

# Internet of Things

journal homepage: [www.elsevier.com/locate/iot](http://www.elsevier.com/locate/iot)

## Blockchain mechanisms for IoT security

Daniel Minoli\*, Benedict Occhiogrosso

DVI Communications, New York, NY, United States



### ARTICLE INFO

**Article history:**

Received 29 May 2018

Accepted 29 May 2018

Available online 14 June 2018

**Keywords:**

IoT

CPS

Blockchains

Security

Integrity

e-health

ITS

Consensus algorithms

Blockchain applications

### ABSTRACT

The deployment of Internet of Things (IoT) results in an enlarged attack surface that requires end-to-end security mitigation. IoT applications range from mission-critical predicaments (e.g., Smart Grid, Intelligent Transportation Systems, video surveillance, e-health) to business-oriented applications (e.g., banking, logistics, insurance, and contract law). There is a need for comprehensive support of security in the IoT, especially for mission-critical applications, but also for the down-stream business applications. A number of security techniques and approaches have been proposed and/or utilized. Blockchain mechanisms (BCMs) play a role in securing many IoT-oriented applications by becoming part of a security mosaic, in the context of a defenses-in-depth/Castle Approach. A blockchain is a database that stores all processed transactions – or data – in chronological order, in a set of computer memories that are tamperproof to adversaries. These transactions are then shared by all participating users. Information is stored and/or published as a public ledger that is infeasible to modify; every user or node in the system retains the same ledger as all other users or nodes in the network. This paper highlights some IoT environments where BCMs play an important role, while at the same time pointing out that BCMs are only part of the IoT Security (IoTSec) solution.

© 2018 Elsevier B.V. All rights reserved.

## I. Introduction

There now is considerable interest in the Internet of Things (IoT) as an evolution of data communications that allows direct, persistent, and automated device-to-device communication (also known as Machine-to-Machine [M2M] communication or Cyber-Physical Systems [CPSs] communication). This article is an overview and advocacy paper for the use of Blockchain Mechanisms (BCM) for certain security requirements in IoT in general and in e-health and Intelligent Transportation Systems (ITS) applications in particular. The principal applications of blockchains to date have been for financial transactions' execution, smart contracts, and cryptocurrencies. However, new potential applications are emerging.

An extensive body of literature related to IoT already exists – this body of literature being consistent with the broad reach of the evolving technology – including but not limited to text books such as [1–10] (and about 100 more) and many technical and research articles. The IoT endeavors to add computer-based logic to a large universe of objects or things, which can then be monitored and/or controlled by a centralized (often cloud-based) analytics or management engine; remote objects are almost invariably connected using wireless networks. In IoT, devices and entities in the physical world are afforded a digital representation. This digital ‘wrapper’ enables interaction with Information and Communications Technology (ICT) elements located on a Local Area Network (LAN), at the other end of a Wide Area Network (WAN), or on a public-, private-, or hybrid-cloud. Some proponents see IoT as the convergence of ICT and Operations Technology (OT) systems.

\* Corresponding author.

E-mail address: [daniel.minoli@verizon.net](mailto:daniel.minoli@verizon.net) (D. Minoli).

The IoT application space is significant; references [11–30] are just a small sample. Additionally, the overlay of drones and/or virtual reality/augmented reality adds yet another dimension. Up to the present, IoT applications have focused on two broad areas: industrial automation in the context of process control in factories, (Industrial IoT); and sensing applications of all sorts, including power grid administration, traffic monitoring, ITSs, smart cities, video surveillance, body area networks/e-health, and crowdsensing (to list just a few). These two areas deal a lot with the physical aspects of the sensors, the wireless link, and to some degree, with analytics. However, there is a third class of applications that deal less with the physical nature of the sensors themselves and a lot more with the data analytics: these applications address the fundamental transformation of Business Processes (BPs) related to common commercial functions such as banking, insurance, enterprise and organizational operations (including government functions), and healthcare delivery optimization. A new wave of Business Process Reengineering (BPR) is expected to take place as part of the Digital Transformation, and will be orchestrated by advancements in IoT ICT/OT capabilities.

Given the scope of the application space, security in the IoT environment is considered critical, especially under the circumstances of (typically) limited computational-, memory-, power-, and control capabilities of the end-nodes and the physical exposure of these end-nodes. While security is certainly important for the first two classes of applications listed above, it is absolutely critical for those business-oriented applications that almost invariably deal with Personally Identifiable Information (PII). Applications such as ITSs, e-health, infrastructure control, and drones may typically also have life-safety implications, therefore security concerns are paramount and dominant. Security and privacy are important end-to-end: starting in the access/edge/fog network, in the core network, and then (possibly) off to the service cloud. Considerable research and advocacy has been undertaken (e.g., [31–41]), but the technical and business needs remain a pressing imperative. This article reviews some of the challenges related to implementing security mechanisms in the IoT nodes and supporting networks; it then focuses on the application of Blockchains, which at a broad level are digitally signed distributed ledgers, to this ecosystem for both security and business logic.

## 2. IoT factors impacting security

The growing prevalence of embedded intelligent systems in virtually all types of consumer devices, and the mission-criticality of some applications (such as surveillance, e-health, and grid control), dictate the need for reliable security. The challenges associated with reliable security in IoT are driven by the following factors:

- IoT/CPS technology and systems are relatively new and are, therefore, less well understood than traditional IT systems.
- IoT/CPS systems are almost invariably distributed over a wide (regional) geography, typically in uncontrolled open environments.
- IoT/CPS systems are often administratively federated, in the context of multiple heterogeneous environments, processes, and technologies, not to mention the diffuse security mechanisms often in place.
- IoT/CPS systems are currently deployed insularly across vendor-specific vertical applications, creating fragmented technology and administrative silos.
- End-to-end comprehensive standards for architecture, networking, or security have not been developed, stabilized, adopted, or implemented; standardization would enable simplicity and the ability to integrate systems (including security) from best-in-breed vendors.
- IoT/CPS endpoints in different (vertical) applications often use different addressing models and addressing formats, creating complexity.
- IoT/CPS Operating Systems (OSs) may typically have streamlined feature sets that limit functional capabilities and/or sophistication.
- IoT/CPS systems often employ inexpensive, low complexity nodal platforms with limited computational power and memory, thus precluding or limiting the use of an on-board heavy-duty firewall, and,
- IoT/CPS endpoint systems have limited electrical power (typically being battery-driven).

The low power and low complexity factors are somewhat mitigated in a case where in an ITS application the sensors/actuators are located in a factory or in an automobile.)

The point of concentration where some (e.g., at a gateway point) or all (e.g., at an analytics cloud point) data are aggregated for managerial surveillance, decision-making, analytics, or storage, is clearly a target-rich environment for intrusion. The dearth or even lack of industry-adopted baseline IoT architectures and standards have limited not only the broad deployment of IoT but also have retarded the integration of security mechanisms into the IoT systems deployed in the field. The ISO/IEC JTC 1/WG 10 Working Group on Internet of Things recently identified over two-dozen reference architectures/frameworks [42], but none have enjoyed or achieved wide industry adoption. Interoperability is a key enabler, and lack of interoperability in both the “user plane” and also in the “management plane” (which encompasses security) impacts deployment scope, deployment timelines and system cost. Table 1 depicts a view of the “as is” (as well as a “to be”) security predicament in the IoT arena. To address some of these challenges, Fig. 1 depicts a reference architecture framework that can be utilized to organize the discussion of the IoT ecosystem and the security considerations.

**Table 1**

“As is” and “To be” IoT security environment.

General IoT layers	Device	Typical Status Quo (“As is”)	Target (“To be”)
<b>Lower layers</b>	Sensors (sensor to base station communication)	<ul style="list-style-type: none"> <li>• No encryption</li> <li>• Weak encryption</li> <li>• Weak communications protocols</li> <li>• No, or pro-forma passwords</li> <li>• Weak passwords</li> <li>• Weak, or no Access Control</li> <li>• Weak Operating Systems (OSs)</li> <li>• Hackable nodal application software</li> </ul>	<ul style="list-style-type: none"> <li>• <b>Blockchains for sensor data (optional but preferable)</b></li> <li>• Strong end-to-end encryption</li> <li>• Robust communication protocols</li> <li>• Use of Transport Layer Security (TLS)</li> <li>• Device health checks</li> <li>• Strong OSs</li> <li>• Strong applications</li> <li>• Strong Identification (ID)</li> <li>• Strong user interface</li> <li>• Memory isolation</li> <li>• Firmware over the Air (FOTA)</li> <li>• Hardware Root of Trust (RoT)</li> <li>• Trusted Execution Environment (TEE)</li> </ul>
	Base Station/Gateway	<ul style="list-style-type: none"> <li>• Weak communication protocols</li> <li>• Hackable device keys</li> <li>• Side channel attack vulnerabilities</li> <li>• Weak OSs in Network Elements (NEs)</li> <li>• Memory leakage</li> <li>• Zero-Day vulnerabilities</li> </ul>	<ul style="list-style-type: none"> <li>• <b>Blockchains for aggregated data</b></li> <li>• Hardware RoT</li> <li>• Strong encryption for data at rest</li> <li>• Strong encryption for transit data</li> <li>• Secure boot</li> <li>• Secure key storage</li> <li>• TEE</li> <li>• Trusted firmware</li> <li>• Anti-rollback mechanisms</li> <li>• Secure counters and clocks</li> </ul>
<b>Upper Layers</b>	Key Management Public Key Infrastructure [PKI])	<ul style="list-style-type: none"> <li>• Weak encryption</li> <li>• Weak communication protocols</li> <li>• Weak OSs</li> <li>• Ability to compromise encryption keys</li> </ul>	<ul style="list-style-type: none"> <li>• Secure Key provisioning</li> <li>• High frequency key rotation</li> <li>• Nested encryption/keys</li> </ul>
	Data Servers/cloud analytics	<ul style="list-style-type: none"> <li>• No encryption for Data At Rest</li> <li>• Weak encryption</li> <li>• Weak communication protocols</li> <li>• Weak media (e.g., unprotected wireless links)</li> <li>• Weak access control</li> <li>• Weak OSs</li> <li>• Hackable analytics application software</li> <li>• Zero-Day OSs and application vulnerabilities</li> <li>• Untested/unreliable third-parties plugins/software modules</li> </ul>	<ul style="list-style-type: none"> <li>• <b>Blockchains end-to-end</b></li> <li>• Strong/tested application</li> <li>• Strong encryption for Data at Rest and data communication</li> <li>• Multi-layer security</li> <li>• Strong communication protocols</li> <li>• Secure physical networks and/or Virtual Private Networks (VPNs)</li> <li>• Strong OSs</li> <li>• Reliable/routine patch processes</li> </ul>

In general terms, cybersecurity has traditionally addressed the following:

- Confidentiality (C): making sure that the data packets are not intercepted and examined; also, making sure that the host is not corrupted to the point that a hacker can appropriate data, credentials, information, or configuration parameters (keeping the data safe from being divulged by/to unauthorized agents).
- Integrity (I): making sure that the packets received (or stored) have not been altered in an unauthorized manner (making sure the data is not modified by unauthorized agents).
- Availability (A): making sure that devices are not prevented from functioning properly and/or performing their function; or, making sure they are not made to operate in an improper or compromised manner. For example, the devices might become infected with viruses, worms, or degraded via other debilitating intrusions and/or exploited through weaknesses in the OS, software utilities, packaged microcode or applications. The term “no repudiation” has also been used in the context of availability.

Other security anomalies can broadly be mapped to these three categories. For example, *Trust & Identity Management* can be categorized as part of the Integrity requirement (i.e. can the user or the data be trusted?) Additionally, one needs to tightly manage how software is modified (e.g. in a system upgrade event), and, also, control how data is modified by a legitimate entity. Blockchain mechanisms are ideal for this requirement. *Authorization & Authentication* can be viewed as supporting part of the Integrity requirement (who is the ‘user’, what privileges does the user have, and what data sets or subsets can this user read/write/modify?)

These requirements apply equally well to IoT/CPS environments. Fig. 2 provides a high-level overview of the requirements and some supportive mechanisms. Confidentiality is achieved with encryption (including VPNs and encryption of data at rest). Integrity can be achieved with digital signatures. When the data is transacted among multiple downstream parties (for example contracts, chain-of-custody, e-health claim processing, and so on), recursive digital signatures as seen

<b>7: Applications</b>	<b>Large pool of IoT applications</b>					<b>In-layer Security</b> Blockchains Authentication & Authorization Encryption & Key Management Trust & Identity Management		
<b>6: Data Analytics &amp; Storage</b>	(Medical) Engine	(Institutional) Engine	Cloud (Medical) SaaS/Big Data	Internet & App Store (Medical/health Apps)	Cloud Storage	<b>In-layer Security</b> Blockchains Authentication & Authorization Encryption & Key Management Trust & Identity Management		
<b>5: Data Centralization</b>	Firm's Intranet	Extranet	Public Cloud	Private Cloud	Hybrid Cloud	(protocols such as but not limited to IPv4, IPv6, MIPv6, PMIPv6, 6LowPAN, 4G/5G, Satellite/LEO/HTS)		<b>In-layer Security</b> Authentication & Authorization Encryption & Key Management Trust & Identity Management
<b>4: Data Aggregation</b>	Edge Networking		Edge Gateway				<b>In-layer Security</b> Blockchains Authentication & Authorization Encryption & Key Management Trust & Identity Management	
<b>3: Fog Networking</b>	Wired (e.g., LAN)	Wireless (e.g., BAN, PAN, ZigBee 3.0, Bluetooth 4.0, LAN)	Wireless (LPWAN, Sigfox, LoRa, Weightless, 4G/5G, Satellite)				<b>In-layer Security</b> Authentication & Authorization Encryption & Key Management Trust & Identity Management	
<b>2: Data Acquisition</b>	Hub	Hub	Hub	Hub	Hub			<b>In-layer Security</b> Blockchains Authentication & Authorization Encryption & Key Management Trust & Identity Management
<b>1: Things (medical devices example)</b>	ECG/EKG Sensor Inertial Sensor	Blood Pressure Sensor Pulse Oximetry Sensor	Medicine Pump Fitness/exercise Sensor	Video Surveillance Panic Button	(partial list)		<b>In-layer Security</b> Blockchains Authentication & Authorization Encryption & Key Management Trust & Identity Management	

Fig. 1. IoT reference framework.

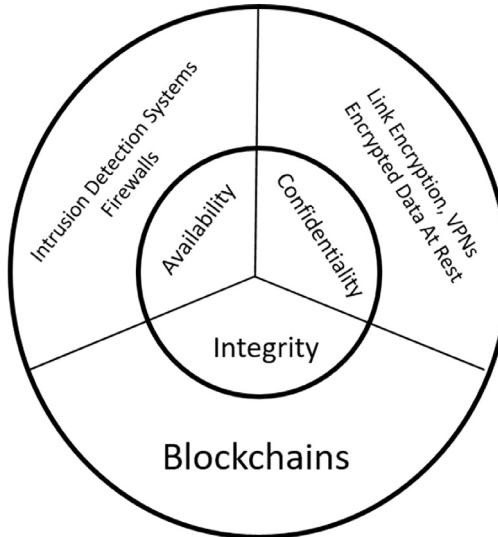


Fig. 2. Security mechanisms for IoT/CPSs.

in blockchains may be ideal. Availability may, in part, be managed with Intrusion Detection mechanisms. Note that the detailed security requirements of distinct IoT systems and applications may differ; therefore, not all IoT/CPS nodes need to comply with the tightest security restrictions; security policies will likely be consistent with the application, the risks and the practical limits of the devices in question. In some applications (e.g., e-health, physical patient monitoring) there typically is a stringent privacy requirement (some even dictated by regulatory regimens); thus, strong security mechanisms are needed. Other applications such as e-mail, videoconferencing, chatting, messaging, or social networking, may require less stringent security.

In some applications there is a need for the IoT/CPS nodes to enjoy a degree of “distributed autonomy”, that is, having the ability for distributed local decisioning, ad hoc self-organization, and topology discovery/management. Examples of autonomous operation include vehicular ad hoc networks (VANETs), ITSs, or a single or a swarm of robots – as more IoT/CPS applications emerge the trend towards autonomous operation of the endpoint devices and towards self-organizing network paradigms will likely accelerate. In these cases, the security considerations are even more critical. In autonomous operation individual endpoints (or clusters of endpoints) are not dependent on a central or cloud-based entity to fulfill their sensing and data collection functions. It follows that a security compromise may not be detected by a centrally-located control and audit system. Appropriate security mechanisms are thus required.

For ITS, Integrity is universally required whether for real-time Vehicle-to-Vehicle (V2V) or Vehicle-to-Infrastructure (V2I) communication, or for administrative traffic such as telemetry and engine functioning, or for example, accident data. Confidentiality (via encryption) is often needed. Availability (non-repudiation) is universally required for V2V and V2I traffic and often needed for other functions.

### 3. Blockchain concepts

The concept of *blockchains* is now receiving considerable research and practical interest. Blockchains provide data integrity across a large number of transactional parties by providing all participants in the ecosystem with a working proof of decentralized trust; classically, this assurance of integrity had to be achieved by utilizing a trusted third party to ‘escrow’ elements of the transaction – a blockchain replaces this trusted third party. A blockchain is a cryptographically-linked list of blocks created by nodes, where each block has a header, the relevant transaction data to be protected, and ancillary security metadata (e.g., creator identity, signature, last block number, and so on.). It facilitates “decentralized consensus” by being a distributed ledger (which is effectively a distributed database), that retains a(n expanding) list of records, while simultaneously precluding revision or tampering of such records retrospectively. Because blockchains are intrinsically resistant to modification of the underlying data, they are perceived as embodying a tamper-resistant incorruptible decentralized digital ledger for economic or logical transactions related to virtually anything of value [43–48]. The blockchain intrinsically provides universal accessibility, incorruptibility, openness and the ability to store and transfer data in a secure manner. Many applications of blockchains have emerged in the recent past beyond the original applications of cryptocurrency, such as bitcoins. The data can, in fact, represent a wide variety of elements, documents, facts, packets, transactions, agreements, contracts, monetary transactions, or signatures. A blockchain can support a wide range of tasks, including allowing parties to draw up trustworthy contracts, storing sensitive information, and transferring money safely—all without the intervention of an intermediary. Possible business applications include claims filing/processing; claim fraud detection, for example to spot multiple claims from a claimant (e.g., medical office) for the same procedure; data decentralization; and cybersecurity management (e.g., data integrity). Another application example is the introduction of new, smart logistics-oriented contracts where invoices pay themselves when a shipment is accepted by the recipient. Additionally, there often are requirements to verify the authenticity of items and systems through multi-stage multi-national supply, distribution and service chains (that might raise concerns about counterfeit items and/or the requirement of tracking legally controlled items such as medicines, medical devices, controlled pharmaceutical substances, arms, negotiable bonds and so on.) An important, proposed application of blockchains is for cybersecurity, specifically for Integrity.

It is not the goal of this paper to provide a formal definition of a blockchain (or a bitcoin); the mathematics of a formal definition are somewhat complex (e.g., see [49–59]); rather, the goals are to provide a brief overview of the blockchain technology, to identify some possible use cases in the IoT environment in general and ITSs in particular, and to advocate further research and development in this arena.

At a broad level, blockchains offer a mechanism for people (or entities) who do not know or trust each other to create a shared record of asset ownership. A blockchain is an “open platform”, a distributed system where the processes are open to examination and elaboration. It is a ledger of data, replicated across a plurality of computers organized in a Peer to Peer (P2P) network. Thus, a blockchain records the transactions on a multitude of distributed hosts, given that a replicated, decentralized database effectively eliminates the possibility of global data corruption (deliberate or accidental). The blockchain is a time-stamped database that retains the complete logged history of transactions on the system; each transaction processor on the network or system retains their own local copy of this database and consensus-formation algorithms allow every copy, no matter where such copy is, to remain synchronized. Specifically, a blockchain consists of *blocks* that hold sets of valid transactions; each blockchain block incorporates the hash of the prior block in the blockchain, juxtaposing the two blocks. The linked blocks form a chain.

Members of the network are anonymous entities (processes, individuals, or users) known as *nodes*. Nodes perform a variety of functions depending on the assumed role. A node can create and propose a transaction, validate transactions, and undertake mining to support consensus and establish the integrity of the data. When nodes create transactions, these are signed by nodes using their private key to validate that these nodes are the true owners of the asset that they are transferring to someone else in the blockchain-secured network. In a blockchain, a P2P network is required as well as consensus algorithms to ensure replication across nodes are undertaken. *Peers* support the state of the distributed ledger. The P2P function implies that there is no central control in the blockchain-secured network and all nodes can communicate directly with each other using an appropriate protocol, allowing for transactions (e.g., documents, data, cryptocurrency) to be exchanged directly among the peers. There typically are two types of peers: *Endorsing peers* and *Committing peers*. Endorsing peers

simulate the transaction execution: they execute and endorse the transaction; endorsement policies specify the rules for the transaction endorsement. Committing peers receive transactions endorsed by endorsing peers, verify these transactions, and update the ledger – they may also be *Orderer nodes* that receive transactions from endorsers, sequence them, and forwards these transactions to committing peers.

Therefore, nodes can be *miners* or *block signers*. Miners create new blocks containing relevant data (to be protected). Block signers validate and digitally sign the transaction. An important assessment that every blockchain network must make is to determine which nodes are able to append a next block to the chain. This decision is made utilizing a *consensus mechanism*. Miners are able to add transactions, verify transactions, and add new blocks. Interactions inside the network utilize cryptographic means to securely identify the source and the sink of the data. When a node (miner) wishes to add data to the ledger, a consensus forms in the network to establish where this data should be captured in the ledger. The blockchain encompasses a data structure of ‘child’ (aka successor) blocks; each block includes sets of transactions, timestamps and links to a ‘parent’ (aka predecessor) block; the linked blocks constitute a chain.

Typically, the consensus mechanism encompasses three steps: the transaction endorsement process where the transaction is simulated by an appropriate process; the ordering process, which decides the sequence in which endorsed transactions are written into the ledger; and validation and commitment process, where committing peers validate the transaction received from the orderers and then commit that transaction to the ledger itself. The P2P messages utilized in the network typically support discovery (initial discovery of other peers in the blockchain-secured network), transaction (querying, invoking, and deploying transactions), synchronization (keeping the blockchain updated on all nodes), and consensus (endorsing the transaction).

In a general model, a transaction (e.g., a cryptocurrency transaction, a contract, some compiled business form) between two parties is captured by a supporting node (host.) The requested transaction is distributed to a P2P network of nodes. Some transaction validation may take place using some baseline user status or token and known algorithms. Scripts are definable logical functions. In their basic, and most often used form they validate a digital signature against a public key. The transaction supports host check if the conditions specified in scripts are satisfied. Once the transaction is verified, the transaction documentation is combined with other transactions to create a new block of data for the distributed ledger. The new block is added to the existing blockchain in a manner that makes the transaction unalterable and permanent. Thus, the information held on a blockchain is a shared database that is automatically and consistently reconciled; that is to say, the blockchain database is not domiciled or stored in any single host or computer, and as a result the records it embodies are expressly public and directly verifiable. No single centralized copy of this information exists that a hacker could corrupt by malicious modification: hosted by many computers simultaneously the data is accessible to one and all. Blockchain technology provides intrinsic data robustness. Since the data is stored as blocks of information that are identical across all the nodes in the P2P network, the blockchain cannot be controlled, manipulated, altered, or deleted by any single entity.

Once a miner node connects to the P2P network, a miner must undertake a number of tasks. These include the most or all of the following [49]. (i) Synchronization with the network: download the pertinent blockchain by requesting historical blocks from other network nodes. (ii) Validation of the transaction: transactions that are transmitted over the network are validated by nodes with full functionality by verifying and validating digital signatures and outputs. (iii) Validation of the block: validating blocks against established rules; this covers each transaction in the block and the nonce value. (iv) Creation of new blocks: as noted, miners can propose a new block by combining validated transactions received over the network. (v) Perform Proof of Work (PoW): miners find a valid block by solving a computational puzzle: miners repeatedly vary the nonce field contained in the header until the hash thus generated is smaller than a predetermined threshold value. (vi) Fetch of the reward: once the node has solved the PoW puzzle it broadcasts the results, allowing other nodes to verify and accept the block; if the block is accepted the miner is “somehow” rewarded. Note that the PoW requires non-trivial computational resources. Some of the steps include retrieving the previous block’s header, gather a set of transactions transmitted over the P2P network into a proposed block; compute the double hash of the previous block’s header with a nonce and the proposed block; establish if the thus-computed hash is smaller than the current threshold difficulty level and the successful PoW problem is solved broadcast the block to the network (and fetch the reward); otherwise repeat the last step.

Blockchains make extensive use of hashing. A hash is an algorithm (for example, the Secure Hash Algorithm Two [SHA-2]) that generates a value based on the data object (such as a message or file, which is typically of variable-length), thus mapping that data object to a smaller fixed-size data object (the “hash result”). Fig. 3 provides a pictorial example. Typical uses of hashing are one-way functions to protect computer passwords retained in storage, or to produce cryptographic digests of texts or documents (in order to ensure data integrity, thereby providing an electronic signature). A cryptographic hash function is a mathematical mapping function for which it is computationally difficult to find a data object that maps to a given hash result (the “one-way” property), or to find two data objects that map to the same hash result (this known as the “collision-free” property). A Merkle tree (also known as hash tree) is a logical tree where leaf nodes are labelled with the cryptographic hash of a data block and non-leaf nodes are labelled with the hash of the labels of its child nodes. Hash trees enable secure and efficient verification of the contents of given data structure [48].

In a blockchain each transaction in the set that comprises a block is hashed to generate a hash value. Hashes are combined into a Merkle Tree. The output of this hashing process is added to the block’s header, along with a hash of the previous block’s header and a timestamp. The new header is input to a cryptographic process to generate a (32-bit) nonce. The nonce is then added to the blockchain.

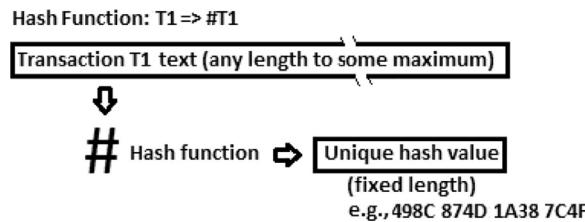


Fig. 3. Hash function.

#### 4. IoT blockchain approaches

Fundamentally the IoT can utilize blockchains to ensure integrity of the business logic data. Table 2 depicts the possible use of blockchains at various layers of the reference architecture framework (an example for e-health applications is also included in the table).

It should be noted that the mechanisms discussed above (P2P network participation, support of appropriate P2P protocols, endorsing peer functionality, committing peer functionality, support of the consensus algorithms, PoW and other related mechanism) give rise to certain overall complexity, especially if the P2P infrastructure is established globally, across an entire IoT ecosystem. Because of the typical limitations of IoT nodes, as discussed in Section 2, it may not always be practical to utilize a full-fledged blockchain-secured network in the generic IoT context; however, certain critical or institutional applications such as smart grids, ITSS, e-health, insurance, and smart contract environments may have sufficient capabilities to support the requisite P2P functionality. Another approach is to establish P2P networks having locally limited scope instead of global scope; this implies that the supporting messages – discovery, transaction querying, invoking, synchronization and consensus – require less aggregate bandwidth and far-end assurance of reliable delivery across large networks; also, the number of transactions and/or blocks to be processed and stored may be smaller. The potential limitations of implementing such roles in generic IoT nodes to create distributed ledgers due to limited computing and storage capacity of IoT devices is perhaps evident and the blockchain capabilities may thus have to be implemented in selected Network Elements (NEs) in the network, as discussed below. One would not expect that a low-end pendent IoT node, such as remote sensor or actuator would vouch for integrity of the entire ecosystem data; thus, only some select NEs may be expected to take on that more onerous role. Another approach would be to use a simple distributed ledger where blocks are digitally signed along the way, but the more elaborate consensus process is not implemented: based on the list of functional requirements listed above for miners.

*End-to-end blockchains.* The source (here being a “miner”) creates a transaction block containing data and creates the first block. Other NEs will append the next block in the blockchain, as the information travels through the network to its ultimate (intended) destination, typically some analytics engine in the cloud for analysis, trending, and likely also storage. Here storage also enjoys the integrity protection of the blockchain. For example, these transactions could be claims, accident photos, and so on.

*Analytics/storage-level.* This is mostly the same as the end-to-end blockchain, except that the transaction is ‘consumed’ at the analytics engine, where the data is extracted and utilized. Here storage would not enjoy the integrity protection of the blockchain, but for some applications (for example, environmental parameter sampling) may be adequate.

*Gateway-level.* Here the individual pendent users create data that is not immediately protected for integrity; however, once the data reaches the gateway, it is incorporated into the blockchain along with data from other users. Fig. 4 is an example of this. One motivation for this approach is that the individual end nodes may lack the computational capabilities to create hashes of (possibly large) blocks of data.

*Site-level.* Here the individual users at a given site (for example sensors or robots on a factory floor) create data that is not immediately protected for integrity at the device level; however, once the data reaches the local concentration node (for example a layer 2 switch, a Wi-Fi access point, a router, a firewall, and so on), it is incorporated into the blockchain along with data from other site users. Again, one motivation for this approach is that the individual end nodes may lack the computational capabilities to create hashes of (possibly large) blocks of data, but the site-based NE would have the computational power.

*Device level.* Here each individual device has the capability, as well as the imposed requirement, to build blockchains of data to be immediately protected.

#### 5. IoT blockchain applications

By way of an example of IoTSec blockchains, we noted above that for ITSS, Integrity is universally required; Confidentiality is often needed, and Availability (non-repudiation) is universally required for V2V and V2I traffic and often needed for other functions. In the example depicted in Fig. 4, gateway-level blockchains are used to ensure integrity of the data in question (for example engine data, Usage-Based Insurance [UBI] data, environmental sensor-data, and so on): the blockchain is started

**Table 2**

In-layer security mechanisms and various uses of blockchains.

Layer	Description	Use case example: e/m-health application	In-layer security mechanism
<b>Layer 7 Applications</b>	This layer encompasses a vast array of horizontal and/or vertical applications or “application domains” (Use Cases.) The list of applications is ‘unlimited’: applications include e/m-health, smart cities, smart building, smart grid, intelligent transport, surveillance, sensing, crowdsensing, intelligent production, and logistics, and so on	The e/m-health application has specific requirements, e.g., regulatory requirements, security requirements, reliability and availability requirements, and so on.	<b>“End-to-end” Blockchains</b> (ideal); application-specific (e.g., e-health); User Case-level Authorization & Authentication; Encryption & Key Management; Trust & Identity Management (these mechanisms being properly adapted to this layer of the IoT ecosystem).
<b>Layer 6 Data analytics and storage</b>	This layer encompasses the “data analytics and storage functions”.	This layer describes functions and possible standardization of medical-related analytics engines. These would be specific to the medical discipline supported by the application, for example, a glucose analysis tool, an oximeter analysis tool, and ECG analysis tool, and so on	<b>“Analytics/storage-level” Blockchains:</b> Storage and analytics applications (enterprise-based and/or cloud-based) Authorization & Authentication; Encryption & Key Management; Trust & Identity Management (these mechanisms being properly adapted to this layer of the IoT ecosystem).
<b>Layer 5 Data centralization</b>	This layer supports the “data centralization” function. This corresponds to the core networking functions of modern networks. It includes the functionality of typically found in institutionally-owned (core) networks, industry-specific extranets, public/private/hybrid cloud-oriented connectivity, and Internet tunnels. These networks achieve their functionality utilizing carrier-provided connectivity services and infrastructure and utilize wireline and/or wireless links.	This layer describes the functionality of a core network used to provide, say a city-wide or campus-wide, medical/health services in the context of an IoT-based application. Typically, it would not be a network completely dedicated just to the medical services (otherwise it would be quite expensive), but shared with other applications.	Core network Authorization & Authentication; Encryption & Key Management; Trust & Identity Management (these mechanisms being properly adapted to this layer of the IoT ecosystem).
<b>Layer 4 Data aggregation</b>	This layer supports the “data aggregation” function. This function may entail some kind of data summarization or protocol conversion (for example mapping from a thin, low complexity protocol used by the IoT clients in consideration of low-power predicaments, to a more standard networking protocol), as well as the edge networking capabilities. The data aggregation function is typically handled in a “gateway” device. Edge networking represents the outer tier of a traditional network infrastructure, the access tier, employing well-known networking protocols.	There may be data summarization points in a network that is used to support IoT medical applications and/or shared with other applications.	<b>“Gateway-level” Blockchains:</b> Data Aggregation (network) Authorization & Authentication; Encryption & Key Management; Trust & Identity Management. (these mechanisms being properly adapted to this layer of the IoT ecosystem).
<b>Layer 3 Fog networking</b>	This layer supports “fog networking”, that is, the localized (location- or neighborhood-specific) network that is the first hop of the IoT client (‘device cloud’) connectivity. Typically, fog networking is optimized to the IoT clients’ operating environment and may use specialized protocols. It could be a wired link (e.g., on a factory LAN say in a robotics application), or a wireless link (on a wireless LAN).	This layer supports the initial communication link used by the medical devices. For example, but not limited to ZigBee, Bluetooth Low Energy (BLE), Wi-Fi, cellular links, and so on.	Fog network/edge network Authorization & Authentication; Encryption & Key Management; Trust & Identity Management (these mechanisms being properly adapted to this layer of the IoT ecosystem).

(continued on next page)

**Table 2** (continued)

Layer	Description	Use case example: e/m-health application	In-layer security mechanism
<b>Layer 2 Data acquisition</b>	This layer encompasses the “data acquisition” capabilities. It is physically constituted of sensors (appropriate to the “thing” and the higher layer “application”), embedded devices, embedded electronic, sensor hubs, and so on. Layer 1 and Layer 2 could be seen as being in symbiosis in the IoT world in the sense that things “married” with sensors become the IoT clients or endpoints. The collected information might be data parameters, voice, video, multimedia, localization data, and so on.	This layer encompasses local concentration devices (base stations) that collect the local signals and data in preparation for additional packaging for upstream transmission. It could be a home-based device that aggregates all the IoT signals in a home, also including signals from the medical devices, or an in-hospital in-room device that aggregates the various monitors worn by a patient.	<b>“Site-level” Blockchains:</b> Aggregation link Authorization & Authentication; Encryption & Key Management; Trust & Identity Management (these mechanisms being properly adapted to this layer of the IoT ecosystem).
<b>Layer 1 Things</b>	This layer is comprised of the universe of “things” that are subject to the automation offered by the IoT. This is a large domain, including (for example) people (with wearables, e/m-health medical monitoring devices, etcetera), smartphones, appliances (e.g., refrigerators, washing machines, air conditioners, etcetera), homes and buildings (including HVAC and lighting systems), surveillance cameras, vehicles (cars, trucks, planes, construction machinery), utility grid elements, and so on.	This layer encompasses medical devices both for in-patient and out-patient applications, as listed in Fig. 1. For example, but not limited to Glucose Meter, Pulse Oximeter, ECG monitor, Event Alerting Device, and so on.	<b>“Device-level” Blockchains:</b> Device level Authorization & Authentication; Encryption & Key Management; Trust & Identity Management (these mechanisms being properly adapted to this layer of the IoT ecosystem).

in the gateway (the reason could be that it might be too onerous to start the blockchain in the remote device in the car itself.)

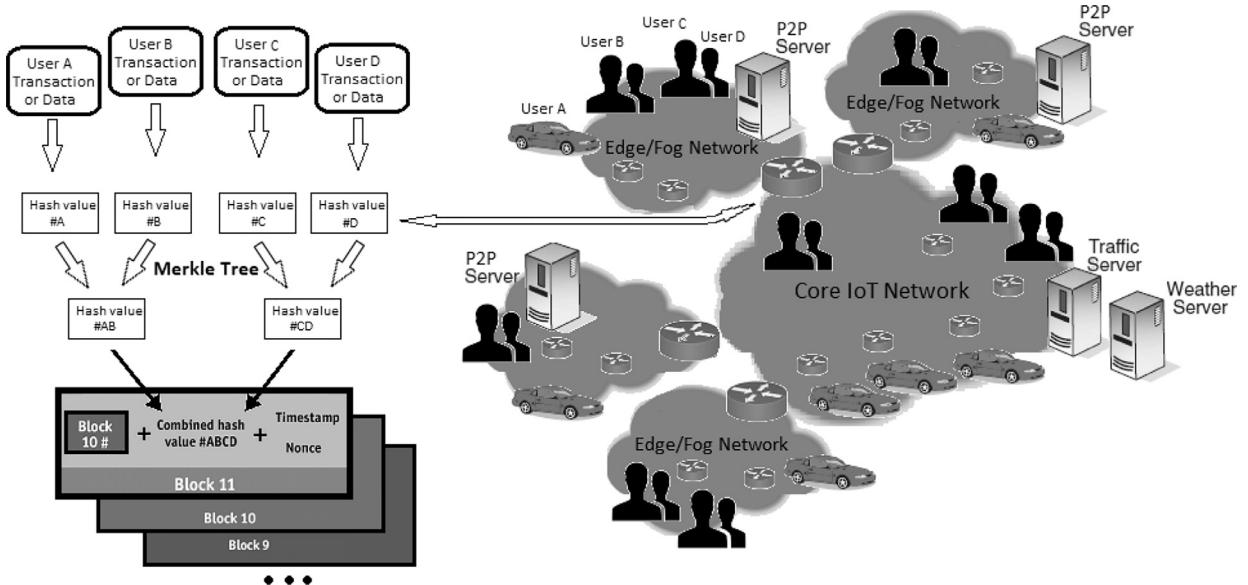
In an IoT-enhanced ITS environment, data generated by a cluster of sensors may be aggregated at a gateway point (V2V and V2I data would typically remain strictly local, but some summarized or administrative data may well be forwarded to a central repository). The aggregated data can be regarded as a transaction that is secured via a blockchain generated at that point. The data is further sent along to a host computer that may belong to some institutional or corporate entity (which may possibly add information at that point), (where again the data may be captured under a blockchain transaction), and then possibly passed up to some node in the cloud, or stored and/or archived somewhere. Fig. 5 illustrates an e-health IoT security application; in this example the gateway-level or site-level device acts as a miner and creates a blockchain for the medical information to be transmitted to the remote medical institution (encryption of the original content may typically also be required.).

At present, It is unclear which version of the above-listed blockchain approaches will be implemented (in a given vertical application or in a given platform); however, blockchains can and may well be used at the application level to validate all types of transactions. For example, the payment of a parking fee as it makes its way through the various financial entities supporting the transaction; or guaranteeing the content of chain-of-custody of some graphic, photograph, image, video, or data form. Other ITS-related applications might include insurance data, such as for UBI applications, or data related to fractional ownership of autonomous vehicles. Moreover, data may include medical sensor data, medical claims, video surveillance screenshots, and so on (e.g., [60,61].)

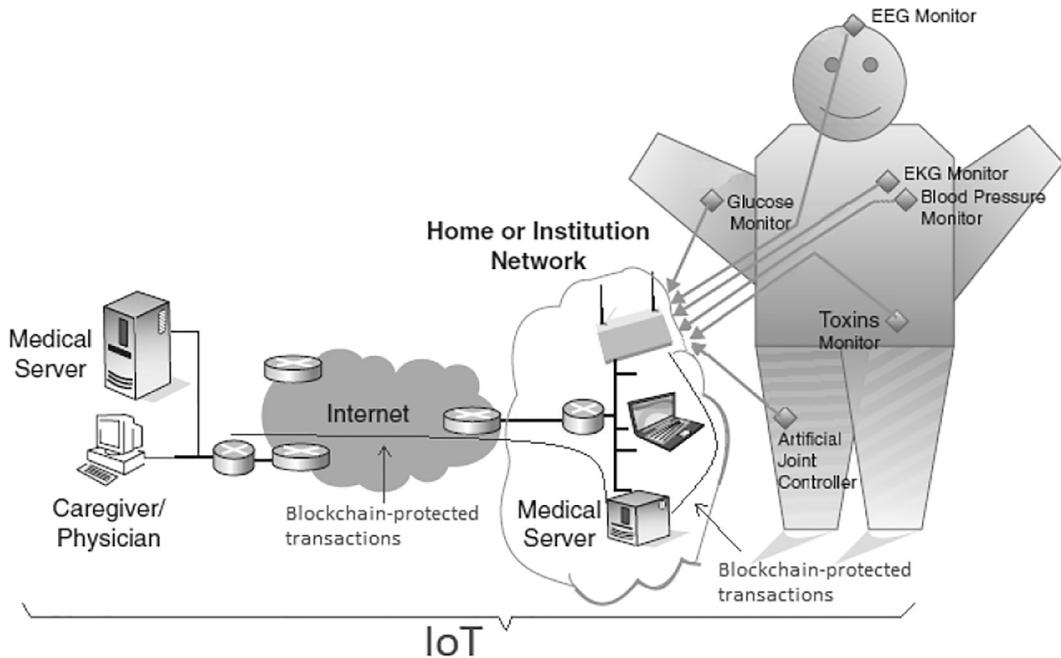
Blockchains can also be used at the lower layer of the communications model to provide integrity for information transfer over a chained number of links, converging from the edge towards a centralized analytics engine or a cloud-based server.

Beyond security per se there are many other applications of blockchains in the IoT environment; these include, but are not limited, to the following:

- Manage device configuration, store sensor data, and enable micro-payments [62];
- support e-business on the IoT (UBI is one example) [63];
- create decentralized, shared economy applications that allow people to monetize their things to create wealth; beyond Airbnb and Uber there are many other opportunities to share in the digital economy, for example sharing applications, e.g., peer-to-peer automatic payment mechanisms, foreign exchange platforms, and digital rights management [64];
- supply-chain provenance [65];



**Fig. 4.** Application of blockchain to smart city/vehicular traffic/ITS IoT/CPS (gateway example).



**Fig. 5.** Application of blockchain to e-health (example).

- Smart Cities [66];
- IoT devices need to communicate and synchronize with each other: using blockchain one can control and configure IoT devices (e.g., manage keys using RSA public key cryptosystems where public keys are stored in Ethereum and private keys are saved on individual devices) [67]; and,
- software push to remote devices, especially IoT devices [68].

## 5. Conclusion

The blockchain concept was originally associated with digital currency, but many other potential uses for the technology are emerging, including Integrity applications for IoT data being transacted around a large multi-tier network and/or archival systems. Blockchains are powerful tools that well beyond basic security applications, as described in this paper,

because they are principally mechanisms for global shared trust. However, because of the typical limitations of IoT nodes it may not always be practical to utilize a full-fledged blockchain-secured network in all IoT applications – certain critical or institutional applications such as smart grids, ITSs, e-health, insurance, and banking may entail nodes with sufficient capabilities to support the requisite P2P functionality.

Even then, while blockchains facilitate IoT Integrity, to support the philosophy of defenses-in-depth, BCMs have to be combined with other security mechanisms including firewalling, encryption, trusted execution environment (secure OSs and secure software updates) and other authorization, authentication, and accounting mechanisms. To the degree that certain firewalling mechanisms are able to be embedded in the end nodes, the developers should do so, because these firewalling mechanisms will (hopefully) protect a group or ensemble of system/ITS nodes from being attacked should a hacker get access to any single node, say in a car he or she may own and/or compromise. The advantage of using blockchains is that they can work at the lower layer of the communications models as well as at the application layer, thus enabling the synergistic use of the mechanism across layers and domains of the IoT ecosystem.

Future research should be directed, among other efforts, at identifying which IoT applications are best suited, at the practical level, to implement blockchain-based security mechanisms and how the distributed ledgers (databases) that support IoT can be optimally implemented. Also, establishing which of the implementation “topologies” described above for creating blockchains at various points in the network are best suited for a given vertical application or in a given platform.

## References

- [1] A. Bassi, M. Bauer, M. Fiedler, T. Kramp, R. van Kranenburg, S. Lange, S. Meissner (Eds.), *Enabling the Internet of Things*, Springer, 2013.
- [2] A.K. Pathan (Ed.), *Securing Cyber-Physical Systems*, CRC, 2015.
- [3] A.M. Rahmani, P. Liljeberg, J.-S. Preten, A. Jantsch, *Fog Computing in the Internet of Things*, Springer, 2017.
- [4] Q. Hassan, A.R. Khan, S.A. Madani (Eds.), *Internet of Things: Challenges, Advances and Applications*, CRC Press, 2017 ISBN 9781498778510.
- [5] A. Pal, B. Purushothaman, *IoT Technical Challenges and Solutions*, Artech HouseISBN: 978-1-63081-111-2, Norwood, Mass, 2016.
- [6] A. Rayes, S. Salam, *Internet of Things From Hype to Reality*, Springer, 2016.
- [7] A. Romanovsky, F. Ishikawa (Eds.), *Trustworthy Cyber-Physical Systems Engineering*, CRC, Boca Raton, FL, 2017.
- [8] B. Adryan, D. Obermaier, P. Fremantle, *The Technical Foundations of IoT*, Artech House, 2017.
- [9] B. Familiar, *Microservices, IoT and Azure*, Springer, 2015.
- [10] D. Minoli, *Building the Internet of Things with IPv6 and MIPv6*, Wiley, 2013.
- [11] S. Srivastava, N. Pal, *Smart cities: the support for Internet of Things (IoT)*, *Int. J. Comput. Appl. Eng. Sci.* (2016) 5–7 Jorhat6.1.
- [12] A. Zanella, N. Bui, A. Castellani, L. Vangelista, M. Zorzi, *Internet of Things for smart cities*, *IEEE Internet Things J.* 1 (1) (2014) 22–32 Page(s)Online ISSN: 2327-4662, doi:10.1109/JIOT.2014.2306328.
- [13] A. Alghamdi, S. Shetty, *Survey toward a smart campus using the Internet of Things*, in: *Proceedings of the 2016 IEEE FORTH International Conference on Future Internet of Things and Cloud (FiCloud)*, Vienna, Austria, Aug., 2016.
- [14] M. Helfert, K.H. Krempels, C. Klein, et al., *Smart cities, green technologies, and intelligent transport systems*, in: *Proceedings of the FORTH International Conference, SmartGreens 2015*, Lisbon, May, 2015.
- [15] Y.R. Rao, *Automatic smart parking system using Internet of Things*, *Int. J. Eng. Technol. Sci. Res. (IJETSR)* 4 (5) (2017).
- [16] *Internet of Things: from sensing to doing*, Tech Trends 2016 Innovating in the Digital Era, Deloitte University Press, 2016 An imprint of Deloitte Development LLC.
- [17] D. Minoli, K. Sohraby, B. Occhiogrosso, *IoT considerations, requirements, and architectures for smart buildings – energy optimization and next generation building management systems*, *IEEE Internet Things J.* (2017) 1–15, doi:10.1109/JIOT.2017.2647881.
- [18] Y. Huang, S. Ali, X. Bi, et al., *Research on smart campus based on the Internet of Things and virtual reality*, *Int. J. Smart Home* 10 (12) (2016) 213–220.
- [19] B. Rashid, M.H. Rehmani, *Applications of wireless sensor networks for urban areas: a survey*, *J. Netw. Comput. Appl.* 60 (2016) 192–219 doi.org/10.1016/j.jnca.2015.09.008.
- [20] F. Shroufa, G. Miragliotta, *Energy management based on Internet Of Things: practices and framework for adoption in production management*, *J. Cleaner Product.* 100 (2015) 235–246. Pages <http://dx.doi.org/10.1016/j.jclepro.2015.03.055>.
- [21] S.K. Tan, M. Sooriyabandara, et al., *M2M communications in the smart grid: applications, standards, enabling technologies, and research challenges*, *Int. J. Dig. Multimed. Broadcast.* 2011 (2011) Article ID 289015.
- [22] X. Cheng, L. Yang, X. Shen, *D2D for intelligent transportation systems: a feasibility study*, *IEEE Trans. Intell. Transp. Syst.* 16 (4) (Aug. 2015), doi:10.1109/TITS.2014.2377074.
- [23] A. Ghazal, C.-X. Wang, B. Ai, D. Yuan, H. Haas, *A nonstationary wideband MIMO channel model for high-mobility intelligent transportation systems*, *IEEE Trans. Intell. Transp. Syst.* 16 (2) (2015), doi:10.1109/TITS.2014.2345956.
- [24] L. Cai, W. Xia, P. Li, L. Zhang, J. Liu, *An intelligent transportation system for hazardous materials based on the Internet of Things (IoT)*, in: *Proceedings of the FORTH International Conference on Information Technology and Management Innovation (ICITMI 2015)*, October 2015.
- [25] S.A. Alvi, B. Afzal, et al., *Internet of multimedia things: vision and challenges*, *Ad Hoc Netw.* 33 (2015) 87–111. <http://dx.doi.org/10.1016/j.adhoc.2015.04.006>.
- [26] G. Muhammad, S.K.M. Rahman, A. Alelaiwi, A. Alamri, *Smart health solution integrating IoT and cloud: a case study of voice pathology monitoring*, *IEEE Commun. Mag.* 55 (1) (2017) 69–73, doi:10.1109/MCOM.2017.1600425CM.
- [27] C. Xu, S. Li, Y. Zhang, E. Miluzzo, *Crowdsensing the speaker count in the wild: implications and applications*, *IEEE Commun. Mag.* 52 (10) (2014) 92–99.
- [28] E. Ronen, A. Shamir, A.O. Weingarten, C. O'Flynn, *IoT goes nuclear: creating a zigbee chain reaction*, in: *Proceedings of the 2017 IEEE Symposium on Security and Privacy (SP)*, San Jose, CA, USA, May 2017, doi:10.1109/SP2017.14.
- [29] S. Haller, “The real-time enterprise: IoT-enabled business processes”, Carsten Magerkurth SAP Research Center St. Gallen/Zürich, SAP Inc. (Switzerland), Proceedings of the IETF IAB Workshop on Interconnecting Smart Objects with the Internet, 2011.
- [30] S. Meyer, A. Ruppen, C. Magerkurth, *Internet of things-aware process modeling: integrating IoT devices as business process resources*, in: *Proceedings of the Conference on Advanced Information Systems Engineering*, 2013.
- [31] Y.S. Lee, J. Jeong, Y. Son, *Design and implementation of the secure compiler and virtual machine for developing secure IoT services*, *Future Gen. Comput. Syst.* 76 (2017) 350–357. Pages <https://doi.org/10.1016/j.future.2016.03.014>.
- [32] J. Zhou, Z. Cao, X. Dong, A.V. Vasilakos, *Security and privacy for cloud-based IoT: challenges*, *IEEE Commun. Mag.* 55 (1) (2017) 26–33, doi:10.1109/MCOM.2017.1600363CM.
- [33] S. Chakrabarty, D.W. Engels, *A secure IoT architecture for smart cities*, in: *Proceedings of the 2016 Thirteenth IEEE Annual Consumer Communications & Networking Conference (CCNC)*, Jan. 2016, doi:10.1109/CCNC.2016.7444889.
- [34] S. Arsi, V.N. Inukollu, S.R. Ravuri, *Security issues associated with big data in cloud computing*, *IJNSA* 6 (3) (2014).
- [35] R.T. Tiburski, L.A. Amaral, E. de Matos, F. Hessel, *The importance of a standard security architecture for SOA – based IoT middleware*, *IEEE Commun. Mag.* (December 2015).

- [36] M. Gault, "Rethinking security for the Internet of Things", Guardtime, Pinnacle Tower Rapenburgerstraat 177/S, 1011 VM Amsterdam, The Netherlands.
- [37] C. Lai, R. Lu, D. Zheng, H. Li, X. Shen, Toward secure large-scale machine-to-machine communications in 3GPP networks, *IEEE Commun. Mag. Suppl.* (2015) 12ff.
- [38] D. Minoli, J. Kouns, K. Sohraby, IoT Security (IoTSec) considerations, requirements, and architectures, in: *Proceedings of the Fourteenth Annual IEEE Consumer Communications & Networking Conference CCNC 2017*, Las Vegas, Jan 2017.
- [39] H. Sedjelmaci, S.M. Senouci, M. Feham, Intrusion detection framework of cluster-based wireless sensor network, in: *Proceedings of the 2012 IEEE Symposium on Computers and Communications (ISCC)*, Cappadocia, Turkey, July 2012, doi:[10.1109/ISCC.2012.6249409](https://doi.org/10.1109/ISCC.2012.6249409).
- [40] A. Dorri, S.S. Kanhere, R. Jurdak, P. Gauravaram, Blockchain for IoT security and privacy: the case study of a smart home, in: *Proceedings of the 2017 IEEE International Conference on Pervasive Computing and Communications Workshops (PerCom Workshops)*, Kona, HI, USA, March 2017, doi:[10.1109/PERCOMW.2017.7917634](https://doi.org/10.1109/PERCOMW.2017.7917634).
- [41] A. Ouaddah, A.A. Elkalam, A.A. Ouahman, FairAccess: a new blockchain-based access control framework for the Internet of Things, *Secur. Commun. Netw.* (December 2016), doi:[10.1002/sec.1748](https://doi.org/10.1002/sec.1748).
- [42] Introduction to ISO JTC1/WG10, ISO materials. <http://iot-week.eu/wp-content/uploads/2015/06/07-JTC-1-WG-10-Introduction.pdf>, June 2015.
- [43] M. Pilkington, *Blockchain technology: principles and applications*, in: F.X. Olleros, M. Zhegu (Eds.), *Research Handbook on Digital Transformations*, Edward Elger Publishing, Northampton, MA, 2016.
- [44] D. Tapscott, A. Tapscott, *Blockchain Revolution: How the Technology Behind Bitcoin Is Changing Money*, Penguin Random House LLC, New York, NY, 2016.
- [45] A. Kosba, A. Miller, E. Shi, Z. Wen, C. Papamanthou, Hawk: the blockchain model of cryptography and privacy-preserving smart contracts, in: *Proceedings of the 2016 IEEE Symposium on Security and Privacy (SP)*, San Jose, CA, USA, May 2016, doi:[10.1109/SP.2016.55](https://doi.org/10.1109/SP.2016.55).
- [46] A. Wright, P. De Filippi, Decentralized blockchain technology and the rise of Lex cryptography. <https://ssrn.com/abstract=2580664>, March 2015.
- [47] X. Xu, C. Pautasso, L. Zhu, V. Gramoli, A. Ponomarev, A.B. Tran, S. Chen, The blockchain as a software connector, in: *Proceedings of the 2016 Thirteenth Working IEEE/IFIP Conference on Software Architecture (WICSA)*, Venice, Italy, April 2016, doi:[10.1109/WICSA.2016.21](https://doi.org/10.1109/WICSA.2016.21).
- [48] R.C. Merkle, "A digital signature based on a conventional encryption function". *Proceedings of the Advances in Cryptology, CRYPTO '87*. Lecture Notes in Computer Science, vol. 293, p. 369. doi:[10.1007/3-540-48184-2\\_32](https://doi.org/10.1007/3-540-48184-2_32).
- [49] I. Bashir, *Mastering Blockchain*, Packt Publishing, Birmingham, UK, 2017 ISBN 978-1-78712-544-5.
- [50] N. Atzei, M. Bartoletti, S. Lande, R. Zunino, "A formal model of bitcoin transactions" eprint.iacr.org. Available online at <https://eprint.iacr.org/2017/1124.pdf>
- [51] K. Brünnler, D. Flumini, T. Studer T., *A Logic of Blockchain Updates*, in: S. Artemov, A. Nerode (Eds.), *Logical Foundations of Computer Science*, Lecture Notes in Computer Science, 10703, Springer, Cham, 2018.
- [52] S. N.Artemov, Explicit provability and constructive semantics, *Bull. Symb. Logic* 7 (1) (2001) 1–36.
- [53] C. Decker, R. Wattenhofer, Information propagation in the Bitcoin network, in: *Proceedings of the Thirteenth IEEE International Conference on Peer-to-Peer Computing*, 2013, pp. 1–10.
- [54] S.I. Matsuo, How formal analysis and verification add security to blockchain-based systems, in: *Proceedings of the Formal Methods in Computer Aided Design (FMCAD)*, 2017, Vienna, Austria, Oct. 2017.
- [55] J. Garay, A. Kiayias, N. Leonardos, The bitcoin backbone protocol: analysis and applications, in: *Proceedings of Eurocrypt*, 2015.
- [56] R. Dennis, G. Owenson, B. Aziz, A temporal blockchain: a formal analysis, in: *Proceedings of the 2016 International Conference on Collaboration Technologies and Systems (CTS)*, Orlando, FL, USA, Nov. 2016.
- [57] B. Huang, Z. Liu, J. Chen, et al., Behavior pattern clustering in blockchain networks, *Multimed. Tools Appl.* 76 (2017) 20099. <https://doi.org/10.1007/s11042-017-4396-4>.
- [58] M.K. Awan, A. Cortesi, Blockchain transaction analysis using dominant sets, in: K. Saeed, W. Homenda, R. Chaki (Eds.), *Proceedings of the Computer Information Systems and Industrial Management CISIM*, Lecture Notes in Computer Science, 10244, Springer, Cham, 2017.
- [59] A. Ouaddah, A.A. Elkalam, A.A. Ouahman, Towards a novel privacy-preserving access control model based on blockchain technology in IoT, *Europe and MENA Cooperation Advances in Information and Communication Technologies*, Springer International Publishing, 2017, pp. 523–533.
- [60] X. Yue, H. Wang, D. Jin, M. Li, W. Jiang, Healthcare data gateways: found healthcare intelligence on blockchain with novel privacy risk control, *J. Med. Syst.* 40 (2016) 218. <https://doi.org/10.1007/s10916-016-0574-6>.
- [61] G. Magyar, Blockchain: solving the privacy and research availability tradeoff for EHR data: a new disruptive technology in health data management, in: *Proceedings of the 2017 IEEE ThirtiethNeumann Colloquium (NC)*, Budapest, HungaryNC, Nov. 2017, doi:[10.1109/2017.8263269](https://doi.org/10.1109/2017.8263269).
- [62] M. Samaniego, R. Deters, Blockchain as a service for IoT, in: *Proceedings of the 2016 IEEE International Conference on Internet of Things (iThings) and IEEE Green Computing and Communications (GreenCom) and IEEE Cyber, Physical and Social Computing (CPSCom) and IEEE Smart Data (SmartData)*, Chengdu, China, Dec. 2016.
- [63] Y. Zhang, J. Wen, The IoT electric business model: using blockchain technology for the Internet of Things, *Peer-to-Peer Netw. Appl.* 10 (4) (2017) 983–994.
- [64] S. Huckle, R. Bhattacharya, M. White, N. Beloff, Internet of Things, blockchain and shared economy applications, *Procedia Comput. Sci.* 98 (2016) 461–466 ISSN 1877-0509.
- [65] H.M. Kim, M. Laskowski, Toward an Ontology-driven Blockchain Design for Supply-chain Provenance, Wiley Online Library, March 2018 <https://doi.org/10.1002/isaf.1424>.
- [66] J. Sun, J. Yan, K.Z.K. Zhang, Blockchain-based sharing services: what blockchain technology can contribute to smart cities, in: *Proceedings of the Financial Innovation*, Springer, December 2016.
- [67] S. Huh, S. Cho, S. Kim, Managing IoT devices using blockchain platform, in: *Proceedings of the 2017 Nineteenth International Conference on Advanced Communication Technology (ICACT)*, Bongpyeong, South Korea, Feb. 2017.
- [68] M. Samaniego, R. Deters, Using blockchain to push software-defined IoT components onto edge hosts, in: *Proceedings of the International Conference on Big Data and Advanced Wireless Technologies BDAW '16*, Blagoevgrad, Bulgaria, November 2016 Article No. 58.



**Daniel Minoli**, Principal Consultant, DVI Communications, has published 60 well-received technical books, 300 papers and made 90 conference presentations. He has many years of technical-hands-on and managerial experience in planning, designing, deploying, and operating secure IP/IPv6-, VoIP, telecom-, wireless-, satellite- and video networks for global Best-In-Class carriers and financial companies. Over the years, he has published and lectured extensively in the area of M2M/IoT, network security, satellite systems, wireless networks, IP/IPv6/Metro Ethernet, video/ IPTV/multimedia, VoIP, IT/Enterprise Architecture, and network/Internet architecture and services. Mr. Minoli has taught IT and Telecommunications courses at NYU, Stevens Institute of Technology, and Rutgers University. He is frequently engaged as testifying Expert Witness in the field of wireless, VoIP, video, and carrier services, supporting patent invalidity, IPR activities, and other legal cases.



**Benedict Occhiogrosso** is a Co-Founder of DVI Communications. He is a graduate of New York University Polytechnic School of Engineering. Mr. Occhiogrosso's experience encompasses a diverse suite of technical and managerial disciplines including sales, marketing, business development, team formation, systems development, program management, procurement and contract administration budgeting, scheduling, QA, technology operational and strategic planning. As both an executive and technologist, he enjoys working and managing multiple client engagements as well as setting corporate objectives. He is responsible for new business development, company strategy, as well program management. He also on occasion served as a testifying expert witness in various cases encompassing patent infringement, and other legal matters.