Blockchain Secured Alternative to Mixed Routing/Non-Routing Wireless Sensor Network Topologies for Industrial Settings

Peter L. Fuhr[1], Sterling S. Rooke[2]

[1]Oak Ridge National Laboratory, One Bethel Valley Road, Oak Ridge, Tennessee, 37831 USA
[2]University of Tennessee, Dept of Electrical Engineering and Computer Science, Knoxville, Tennessee, 37996, USA

---***---

Abstract - *Mesh networking of wireless sensors implies that individual sensor nodes will be able to communicate with neighboring nodes thereby forming a communication fabric. In the case of traditional wireless sensors, their radio frequency coverage – or RF footprint – is defined by the maximum separation distance between neighboring nodes while still achieving some level of, typically degrading from maximum, information transfer (throughput). Security issues arise in the situations where the sensor nodes are deployed near the physical boundary of an industrial site (edge nodes). In the more general case of the sensors relying on omnidirectional antennas, the edge nodes' RF footprint may extend beyond the edge of the facility. If the edge nodes perform as routing nodes, then it may be possible for similar sensors/devices outside of the facility boundary to join the network. While various schemes have been implemented to address this security issue, we report on the possibility of using blockchain for security of such edge nodes.*

Key Words: *wireless sensors, mesh networking, blockchain*

1. REAL DETAILS OF MESH NETWORKING IN AN INDUSTRIAL SETTING

There is a vast amount of "how mesh networks work" information circulating in the literature ranging from marketing briefs to technical papers [1-7]. In the context of an industrial setting, it isn't always so simple as to just move the wireless transmitters around to get better RF overlap while performing the measurement at a specific required plant location in order to provide useful information to the process engineer. A typical mesh network topological diagram is shown in Fig. 1. In the situation shown, each node is able to communicate with each other node.

While Fig. 1 represents an idealized situation optimal for discussion purposes, indicating that each node can communicate with every other node, the reality is that this would require each node to project its RF signal over every other node. Assuming circular radiation patterns and that each wireless sensor transmits at the same power with identical omnidirectional antennas, then the associated RF footprint for this idealized situation is as shown in Fig. 2.

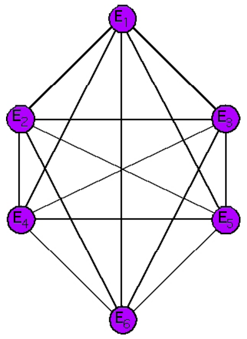

Fig. 1. Typical mesh network diagram.

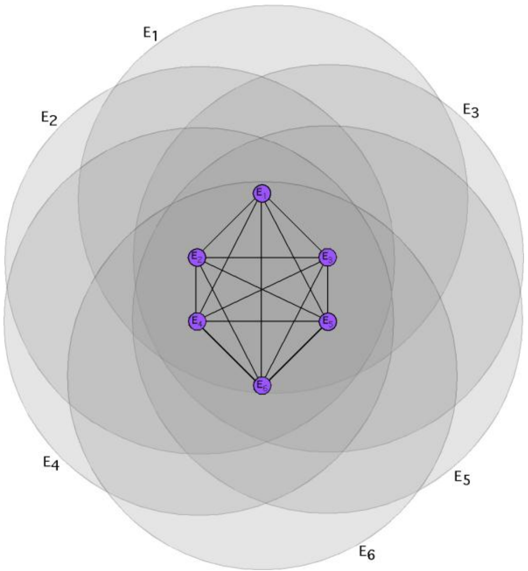

Fig. 2. Requirement for mesh-networking communication of Fig. 1's topology.

While Figs. 1 and 2 show the RF footprint realities associated with wireless mesh networks[1], the reality of industrial wireless sensors operating in mesh network topologies is slightly different. Consider the following situation: as previously mentioned, the circles shown in Fig. 2 represent the idealized RF "footprint" of each radio-enabled device. The "canyons of metal" and general reflective surfaces found throughout an industrial or utility site can significantly vary the actual RF footprint from circular. The implications of the mesh requiring

[1] …with identical omnidirectional antennas and radiated powers…

overlapping RF footprints for full-mesh-functionality and redundant information transport paths when such footprints may vary significantly from circular – and from each other – are, from an industrial deployment perspective: a fully-integrated mesh, as shown in Fig. 1 therefore requires a number of transmitters to be located in (relatively) close proximity.

The more realistic deployment scenario involves a cloud or cluster of wireless field transmitters that are in communication with and controlled by a wireless gateway device. The gateway serves multiple roles, including:

(1) coordinating the mesh routing table,

(2) keeping track of the data transmission and network timing functions,

(3) administering network security (frequently working with a companion security manager), and

(4) administration of any frequency channel "blacklisting/whitelisting".

The practical situation is that as shown in Fig. 3 for a simple wireless sensor network consisting of a gateway and four nodes.

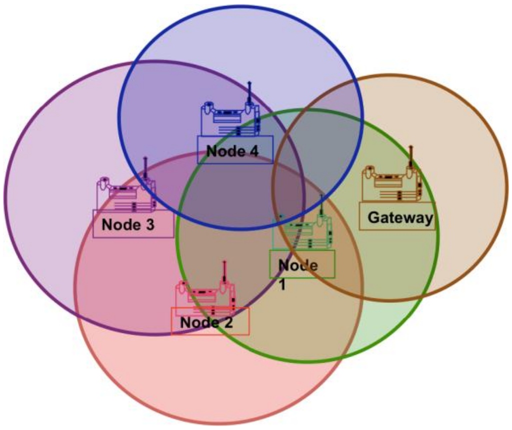

Fig.3. Idealized RF footprint map for a mesh network gateway and four nodes.

Similar to Figs. 1 and 2, the color-coded Fig. 3 diagram is meant to simply represent how the radio transceiver (Gateway/Node) must be within the RF footprint of its neighbors to be able to communicate with each other. In Fig. 3's hypothetical topology, the Gateway can *only* communicate with Node #1 (for the Gateway lies within Node 1's RF footprint). Similarly, Node #1 lies within the RF footprint of the Gateway, Node #2 and Node #4 – but not Node #3. Therefore, from an RF "coverage" and associated information transport perspective, Node #1 is able to relay messages from Nodes 2 and 4, but not Node #3. The associated mesh network connectivity diagram is shown in Fig. 4 - which is quite different from the idealized situation of Fig. 1.

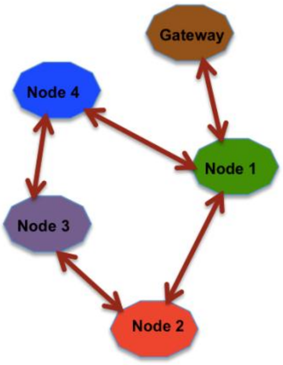

Fig. 4. The connectivity diagram for Fig. 1's RF footprint coverage map.

Please note that in this hypothetical deployment scenario, a non-robust communication network may encounter a catastrophic network failure if the link between the Gateway and Node #1 fails. The single-point of failure may be alleviated by repositioning the Gateway and/or the Nodes – a situation that an RF engineer may suggest, but that may not be feasible due to the actual locations of where the measurements are to be made.

2. Routing and Non-Routing Wireless Sensor Nodes

As their name implies, routing sensor nodes have the dual capability of taking readings from their attached sensors as well as communicating with neighboring sensor nodes. In certain programmed activity, such a dual capability sensor node may be (via some process) appending its own sensor measurements with similar packetized data coming from those neighboring sensor nodes. While various protocols utilize methods for restricting neighboring nodes from "joining the network[2]" exist, the general requirement then devolves into each device either (a) possessing a table of allowed devices (nodes) or (b) communicating with the gateway providing "new" node information then receiving instructions as to if the "new" node should be allowed to join the network. This situation is depicted in Fig. 5.

An alternative to this scenario of all nodes being routing nodes, is to have sensor nodes configured to function as non-routing nodes. In this configuration, such nodes do not possess the capability of serving as information pass-throughs, but simply provide sensor readings into the network. An alternative view of their performance is that they are the edge-of-the-network nodes and do not repeat or transport readings/information from any other node. The deployment scenario is that the non-routing nodes are positioned near the facility perimeter. Therefore, even though the RF footprint extends outside of the facility, the nodes simply do not repeat/relay/broadcast messages or information. Note that the routing and non-routing nodes must be deployed in a physical layout such that each non-

[2] A common practice is the whitelisting of "allowed" devices.

routing node may communicate with at least one routing node. This mixed-node deployment strategy places an extra burden on a facility's maintenance and/or operations staff due to the need to not inadvertently placing a routing node where a non-routing node should be. Such a deployment scenario is illustrated in Fig. 6.

A specific need for device authorization is depicted in Fig. 7 – an illustration of the Texas Ship Channel – where numerous companies operate side by side perhaps with similar systems from a single vendor. The use of non-routing nodes being deployed at the periphery of each facility – coupled with routing nodes' deployment to ensure minimization of a node's RF footprint extending beyond the facility perimeter – is required.

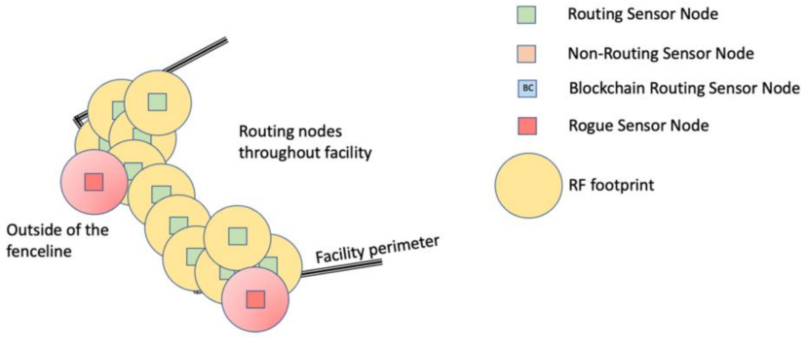

Fig. 5. Sensors nodes capable of routing messages.

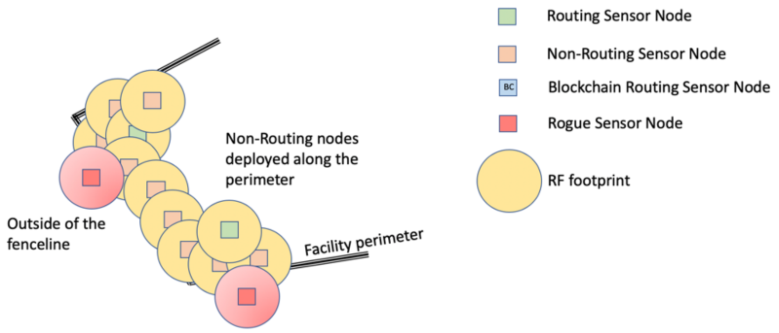

Fig. 6. Non-routing nodes are (physically) deployed along the periphery of the facility.

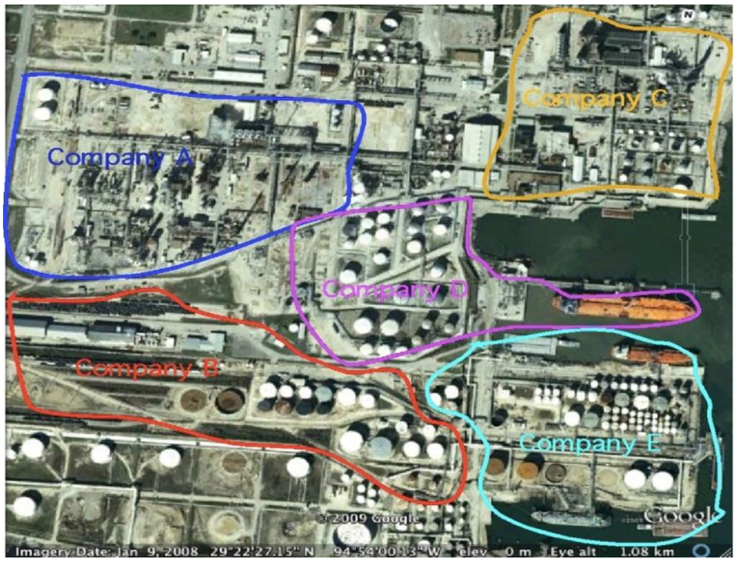
Company A
Company B
Company C
Company D
Company E
© 2009 Google
Google
Imagery Date: Jan 9, 2008 29°22'27.15" N 94°54'00.13" W elev 0 m Eye alt 1.08 km

Fig. 7. Aerial view of the Texas (USA) ship channel where numerous industrial facilities are in close proximity to one another. Networks deployed at neighboring facilities will not "cross-talk" if non-routing nodes are deployed along the periphery of each facility.

3. Provisioning of Mixed Routing & Non-Routing Edge Nodes

Mesh networks exhibit various operational characteristics for data transport in RF/physical environments where the attenuation and multipath circumstances may vary. This requires that the nodes be capable of routing traffic from their neighbors (in accordance with the network algorithm being used). From an implementation perspective, this allows the maintenance crew to deploy the nodes where they need to be. But from a security perspective, this is not acceptable. This situation may be taken care of by proper settings inside the gateways (using unique IDs for each plants' networks).

The provisioning of devices being added to the sensor network is complex. Consider the provisioning state diagram, presented as Fig. 8, which illustrates the steps necessary to add/replace a sensor node. Note that this is a complex coordination of security keys being exchanged between the nodes and the gateway/controllers.

4. Blockchain for Sensor Validation

The implementation of sensor nodes programmed with blockchain[3] capabilities significantly reduces the deployment and provisioning complexities associated with the mix of routing and non-routing nodes. While a frequent use of blockchain/DLT is tracking information exchanges (transactions) [8-18], in this case of blockchain equipped sensor nodes, the blockchain is used for authentication of the nodes themselves. Such a process occurs for because device information is released to all members of the network through the distributed ledger and new information is updated in real-time, providing reliability and traceability of information [19-26].

Deployment of blockchain equipped sensor nodes removes the need for the two categories of sensor nodes: routing and non-routing for all devices are routing capable. The capability of a "new" node – such as a rogue node – to communicate with the network fabric is restricted by examination of the ledger itself. If a new node attempts to broadcast, the blockchain is queried as to if this new node is allowed to join the network. The deployment situation is illustrated in Fig. 9.

The reduction in deployment – and cataloging – routing and non-routing sensor nodes' locations eases the tasks for facility maintenance and operation. A single class of devices are used with network-centric (blockchain) validation of a device's "permission" to join the network used. Devices that are "beyond-the-fence" are not authenticated into the network traffic flow and therefore inherently not a threat, leading to no need for routing/non-routing node distinction.

5. Summary

The requirement to deploying a mixture of routing and non-routing wireless sensor nodes to address security issues that may arise due to RF footprints' extending beyond a facility's physical boundary leads to maintenance and operational impacts. The use of sensor nodes that may operate in a blockchain alleviates the deployment issues.

6. References

[1] Y. Ai, M. Peng, and K. Zhang, "Edge computing technologies for internet of things: a primer," Digital Communications and Networks, vol. 4, no. 2, pp. 77–86, 2018.

[2] A. Alrawais, A. Alhothaily, C. Hu, and X. Cheng, "Fog computing for the internet of things: Security and privacy issues," IEEE Internet Computing, vol. 21, no. 2, pp. 34–42, 2017.

[3] R. Buyya and A. V. Dastjerdi, Internet of Things: Principles and paradigms. Elsevier, 2016.

[4] A. Haroon, M. A. Shah, Y. Asim, W. Naeem, M. Kamran, and Q. Javaid, "Constraints in the iot: the world in 2020 and beyond," Constraints, vol. 7, no. 11, 2016.

[5] A. Musaddiq, Y. B. Zikria, O. Hahm, H. Yu, A. K. Bashir, and S. W. Kim, "A survey on resource management in iot operating systems," IEEE Access, vol. 6, pp. 8459–8482, 2018.

[6] M. Conoscenti, A. Vetro, and J. C. De Martin, "Blockchain for the internet of things: A systematic literature review," in Computer Systems and Applications (AICCSA), 2016 IEEE/ACS 13th International Conference of. IEEE, 2016, pp. 1–6.

[7] Y. Yang, L. Wu, G. Yin, L. Li, and H. Zhao, "A survey on security and privacy issues in internet-of-things," IEEE Internet of Things Journal, vol. 4, no. 5, pp. 1250–1258, 2017.

[8] S. Nakamoto, "Bitcoin: A peer-to-peer electronic cash system," 2008.

[9] I. Bashir, Mastering Blockchain. Packt Publishing Ltd, 2017.

[10] W. Mougayar, The business Blockchain: promise, practice, and application of the next Internet technology. John Wiley & Sons, 2016.

[11] J. wood, "Blockchain of things, cool things happen when iot and distributed ledger tech collide," Online, 2018, https://medium.com/trivial-co/Blockchain-of-things-cool-things-happenwhen-iot-distributed-ledger-tech-collide-3784dc62cc7b.

[3] …or more formally distributed ledger technology (DLT)…

[12] Sun, J.; Yan, J.; Zhang, K.Z. Blockchain-based sharing services: What blockchain technology can contribute to smart cities. Financ. Innov. 2016, 2, 26.

[13] Zheng, Z.; Xie, S.; Dai, H.; Chen, X.; Wang, H. An overview of blockchain technology: Architecture, consensus, and future trends. In Proceedings of the 2017 IEEE International Congress on Big Data (BigData Congress), Honolulu, HI, USA, 25–30 June 2017; pp. 557–564.

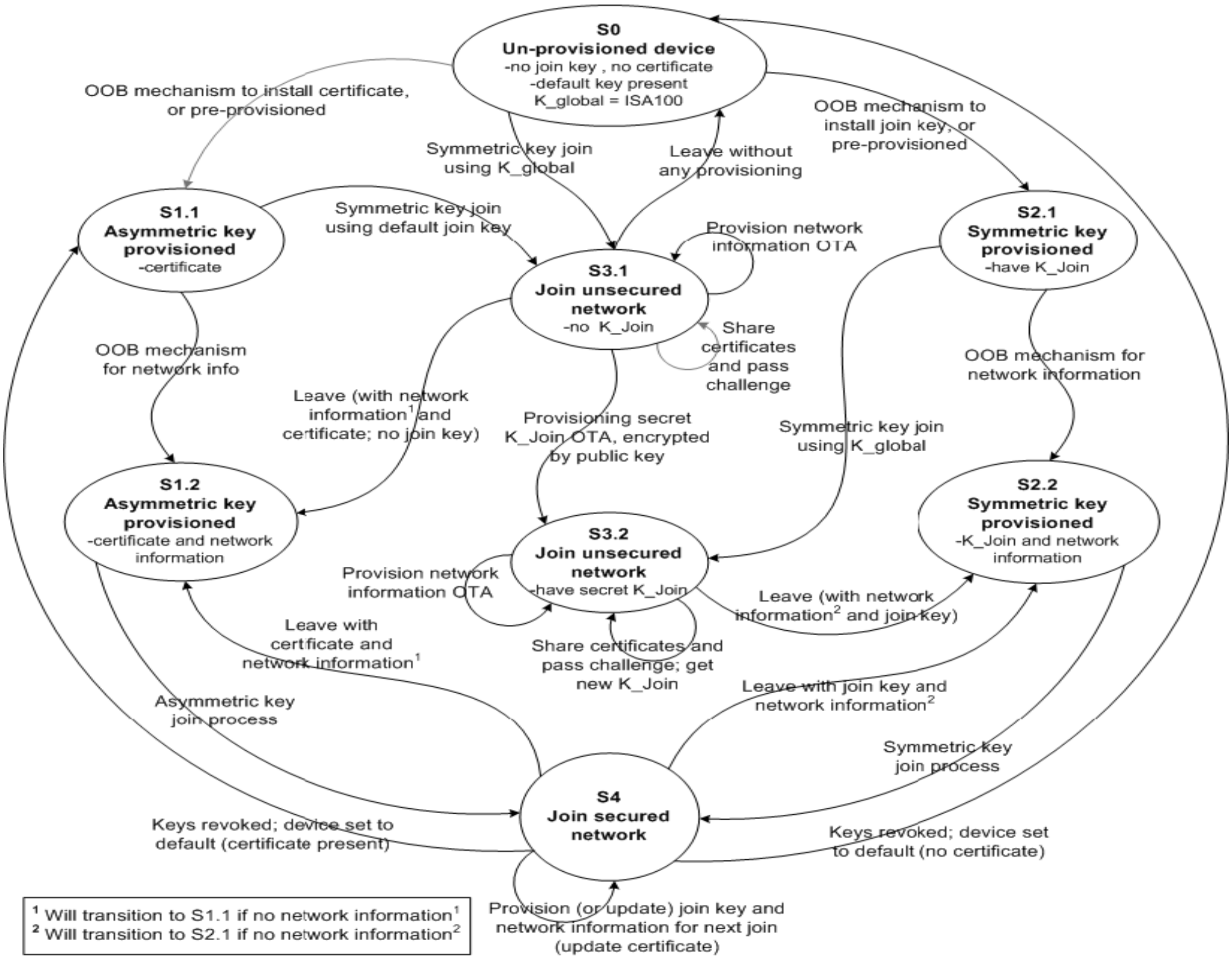
S0
Un-provisioned device
-no join key , no certificate
-default key present
K_global = ISA100
OOB mechanism to install certificate, or pre-provisioned
OOB mechanism to install join key, or pre-provisioned
Symmetric key join using K_global
Leave without any provisioning
S1.1
Asymmetric key provisioned
-certificate
Symmetric key join using default join key
Provision network information OTA
S2.1
Symmetric key provisioned
-have K_Join
S3.1
Join unsecured network
-no K_Join
Share certificates and pass challenge
OOB mechanism for network info
OOB mechanism for network information
Leave (with network information¹ and certificate; no join key)
Provisioning secret K_Join OTA, encrypted by public key
Symmetric key join using K_global
S1.2
Asymmetric key provisioned
-certificate and network information
S3.2
Join unsecured network
-have secret K_Join
S2.2
Symmetric key provisioned
-K_Join and network information
Provision network information OTA
Leave (with network information² and join key)
Leave with certficate and network information¹
Share certificates and pass challenge; get new K_Join
Leave with join key and network information²
Asymmetric key join process
Symmetric key join process
S4
Join secured network
Keys revoked; device set to default (certificate present)
Keys revoked; device set to default (no certificate)
Provision (or update) join key and network information for next join (update certificate)
¹ Will transition to S1.1 if no network information¹
² Will transition to S2.1 if no network information²

Fig. 8. State transition diagram showing various paths to joining a secured network.

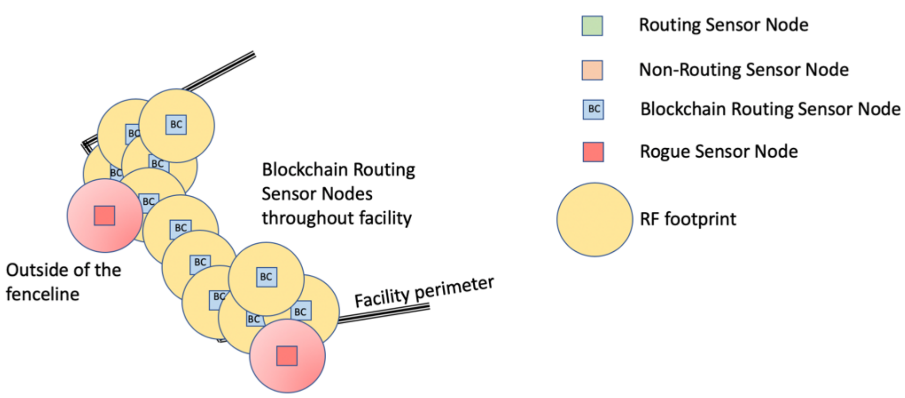

Fig. 9. Deployment scenario for blockchain-capable sensor nodes along the periphery of a facility.

[14] Kraijak, S.; Tuwanut, P. A survey on internet of things architecture, protocols, possible applications, security, privacy, real-world implementation and future trends. In Proceedings of the 2015 IEEE 16th International Conference on Communication Technology, Hangzhou, China, 18–20 October 2015; pp. 26–31.

[15] Sharma, P.K.; Park, J.H. Blockchain based hybrid network architecture for the smart city. Future Gener. Comput. Syst. 2018, 86, 650–655.

[16] Nakamoto, S. Bitcoin: A Peer-to-Peer Electronic Cash System. 2008. Available online: http://www.academia.edu/download/54517945/Bitcoin_paper_Original_2.pdf (accessed on 3 May 2019).

[17] A. Reyna, C. Martín, J. Chen, E. Soler, and M. Díaz, "On blockchain and its integration with iot. challenges and opportunities," Future Generation Computer Systems, 2018.

[18] H. F. Atlam, A. Alenezi, M. O. Alassafi, and G. Wills, "Blockchain with internet of things: Benefits, challenges, and future directions," International Journal of Intelligent Systems and Applications, vol. 10, no. 6, pp. 40–48, 2018.

[19] Q. He, N. Guan, M. Lv, and W. Yi, "On the consensus mechanisms of blockchain/dlt for internet of things," in 2018 IEEE 13th International Symposium on Industrial Embedded Systems (SIES). IEEE, 2018, pp. 1–10.

[20] A. Dorri, S. S. Kanhere, R. Jurdak, and P. Gauravaram, "Blockchain for iot security and privacy: The case study of a smart home," in Pervasive Computing and Communications Workshops (PerCom Workshops), 2017 IEEE International Conference on. IEEE, 2017, pp. 618–623.

[21] K. Christidis and M. Devetsikiotis, "Blockchains and smart contracts for the internet of things," Ieee Access, vol. 4, pp. 2292–2303, 2016.

[22] K. Wüst and A. Gervais, "Do you need a blockchain?" in 2018 Crypto Valley Conference on Blockchain Technology (CVCBT). IEEE, 2018, pp. 45–54.

[23] T. Laurence, Blockchain for dummies. John Wiley & Sons, 2017.

[24] X. Decuyper, "How does a blockchain work," Online, 2018, https://savjee.be/videos/simply-explained/how-does-a-blockchain-work/.

[25] M. A. Ferrag, M. Derdour, M. Mukherjee, A. Derhab, L. Maglaras, and H. Janicke, "Blockchain technologies for the internet of things: Research issues and challenges," IEEE Internet of Things Journal, 2018.

[26] A. T. Norman, Blockchain Technology Explained: The Ultimate Beginners Guide About Blockchain Wallet, Mining, Bitcoin, Ethereum, Litecoin, Zcash, Monero, Ripple, Dash, IOTA And Smart Contracts.