基于双区块链的信息记录安全存储与共享

张朋伟　涂昳颖
（江西交通职业技术学院，江西 南昌 330013）

摘要：在物联网、互联网的推动下，双区块链技术创新方面的投资量逐渐提升，为信息安全存储与共享技术的实现提供了重要支撑。随着产品、服务、商业模式的创新浪潮席卷全球，铁路企业要进一步引起对双区块链技术应用的重视，通过数据技术创新夯实自身发展基础。本文首先以高速铁路接触网供电监测数据为例，分析双区块链技术在信息记录安全存储与共享的应用优势，然后结合相关实践经验，探析相关数据信息处理平台的搭建与该技术应用的未来发展趋势。

关键词：双区块链；信息记录；存储；共享

双区块链技术是信息时代的特有的产物，其在信息记录安全存储与共享中的应用，有效满足了现代交通信息工程中的各个主体在数据制作、使用、查看、保密等方面的需要。经过技术升级之后，双区块链的去中心化、开发性、可追溯性特征得到显著强化，对交通信息记录安全存储与共享的支撑作用实现了进一步提升。

一、双区块链技术在信息记录安全存储与共享的应用优势

（一）提升数据安全性和可视性

以双区块链技术为工具，对信息数据流进行管理、交互，可以大幅度提高数据在传输过程中的准确性、完整性及安全性，相关主体准确掌握供电数据信息。

（二）扩大服务对象

双区块链技术具有数据可追溯、易分割、不能篡改等优点，链上部门可以通过区块链进行数字化操作将相关信息数据进行拆分、转发，这有效扩大了相关主体获取数据的安全性和便捷性，提升了信息记录的服务对象。

（三）强化风险管理

首先，双区块链技术具有共识机制上的优势，是一种基于数据记录与共享需求而发展起来的服务，实现了多方交差验证，促使数据真实性得到更为充分的保证。其次，双区块链技术具有可追溯优势，可以使产生的网供电监测数据记录更为清晰，方便企业进行风险管理。

二、基于双区块链的高速铁路信息记录安全存储与共享

（一）高速铁路联盟链感知节点分布框架

1. 感知节点分布框架

基于双区块链的感知节点分布框架主要包括前一区块、区块头、区块体以及后一区块等几个部分。区块头主要包括前一区块的 Hash 值、时间戳、随机数以及目标哈希，其中当前区块的目标哈希值是利用哈希（Hash）计算方法，根据前一区块的块头进行计算获得，如此设计区块头感知节点分布框架，能够使所有的区块组合成依赖前一个区块的不可篡改但可追溯的链，从而有效降低信任成本。Merkle 树可以利用哈希过程，根据这些数据信息形成唯一的 Merkle 根，并储存到区块头。区块体是数据存储的机构，其中主要存储的内容是当前区块在交易过程中所拥有的数据交易量以及验证通过的区块在新建时所产生的数据交易记录。把区块链技术应用到铁路供电网等分布式数据存储中，可以有效防止的数据结构遭到篡改，提升相关数据储存的安全性。

2. 区块链分类

在高速铁路信息记录系统中，可使区块链按参与方分类，并将其分为私有链、联盟链以及公有链。参与主体可以对这些区块链上的信息进行匿名访问，它们的区别主要体现在中心化程度、参与主体控制以及其中所储存信息的公开程度三个方面。其中，私有链采用了单中心设计方法，中心控制者可以规定参与成员身份，其中所储存的信息是向公司内部公开的；联盟链采用了多中心设计方法，参与主体的控制权需要建立在预选认证节点上，其中所储存的信息是向联盟内部公开的；公有链采用了去中心化设计方法，可以在任意节点接入控制权限，其中所储存的信息是完全公开的。对于高速铁路 WSN 感知节点来说，双区块链技术在铁路用电监测信息采集与储存中的应用，可以帮助系统较为有效地抵御恶意篡改、单点失效攻击以及重放攻击等常见攻击行为，有效提升了区块链结构的安全性和灵活性。

3. 联盟链感知节点

联盟链 SN 分布框架主要由机房、传感器、采集基站负责区域等构成。在目前高速铁路供电线路上，以 3 公里为一个间隔，配置一个包含无线网络及专用网络的通信机房。该机房以铁路供电系统为电能来源实现运行，因此可以不计其能量损耗。但是需要关注的是在铁路供电线路上，非共识传感器的共识节点在工作中必须把采集到的供电监测数据向上传输到机房进行分析。因此在铁路供电数据监测过程中为了降低逐跳通信中刹那生的能量损耗，需要将全部的机房设置为联盟区块链的预选节点（DS）。分析常用联盟链感知节点分布框架可知，周边 1–2 公里范围内的全部 SN 只需要将采集到的数据传输给 DS 即可。

（二）高铁供电监测数据的安全存储

1. 基于联盟链的数据存储

基于联盟链的数据存储系统信息储存安全性更高，在数据存储过程中，它不会依赖 WSN 中唯一的可信任中心节点对有关数据的进行保存。因此可以利用联盟链技术，在预选铁路沿线建设供电监测数据采集基站（DS），利用这些节点完成存储数据、验证、共识以及公开审计。作为整个系统实现双链存储的核心，各个 DS 之间需要竞争将数据传输至区块链的写入权。针对区块链上各个部分在系统中发挥的作用，需要为其设计监测中心、采集基站以及传感器感知节点等实体。其中，SN 需要完成监测数据的采集与传输，同时对于监测目标需要满足系统删除或加入节点的基本要求。另外采集基站（DS）由控制器与本地存储模块构成，需要完成对周边 SN 传输的感知数据的收集，并且能够验证 SN 的真实性与合法性。

2. 系统的初始化

借助哈希信息验证码（HMAC）技术，系统能够完成初始化任务。技术人员则需要为 SN 装置智能嵌入式设备，使其在经过 MC 的身份认证之后，成为 WSN 许可感知节点，并取得该节点的地址信息 loc 与属性集合 type。被 MC 认证为合法之后，DS 即可获得相关权限和信息，并完成数字签名、数据加密以及对 SN 的验证工作。

3. 双链数据存储模型

联盟存储链基于预选节点建设的防篡改的点对点（P2P）、集体维护、去中心化网络。各个预选节点(DS)之间需要进行对等计算，即在成功实现一次共识之后，每个参与计算的节点都会同样拥有区块链副本，通过这种方式可以避免在某一个节点被非法攻击时，因该节点所储存数据的丢失、篡改导致整个无线传感器网络的数据收到安全威胁，是当前避免因非法攻击造成的接触网供电监测数据失效的常用手段之一。

（1）传输监测数据。在系统进行初始化完成以后，验证完成的感知节点 SN 需要从其本身所在的 DS 中，把计算后产生的最新数据区块索引复制，该索引指明了各监测数据存储的具体有效位置。

（2）监测中心。监测中心拥有最高权限，它需要完成整个系统的初始化任务，并且在工作过程中不可以被第三方掌握。在监测数据聚合模块，SNi 需要将上传数据内的时间戳交给 DS 加以验证，以有效避免重放攻击；通过验证之后，再通过 SNi 的 PKsi 对 HMAC 的身份加以认证，以确认其身份合法性；接着把 SNi 认定的合法数据保存到存储区域；在某一个时间周期的节点上，借助 DSi 把该时间段内的所有监测数据进行聚合，然后给聚合起来的数据加一个时间戳进行标记，完成监测数据的数字签名，进而确保有关监测数据的合法性；之后在下一次共识过程把相关数据录入区块链。

（3）数据区块上链，即把在 DS 之间共识过程中生成的数据区块连接到存储联盟链，完成数据写入工作。

（4）数据存储双链，这是一个数据计算与储存过程。由于该系统是在区块链数据结构中对各条数据进行哈希计算，所以能够把数据的哈希值录入到 DS 存储池。在数据区块中，处于最后位置的每一种类型上链数据的哈希值均都可以与 type 结合，实现标记；在数据存储中不同类型的 last data hash 都需要遵守一定存储规则进行存储。将在当前计算过程中产生的数据哈希值记为 parent hash。当把产生的监测数据录入区块链以后，parent hash 则会转化为当前区块中相应类型的 last data hash，等待下一个数据处理环节。经过一段时间的积累之后，根据 hash 值把相关监测数据单独构建一条 hash 链，这个 hash 链能够标记各条历史数据的位置，而且它是以依附的形式存在链上，故而具有不可篡改或者伪造的特性。

4. 共识算法

在铁路供电线路中需要按照规定设置通信机房，也就表明在本存储联盟链系统中所设置的共识节点也是固定不变的，一般情况下不会出现有节点删除或新节点加入的情况。在监测数据安全存储系统设计任务中，可以忽略不计节点的动态变化，若遇到由于特殊原因确需更换 SN 的情况，技术人员可以在监测中心进行整个系统初始化的时候完成身份认证。因此，当前的铁路运营系统中多选择拜占庭（PBFT）算法共识机制完成区块共识。在个算法中，主要包括主节点广播区块、从点验证区块、从节点确认和比较以及主节点反馈等四个数据处理阶段。第一，在主节点广播区块这一阶段的主节点是 DS，该阶段主要是负责把新数据区块、数据区块的哈希值，以及数字签名等信息数据传递给相应的从节点，为查验工作的开展提供依据。第二，在从点验证区块这个阶段，负责对每个节点发送给主节点的数字签名，并且对数字签名加以验证，再对这些交易数据进行分析执行。当完善所有交易过程以后，根据交易结果，对于新的区块哈希摘要进行计算，且需要加上数据数字签名，随之把相关数据信息反馈给整个区块链安全存储网络。第三，进入到从节点确认和比较阶段，在该阶段，所有节点对接收到的哈希摘要、交易结果进行整理与汇总，形成新的信息数据，并发送给主节点。第四，进入主节点反馈的阶段，在这一阶段所有主节点对收到的消息进行整理。如果从节点总共发送给主节点 commit 消息 2f+1 条，那么主节点就可以把从节点审计结果和新区块记入到本地状态数据库与区块链，需要对已经验证通过的新数据区块进行数字签名。并将数字签名后的数据反馈给从节点之后，这个数据区块将会根据时间顺序存储到联盟链之中。

三、基于双区块链的信息记录安全存储与共享技术发展方向

（一）进一步技术创新

在未来的双区块链技术应用中，将更加注重隐私保护、跨链技术、密码算法以及共识机制等方面区块链核心技术的创新。当前，双区块链在这方面的应用尚缺乏完美的生态系统，铁路企业需要通过合理的激励机制吸引参与者，并进行全面布局，加强对监督管理、配套设施、标准化工作、商业模式探索、技术研究方面的探索。鉴于中国区块链标准体系尚且处于缺失状态，链上不同主体之间的沟通成本较高，相关信任机制相对复杂，影响了该技术在信息安全存储与共享方面的广泛应用，铁路企业可以建立一个统一的应用标准化体系，以提升不同主体之间的信息沟通效率，拓展双区块链技术在供电监测数据处理中的应用。

（二）构建完善的监管合规机制

针对双区块链技术的监管措施还处于相对空白的阶段，政府需要针对该项技术的应用现状与发展趋势，建立健全新模式的责任识别机制。对于信息安全存储与共享来说，明确责任与底线，是促进区双块链正常运行、保障数据安全、促进铁路科技创新的关键。相关监管机构应以自治原则和技术原则为基础，清晰国家对链上企业与平台运营商的权力界限，并尽最大可能做到保持政策的一致性以及尊重技术中立。此外，还要将基于双区块链技术的创新形式纳入监管，对相关准入机制加以明确，支持、鼓励更多安全可靠、有远见的企业投入到双区块链技术创新中。

四、结语

总而言之，随着运营监测数据种类的增多、数据量的增大，双区块链技术的应用优势将得到进一步凸显。相关技术人员要意识到，运营监测数据储安全将直接影响铁路事业的进一步发展，并积极探索技术创新的新方法、新方向，从而更为有效地解决数据篡改、恶意伪造等问题带来的不利影响。

参考文献：

[1] 李鹏 . 基于双区块链技术的数据共享平台的实现 [J]. 网络安全技术与应用，2022（01）：64-65.

[2] 朱颖婷，杨立鹏，单杏花 . 基于双区块链技术的旅客联程运输数据共享和售票方案研究 [J]. 铁道运输与经济，2022，44（04）：16-21

[3] 孟文出 . 双区块链技术如何解决身份信息管理难题 [J]. 计算机与网络，2022，48（02）：39.

[4] 张利华，蒋腾飞，姜攀攀，李晶晶，张朋伟 . 基于区块链的高速铁路监测数据安全存储方案 [J]. 计算机工程与设计，2020，41（04）：933-938.

课题项目：2020 年度江西交通职业技术学院科技项目“基于区块链和 SMS4 的高速铁路接触网供电监测数据安全研究”（课题编号：2020KY09）