doi:10.11835/j.issn.1000-582X.2020.245

联盟链技术在特种设备健康检测体系中的应用

赵 辉,文俊浩,黄秋子,周 巍,杨正益
(重庆大学 大数据与软件学院,重庆 400044)

摘要:特种特备健康检测监测云平台的建设正在开启整个行业“服务化”的进程,建成之后或将在服务重用、服务沉淀上取得良好的效果。“服务化”带来优势的同时也带来一些挑战,因其需要进行远程服务调用并共享部分行业数据,服务调用过程中的数据安全性以及隐私性保护成为文章关注的焦点。文章提出基于联盟链技术建立特种设备健康检测体系生态,通过联盟链弱中心化的特征以解决服务调用过程中的数据安全及隐私性保护问题,进而一定程度上对服务安全性和隐私性提供保障。

关键词:特种设备;联盟链;智能合约;服务安全;服务隐私
中图分类号:TP311.5 **文献标志码**:A **文章编号**:1000-582X(2020)07-001-05

The application of consortium blockchain in health inspection system for special equipments on service security and privacy protection

ZHAO Hui, *WEN Junhao*, *HUANG Qiuzi*, *ZHOU Wei*, *YANG Zhengyi*
(School of Big Data & Software Engineering, Chongqing University, Chongqing 400044, P. R. China)

Abstract: The construction of special equipments, health detection and monitoring cloud platform starts the process of “service” of the whole industry, which can achieve a lot in service reuse and service precipitation. However “service” brings advantages as well as some challenges. Since it requires remote service calls and needs to share some industry data, data security and privacy protection during service invocation become a major problem, the solution of which is the focus of this paper. The establishment of the special equipment health detection system based on the consortium blockchain technology was proposed to solves the data security and privacy protection problems in the service invocation process, providing protection for service security and privacy to some extent.

Keywords: special equipments; consortium blockchain; smart contract; service security; service privacy

互联网行业中“服务化”的概念快速普及,从企业服务总线(ESB, enterprise service bus)到远程过程调用(RPC, remote procedure call),再到微服务,随着服务的沉淀和持续发展,服务已然成为各行各业发展中的“基础性”资源。近年来,特种设备建设规模日益扩大,电站锅炉、气瓶、储罐、起重机械等特种设备设施数量快速增加[1],随之设备的安全问题也日益突出,其正常安全地运行不仅关系到国民经济的正常发展,而且

收稿日期:2019-12-10
基金项目:国家重点研发计划资助项目(2018YFF0214706)。
Supported by the National Key Research and Development Program of China (2018YFF0214706).
作者简介:赵辉(1994—),男,硕士研究生,主要从事服务计算、区块链等研究。
通讯作者:文俊浩,男,教授,博士生导师,主要从事软件工程研究,(E-mail)jhwen@cqu.edu.cn。

更关乎人民生命财产安全。特种设备的健康检测体系显得尤为重要。文中拟打造一个特种设备健康检测监测云平台,通过与全国各地多个“节点”相连为其提供数据分析、检测监测、设备健康管理等协同服务体系。在这种情况下,平台的建设打破了传统“烟囱式”的系统建设方式,通过构建行业业务中台和数据中台并实现服务重用的方式降低了服务的维护成本和难度,不必付出重复的服务建设与维护成本,更有利于服务的沉淀和持续发展。但是,随之而来的服务安全和隐私性问题也引发了行业的担忧。部分特种设备数据属于机密数据,在服务调用过程中,如何保证数据的安全性、完整性,部分数据对其他节点的不可见性[2]等服务安全和隐私问题成为一个亟待解决的问题。

1 相关技术介绍

1.1 区块链与联盟链

区块链,是随着比特币等数字加密货币的日益普及而逐渐兴起的一种全新的去中心化基础架构与分布式计算范式,颇似一个分布式的公共账本。区块链技术作为继蒸汽机、电力、互联网之后下一代革命性的核心技术,是因为自身不可篡改的特性从根本上改变了信任方式。区块链技术的发展解决了数据的信任和安全问题,具有去中心化、信息不可篡改、自治性、开放性、匿名性五大特点[3]。

区块链实则是几种技术方案的统称,其包含公有链、私有链、联盟链三大分支。在整个公有链系统中,没有角色拥有对系统的绝对控制权,不依赖于中心化、层级化的结构,每个参与的数据块都拥有平等的权利和义务,共同地维持数据更新。在区块链公有链上的每一个数据块都拥有同等的权利,这使得每一个数据块都能够获得完整的数据备份,所有在链上的数据都是公开和透明的,公有链对所有节点无授权机制。私有链只对个人或单独的实体开放,其数据区块的产生不需要每个节点都进行验证,这一特点赋予了私有链具有极好的隐私保障以及区块生成速度快、成本低的特点。

联盟链区别于公有链,其采用多中心的方式,可通过预先设定参与节点、权限控制等方式成为介于公有链和私有链的“中间态”产品[4]。联盟链具备以下4个特征。

1.1.1 弱中心化

与公有链不同的是,联盟链在某种程度上只属于联盟内部的成员,通过共识机制确认,因联盟链的节点数量是相对有限故极易达成共识。

1.1.2 可控性较强

公有链一旦形成区块,则具备不可篡改的特性。由于公有链的节点是海量的,只有拥有全网51%及以上的计算资源才具备篡改区块数据的可能,现阶段无法完成。而对于联盟链,只要所有机构中的大部分节点达成共识,即可将区块数据进行更改。

1.1.3 数据不会默认公开

不同于公有链,联盟链的数据只限于联盟里的机构及其用户才有权限进行访问。另外,为有效管理联盟节点数据并保障数据安全,可为联盟链中的多个节点分配不同的私钥、公钥对区块数据进行加密[5]。

1.1.4 交易速度快

联盟链本质上还是私有链,由于其节点数量相对较少,达成共识容易,故区块的形成速度相较于公有链提高很多。

联盟链在保留了公有链的部分特点后依托于特定范围内多个网络节点互联的业务场景可最大程度上发挥出联盟链的价值。特种设备健康检测监测平台可依托联盟链构建联盟链网络,如图1所示。

其中特种设备健康检测体系中的中台服务集群提供了大量的服务,Fabric网络为底层区块链网络,在每次生成新的区块时,需要进行权限校验,IPFS配合Fabric做区块链数据存储,API Service则提供对外的服务接口[6]。通过联盟链可实现将到达服务的请求数据对联盟外的任意节点隔离,使其不具备读写权限。另外,针对不同服务间的差异性,联盟链中还存在多个管道,针对不同的服务以及节点本身的特点每个管道中的节点存在一定差异性。而同一管道中的区块数据会进行同步操作,管道中的节点无法同步其他管道中的区块数据,故可通过管道实现数据隔离,保障到达服务的请求数据无法被非授权节点获得。

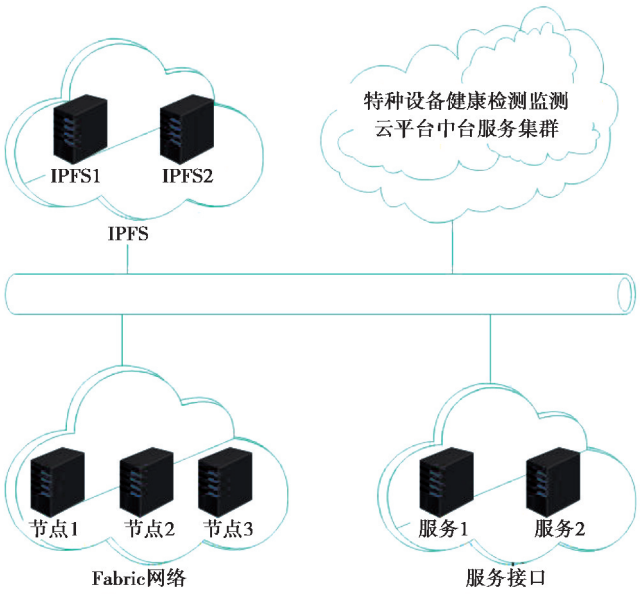

图 1　联盟链网络

Fig. 1　Alliance chain network

1.2　智能合约

智能合约是一段运行在区块链系统中的代码，也是一套数字形式的承诺。运行在区块链系统上的节点都必须遵循其相应的规则。相较于传统的程序代码，智能合约程序具备一些特殊的“品质”。第一，在联盟链中同一个通道(channel)中的节点共享数据，即智能合约处理的数据是公开透明的。第二，得益于区块链采用的密码学算法，智能合约的执行痕迹无法被篡改，不可伪造，不可抵赖[7]。第三，智能合约具有永久运行的特质，只要区块链网络中有一个节点在运行，智能合约就不会停止。第四，对于每一次加入区块的数据，智能合约都会在权限范围内的所有节点上运行同一段程序以进行准确性校验，故可保证写入区块中的数据为正确的数据，有效实现了数据的一致性。在特种设备健康检测监测平台中，智能合约一方面能通过上述特征保证数据的隔离、不可篡改等特性，另一方面，还可以在智能合约中实现更小粒度的权限控制。进一步在服务调用的过程中保障数据的隐私性，进而更好地保障服务安全与隐私性保护。

2　技术应用

2.1　联盟链在服务安全方面的应用

在特种特备健康检测体系中，通过建立联盟链的方式在一定程度上保障在服务调用过程中的数据安全性，进而为服务安全性提供保障[8]，防止在调用服务过程中数据被非法读取或篡改等。

首先，联盟链具有部分去中心化的特征，从某个程度来讲联盟链只属于联盟内部节点，进而保障了联盟链外的其他节点无法读取或篡改区块上的数据，在实现了数据隔离的基础上一定程度保障了数据的安全性和完整性。另外，由于区块链在联盟链中只有同一通道内，2/3 以上的授权节点同意后才可修改区块信息，故一定程度上可保证数据的不可更改性与完整性，同时数据修改可追溯等。

在特种设备健康检测监测云平台中，部署了数据分析、检测监测、设备健康管理等服务。平台和相应节点在同一个管道内，某节点的服务调用过程简述如下：

1)节点将发送至服务的请求数据写入联盟链中；

2)特种设备健康检测监测云平台通过定时任务读取联盟链中的新数据并调用对应的服务接口；

3)服务处理新的请求数据；

4)特种设备健康检测监测平台将服务输出结果写入联盟链中并调用对应节点的接口发送消息通知；

5)节点读取联盟链中服务器写入的数据信息。

在上述过程中，平台与节点间的信息交互借助联盟链来完成，极大程度上保证了服务调用过程中数据的安全性、完整性、一致性等，同时该过程也存在实时性较差的特点，适用于对实时性要求不高的服务调用场景。

2.2 联盟链在服务隐私方面的应用

在服务调用过程中，数据的安全性、完整性等固然重要，部分数据的隐私性保护也在联盟链中得到了较好的体现。由于联盟链具备多通道的特点，可将互相信任并可呈现敏感数据信息的节点加入同一通道中，通道中的节点方可具备读写及共享数据的条件，数据信息对通道外的节点则不可见。另外，通道内的节点可以进行更小粒度的权限配置管理，节点可在智能合约中进行权限校验[9]，只有被授权读操作权限的节点才有资格读取数据信息。同理，只有被授予写操作权限的节点才有资格写入数据信息。

在特种设备健康检测体系中，针对服务调用过程中数据的隐私性保护，节点在联盟链中的部署规则为：

1)同一个行政省的节点部署在同一个通道中，可在一定程度上打破数据壁垒实现数据共享的基础上，保障了服务调用过程中数据的隐私性，进而保障服务隐私；

2)同一个节点可在多个通道中重复出现，增加灵活性，可根据实际场景决定数据的共享情况；

3)同一个通道内的不同节点具有不同的读写权限，可根据节点的级别进行权限的个性化设定，在增强隐私性保护的同时满足业务场景需求。

3 系统设计

研究以同一通道内的节点与特种设备健康检测监测云平台中台服务集群的交互为例，系统架构如图2所示。

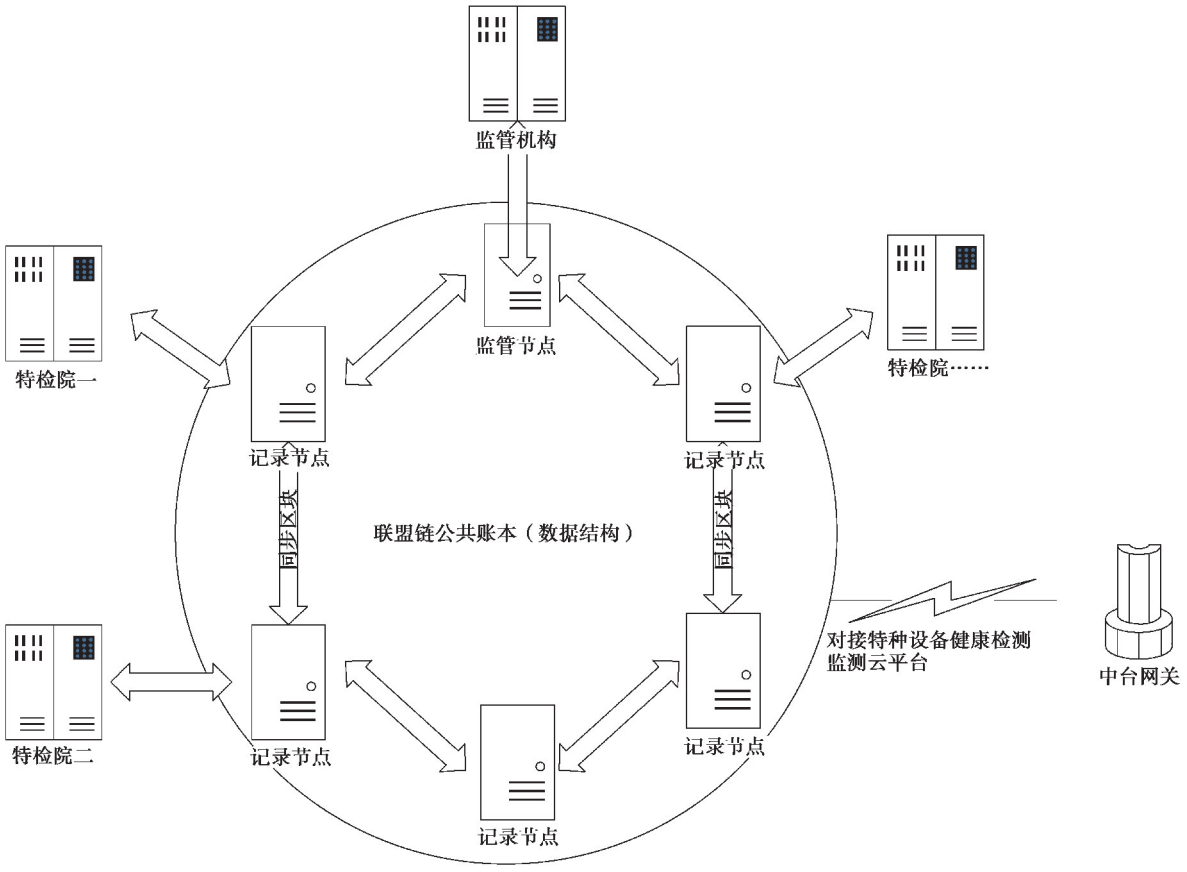

图2 系统架构

Fig. 2 System architecture

系统将从以下几个方面设计：

1)搭建联盟链网络，引入各地特检院、云服务平台中台服务集群等机构共建联盟链(数据存储结构)。

使用通信信道加密保证节点通信安全，使用可插拔的共识算法，如PBFT、RAFT等实现高效的节点共识，使用零知识证明、同态加密实现隐私数据保护[10]。

2)设计智能合约模板。由于不同类型的设备、不同的系统服务类型交互的数据具有不同的特点。例如电站锅炉健康检测服务，主要根据设备当前状态值与健康状态阈值等指标进行评测。系统通过抽象出通用要素设计为父合约，将个性化要素设计为子合约，通过父合约调用子合约可实现灵活的智能合约模板，进而

实现灵活的业务场景[11]。

3)链下系统和链上系统相结合的方式[12]。某些系统服务需要进行大量的计算、数据处理等，耗时可能大于区块生成时间，此类相对复杂的业务可链下执行，而利用链上智能合约做正确性证明，减少链上业务处理压力。

特种设备健康检测监测云平台通过数据可信任，永久记载、安全保护引入联盟区块链，一方面，联盟链的鉴证证明功能，可以帮助特种设备健康检测系统、数据中台和业务中台的运营更加透明化[13]。另一方面，联盟链技术去信任化操作，过程相对透明，帮助实现部分自动化服务，效率更高。

4　未来展望

在区块链技术中，公有链因其完全去中心化以及数据的透明性等特征，在数据私密性上存在较大的限制。私有链因其强中心化的特征，其通常情况下适用于内部组织架构的企业或个人，在使用范围上受限严重。而具有弱中心化特征的联盟链或将成为未来区块链技术发展的主流形态[14]。文中主要阐述了基于联盟链的服务安全及隐私性保护在特种设备健康检测体系中的应用，现在还存在部分限制，如针对部分对实时性要求较高的复杂服务请求场景则不够友好[15]。但是随着计算资源的进一步普及以及区块链技术的逐渐成熟，联盟链技术在各个行业中将会得到更好的应用，取得更好的落地效果。当然，联盟链技术也或将在各个行业的服务安全及隐私性保护上得到长足的发展。

参考文献：

[1] 庄淑淳. 特种设备安全法规标准体系现状与发展[J]. 中国标准化，2018(10)：248-249.
ZHUANG Shuchun. Status and development of special equipment safety regulation standard system [J]. China Standardization，2018(10)：248-249.(in Chinese)

[2] Yu D，Jin Y，Zhang Y，et al. A survey on security issues in services communication of Microservices-enabled fog applications[J]. Concurrency and Computation：Practice and Experience，2018：e4436.

[3] Reyna A，Martín C，Chen J，et al. On blockchain and its integration with IoT. Challenges and opportunities[J]. Future Generation Computer Systems，2018，88：173-190.

[4] Crain T，Gramoli V，Larrea M，et al. (Leader/randomization/signature)-free byzantine consensus for consortium blockchains[J/OL]. Computer Science，2017.[2019-10-25]. https：//arxiv.org/abs/1702.03068v2.

[5] Zhang A，Lin X. Towards secure and privacy-preserving data sharing in e-health systems via consortium blockchain[J]. Journal of Medical Systems，2018，42(8)：140.

[6] Shen H，Xiao Y. Research on online quiz scheme Based on double-layer consortium blockchain[C]// 2018 9th International Conference on Information Technology in Medicine and Education (ITME). Washington，DC，USA：IEEE Computer Society 2018，6：956-960.

[7] Zhang Y，Kasahara S，Shen Y，et al. Smart contract-based access control for the Internet of things[J]. IEEE Internet of Things Journal，2018，6(2)：1594-1605.

[8] Zhou B，Shi Q，Yang P. A survey on quantitative evaluation of web service security[C] // IEEE Trustcom 2016/ BigDataSE/ ISPA. IEEE，2017.

[9] Qi L Y，Meng S M，Zhang X Y，et al. An exception handling approach for privacy-preserving service recommendation failure in a cloud environment[J]. Sensors，2018，18(7)：2037.

[10] Sifah E B，Xia Q，Agyekum O B O，et al. Chain-based big data access control infrastructure[J]. The Journal of Supercomputing，2018，74(10)：4945-4964.

[11] Ying W C，Jia S L，Du W. Digital enablement of blockchain：Evidence from HNA group[J]. International Journal of Information Management，2018，39：1-4.

[12] Xia Q，Sifah E，Smahi A，et al. BBDS：blockchain-based data sharing for electronic medical records in cloud environments [J]. Information，2017，8(2)：44.

[13] Eyal I，Sirer E G. Majority is not enough：Bitcoin mining is vulnerable[J]. Communications of the ACM，2018，61(7)：95-102.

[14] Dorri A，Luo F J，Kanhere S S，et al. SPB：A secure private blockchain-based solution for distributed energy trading[J]. IEEE Communications Magazine，2019，57(7)：120-126.

[15] Zhang H K，Lu Z H，Xu K，et al. Artificial intelligence platform for mobile service computing[J]. Journal of Signal Processing Systems，2019，91(10)：1179-1189.

（编辑　詹燕平）