

Blockchain Based OT Monitoring Solution (BBOTMS)

Who are we?

Asif Hameed Khan (@stix2taxii)

- OT/ICS Cybersecurity
- Cyber Threat Intelligence (CTI)
- Digital Forensics and Incident Response (DFIR)
- Platform- OTISP (OT Threat Information Sharing Platform)



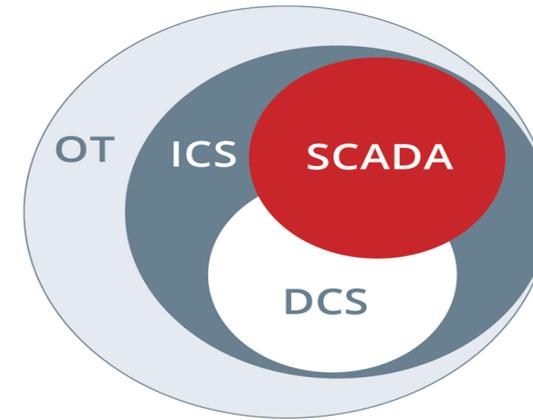
Gagandeep Singh Jattana (@gaganjattana)

- IoT Penetration Testing
- Hardware Security Testing
- Firmware Analysis



Introduction to Operational Technology (OT)

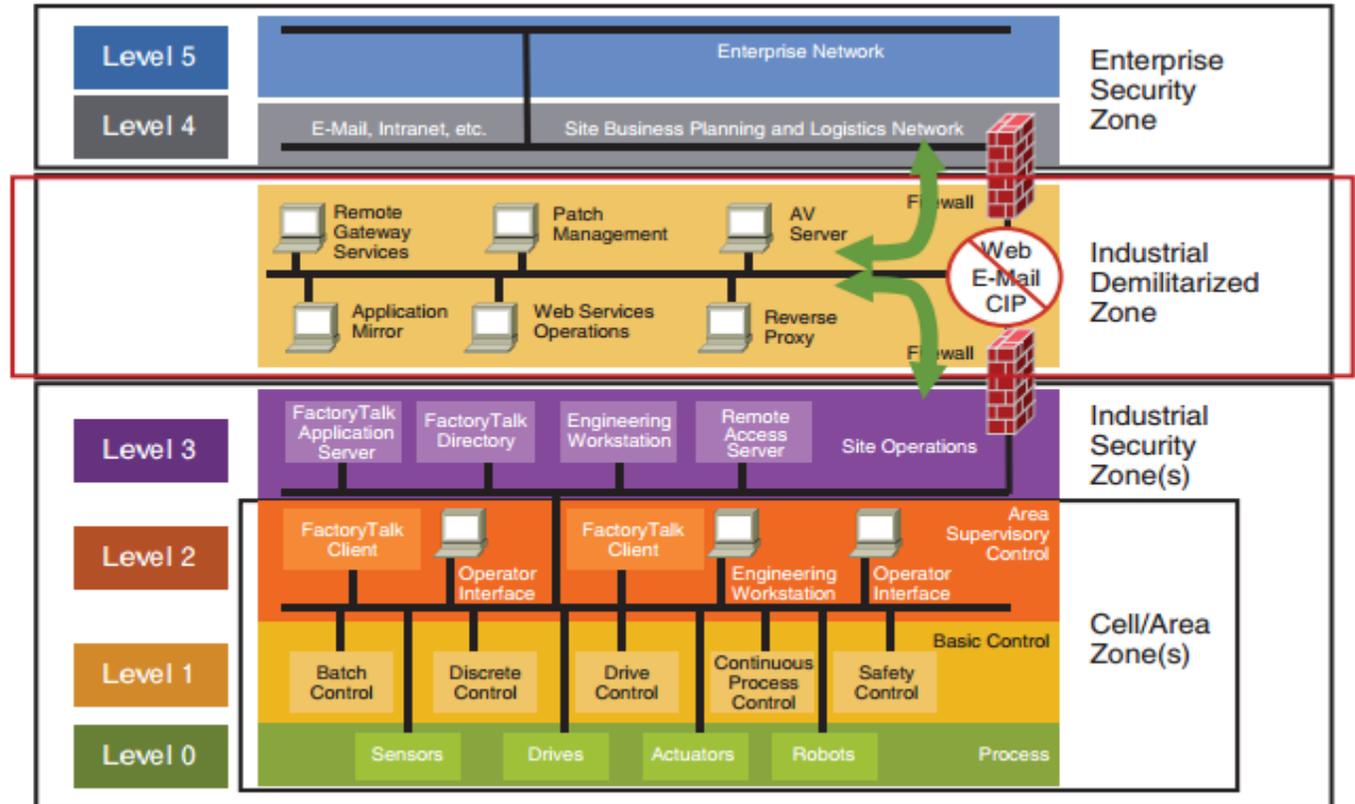
- Industrial Control Systems (ICS) is a general term for hardware and software working together to achieve Industrial objectives.
- Supervisory Control and Data Acquisition (SCADA) is a monitoring of the functioning of ICS. Operations are controlled offsite/remotely.
- While DCS are functionally very similar, DCS is generally employed at large, continuous processing facilities. Operations are controlled onsite rather than remotely.
- Operation Technology (OT) refers to the computing systems used to manage the whole Industrial operations.



Source- <https://www.securicon.com/whats-the-difference-between-ot-ics-scada-and-dcs/>

Introduction to Operational Technology (OT)

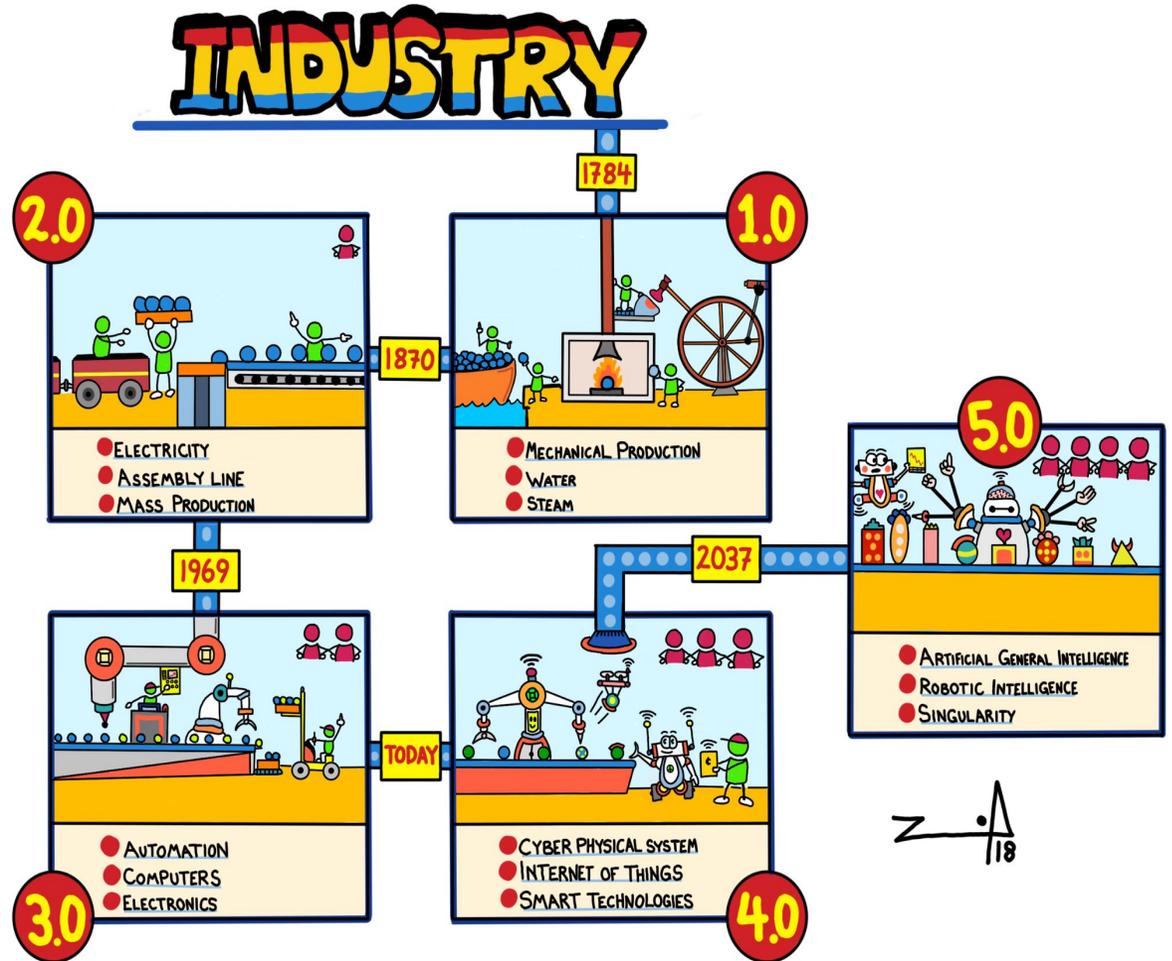
- Purdue Enterprise Reference Architecture (PERA)
- Developed by Purdue University
- Conceptual architecture
- Good source to start
- Basis of all well known ICS Architectures available



Source- <https://www.sans.org/reading-room/whitepapers/ICS/paper/36327>

Why OT Security?

- Industry 4.0 and Industry 5.0
- Commercial Off The Shelf (COTS) Products
- Integration of IoT in OT → IIoT
- Enterprise and Process Control Network Connectivity
- Cyber breach in OT environment may have permanent impact (i.e Environmental, Human loss etc)



Source- <https://twitter.com/zaidlearn/status/981083540631699461>

Common Myths

- We have a Firewall and IDS Deployed
- We are Air-Gapped
- We have SIS and Safety Devices Deployed
- Why Hacker will Target Us?
- We are not connected to business network
- IT Security vs OT Security (IT>OT)

Note: OT Security > IT Security

Source- https://media.kaspersky.com/pdf/DataSheet_KESB_5Myths-ICSS_Eng_WEB.pdf



We have SIS and latest Safety PLC deployed!

We are Air-Gapped !

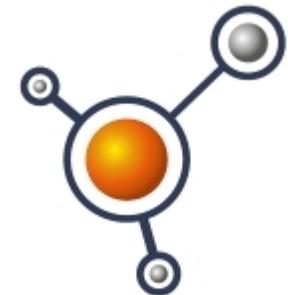


Why Hacker will Target Us?



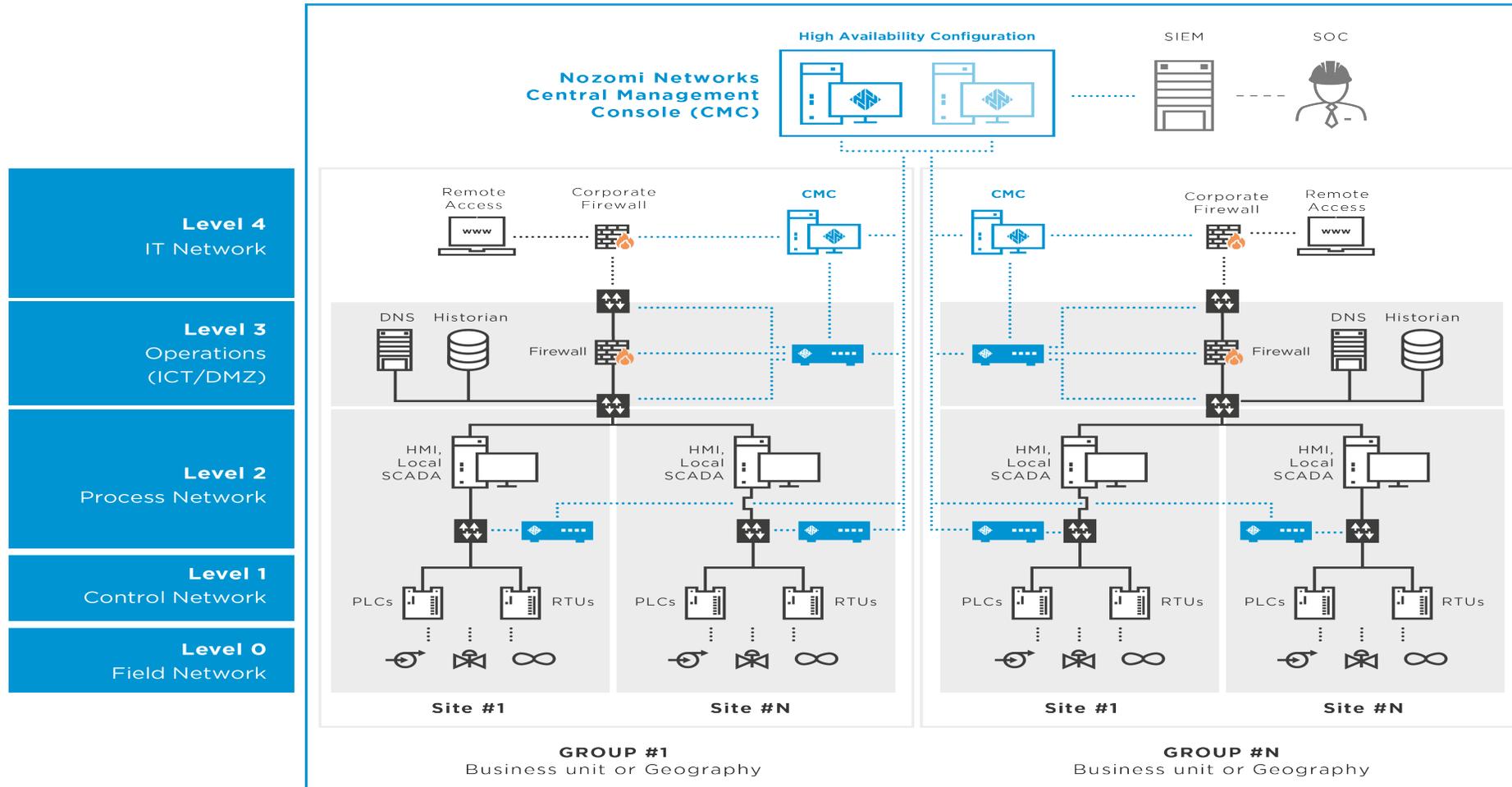
OT Monitoring Solutions

- Referred as OT SOC (Security Operation Centre)
- Passive and Active Mode of Monitoring
- 24x7 Continuous Monitoring of OT Assets
- OT SOC → Enterprise SIEM → SOAR
- Many Vendors in the Market



Source- <https://www.gartner.com/reviews/market/operational-technology-security>

OT Monitoring Solutions



Source- <https://www.nozominetworks.com/blog/nozomi-networks-scales-globally-to-deliver-advanced-ics-cybersecurity/>

Challenges in OT Monitoring Solution Deployment

Challenges:

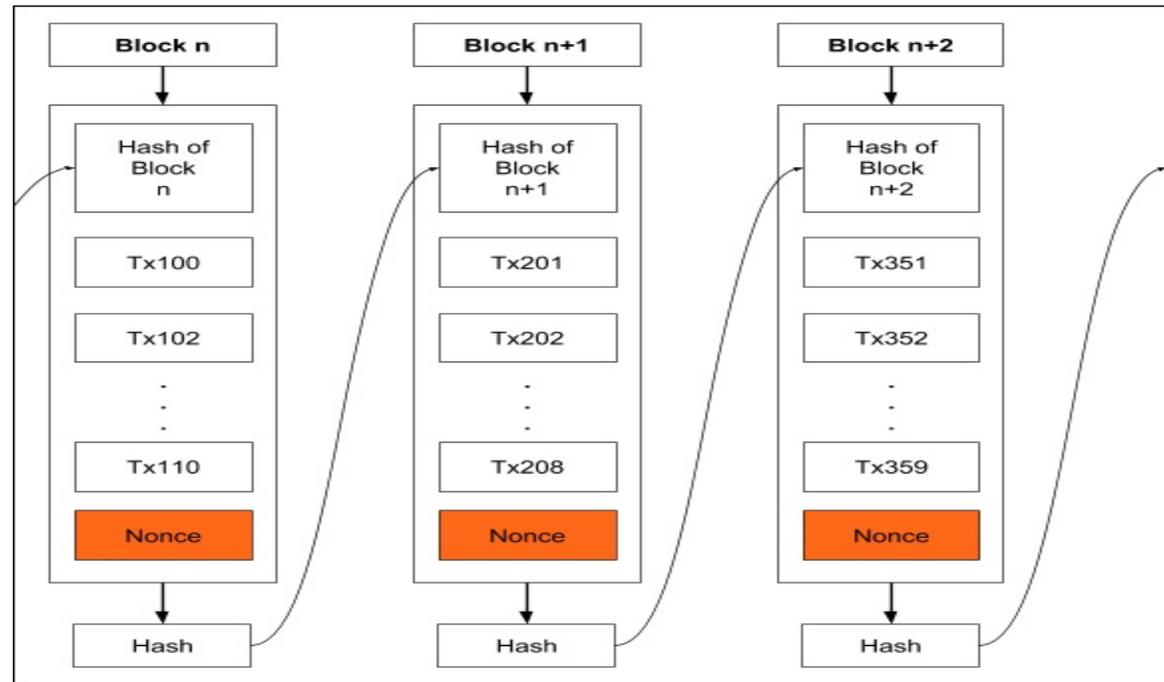
- Separate/Parallel Network Deployment for OT <-> IT Connectivity.
- Increase in Connectivity between Process Control Network and Business Network → Threat Vector
- Third Party Vendor Connectivity to OT SOC and Enterprise SOC.
- Access Control/Accountability and Authorization → IAM, PIM and PAM



Source- <https://www.nozominetworks.com/blog/overcoming-it-ot-cybersecurity-convergence-roadblocks/>

What is Blockchain?

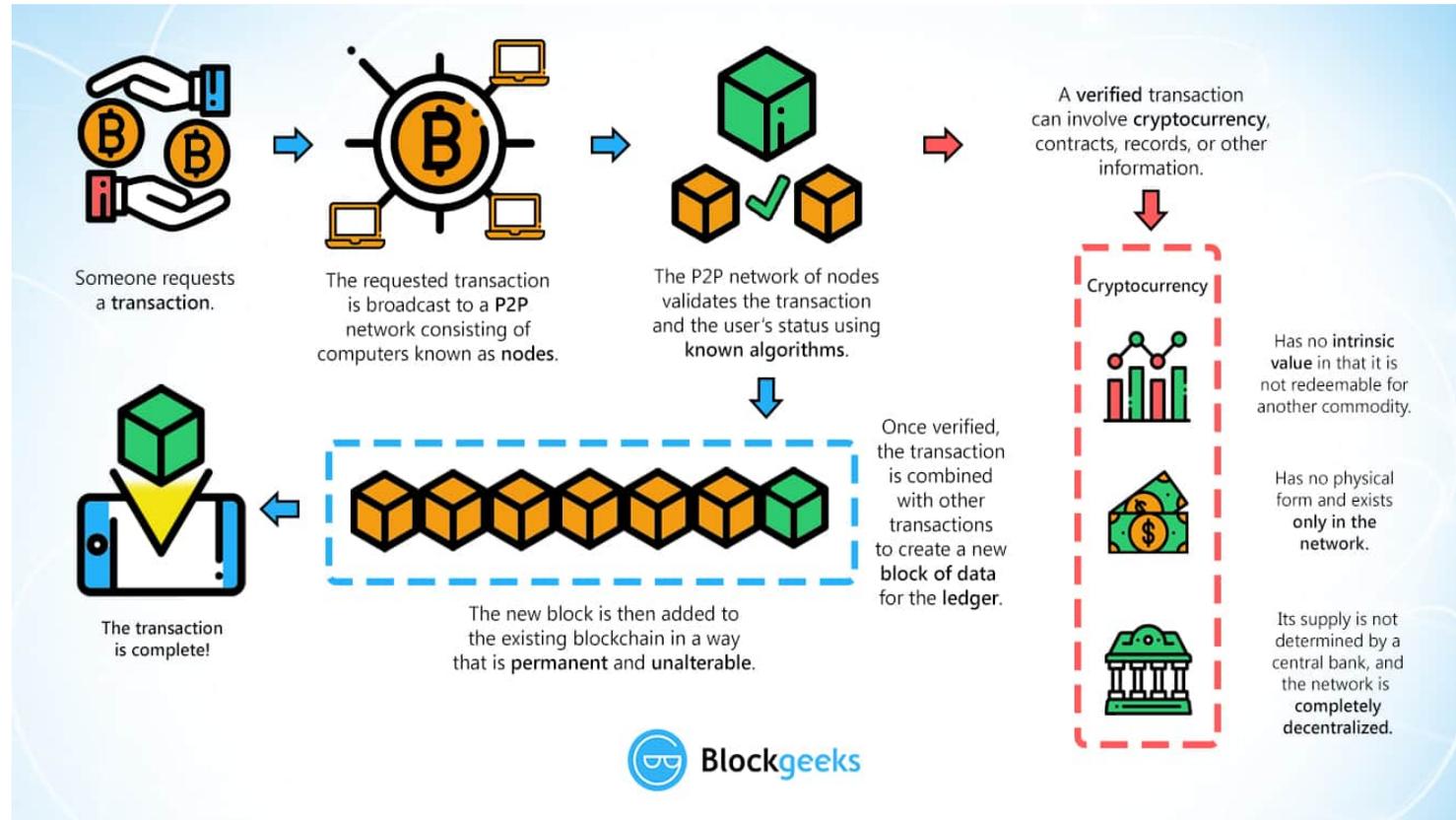
- Database of blocks with hash linking between the nodes
- Similar to chain of link list except of pointers we have Hash connectivity
- First blocks contains the configuration for the whole database known as Genesis Block



Source- https://www.tutorialspoint.com/blockchain/blockchain_proof_of_work.htm

Blockchain Concepts

- Decentralization → No Single Point of Failure and High Availability
- Transparency → No Man in The Middle (MiTM)
- Immutability → Database can not be tampered and deleted once created



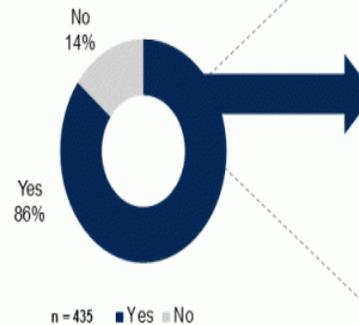
Source- <https://blockgeeks.com/guides/what-is-blockchain-technology/>

Blockchain Use Cases

- Bitcoin and Decentralized Currency
- Governance
- Identity and Access Management (IAM)
- Asset Tracking
- Data Management
- Internet of Things (IoT)
- Digital Forensics
- Cyber Threat Intelligence (CTI)
- Decentralized Applications

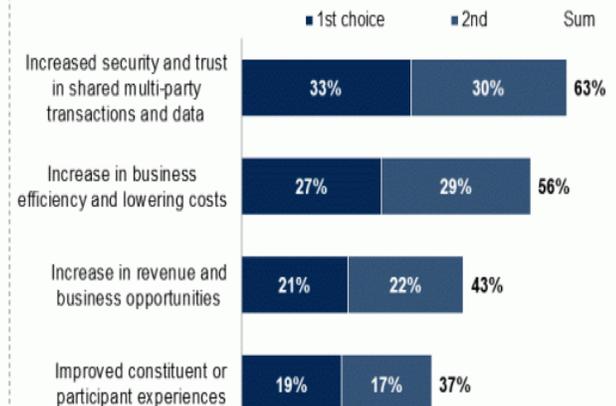
Increased Security, Trust and Lowering Costs Cited as Top Benefits of Blockchain/IoT

Implemented or planning to implement blockchain in conjunction with IoT
Percentage of Respondents



Benefit of implementing integrated IoT with blockchain networks

Sum of top 2 ranked



Base: Those organization implemented/implement blockchain specifically in conjunction with an IoT implementation (Q16B). Excludes Don't know Q16b. And, has/is your organization implemented/implement blockchain specifically in conjunction with an IoT implementation? Q17. What are the top 2 benefits for your organization of implementing integrated IoT and Blockchain networks?
SOURCE: Gartner IoT Implementation Trends, Survey respondents were screened for several demographic factors, to include only companies that had already implemented IoT in the U.S. and other demographic constraints — see full Methodology description for details

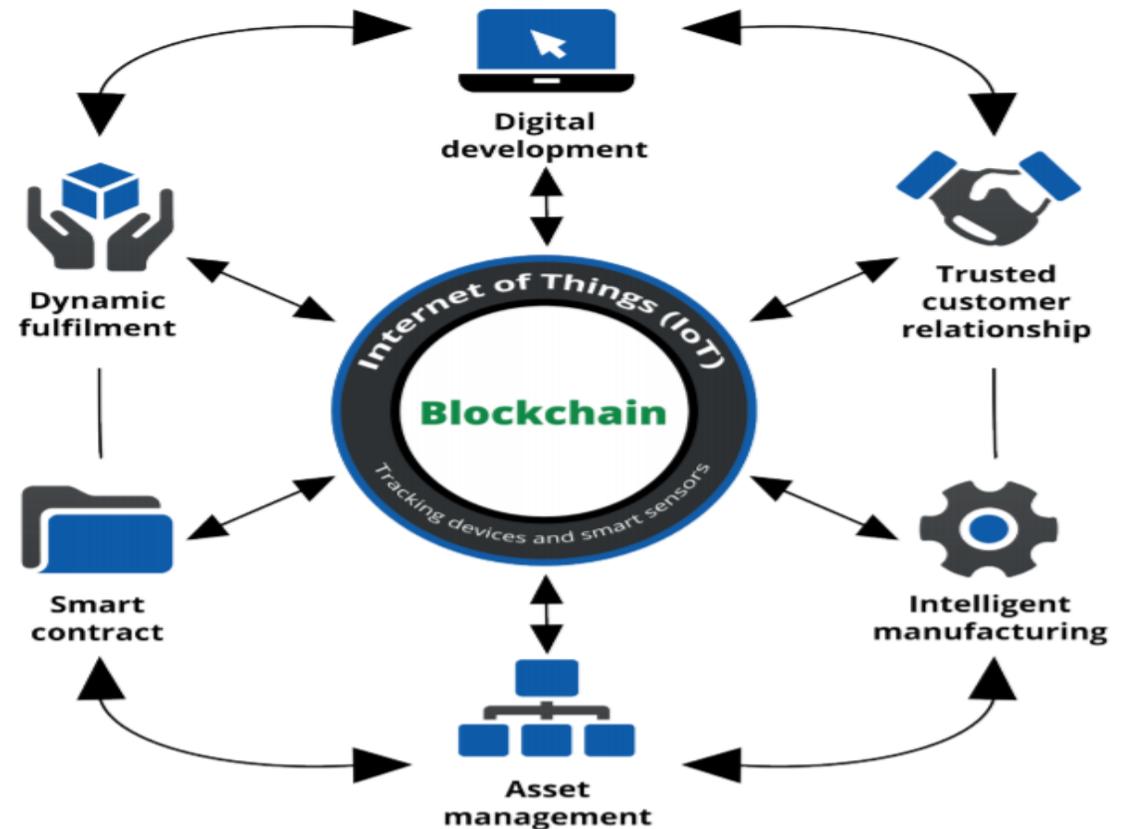
© 2019 Gartner, Inc. and/or its affiliates. All rights reserved. Gartner is a registered trademark of Gartner, Inc. and its affiliates.

Gartner

Source- <https://blogs.gartner.com/avivah-litan/2019/12/05/iot-integration-sweet-spot-blockchain-per-gartner-survey/>

Applicability of Blockchain in OT Monitoring

- Decentralized Network and Applications
- Immutable Database
- No Tampering
- Consensus
- Privacy
- Act as an Intermediate network between IT and OT.



Source- <https://www.capgemini.com/au-en/wp-content/uploads/sites/9/2018/10/Blockchain-and-Industry-4.0.pdf>

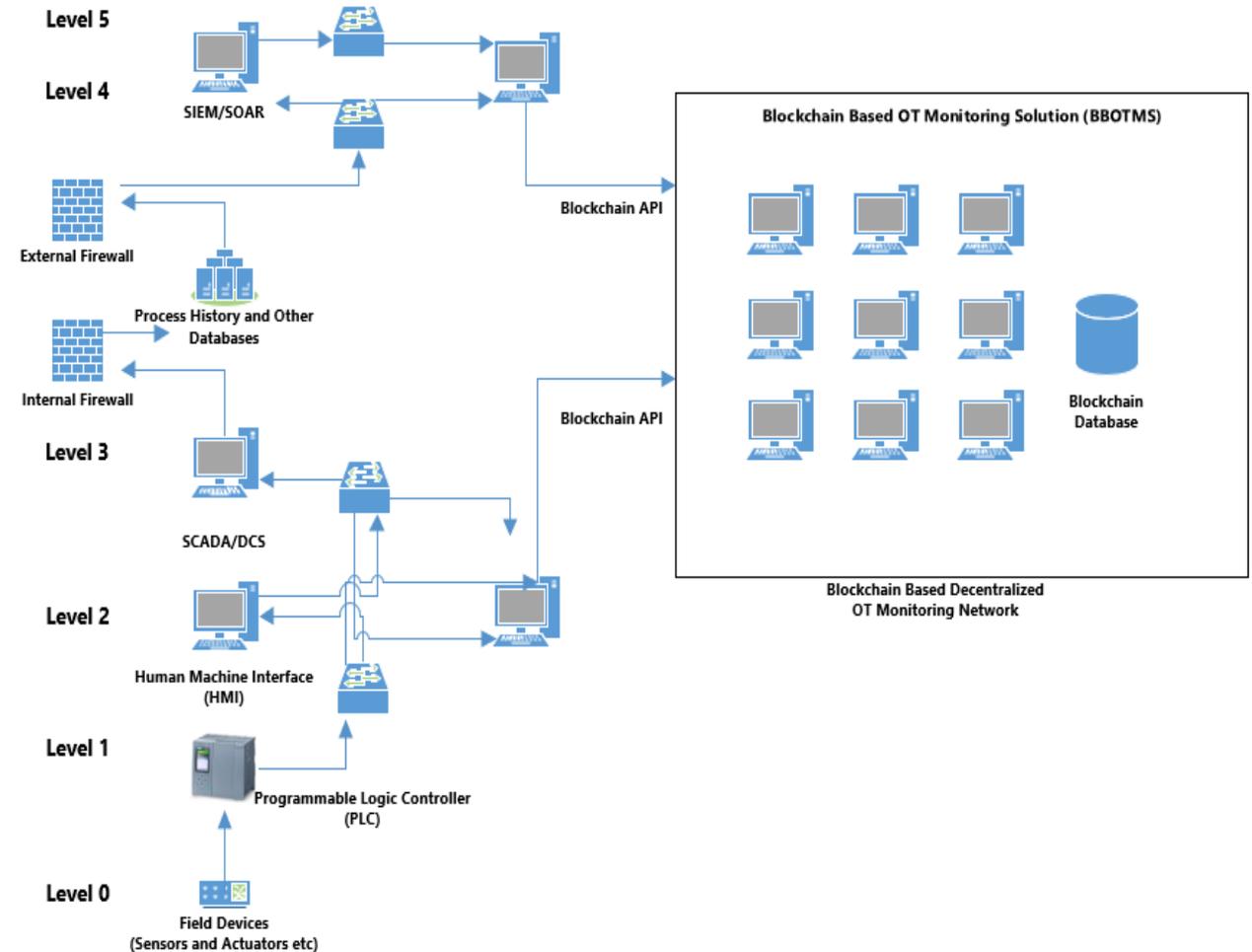
Proposed Work - BBOTMS

Benefits

- Decentralized OT SOC
- Access Control/Accountability and Authorization
- Robust Cyber Threat Intelligence (CTI) Database
- Secure Connectivity to the Enterprise/Business Networks
- Robust Network Forensics

Challenges

- All Challenges associated with the Blockchain Technology



Why Not Hashgraph?

Benefits over Blockchain

- 50,000 Times Faster Speed
- Equal level field
- Provable or Verifiable
- Secure by Byzantine
- Cheap and 100% Efficient

Limitations

- Patented Technology
- Not Easily Available
- Integration Issues

	1ST GENERATION	2ND GENERATION	3RD GENERATION
	 BITCOIN BTC	 ETHEREUM ETH	 HEDERA HBAR
TRANSACTIONS PER SECOND	3+ TPS	12+ TPS	10,000+ TPS ¹
AVERAGE FEE	\$0.20 USD ²	\$0.13 USD ³	\$0.0001 USD
TRANSACTION CONFIRMATION	10-60 MINUTES	10-20 SECONDS	3-5 SECONDS (w/finality)

Source-<https://www.hedera.com/>

Thank You!