Blockchains as security-enabler for industrial IoT-applications

Volker Skwarek
Hamburg University of Applied Sciences, Hamburg, Germany

Received 16 September 2017
Revised 5 October 2017
Accepted 16 October 2017

Abstract

Purpose – This paper aims to describe a method for Internet-of-Things-devices to achieve industrial grade reliability for information transfer from wireless sensor systems to production systems using blockchain technologies.

Design/methodology/approach – An increased security and reliability of submitted data within the sensor network could be achieved on an application level. Therefore, a lightweight, high-level communication protocol based on blockchain principles was designed.

Findings – Blockchain mechanisms can secure the wireless communication of Internet-of-Things-devices in a lightweight and scalable manner.

Originality/value – The innovation of this research is the successful application of general blockchain mechanisms to increase security of a wireless sensor system without binding to a dedicated blockchain technology.

Keywords Blockchain, Smart production, Sensor networks, Oracles, Smart contracts, (industrial) internet-of-things

Paper type Research paper

1. Introduction

The Internet-of-Things (IoT) currently rules many activities in research and development of mobile and wearable devices. This not only refers to smart phones. According to the analysts IDC, the number of sold smart watches tripled from 7.1 million devices in Q3/2014 to 21.2 million devices in Q3/2014 (Farooqui, 2015). In a 2014 analysis, the ABI Research data estimated the market increase for all wearables from 53.8 million devices in 2013 to 146.2 million sold units in 2015 (J'son and Partners Consulting, 2015) – numbers only representing the private-user market for wearables such as smart watches. Not considered in these numbers are mobile phones, wireless monitored health devices such as insulin pumps, blood pressure and heart rate monitors and many more. The engineering services company Libelium listed more than 50 applications (Libelium Comunicaciones, 2015) for using IoT-devices in a personal, semi-professional or professional manner. For professional applications, such devices either are referred to as *industrial Internet-of-Things* (IIoT) or – according to their use-case – as smart metering, smart grid, smart production or smart-X, in general.

This paper forms part of a special section on 'Blockchain on business and entrepreneurship'.

Asia Pacific Journal of Innovation and Entrepreneurship
Vol. 11 No. 3, 2017
pp. 301-311
Emerald Publishing Limited
2071-1395
DOI 10.1108/APJIE-12-2017-035

Such smart-X systems can usually be characterized as networked sensors with communication capabilities – also referred to as a cyber-physical system (CPS) – sending its data for further processing, aggregation and evaluation to a cloud service.

As mobile systems are very sensitive on their energy budget – typical capacities for portable LiPo-batteries used in wearable IoT-devices range from 1 to 5,000 mAh – may result in operating times from a few hours for smart phones to several days or few weeks for smart watches. This mainly depends on the processor load, measuring intensity, display operation and wireless transmission rate of a device. The Ragone diagram in Figure 1 shows the operating time of a typical mobile energy supply under full load as diagonal lines. The markers indicate the capacity of typical energy storages. Additionally, on the left-hand axis, the potential additional power as produced from autonomous energy sources is shown. This leads to the conclusion that energy is a very scarce resource for IoT-devices, and needs to be carefully managed.

Apart from customer comfort, there are several – especially professional – use cases such as cargo-monitoring in a supply chain, environmental measurements for smart-city applications or long-term ECG monitoring for a patient with a heart disease, requiring very long and reliable operating times. But this increase in usability and customer acceptance often results in a severe lack of device- and data protection, and very insecure systems as additional computational loads have to be reduced to a minimum.

This lack of security is one of the major issues that make IIoT-systems very unattractive for professional users. For example, for applications such as smart production or smart grid management, the risk of a fatal intrusion with severe effects on production outcome, energy infrastructure or public safety and health is too high for a wide acceptance of wireless sensor systems in smart-X-applications. A famous example is the Philips-Hue-attack (Ronen *et al.*, 2016), where remote-controlled light bulbs could be attacked, reprogrammed and spontaneously turned on for a whole city, leading potentially to a black-out due to the sudden energy consumption. This attack bases on a feature of the Zigbee-protocol, allowing over-the-air updates among network nodes. As soon as an attacker has conquered one node, he can gain control over the complete network.

In this article, we describe a concept about how blockchain- and distributed-ledger-principles can be used for securing a sensor network with a lightweight protocol. The

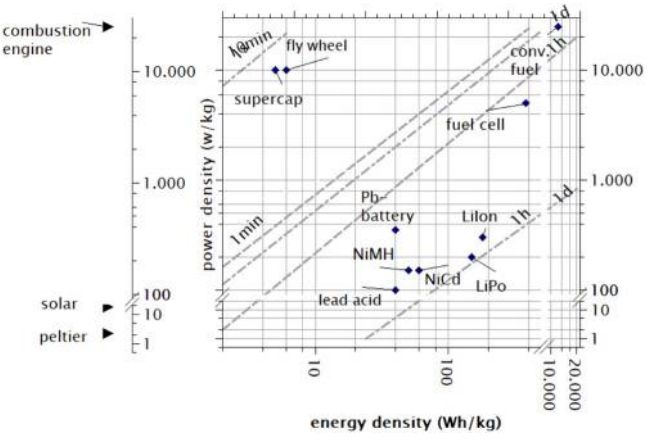


Figure 1.
Ragone diagram about the operation time of a mobile device with an energy-storage system under maximum load

protocol is specially designed for short- and low-data-rate transmission with low calculation effort on the processor.

Section 2 of this article presents a short overview of professional, industrial IoT applications on blockchains. Section 3 explains the potential security risks and solutions, as provided by blockchains. Section 4 derives and explains a lightweight protocol for wireless sensor networking according to blockchain principles. Section 5 closes with a short summary and an outlook.

2. Applications for industrial Internet-of-Things-blockchains

2.1 General considerations about Internet-of-Things-systems

Currently, blockchains are used for countless number of applications, regardless of whether they are suited for it. In a comprehensive overview, e.g. the company *Marmelab* already listed more than 80 application-specific blockchain derivatives in 20 different areas (Zaninotto, 2016). Today's numbers might be, by a magnitude, higher as the blockchain development and start-up-community increased their activities worldwide. However, not all applications are reasonable as they do not leverage the advantages of a blockchain technology but leverage the disadvantages of high redundancy (i.e. unused calculation effort), required networking capacity, energy effort for consensus and distribution mechanisms. Therefore, the applications that are generally suited should be considered first, deriving them from general blockchain- and DLT-properties (Boucher, 2017, p. 6):

- decentralization without hierarchy – at least theoretically; in real applications, a hierarchy is given, e.g. due requirements in network topology;
- full transparency; and
- lack of trustworthiness in terms of freedom of manipulation of the distributed information.

Generic fields of application using these properties are the following:

- permanent and immutable storage of information or at least their proof-of-existence by putting a hash of the information on the chain;
- distribution of information and transactions among various (independent) partners; and
- secured execution of transactions or applications – e.g. by smart contracts.

Additionally, it has to be taken into consideration that there are also special requirements coming up from IoT-devices themselves. These are mostly derived from the research area of (mobile) wireless sensor networks (WSN) or CPS in general, where IoT-systems are derived from. Obaidat and Misra (2014, p. 16) or Dargie and Poellabauer (2010, chap. chap. 1.2) list them as follows:

- lifetime restrictions;
- limited energy provision;
- unreliable communication due to wireless transmission;
- security;
- design constraints – e. g. the need to be small; and
- need for self-configuration and fault tolerance.

2.2 Attributes of the industrial Internet-of-Things and consequences for blockchain applications

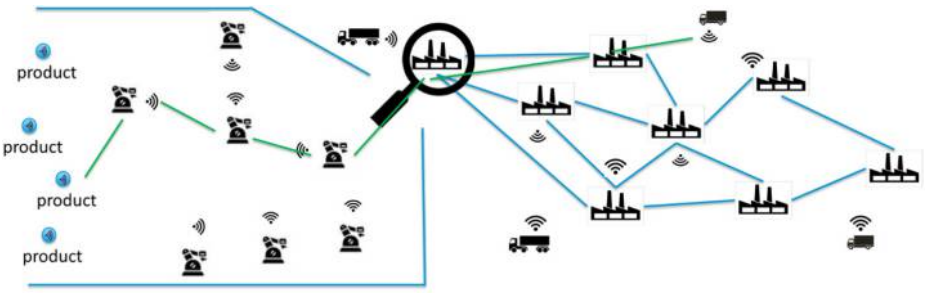
The current trend for the digitization of industrial processes is subsumed in the term *smart-X*, whereas the "X" usually is replaced by the concrete field-of-application such as *smart-production, smart-grid* or *smart-cities*. The term *smart* reflects the highly dynamic reconfiguration of the complete system according to actual environment, product, production or customer requirements. In the context of smart production – also called industry 4.0 – the German Ministry of Economy (BMWi) defined the digitization strategy of the German Government as follows:

> [. . .] In addition to the digital production site, production and logistics will be networked beyond the border of a (added by the author: single) company for optimizing the material flow, to detect errors earlier and to react in a highly flexible manner towards changing customer expectations and market requirements. [. . .] (Bundesministerium für Wirtschaft und Energie, Referat Öffentlichkeitsarbeit, 2016, translated).

Therefore, industrial systems shall be able to handle single-piece-productions dynamically. Such requirement is hardly achievable by a central management system as the risk of a single-point-failure in case of a malfunction is too high, and the required processing power and communication bandwidth for such a system may be a limiting issue.

Consequently, these systems are usually distributed and transaction based. In contrast to a process-based system, a transaction-based system acts fully asynchronously on demand. This means, that there is no instance of central coordination, synchronizing all actors, but that the single instances have to request activities by sending transaction requests into the system, expecting a recipient processing this request. For example, such a transaction can be initiated by an enterprise–resource-planning (ERP)-system, ordering a new product from the production floor. This request is received by a semis (= raw product), initiating its own production. Now the semis step-wise requests all production tools by sending messages to them. The messages are processed as soon as there are spare resources (see example in Figure 2).

This transaction-based method of system control not only applies to smart-production but also to any smart-X-application: for smart-health, a vital sign sensor detects abnormalities and requests a doctor's interaction, and a smart-grid measures a dropping grid frequency and buys more energy. Therefore, the asynchronous-system-control initiated by decentral devices is part of the smart-X-concept.



Note: A semis requests resources among the indicated line including transports to other facilities and customers

Figure 2.
Example for a dynamic, de-centrally initiated and controlled production process

The consequence of failures in IIoT-device is more severe than in regular IoT-devices: As a system causes a personal or economic fatality, the requirements in any terms of safety, security and availability are far higher than for regular IoT-systems. In situations where a consumer device in case of a failure can be restarted or data simply are wrong or missing, an industrial device usually operates in a networked cluster as explained above. A single failure may influence the whole process chain and lead to stopping production, an energy blackout for a city (Ronen *et al.*, 2016) or shipment failures at smart-transportation.

Usually, these high requirements can only be fulfilled with measures resulting in a higher energy consumption, which again contradicts the need for a long operating time of usually battery-driven mobile IoT-devices. As neglecting or diminishing security and safety is no option, the detectability of system manipulations by chaining and distributing blocks as introduced by Schneider and Kelsey (Schneider and Kelsey, 1997) seems to be a solution. In this case, the IoT-devices only need to provide low security according to their energy budget, while communicating all information by chaining and broadcasting them. Any irregularities can later be detected and handled by other devices with more energy such as gateways or production machines.

Therefore, blockchain and distributed ledger technologies seem to be predestined for higher security demands in IIoT-systems with the chance to reduce the energy need on the sensor device. Blockchains are able to secure the transferred information against manipulation (= security) and errors (= safety).

3. Detailed security considerations for industrial Internet-of-Things-blockchains

The general considerations above about the applicability of blockchain technologies will be further explained and analyzed in the following subsections.

3.1 Security risks in wireless sensor networks

As WSNs – and IoT-devices as a subset of WSN – transmit their information over the air and, therefore, use an open channel, which is why it is generally rather easy to attack them. A comprehensive, but by far not complete list of potential attacks on all, network layers is shown in the following items composed from multiple publications (Dargie and Poellabauer, 2010, chap. 11.3; Obaidat and Misra, 2014, chap. 10.4; Raghavendra *et al.*, 2006, chap. 12):

- *physical layer*: jamming, radio interference, tampering or destruction;
- *data link layer*: continuous channel access (exhaustion), collision, unfairness, interrogation or sybil attack;
- *network layer*: sinkhole, node capture, selective forwarding/black hole attack, rushing attack, sybil attack, wormhole attack, spoofed, altered or replayed routing information, acknowledgment spoofing, misdirection, internet smurf attack and homing;
- *transport layer*: flooding and de-synchronization att.; and
- *application layer*: overwhelm attack, path-based DOS attack and reprogram attack.

Therefore, it is obvious that WSNs are extremely vulnerable to a high number of attacks. Although this is covered by intensive research – a search request in the IEEE online library (ieeexplore.ieee.org) for "wireless sensor network" and "security" in the document title returned 385 results – WSNs can only be specifically secured according to their application and the individual constraints in resources and power, lack of central control or missing

peripherals. With the increased attractiveness and distribution of WSNs by IoT-devices, it is expected that the number and form of attacks on WSNs will increase, so new methods and principles for security have to be found (Dargie and Poellabauer, 2010, p. 282; Obaidat and Misra, 2014, p. 242).

Consequently, it is broadly accepted, that a WSN cannot be made equally secure as wired systems, so a different approach from Schneider and Kelsey, some of the developers of basic blockchain principles – the hash-chained blocks – will be followed:

> The tamper resistance is expected to keep most attackers out, but it is not 100 per cent reliable. [. . .] Moreover, we would like this log to survive successful tampering, so that when the wallet is brought in for inspection it will be obvious that the wallet has been tampered with Schneider and Kelsey (1997, p. 1).

The effort for attacks on nodes shall be maximized, whereas successful attacks shall be made transparent.

3.2 Security improvements using blockchain methods

If a WSN can only be insufficiently secured, it, nevertheless, has to be protected and be prepared for the detection of intrusions. Here, as one piece of the puzzle, the basic concept tamper-awareness and fraud-detection as introduced by Schneider and Kelsey will be followed. Additionally, the basic blockchain concept, as introduced by Nakamoto (2008), will be examined for parallel requirements and partly transferred into the domain of WSN to secure the communication of IIoT-devices.

The essential principle beyond Nakamoto's assumptions of securing an information exchange within a distributed system is the Byzantine fault tolerance (BFT), as described by Lamport *et al.* (1982): Within a communication system, erroneous messages shall be distinguished from correct messages among the participants, which can be solved with the redistribution of the same message in multiple rounds among multiple paths and multiple communication partners. If the number of correct messages exceeds certain mathematical rules, then the majority of the received message contains the right information. Briefly speaking, the number of false messages must be significantly lower than the correct ones.

For m traitors (= faulty messages) at least $3m + 1$ nodes, $2m + 1$ communication paths and $m + 1$ rounds of messages must be exchanged. Messages between nodes do not need to arrive synchronously but with a time shift and a re-constructible order.

Nakamoto just turns this mathematical problem into the practical BFT: As long as the number of honest nodes, information and communication cycles is far higher than the traitors and the order of sent and received information cannot easily be changed; for example, because they are hashed, the system is secure with reliable information (Castro and Liskov, 1999; Kellermann, 2002). In terms of Nakamoto, double spending (= false information) needs to be avoided by building a verified transaction ledger (= ordered information with proof) and a consensus (= the majority of participants confirms the correctness of the proof by continuing to hash the new information on the basis of the proof of the old information).

So basically, a secured communication system can be built on the concepts of the following:

- proofing and temporally ordering information;
- confirming the proofs and the order;
- making the order immutable; and
- distributing this information.

Branches containing erroneous information may be temporarily created, but with a majority of honest participants, the correct information will survive and the branch will be deleted.

4. Transfer of blockchain concepts to industrial Internet-of-Things-systems

As already argued above, IIoT-systems require higher availability and reliability of information. In terms of prioritization, the total cost of a system, the size, weight or form factor are less relevant as long as they fulfill their function reliably. Therefore, lightweight protocols with the above derived properties of a blockchain have a high potential to achieve the required reliability for IIoT networks.

Already some blockchains support the connection of external devices – called *oracles* – such as Ethereum (ethereum.org) or Ripple (ripple.com) (Thomas and Schwarz, 2014) triggering on- or off-chain-applications, called smart contracts. But here, the sensors are only directly connected to the oracles without additional security, so IIoT-devices operate on the same security level, only storing their data on a blockchain instead of a database. Iota (iota.org) can be considered IoT-based blockchain-system (Popov, 2016). However, this again is a blockchain-technology on its own, which is not designed to be directly connected to other blockchains.

Consequently, a sensor-chain-like system needs to be developed, securing IoT-devices with blockchain methods, independent from the decision on which cloud based blockchain to use for storing or processing the data. In the following subsections, some design considerations derived from the criteria in the preceding section for a sensor-chain are described.

4.1 Device identification

If devices create data and data are considered as transactions, the transactions can only be checked for uniqueness and "double spending" (= malicious data) for a unique association to an IoT-device. Therefore, a unique identity (ID) is required.

For the IoT-blockchain, IDs will be composed of sets of different properties of an IoT-node. This may contain the device number, a binary representation of measured data types or its location for portable or mobile sensors. This ID will be cross-checked multiple times (Figure 3) by direct computation and comparison, the comparison by special nodes with extended capabilities and cross-communication and verification among those additional nodes.

It is also fraud proof as these *unique properties* can be verified: for example, the data types as potential element of such an ID can directly be seen in the transmitted data, or the

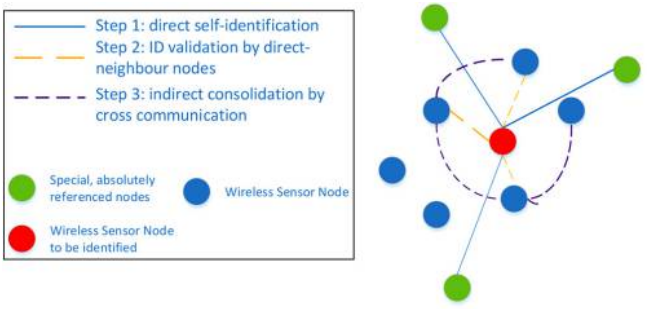


Figure 3.
Identification and verification process

position can be cross-checked with other principles such as triangulation of the signal strength.

This device identification makes the device and its data unique which is the most important precondition for the proof-of-work and consensus.

4.2 System topology, creating a blockchain and distributing a ledger

For an optimum performance in a potentially spatial–dynamic sensor network, the system topology is an important factor in terms of the desired functionality as well as the energy effort. Unlike a wired network with network nodes without any energy restriction, for IoT-devices in a WSN, a peer-to-peer network is not the first choice. Due to the limited communication range of the nodes, usually a multi-hop routing is required to bridge the distance to a border–gateway into another long range, e.g. a wired network. As nodes may sleep or move, node management has to be performed and a permanently updated routing table has to be maintained and communicated.

Therefore, an asynchronous unrouted point-to-multipoint broadcast-network with a longer listening- than sending-interval for every node is preferred. With a sufficient number of nodes – an assumption already arisen in section 3.2 for the pBFT – the messages of all nodes can be received by all nodes either directly or indirectly within a certain amount of time. Here, different neighborhood relationships of nodes and messages have to be considered (Skwarek and Monecke, 2016), basically distinguishing between ego-nodes (the actual node itself), direct and indirect neighbors.

A permanent process of receiving information from the network, packing this and own information into a new message and redistributing it, lead to a distributed ledger of all information available on the whole network (Figure 4).

Each sensor may not see all information of all other participants instantly, but over a certain time span, a full network-wide information map is created inside every sensor. Therefore, this is equivalent to a full-node ledger in blockchain terminology. The node-knowledge is spatially retarded and memory-wise limited. However, in a stationary network with sufficient node memory, the node- and system-knowledge become identical over the time. Realistically, the local node only carries an incomplete ledger.

4.3 Time-stamping and consensus

Realistically, all nodes have due to latencies during the information transfer and memory-caused limitations an incomplete and partially outdated picture of the complete network information (Figure 5). This requires every node to regularly update its node-knowledge with all messages received from all other nodes. As these messages may be incomplete, outdated, accidentally wrong or malicious, every node has to consolidate this information. False or outlying information will so be eliminated, and it is not possible to take part in the communication process with just inserting any arbitrary information into the network.

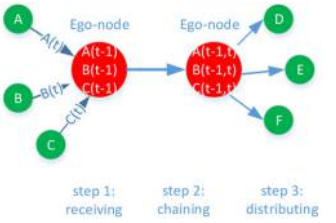


Figure 4.
Protocol steps of receiving, chaining and distributing

The outcome of this process should be a consolidated value, which will be further used by other network nodes during their consolidation process. Otherwise, this part of a message, which may be accidentally or intentionally wrong, may not be forwarded, neglected or even forgotten over time.

Now, a malicious node may actively try to change the order of information to pretend that all the measurements are right, but need to be reordered by changing time stamps of parts of the information history being broadcasted. Also, this history has to be equal to the node-knowledge of other network participants as they have also created a timeline of information.

4.4 Byzantine fault tolerance and scalable security

As derived and argued above, this network is a full implementation of the concepts of (p) BFT: With a high number of participants, multiple network paths due to message broadcast and many communication cycles with asynchronous repetitions of consolidated and historical cued messages, the conditions for at least the practical BFT are met. Singular false messages from malicious nodes can be detected and eliminated with various mechanisms as listed in the following text:

- *missing or unknown node ID*: if a node ID is not known, the node has no history among other nodes in the network, and therefore, it either may be directly excluded from message processing or has at least a very low reputation, until it has built up a history inside other nodes knowledge;
- *hijacked node ID*: as an ID is composed of several properties of a device and is more than a simple serial number, it can also be generated and cross-checked with additional information such as the nodes location. If all information is somehow captured and a false ID is successfully generated, the original correct node can create an alarm that something with its ID distributes messages that are not aligned with its own history. Therefore, a manipulation is at least detectable.
- *sending selectively wrong information*: single pieces of wrong information will be suppressed by the authorized nodes as they do not contain history information. Therefore, they cannot be sequenced or at least be sequentially checked against the other information and no timestamp can be created. As the timestamp will be missing or cannot be verified, "the block cannot be chained" and the information will be dropped.
- *sending sequences of wrong information*: the detection mechanism is similar to selectively wrong information. But here, the complete (historical) sequence also can be considered unknown be other nodes and can therefore be detected and suppressed.

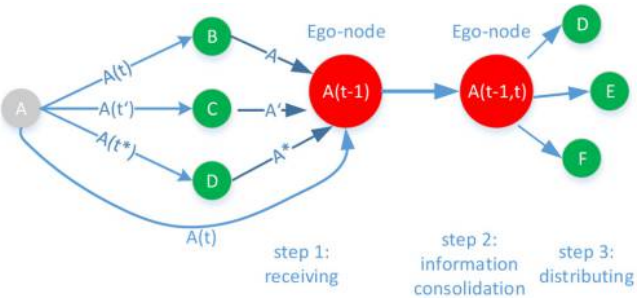


Figure 5.
Information consolidation phase

Consequently, with a low number of malicious nodes or information, wrong messages are detected. Only if one or many nodes start permanently intruding the IoT-network with continuous wrong information, they might be able to build up something like a history, which might eventually be accepted by other network participants as authorized and true information. However, this process will be accompanied by a preceding phase where the intrusion is detectable.

As this security process is time- and energy-consuming, it is scalable in terms of transferred length of history, consensus algorithms, rejection intensity and mechanisms and spatial and temporal map size within each node. Therefore, for a high security level, measures can be taken requiring a high level of energy. On the other hand, this mechanism may also be applied to energy-restricted systems with the risk of a lower security level.

5. Summary and outlook

In this article, a principle for increased information security for IIoT-systems organized in wireless sensor networks was presented. Mechanisms from blockchains and distributed ledger technologies were derived and adopted to microcontrollers, with a small energy budget and low calculation capabilities. It was shown that principles such as chained blocks, distributed ledger, time-stamping and consensus could be transferred. This leads to a higher effort for intruders to gain access to the communication process and to inject false information.

In the next steps of research, this concept will be implemented into different domains of application such as long- and short-distance communication, self-sufficient nodes with extensive sleep cycles and transferred to various cloud-based blockchains for permanent information-keeping.

References

Boucher, P. (2017), European Parliament, Directorate-General for Parliamentary Research Services, European Parliament, European Parliamentary Research Service, Scientific Foresight Unit, 2017, How blockchain technology could change our lives: in-depth analysis.

Bundesministerium für Wirtschaft und Energie, Referat Öffentlichkeitsarbeit (2016), *BMWi - Industrie 4.0 [WWW Document]*, Industrie 40 Digital, Wirtsch, available at: http://bmwi.de/DE/Themen/Industrie/industrie-4-0.html (accessed 12 April 2016).

Castro, M. and Liskov, B. (1999), "Practical Byzantine fault tolerance", *in Proceedings of the Third Symposium on Operating Systems Design and Implementation (OSDI '99)*, USENIX Association, Berkeley, CA, pp. 173-186.

Dargie, W. and Poellabauer, C. (2010), *Fundamentals of Wireless Sensor Networks: Theory and Practice*, Wiley, Chichester, West Sussex, Hoboken, NJ.

Farooqui, A. (2015), "Samsung is reportedly the world's largest smartwatch vendor [WWW Document]", available at: www.ubergizmo.com/2015/03/samsung-is-reportedly-the-worlds-largest-smartwatch-vendor/ (accessed 9 December 2017).

J'son and Partners Consulting (2015), "Russian and global market of hi-tech wearable devices, results of 2014 - IT, clouds, ecquipment & gadgets | RUSSIAN ANALYTICS [WWW Document]", available at: http://json.tv/en/ict_telecom_analytics_view/russian-and-global-market-of-hi-tech-wearable-devices-results-of-2014 (accessed 9 December 2017).

Kellermann, C. (2002), *Practical Byzantine Fault Tolerance Ein Algorithmus von Miguel Castro*, Uni Erlangen, Erlangen.

Lamport, L., Shostak, R. and Pease, M. (1982), "The Byzantine generals problem", *ACM Transactions on Programming language Systems (Toplas)*, Vol. 4 No. 3, pp. 382-401.

Libelium Comunicaciones (2015), *50 Sensor Applications for a Smarter World*, Libelium Communicaciones Distribudas S.L., Zaragoza/ESP.

Nakamoto, S. (2008), "Bitcoin: a peer-to-peer electronic cash system", available at: https://bitcoin.org/bitcoin.pdf

Obaidat, M.S. and Misra, S. (2014), *Principles of Wireless Sensor Networks*, Cambridge University Press, Cambridge, New York, NY.

Popov, S. (2016), "The Tangle (Whitepaper)", available at: Iota.org

Raghavendra, C.S., Sivalingam, K.M. and Znati, T. (Eds) (2006), *Wireless Sensor Networks*, Springer, New York, NY.

Ronen, E., O'Flynn, C., Shamir, A. and Weingarten, A.O. (2016), IoT Goes Nuclear: Creating a ZigBee Chain Reaction, available at: www.wisdom.weizmann.ac.il/~eyalro/iotworm/iotworm.pdf

Schneider, B. and Kelsey, J. (1997), "Cryptographic support for secure logs on untrusted machines", *Proceedings of the 7th USENIX Security Symposium: Presented at the 7th USENIX Security Symposium, San Antonio, TX*.

Skwarek, V. and Monecke, M. (2016), "Niedrigstenergie-Ortungsverfahren nach dem Prinzip der Schwarminitelligenz", presented at the VDE-IoT-Kongress, VDE Verlag, Mannheim.

Thomas, S. and Schwarz, E. (2014), "Smart oracles: a simple, powerful approach to smart contracts (Whitepaper)", Codius.

Zaninotto, F. (2016), "The blockchain explained to web developers, part 1: the theory", available at: http://marmelab.com/blog/2016/04/28/blockchain-for-web-developers-the-theory.html (accessed 9 December 2017).

Further reading

Skwarek, V. (2017), "Sensornetze und Schwarmintelligenz in industriellen Anwendungen", in Borgmeier, A., Grohmann, A. and Gross, S.F. (Eds), *Smart Services und Internet der Dinge*, Geschäftsmodelle, Umsetzung und Best Practice, Hanser, München.

Corresponding author

Volker Skwarek can be contacted at: volker.skwarek@haw-hamburg.de