中关村区块链产业联盟
ALLIANCE FOR BLOCKCHAIN INDUSTRY · Z-PARK

区块链数据模型技术与应用研究报告

（2023 年）

中关村区块链产业联盟

2023年11月

版权声明

编制说明

组 织 单 位：中关村区块链产业联盟

牵头编制单位：（排名不分先后）

中国信息通信研究院、北京航空航天大学、北京邮电大学、中国联合网络通信集团有限公司

参与编制单位：（排名不分先后）

树根互联股份有限公司

中兴通讯股份有限公司

布比科技股份有限公司

溪塔科技股份有限公司

本体网络科技有限公司

编写组主要成员：（排名不分先后）

刘阳、池程、程彤彤、张钰雯、郭剑南、黄峥、赵正涌、崔婕、胡凝、加雄伟

前　言

区块链技术的集成应用在新的技术革新和产业变革中起着重要作用，全球主要国家都在加快布局区块链技术发展。以习近平同志为核心的党中央高度重视区块链发展，多次强调要把区块链作为核心技术自主创新的重要突破口，明确主攻方向，加大投入力度，着力攻克一批关键核心技术，加快推动区块链技术和产业创新发展。

随着以“数字新基建、数据新要素、虚拟新经济”为核心特征的数字经济发展的全面来临，全球各国和产业界都高度重视区块链基础设施推动数字经济发展的重要动能，欧盟区块链服务基础设施 EBSI、印度国家区块链框架 NBF 等国家级重大工程先后启动建设。“星火·链网”是我国为持续推进产业数字化转型，利用区块链自主创新能力而谋划布局的数字经济“新型基础设施”，以代表产业数字化转型的工业互联网为主要应用场景，以网络标识这一数字化关键资源为突破口，推动区块链的应用发展，发挥实现新基建的引擎作用。

为了进一步凝聚产业共识，推动区块链基础设施规模化发展，启动了“星火·链网”系列报告编制工作，希望能够有助于产业界和学术界凝聚共识，更好地发挥区块链作为基础设施的作用，为技术和产业变革提供创新动力。本报告聚焦“区块链数据模型”方向，通过理清“区块链数据模型”概念，分析“区块链数据模型”核心挑战和发展路径，将有助于推动区块链基础设施与数据模型融合化部署，优化区块链基础设施性能，推动区块链基础设施规模化落地。

目 录

图 目 录

表 目 录

一、区块链数据模型整体概述

随着区块链技术的蓬勃兴起，类似金融、物流及医疗等行业的应用案例借助着其可溯源，安全性和去中心化等特点纷纷加速落地，每个相关行业的不同机构之间可以共同维护和共享参与方的数据，确保每个参与角色都能够对提案进行背书，并通过一定的共识算法和排序服务来促成不同节点上分布式账本内容的一致性。同时，区块链也以其特殊的数据结构，使得区块链具有数据传输以及信任管理的能力。

区块链将数据区块以顺序相连的方式组合成的链式数据结构，并以密码学方式保证的不可篡改和不可伪造的分布式账本。每个区块中的数据可以包括交易信息、合约代码、状态变化等，这些数据的组织方式和存储规则构成区块链数据模型的基础，本文主要针对区块链链上数据模型展开研究。链上数据涉及到区块链如何组织、存储和检索数据，是区块链网络中的数据结构，用于记录和维护交易、合约和其他信息。区块链数据模型的研究影响区块链的性能、安全性和可扩展性，现阶段，区块链数据模型主要体现以下特征:

数据模型作为区块链底层架构保证系统平稳运行。不同于隐私计算，网络技术，跨链技术等区块链的功能基础。数据模型作为一种数据规范，是实现区块链技术的重要基础。区块链技术利用数据模型能够整合各个模型层次的数据，形成统一规范的标准数据库，实现信息技术与垂直行业的打通连接，共同构成数字经济的重要举措。同时，伴随着区块链技术在各行各业的快速布局与应用，规范

化的数据模型更有利于区块链技术的拓展与管理。加速区块链技术的平稳推进。

数据模型作为区块链数据范式保证信息顺利交互。区块链数据模型是保存区块链数据的一套“模具”，把所有的数据，按照“模具”的形状、规格、关系装载起来。优秀的“模具”设计，可以将数据装载的整整齐齐，调理清晰。反之，“模具”设计的不好，数据会存在大量的冗余，杂乱无章；用数据的时候，如同拆解一团乱麻，耗费大量的时间和资源。在数字化不断推进的社会，作为“灵魂”的数据，必须要快速流动与交互。统一规范的区块链数据模型能够有效缓解数据孤岛，子链交互等诸多问题。

数据模型作为区块链数据容器保证信任可靠传输。设备从物理世界收集数据并传输到数字世界，数据的真实、准确、完整、安全是一切数字世界的基础。就公共基础设施而言，错误的数据会导致治理的混乱；就企业而言，混乱的基础数据可能导致预测出现偏差，使竞争走上错误的轨道；由物理属性、实体间交互和未来状态组成的新数据流可以实现在数字世界和物理世界之间无缝交换。数据模型能优化区块链数据的分级授权和共享，依托区块链防篡改、可追溯的特性，可以在保持数据的可信和安全的情况下，实现数据传输。

二、区块链数据模型重点问题

区块链数据可以支持在开放网络环境中的去中心化管理,但是其自身模型设计方面仍然面临着诸多问题。其核心问题体现在数据存储、事务处理性能、查询处理优化等方面。

去中心化存储崛起，导致区块链数据具有差异化存储结构。在区块链系统中,数据以区块作为基本存储单位。为了方便数据的存取,多数区块链系统利用 LevelDB 这一基于 Key-Value 结构的数据库存取数据,而部分区块链系统则选择利用文件系统或关系型数据库进行存储。不同的数据模型对应产生不同的数据存储区域划分及其固化模式，而且与传统的分布式数据库或其他去中心化存储系统相比,区块链网络中的节点均需存储数据的备份,使得数据存储在区块链框架下产生新的挑战。

快速事务执行要求，需要区块链数据模型支持并发运行。在区块链中,智能合约的一次执行相当于数据库中的一个事务。在传统的数据库中,事务处理需满足 ACID 特性（原子性 Atomicity、一致性 Consistency、隔离性 Isolation、持久性 Durability）。在区块链系统中,分布式架构的一致性要求导致事务运行速度大大降低。为了提高系统的吞吐量,部分区块链的数据模型需要支持事务处理并发机制。但是,区块链系统的并发控制与分布式数据库的并发控制相比有诸多不同。一是区块数据模型的差异将导致针对事务的并发控制需要考虑区块的提交方式。二是部分区块链中的事务处理流程与数据库中的事务不同。因此如何设计合适的区块数据模型，对事务的

执行效率有重大影响。

链上查询效率低下，促使区块链数据模型支持快速查询。由于区块链应用于不可信的环境,其查询处理的过程可归类为一般查询处理和可信查询处理。一般查询主要针对的是溯源查询等。可信查询处理对查询结果的验证技术需要数据拥有者产生一个利用私钥生成的签名，后续会利用该签名进行验证。另外,基于传统数据库生成的签名往往基于的是静态数据库，而区块链是一个动态的分布式数据存储系统，合适的区块链数据模型可以有效提高区块链系统的查询效率。

三、区块链的数据模型关键技术

（一）区块链数据模型整体框架

以工业互联网与区块链为代表的新型基础设施逐步成为我国面向未来，打造科技创新驱动、提升数字竞争力的重要保障，也是应对后疫情时代下经济复苏的必要举措。随着区块链技术的不断发展，区块链数据模型的技术价值日益提升。在区块链技术的 5 层体系架构中，数据层定义了各节点中数据的联系和组织方式，利用多种算法和机制保证数据的强关联性和验证的高效性。数据层相当于区块链四大核心技术中的数据结构，即“区块+链”的结构。从初始区块起，区块链系统将一直在新添加的区块，每个区块包含了哈希值、随机数、认证交易的时间戳、交易信息数据、数据签名等，是整个区块链系统中最底层的关键技术。

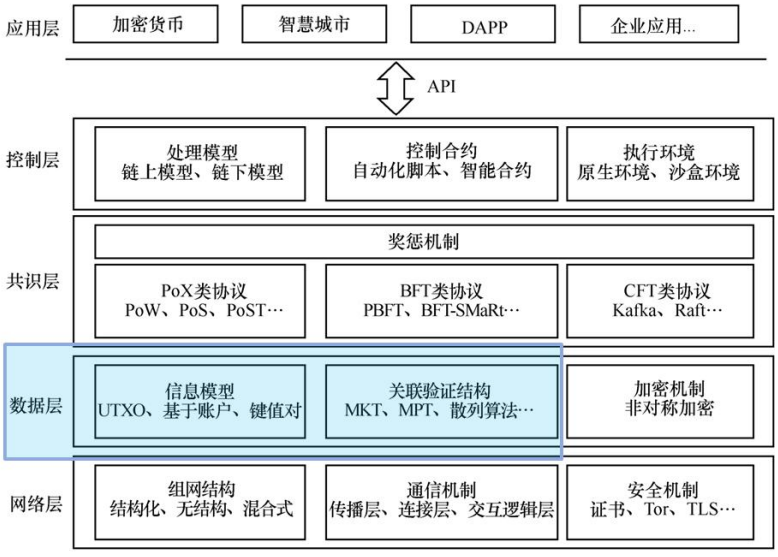

图 1 区块链架构体系

数据层的信息模型是指节点记录应用信息的逻辑结构，区块链的信息模型主要包括 UTXO 模型和账户余额模型。区块链数据的关联

验证结构则是依托区块链的基本数据单位 “区块（block）”。区块由区块头和区块体两部分组成，区块体包含一定数量的交易集合；区块头通过前继哈希连接维持与上一区块的关联从而形成链状结构。基于传统数据层的数据模型要求，在图 2 中，区块链数据模型整体被分为：账户数据模型，区块数据模型以及交易类数据模型。

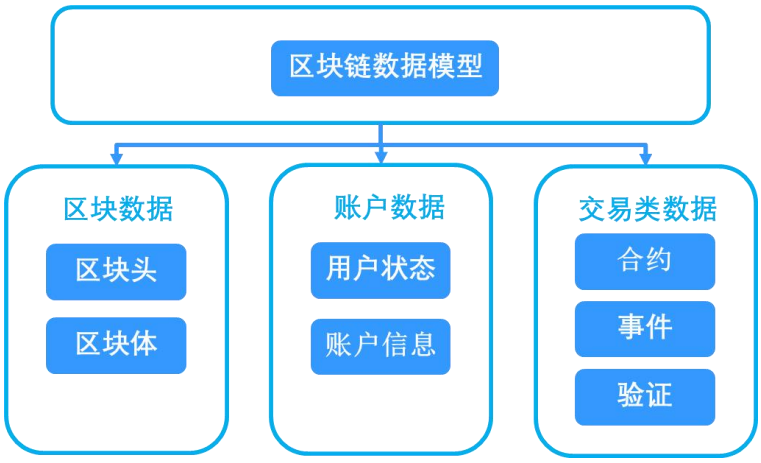

图 2 区块链数据模型分类

尽管现阶段区块链系统拥有不同的数据模型，但任何区块链数据模型设计与实现通常具备以下特性：

数据语义具有完备性：能够完整描述交易过程和结果，包含提交者身份、交易内容等信息，并能通过所有区块重现世界状态。

数据来源具有可验证性：区块头或元数据中包含区块生成信息、哈希链等信息，用于验证区块的合法性与正确性。

数据格式具有可扩展性：区块数据结构中考虑向未来兼容的可能性，通过预留字段或模糊字段等手段，为扩展功能留出空间。

数据结构具有兼容性：区块数据结构出现变更时，能够向下兼容旧版本的节点运行时；同时不同的节点实现能够通过兼容的数据结构进行通信。

（二） 账户数据模型

目前的区块链技术中，账户数据模型主要有两种形式，一种是以比特币为代表的**UTXO 模型**。另一种是以以太坊为代表的基于**账户余额模型**的记账模式。UTXO 模型通过链式拓扑的方式组织所有交易数据的输入和输出，每一个交易的输出最终都能追寻到一个货币源头，也就是当前比特币被挖出时的区块的第一笔交易。比特币通过 UTXO 模型作为其交易信息底层存储的数据结构。基于账户余额模型的记账模式和现在银行卡记账方式类似，通过记录交易者的账户与余额信息从而实现合约事务的顺利进行。

1. UTXO 模型

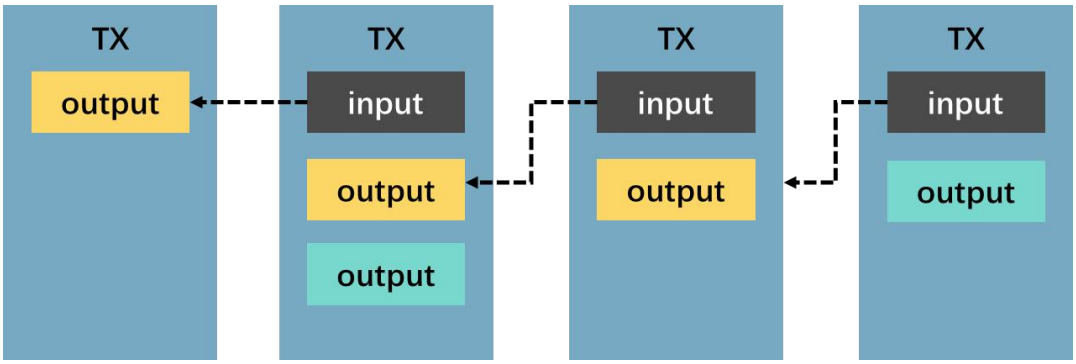

图 3 UTXO 模型

UTXO 模型是未花费的交易输出的记账模型。它是比特币交易生成及验证的一个核心概念。交易构成了一组链式结构，所有合法的比特币交易都可以追溯到前向一个或多个交易的输出，这些链条的源头都是出块奖励，末尾则是当前未花费的交易输出。由于在 UTXO 中没有账户的概念，所以系统可以并行地处理交易，同时不可变的账本能够在比特币节点快速更新时，也能清晰的记录整个网络中每

一笔交易数据的快照，使得整个区块链交易清晰透明。当需要计算某个地址中的余额时，系统会遍历整个网络中的全部相关区块，验证交易与余额。

表 1 UTXO 数据模型的字段描述

字段	名称	描述
版本	Version	交易规则
输入数	Tx_In	交易输入列表的数量
输入列表	Tx_In_List	一个或多个交易输入
输出数	Tx_Out	交易输出列表的数量
输出列表	Tx_Out_List	一个或多个交易输出
锁定时间	Lock time	锁定时间

从结构来看，交易主要的两个单元字段就是交易的输入和输出。输入表示着交易的发送方，输出表示着交易的接收方及给自己的“找零”，在各类区块链浏览器上能看到的输入比特币之和与输出比特币之和之差就是这笔交易的矿工费。由于所有交易的输入必然是前面某笔交易的输出，所以交易最核心的字段是交易的输出。

UTXO 模型的用户利用新的地址用于转账和交易，新地址与原地址之间的关系很难被追踪，更好地保证用户的隐私；UTXO 模型理论上来说可以并行地利用不同的 UTXO 签发多笔交易，并广播到网络中；以比特币为例，在比特币进行交易时，每一次交易的输入值都必须全部花掉，不能只花掉部分。比如，转账地址需要 10 个比特币，输出比特币的钱包地址中只有 10 个比特币，发起一个交易就可以

把比特币转到目标钱包地址中。但钱包地址中有 15 个比特币，那从输出钱包地址中转 10 个比特币至目标地址，同时转 5 个比特币给自身新的钱包地址。

2. 账户余额模型

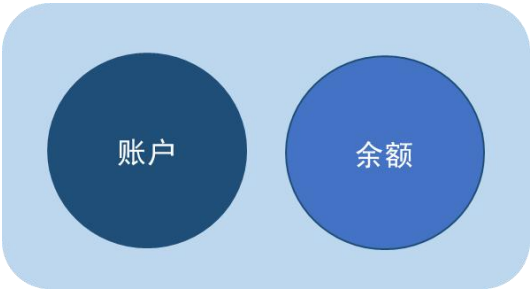

图 4 账户余额模型

账户余额模型：相比于 UTXO 模型，账户余额模型是一种非常容易理解的区块链应用模型，它与我们生活中的账户模型非常相似，只是为了保证账户的安全，使用了签名以及 nonce 的机制阻止恶意的攻击。这种基于账户余额模型的应用包含所有账户余额的全局状态，在进行转账时，需要由节点对账户的余额进行验证，判断当前账户是否有足够的余额进行转账。现阶段，采用账户余额模型的区块链，其包含两种账户：外部账户和合约账户。

外部账户（externally owned accounts），由密钥控制。外部账户创建流程：首先要创建随机私钥（以以太坊为例：64 位 16 进制字符/32 字节）；其次从私钥推导出公钥（以以太坊为例：128 位 16 进制字符/64 字节）；最后从公钥推导出地址（以以太坊为例：40 位 16 进制字符/20 字节）：

合约账户（contract accounts），由智能合约的代码控制。合

约账户不是通过公私钥对控制的。一个合约可以调用另外一个合约，所以要通过 nonce 值记录调用的次数。合约账户不能主动发起交易，所有的交易只能由外部账户发起，外部账户发起交易如果调用合约账户，合约账户可以发送 message 调用另外一个合约，但是合约无法自身发起交易。

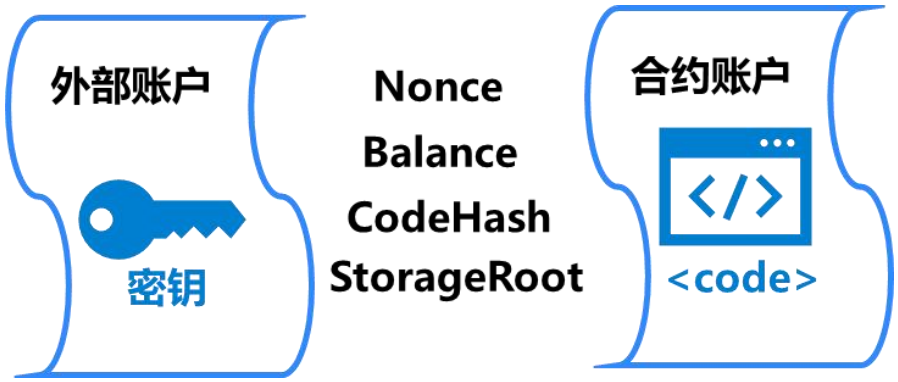

图 5 账户余额模型的账户类型

以以太坊为例，账户模型包括四个字段：一个随机数（nonce）、账户的余额（balance）、存储（storageRoot）、合约代码（codeHash）。

Nonce: 如果账户是外部账户，nonce 代表从此账户地址发送的交易序号。如果账户是合约账户，nonce 代表此账户创建的合约序号。

Balance: 此地址拥有余额的数量。

StorageRoot: Merkle Patricia 树的根节点 Hash 值。Merkle Patricia 树会将此账户存储内容的 Hash 值进行编码，默认是空值

CodeHash: 此账户虚拟机代码的哈希值。对于合约账户，就是被 Hash 的代码并作为 codeHash 保存。对于外部拥有账户，codeHash 域是一个空字符串的 Hash 值。

只有合约账户才有代码，其中存储的是 codeHash。这个字段在生成后是不可修改的，这意味着智能合约代码是不可修改的。

表 2 外部账户与合约账户的区别

项	外部账户	合约账户
私钥	✓	无
余额	✓	✓
代码	无	✓
签名	无	✓
控制方法	私钥	外部账户的合约

账户余额模型的优点在于：每一笔交易都需要有一个签名，交易的输入和输出都是地址，能够节省存储空间；因为创建交易时不需要对过去的 UTXO 进行签名，可以从任何时间点开始同步区块的状态，利于编写轻量级客户端。

无论是 UTXO 模型还是账户余额模型，都能够很好地解决区块链世界中的“安全”问题，保证交易的合法，从原理上杜绝一些可能的攻击行为，实现原理的不同其实也只是由于出发点不同，在设计时权衡了利弊。

（三） 区块数据模型

1.链式结构模型

由区块按照发生的时间顺序,通过区块的哈希值串联而成,是区块交易记录及状态变化的日志记录。每个区块有自己的时间戳，每个时间戳应当将前一个区块的时间戳纳入其随机散列值中，这样就形成了链条。共识算法是为了维护系统中只有一条唯一的合法链，任何分叉链都被视作对系统的攻击。正是基于此种考虑，比特币系统产生新块的时间被设定为 10 分钟,系统需要足够的时间保证新块

被传递给所有的用户节点，保证最长链的产生者会有更多的竞争者，保证系统会有更少的分叉。

区块链的链式结构具有以下优势:

安全性: 区块链的链式结构以其不可篡改性而闻名。每个区块都包含前一个区块的哈希值，这种连接方式使得一旦数据被写入区块链，很难修改。数据的安全性和可信度很高，适用于需要高度安全性的应用，如数字货币和金融交易。

可预测性: 区块链的共识机制通常比较简单，例如，比特币使用的工作量证明（Proof of Work，PoW）和以太坊的以太坊 2.0 使用的权益证明（Proof of Stake，PoS）。简单性使得区块链在运行和维护方面具有较高的可预测性，确保系统的稳定性和一致性。

广泛认可: 区块链的链式结构在过去十多年内得到广泛接受和采用，这意味着它拥有庞大的生态系统、开发社区和支持。这种认可使得区块链容易与传统金融机构、政府监管机构等合作，以实现更广泛的采用。

2.DAG 结构模型

不同于链式区块链中每个区块只能有一个父节点,DAG 结构模型允许每个区块指向两个或者两个以上的区块，容纳了很多分叉，这些分叉共同构成了一幅有向无环图。其次，它允许每个区块只有一个交易，而链式区块链中每个区块中的交易可能多达几千笔，如比特币。最后，DAG 结构中的交易在进入系统之前就已经确立了相互之间的引用关系，该引用关系为交易确立了局部的时间先后关系，而

链式区块链中默认交易之间是无序的，交易之间的顺序是由矿工来随机决定的。

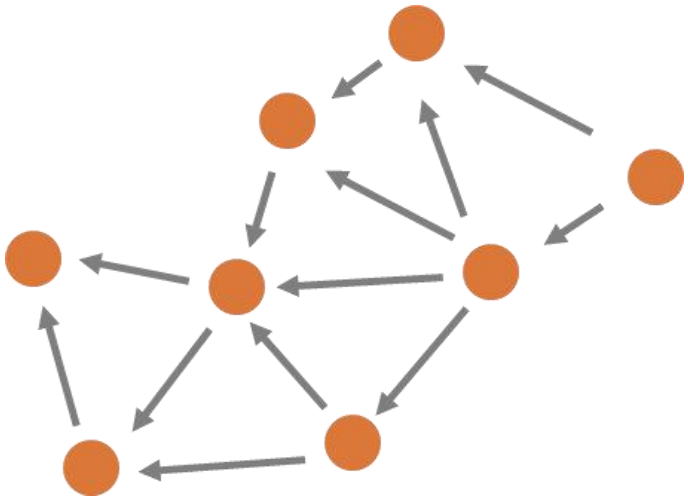

图 6 DAG 结构图

当用户向区块链中添加数据时,所在网络节点创建新的存储单元并将其广播给其他节点,每个单元中必须包含一个或多个先前单元的哈希值(与本单元直接相连的单元称为父单元),这样做的目的是使得各单元之间有序,如果尝试修改其中一个单元,则必须改变它所有的子孙单元,如此就保证了数据的防篡改性。如果沿着父子链的历史单元前进,当同一个单元被多个后来的单元引用时,会观察到很多分叉,当同一个单元引用多个较早单元时,会出现融合,最终形成一个有向无环图(DAG)结构。

链式结构在保证去中心化和安全性的前提下无法大幅度的提高扩展性，导致难以商业化运用。而对于 DAG 结构的区块链，如果网络足够强大，能够大幅度的提高扩展性，采用 DAG 技术的分布式数据库，起步就可以把每秒事务处理（TPS）做到 10 万以上，还能把交易费用做到极低。DAG 技术作为区块链的一个有益补充，其异步通

讯机制在提高扩展性、缩短确认时间和降低支付费用方面优势明显，也是未来去中心化技术领域发展方向之一。

无论链式结构还是 DAG 结构，区块数据是构建区块链系统的核心要素之一， 区块数据中主要包括区块高度、区块哈希、前一区块哈希、区块时间戳、区块发起者、区块签名、版本信息、交易列表、多重签名、随机数、交易总数、默克尔根、其它数据等。

表 3 区块模型的整体结构

名称	类型	含义
HEADER	Byte 数组	区块头，存储区块编号、哈希等信息
DATA	Byte 数组	区块体，存储交易数据
METADATA	Byte 数组	区块元数据，存储签名、交易校验等信息

表 4 区块头数据结构

名称	类型	含义
NUMBER	Uint64	区块编号
PREVIOUS_HASH	Byte 数组	上一个区块的哈希
DATA_HASH	Byte 数组	当前区块的数据哈希
Block Version	Byte 数组	当前区块版本号
Block Timestamp	Unit64	本区块的生成时间刻度
Nonce	Unit64	竞争记账权的 Hash 计算的可变参数
List	Byte 数组	区块中的交易列表

表 5 区块体数据结构

名称	类型	含义
DATA	Byte 二维数组	用于序列化 Envelope 数组

（四）交易类数据模型

交易类数据只要包含交易信息与交易状态信息，其中我们将交易信息也分为交易数据模型以及合约数据模型。

1.交易数据模型

针对交易数据模型信息，主要包括交易发起者标识、交易接收者表示、交易发起者签名、交易内容数据、交易 ID、其它数据等。

交易数据模型通常具备以下特性:

可验证性: 能够通过签名验证交易数据的数据完备性

完备性: 能够通过交易识别发起者、合约标识和合约参数

唯一性: 交易应当具备全局唯一的标识，同时能够使用较低成本防止重放攻击。

表 6 常见交易数据格式

名称	类型	含义	备注
发起者标识	Byte 数组	用于标识交易发起者身份	必选
接收者标识	Byte 数组	用于标识交易接收者身份	必选
发起者签名	Byte 数组	保障交易的真实性	可选
交易时间	Byte 数组	记录交易时间	可选
交易额度	Byte 数组	交易涉及资产的变更数量	可选
处理费用	Byte 数组	交易中产生一定的交易费用	可选
附加数据	String	为部分业务提供的备选字段	可选

2.合约数据模型

合约数据通常指智能合约，是定义为在区块链上运行的应用或程序，简单来说智能合约就是一个确定性的计划，当满足某些条件

的时候它会执行特定的任务。合约数据主要包括合约标识、合约哈希、版本信息、代码哈希、代码信息、合约类型、ABI 描述、合约状态、合约名称、合约发起者、时间戳等，用于记录区块链用户的交易记录。通常，合约的数据模型以外部账户模型为载体，记录的信息与账户数据格式相对应。

智能合约有以下几个特征:

分布式: 智能合约在区块链网络的所有节点中被复制和分发。

一致性: 在满足要求的情况下，智能合约仅执行其预先设计好的操作，而且无论任何节点的执行它的结果都是一致的，

自动化: 它可以自动的执行各种任务，就像是自动程序一样，但是在没触发智能合约的情况下将保持休眠状态，不会执行任何的操作。

不可篡改: 智能合约一经部署就无法再更改了。

表 7 常见合约数据格式

名称	类型	含义	备注
合约标识	Byte 数组	唯一的确定的地址标识，供调用方访问合约的代码	可选
合约版本号	Byte 数组	使用版本号标识不同的版本	可选
合约代码	Byte 数组	经过指定编译器编译生成，供区块链上的虚拟机调用执行	可选
合约存储	Byte 数组	合约执行过程生成的状态数据集合	可选

四、区块链数据模型应用实践

（一） 中国信通院：“星火·链网”账户模型

1.需求分析

区块链经过多年的应用与发展，账户数据模型逐渐成熟，尤其是在智能合约引入之后，对账户数据模型与交易类数据模型的发展起到了正向推动的作用。然而区块链的快速发展，各方建立自身区块链系统，差异化的账户模型结构也给链间数据互通造成了极大的困扰，也对账户模型与交互模型都提出了更高的要求。

2.技术方案

“星火·链网”底层采用“1+N”主从链群架构，基于一条主链打造全链互联互通平台，主链制定统一的跨链数据规范和交互协议，为各区块链跨链交互提供了标准互操作协议，推进链群规范化、规模化建设；各子链之间通过主链实现互联互通、数据跨链互操作，为整个生态发展提供数据共享平台，促进产业发展共促互融。

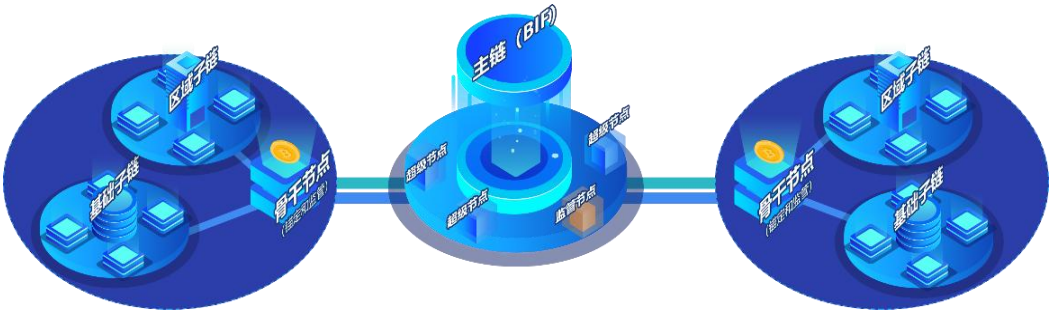

图 7 “星火·链网”整体架构

案例 1 “星火·链网”数字身份服务-星火通
不同于现在的公链，星火链节点和用户都要经过审核后才准入使用星火链功能，星火链的运行受到相关方的严格监管。做星火链应

用开发前，需要了解下星火·链网的帐号，交易和费用等基础机制。星火链帐号采用账户余额模式，其实质为通过非对称加密技术保护的一对公私钥，每个星火·链网帐号都会有以下几个属性:

账户地址，实质为公钥的编码转化结果，只有拥有私钥的用户才能使用对应地址发出交易。一般为星火链网自生基于分布式身份标识产生的 BID 账号，基于密码学算法，用户可以自生成唯一的 BID，作为其身份标识和其在星火主链使用的账户地址，通过自生成的私钥赋予用户链上自主管理身份标识和身份信息的能力。Nonce: 每个账户从 0 开始的计数，代表该账户发起的交易数量，同时用来防止签名重放攻击。 当账号执行一笔交易入链后，无论交易成功还是失败，账号的 nonce 就会加 1。当使用账号发起交易时，需要指定该交易 nonce，其值必须比当前账号的 nonce 大 1，当一个账号被新建时，它的 nonce 为 0。Contract: 标明一个帐号是否是智能合约帐号。Balance: 账户余额。

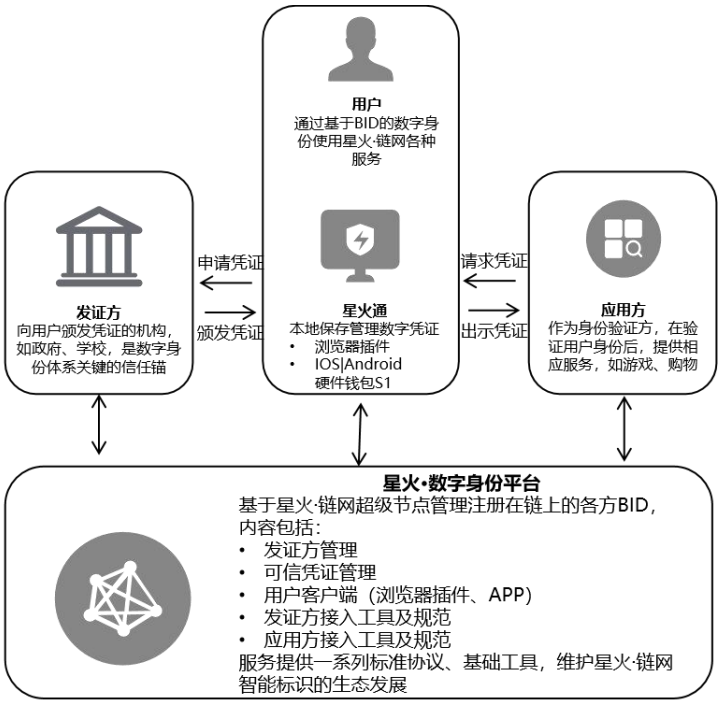

图 8 星火通账户模型示意图

用户实体身份标识存储于主链，凭证等具体的身份信息均存储于链下，用户实体可选择使用星火通客户端，将凭证保存于自己本地，或加密后分片备份至星火超级节点 TEE 可信执行环境，同时，用户实体可将身份信息从本地选择性披露给其他实体。星火数字身份 ID3Entry 为金融、医疗、政务等应用场景提供统一的分布式数字身份服务。

案例 2 “星火·链网”-数字原生资产平台(DNA)

目前星火应用生态处于起步阶段，随着业内区块链应用生态的发展，数字藏品发展迅速。现阶段，国内数字藏品市场处于个平台通过联盟链发行数字藏品的阶段，于用户而言无法通过个人信息查询名下所有数字藏品情况。且数字藏品在流转过程中的平台安全性问题也需要得到解决，所以目前市场需一个能够长期运营并且支撑数字藏品行业发展的区块链基础设施，为了将诸类应用嫁接到星火链网，保证资产创建后的规范性和通用性，参照非常成熟的以太坊 ERC721，开发基于星火链网的数字资产协议标准的数字原生资产平台（DNA）。

图 9 DNA 平台架构

在以太坊 ERC721 基础上，DNA（digital native assets，数字

原生资产）根据星火链网的应用场景进行以下改进:

钱包地址和合约地址为 BID: DNA 协议中用于接收、发送 NFT 的钱包地址和合约地址为 BID，与星火链网钱包相互兼容。最终实现用户注册一次钱包，连接星火链网主链所有应用。

监管功能: 监管方作为去中心化的第三方对 NFT 的合法合规进行监管，监管规则写入“监管合约”中，监管过程全部公平透明。违反监管的 NFT 资产将被“冻结”，“冻结”后不能进行转让。但是监管方无权“销毁”或“转让”用户的 NFT 资产。

每个 NFT 生成一个 BID 身份: 每个 NFT 都会生成一个 BID 身份，用户可以通过解析主链 BID，获取相关信息，如创建 NFT 的合约地址、NFT 名称、tokenId、tokenURI 等。

metadata 格式: DNA 协议中规范了元数据（metadata）的格式内容，避免不同应用方展示 NFT 的信息不一致而混乱。

内容	描述
seriesId	集合 ID
seriesIssuer	发行方
dnaName	数字资产名称
dnaDes	数字资产描述
dnaNumber	数字资产编号
url	数字资产 url
hash	数字资产源文件哈希值
dnaType	数字资产类型
extension	扩展字段，用户自定义

（二）布比科技：区块数据模型实践与应用

1.需求分析

目前，随着区块链技术应用的逐步成熟，区块本身数据模型的设计逐步成熟，区块链性能的突破更多的是在区块本身的连接方式上进行突破，然而，目前区块链的架构大多是单链架构，而单链受限于网络中单节点的性能极限吞吐量总会达到上限，数据多采用链上存储机制，因此无法满足性能、容量及其他要求，基于 DAG 结构的数据模型尽管能在性能上有大的突破，但是技术成熟度依旧不足。

2.技术方案

布比区块链采用多链分片技术，可根据不同业务场景需求对数据做切分，横向提高区块链的吞吐量。多链分片技术是一种“二层扩容技术”，可从一条主链平滑地扩展多条子链，每条链都负责部分计算和存储业务，即链的数量可以随着业务量和数据的增加而增加。主链负责管理子链，保障链的安全性；子链继承主链的安全性，并且承载业务运行，子链的数据增长不会影响到主链及其他子链的效率，有效实现了资源隔离。

案例 3 布比区块链-商用级区块链底层平台
布比打造了完全自主知识产权、高性能可扩展、产品化成熟的商用级区块链底层平台。过去 5 年，经过大量场景验证，布比区块链取得底层技术关键突破：应用开发友好的智能合约、安全高效的共识算法、可靠的隐私保护、并行快速的多链，以及可扩展的跨链技术等创新；同时，经过大量实际业务积累，布比区块链实现了产品化重要突

破：应用可快速构建、可视化运维、技术合规及资金账户体系等，形成完整的产品服务能力。

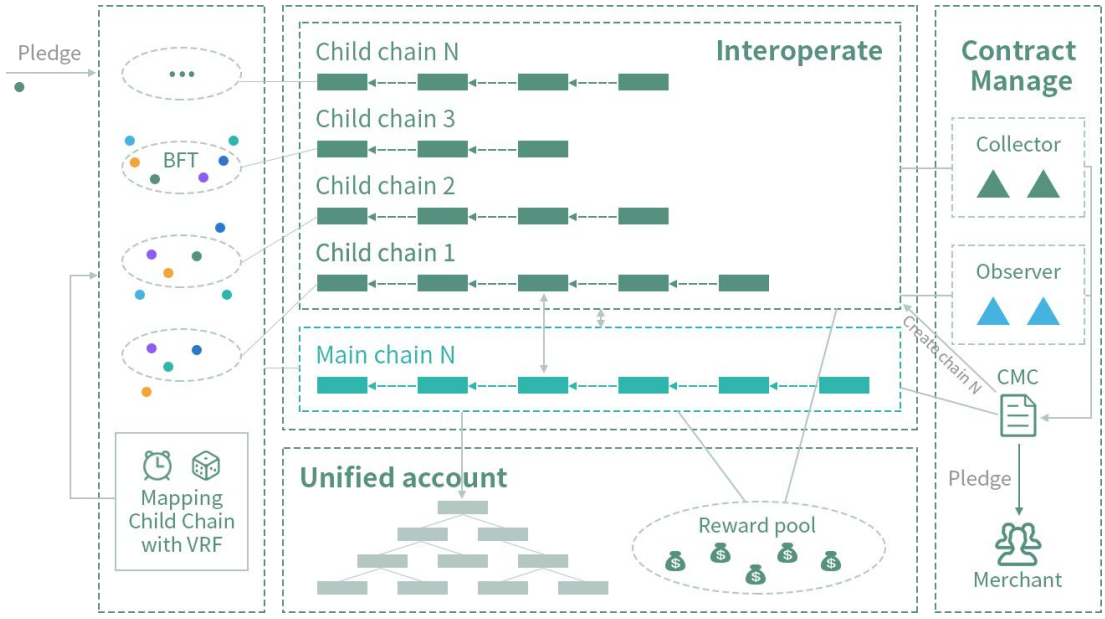

图 10 并行快速的多链分片

布比多链账本通过数据结构的优化实现高可扩展性，具体包括：统一账户结构、区块结构、交易树、收据树等。采用全局统一账户结构，目的是让用户在只生成一对公私钥的情况下，即可在所有链上发起交易，且保证多链之间的交易不会有重放攻击问题。每个账户都有一个账户存储树。账户树包括了从地址到账户状态之间的映射，账户存储树保存了与智能合约相关的数据信息。账户树的根节点哈希值由区块保存，标示了区块创建时的当前状态。

（三）中国信通院：“星火·链网”交易类数据模型

1. 需求分析

随着区块链的不断发展，以太坊的出现首次将区块链和智能合约结合，通过以太坊虚拟机来处理区块链上的交易。 区块链确保了

智能合约的用户在可信的环境下遵循合约规则自动执行合约代码。交易类数据模型页主要体现在现有的智能合约代码中，像任何程序一样，智能合约经常会产生错误。然而，智能合约和常规程序的不同之处在于，智能合约代码中的错误可能会造成巨大的影响。因此，针对合约数据模型的完备设计，是当前区块链交易数据的应用需求。

2.技术方案

“星火·链网”主链提供给用户一体化的智能合约集成开发调试环境，支持不同语言开发的智能合约，让用户更便捷的快速构建基于智能合约的业务共识，不仅具备基本的 IDE 功能，还专门提供了智能合约安全检查服务，同时星火主链同时支持多种智能合约语言及合约引擎，通过执行环境为智能合约执行引擎提供统一的数据访问接口等能力，提供全生命周期管理服务。另外星火主链还提供了多样化的合约模板，让开发者仅填写少量参数即可快速构建安全可靠的智能合约，在执行性能、安全性、多语言支持、开发友好、应用扩展等方面提供更好的支持。

案例 4：“星火·链网”-安全可插拔智能合约基础框架
“星火·链网”自主研发了可插拔的智能合约引擎，提供了一套新的可插拔的区块链智能合约底层引擎，通过可插拔引擎适配器，基于隔离的容器环境，可以支持运行各种主流编程语言开发的智能合约。

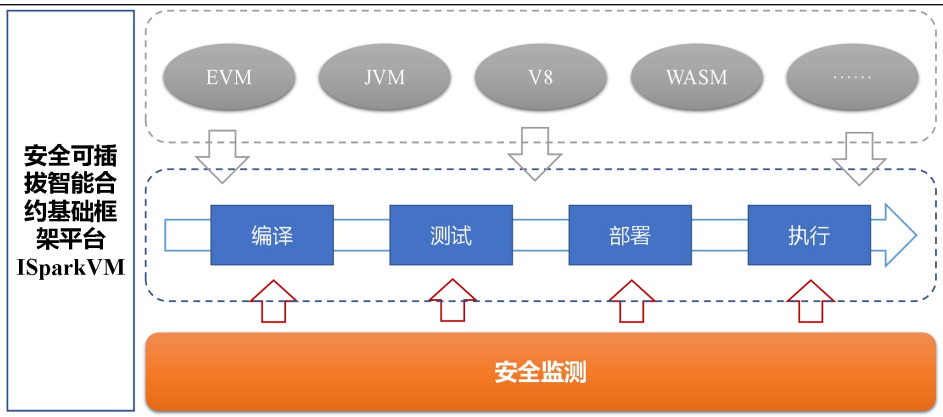

图 11 安全可插拔智能合约基础框架平台 ISparkVM

安全可插拔智能合约基础框架 ISparkVM，可以支持多种智能合约引擎，包括 EVM（支持 Solidity 语言）、JVM（支持 Java 语言）、V8（支持 JavaScript 语言）、WASM（支持 C/C++语言）等。ISparkVM 主要有智能合约编译、测试、部署、执行、安全监测等组件，其中编译组件可以通过编码语言进行自动识别，并调用相应智能合约引擎的编译器；部署和执行组件提供了统一接口便于第三方系统的调用；安全监测组件提供了针对智能合约代码层面可能存在的漏洞监测手段，同时在智能合约执行的过程中也会系统资源进行监测，发现异常会及时告警并处置。

五、区块链数据模型总结展望

区块链作为一个新兴的技术发展方向和产业发展领域，持续的获得了广大产业的关注，推动区块链的发展需要认清现阶段区块链面临的问题，现阶段区块链依旧处于快速发展阶段，加速区块链数据模型与新技术的适配融合，打造产业新模式推动技术变革，依旧是广泛讨论的话题。除了要进一步加快区块链与互联网、工业互联网深度融合，还要进一步与隐私计算、物联网等技术相互融合，通过融合技术区块链数据模型应用范畴，共同促进下一代信息技术的发展，促进实体经济“降成本”“提效率”，构建“诚信产业环境”。

（一） 强化区块链数据模型与隐私计算融合，推动数据隐私安全

区块链数据模型适配性设计，可以有效的支撑隐私计算，可实现多节点间的协同计算和数据隐私保护。大数据背景下存在的数据过度采集、数据隐私保护等问题可以通过区块链与隐私计算结合解决。利用合适的数据模型构建区块链底层架构确保计算和数据可信，基于隐私计算实现数据可用不可见，两者相辅相成，实现更广泛的数据协同。

（二） 加速区块链数据模型与物联网技术融合，实现数据安全可信

基于现有的工业互联网国家顶级节点作为工作基础，以既有的应用实践探索新模式。在融合物联网设计的数据模型基础上，进一

步将数据模型跟物联网进行融合，有利于构建更加包容的协同网络，通过区块链的不可篡改、共识机制以及去中心化等功能特性，实现物联网设备安全防护，实现物联网数据的隐私保护，解决传统物联网存在的设备信任与数据安全等问题。

（三） 推动区块链数据模型与传统技术融合，加快可信数据应用

区块链的应用呈现“一点突破，多点开花”的发展态势，目前应用领域已经拓展到工业制造、能源行业、物流行业、食品行业、智慧政务、智慧医疗、产品溯源、供应链金融等众多领域。针对不同领域的区块链数据模型，建立统一的数据模型库，是打破数据沟通阻碍的重要手段。

中关村区块链产业联盟

地址：北京市海淀区学院路 51 号首享科技大厦 2 层

邮编：100083

微信公众号：中关村区块链产业联盟