iiotTrust® 产品白皮书

基于区块链的工业互联网协作存证平台

（版本：2.2）

北京远景视点科技有限公司
2019-11

前言

随着以物联网、云计算、大数据、区块链、人工智能等为代表的新一代信息技术与传统产业的加速融合，以及“中国制造2025”战略的实施，我国已经进入工业智能化建设的高峰期，关键基础设施互联互通的需求正不断增强，工业互联网建设及关键基础设施互联互通的速度已经超出了人们的预期。一系列新的生产方式、组织方式和商业模式不断涌现，正推动全球工业体系的智能化变革。作为新工业革命的关键基础设施，工业互联网代表着国家新一代信息基础设施重要发展方向，已经成为涉及国家经济命脉的工业体系的神经中枢。

和传统互联网一样，工业智能化和工业互联网的发展也伴随着严峻的安全挑战，在工业互联网领域，网络攻击已经可以将破坏行为从虚拟世界转移到现实世界，大量关系到国计民生的关键基础设施以及工业网络面临攻击威胁。因此，加强关键基础设施及工业网络的安全防护能力、威胁感知能力至关重要。区块链技术的去中心化分布式网络，节点共识强一致性，数据防篡改可追溯等特性，可以为工业互联网设备间的安全通信、安全协作提供有效保障，iiotTrust 基于区块链技术，面向工业互联网应用场景，为解决此方面问题提供产品级解决方案。

什么是工业互联网

工业互联网是全球工业系统与高级计算、分析、感应技术以及互联网连接融合的结果，是工业智能化发展的关键综合信息基础设施。工业互联网包含了工业控制系统、工业网络，同时也包含了大数据存储分析、云计算、商业系统、客户网络等商业网络基础设施。“信息技术承载的商业网络(IT, Information Technology)”与“操作技术承载的工业网络(OT, Operation Technology)”之间的连通构成了“工业互联网”**[1]**。

在工业互联网中，IT/OT 融合已成为必然趋势。IT/OT融合，是指以数据计算为核心的信息技术(IT)系统和以监控事件、过程、设备并在企业和工厂生产中做出调整的操作技术(OT)系统的融合。诸如无线传感器和执行器网络(WSAN)之类的传感器和连接系统越来越多地被纳入工业环境的管理，如水处理，电力和工厂的管理。而商业网络的信息系统中也越来越多地整合设备通信、日志检索、执行计划等控制界面。信息自动化、通信和网络在工业环境中的整合是日益增长的工业物联网(IoT)的组成部分。

工业互联网的特点

工业互联网的特点可以从两大视角来分析，工业企业：由内及外，渐进、改良、升级，生产系统的智能化；互联网企业：由外及内，变革、颠覆、重构，商业系统的智能化。两者之间的关系如图 1 所示。

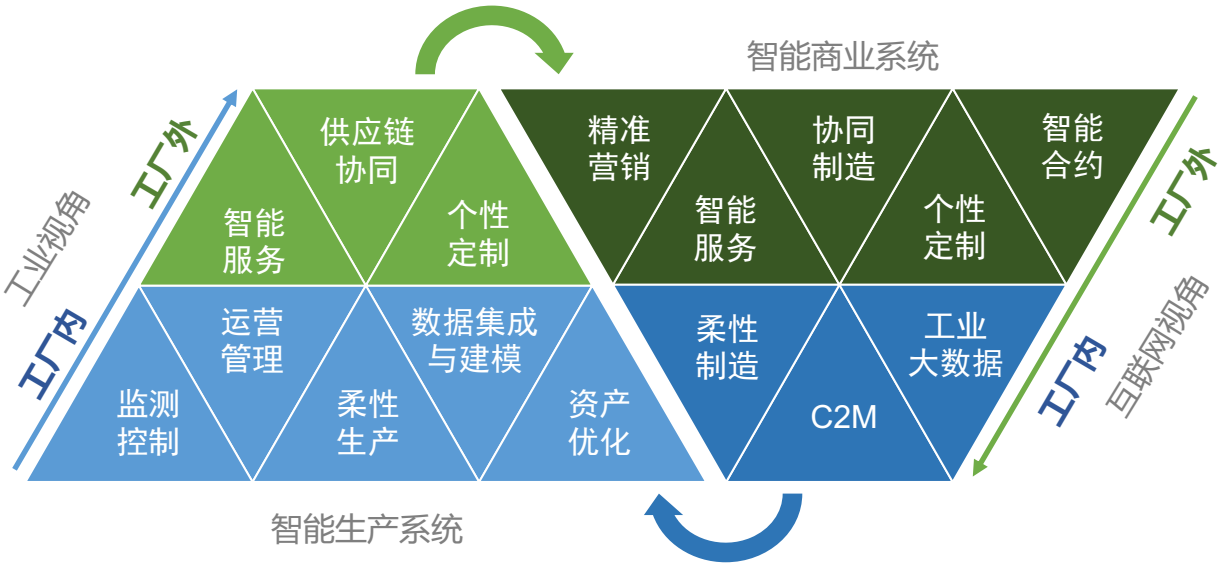


图1

工业企业和互联网企业具有类似的发展趋势和特征，智能化不断提升，逐步向智能生产系统和智能商业系统迈进。同时，工业企业和互联网企业的信息物理系统、安全共享、安全组织、安全市场的融合加速了 IT 和 OT 的一体化。

工业互联网安全挑战

工业智能化和工业互联网的发展既是我国经济变革的难得战略窗口期，又面临着严峻的安全形势挑战，工业互联网安全显得尤为重要。网络攻击日益加剧，甚至恐怖主义威胁已逐步渗透到工业控制领域，加强关键基础设施及工业网络的安全防护能力和威胁感知能力迫在眉睫，保护国家基础设施安全已经刻不容缓。与此同时，世界大国都在谋求网络战略优势，掌握网络空间控制权、规则权和话语权，网络对抗和网络攻击事件愈演愈烈，网络空间博弈加剧，信息安全已成为国家地区间博弈的主战场。

2009年，震网（Stuxnet）电脑病毒攻击了伊朗铀浓缩工厂的工业控制系统。震网通过USB驱动器引入到单个机器中，攻击分为两个部分。首先，

为了掩盖其行为，病毒秘密地记录了正常的工厂操作。然后，将这些正常数报告给操作员，在正常反馈数据的掩护下，它开始发送错误指令，破坏984个浓缩离心机，使它们失去控制。整个攻击使浓缩效率降低了30%**[2]**。2012 年 12 月，震网病毒攻击美国 Chevron 等 4 家石油公司。根据 RISI 数据库统计，发生在工控领域的安全事件与涉及的工业行业，数量明显增多**[3]** ，如图2、图3 所示。

图2

图3

工业网络(OT)对信息安全的需求不同于商业网络(IT)，商业网络保密性优先级最高，其次是完整性、可用性。工业网络(OT)则有明显的不同，工业网络更为关注的是系统设备的可用性、实时性，除此特点外，IT 系统和 OT 系统之间仍然存在很多差异性，如表 1 所示**[4]**。

分类	**IT系统**	**OT系统**
可用性需求	可重启、热切换	高可用（不能重启）、计划性中断、重要系统冗余
管理需求	保密性、完整性、有效性、隐私	人身安全、有效性、完整性、保密性、隐私
体系安全焦点	IT资产及信息、中央服务器更重要	边缘设备与中央设备一样重要
未预期的后果	安全解决方案围绕典型的IT系统进行设计	安全工具必须先测试以确保不会影响ICS的正常运作
实时性交互	交互时效可有弹性，可实施严格限制的访问控制	实时性、紧急响应，访问控制不能妨碍必要的人机交互
系统操作	典型的操作系统、自动部署、持续升级	专有的操作系统、无安全功能、软件变更须验证
资源限制	近3~5年主流硬件，有性能冗余	按需设计，可能10~20年前的设备刚好够用
通信	标准通信协议、有线、无线	专有标准，异构、难互操作

表1

由于 IT 系统和 OT 系统之间存在的众多差异，当工业互联网的 IT/OT 进行融合时会带来很多安全挑战。

(1)攻击面越来越大工业互联网 (IIOT, Industrial Internet of Things) 端点的增加，给工业控制系统 (ICS, Industrial Control System)、数据采集与监视控制系统 (SCADA, Supervisory Control And Data Acquisition) 等工业设施带来了更大的攻击面。与传统 IT 系统相比较，IIOT的安全问题往往把安全威胁从虚拟世界带到现实世界，可能会对人的生命安全和社会的安全稳定造成重大影响。

(2)工业设备资产的可视性严重不足阻碍了安全策略的实施。要在工业互联网安全的战斗中取胜，“知己”是重要前提。许多工业协议、设备、系统在设计之初并没有考虑到在复杂网络环境中的安全性，而且这些系统的生命周期长、升级维护少也是巨大的安全隐患。

(3)IT 和 OT 的安全管理仍然互相独立操作困难，很多企业的 IT 和 OT 是完全独立的，两支团队无法高效地合作，难以满足 IT/OT 一体化的安全需求。

iiotTrust为工业互联网提供可靠计算

在工业互联网的应用场景中，终端设备受计算性能、存储空间等物理限制，一般无法运行复杂安全协议及算法。此外，由于物理空间环境的限制，设备传感器通常采用蓝牙、ZigBee、Wi-Fi、Lora 等无线通信技术收发数据指令，区别于有线网络，无线传感网络(WSN, Wireless Sensor Networks)基于其开放的特性，更易受到安全攻击,如何保证工业互联网中数据的安全和可靠成为了一个重要的问题**[5]**。

层	攻击类型
物理层	阻塞攻击（Jamming） 无线电干扰（Radio Interference） 篡改（Tampering）
数据链路层	持续信道消耗（Continuous Channel Exhaustion） 碰撞攻击（Collision） 非公平竞争（Unfairness）
网络层	槽洞攻击（Sinkhole） 黑洞攻击（Black Hole） 女巫攻击（Sybil Attack) 方向误导攻击（Misdirection）
传输层	失步攻击（De Synchronization） 洪泛攻击（Hello Flood）
应用层	分布拒绝服务攻击（Distribute Denial of Service）

表2

iiotTrust作为采用区块链技术的协作存证平台，具有防篡改、可追溯、强一致性和去中心化等特性，可以为工业互联网场景下IT/OT融合提供一个可靠的去中心化通信网络**[6]**，工业互联网上各节点之间的控制、协作数据可以通过“交易(TX, Transaction)”的方式记录到区块链网络中。

iiotTrust主要包括以下几点核心特性:

1、去中心化，iiotTrust区块中的数据可以通过多个站点、不同地理位置或者多个机构组成的网络进行分享。所有网络成员都可以获得与其他成员内容一致的唯一、真实数据副本。区块中的任何数据改动都会在所有的其他网络成员的副本中被反映出来。

2、共识机制，iiotTrust区块中所存储数据信息的安全性和可靠性是通过公钥、私钥以及签名来保证，从而实现密码学层次上的一致性维护。根据

网络中达成共识的规则，区块中的数据可以由一个、部分或者全部参与者共同进行更新。网络中的参与者根据共识原则来制约和协商对记录的更新，不需要将信任托付给中间的第三方机构。

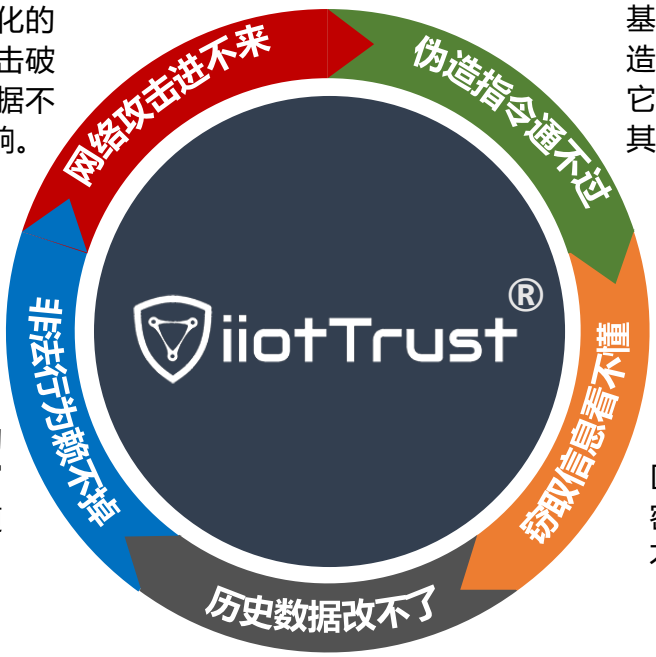
3、不可篡改，iiotTrust中的每条记录都有唯一的时间戳和唯一的密码签名，这使得区块数据成为网络中所有交易的可审计历史记录。任何网络成员对数据的修改必须根据共识机制与其他网络成员达成一致方可以完成。

iiotTrust的核心优势

以区块链的技术特性为依托，iiotTrust为多方设备之间的数据安全协作提供了一个新的选择。在工业互联网场景下，区块链可以有效的解决协同制造设备之间的协调和信任问题，在提高效率的同时降低安全风险，与传统的数据中心化方式相比，区块链采用去中心化的网络结构，提高了交易的透明度，避免权力过度集中的中心结构发生腐败和欺诈的可能性**[7]**。同时因为区块账本由所有网络成员共同维护，所以单一网络节点受到攻击并不会对账本本身造成重大影响，有利于保护整个分布式网络稳定性和安全性 。

区块链为非中心化的分布式网络，攻击破坏部分节点的数据不会对整体产生影响。

基于节点共识机制，伪造的指令，无法通过其它节点的确认，因此将其写入区块链中。



所有通信指令均以TX的形式写入区块链，可随时进行审计。

区块链通过密码学加密技术确保敏感数据不会被非法访问。

区块链中的历史数据均带有时间戳和密钥签名，通过共识机制确何数据无法被修改。

iiotTrust产品架构

iiotTrust区块链协作存证平台内置基于pBFT算法的共识模块，支持面向业务的智能合约。此外，平台支持多协议接入API，可轻松实现物联网设备和应用系统的接入，同时提供支撑日常运营管理的认证授权、平台管理、区块浏览等功能模块。

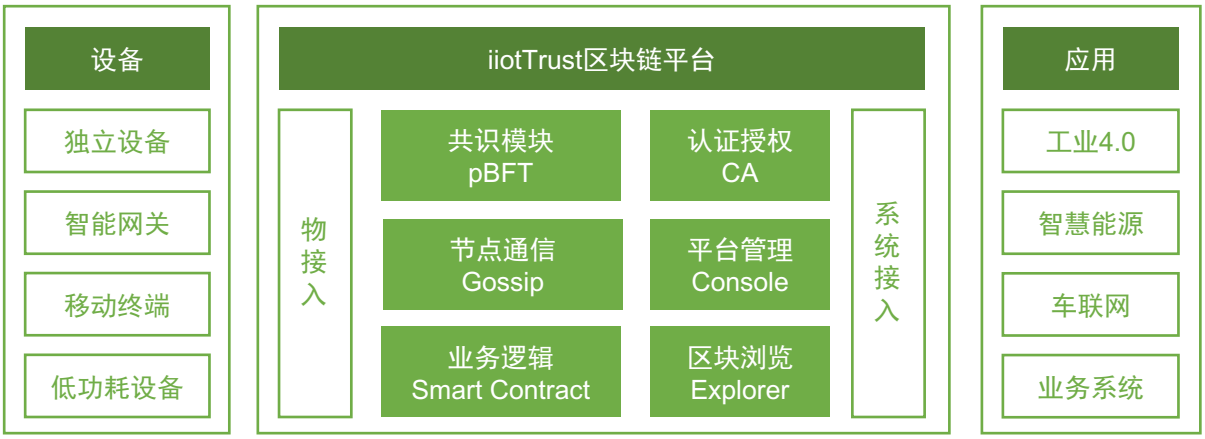


图4

iiotTrust应用场景

1、指令安全通信，通过iiotTrust发送通信指令，节点间的共识机制可确认下发者的身份、内容真实可靠，通过密码学算法确保关键信息仅特定接收方可读取。

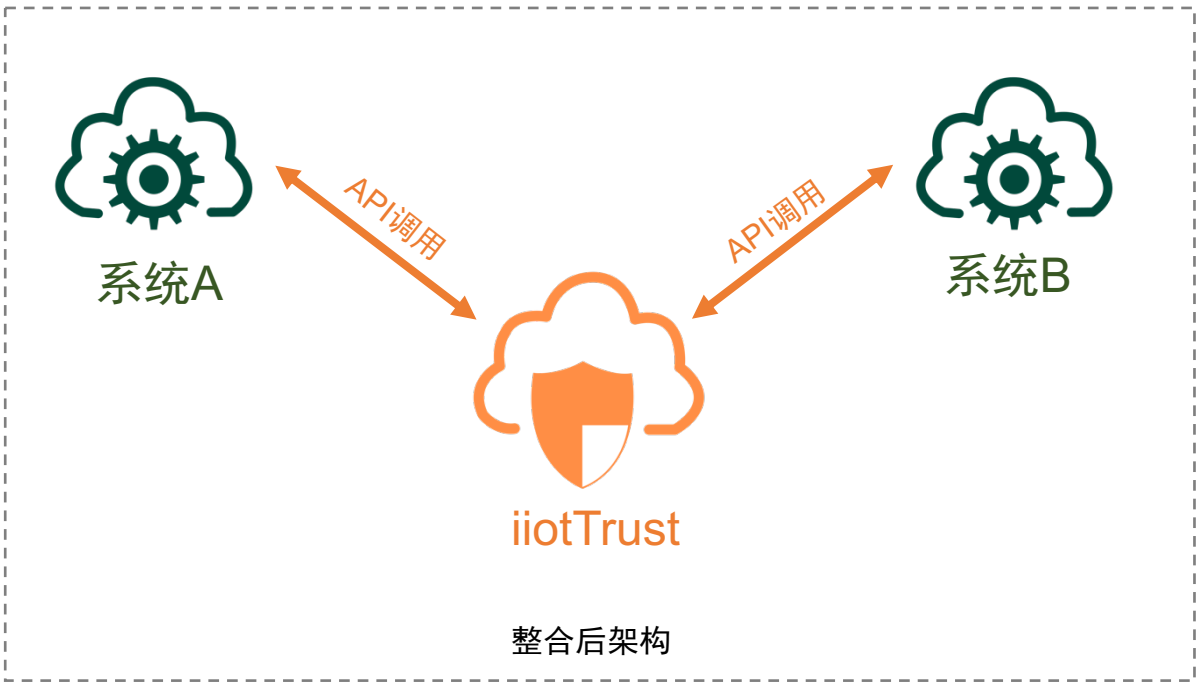
2、组织间通信存证，所有经iiotTrust区块链进行通信协作的信息，在各节点间均不可篡改，并永久保存，组织间的关键业务流转，记录在链上，可以根据业务需要进行追溯。

3、风控及审计，利用区块链的不可篡改特性，可以将iiotTrust接入客户的业务系统，将操作人员的操作行为记录在链上，并通过智能合约来充当规则引擎，对异常操作行为进行识别。同时利用不可篡改的特性，可对操作人员的操作历史进行合规审计。

4、接口调用配额管理，iiotTrust记录在区块链上的信息是以“交易”的形式进行存储的，因此，可以在iiotTrust上发行内部流转的Token（通证），可以设计为每次交易都消耗一定量的Token，并可以追溯每次配额消耗对应的交易记录，从而精确控制接口调用操作次数，防止接口滥用。

iiotTrust与原有系统的整合

iiotTrust自身支持MQTT、REST、RPC、Kafka等广泛接入方式，对原系统业务逻辑无侵入，仅需适配原有系统的通信接口，最小化系统改造，降低企业实施成本。



原有系统整合iiotTrust后，可以令系统间通信指令不可篡改、历史记录追溯可查，关键信息可加密。整体提升IT、OT系统间的协作安全性及可靠性。

参考文献

[1] 工业互联网产业联盟(AII). 工业互联网体系架构[R]. 北京:工业互联网产业联盟, 2016.

[2] D. Kushner, “The Real Story of Stuxnet,” IEEE Spectrum 53, No. 3, 48 (2013).

[3] Industrial Security Incidents Database (ISID) [EB/OL].http://www.risidata.com/

[4] 陶耀东，工业互联网IT/OT一体化的安全挑战与应对策略[J]，《电信网技术》,2017年.11期

[5] Volker Skwarek, Blockchains as security-enabler for industrial IoT-applications[C]. Asia pacific Journal of Innovation and Entrepreneurship. Vol.11 No.3, 2017:301-311

[6] WangH, OsenOL, LiG, et al. Bigdata and industrial internet of things for the maritime industry in northwestern norway[C]. TENCON 2015-2015 IEEE Region 10 Conference. IEEE, 2015:1-5.

[7] Azaria A, Ekblaw A, Vieira T, et al. MedRec: Using Blockchain for Medical Data Access and Permission Management[C]. International Conference on Open and Big Data. IEEE, 2016:25-30.

PROINSIGHT
远 景 视 点

北京远景视点科技有限公司
http://proinsight.io
010-56222080
biz@proinsight.io