有广东、浙江、江苏、上海、福建、

[1] 2019 年中国区块链市场分析报告-产业规模现状与发展规划趋势

贵州、山东、江西等 12 个省和直辖市发布了区块链指导意见，上海、杭州、苏州、广州、长沙、重庆、成都等城市为了吸引更多区块链企业落户当地产业园区，甚至专门针对区块链初创企业落户、企业经营、高层次专业人才落户、购房补贴以及生活补助等方面都出台了相应的扶持政策。

1.3. 区块链简介

2008 年比特币问世，区块链技术不断的发展。

区块链本质上是一个去中心化的分布式账本数据库。区块链作为点对点网络、密码学、共识机制、智能合约等多种技术的集成创新，提供了一种在不可信网络中进行信息与价值传递交换的可信通道。

比特币作为区块链 1.0 的代表，解决的是区块链的有无问题。以太坊作为区块链 2.0 的代表，解决的是区块链的智能问题，它支持发布智能合约，使区块链进入可编程时代。

区块链有很多的应用场景，可是现有区块链的性能却严重制约着它的发展。

1.4. 高性能需求

TPS（Transactions Per Second）又称“系统的吞吐量”，即“系统每秒钟能够处理的交易数量”。

当前区块链最大的问题是性能问题。下图为部分公链的单日最大交易量（2019/10/1 前的数据）[2]：

名字	数据日期	交易量	TPS	备注
BitCoin	2017/12/14	490644	5.67875	
Ethereum	2018/01/04	1349890	15.6237	
TRON	2019/07/22	5280790	61.1203	
EOS	2018/11/10	11557159	133.7634	

据统计，对于一台普通的计算机，拥有 13Mbps 的互联网连接，E5-1620@3.5GHz 4Core 的 CPU，16G 内存，512G SSD 硬盘(250MB/s)，网络带宽导致的 TPS 理论上限约为 7 千 TPS，硬盘文件 I/O 导致的 TPS 理论上限为 5 万 TPS，CPU 处理能力导致的 TPS 理论上限约为 5 万 TPS[3]。

现有的单链式结构，存在着带宽、存储、计算等单节点资源瓶颈。

区块链技术和学术专家提出多种高性能方案[4]：

类别	DAG	并行	减少共识节点数
优化层面	拓扑	架构	共识
安全性	高	高	可能降低
资源消耗	低	低	低
扩展能力	好	好	一般
难度	高	高	中

[2] 数据来自 https://tokenview.com/
[3] 时戳资本：分片研究报告
[4] 中国信通院：2018 区块链白皮书

性能	高	高	中
案例	IOTA Byteball Hashgraph	Ethereum（分片） TrustSQL（子链） Fabric（多通道）	Algorand BitcoinNG PoS

跨链技术：不同区块链之间的交互技术。

跨链技术对比：[5]

类别	公证人	侧链/中继	哈希锁定
跨链方向	双向	双向/单向	双向
资产交换	支持	支持	支持
资产转移	支持	支持	不支持
信任	需要第三方	不需要	不需要
类型	协议	技术架构	算法
难度	中等	困难	容易
案例	Ripple	BTC relay Poldadot COSMOS	Lightning network

跨链项目主要是解决不同区块链之间的通信问题（孤岛问题），能够将部分交易转移到其他链上，从而减少单系统内的交易，缓解系统压力。

本项目采用的方案是重新定义架构，以同构的多链并行处理的方式，提升单个区块链系统的性能，不涉及跨系统的通信。接下来将介绍现有部分项目的特点。

1.4.1. IOTA

IOTA（中文埃欧塔），是于 2014 年众筹的一个项目，宗旨是利用 DAG（有向无环图，IOTA 里叫做 Tangle——缠结）代替区块链实现分布式、不可逆（由密码学保证）信息传递的一种技术，在此基础上集成加密货币功能，服务于物联网。基于 DAG 的设计没有区块的概念，扩容不受区块大小的限制，其可伸缩性取决于网络带宽、CPU 处理速度和存储容量的限制。

因为 IOTA 整个网络目前的算力极低（通常在 1~2TPS 左右，一台较好的电脑即可达到），因此目前的 IOTA 网络的交易确认并不是利用的缠结内在特性，而是利用了“协调器”，协调器工作时，交易由一个特定的地址发出，该地址发出的交易被全网无条件接受，它被固化在 IOTA 全节点的代码中，因此 **IOTA 目前阶段是一个中心化系统**，整个网络的确认都由协调器负责；此外 DAG 技术在网络交易传播方面并无优势，所有节点仍然需要通过广播接收到所有交易信息，因此 IOTA 的无限扩展特性与区块链系统放宽区块大小本质上是一样的。[6]

优点：是交易免手续费，有效交易越多，系统越可靠，支持离线交易。

缺点：是容易受到 DOS 攻击，容易出现双花问题，一个地址只能使用一次。

DAG 虽然是一种很新颖有潜力的技术，然而基于它的 IOTA 网络目前在技术上仍处于实验室阶段。

---

[5] 中国信通院：2018 区块链白皮书

[6] http://www.sohu.com/a/225441526_100078137

1.4.2. Ethereum[7]

分片原本是数据库设计中的一种概念，指将数据库中的数据分割成多个数据分片存储在不同的服务器上。当进行搜索时，仅需访问特定分片即可获得搜索结果，减少了服务器访问压力，从而提高数据库性能。

在区块链中，分片指将区块链中的节点分成若干个组，每组节点组成一个分片。原先区块链中每个节点需要对网络中的每笔交易进行验证，分片后，每个节点仅需处理网络中的一小部分交易。各分片并行工作，从而实现对区块链的横向扩展。

分片技术有很多阶段，也有很多技术难点。当前都没有完整可用的方案，方案的实现落地还需要漫长的时间。

以太坊将其分为 6 个阶段，计划 2020 年启动第一个阶段，后续的 5 个阶段还没有具体方案。

1.4.3. Fabric

IBM 提供的 Hyperledger Fabric 也是采用**联盟类型区块链**的一种，并通过“PBFT”实现了快速交易验证; 一个共识算法，其中交易通过大多数可信节点的同意进行验证。

Hyperledger Fabric 架构使用具有保证的发布-订阅模式消息传递通道（如 Kafka 中的主题分区）将共识服务与交易日志（账本）分离。共识服务由称为 Orderers 的网络节点提供，并且账本由 Peer 节点管理。

每个 Peer 节点连接到共识服务的一个或多个通道，就像发布-订阅通信系统中的客户端一样。在通道上广播的交易按共识的顺序排列（例如 PBFT、kafka），订阅通道的 Peer 节点接收到加密的区块。 每个 peer 节点验证区块并将其提交到账本，然后向应用程序提供其他使用账本的服务。

在共识服务上支持多通道消息传递，使得 Peer 节点可以基于应用访问控制策略来订阅任意数量的通道; 也就是说，应用程序指定 Peer 节点的子集中架设通道。 这些 peer 组成提交到该通道交易的相关者集合，而且只有这些 peer 可以接收包含相关交易的区块，与其他交易完全隔离。

此外，peers 的子集将这些私有块提交到不同的账本上，允许它们保护这些私有交易，与其他 peers 子集的账本隔离开来。应用程序根据业务逻辑决定将交易发送到 1 个或多个通道。 这不是内置的限制，区块链网络不知道并假设不同通道上的交易之间没有关系。

Fabric 的多通道机制并不适用于公有链系统。因为公有链的每个节点都可能是不可信的，且节点随时可能新增或减少，会出现各种各样的异常和攻击，且无法保证固定的 peers 子集。

1.4.4. Poldadot[8]

Polkadot 是由原以太坊主要核心开发者推出的公有链。它旨在解决当今两大阻止区块链技术传播和接受的难题：即时拓展性和延伸性。Polkadot 计划将私有链/联盟链融入到公有链的共识网络中，同时又能保有私有链/联盟链的原有的数据隐私和许可使用的特性。它可

---

[7] 时戳资本：分片研究报告

[8] Polkadot 白皮书

以将多个区块链互相连接。

Polkadot 是一个可伸缩的异构多链系统。这意味着不像以往那些专注于不同程度潜在应用功能的单个区块链实现，Polkadot 本身被设计成不提供任何内在的功能应用。Polkadot 提供了中继链（relay-chain），在其上可以存在大量的可验证的、全局依赖的动态数据结构。我们称这些平行的结构化的区块链为平行链（parachains），尽管也不要求它们必须是一条链。

跨链交易的问题用一个简单的队列机制解决，这个队列用梅克尔树（Merkle tree）来保证数据真实。中继链的任务是把交易从来源平行链的出口队列转移到目的平行链的入队列。已转发的交易会在中继链上被引用，而不是中继链自身的交易。为了预防一条平行链往另一条平行链发送垃圾交易，规定在在前一个块结束后，发送每一个交易时，目标平行链的入队列不能太大。如果区块处理完后，入队列太大，那么目的平行链会被看做是饱和了，接下来的几个块里就不会再路由交易给它，直到入队列降到临界值以下。

Polkadot 通过定制一套比较严格的制度，采用了钓鱼人和收集人的理念，从而尽量避免恶意操作。本质上 polkadot 还是想用制度来解决技术问题。[9]

1.4.5. COSMOS[10]

Cosmos 是 tendermint 团队推出的一个支持跨链交互的异构网络。Cosmos 采用的 Tendermint 共识算法，是一个类似实用拜占庭容错共识引擎，具有高性能、一致性等特点，而且在其严格的分叉责任制保证下，能够防止怀有恶意的参与者做出不当操作。

Cosmos 上的第一个空间叫做"Cosmos Hub"。Cosmos Hub 中心是一种多资产权益证明加密货币网络，它通过简单的管理机制来实现网络的改动与更新，还可以通过连接其他空间来实现扩展。

Cosmos 网络的中心及各个空间可以通过区块链间通信（IBC）协议进行沟通，这种协议是针对区块链网络的，类似 UDP 或 TCP 网络协议。 代币可以安全快速地从一个空间传递到另一个空间，两者之间无需体现汇兑流动性。相反，空间内部所有代币的转移都会通过 Cosmos 中心，它会记录每个空间所持有的代币总量。这个中心会将每个空间与其他故障空间隔离开。因为每个人都可以将新空间连接到 Cosmos 中心，所以 Cosmos 也可以兼容未来新的区块链。

它要求每个区块链都需要集成 IBC 协议。

1.5. 本项目的技术方向

现有的高性能方案中，并没有一个方案真正解决高性能问题；跨链技术中，通过协议或方案实现不同的区块链的通信问题，也没有解决单系统的性能问题，同时单个智能合约的吞吐量依旧受限于单个区块链的性能。

本项目通过全新的架构，采用多链并行的方式，实现数据的并行处理，从而提高系统的整体性能[11]。本系统不涉及与其他区块链系统的通信问题。

以单条链 10TPS 计算[12]，系统支持最多 2^{64} 条链，那么最终性能将可以达到 $10*2^{64}$TPS，

---

[9] https://zhuanlan.zhihu.com/p/68694986
[10] https://www.8btc.com/course/4700
[11] 每条链都是系统不可分割的一部分。
[12] 一条链的性能可以远远高于 10TPS。

该数值远远超过当前所有区块链性能总和。

本系统满足普通区块链的基本特性：去中心化、数据可追溯、数据不可篡改、智能合约。

新增特性：按需增加新链、跨链转移代币、智能合约跨链访问数据。

本系统的跨链操作是指在系统中不同的链之间的操作。

智能合约的性能极限不受限于单链的性能，可以通过不同链上部署相同合约，并通过跨链通信实现智能合约的高性能。

接下来将从多个维度讲解方案的技术原理，包括共识算法、链与链的逻辑关系、区块结构、数据存储方式、账户系统、智能合约等方面。

2. 共识算法

PORW：Proof of Register and Work，注册制工作证明。

持有代币的人都可以注册成为矿工，注册过的矿工计算算力时，有一定的算力加成。

矿工注册的是某一个区块的记账权，注册用的代币将被冻结一段时间(50000 个区块，约一个月)，以避免该矿工一直成为注册矿工。注册需要的代币超过区块奖励。

没有注册过的矿工也可以参与挖矿，只是没有算力加成。

每个区块最多允许 11 名注册矿工。系统没有预分配代币，所以初始所有人都没有代币，这个时候，没有注册矿工，只有 POW 作为共识机制。

区块的生成时间是固定的，默认为 1 分钟[13]一个区块，每次选择算力最高的区块作为新区块。

注册成为矿工是通过注册交易[14]完成的，所有注册信息都在链上，透明公开。

为了确保区块的挖矿者身份不被冒用[15]，每个区块都会携带矿工的签名。这种方式也可以限制公有矿池的规模。因为每次计算区块哈希，都需要先对区块进行签名。如果矿池公布私钥，那么它的代币随时可能被转移走；如果不公布私钥，那么只能自己签名，每次签名完，再交给矿工计算哈希，那么矿池的签名速度将成为最大的瓶颈，将难以满足，同时矿池与矿工之间也需要大量的签名信息同步，两者间的网络能力也成为瓶颈。这样就大大限制矿池的规模。

2.1. 区块确认

采用的是 PORW，所以它和比特币一样，为了确保一个交易是不可逆转的，可以等待 6 个区块确认。一个区块生成时间为 1 分钟，所以区块确认时间为 6 分钟。

3. 链

3.1. 概念

如果一条链 a 创建了一条新的链 b，则链 a 为链 b 的父链，链 b 为链 a 的子链。

---

[13] 新链有更小的间隔，且间隔时间可以根据需要进行调整。

[14] 交易有多种类型，注册交易仅仅是其中的一种

[15] 因为支持智能合约，系统不可预测的情况更多，就有可能冒用他人挖矿，执行恶意的智能合约

系统初始只有一条链，它没有父链，其他的链都有父链。
每条链可以创建 2 条子链，分别叫做左子链和右子链。

3.2. 链间的逻辑关系

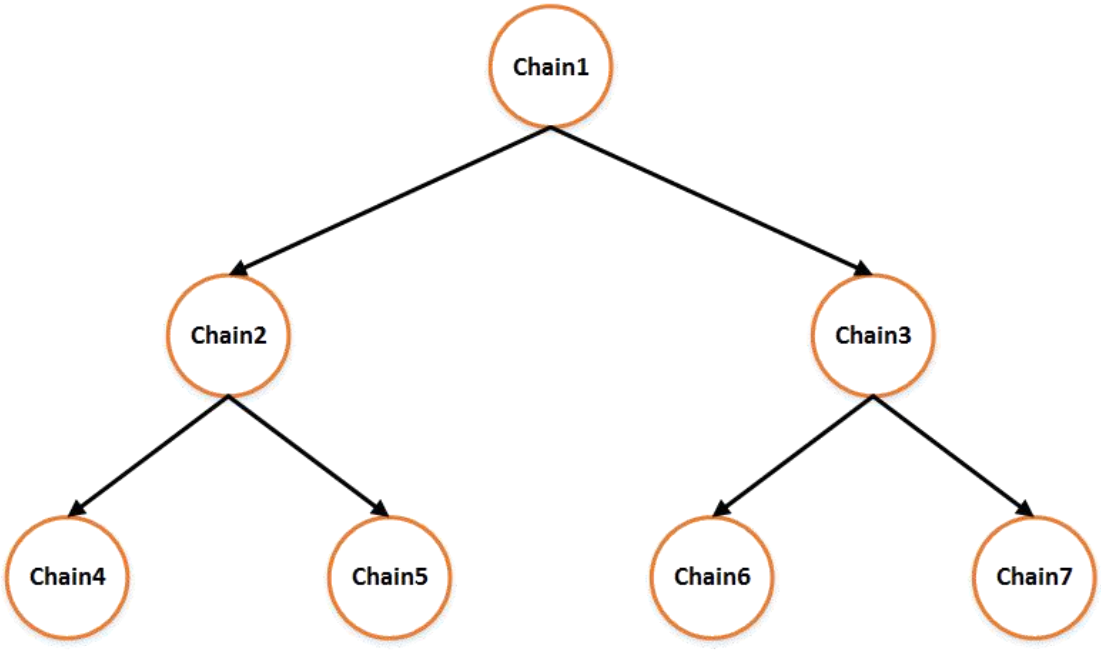

图 1 链的逻辑关系

所有链将组成一个二叉树，这就是它们的逻辑关系。
链 ID 为 64 位数字，从 1 开始，所以最多可以有 2^{64}-1 条链。
每条链可以有 2 条子链。
通过这种方式，链的数量和位置确定，方便扩展和跨链访问。

3.3. 链的创建

整个系统的第一条链是由开发团队创建，创建过程和其他区块链系统一样。
其他的链都是通过“创链交易”创建的。
每条链允许创建 2 条子链，只要条件满足，任何人都可以创建。
第二条和第三条链的创建没有限制，任何人随时可以创建。
后续链的创建，需要满足以下几个条件：
a.链的平均交易量大于 300K，避免无限制创建。
b.需要花费代币，代币量最大为区块奖励的一万倍，平均交易量越大，花费越低。
c.子链不存在才能创建。
d.先创建左子链，后创建右子链。
e.创建右子链时，左子链的区块 ID 必须大于 50000。

3.4. 区块结构

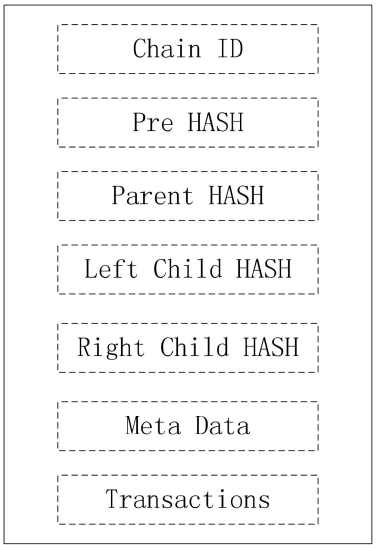

图 2 区块结构

新的区块结构增加了 Chain ID，Parent Hash，Child Hash。

成员说明：

Chain ID：标记区块属于哪一条链，第一条链的 ID 为 1。左子链 ID 为当前 ID*2，右子链 ID 为当前 ID*2+1。

PreHash：本链前一个区块的哈希值。

Parent Hash：父链区块的哈希值，没有时为空值。

Left Child Hash：左子链的区块哈希值，没有时为空值。

Right Child Hash：右子链的区块哈希值，没有时为空值。

Meta Data：其他的区块信息，包括时间戳、签名、矿工地址等

Transactions：交易列表

区块的大小限制默认为 1M[16]。该值只是区块中交易的总大小，不包含区块头信息。

每条链的第一个区块都相同，称其为创世区块。该区块中包含第一个交易，该交易创建了链上第一个智能合约（系统合约），该合约提供了一些系统 API。

创世区块的 Chain ID 为 0。

3.5. 链间区块关系

假设当前链为 Chain2，它的父链为 Chain1。Chain2 当前的区块为 B2.i(B2 表示 Chain2 上的区块，i 表示第 i 个区块)，它的 ParentHash 为 B1.j，要求 B2.i 的时间戳减去 B1.j 的时间戳大于 8 分钟且小于 10 分钟。

时间差大于 6 分钟（区块确认时间），能够确保区块回滚不影响到父链和子链。

时间差小于 10 分钟，是为了能够跨多条链访问数据。跨一条链，最大时间差为 10 分钟；跨 n 条链，最大时间差为 n*10 分钟。只要保证区块时间与数据时间[17]的差超过 n*10 分钟，就是有效数据，能够跨链访问。

---

[16] 该值可以根据需要，动态调整。

[17] 数据有时间信息，具体看后续的数据章节

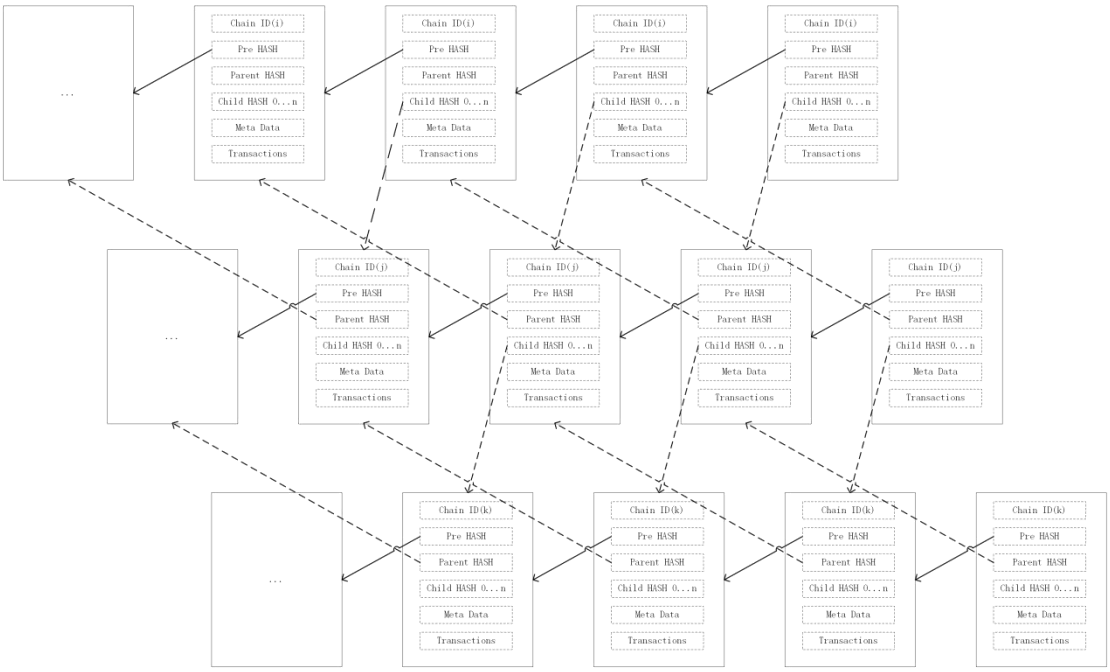

图 3 区块间的关系

上图是简化的三条链之间的区块关系，仅仅是简单示意，实际的父子区块的距离更远，时间差为 8-10 分钟。

区块链的数据不可篡改是通过前后区块的哈希锁定实现的。本项目将其进行扩展到父子链的区块哈希锁定。从而能够实现父子链区块的不可篡改。

通过父子链间的区块哈希锁定，能够保证跨链读取的信息的一致性。

同时限制了父子区块的时间差，这样能够实现跨多链访问，只要通过（链间距离*最大时间）判断数据的有效性。

3.6. 区块间隔

区块间隔：一条链上相邻区块的时间差。

本系统中，时间最小单位为 1 毫秒。

第一条链的区块间隔为 1 分钟，新链的区块间隔降为其父链的 15/16。

新链有更小的区块间隔，出块速度更快。

区块的间隔可以根据需要调整，最大为 1 分钟。

3.7. 区块有效性的校验

校验区块时，如果 Parent Hash 非空，会查询父链中对应区块的信息，如果不存在，则为非法区块，丢弃；存在，判断时间差是否在（8,10）分钟里，时间不对，丢弃；时间正常，获取父区块对应的子链区块，如果子区块不在本链中，表示非法区块，丢弃；都正常，则开始验证区块的其他信息，包括交易等。Child Hash 也是一样的校验。

3.8. 突破单节点性能

前面说过， 一台普通计算机的 TPS 理论上限约为 7 千 TPS。

如果要让整个系统的 TPS 更高，一种方式是使用高性能的计算机，另一种就是将单计算机处理改为多计算机处理。

本系统使用多链方式，链与链可以并行处理，所以可以将不同的链的处理放到不同的计算机上，实现并行处理，避免单节点的硬件、网络等瓶颈。

这样就能够做到系统性能根据链的增加而线性增长。

如果某个节点性能不足，可以新增一个计算机，将部分链的处理转移到新计算机上，从而提升节点的硬件和网络能力。

4. 数据

4.1. 逻辑存储结构

每条链有独立的数据存储文件

每个智能合约都独立的数据存储空间

每个智能合约可以创建多个数据表

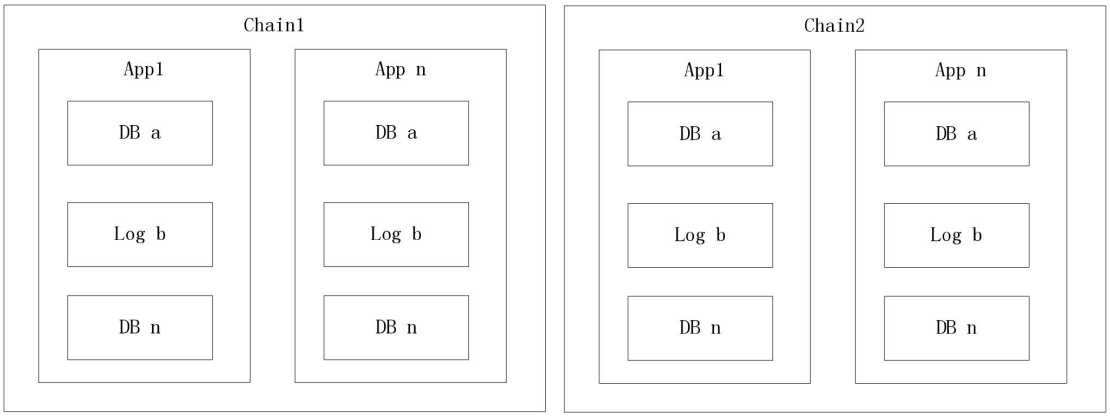

图 5 数据逻辑结构

4.2. 数据类型

所有的数据都是简单的 key:value 形式，key 和 value 都是字节数组。数据的读写都需要消耗 Energy。

DB 型数据：

普通、常用的存储类型，支持智能合约的任意读写。

Log 型数据：

日志型数据，它允许跨链读，不允许覆盖写。

4.3. 数据的生命周期

所有的数据都有生命周期，生命周期越长，需要的 Energy 越多。生命周期终止，数据将被删除。从而可以淘汰无用数据。

日志型数据的生命周期是固定的一年，通过数据的生命周期，可以计算出日志写入时间，跨链读取将以这个时间和区块的时间比较，如果大于 n*10 分钟（n 为两条链的距离），则日志数据是有效的。从而实现可信的跨链数据读取。

4.4. 数据权限控制

数据只能由智能合约读写，其他智能合约未经允许，无法读写该智能合约的数据。

为了方便用户操作，使用智能合约的私有对象作为数据对象，系统通过反射，获取私有对象所属的智能合约和对象名。其他智能合约无法创建和获取该智能合约的私有对象，就无法读写对应的数据。

如果智能合约希望自己的数据能够被其他智能合约读写，需要智能合约主动提供数据操作接口，其他智能合约通过引用该合约，调用相应接口，从而操作相应数据。

智能合约允许读取其他链上相同智能合约的 log 数据，这种方式使智能合约能够跨链转移数据；通过不同的链，并行处理数据。

4.5. 数据回滚

当出现多个矿工挖到同一个区块时，系统会选择算力和最大的区块。出现这种情况时，需要回滚已经处理过的区块，并处理新区块。

当前处理区块时，都会根据区块哈希，创建一个操作历史记录。当需要回滚区块时，将遍历这个历史记录，用旧的数据覆盖当前数据，并删除该历史记录。从而简单的实现区块的回滚。

5. 交易

交易有不同的分类，不同交易有不同的操作码。

这样做的好处就是明确用户行为，简化系统复杂度。

5.1. 操作码列表：

OpsTransfer：用于普通的链内转账

OpsMove：用于链间的转账

OpsNewChain：用于创建新的子链

OpsNewApp：用于创建智能合约

OpsRunApp：用于执行智能合约

OpsRegisterMiner：用于注册矿工（注册过的矿工有算力加成）

OpsUpdateAppLife：更新智能合约的生命周期

5.2. 交易的数据结构

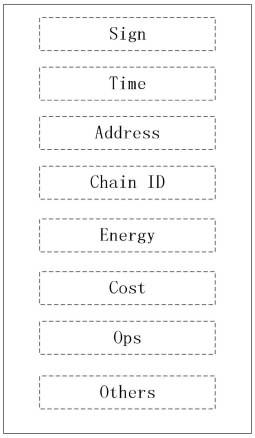

图 4 区块结构

成员说明：
Sign：交易的签名信息
Time：交易的时间戳
Address：交易的发起者
Chain ID：交易所属的链 ID
Energy：交易手续费
Cost：交易的金额
Ops：交易的操作码
Others：不同交易携带的数据

5.3. 交易时效性

区块只允许接收 10 天内的区块，超过时限的区块将被丢弃。
这是因为系统为了代理账户[18]而增加的限制。

5.4. 链间转账

系统默认支持向相邻链（父链或子链）转账，系统处理该转账交易时，扣除发起人相应的代币，并将转账信息记录到 logSync 对象中。

相邻链处理区块时，会读取本链的 logSync 信息，如果信息的时间满足要求，且目标链为自己，则系统自动为转账人增加相应的代币。

链间转账交易被打包进区块后，转账完成时间为 8-10 分钟（链间信息同步时间）

[18] 本系统新增加的一种账户，可以降低账户过度签名的风险。

6. 账户

6.1. 账户类型

孚衍系统的账户有分类，长度 24 字符。

第一个字符用于标示地址的类型。

0x01 为默认的账户

0x02 为代理账户，当账户需要频繁签名时，可以通过代理模式，指定签名代理人，避免自己的账户因过度签名影响账户安全。

0xff 为公共账户，它是公有合约的账户，只有对应合约才能操作该账户。

其他的值将用于后续的扩展需求

每个公有合约都拥有自己的账户，私有合约的账户就是合约创建者，智能合约能够操作创建者的账户。公共智能合约的账户为公共账户，账户只能由对应合约操作。

6.2. 代理账户

如果一个账户，如大公司的对外账户，它不适合经常修改账户地址，但又必须经常签名，过多的签名将严重影响账户的安全性。通过代理签名，那么它每个月只需要授权一次（签名一次），其他都是代理账户进行签名。即使代理账户因为过度签名，导致安全问题，影响也仅仅是被授权的那一个月，后续该代理账户将失效。大大减少主账户的签名次数，从而降低被破解的风险。

代理账户的签名有 2 部分，第一部分为授权签名，第二部分为信息签名。签名信息的长度为普通签名的 2 倍。

授权签名是有时间限制的，授权有效期为一个月。每个签名信息都携带时间戳，通过时间戳，算出授权范围，再根据签名，得到公钥（错误的时间将得到错误的公钥），通过比较公钥是否一致，就能够知道签名是否有效。

6.3. 管理员角色

系统允许公有智能合约注册为管理员合约，管理员合约可以对部分系统参数微调（每次调整 1%）。注册成为管理员和调整参数，都需要花费代币。

可以调整的参数有：区块大小限制，区块间隔时间，预留参数等。

它还可以删除超长时间未使用的账户，该时间最小为 5 年，它由账户中的金额决定。

7. 奖励

7.1. 代币单位

代币单位分别为 t0，t3，t6，t9。

t9=1000*t6，t6=1000*t3，t3=1000*t0。

7.2. 奖励

每次挖矿（生成有效区块），都能够得到代币奖励。

奖励由三部分组成：

a. 默认的区块奖励，第一条链初始为 5000*t9。

b. 历史手续费分成，每个交易的手续费，都有一半会进入系统智能合约的公共账户，用于分发给后续的矿工。

c. 当前交易的手续费，当前交易手续费一半分给当前的矿工，一半进入公共账户。

每个区块生成时，开发团队会自动获得 1%区块奖励和 1%历史手续费奖励。

7.3. 区块奖励递减规则

第一条链的初始奖励为 5000*t9，子链为父链的 90%。

每经过 500000 个区块（约 1 年），奖励降为 90%。

区块的最低奖励为 50000*t0。

系统的代币总量将由链的数量决定，链的数据将由交易的数量决定。所以需求越高，交易越多，链就可以越多，代币总量也就越多。

如果只有一条链，第一年的代币总量为:区块总数：365*24*60，前 500000 奖励为 5000，之后的奖励为 5000*0.9。结果为：500000*5000+25600*5000*0.9(t9)=2,615,200,000t9

8. 智能合约

8.1. 编程语言

使用 golang 作为编程语言（对部分关键字限制，以保证处理的有序性），而不是重新创造编程语言。

golang 是一个简单、易用的编程语言，它有完善的帮助文档和开发工具。它是强类型校验，编译阶段就能够校验发现很多 bug。它是模块化的，本系统能够简单屏蔽外部功能，使智能合约处在简单可预期的环境中。已经有大量的 golang 开发人员，他们如果要开发智能合约，非常容易上手。

8.2. 智能合约的分类

公私之分：

公有合约：它用合约的代码，计算哈希作为合约的名字。它的账户是公有账户。

私有合约：它用合约的代码哈希和用户账户进行二次哈希作为合约的名字，所以不同的人使用相同的代码创建的私有合约都不一样，它的账户是创建者的账户，允许合约操作该账户。

只要是相同的代码，发布的公有合约都有相同的名字。

相同代码的合约，在不同的链上，具有相同的名字，支持跨链访问相同合约的 Log 信息。

功能之分：

可执行合约：该合约允许用户调用，合约有执行入口，默认任何人都可以调用合约。

可被引用合约：该合约能够被其他合约 import，从而组成功能更加强大的合约。

一个合约允许同时拥有这两种功能。

8.3. 智能合约说明

系统要求合约发布的都是源码，任何人都可以看到源码的内容。相比编译后的二进制程序更方便查看、更容易理解。

智能合约发布后，所有的代码逻辑就固定了，通过看懂代码，从而更加信任智能合约。

所有合约都只能 import 链上的其他合约，不允许 import 链外的模块，不支持 import golang 的系统模块。部分会导致程序无序的关键字将被禁止，如 go、select、rang、recover、cap。

每条链都包含相同的系统合约，通过它，能够读写数据（存储），转账等。公有合约只能 import 公有的合约，从而保证任何人都可以将公有合约发布到其他链上。私有合约允许 import 任何合约，不做限制。

发布的合约，将在每个节点上被编译成程序，支持用户调用。

合约的执行需要消耗 Energy，它就是代币，它的消耗根据合约执行的代码行数决定。合约在节点中编译时，会被动态增加代码行覆盖统计，它将作为合约执行手续费的一个依据。

8.4. 跨链读取信息

智能合约可以通过 Log 对象，实现跨链读取信息。接口由系统合约提供，支持跨多条链读取信息。

读取的信息是由另一条链上的相同合约写入的。

日志的时间差必须要大于 n*10 分钟。时间差为当前区块时间-日志写入时间；n 为当前所在的链与日志所在链的逻辑距离（二叉树上从一个点到另一个点的距离）。如果时间不满足，将返回空值。

8.5. 智能合约的性能

一条链上的智能合约的 TPS 性能取决于链的 TPS 性能，单链上合约性能理论上趋近于所在链的性能。

智能合约通过在不同链上发布，使用多链的并行处理机制，实现智能合约整体性能的扩展。

智能合约又可以通过 Log 的跨链读取功能，实现数据的跨链转移。

所以智能合约的极限性能就是整个系统的性能。

9. 理论数据

9.1. 交易大小

普通转账交易：147 字节，若携带信息，会增加

跨链转账交易：139 字节，若携带信息，会增加

创建智能合约的交易：由智能合约的大小决定，系统智能合约有 1800 行代码，大小为 11070 字节

执行智能合约的交易：由携带的数据大小决定，最小为 155 字节

9.2. 单区块包含的交易量

默认区块大小为 1M（不包含区块头信息），第一条链的默认区块间隔为 1 分钟。

如果都是普通转账交易（147 字节），则最多可以有 6802 个交易，则单链的 TPS 为 113。

如果是混合交易，假设平均交易大小为 200 字节，则可以有 5000 个交易，则单链的 TPS 为 83。

系统支持动态调整区块大小和区块间隔，这样就能够提升单链的 TPS 上限。

9.3. 理论性能

第一条链一分钟一个区块，一个区块 1M 大小，交易平均 200 字节，则链的 TPS 上限为 83。

第二、三条链的区块生成时间为 56 秒，它的 TPS 上限为 89。

如果系统只有 3 条链，其他系统参数都不修改的情况下，TPS 上限为 261。

单条链的 TPS 上限依赖于区块大小和区块生成速度，这两个参数都可以通过管理员（智能合约）动态调整，从而提升 TPS 上限。

整个系统的 TPS 上限将随着链的数量增加而线性增加。

链的 ID 为 64 位数字，所以最多可以有 2^{64}-1 条链。

整个系统的 TPS 上限将大于 $83*2^{64}$。

10. 结论

区块链应用越来越广，对区块链的性能提出越来越高的要求。现有的公链都难以满足日益增长的应用需求。随着世界的数字化、自动化，区块链将成为重要的信任通道，具有不可估量的市场前景。

我们提出了一种全新的架构，以系统的高性能为主目标。通过多链并行，可突破带宽、存储等单节点资源瓶颈，实现横向拓展的扩容方案，实现系统的高性能；通过单链前后区块的哈希锁定和父子链区块的哈希锁定，实现数据的不可篡改性；支持动态增加新链，实现系统的可扩展性，从而线性提升系统的整体性能；支持不同的链发布相同的智能合约，合约可以通过跨链读取信息实现跨链通信，从而实现合约的超高性能。

它将成为区块链 3.0 的代表。