Received: 26 April 2021 | Revised: 22 April 2022 | Accepted: 14 June 2022

DOI: 10.1002/spy2.251

Key challenges in security of IoT devices and securing them with the blockchain technology

Blake Bryant[1] | **Hossein Saiedian**[1,2]

[1] Electrical Engineering & Computer Science, The University of Kansas, Lawrence, Kansas, USA

[2] Institute for Information Sciences, and Electrical Engineering & Computer Science, The University of Kansas, Lawrence, Kansas, USA

Correspondence
Hossein Saiedian, Electrical Engineering & Computer Science, The University of Kansas, Lawrence, KS, USA.
Email: saiedian@ku.edu

Abstract

Internet of Things (IoT) data processing enables rapid access to large volumes of data with the possibility of improving service-oriented business models. As such, the rapid adoption of IoT devices has resulted in a large number of low-powered devices integrating into traditional communication networks and influencing practically all assets of everyday life. However, the integration of IoT devices into traditional networks comes at a price, often in the form of added security challenges or administrative complexity. Some of these challenges may be addressed by leveraging technology developed from an unlikely source, crypto currencies. Crypto currencies introduced the notion of a blockchain, which is comprised of several underlying technologies that may be combined with IoT protocols to enable secure mechanisms for reaping the benefits of IoT devices. This paper introduces key challenges in securing IoT devices as well as important components of blockchain technology that may contain the keys to addressing these challenges. Emerging IoT security solutions are identified and evaluated based on their assessed effectiveness.

KEYWORDS

bitcoin, blockchain, byzantine fault tolerance, internet of things, IOTA, proof of work, security, smart contracts

1 | INTRODUCTION

The introduction, and rapid adoption, of autonomous computing devices, known colloquially as the Internet of Things (IoT), has resulted in an explosion of new devices integrating themselves into communication networks. The IoT brings new capabilities as well as new security challenges. Though IoT devices are capable of connecting to and through traditional IP based networks, the underlying mechanisms of IoT communications are far more complex and consequently more difficult to secure.[1] Furthermore, IoT devices are often introduced into networks with a "functionality first," "security second" mentality, which results in implementation errors ranging from universal vendor certificates to default username and password combinations installed on IoT devices.[2]

It is no surprise that the rapid introduction of insecure IoT devices was followed by record breaking denial of service attacks (DoS) in 2016.[3] The attack surface introduced by the emergence of the IoT may be expressed with a recent estimate that 8.4 billion IoT devices were connected to the Internet in 2017, according to a report from the research and advisory firm Gartner, Inc.[4] In depth analysis of all security challenges introduced by the IoT is beyond the scope of this paper; however, the unique security challenges introduced by IoT network communications may be partially addressed by the introduction of another emerging technology, the blockchain.

Blockchain technology was originally devised as a mechanism to conduct commercial transactions with digital currencies via a process independent of third-party intervention.[5] However, if one removes the commercial aspect of blockchain, the underlying technologies effectively implement a distributed database capable of establishing trust through consensus rules and transferring values between nodes.[5] As such, the technological components that birthed the blockchain may be used to implement a distributed trust technology to ensure scalability, privacy and reliability of IoT devices.

1.1 | Motivation for the work

The number of connected IoT devices in circulation are now counted in the billions. Recent estimates place the value of the Internet of Things (IoT) market to be worth more than $250 billion in 2019, with estimated growth exceeding $1.4 trillion by 2027[1] Considering the incredible size, and potential economic impact, of IoT devices, it is necessary to consider the potential challenges and opportunities for enabling future success with IoT enabled markets.

Blockchain, another technology rapidly gaining popularity within computer science research circles, is often attributed with the ascension of cryptocurrency markets, now valued at over $1 trillion for Bitcoin alone.[2] Despite the obvious attraction to blockchain research driven by the prospect of tapping into the immense economic potential of cryptocurrencies, blockchain research has also unlocked insights into new methods for securing computer network traffic. These insights offer unique ways to ensure authenticity, integrity, and reliable storage of data in transit between network devices. This paper is motivated by the attributes of blockchain technology that could be reappropriated to address challenges with the growing global deployment of IoT devices.

This paper is organized as follows: Section 2 provides a brief introduction to security challenges in IoT devices that blockchain technologies may be capable of addressing. These challenges include the establishment of trust in ad-hoc networks and decentralized management of dynamic networks. Section 3 introduces key blockchain concepts that are relevant to providing IoT security solutions. These concepts include the distributed ledger, consensus mechanisms and smart contracts. Section 4 introduces novel IoT security solutions based on blockchain technology. Novel solutions in this section include successful implementations of, or novel improvements to, blockchain technologies suitable for IoT environments. Finally, Section 5 concludes the paper and alludes to future research in the area.

2 | SECURITY CHALLENGES IN IOT DEVICES

IoT devices are unique in that they were originally devised to integrate into and dissolve from existing networks with ease. However, this approach conflicts with traditional network management procedures focused on regulating communication between relatively static resources.[6] Additionally, the ubiquitous networking capability of IoT devices required the establishment of new networking protocols and addressing schemes to bridge the gap between self-forming and traditional networks.[1,6] These new protocols exist in varying levels of maturity and standardization, with the possibility of introducing security vulnerabilities into networks when devices attempt to negotiate connections with existing infrastructure.[7-9] Furthermore, network engineers are unlikely to configure IoT devices individually as the sheer volume of devices have rendered manual configuration infeasible. As such, IoT devices suffer from two primary security problems: establishing trust within a network on an ad-hoc basis and providing a means of managing a dynamic network of decentralized IoT devices. Device management concerns pose unique challenges with performance constrained devices,[10] as well as executing bidirectional communication securely[11] and implementing secure, scalable, data storage schemes for IoT data.[12,13]

2.1 | Establishing trust in ad-hoc networks

Originally, IoT communication establishment was based upon assumed mutual trust between components of the network, either between nodes themselves, or nodes and a central management system for example, a base-station.[14-16] IoT authentication protocols are often designed under the premise that IoT hardware is resource constrained and should rely primarily on symmetric encryption to decrease computational rigor of Perrig et al.[15] This semi-trusted model was required to establish an authoritative source from which to derive seed values for session key establishment between IoT devices and facilitate future symmetric encryption between nodes. These assumptions often result in vendors embedding shared secret keys within the firmware of IoT devices to facilitate the establishment of session keys between devices.[2,17-19]

Understanding IoT trust models requires a basic understanding of IoT network architecture. IoT networks complicate traditional networking schemes by introducing heterogeneous network stacks. This paper will use the Z-Wave authentication protocol as an example of IoT trust establishment. Figure 1 depicts five common IoT protocols, with Z-Wave being merely one of many alternatives for IoT communications. Each protocol is represented by a different stack in a manner similar to the OSI model. The OSI model is commonly used to demonstrate communications in traditional networking.[20]

In addition to separate stack structures, each protocol uses proprietary data structures to establish and maintain their prospective sections of the network. Figure 2 depicts the structure of a Z-Wave network packet. Finally, each IoT protocol implements proprietary authentication protocols to establish secure connections between nodes.

The Z-Wave authentication protocol is depicted in Figure 3 and summarized as follows[17,18]:

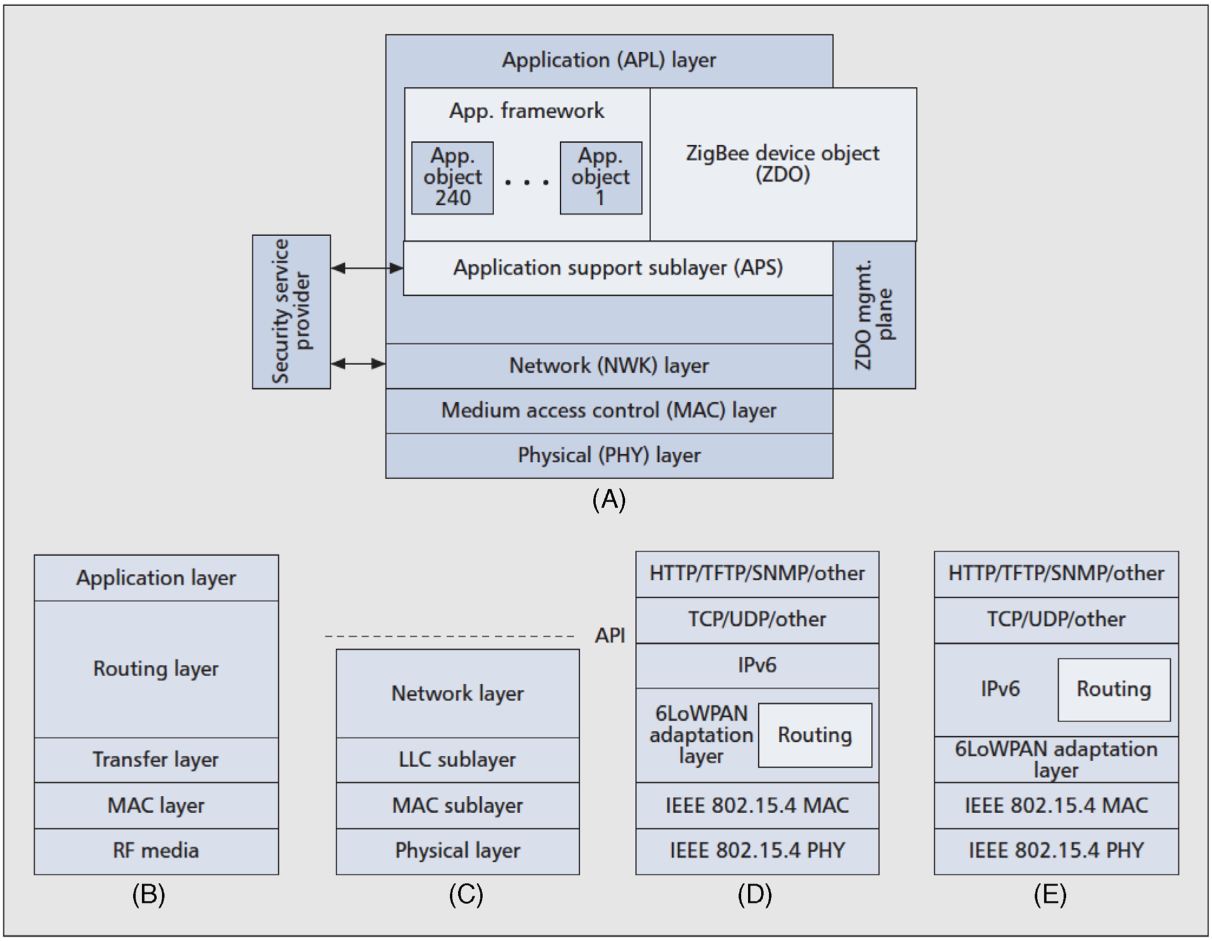

FIGURE 1 Common IoT Protocols: (A) ZigBee, (B) Z-Wave, (C) Wavenis (D), 6LowPAN [mesh under], and (E) 6LoWPAN [route over]

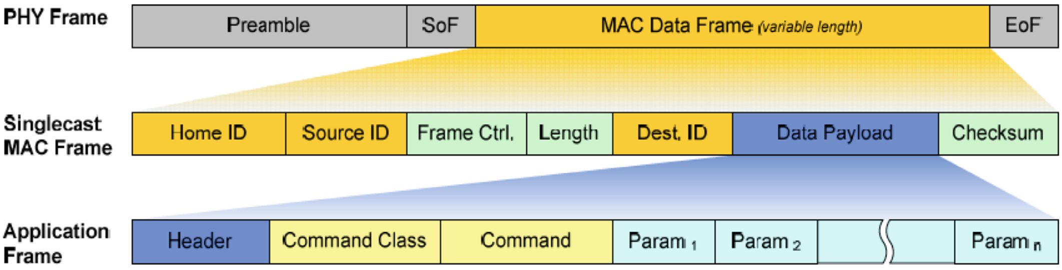

FIGURE 2 Z-wave network packet format[17,18]

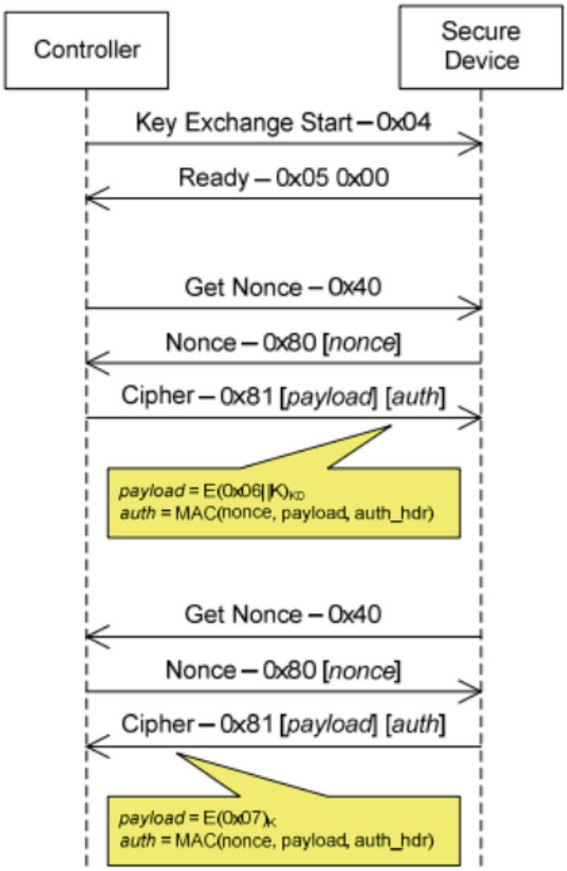
Controller
Secure Device
Key Exchange Start – 0x04
Ready – 0x05 0x00
Get Nonce – 0x40
Nonce – 0x80 [nonce]
Cipher – 0x81 [payload] [auth]
payload = E(0x06||K)KD
auth = MAC(nonce, payload, auth_hdr)
Get Nonce – 0x40
Nonce – 0x80 [nonce]
Cipher – 0x81 [payload] [auth]
payload = E(0x07)K
auth = MAC(nonce, payload, auth_hdr)

FIGURE 3 Z-wave key exchange protocol[17,18]

- An encryption key is generated using hardware-based pseudo random number generator (PRNG) on the Z-Wave chip.
- A temporary default key on the chip is used to encrypt the encryption key from the previous step resulting in a network key (K_n)
- The Controller and Secure Device both use AES[21] encryption in ECB mode to derive two new 128-bit keys from (K_n), a frame encryption key (K_c) and a data origin authentication key (K_m):

  - $K_c = AES - ECB_{K_n}\ (Passwd_c)$
  - $K_m = AES - ECB_{K_n}\ (Passwd_m)$

- AES Cipher Block-Chaining (AES-CBC) is used to generate a message authentication code (MAC) based on the origin authentication key (K_m). MAC components include: the initialization vector (IV), security header (SH), source node ID (SRC), destination node ID (DST), length of the payload (LEN) and the encrypted payload (C). C is generated using the frame encryption key (K_c) with the AES algorithm in OFB mode. Inputs for C include the initialization vector (IV) and plaintext variable containing the Z-Wave command header, class, ID and parameters:

  - $MAC = AES - CBCMAC_{K_m}\ (IV,\ \ SH, \| \ SRC \| \ DST \| \ LEN \| \ C2)$
  - $C = AES - OFB_{K_c}\ (IV, P)$

This Z-Wave authentication protocol was discovered to possess several critical vulnerabilities when implemented in home automation devices.[17,18] Specifically, weak vendor pre-shared keys were used to establish session keys during authentication and could easily be harvested during device installation. Additionally, the lack of state management on devices allowed for attackers to inject new "temporary keys" used for session key management via a key reset function. Both vulnerabilities stem from a challenge in verifying IoT entities prior to exchanging secure information.

Rather than assume IoT devices will be introduced into a trusted, or semi-trusted network, it is better to analyze IoT networks through the lens of the widely-accepted Dolev-Yao threat model.[22] As such, it is assumed it is feasible for an attacker to physically capture communication traffic between devices for eavesdropping and offline analysis. This assumption is validated by the Z-Wave scenario presented previously, as well as the fact that most IoT protocols communicate via wireless communication reliant on message broadcasts to establish communication between nodes.[15] With these assumptions, the use of pre-shared keys may not be enough to ensure accurate node identification and prevent man-in-the-middle attacks on IoT wireless networks. Therefore, a need exists for a different mechanism capable of providing node identification, and possibly reputation, information within a dynamic IoT environment.

Unfortunately, alternative trust models to PKI are not perfect. It is common for IoT networks to implement internal vouching mechanisms to replace or augment standard PKI approaches. As such, defamation, recommendation, and collusion attacks are possible.[13] Defamation attacks involve a malicious entity attempting to claim a trusted authority, such as a certificate authority, has been compromised and is therefore no longer trustworthy. Such an attack could allow an attacker to supplant trust of the defamed authority with a weaker trust mechanism, such as peer device vouching for the authority of another. Recommendation attacks capitalize on authority inherited by malicious devices in a community trust model to vouch for the reputation of others. This inherited authority may be used to either demote or promote the trust new devices should place in other peer devices. Finally, collusion attacks rely on two or more malicious devices to implement defamation and recommendation attacks in concert to promote themselves as authorities of trust, ultimately subverting the security model designed to control access to join the IoT network.

2.2 | Decentralized management of dynamic networks

IoT networks may rapidly expand or contract due to the malleable nature of IoT device connection establishment discussed in the previous section. As such, it is often difficult to establish a consistent form of centralized device management. The traditional model for IoT device management is to rely on either a network gateway, that bridges the network gap between IoT network and traditional IP-based network layers, or via a cloud management service.

However, this centralized management paradigm results in a centralized authentication and authorization system. Such a management fabric becomes a convenient vector for malicious actors to assume control over IoT devices or migrate from the IoT communication network into traditional IP-based networks via the central management system. Additionally, cloud based IoT management solutions may expose IoT data to privacy issues.[21] IoT devices are unique in that much of their utility is derived from their ability to establish connectivity autonomously, as such, autonomous distributed management of IoT devices seems to be a natural evolution of IoT management.

Furthermore, assuming decentralized management is achievable, IoT devices pose unique challenges that may not be present in traditional networks. These challenges include mobility, accessibility, concurrency, performance constraints, and scalability.[23] In this context, mobility refers to the ability to enforce different management policies across large spanning geographic or logical networks, which IoT devices may migrate between during their useful lifespan. Ideally IoT management systems would allow for variation in policies based on these physical or logical differences. Accessibility refers to unique challenges in communicating with IoT devices, which may vary their responsiveness to network requests based on periodic lapses in consciousness designed to decrease power consumption and preserve battery life. Concurrency refers to the possibility that IoT devices may incur instances of dual membership to disparate managing systems, for instance during migration between management domains. Not all of these challenges are unique to IoT devices; however, IoT devices are unique in that these aforementioned challenges must be addressed within the context of performance constrained hardware and apply to deployments that exceed thousands, or hundreds of thousands, of systems.

Data management also poses a unique challenge within the context of IoT devices. IoT devices are commonly deployed to collect sensor data intended for aggregation and processing by other systems. Their uniquely small form factor, low power consumption, and long battery life make them ideal for this purpose. However, they are ill suited for protecting the data they collect while in transit to more powerful aggregation and processing nodes. Secure transport typically relies on cryptography to ensure confidentiality, integrity, and authenticity of network data, all of which could be aided through the application of blockchain technology, as was depicted in the work of Zhang et al.[13]

3 | KEY BLOCKCHAIN CONCEPTS

The blockchain technology presents an innovative approach to store information, execute transactions and establish trust in an open environment. A comprehensive review of its uses for security and privacy purposes is given by Zhang et al.[24] Blockchain features to achieve availability, consistency, and data integrity is surveyed by Kolb et al.[25] The application of blockchain technology in diverse services, for example, supply chain tracking, digital forensics, insurance payments, and health-case record sharing are discussed in Laphou et al.[26] An overview of the state of the art in blockchain technology using a systematic and multi-vocal approach and also elaborating on its architecture is presented by Butjin et al.[27] The blockchain technology has many diverse applications, such as electronic voting, supply-chain communications, international payments, tracking music royalties, smart contracts, and such.

There are several underlying concepts that make blockchain possible, however the most pertinent concepts for this paper are the notion of a distributed ledger, consensus mechanisms, and smart contracts.

3.1 | The blockchain distributed ledger

The distributed ledger provides a mechanism for decentralized data management, transaction authentication and data integrity, all managed through public key cryptography. Rather than rely on a centralized data repository, a distributed ledger functions as a data structure shared by the blockchain community. All nodes may validate transactions and preserve data integrity. The ledger contains a chronologically ordered set of transactions contained with data structures called "blocks." Blocks are based upon Merkle trees, which provide a mechanism for containing the hashes of previous transactions within a single hash code while using very little computational or memory resources.[28] Additional information within a block describes the transactions contained within the ledger, specifically: the Merkle root, difficulty of a Proof of Work (PoW) function, previous block hash, timestamp and a nonce.[5] Figure 4 illustrates the structure of a block.

Blockchain mining, in a traditional sense, is based upon a concept called PoW to prevent unauthorized transactions from manipulating the blockchain. PoW is based upon computers generating solutions to math problems that are hard to generate but simple to verify. Therefore, an attacker must drastically limit the number of messages they can send as each transmission "costs" them something, analogous to paying postage for sending a letter, though normally with computing resources rather than traditional currency.

Mining is the process by which transactions are added to the blockchain. This process is secured through a mechanism known as PoW. PoW is computationally expensive and therefore not suited for IoT devices.

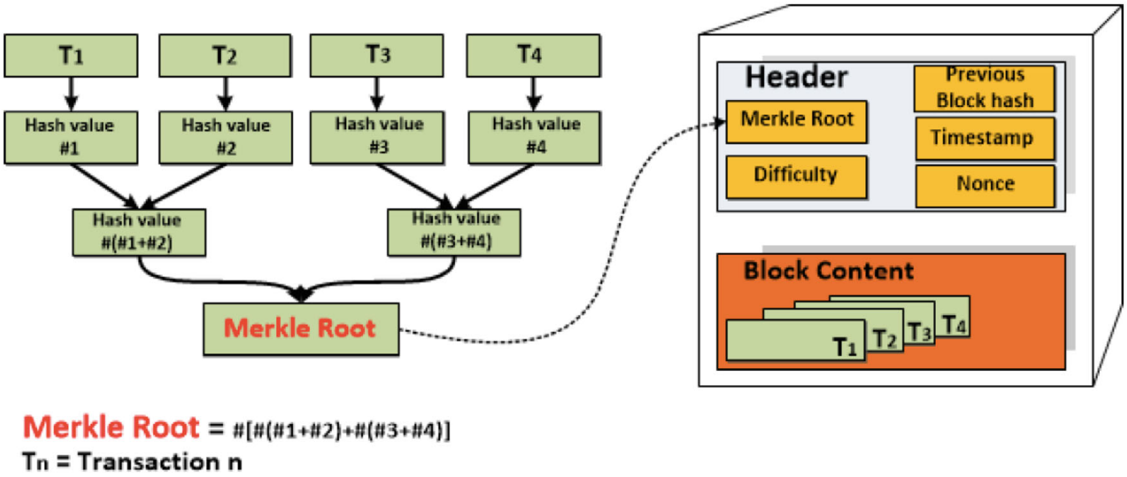

FIGURE 4 Distributed ledger block structure[5]

3.2 | Consensus mechanisms

Consensus mechanisms provide a means by which anonymous contributions may be deemed trustworthy by a collection of nodes. This is an essential element in validating traffic between nodes and ensuring the integrity of the blockchain.

Blockchain consensus mechanisms are often referenced in the context of the Byzantine Generals Problem (BGP). The BGP refers to a notional historical event involving multiple military commanders attempting to agree on conditions for launching an attack during a war. If all generals agree on an action, then they will all prosper; however, if they do not operate in unison, then they will be vulnerable to a counterattack. It is assumed that there could exist a small number of traitors (or misinformation) amongst the generals. One solution to resolving potential misinformation is through the use of a majority voting system, commonly referred to as a Byzantine Agreement.[5] The process by which majority voting is conducted within blockchain systems is referred to as a consensus algorithm.

There are several variations of consensus algorithms amongst blockchain technologies. The traditional consensus algorithm is based on a process referred to as PoW. PoW forces participants to solve a computationally difficult hashing problem which is easy to verify.[29] The difficulty in the problem prevents malicious actors from spoofing the voting process and all members of the network can verify the work has been conducted through asymmetric mathematical operations. This PoW concept is the "mining" portion referenced colloquially as "bit mining." Once PoW has been presented, the node that generated the PoW solution is rewarded with the ability to add to the blockchain.

PoW works well when generating commodities such as bitcoins. However, PoW is not an effective consensus mechanism for resource constrained IoT devices. PoW requires all participants to attempt to conduct work whether they solve the solution first or not, leading to an immense waste of computing resources should they fail to derive the correct solution before other devices. Other consensus algorithms have been developed that are less resource intensive and therefore suitable for IoT nodes. These algorithms replace processing power with some other resource that nodes may possess and include[5]:

- Proof of Stake
- Delegated Proof of Stake
- Proof of Authority
- Proof of Capacity
- Proof of Elapsed Time
- Algorand
- Ledger Consensus Protocol
- Stellar Consensus Protocol
- Delegated Byzantine Fault Tolerant

Amongst these algorithms, Proof of Elapsed Time (PoET), appears to be a promising consensus mechanism for IoT devices. PoET was proposed by Intel based upon its trusted computing platform SGX.[30] PoET implements a lottery algorithm for distributing wait times between nodes, which in turn is used to calculate node voting. Furthermore, wait time values are randomly generated and concatenated with the PoET solution to facilitate peer validation. Peer validation is made possible through exponential distribution of random time variables; thus making it difficult to spoof wait values, but easy to verify compliance with the distribution. PoET offers two major advantages over the other algorithms:

- Efficiency: participating nodes are not required to conduct computation before creating a new block.
- Fairness: each CPU only receives one vote.

However, one key limitation of the PoET algorithm is reliance on Intel proprietary equipment. This was noted as a key limiting factor during Bamakan et al.'s work[31] to benchmark the relative performance of consensus algorithms. Bamakan et al noted PoET was capable of achieving fair consensus amongst nodes with low resource and energy consumption, but was not suitable for their comparative evaluation of other consensus algorithms due to the proprietary nature of the systems this algorithm was designed for.

Table 1 reflects the results of the Bamakan et al. study which entailed a multivariable analysis of blockchain consensus algorithms. The Bamakan et al. study evaluated consensus algorithms based upon algorithm performance (measured as

TABLE 1 A comparison of consensus algorithms based on their representative cryptocurrencies[31]

Row	Consensus algorithms	Cryptocurrencies	Algorithm	Genesis Block	Rank	Market CAP ($)	TPS	Block Time Minutes	Mining reward
1	PoW	Bitcoin	SHA256	January 3, 2009	1	180,207,092,238	7	10	12.5 BTC
		Ethereum	Ethash (KECCAK256	July 30, 2015	2	22,757,000,420	15	0.25	2
		Litecoin	Scrypt	October 8, 2011	5	4,587,952,794	28	2.3	25
		Monero	Cryptonight	April 18, 2014	11	1,268,871,523	30	2	4.9
		Zcash	Equihash	October 28, 2016	28	348,443,197	27	2	10
2	PoS	Waves (LPoS)	LPoS	June 12, 2016	55	100,304,755	100	1	Non-minebable
		Qtum	POS 3.0	December 26, 2016	36	202,601,750	70	2	Non-minebable
		Nxt	SHA256	November 24, 2013	175	16,162,355	100	1	Non-minebable
		Blackcoin	Scrypt	February 24, 2014	500	4,569,548	0	1	Non-minebable
		Nano	Blake2b	February 29, 2016	45	123,741,646	7000	Instant	Non-minebable
3	DPoS	EOS	OPOS	July 1, 2017	7	3,641,735,649	4000	0.5	Non-minebable
		Cardano	Ouroboros (DPoS)	December 26, 2017	12	1,266,573,741	257	0.33	Non-minebable
		TRON	DPoS	August 28, 2017	13	1,186,299,015	2000	0.05	32 TRON
		Lisk	DPoS	January 30, 2016	47	118,714,644	3	0.284	Non-minebable
		BitShares	DPoS	July 19, 2014	58	91,575,735	100000	0.05	Non-minebable
4	PBFT	Ripple	N/A	April 11, 2013	3	12,010,477,031	1500	0.06	Non-minebable
		Stellar	N/A	April 6, 2016	10	1,410,189,643	1000	0.08	Non-minebable
		Zilliqa	Keccak	January 12, 2018	79	59,022,911	0	45s to 4 m	Non-minebable
5	PoC	Burst	Shabal256	August 11, 2014	190	14,417,212	80	4	460
6	DAG	IOTA	Curl-P	October 21, 2015	17	788,711,735	1000	Instant	Non-minebable
		Byteball (Obyte)	DAG	September 5, 2016	262	17,301,594	10	0.5	Non-minebable
		Travelflex	DAG	December 2, 2017	1374	163,648	3500	1	30,00 TRF
7	PoA (Hybrid PoW/PoS)	Dash	X11	January 19, 2014	16	850,165,302	56	2.5	2.09
		Decred	BLAKE256	December 15, 2015	32	233,089,579	14	5	18.22
		Komodo	Equihash	September 1, 2016	67	80,699,867	100	1	3.00 KMD
		Peercoin	SHA-256	August 19, 2012	373	7,844,163	0	10	37.36 PPC
		Espers	HMQ1725	April 28, 2016	1026	625,199	0	5	5000
8	dBFT	NEO	RIPEMD160	October 17, 2016	20	650,866,809	1000	0.25	Non-minebable
9	PoI	NEM (XEM)	Ed25519	March 31, 2015	26	403,570,701	10000	1	Non-minebable
10	PoB	Slimcoin	Dcrypt	May 07 2014	2661	16,195	0.00003	1.5	50.00 SLM

TABLE 2 A resorting of the consensus algorithms highlighting resource constraints

Rank	Consensus algorithm	Hardware limitation	Exemplary crypto-currency	Transactions per second	Block time minutes
1	PoW	CPU	Bitcoin	7	10
2	PoW	CPU	Ethereum	15	0.25
3	PBFT	none	Ripple	1500	0.06
5	PoW	CPU	Litecoin	28	2.3
7	DpoS	storage	EOS	4000	0.5
10	PBFT	none	Stellar	1000	0.08
11	PoW	CPU	Monero	30	2
12	DpoS	CPU	Cardano	257	0.33
13	DpoS	CPU	Tron	2000	0.05
16	PoA	CPU & storage	Dash	56	2.5
17	DAG	none	IOTA	1000	Instant

throughput), profitability of mining, degree of decentralization, and security or vulnerabilities. This study was not specifically focused on IoT applications and therefore did not place a high importance on resource consumption. Additionally, profitability of mining exemplary implementations of said algorithms received considerable weight during comparison. As such, the top-rated consensus algorithms were dominated by implementations of PoW or delegated proof of stake (DPoS); both requiring large investments in processor or storage hardware, respectively.

However, the Bamakan study did identify two resource friendly consensus algorithm approaches, placing in the upper third of favored consensus algorithms in their study: practical byzantine fault tolerance (PBFT) and directed acyclic graphs (DAG). Table 2 reflects a resorting of the Bamakan study results, as well as the addition of a column indicating resource constraints based on the chosen algorithm. Notably, PBFT and DAG are not constrained by processor or storage capabilities of participating nodes, and therefore would be the leading consensus algorithms to be used in IoT applications. The DAG approach is cited as a critical component in several of the security solutions outlined within Section 4 of this paper.

3.3 | Smart contracts

Blockchain technology may be used to establish smart contracts between IoT devices. Smart contracts provide a mechanism for establishing rules to govern interactions (eg, decentralized configuration management) as well as decentralized identity management through the blockchain audit trail.

The concept of smart contracts was originally introduced by Nick Szabo in the mid 1990's.[32] Smart contracts may be viewed as addressable scripts stored within the blockchain that adhere to the principles of public-key cryptography. This enables instructions to be sent to all nodes (form an authenticated source with non-repudiation) or encrypted in a manner executable by only individual nodes.[32] As such, smart contracts provide a secure mechanism for managing data-driven interactions in a decentralized network. Furthermore, transactions also become recorded within the blockchain and are therefore auditable, adding an additional layer of security.

In Table 3, we compare six blockchain solutions on five key challenges or key attributes, more specifically, performance, trust between devices, security in transit, data integrity, and device management.

4 | NOVEL IOT SECURITY SOLUTIONS BASED ON BLOCKCHAIN TECHNOLOGY

Many researchers are adopting the blockchain as a mechanism to address security shortfalls within IoT implementations. Some have proposed implementing blockchain technology to improve decentralized asset and identity management in IoT networks; though this research did not result in a practical system prototype or validation data. Perrig et al.[15] devised

TABLE 3 A comparison of six blockchain solutions with respect to five key attributes

	Performance	Trust between devices	Security in transit	Data integrity	Device Management
PoW refinement	×	×			
PKI		×	×	×	
Dedicated Mgmt network	×		×	×	×
Preinstalled vendor keys	×				×
Distributed ledger		×		×	

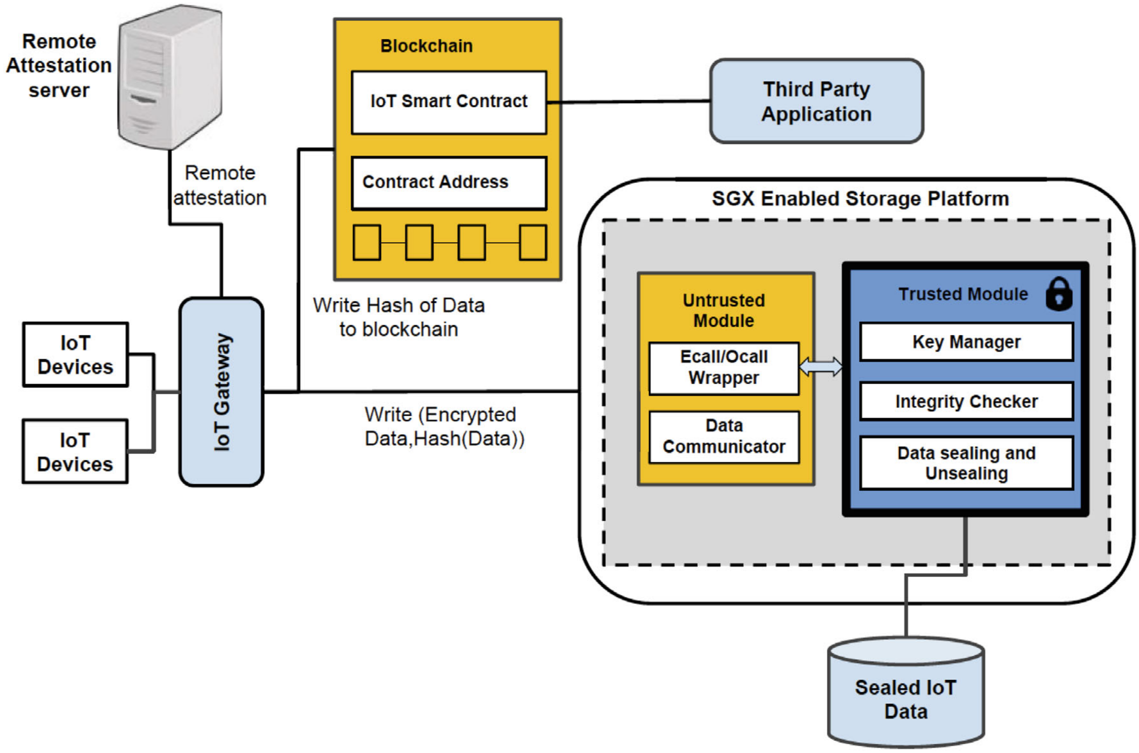

FIGURE 5 Ayode IoT smart contract architecture[21]

a secure routing subsystem for IoT devices, called SPINS, based on blockchain technology; however, this work is also limited to the development of theoretical protocols and lacks validation data.[15] Dorri et al.[33] proposed a solution to IoT network management leveraging a novel consensus algorithm based on a peer-to-peer reputation system.[33] The Dori system focused on network resource consumption and generated validation data via the NS3 simulator in order to remove resource consumption associated with traditional POW mining. The common limiting factor for IoT performance within these works lies in the adoption of an alternative to the POW mechanism within the blockchain.

A promising solution to configuration management in IoT was presented by Ayoade et al. Ayoade devised a prototype system, leveraging the Intel SGX platform and the Ethereum blockchain, to issue contracts for IoT devices. These operations secured through smart contracts included user registration, device registration, and data read/write access policy definition to blockchain storage. Figure 5 depicts the Ayoade smart contract architecture and Figure 6 outlines the data flow of using smart contracts to manage IoT devices.

The works mentioned in the preceding paragraphs outlined the potential security gains of applying blockchain technology to IoT implementation; however, other works have focused on optimizing blockchain technology to decrease resource costs associated with its implementation. Sompolinsky et al. proposed improvements to the processing time required by BITCOIN with the introduction of the Greedy Heaviest-Observed Sub-Tree (GHOST) algorithm.[34] The

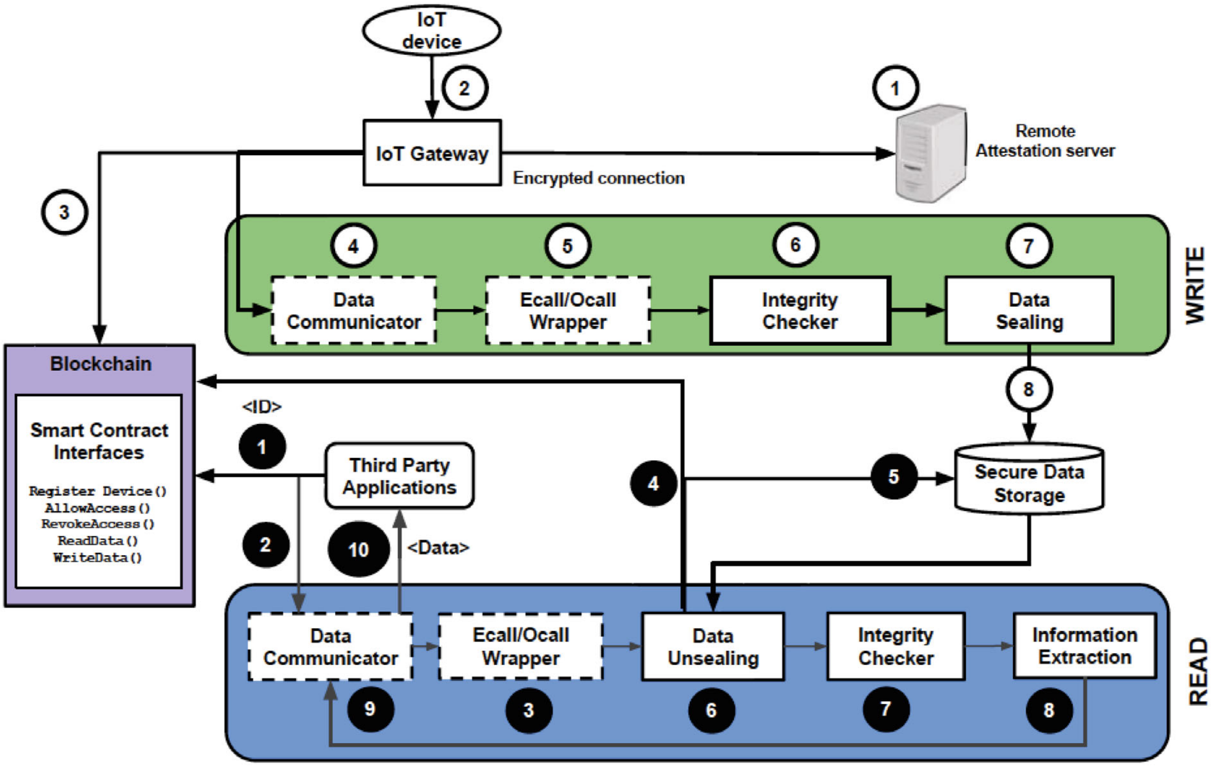

FIGURE 6 Ayode IoT smart contract data flow[21]

GHOST algorithm provides a mechanism for accounting for divergent paths along the blockchain rather than merely implementing the longest chain rule. This work introduced performance improvements in transaction times thus decreasing processing and storage requirements. Additionally, this work introduced a degree of protection against double-spending or injection attacks against the blockchain. A similar mechanism to the GHOST protocol has been implemented in the Ethereum cryptocurrency.[34]

Popov expanded upon the works of Sompolinsky et al., who were shifting away from the traditional linked list style structure of the blockchain. Popov's work resulted in the development of a new protocol referred to as the "tangle".[35] The tangle implements a directed acyclic graph (DAG) data structure and is leveraged in the cryptocurrency IOTA. IOTA was specifically designed as an optimized protocol for use within the IoT industry and takes advantage of decreased storage requirements as well as improved transaction processing efficiency. The DAG structure also introduces a novel validation mechanism wherein nodes may leverage knowledge of the DAG structure to verify transactions rather than reproduce the entire blockchain or rely on PoW based consensus mechanics. Finally, the Tangle algorithm allows for conducting cryptocurrency transactions asynchronously, resulting in higher transaction throughput.

Masood et al. evaluated many of the consensus algorithms within this paper, to include IOTA and lauded IOTA for its high transaction rate, low energy consumption, and ability to operate in an untrusted environment.[36] However, Masood et al. criticized the IOTA algorithm as "homemade crypto" and indicated a high degree of centralization is required for its implementation. It is possible that the IOTA DAG implementation may be improved to address these shortcomings.

Novo proposed a solution to scalable decentralized management of IoT devices using a separate blockchain network, effectively decoupling the performance requirements of blockchain computing from IoT devices and placing them within a dedicated management network. This management network in turn may be used to add or remove management nodes as necessary to maintain scale with an ever-changing population of managed IoT devices.[23]

Zhang et al. also proposed a solution to secure IoT network communications through the addition of a separate blockchain-based network dedicated to instituting confidentiality, authenticity, and integrity of sensor data.[13] This approach capitalized on the ability of blockchain-based network protocols to maintain stored data, such as trusted sensor lists, within the blockchain. This allowed for sensors to identify and authenticate to trusted nodes without the need for dedicated local data storage, therefore circumventing storage limitations on constrained IoT devices while still implementing a decent trust model.

5 | CONCLUSIONS

This paper presented several of the security challenges introduced by adoption of Internet of Things (IoT) devices into traditional networks as well as key mechanisms within emerging blockchain technology that may be suitable for IoT security solution development. The block chain components of a distributed ledger, consensus mechanisms, and smart contracts were explained in order to establish context for understanding proposed novel IoT security solutions. Finally, contemporary works in IoT security leveraging blockchain technology were reviewed to determine the feasibility of continuing research in this area. The number of works being developed in this area indicates strong interest and potential for developing blockchain solutions for select IoT security challenges. Additionally, the model established by the work of Ayoade et al. could be expanded to develop additional operations for the secure management of IoT devices, networks, and data within them. There also appears to be promise in potentially devising more efficient algorithms to replace the blockchain notion of PoW, as was introduced in the work of Dorri et al.

Novo and Zhang et al. proposed novel approaches to dealing with the performance burden of PoW by decoupling blockchain computation from IoT devices and establishing separate blockchain-based management networks.

Finally, there appears to be a shift within crypto currency community toward modifying the blockchain data structure to improve performance. Sompolinsky and Popov both devised novel approaches to improving blockchain performance by deviating from the linear structure of the blockchain and implementing tree or graph data structures. The Popov implementation of directed acyclic graphs shows great promise within IoT environments but could be improved to reduce the degree of centralization required for its implementation.

ENDNOTES

[1] Hardware & Software IT Services/Internet of Things (IoT) Market, Fortune Business Insights. Report ID FBI100307, July 2020, https://bit.ly/3rcQB8R.

[2] Pound, Jesse. Bitcoin hits $1 trillion in market value as cryptocurrency surge continues, CNBC Business News, https://cnb.cx/3f91Nko.

DATA AVAILABILITY STATEMENT

Data sharing not applicable - no new data generated, or the article describes entirely theoretical research

ORCID

Hossein Saiedian https://orcid.org/0000-0001-5060-6332

REFERENCES

1. Russell B, Van Duren D. The IoT in the enterprise. *Practical Internet of Things Security*. Brimingham: Packt Publishing Ltd; 2016:21-29.
2. Kolias C, Kambourakis G, Stavrou A, Voas J. DDoS in the IoT: Mirai and other botnets. *Computer*. 2017;50(7):80-84.
3. Krebs B. Krebs on Security - Krebs on security hit with record DDoS, 2016a. https://krebsonsecurity.com/2016/09/krebsonsecurity-hit-with-record-ddos Accessed December 2, 2018
4. Gartner. Gartner says 8.4 billion connected “things” will be in use in 2017, up 31 percent from 2016, 2017. https://gtnr.it/3998YFC. Accessed December 2, 2018.
5. Panarello A, Tapas N, Merlino G, Longo F, Puliafito A. Blockchain and IoT integration: a systematic survey. *Sensors*. 2018;18(8):2575.
6. Ranasinghe D, Mcfarlane D, Harrison M. Adding sense to the internet of things - an architecture framework for smart object systems. *Pers Ubiquitous Comput*. 2012;16:29-308.
7. Mainetti L, Patrono L, Vilei A. Evolution of wireless sensor networks towards the internet of things: a survey. SoftCOM 2011, 19th international conference on software, telecommunications and computer networks, Split, Croatia, 2011;1-6.
8. Oorschot P, Smith S. The internet of things: security challenges. *IEEE Secur Priv*. 2019;17(5):7-9.
9. Tschofenig H, Baccelli E. Cyberphysical security for the masses: a survey of the internet protocol suite for internet of things security. *IEEE Secur Priv*. 2019;17(5):47-57.
10. Lockl J, Schlatt V, Schweizer A, Urbach N, Harth N. Toward trust in internet of things ecosystems: design principles for blockchain-based IoT applications. *IEEE Trans Eng Manage*. 2020;67(4):1256-1270.
11. Liu H, Han D, Li D. Fabric-IoT: a blockchain based access control system in IoT. *IEEE Access*. 2020;8:18207-18218.
12. Fawaz K, Shin K. Security and privacy in the internet of things. *IEEE Comput*. 2019;52(4):40-49.
13. Zhang L, Li F, Wang P. A Blockchain-assisted massive IoT data collection intelligent framework. *IEEE Internet Things*. Accepted for Publication. 2021;15. doi:10.1109/JIOT.2021.3049674
14. Bhattarai S, Wang Y. End-to-end trust and security for internet of things applications. *IEEE Comput*. 2018;51(4):20-27.
15. Perrig A, Szewczyk R, Wen V, Culler D, Tygar JD. SPINS: security protocols for sensor networks. *Wireless Netw*. 2002;8(5):521-534.
16. Ren K, Lou W, Yu S, Zhang Y. Multi-user broadcast authentication in wireless sensor networks. *IEEE Trans Veh Technol*. 2009;58(8):4554-4564.

17. Fouladi B, Ghanoun S. *Honey, I'm Home!!: Hacking ZWave Home Automation Systems*. Las Vegas, NV: Black Hat USA; 2013a.
18. Fouladi B, Ghanoun S. Security evaluation of the Z-wave wireless protocol. Blackhat USA 2013. Las Vegas, 2013b
19. Krebs B. Krebs on Security- Source code for IoT botnet 'Mirai' released, 2016b. https://krebsonsecurity.com/2016/10/source-code-for-iot-botnet-mirai-released Accessed December 2, 2018
20. Gomez C, Paradells J. Wireless home automation networks: a survey of architectures and technologies. *IEEE Commun*. 2010;48(6):92-101.
21. Ayoade G, Karande V, Khan L, Hamlen K. Decentralized IoT data management using blockchain and trusted execution environment. 2018 IEEE International Conference on Information Reuse and Integration for Data Science, Salt Lake City, UT, USA, 2018;15-22. doi:10.1109/IRI.2018.00011
22. Dolev D, Yao AC. On the security of public key protocols. *IEEE Trans Inform Theory*. 1983;29(2):198-208.
23. Novo O. Blockchain meets IoT: an architecture for scalable access management in IoT. *IEEE Internet of Things*. 2018;5(2):1184-1195.
24. Zhang R, Zue R, Liu L. Security and privacy on Blockchain. *ACM Comput Surv*. 2019;52(3):34. doi:10.1145/3316481
25. Kolb J, AbdelBaky M, Katz R. Core concepts, challenges, and future directions in blockchain: a centralized tutorial. *ACM Comput Surv*. 2020;53(1):39. doi:10.1145/3366370
26. Laphou L, Zecheng L, Hou S, Ziao B, Guo S, Yang Y. A survey of IoT applications in blockchain systems: architecture, consensus, and traffic modeling. *ACM Comput Surv*. 2020;53(1):39. doi:10.1145/3372136
27. Butjin B, Tamburri D, Heuvel W. Blockchains: a systematic multivocal literature review. *ACM Comput Surv*. 2020;53(3):32-37. doi:10.1145/3369052
28. Merkle RC. A Digital Signature Based on a Conventional Encryption Function. CRYPTO '87 A Conference on the Theory and Applications of Cryptographic Techniques on Advances in Cryptology, London, UK. 1987;369-378.
29. Dwork C, Goldberg A, Naor M. On Memory-Bound Functions for Fighting Spam, Proceedings of the 23rd Annual International Cryptology Conference, LNCS volume 2729, pp. 426–444, Santa Barbara, California, USA, August 2003.
30. Chen L, Xu L, Shah N, Gao Z, Lu Y, Shi W. On Security Analysis of Proof-of-Elapsed-Time (Poet). 19th International Symposium on Stabilization, Safety, and Security of Distributed Systems, Boston, MA, USA, 2017;282-297.
31. Bamakan S, Motavali A, Bondarti A. A survey of blockchain consensus algorithms performance evaluation criteria. *Expert Syst Appl*. 2020;154:113385. doi:10.1016/j.eswa.2020.113385
32. Christidis K, Devetsikiotis M. Blockchains and smart contracts for the internet of things. *IEEE Access*. 2016;4:2292-2303.
33. Dorri A, Kanhere S, Jurdak R. Towards an optimized blockchain for IoT. Second international conference on internet-of-things design and implementation, Pittsburgh, PA, USA, 2017;173-178.
34. Sompolinsky Y, Zohar A. Secure High-Rate Transaction Processing in Bitcoin. International Conference on Financial Cryptography and Data Security, Berlin, Springer, 2015;507-527.
35. Popov S. The tangle, 2016. https://iotatoken.com/IOTA_Whitepaper.pdf.
36. Masood F, Faridi AR. Consensus algorithms in distributed ledger technology for open environment. 2018 4th International Conference on Computing Communications and Automation (ICCCA), 2018;1-6.

How to cite this article: Bryant B, Saiedian H. Key challenges in security of IoT devices and securing them with the blockchain technology. *Security and Privacy*. 2022;e251. doi: 10.1002/spy2.251