Public Blockchains for Resource-constrained IoT Devices - A State of the Art Survey

JingHuey Khor, Michail Sidorov and PehYee Woon

Abstract— **Although blockchain offers a lot of benefits for the Internet of Things (IoT) network in terms of security, there are a number of barriers to its widespread adoption. Since many IoT networks consist of battery-powered devices with limited computing capabilities, one of those adoption barriers is the IoT end node itself. Several articles provided a general survey of the blockchain integration with IoT applications. However, a detailed analysis of this integration is missing, possible challenges are omitted, and no solutions that would enable the integration are presented. Furthermore, none of the surveys focused on reviewing public blockchains for IoT devices with low computational capabilities and limited energy resources. Therefore, the aim of this paper is to provide the results of an in-depth study that covers challenges faced by existing public blockchains with IoT device integration. This paper looks into resource-constrained IoT device classification and the wireless communication protocols used by them. It examines challenges that are required to be overcome for the successful integration of resource-constrained IoT end nodes with existing public blockchains. It then looks at the proposed solutions and their feasibility. A detailed review of possible security attacks on an IoT blockchain network is provided. As a result, a list of important characteristics that a public blockchain should possess in order to be integrated with a resource-constrained IoT network is proposed. Finally, the requirements for the IoT end nodes themselves are specified.**

Index Terms— **IoT, Public Blockchain, Resource-constrained**

I. Introduction

Internet of Things (IoT) interconnects numerous devices for the purpose of exchanging and updating data for various applications used in a smart city, smart home, smart car, smart healthcare and other smart environments. IoT network itself requires low latency communication to avoid delays, and high throughput in order to support billions of devices, be it via wireless or wired means. IoT devices are either connected to the internet directly, e.g. using cellular connection, Wi-Fi, or indirectly, where a certain IoT protocol is used to communicate with a base station or a gateway in the first instance and then the gateway acts as a portal to the internet. Currently, using a direct cellular connection, e.g. Long Term Evolution (LTE), also known as 4th Generation (4G), for IoT device communication imposes a strain on the edge node itself, mainly due to the large power requirements. To address this, Long Term Evolution for Machines (LTE-M) and later Narrowband IoT (Nb-IoT) were introduced, specifically targeting IoT applications. While they did lower power requirements, it is still not enough for the device to function without periodic battery replacement, which ideally should be avoided for IoT devices. The upcoming fifth Generation (5G) network promises large improvements in terms of faster communication speeds, lower latency, and better connectivity, especially for low-power devices like sensor nodes used for IoT and Industrial Internet of Things (IIoT). IIoT, as a subset of IoT, is targeted at things used in the industrial environment. It requires higher security features compared to the standard IoT devices. Therefore, the integration of blockchain technology with IoT and IIoT networks would be able to act as an additional security layer that provides protection for both of the ecosystems.

A number of survey articles dedicated their attention to the blockchain integration with IoT applications and mostly covered implementation issues and challenges [1-17] while providing only a general overview of blockchain technology to the audience. Hence, they lacked in a detailed analysis of blockchain integration with IoT applications. Furthermore, none of them focused on public blockchains for IoT applications and the prospects of using resource-constrained IoT devices with them. Therefore, the main objective of this paper is to provide a comprehensive study of the existing public blockchains applicable for integration with resource-constrained IoT devices. Readers who require a basic introduction to blockchain technology and glossary are encouraged to refer to the information available in [1-17] articles.

The following lists the main contributions of this paper:

1. An in-depth state-of-the-art survey of the existing public blockchains targeting IoT networks is conducted.
2. Resource-constrained IoT devices and IoT communication protocol are examined.
3. Challenges faced by the integration of the existing public blockchains with resource-constrained IoT devices are analyzed.
4. Existing solutions for the above mentioned challenges are described and their effectiveness for resource-

[T]his paragraph of the first footnote will contain the date on which you submitted your paper for review. "This work was supported by Malaysian Ministry of Higher Education (MOHE) under Grant No. FRGS/1/2018/ICT04/USMC/02/1."

J.H. Khor is with the University of Southampton Malaysia, No.3, Persiaran Canselor 1, Kota Ilmu Educity, 79200, Iskandar Puteri, Johor, Malaysia (e-mail: J.Khor@soton.ac.uk)

M. Sidorov is with Toyohashi University of Technology, 1-1 Tempaku-cho, Toyohashi, Aichi 441-8580, Japan (e-mail: mike@usl.cs.tut.ac.jp).

P.Y. Woon is with University of Southampton Malaysia, No. 3, Persiaran Canselor 1, Kota Ilmu EduCity, 79200 Iskandar Puteri, Johor, Malaysia (e-mail: w.peh-yee@soton.ac.uk).

constrained IoT devices is analyzed.

5. The major possible security attacks on IoT public blockchain networks are analyzed.
6. The future trend for integrating the resource-constrained IoT devices with public blockchains is analyzed.
7. Characteristics that a public blockchain should possess in order to be integrated with a resource-constrained IoT network are proposed.
8. Characteristics of hardware that IoT device needs to have for integration with a public blockchain are listed.

The remaining of this paper is structured as follows: Section II gives a brief background knowledge of blockchain and looks into relevant work. Section III analyzes the integration of existing public blockchains with resource-constrained IoT devices, and looks into challenges of this integration in Section IV. Section V looks into existing solutions for the challenges described in the previous section and Section VI describes possible security attacks on an IoT public blockchain network. Section VII analyzes the possibility of using Class I IoT devices with public blockchains and Section VIII describes the future trend for integrating the resource-constrained IoT devices with public blockchains. Section IX concludes the paper. Detailed structure of this paper is presented in Fig. 1.

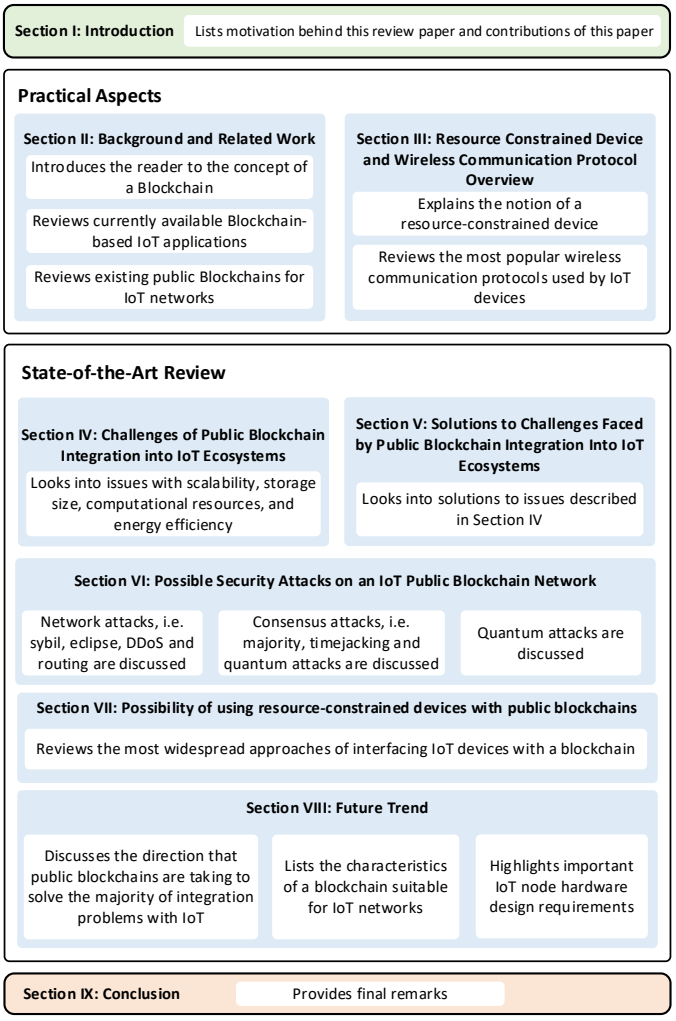


Fig. 1. Detailed article structure

II. Brief Background and Related Work

A. Brief Background Knowledge

Blockchain is a form of a Distributed Ledger (DL) where data is stored using multiple nodes, eliminating the possibility of a single point of failure [18]. Due to its decentralized nature, blockchain offers immutability and a tamper-proof record of data storage [19]. Blockchains can be divided into four main types based on their visibility and accessibility. These types are public, permissioned, private, and hybrid.

Public blockchain is accessible to any user in the world and grants equal read and write rights. All users are allowed to participate in executing a consensus algorithm, which determines how transactions are added to a new block and ensure that all nodes are synchronized. The most known and widely used implementations of public blockchains are Bitcoin, Litecoin, Dash, Monero, Ethereum, etc. [20, 21].

Private blockchain, on the other hand, has strict permissions for reading and writing data. These permissions are mainly reserved for a single authority trusted by other users [22], while users who join the network are only granted with limited access. In this case, private blockchain provides both a higher privacy level and protection, thus, it is better suited for banking and finance industries [23, 24].

Permissioned blockchain, similarly to a private one, requires users to obtain permission to join the network. Few nodes are predetermined to participate in a consensus process [8]. However, unlike a private blockchain which has veto power, permissioned one is controlled by a group of entities, whereby each of these entities has equal rights to participate in a consensus process.

Hybrid blockchain combines both public and private blockchains, with the public one providing accessibility to all users and a private blockchain running in the background to control access to modifications. The leading hybrid blockchains include Libra [25], Dragonchain [26] and XinFin [27].

Consensus, as mentioned before, is an algorithm that is used to reach an agreement in a blockchain. Since it can be executed using several means we can divide all consensus algorithms into two main groups, namely those that require specialized hardware and those that do not. Proof of Work (PoW) is the first and the most widespread consensus algorithm that requires specialized hardware e.g. Graphics Processing Units (GPUs), Field Programmable Gate Arrays (FPGAs) or Application Specific Integrated Circuits (ASICs). In order to execute it, nodes are required to solve a cryptographic hash function puzzle in order to add a new block to the blockchain. This process is typically called mining. Since mining is incentivized with rewards the nodes compete with each other to obtain it. [28]. The first node that solves the puzzle will be granted permission to create a block and receive the reward. PoW, however, is not suitable for implementation in an IoT network since it requires a lot of computational power to solve the puzzle.

Proof of Stake (PoS), Delegated PoS (DPoS), and Byzantine Fault Tolerance (PBFT) [29] belong to consensus algorithms that do not require specialized hardware that performs complex

calculations. In PoS the participants validate transactions by staking the amount of wealth they pose and in return collect network fees as an incentive [28]. The principle of DPoS is similar to PoS, albeit the major difference being inclusion of a delegate that represents the stakeholders [30]. BFT, or a solution to the original Byzantine General Problem, is used by a number of major blockchains, e.g. Stellar uses federated Byzantine agreement [31], Ripple uses Ripple Protocol Consensus Algorithm [32], NEO uses delegated Byzantine Fault Tolerance [33], and Hyperledger Indy uses Redundant Byzantine Fault Tolerance [34]. While their principle differs, the main purpose of these algorithms is to reach consensus without involving a third party.

B. Blockchain-based IoT Applications

A number of research studies focused on the integration of blockchain technology into various IoT applications have been performed. The applications include but not limited to:

1. Smart Industries, where the visibility and transparency of goods in supply chains were increased by introducing a blockchain [35, 36]. The process involved tracking the goods throughout the whole time in a supply chain, from raw material to final products. This kind of tracking process helps to ensure the food safety, pharmaceutical genuineness of drugs, and authenticity of branded goods.
2. Smart Cities. Blockchain integration improved interoperability by enabling secure interconnectivity and data-sharing between various systems [37, 38]. Smart cities combine together new technologies and different services e.g. smart healthcare [15], smart infrastructure, smart buildings, smart mobility and smart energy [39-42] for the purpose of making our everyday lives safer and more convenient.

Some of these studies integrated permissioned blockchains with IoT applications due to higher transaction speeds compared to public ones [36, 39]. From a number of available permissioned blockchains Hyperledger Fabric [43], Hyperledger Sawtooth [43], and Hdac [44] stand out the most. Hyperledger is popular because it is open-sourced, while Hdac is well accepted due to its IoT contract platform. However, same as private and hybrid blockchains, permissioned blockchains rely on trustworthy institutions, thus, are not completely secure. To mitigate the drawback some of the studies proposed to use public blockchains for a better security [35, 40]. Ethereum blockchain is the most likely one used since it has smart contract features that can aid in creating secure applications. Although convenient, Ethereum is not suitable for IoT applications mainly due to its low scalability and low throughput, at this point in time, due to the usage of PoW consensus. Ethereum manages to validate around 15 transactions per second (TPS). For real-world applications, this is not enough. Since Ethereum strives to be a blockchain platform for other projects, a low TPS would mean network congestion resulting in a bottleneck. To process a transaction faster and skip the usual queue the transaction can be given a higher priority. However, this will directly translate into higher transaction fees. A situation like this has already been observed in the past in which a single decentralized application (DApp) i.e. Crypto Kitties managed to congest the Ethereum Network. As a solution Ethereum 2.0 will switch to PoS with an aim of providing higher network throughput at a lower transaction cost.

C. Existing Public Blockchains for IoT Networks

Numerous public blockchains were introduced for IoT networks as shown in Table I. These blockchains are categorized based on their focus area, consensus algorithm, the need for specialized hardware, transaction rate and ledger size. Note that the transaction rate in the table refers to its existing network transaction rate, not the ideal maximum transaction rate stated in their respective white papers. Although some of these blockchains (i.e., BlockMesh, Power Ledger, etc.) claimed that they have their customized consensus algorithms, but they are built on top of Ethereum blockchain. Therefore, their consensus protocol and full ledger size is determined by Ethereum blockchain. Among these blockchains, IOTA [45], VechainThor [46], and Waltonchain [47] are more widely known public blockchains targeted at IoT.

TABLE I
PUBLIC IOT BLOCKCHAIN CATEGORIZATION

Blockchain	Focus area	Consensus protocol	Specialized Hardware	Transaction rate (TPS)	Full ledger size (GB)
Atonomi	Diverse	PoW	No	15	298
IOTA	Diverse	MCMC	No	10	Undefined
IoT Chain	Diverse	PBFT	No	Undefined	Undefined
Ambrosus	Supply Chain	PoA	No	10	Undefined
Waltonchain	Supply Chain	WPoC	Yes	7-15	Undefined
Origin Trail	Supply Chain	PoW	No	15	298
VechainThor	Supply Chain	PoA	Yes	50	Undefined
Slock.It	Hardware connectivity	PoW	No	15	298
BlockMesh	Hardware connectivity	PoW	Yes	15	298
Helium	Hardware connectivity	Proof of Coverage	Hybrid	Undefined	Undefined
FOAM	Location data	Proof of Location	No	Undefined	Undefined
Fysical	Location data	PoW	No	15	298
Power Ledger	Energy	PoW	No	15	298

[1] Undefined – unable to get the specific information from the available resources

IOTA is counted as one of the first public DL IoT platforms. It leverages the technology called Tangle, which uses Markov Chain Monte Carlo (MCMC) algorithm to achieve consensus [45]. The advantage of this protocol is that each incoming transaction must approve two previous transactions in order to be considered valid. Fig. 2 shows an example of this process. More specifically it depicts how the algorithm randomly selects

This article has been accepted for publication in a future issue of this journal, but has not been fully edited. Content may change prior to final publication. Citation information: DOI 10.1109/JIOT.2021.3069120, IEEE Internet of Things Journal

two unconfirmed transactions, known as tips (*A* and *C*), to check and approve two non-conflicting transactions. The tips, *A* and *C*, are then approved by a new transaction *X*. The right bottom corner number represents transaction weight, while the left top corner number represents a cumulative weight. In a Tangle, highly weighted tips are given more consideration to ensure that the heavier branch includes valid transactions. This is important because the heaviest branch of transactions is considered as a valid Tangle. The founder of IOTA claimed that this approach is capable of providing high scalability with 1000 TPS, high security and interoperability to the IoT network. However, since IOTA uses a ternary system it does have interoperability issues, and the model itself is leaning towards a centralized network. Although the ternary system is more efficient in terms of power consumption [45], all existing IoT devices use a binary system. Thus, the IoT devices themselves need to waste more power in converting the ternary value to binary back-and-forth multiple times, which results in significant storage and computational overhead imposed on the system. In addition, IOTA used a central coordinator to protect the Tangle network from a malicious entity trying to perform a hash rate attack [45]. In order to solve this centralization issue, IOTA launched a testnet without the coordinator on March 2019, called Znet. This testnet introduced the Coordicide protocol enabling IOTA to function in a decentralized manner. IOTA then released Coordicide Alphanet on February 2020, which is one of the milestones achieved to reach a coordinator free mainnet. This Alphanet added several new features, including autopeering for automatic peer discovery, gossip layer for transaction exchange, and transaction rate control.

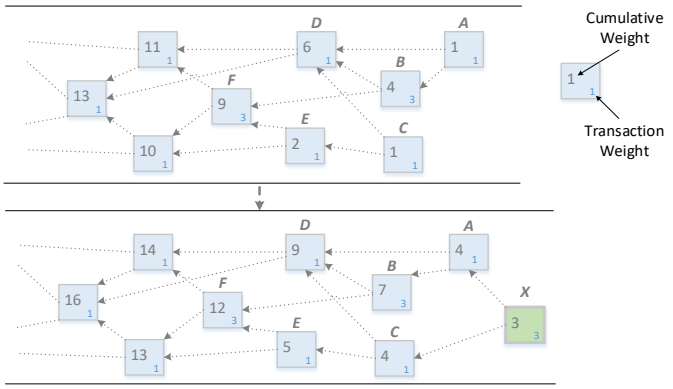


Fig. 2. Tip selection process in a Tangle [14].

Vechain is another blockchain created specifically for IoT networks. It initially launched as a project using Ethereum blockchain, but then migrated over to its own chain named VechainThor. The main aim of VechainThor is to facilitate tracking of goods and merchandise, and can be considered as a blockchain-based supply chain management system. VechainThor uses its in-house built smart chips for tracking goods [46]. The smart chip can be used together with different IoT devices, such as near field communication chips, Radio Frequency Identification (RFID) tags, or Quick Response (QR) codes. VechainThor platform claimed that it can scale up to 10000 TPS by using the Proof of Authority (PoA) consensus mechanism [46]. PoA requires a significantly lower number of validators compared to other algorithms since it is an optimized PoS that stakes the identity instead of a coin, where only selected authority masternodes can validate a block. Therefore, VechainThor can reach consensus without the need of communicating between the nodes. However, VechainThor is not fully decentralized as all authority masternodes are required to reveal their identity to Vechain Foundation.

Waltonchain is another public blockchain platform that is aimed at supply chains. It is used to store the tracking data collected from the proprietary RFID chips attached to IoT devices. Initially, Waltonchain used Proof of Stake Trust (PoST) as a consensus mechanism, where a node reputation-based system with a PoS was utilized to achieve consensus [47]. This PoST protocol ensured that nodes staking more than 5000 Waltonchain coins became masternodes and were allowed to validate transactions. The higher the reputation a masternode has, the more rewards it will obtain. Waltonchain employed a multi-chain design to solve scalability issues where the child chain could process transactions in parallel with the consensus being passed on to the parent chain. However, similar to other blockchains that used PoS, Waltonchain inherited the same drawback whereby design nodes with higher stake had a higher chance to verify transactions. This meant that nodes with a higher stake would have a high chance of taking control of the network. To avoid this, Waltonchain proposed to use Waltonchain Proof-of-Contribution (WPoC) consensus which combines the concepts of PoW, PoS, and Proof of Labour (PoL).

Although the aforementioned public blockchains focused on integration with an IoT network, a successful integration with the resource-constrained IoT devices is yet to be seen [48].

III. Resource-constrained Device and Wireless Communication Protocol Overview

This section classifies IoT devices and looks into the most widely used communication protocols used for data exchange. The computing power of IoT devices can be split into four classes, with resource-constrained IoT devices specified as Class I, as seen in Table II. These devices have low processing capabilities and typically rely on an embedded 8-32 bit Micro Controller Units (MCUs). They have low storage capabilities, up to 256 kB of Read Only Memory (ROM) and 32 kB of Random Access Memory (RAM) and offer minimal network protocol support. Bluetooth Classic, Bluetooth Low Energy (BLE), IPv6 over Low -Power Wireless Personal Area Network (6LoWPAN), Zonal Intercommunication Global-standard (ZigBee), RFID, Near Field Communication (NFC), Long Range (LoRa), SigFox, Weightless (N, P and W), and Ingenu communication protocols are typically supported by this class of devices.

From the table, typical power consumption is defined as the amount of power consumed during the normal operational mode of the chips that supports the relevant communication protocol. Pulsed drain is defined as the amount of power used when the module is transmitting (TX) the data and it is usually number of times higher than the normal operational mode.

TABLE II
IOT DEVICE CLASSIFICATION

Class I	Class II	Class III	Class IV
Low power devices	Moderately powerful devices	Powerful devices	Gateway or high-performance endpoints
Typically consume <10 mW, Up to 500 mW in TX mode	Typically consume >10 mW Up to 1 W in TX	1 W - 10W	> 10 W
8 - 32 bit MCU	32 bit MCU	32 bit MPU	32 - 64bit MPU / SoC
Bluetooth Classic, BLE, ZigBee, Z-Wave, NFC, RFID, LoRa, SigFox, Ingenu, Weightless	Cellular, Ethernet, or Wi-Fi	Ethernet or Wi-Fi	Multi-protocol support including Ethernet, Wi-Fi, ZigBee, BLE, Bluetooth, LoRa, Sigfox, etc.
Used in sensor nodes	Mobile phones, IoT devices with constant power supply	Low-end gateways	High-end gateways

All data compiled from datasheets listed in [49-53]

A. Typical Communication Protocols Used for Resource-constrained Devices

1) Bluetooth Classic and BLE

Bluetooth Classic is a Personal Area Network (PAN) technology that is typically used for short-range data transmission in the 2.4 GHz Industrial Scientific and Medical (ISM) band. BLE is an evolution of the above and was invented to solve the problem of high power consumption faced by Bluetooth Classic. BLE is optimized for sporadic transmissions where it always remains in sleep mode until triggered [54]. The physical layer (PHY) of BLE supports 20 bytes of payload per packet and it has a lower data rate of 250 kbps compared to the 700 kbps of Bluetooth Classic.

2) ZigBee, Z-Wave and 6LoWPAN

ZigBee [55] is another WPAN protocol used for short-range and low-power data exchange, it uses the 2.4 GHz ISM band. ZigBee nodes operate either in a Full-Function Device (FFD) mode that utilizes the full set of the IEEE 802.15.4 Media Access Control (MAC) layer, or a Reduced-Function Device (RFD) mode that performs only a limited number of tasks. FFD devices include a coordinator and a router. Each ZigBee network has at least one coordinator to manage and handle data in the network. Routers are intermediary devices that are used to expand the network coverage by permitting data to pass to other devices. In contrast, end devices that are RFD are used to communicate with FFD devices and operate at low duty cycle power to consume less power. By using a mesh network, ZigBee's communication range can be increased up to 100 meters.

Z-Wave, similarly to Zigbee, is a mesh network and also uses the IEEE 802.15.4 standard. However, Z-Wave uses proprietary radio system and targets the sub-GHz ISM band, eliminating the possible interference with 2.4 GHz Wi-Fi networks, since the main application target for Z-Wave is home IoT. Numerous manufacturers produce Zigbee radios and the IoT applications vary greatly. Both Zigbee and Z-Wave target local area sensor networks.

6LoWPAN is a competitor to Zigbee and was developed to transmit data using an internet protocol. Advantage of 6LoWPAN is that it can communicate with other 802.15.4 devices as well as other types of devices on an IP network.

3) Radio Frequency Identification (RFID) and Near Field Communication (NFC)

RFID is a very short range technology that uses electromagnetic (EM) fields to identify and track objects. RFID system consists of three components – a tag, a reader, and a backend server [56]. The operating frequency of RFID technology can be divided into three bands, namely low frequency (LF), high frequency (HF), and ultra-high frequency (UHF). Passive RFID tags do not have a battery and they are powered using EM energy transmitted from the reader. Unlike passive RFID tags, semi-passive tags and active tags are powered using their own battery. Semi-passive tags rely on the EM energy received from a reader to broadcast the signal, active tags however rely on their own battery.

NFC is an evolution of RFID, it works only at a very close distance usually within 4 cm, but can extend to 20 cm in some cases. The close proximity allows for a greater security, thus NFC is well suited for point of sale or point of purchase purposes.

4) LoRa and LoRaWAN, SigFox, Ingenu, and Weightless

LoRa [57] is an emerging Low Power Wide Area Network (LPWAN) technology that was developed specifically for IoT applications. It enables real-time data collection with low power consumption and covers a wide communication area [58]. SigFox [59], Ingenu [60], and Weightless [61] are all competing protocols. LoRa outperforms them since it is designed to be more cost-efficient and provides less interference compared to other devices [62, 63]. LoRaWAN is a MAC layer designed for the LoRa Physical Layer (PHY). Thus the two should not be confused. There are numerous modules that only support LoRa modulation and do not have the MAC layer. Numerous applications were successfully implemented that use LoRa as a means of communication for IoT sensor nodes and IIoT devices alike [64, 65]. The recently released LoRa 2.4 GHz standard, however, is only applicable for local area communication, since the supported transmission range is diminished.

5) Cellular Protocols : 4G, LTE-M, Nb-IoT, 5G

Cellular protocols usually require higher processing capabilities, which directly result in a higher power consumption negatively affecting battery powered devices. As mentioned before, 4G or LTE consumes the most power, with LTE-M and Nb-IoT coming in second. The advantages of cellular protocols can be clearly visible in their coverage area, since the infrastructure is already in place. Currently 5G is being pushed as the evolution that will enable fast

communication speeds, lower latency and lower power consumption that IoT devices need.

B. Resource-constrained Device Specifications

Table III shows the comparison among resources constrained IoT devices and their common usage in IoT applications. The instruction execution speed determines the processing capabilities of an MCU. A typical 8-bit MCU usually runs at 8 - 24 MHz and is capable of executing 8 - 24 Million Instructions Per Second (MIPS) while a 16 or 32-bit MCUs normally run up to 32 - 48 MHz and processes 32 - 48 MIPS respectively. In addition, an 8 bit MCU has 8 data buses where it supports values from 0 to 2^8-1. In contrast, a 32-bit MCU has 32-bit data buses and supports values from 0 to 2^{32}-1. Furthermore, the onboard ROM and RAM sizes are limited to 512 kbit and 20 - 32 kB respectively. Thus, it is a significant challenge to integrate blockchain with resource-constrained IoT devices, since the device is required to have a fast processing core to support the complexity of a cryptographic consensus algorithm and a large storage capacity to support the ledger.

TABLE III
RESOURCE-CONSTRAINED IOT DEVICE COMPARISON

Protocol	Bluetooth Classic, BLE	ZigBee, 6LoWPAN, Z-Wave	RFID, NFC	LoRa, Sigfox, Ingenu, Weightless
MCU	8 - 32 bit	8 - 32 bit	16 bit	16 - 32 bit
ROM	32 - 384 kB	32 - 384 kB	Passive RFID: 1024 bit Semi-passive RFID: 17.52 kbit Active RFID: 2-128 kbit	32 - 512 kB
IoT application	Healthcare, Smart home	Healthcare, Agriculture, Smart energy, Home Automation	Supply Chain, Healthcare, Agriculture, Contactless Payment	Healthcare, Agriculture, Smart energy, Smart Metering

IV. CHALLENGES OF INTEGRATING PUBLIC BLOCKCHAINS WITH IOT ECOSYSTEMS

There are various challenges that public blockchains need to overcome before they can be successfully integrated with IoT ecosystems. Most of these challenges are various in nature, however, they are mostly related to scalability, ledger size and computational resources needed for participating in the consensus process.

Resource-constrained IoT devices, given their low memory storage and slow processing power, as mentioned in Table III, are incapable of supporting blockchain needs that require a large ledger size and high computational resources. Additionally, given the low transaction rate of the existing blockchain consensus algorithms, a public blockchain is incapable of supporting a large number of connected IoT devices.

A. Scalability

In a blockchain, latency can be divided into block latency and transaction latency. Block latency is the time needed to add a new block to a blockchain, while transaction latency is the time required for a transaction to be added in a block and stored in a blockchain. These latencies have a serious impact on the IoT ecosystem's scalability. The number of IoT devices in smart city applications in European Union is expected to reach 53.63 million by 2025 [66]. This increasing number of nodes in a blockchain causes transmission overhead because every transaction needs to be broadcasted to all of the nodes. Real-time transactions are important to IoT applications targeting human health or digital asset protection, i.e. healthcare, smart homes, etc.

B. Storage size

IoT devices in blockchain-based IoT environments are required to store ledgers at the IoT nodes themselves. Generally, there are two types of nodes in a public blockchain – full nodes and lightweight nodes. A full node needs to store a full copy of a blockchain; it also needs to accept, validate, and relay transactions to other nodes. Unlike a full node, a lightweight node only needs to store the headers of all the blocks in the blockchain. Lightweight nodes verify transactions using a Simple Payment Verification（SPV）method [67]. This method allows them to transmit their transactions to the network with the help of the full nodes, thus the lightweight node needs to be connected to a remote full node. At the time of writing this paper, the size of the full Bitcoin blockchain is approximately 277 GB [68]. In contrast, around 4 TB of space is needed to store the full Ethereum archive chain [69]. In fact, the blockchain size of Bitcoin was around 240 GB back in September 2019 [68], which subsequently has only increased by 37 GB within the last 7 months. Ethereum blockchain, however, was already around 3 TB back in September 2019 [69], and its size has increased substantially mainly due to the fact that there are a lot of decentralized applications running on an Ethereum. They, in turn, generate a lot of transactions resulting in increased storage needs. The size of a Bitcoin lightweight node is around 66 GB and about 200 GB for Ethereum. However, resource-constrained IoT devices, given their small memory storage (normally less than 256 kB), can neither be full nodes nor lightweight nodes. Therefore, resource-constrained IoT devices face a huge challenge in being integrated with public blockchains, irrespective of IoT applications.

C. Computational resources

Among the existing consensus algorithms, PoW requires the highest computational resources. This is intended by design, and the process behind obtaining a specific hash value for solving the cryptographic puzzle. Although other consensus algorithms do not need to perform heavy computations, they are still required to have a certain amount of computational power to reach consensus, broadcast and validate transactions, etc. For example, a node of Algorand blockchain that implements pure PoS requires the system to have 4-8 GB of Random Access

Memory (RAM), a 4 core 32/64 bit Central Processing Unit (CPU), and a 100 Mbit internet connection speed [70]. Therefore, IoT applications, as mentioned in Section II.A, that use resource-constrained IoT devices are unable to directly participate in a consensus process mainly because of the intensive computational requirements imposed by the process itself.

D. Energy consumption

Many public blockchains that use PoW rely on a process called mining to achieve consensus and generate a new block, which requires nodes to have a very high level of computing resources. As an upgrade to the network, Ethereum proposed to switch from PoW to PoS, where the validator is selected based on the number of stakes. With PoS it is possible to save 99% of energy required by PoW, since mining process is not required. Apart from PoS, other consensus algorithms designed to avoid energy-intensive mining process exist. These consensus algorithms include DPoS, PoA, PBFT, Proof of Importance (PoI) [71], etc.

V. Existing Solutions to Challenges Faced by Public Blockchain Integration With IoT Ecosystems

Scalability, storage, processing power, and energy efficiency are all challenges related to the IoT oriented public blockchains [72]. These challenges have to be solved in order to enable the widespread adoption of public blockchain technology in the IoT ecosystem. Several solutions have been introduced to address them, however, not all of them are suitable for resource-constrained IoT devices, as discussed below.

A. Scalability

There are numerous solutions in the development or implementation phases aimed at fixing the scalability issues, described as follows:

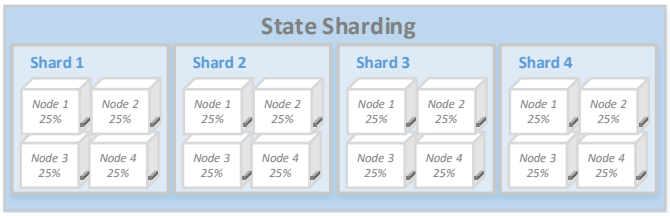
1) Latency Reduction

In order to solve this particular scalability issue, a public blockchain named Zilliqa has improved the classical PBFT by introducing multi-signatures in order to reduce the communication overhead [73]. Another improved version of PBFT is a Secure PoS (SPoS), which is implemented in an Elrond blockchain. The SPoS consensus algorithm is a combination of PoS and PBFT [74]. Consensus algorithms that use the improved version of PBFT have significantly lower latency compared to Bitcoin's PoW. The latency of Bitcoin's PoW consensus algorithm is 600s, while the latency of Elrond's SPoS is 4s, and 120s for Zilliqa's improved version of PBFT [75].

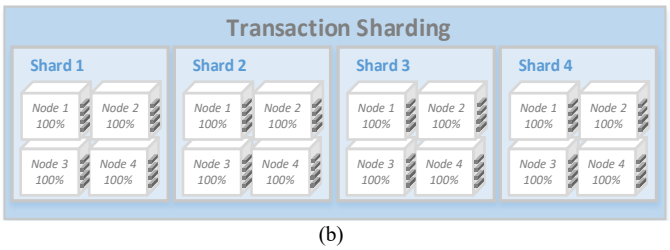
2) Sharding

Sharding is a process of categorizing the blockchain nodes into smaller groups called shards. These shards can be formed based on the nodes' addresses, e.g. all addresses starting with 0x00 will be grouped into one shard, all addresses starting with 0x01 will be grouped into another shard, etc. Sharding is capable of improving the scalability of an IoT blockchain by allowing to validate a huge amount of transactions in parallel. However, this shard categorization approach is vulnerable to single-shard takeover attack, where an attacker takes over the majority of the validators in a shard, e.g. an attacker needs to attain 1% of nodes to dominate a shard if a blockchain network is split into 100 shards, known as a 1% attack. This attack, however, can be prevented by using a random sampling approach, where the validators are randomly assigned to a shard.

Nodes in different shards can exchange information through cross-shard communication in order to verify a transaction. However, most of the proposed networks that use sharding are faced with cross-shard communication issues. It requires carefully designed security measures to ensure secure cross-shard communication. Sharding can be divided into two main categories: state and transaction sharding. State sharding is the process that partitions data on each shard to sub-states. As shown in Fig. 3(a), each of the partitioned pieces of data will be put onto different nodes to operate. Therefore, the memory size requirement for storage on each node is reduced. In contrast, for transaction sharding as shown in Fig. 3(b), each node needs to store a complete global ledger. Although state sharding is better compared to the transaction sharding in terms of storage size, it is susceptible to a single shard takeover attack because once a shard is compromised, it is impossible to recover the complete network ledger, since the compromised shard has the required portion of data. Several blockchains proposed to use state sharding method to improve scalability, such as Ethereum, Quarkchain, Harmony, OmniLedger, RapidChain, Elrond, etc. Ethereum is still working on its state sharding as it is a challenge to design a sharding method that is safe from a single-shard takeover attack, and at the same time does not sacrifice the transaction speed due to cross-shard transactions.



a)



(b)

Fig. 3. Storage of a blockchain ledger for each node in (a) state sharding and (b) transaction sharding

As an example, Quarkchain is using state sharding and PoW as its consensus algorithm. However, Quarkchain has a high degree of cross-shard communication, which has a lower throughput compared to Ethereum. In addition, Quarkchain does not limit the minimum and maximum nodes per shard. Therefore, it is also vulnerable to a single-shard takeover attack

This article has been accepted for publication in a future issue of this journal, but has not been fully edited. Content may change prior to final publication. Citation information: DOI 10.1109/JIOT.2021.3069120, IEEE Internet of Things Journal

if the number of nodes in the shard is very low. In contrast, Zilliqa and Blockclique both use transaction sharding. Zilliqa was the first one to propose using sharding to address the scalability. However, the use of transaction sharding, which requires high storage memory, prevents resource-constrained devices from joining the network. Zilliqa's sharding is also susceptible to a single-shard takeover attack as it counts on PoW as its randomness generation mechanism [76].

3) Side-chain

Side-chain is a second layer blockchain. It exists alongside its main-chain and interacts with the main-chain using a two-way peg mechanism. This approach allows for transactions to be conducted off the main-chain, where tokens or digital assets can be interchanged between the side-chain and the main-chain. During this process, tokens or digital assets will be locked at the main-chain to allow transactions to happen at the side-chain, or vice versa. The result of this approach is higher transaction throughput [77]. A security protocol, such as SPV is needed to guarantee a proper transaction process to happen in both blockchains. SPV allows nodes to access blocks header to verify the validity of transactions using Merkle tree, as shown in Fig. 4. In this figure, four transactions are structured using Merkle tree and are hashed until the last hash value is obtained. This last hash value is the Merkle root.

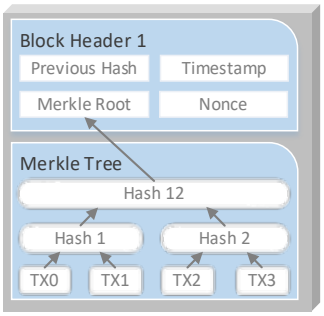
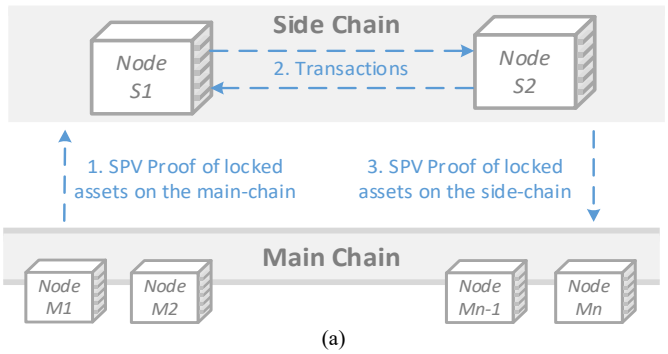
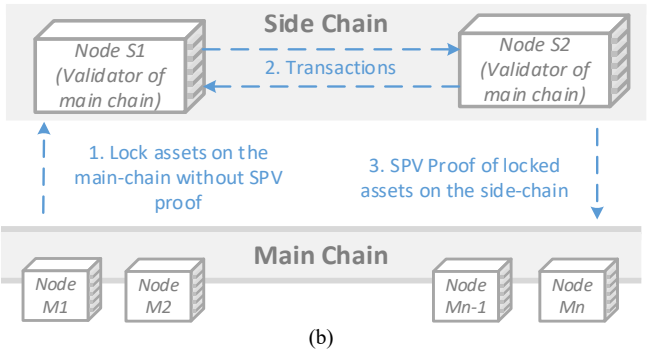


Fig. 4. Block header structure

There are two types of two-way peg mechanisms, namely symmetric two-way peg and asymmetric two-way peg, as shown in Fig. 5. For symmetric two-way peg, an SPV is required both for the main-chain and the side-chain. In contrast, for an asymmetric two-way peg, a SPV is only required when transferring token back to the main-chain, since nodes of the main-chain are not the validators for the side-chain.



(a)



(b)

Fig. 5. (a) Symmetric two-way peg (b) Asymmetric two-way peg

On the other hand, nodes of the side-chain participate in validating main-chain's transactions, thus they are aware of the state of the main-chain. As a result, SPV proof is not required for transferring assets from main-chain to side-chain. Side-chain also offers benefits in adding new features for the main-chain via smart contracts [78] without compromising the main-chain. Furthermore, it increases privacy protection during token or digital asset transfer [79]. Since side-chain is an independent blockchain, it has its own security mechanism to reach consensus. This means that security protection of the side-chain is independent of the main-chain, and a security problem on the side-chain will not affect the main-chain. Additionally, side-chain is attached to the main-chain. This provides lower incentives for miners as it is unable to attract them to join and participate in securing the network. As such, there are side-chains that reach consensus using federation. A federation is a group of miners that act as intermediaries between the main-chain and a side-chain [78]. Members of this federation can be selected by the side-chain developers. Thus, this creates a risk of trusting this federation since the members can be controlled by the developers.

4) State-channel

State channel has been used in IoT blockchain to enable IoT devices to perform transactions offline with the help of third parties [80, 81]. State-channel is a two-way communication channel that is used to enable instant and anonymous transactions between two participants. Unlike side-chain, state-channel is not a blockchain, but a general form of payment channel. Fig. 6 illustrates how transactions of a blockchain are outsourced to a second layer via 2-way state-channel. The process consists of 3 steps. Firstly, when a channel is open, a committed amount of tokens or cryptocurrency by participants is locked to prevent them from being used in an on-chain transaction. Next, transactions in the communication channel are then signed using the private keys of the participants involved in the channel. This ensures the transactions are not exposed to others. The verification of transactions is instantaneous as it involves only the participants in the channel to validate them. The participants have to stay always available to monitor the channel. Lastly, when the channel is closed by participants, the last updated state of transactions will be updated in the main blockchain. The channel can also be closed at a predetermined point in time or after reaching a certain amount of transactions.

This article has been accepted for publication in a future issue of this journal, but has not been fully edited. Content may change prior to final publication. Citation information: DOI 10.1109/JIOT.2021.3069120, IEEE Internet of Things Journal

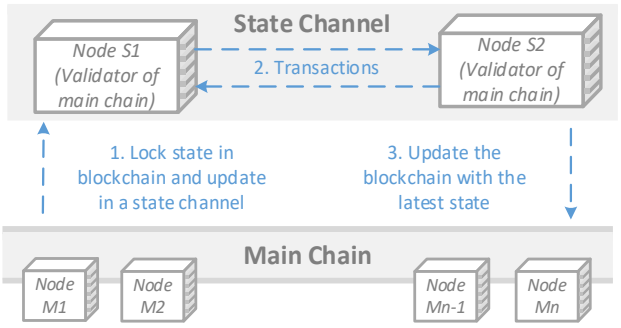


Fig. 6. State channel transaction with a blockchain

Lightning Network [82] and Raiden [83] are the best examples of state-channels where Lighting network is able to increase the total number of Bitcoin transactions and Raiden is useful to enable Ethereum scalability. However, this method is not recommended for IoT networks that involve massive numbers of connected devices because transaction fees will apply and the total amount will be significant in the long run. In addition, the transaction fee is also subjected to the volatility of cryptocurrency.

5) Different data structure

Some distributed ledgers chose to implement a blockless concept and utilized Directed Acyclic Graph (DAG) to achieve consensus. IOTA, COTI, Hashgraph, Byteball, etc. are just some of the representatives. While they still call themselves blockchains, the underlying technology is slightly different. The DAG-based distributed ledgers outperform traditional blockchains in terms of scalability. They allow multiple blocks to co-exist, thus allowing the nodes to operate in parallel. In addition, DAG DL technologies allow for transactions to happen simultaneously as their structure does not require block time. Therefore, they can achieve far greater scalability, reaching at least 1000 TPS.

B. Storage size

As time passes the size of the distributed ledger continuously increases. In some cases, this is not desirable. Thus, different methods exist for managing its size. These include, but not limited to pruning, using snapshots or using off-chain solutions.

1) Pruning

Pruning is a process of removing less relevant information to reduce local storage size. Bitcoin pruning enables a node to keep the last 550 blocks to validate transactions, instead of the full blockchain copy [84]. With a block size of 1 MB, a node requires to have a storage space of 550 MB, instead of 277 GB. However, the drawback of this process is that a node needs to download the entire transaction history before it can actually perform pruning to reduce the storage size.

Recently, Monero added a pruning function to its daemon software in order to remove a lot of unnecessary information. For Monero, a node can remove approximately 2/3 of the total blockchain. This means it only needs to store 20.33 GB instead of 61 GB for the time being. Nodes will prune 7/8 of the transaction data, and the remaining 1/8 transaction data will be used to sync with other nodes [85].

2) Snapshot

The storage size of a full node can be reduced through a snapshot, because it is able to group several transfers to the same address into one record e.g. IOTA uses a global snapshot to keep its ledger database size small [45]. Unfortunately, some of the data is lost during the snapshot process, which might be important to applications that require access to full raw transaction record. Fortunately, this can be solved by using a Permanode, a node that stores the entire data permanently, and has no effect on global pruning. In the case of IOTA, global snapshots are not decentralized and performed only by IOTA coordinator to keep everything in sync. This avoids different nodes having a different set of ledgers. However, the constant increment of ledger size has caused global snapshot to become increasingly impractical to perform as it requires the coordinator to be stopped temporarily to perform pruning and generate a snapshot state. The coordinator is only then can be restarted after the generated files are verified. Recently, IOTA launched a local snapshot function to overcome the lengthy process of global snapshot [86]. This local snapshot function allows the nodes to have a smaller memory storage since nodes are able to sync with a smaller local file through a bootstrap mechanism. The newly launched Coordicide protocol also supports the local snapshot feature.

3) Off-chain

Off-chain provides an interesting solution to the storage size management. Instead of storing a fully complete data on the blockchain, the off-chain blockchain just needs to store hash values of transactions. These hash values can then be used to obtain full data stored outside of the blockchain, called the off-chain storage. This off-chain storage is decentralized and can be used by blockchains as it can provide access to original data within a peer-to-peer network. The existing decentralized storages include InterPlanetary File System (IPFS), StorJ, BigchainDB, Filecoin, Swarm, etc. However, this approach is not efficient as it requires a user to run and maintain three different pieces of software needed to run the blockchain node, the decentralized storage node, and the middleware. Blockchain node and the decentralized storage node need to be run simultaneously and are coordinated by middleware. This middleware has the capability to store the original data in an IPFS and add a hash value of the data to the blockchain. In addition, the middleware is able to fetch the original data from the decentralized storage based on a hash value. The integrity of this data can be then verified by IPFS node to ensure there is no modification made to the original data. MultiChain platform, however, solves the need to run three pieces of software by providing a fully integrated and seamless solution for storing the off-chain data.

C. Computational resources

Although PoW algorithms require the highest computational resources, other consensus algorithms e.g. MCMC tip selection algorithm used in IOTA, PoA, and PoS, still require computational power to reach consensus, broadcast and validate transactions, etc. [87, 88]. In this case, IoT devices

usually offload their computational operations to proxy servers, cloud, sidechains, or edge devices [89]. This method is known as off-chain computation, where computational tasks are performed outside of the local device. There are several blockchains that use this off-chain method to increase the performance of their blockchain, such as Origo, HashCorp, Covalent, etc. Currently methods include cloud server offload, side-chain offload, egde computing offload, and specialized hardware offload. The following looks into these methods in a more detailed manner.

1) Cloud server offload

Cloud offload was designed especially for the purpose of offloading intensive computational tasks to a remote server for faster processing, which in general cannot be supported by the resource-constrained edge devices [90]. However, the existing cloud computing systems are highly centralized, which introduces security issues. For example, Infura was developed to enable users to run decentralized applications without the need of setting up an Ethereum node. Infura is operated by ConsensSys, and is highly reliant on cloud server services provided by Amazon. Thus, if Amazon decides to turn off its cloud servers, all decentralized applications pointed at Infura would stop working. To solve this issue, decentralized cloud systems are emerging, e.g. iExec, Golem, SONM, and DADI are the active players in blockchain-based decentralized cloud computing.

In the case of IOTA, a node uses lightweight PoW to find a correct nonce in order to gain the right to attach a transaction to the Tangle. This mechanism is useful for preventing spamming. Therefore, PoW of IOTA serves a different function compared to e.g. PoW of Bitcoin, where the latter is used to reach consensus. However, since most of the IoT devices are resource-constrained, IOTA has to offload PoW computation to a more powerful proxy server, a service IOTA calls PoWbox [91] or Amazon Web Services (AWS) Lambda [92]. IOTA PoWbox enables users to implement the IOTA node without the need of installing and configuring their local devices. Resource-constrained devices can make application program interface calls to the PoWbox and offload PoW computation to IOTA's dedicated GPU farm [91]. Other than using PoWbox, resource-constrained devices can use AWS Lambda to execute *attachToTangle* function to perform IOTA PoW without the need of running the computations locally [92].

Cloud server offload is not recommended to be implemented in blockchain-based IoT networks mainly because of the centralization.

2) Side-chain offload

The important benefits of using a side-chain would include the ability to offload computational tasks that do not require the full blockchain to operate. Furthermore, sidechain allows performing different computations off the main chain without having to introduce major changes in the main chain's protocol. Noteworthy side-chain projects include Plasma, Liquid, Rootstock, Alpha, etc.

3) Edge computing offload

Offloading computational tasks to cloud servers usually introduces high latency mainly because of the distance between the cloud and a node. Therefore, edge computing has been proposed to be used in a blockchain network to perform computational tasks closer to end devices. Edge computing was known as mobile edge computing until 2017, but then the name was changed to Multi-Access Edge Computing (MEC) since its benefits were not only limited to mobile networks, but also wireless and wired networks. MEC can be used to enable nodes to offload computational tasks to either an edge server or an edge computer [93]. The close physical proximity of the edge server to the edge devices ensures low latency communications [90].

4) Specialized hardware offload

A range of specialized hardware accelerators, such as FPGAs or ASICs, have been utilized to perform heavy computations to reach consensus in public blockchains. Even GPUs, which generally target graphics processing, have been repurposed for many PoW public blockchains such as Ethereum, Ethereum Classic, etc.

At this point in time, some blockchains require high-performance ASICs to achieve efficient participation in the consensus process. Blockchains such as Sia, Bitcoin, Litecoin, etc., allow their participants to receive incentives in proportion to their computational power. However, the specialized hardware used for mining usually consists of dozens of ASIC chips working in parallel. This approach increases the computational speed, which in turn increases the power consumption, e.g. Sia's Obelisk SC ASIC consumes 500W, while Bitcoin Antminer S9 ASIC is specified to draw 1375W. Comparing this to the use of GPUs or CPUs for consensus, the ASIC miners are in a performance league of their own, although this is also PoW consensus dependent. Some public blockchains try to deter the use of ASICs by including different algorithm functions that make up the consensus. This makes ASIC design either hard or unpractical due to the increased number of algorithms. Even though the benefits of using ASICs are visible for mining purposes, using them for resource-constrained IoT nodes in the same manner as how the traditional PoW blockchains use them is unfeasible.

An interesting solution is provided by High Performance Blockchain (HPB), which takes a heterogeneous approach. An approach that includes using dissimilar coprocessors to speed up some of the computations. In this case, a Blockchain Offload Engine (BOE) is used to participate in the consensus process, significantly increasing the computational speed and removing the main processor's strain right from the start [94]. In essence, BOE is a board with a Peripheral Component Interconnect express (PCIe) interface that houses a Zynq UltraScale+ XCZU7CG-FFVC1156 Multi-Processor System-on-a-Chip (MPSoC) [95]. This MPSoC is pre-programmed with modules dedicated to perform specific tasks. One of the modules is a TCP Offload Engine, that is responsible for TCP/IP flow. This engine allows removing the bottleneck of processing the data flow introduced by the general-purpose CPU. Another module

is an Elliptic Curve Digital Signature Algorithm (ECDSA) module that performs signature verification and is essential for fast transaction processing. Finally, a dedicated hardware random number generator adds another layer of security, compared to commonly used pseudo-random number generators. All of this allows BOE to speed up the signature verification process by 5 times compared to the node without BOE and with only 5% of CPU utilization. Although specialized hardware can provide faster verification time, the development of specialized hardware for a blockchain requires a significant time investment and can be hard to design. Thus, up to writing, HPB is the only blockchain with real specialized hardware to offload heavy computations from a node.

For IoT sensor nodes, an onboard heterogeneous approach, like used in BOE, is more viable to be implemented, which is discussed in Section VIII.

D. Energy consumption and efficiency

In this case, energy consumption is defined as the amount of energy consumed during interaction with a blockchain per unit of time. This interaction can either be generating a transaction, writing data, reading data, or participating in the consensus mechanism and does not include other tasks done by the IoT node such as sensing. On the other hand, energy efficiency defines how much of energy is needed to complete these actions.

Blockchains utilizing PoW require the most amount of energy by definition to participate in the consensus. Although there are other algorithms such as PoS, PoA, and PBFT, which are more energy-friendly by design compared to PoW, nevertheless, resource-constrained IoT devices are still unable to support them. Therefore, the advancements, shift, or development of new technologies as described in this subsection might be able to enhance the hardware performance of the resource-constrained IoT devices.

1) Semiconductor manufacturing process node

The process node defines how advanced the techniques are for manufacturing integrated circuits and is named with a number, e.g. 22nm, 14nm, 10nm, etc. This number corresponds to the transistor's gate length and the half distance between the two features on the wafer. However, currently, this is not the case, and manufacturers do not follow this notation. Different IC manufacturers use either their own facilities, external foundries, or both. Leading external foundries, as of the time of writing, that offer their semiconductor manufacturing services are Taiwan Semiconductor Manufacturing Company (TSMC), GlobalFoundries, United Microelectronics Corporation (UMC), Semiconductor Manufacturing International Corporation (SMIC), Samsung, etc. Intel uses their own facilities and is currently transitioning to 10 nm process node while TSMC is already using 7 nm node [96]. Although the node process is different, the feature size when compared seems to be quite similar.

Reducing the node size enables manufacturers to make chips that occupy less space, use less power, and operate at a lower voltage [96]. This is possible because of advances made in the photolithography process. However, the pace at which manufacturers shrink the die features has slowed down recently, since more advanced photolithography techniques are needed to push the boundaries such as the adoption of extreme ultraviolet lithography, etc. It is very common for the newly released CPU chips and GPU chips or high performance FPGAs and ASICs to be manufactured using the latest cutting edge process node. However, this is not true for the microcontrollers used in IoT devices, since manufacturers tend to prioritize profit. Profit highly depends on the yield, i.e. the percentage of functional devices in the wafer. If the yield is low, which is the case with an immature process, then the device's total cost will be higher. Furthermore, manufacturing state-of-the-art masks used during the latest cutting edge photolithography process is extremely expensive, which would make it impractical in terms of cost when the microcontroller manufacturer has hundreds of devices on offer in their component portfolio. In addition, while the microcontroller core would require 1.2 V - 1.8 V due to finer process node, the Input/Output (I/O) die itself ideally would need to operate at 3.3 V or 5 V, to satisfy the requirements of the peripherals being connected to the device, i.e., sensors such as temperature, humidity, accelerometers, etc. This requires additional on-chip components such as voltage regulators for power delivery, introducing a certain degree of design inconvenience to the system. Therefore, microcontrollers usually opt-in for a more mature process, having a higher yield, which results in a lower overall price of the manufactured device.

However, disregarding the choice made by the manufacturers, the advances made in the node process directly impact the computational performance and the energy efficiency of the ICs in a positive manner. As mentioned in the letter from Texas Instruments (TI) [97], a process shrink from 130 nm to 90 nm resulted in a 40% performance improvement of the same IC, although architectural refinements had to be done as a result of the node change. Similar result was noted by Xilinx, where an increase of 2-5 times performance per watt was observed after a move from 28 nm to a 16 nm process [98]. PoW network participants, who try to maximize their network rewards, are well aware of the benefits of using the latest cutting edge equipment. Bitmain, one of the biggest manufacturers of Bitcoin mining equipment, uses the latest 7 nm node from TSMC foundry for their SHA-256 ASIC production in order to offer the best performance and energy consumption products to the market. Xilinx also utilizes TSMC for their UltraScale line of FPGAs, which are then used either in mining equipment produced by other manufacturers, or Xilinx reference cards themselves are repurposed to fit the needs of the PoW algorithm participants.

Despite these benefits, the majority of current microcontrollers used in IoT devices are still manufactured using old process nodes [99-101]. Table IV illustrates this situation in more detail. It shows the comparison between the current node processes used for manufacturing respective products by some of the popular semiconductor design and manufacturing companies.

This article has been accepted for publication in a future issue of this journal, but has not been fully edited. Content may change prior to final publication. Citation information: DOI 10.1109/JIOT.2021.3069120, IEEE Internet of Things Journal

TABLE IV
PROCESS NODES USED FOR IC MANUFACTURING

Semiconductor design company	Current process node and foundries used	Product
Espressif	40 nm TSMC node	32 bit MCUs
Microchip	130 – 1000 nm own nodes	8-32 bit MCUs
ST Microelectronics	40 – 1000 nm own nodes	8-32 bit MCUs
Texas Instruments	32 – 1000 nm own nodes 28 nm TSMC node	8-32 bit MCUs, DSPs, etc. Sitara SoCs
NXP Semiconductors	90 nm – 3 micron own nodes	8-32 bit MCUs
Advanced Micro Devices	7 nm TSMC node	AMD Ryzen CPUs, Radeon AMD GPUs
Intel	10 - 28 nm own nodes	Intel CPUs Intel Chipsets
Samsung	5 – 45 nm own nodes	Exynos SoCs
Qualcomm	7 nm TSMC node 8 nm Samsung node Global Foundries, UMC, and SMIC nodes	Snapdragon SoCs
nVidia	7 nm TSMC node 8 nm Samsung node	GeForce GPUs
Xilinx	7 nm TSMC node	Versal Adaptive Compute Acceleration Platform
	16 nm TSMC node	UltraScale+ FPGA Family
	20 nm TSMC node	UltraScale FPGA Family
	28 nm own node	Virtex-7, Kintex-7, Artix-7, Zynq-7000, Spartan-7
	40 and 45 nm own nodes	Virtex-6 and Spartan-6

All data compiled from articles listed in [98, 102-111]

It is clearly visible that the majority of 8-32 bit MCUs are using processes larger than 32 nm. Compared to the process nodes used for manufacturing modern CPU, GPU and FPGA dies, that is at least 10 years of delay in adoption since the process launch [112], as shown in Fig. 7.

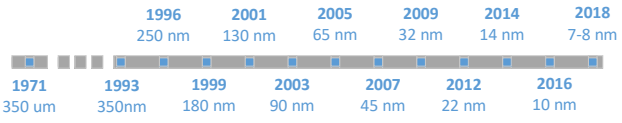


Fig. 7. Semiconductor manufacturing process technology timeline.

Therefore, if the current microcontrollers switch to the newest semiconductor manufacturing nodes, this will enable them to consume less energy while performing the same operations at a greater speed. This will further enable manufacturers to integrate more flash memory that is required to interact with the blockchain, therefore, expanding the IoT and blockchain integration possibilities.

2) Integration of Artificial Intelligence (AI) in the consensus algorithm

The possibility of using AI for different purposes is being continuously explored both by engineers and researchers. A good example of utilisng AI was shown by Google where AI has been successfully used to help reduce the energy consumption of a cooling system by 40% in one of the data centers [113]. Therefore, it is believed that applying machine learning algorithms would help to optimize energy consumption and make blockchain more cost-effective. For example, the mining process could be more productive with the help of AI where miners are able to solve a difficult puzzle more efficiently. In addition, the AI-powered mining algorithms would be able to improve their mining skills by prioritizing tasks and assigning specific nodes to perform critical tasks first [114]. Intel filed a patent on an AI-powered mining system that harnesses power from the PoW mining process and uses it for genetic data sequencing application [115]. Other than PoW, AI also can be integrated with other consensus algorithms, i.e, PoS and DPoS, to enhance the selection process of validators [116].

3) Energy harvesting techniques for IoT devices

Energy harvesting is emerging to enable low power IoT devices to operate by harvesting the energy from an external source e.g., vibration, electromagnetic radiation, and converting it into electrical energy without relying on batteries or eliminating the need to replace them. There is a variety of energy sources that can be used to harvest electrical energy. These are shown in Table V. However, not all of them are suitable for resource-constrained devices. The main factors that determine the suitability of energy harvesters for resource-constrained IoT devices include mainly their power output and size. Small energy harvesters typically generate the energy in a range of 1 μW to 100 mW for low power IoT devices [117]. However, since most of the energy harvesters generate intermittent power, temporary energy storage such as supercapacitor is needed to supply harvested energy to the IoT devices. In addition, the size of the energy harvester should be small, or at least not larger than the space of the original energy source. Although photovoltaic cells provide high power density outdoors, they require constant exposure to light which limits their application in many IoT use cases. Therefore, the generated power is small in a very low light environment, as shown in Table V. Harvesters that convert thermal energy into electricity are capable of harvesting large amounts of power, considering their size. However, they can only operate in areas where a temperature difference is present between two sides of the energy harvesting element. Radio Frequency (RF) energy harvesters are capable of generating the highest power output compared to other energy harvesting techniques per given area. However, their application is limited due to low efficiency indoors and multipath propagation effects. Mechanical energy harvesting, especially piezoelectric, is commonly used in IoT applications that require small amount of power, such as push-button wall switch or a door sensor. However, this type of energy harvester requires a constant vibration or motion source,

thus limiting the use cases [118]. In order to solve the limitations of conventional energy harvesting techniques, hybrid energy harvesting is emerging to provide reliable and constant power to IoT devices. However, this approach increases the complexity and size of energy harvesters [119, 120].

TABLE V
COMPARISON OF ENERGY HARVESTING SOURCES FOR IOT DEVICES

Energy	Transducer	Generated Power, μW	Harvester Size, mm^2	Generated Power per mm^2 ($\mu W/mm^2$)
Mechanical	Piezoelectric [121]	41	5	8.200
	Triboelectric [122]	60	225	0.270
	Magnetoelectric [123]	8	375	0.002
Thermal	Thermoelectric [124]	18,000	324	55.556
Solar	Photovoltaic [125]	100	500	0.200
RF	Rectenna [126]	328,000	25	13,120.000

VI. POSSIBLE SECURITY ATTACKS ON AN IOT PUBLIC BLOCKCHAIN NETWORK

Security attacks on IoT public blockchain networks can be split into two main categories, namely network attacks and consensus attacks. In a blockchain network, each node learns about the peers in the network using a gossip protocol. Although network attack is a difficult task to execute in a decentralized peer-to-peer network, a possibility of it happening still exists. Consensus type of attacks include a variety of double-spend attacks, such as Finney, race, and selfish mining [127]. Double-spend attack typically causes transaction failure because the same token is used twice. Blockchains that implement PoW like Bitcoin, Bitcoin Cash [128], and LTC overcome the double-spend attack by waiting for at least 6 confirmations to assure the transaction is not double spent. Blockchains that implement PoS, such as Cardano [129] mitigates double-spend attack by deducting stakes of attackers if they validate a fraudulent transaction. PBFT on the other hand eliminates the possibility of a double-spend attack by enabling validators to validate a block and then provide finality to the consensus decision. The validity of the block would be verified if it has valid signatures.

Traditional IoT devices collect data from sensors and store it in a database. In a blockchain network, each time an IoT device executes a write function it counts as a one transaction. Thus, using a blockchain that imposes fees for each transaction is impractical, mainly due to the volatile nature of cryptocurrency. Yosemite X [130] is the first public blockchain that operates based on a stablecoin, where its cryptocurrency is pegged to a fiat currency, e.g. United States dollar. Blockchains that reward its participants for executing the consensus mechanism are not applicable for an IoT network since they are susceptible to double-spend attacks. The purpose of this reward system is to maintain a decentralized system. Thus, there is a need to have a public blockchain that can reach consensus without the use of cryptocurrency as an incentive, especially in the case of IoT networks that process huge amounts of transactions per day. This shift would effectively allow mitigating the double-spend attacks. Besides this attack, king, and quantum attacks. The following describes possible attacks on a blockchain network in depth.

A. Network Attacks

1) Sybil attack

Sybil attack is an attack that allows a malicious party to gain control of a blockchain network by owning a huge number of malicious nodes. Attackers can control the network either by manipulating transactions or flooding the network with bad transactions. PoW mitigates this kind of attack by making the attack itself expensive to execute. Attackers need to use a lot of computational resources to produce a block. Similarly to PoW, it is also expensive to perform Sybil attack on PoS. In this case, the attackers need to possess a large number of native cryptocurrency coins in order to add a new block to the blockchain. While PoW and PoS are safe from this attack, PBFT is susceptible. An attacker can compromise the entire network by manipulating a large number of virtual nodes in the network. Therefore, several blockchains, such as Ziliqa, use the PBFT consensus protocol in conjunction with PoW to prevent Sybil attack, whereby PoW is conducted after every 100 blocks.

2) Eclipse attack

Unlike Sybil attack, instead of attacking the majority of the network nodes, an attacker instead blocks all communication from a single specific node. This stops the node from communicating with the blockchain network as it is being compromised by the attack. A Bitcoin node can support a maximum of 117 incoming connections and 8 outgoing connections [131]. Since the number of outgoing connections is very low, the attacker can easily compromise a node and force it to establish connections only to the malicious nodes. In order to manipulate the node's outgoing connections, the attacker needs to modify the node's connection information with the attacker's IP addresses in the new table. After this modification, the node will only attempt to establish a connection with malicious nodes. When a new connection is successfully made by the node, it will add the IP address to the tried buckets. Heilman at. el. proved that the possibility of performing an eclipse attack on Bitcoin's peer-to-peer network is high, where the success rate of the attack is 98.8 % in a worst-case scenario and 84 % for live Bitcoin node scenario [132]. If an attacker successfully performs an eclipse attack, other attacks to break the consensus layer can be performed subsequently.

Marcus *et al.* demonstrated that the Ethereum network at one point was significantly less secure than the Bitcoin network since attackers need to compromise only two machines [133]. This is because Ethereum versions prior to Geth version 1.8 allowed one machine to run an unlimited number of Ethereum nodes by using a different ECDSA public key. Therefore, attackers could have easily created thousands of Ethereum node

IDs by generating ECDSA public keys through the key generation algorithm.

3) Distributed Denial of Service (DDoS)

DDoS attack is an attack where multiple systems are compromised in order to perform Denial of Service (DoS) attack on a single system. Normally, the attack is used to prevent legitimate users from accessing a resource such as computer system, network, server, etc. DDoS attacks are broadly used on the Internet by generating a high volume of requests to the same server preventing legitimate users from receiving the information they need [134]. An attacker can turn computers into botnets by sending emails with malicious software attached in order to infiltrate the computers. The attacker would then gain access to the computers once they are compromised and use them to perform DDoS attacks by overwhelming the target with more requests than it can handle. Thus, using up its entire bandwidth. Blockchain is believed to be safe from DDoS attacks mainly because it is impossible for the attacker to compromise all of the decentralized nodes connected to the network. In addition, blockchain also can be used to mitigate the DDoS attack by providing extra bandwidth to the affected system. However, vulnerabilities in smart contracts might enable DDoS attacks to happen in a blockchain by blocking nodes from transmitting and receiving transactions. Hence, the compromised nodes would not be able to participate in the consensus process, e.g. TRON blockchain was found to be vulnerable to a DDoS attack [135]. Attackers could perform the DDoS attack by using only one computer to deploy a smart contract repeatedly, and thus congest the network with megabytes of bytecode. Since TRON wallet allowed all of the network's available memory to be taken up by a single party with just one computer, the DDoS attack could have affected the entire network.

4) Routing attack

Routing attack usually happens when Internet Service Providers (ISPs) are compromised and intercept internet traffic. According to the data collected from 5 November 2015 to 15 November 2016, 30% of the Bitcoin nodes are hosted by 13 ISPs and 3 ISPs route 60% of all transaction traffic [136]. This proves that Bitcoin nodes are not being spread uniformly, and make the whole Bitcoin network relatively easy to be intercepted by a malicious ISP. Routing attacks can be split into two main categories, namely partition attack and delay attack. Partition attack happens when a set of nodes is made to completely disconnect from a network [136]. Thus, there is no transaction exchange between nodes that are connected to the network and nodes that are not. Delay attack happens when a subset of node connections is intercepted to slow down the propagation of blocks towards or from a given set of nodes [136].

B. Consensus attacks

1) Majority attack

The majority attack, also known as 51% attack, 33% attack, 25% attack, etc. The naming mainly depends on how the consensus algorithm defines the majority. For Bitcoin PoW, a 51% attack can occur if an entity is able to control more than half of the networks' computational power with a malicious intent to use this power to its own benefit. If the attack is successful, the attacker would be able to control the consensus in the network [137]. 51% attacks represent a major problem for blockchain networks that use PoW algorithm. On top of this, the fast evolution of mining pools has increased the possibility of gaining more than half of the computational power in the network even higher. A situation like this has already happened several times throughout the short history of Bitcoin and many other PoW networks. The 51% attack, however, is much more difficult to execute for PoS, because the attacker needs to have more than 51% of coins, instead of computation power [138].

2) Timejacking attack

Nodes in blockchain networks need to keep track of time in order to be in sync with other peer nodes. This can be done by implementing an internal clock system where timing is derived from the median clock time of all its peers. A timejacking attack, as its name suggests, is an attack in which an adversary manipulates timestamps of a target node by connecting it with multiple malicious nodes that have a slower clock [139]. As a result, the target node will reject new blocks received from the network because their timestamp is always greater than the time generated by its internal clock. Consequently, the target node will be isolated from the rest of the network. This way attackers could dominate the entire network and increase the probability of being selected as transaction validators.

3) Quantum attacks

Blockchain uses public key encryption to generate a pair of keys. This pair consists of a private key, only known to the owner, and a public key, which is derived from the private key. The security of a public key encryption relies on the difficulty of hard computational problems, such as integer factorization, logarithmic discretization, or elliptic-curve. This makes it very easy to generate public keys from private keys, and the algorithm makes it very difficult to do the reverse using traditional computing systems. However, the aforementioned hard problems are proven to be vulnerable to quantum attacks.

Shor's algorithm, a polynomial-time quantum computer algorithm for integer factorization, is able to speed up the process of breaking these hard problems. As a consequence, by using it, the ECDSA, a cryptographic algorithm used by Bitcoin for generating the keys, was successfully broken and a private key was extracted [140]. In addition, Grover's algorithm [141], a quantum algorithm that has a high success rate of finding an input to a function that produces a particular output value, may be used to speedup pre-image attacks on hash-based cryptography using a quantum computer. This quantum algorithm requires $O(2^{n/2})$ to find a hash collision, compared to $O(2^n)$ for a modern computer. However, this speedup can be mitigated by doubling hash digest length, which means doubling output length of a hash function. For example, a hash digest with at least 256 bits must be selected in order to achieve 128-bit security [142].

Several cryptography algorithms are believed to be secure from quantum attacks. These are hash-based signatures, code-based, multivariate, supersingular elliptic curve isogeny and lattice-based cryptographies. They are known as post-quantum cryptographies. Several existing blockchains were developed using post-quantum cryptography, as shown in Table VI. All of them employ hash-based cryptography with either Secure Hash Algorithm (SHA) 2 or SHA3 hash functions utilized. Hash-based signature is well accepted in the existing blockchains compared to other post-quantum cryptographies, mainly because of the flexibility of switching to other more secure hash functions. This has happened to IOTA, where its hash function had to be switched to SHA-256 after the original Curl hash function was found to be insecure [143].

TABLE VI
EXISTING QUANTUM RESISTANCE BLOCKCHAINS

Blockchain	Post-quantum Cryptography	Scheme	Hash Function
Nexus	Hash-based	Signature Chains	Skein-1024 Keccak 1600
IOTA	Hash-based	Winternitz signatures	Keccak-384
QRL	Hash-based	Extended Hash-based Signatures	SHA-256
Corda	Hash-based	Blockchained Post-Quantum Signatures	SHA-256
GEO	Hash-based	Lamport Signature	Blake2
Mochimo	Hash-based	Winternitz Type One-time Signature	SHA-256

However, hash-based signature schemes have larger public key and signature sizes than ECDSA ones (i.e., 24 KB vs. 106 bytes). Thus, these huge key and signature sizes require large storage, a requirement that is hard to fulfill with resource-constrained devices.Code-based and multivariate cryptographies are also not suitable to be implemented in resource-constrained IoT devices because the former requires a large public key size, and the latter requires a large storage capacity. For example, in order to achieve a 256-bit security level, code-based cryptography requires a public key that is 1828 times bigger compared to elliptic curves cryptography and 61 times bigger than Rivest-Shamir-Adleman [144]. Although multivariate cryptography requires modest computational resources [145] because it works over small binary fields and uses lightweight public key encryption, it needs to store a large random-looking matrix, which makes it not suitable for resource-constrained devices. Lattice-based cryptography and supersingular elliptic curve isogeny cryptography both have a smaller key size compared to code-based and multivariate cryptographies [146, 147], but the latter generates a large signature. Therefore, intensive computation is required in order to compress the large signature, thus making it not suitable for the implementation in resource-constrained IoT devices [148]. In contrast, lattice-based cryptography is getting more popular in IoT ecosystems since it provides faster operations.

Several research studies have been done to improve and optimize the post-quantum cryptographies for implementation in IoT devices, as shown in Table VII. The public key size and private key size of the improved cryptographies have been significantly reduced compared to other well-known post-quantum cryptographies that target constrained IoT devices, such as BLISS [149], enTTS [150], and Rainbow [150].

TABLE VII
ULTRALIGHTWEIGHT POST-QUANTUM CRYTOGRAPHIES

Post-quantum Cryptography		Security level, *bits*	Platform	Frequency *MHz*	Public key size, *bytes*	Private key size *bytes*
Hash-based	Distributed Ledger One-time Signature [151]	384	CPU	2,400	800	800
Coded-based	Quasicyclic Medium Density Parity Check [152]	80 128	Xilinx Virtex 7	177	600 1,270	1,200 2,540
Multivariate	HiMQ-3^{big} [153]	128	ATxmega384C3	32	146,129	12,953
Supersingular elliptic curve isogeny	Supersingular Isogeny Key Encapsulation [154] SIKEp434	Undefined	Cortex-A55 Cortex-A75	1,766 2,803	330	Undefined
Lattice-based	InvRBLWE-Lightweight [155]	190	Xilinx Spartan6 ASIC (45nm)	174 33	Undefined	Undefined
	NTRUEncrypt EES401EP1 [156]	128	Cortex-M0	32	556	639
	IBE [157]	80	Cortex-M0 Xilinx Spartan6	32 174	4,000	2,000
	RLizard [158]	104 128	ARM Cortex-M3	86	672 1152	401 385
	Ring-LWE [159] High speed	128	ATxmega128A1	32	Undefined	Undefined

This article has been accepted for publication in a future issue of this journal, but has not been fully edited. Content may change prior to final publication. Citation information: DOI 10.1109/JIOT.2021.3069120, IEEE Internet of Things Journal

BLISS belongs to the lattice-based cryptography and has the smallest key size compared to the other two. It requires 2 kB private key and 7 kB of public key, for a 128-bit security level. In contrast, the optimized lattice-based NTRUEncrypt [156] requires 556 B of public key size and 639 B of private key size only for the same 128-bit security level. Multivariate-based Rainbow scheme takes 257 ms to sign a message and 288 ms to perform a verification operation using a 32 MHz microprocessor. However, the optimised multivariate cryptography [153] has simplified the message signing and verifying operations, where it takes 30 ms to sign a message and 69 ms to verify it using a 32 MHz microprocessor. Ebrahimi *et al.* proved that their proposed ultralightweight lattice-based cryptography requires only 7.5k gates and consumes 0.18 mW, which is applicable for use with ultra low-power energy harvesters. In addition, the time needed for a 32 MHz microprocessor to perform encryption and decryption operations is 1.5 ms and 7.6 ms respectively.

VII. Possibility of Using Resource-constrained IoT Devices with Public Blockchains

Currently, some degree of IoT device integration with blockchain is proposed. However, the majority of proposed designs follow the same patterns. These include omitting the IoT node as a blockchain node and instead using a base station to connect to a remote blockchain node [160, 161], as seen in Figure 8. In this case, the IoT node itself has no direct interaction with the blockchain because this is done by the base station. A similar approach was followed in [162, 163], where the IoT nodes generate and sign transactions locally, then send them to a gateway, albeit in this case, a wired serial communication was used instead of the wireless one for simplicity. The gateway then interacts with a remote blockchain node. A notable observation from this study is that the board equipped with an MCU that had the lowest processing capabilities in their test, ATMega328P, required the most energy per unit of time to generate a transaction. Apart from the design architecture, this would also imply that an older semiconductor manufacturing process was used for device fabrication.

Other approaches include using a more powerful device to interact with a blockchain, as shown in Figure 9 [164, 165]. A notable example is the usage of Class II IoT devices [165]. In this setup, an ESP32 SoC from Espressif was used to establish a connection and transact on an Ethereum blockchain. In order to solve computational power and memory storage issues, a smart contract had to be compiled and deployed on another more powerful machine first before running it on the ESP32 device. In addition, this device had to be connected to a remote trusted blockchain node, i.e., Infura, since it is impossible to participate in the PoW consensus mechanism due to the lack of computational resources. Another approach used an IoT node as a light blockchain node to eliminate the need for a remote trusted blockchain node [164, 166].

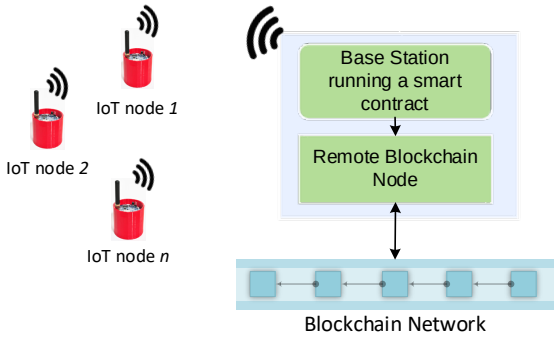


Fig. 8. IoT node connection to the blockchain network via base station.

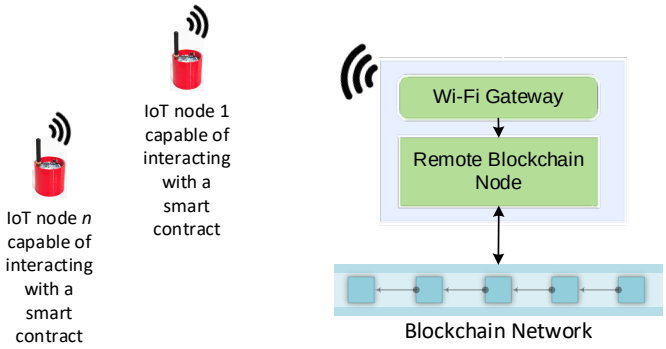


Fig. 9. IoT node connection to the blockchain network via wireless internet gateway.

The successful use case of Class II IoT devices with a public blockchain through a remote node proves that it is possible to use Class I device as a public blockchain node with a proper implementation. However, up to writing, there is no successful deployment of a Class I IoT device acting as a proper node for a public blockchain.

VIII. Future Trend for Integrating Resource-constrained IoT Devices with Public Blockchains

A. The Future Roadmap of Public Blockchains for IoT

This section reviews the future roadmap, i.e. the future trend, of some of the existing public blockchains applicable for IoT networks such as Ethereum, IOTA, and HPB. This section particularly emphasizes how these blockchains address and try to improve their significant drawbacks, such as scalability, ledger size, computational resource requirements, etc. Other public blockchains aimed at IoT are not included because the roadmap is not made available to the public.

1) Scalability

Ethereum has created a roadmap that comprises 6 phases to implement sharding on Ethereum 2.0 network [167]. Basic sharding (phase 1) has been introduced with Ethereum 2.0 to improve the network's scalability. The aim is to create an infinite sharding, also known as super-quadratic sharding. This sharding would allow the Ethereum network to have shards within shards to support hundreds of thousands of transactions per second.

IOTA 3.0 on the other hand will use both fluid sharding and data sharding to improve the scalability of its first and second layers.

2) Storage size

All full nodes in Ethereum 1.0 require storing all data of the entire network. Therefore, the successful implementation of sharding in ETH 2.0 would significantly reduce the ledger size.

Instead of following the same approach, IOTA provides a Chronicle framework. This framework allows anyone to set up a permanode that stores the entire network's transaction history in a distributed database called Scylla [168] and use it for their purposes.

3) Computational resources

Ethereum started the transition from PoW to PoS with its Ethereum 2.0 release. This change addresses the computational resources required to participate in the consensus directly. By switching to PoS, miners will become redundant, and there is a higher chance for resource-constrained devices to participate in the consensus.

From the 30 most recently launched blockchains listed in [169], 21 of them used Ethereum as a base network. This is not surprising, as Ethereum has been a catalyst for different blockchain projects. 4 of the remaining 9 use PoS consensus algorithm, i.e. Gard Governance token, Edumetrix coin, VKF platform, and PBS chain, and 2 of them utilize DPoS-based algorithm (i.e. 7Finance and ReapChain). This proves that the PoS could become a dominant consensus algorithm in blockchain technology.

4) Energy efficiency

Since the latest trend regarding the consensus algorithm is to move away from PoW, as mentioned in the previous section, the energy required to validate a transaction will be greatly reduced.

5) Security

With the gradual move to Ethereum 2.0, the update introduced protection against quantum attacks. Specifically, post-quantum hash-based RANDAO functions have been integrated in the Beacon Chain for generating random numbers [170]. Beacon Chain exists as a separate chain along the side of the current Ethereum mainnet as of now. Its main purpose is to incorporate the upgrades like PoS, sharding, etc. The eventual goal is to merge the mainnet and Beacon Chain under the coordination of the latter.Ethereum 2.0 also plans to switch to quantum-resistant hash-based signature schemes with small signature size, such as eXtended Merkle signature scheme and SPHINCS [171].

Furthermore, zero-knowledge proofs will be utilized by both Ethereum 2.0 and HPB 2.0, to improve privacy [167, 172]. Ethereum 2.0 will integrate zero-knowledge Succinct Non-Interactive Argument of Knowledge (zk-SNARKs) in its second layer network. This zk-SNARKs have some drawbacks such as being vulnerable to quantum attacks and the requirement of a trusted setup, thus, this approach will eventually shift to quantum resistant zero-knowledge Scalable Transparent Arguments of Knowledge (zk-STARKs). The latter do not rely on private-public key pairings and instead are based on collision-resistant hashing, further, a trusted setup is not necessary in this case [167].

6) Cost

IoT applications such as smart industries and smart cities require devices to share information by performing micro-transactions actively. Currently, the majority of IoT devices used Ethereum for integration, specifically, one of Ethereum testnets. The drawback of this is that while the testnets are essentially free to use, since a certain amount of local testnet ETH currency for experiments is provided, the interaction with the mainnet requires real ETH. Each transaction on a blockchain incurs a certain cost priced in gas with the final fee paid in ETH. This cost depends on what function is executed, which is a significant drawback since it contributes to the running costs of the deployed IoT network. At present, only a few public blockchains offer zero transaction fees. These are EOS [173] and IOTA [45]. Feeless transactions are made possible by enabling developers, companies, or platforms to bear the transaction cost. However, most of the existing public blockchains require fees to process them, which hinders their integration with IoT. However, the scalability improvement will enable Ethereum 2.0 and Ethereum 3.0 networks to reduce gas prices and allow IoT devices to make automated micro-transactions [174].

From the analysis conducted in the previous sections, the list of the characteristics that a public blockchain should possess to enable the possibility of using Class I devices as blockchain nodes is summarized as follows:

a. Scalability
   - Use consensus algorithms that provide a low transaction latency.
   - Use sharding to speed up the consensus process.

b. Storage size
   - Store only important information in the ledger.

c. Computational resources
   - PoW algorithms should be avoided.
   - Offload heavy computational processes to a cloud server or edge devices.

d. Energy efficiency
   - Use main MCUs manufactured using a newer semiconductor technology.
   - Use hybrid energy harvesting technologies to provide sustainable energy.

e. Security
   - Consensus protocol should not rely on a centralized party.
   - Amount of stake or identity should not be a factor when selecting a node to validate transactions, as these factors can be easily manipulated by attackers.
   - Use hash-based cryptography in the design of a consensus algorithm to prevent quantum attacks.

f. Running costs
   - Blockchain should adopt a fee-less model to minimize running costs.

B. IoT node requirements

While the blockchain ideally should possess the characteristics mentioned above, there are some aspects of the IoT node design that should be considered as well. These include, but are not limited to using dedicated hardware accelerators, appropriate private key storage, and Over-The-Air (OTA) updates. Neither of these factors were considered in the node implementation described in the previous section, however, they are very crutial for a safe and robust IoT node implementation that targets integration with a blockchain network.

1) Hardware accelerators.

Using hardware accelerators implies a heterogeneous approach. These hardware accelerators speed up certain functions and can be used for a variety of applications, as was previously demonstrated in [175]. Currently, two approaches are possible for IoT purposes, either using an on-chip or an off-chip solution.

The on-chip solution includes an accelerator embedded in the MCU itself. These accelerators can either be programmable FPGAs or specialized modules, e.g., Low-Energy Accelerator (LEA) module from TI integrated into their MSP430FR599x Ferroelectric Random Access Memory line of MCUs [176]. LEA is a 32-bit hardware accelerator designed to perform operations that would take a long time to complete on the MCU core itself, such as signal processing, matrix multiplications, finite impulse response, infinite impulse response, fast Fourier transform, etc. – acceleration that IoT end nodes would benefit from, although is mainly application dependent. The MCU core itself is 16-bit based on a Reduced Instruction Set Computer architecture with a clock speed of up to 16 MHz, which perfectly fits the definition of a Class I resource-constrained device. SmartFusion2 from Microsemi / Microchip in another example [177]. However, this device is more powerful compared to the offerings from TI. The SoC combines a 32-bit Arm Cortex-M3 core processor running up to 166 MHz and an FPGA with 5K- 150K Lookup Tables (LUTs). ProAsic3\e and ProAsic3L SoCs with ARM Cortex-M1 and 330-35K LUT FPGAs is a similar solution from the aforementioned manufacturer. The FPGA part of this SoC can be programmed to perform acceleration.

While the on-chip solution has the accelerator embedded, the off-chip solution implies offloading some of the computations to a different dedicated onboard chip, like a small pre-programmed FPGA, ASIC, or a dedicated cryptographic co-processor IC. Although this approach increases the complexity and size of the printed circuit board, which might not be viable in all cases, it gives the designer flexibility in choosing the applicable ICs and avoids being limited to a fraction of devices that have on-chip accelerators. The off-chip approach is, therefore, currently more popular. A bottleneck introduced by input/output data transfer between the host MCU and the accelerator, and the need to secure the link between the MCU and external accelerator would be among the design considerations that need to be accounted for.

Since each blockchain is unique and uses different cryptographic functions, there is no universal accelerator implementation that would be able to cater to all of the blockchains. Although some accelerators exist that can aid in accelerating certain functions for several blockchains. The widely adopted ECDSA algorithm for sign and signature verification can be sped up using the crypto ATTEC508A [178] and ATECC608B [179] chips from Microchip. However, the variant of the elliptic curve determines the applicability for blockchain purposes. Table VIII demonstrates this in detail.

TABLE VIII
ATTEC508A AND ATTEC608B CRYPTOGRAPHIC FUNCTION SUPPORT

Cryptography	Type	Application	Blockchain
Hash function	SHA256	Address creation	Bitcoin, NEO, XRP, Dash
ECDSA	secp256k1	Transaction signing and verification	Bitcoin, Ethereum, ZCash, XRP, EOS, DASH
ECDSA	secp256r1	Transaction signing and verification	NEO, Tezos

Both ICs support SHA256 hash function. This could be used for address creation in some of the blockchains. Furthermore, these chips support hardware acceleration for the NIST standard P256 prime curve known as secp256r1. However, they do not support the secp256k1 elliptic curve, which is used for most of the blockchains. Although these chips cannot be used to sign the transactions directly, they can be used indirectly to verify the secp256r1 hardware signature, e.g., for Ethereum this can be done at the Ethereum Virtual Machine, and generate a compatible secp256k1 signature for the transaction [180].

A number of researchers have also successfully proposed acceleration approaches for various blockchains. Korotkyi *et al.* showed that is possible to accelerate the original Curl P27 function used in IOTA, prior to their move to Kerl, a ternary version of SHA-3 [181]. Their FPGA implementation allowed for more than 30 times speedup for Curl P27 hash calculation compared to a software implementation running on an ARM Cortex A9 processor [182]. SHA-3 algorithm was also accelerated as demonstrated in [183], with the test platform providing a 1.5 times increase in speed over the software implementation running the same Cortex A9 processor. The Curl P81, the latest iteration of the hashing algorithm used for PoW and transaction hash generation in IOTA, was accelerated as shown in [184]. The implementation provided a 400 times speedup. Furthermore, Keccak384 used in Kerl for address and signature generation, and signature verification was also sped up in the same implementation. Hardware acceleration allowed to finish calculations 40 times faster compared to a pure software implementation. Finally, another recently proposed implementation of the lightweight hashing algorithm for IOTA named Troika, already has an accelerator design written in hardware description language ready to be deployed on an FPGA [185]. The measured speedups for each function are summarised in TABLE IX. From the results, it is clear that devices with hardware accelerators, be it on-chip or off-chip, would greatly help to speed up various functions used in blockchain, which inherently reduce energy consumption compared to devices without these modules - a result that comes from finishing the processing faster and more efficiently.

TABLE IX
HARDWARE ACCELERATOR SPEEDUP SUMMARY

Crypto Function	Hardware Accelerator Platform Specification	Reference Platform Specification	Speedup, *times*
Curl P27	5CSEBA6U23I7 Cyclone V SoC FPGA	ARM Cortex A9	>30x
Curl P81	Cortex M1 + Xilinx Spartan 7 XC7S50	Rasbberry Pi 3B @ 1.2 GHz	>300x
Keccak384	Cortex M1 + Xilinx Spartan 7 XC7S50	Cortex M1 @ 100MHz	>43x
		Cortex M4 @ 72MHz (STM32F302)	>41x
		Rasbberry Pi 3B @ 1.2 GHz	1.25x
		Cortex M3 @ 48MHz (STM32F103)	>70x
SHA-3	Xilinx ZYNQ XC7Z020-1CLG400C SoC FPGA	ARM Cortex A9	>1.5x
Troika	Cortex M1 + Xilinx Spartan 7 XC7S50	Cortex M1 @ 100MHz	>865x
		Rasbberry Pi 3B @ 1.2 GHz	>20x
		Cortex M4 @ 72MHz (STM32F302)	>460x

Data compiled from [181-183, 186, 187]

2) Private key storage.

In order for the node to sign transactions, it needs to have its private key stored on-board. This key has to be stored securely; otherwise, the malicious actors would be able to impersonate the connected node and use it with ill intent if it falls into the wrong hands. Unfortunately, general-purpose microcontrollers typically do not provide this storage. Thus, MCUs or SoCs that specifically target IoT applications, such as ESP32-S2, ESP32-S3 from Espressif [188], LPC18Sxx series from NXP [189], and Renesas RA [190] family offer this option. For devices that do not have secure on-chip key storage, it is possible to use external ICs. These devices can offer not only secure storage but also aid in secure authentication, provide hardware-based crypto acceleration, anti-tampering, and protection from a side-channel attack, e.g. ATSHA204A [191], ATECC608B crypto authentication devices from Microchip [179]. As in the case of using an off-chip hardware accelerator, the link between the IC that stores the private key and MCU has to be secured.

3) Software upgradeability via Over-The-Air (OTA) updates.

Blockchains tend to change their consensus algorithms. This change has happened numerous times in the past already, and indeed happening at this current point in time with Ethereum transitioning to ETH 2.0, ETC switching from Ethash to ETChash, etc. The problem with this is that the communication mechanism with the blockchain might need adjustments. Therefore, it is crucial to enable OTA updates in case the mechanism of communication or transaction generation needs to be changed. Otherwise, a manual firmware update would be needed, and in case the node is deployed in a remote location, that would result in a potential trip to the site that requires time and additional resources.

IX. CONCLUSION

A comprehensive survey of the existing public blockchains for resource-constrained IoT devices was conducted in this paper. Numerous public blockchains aimed at IoT networks were identified, such as IOTA, Vechain, Waltonchain, etc. However, all of them face a number of challenges before they can be fully integrated with IoT networks dominated by resource-constrained IoT devices, such as sensor nodes. These IoT nodes were identified as Class I devices, since they have low processing capabilities, low power consumption, and minimal network protocol support. Scalability, storage size, computational resources, energy efficiency, and security are the main challenges that public blockchains need to overcome before a successful integration takes place. Several solutions were proposed to solve the aforementioned issues, however some of these solutions are not suitable for use with resource-constrained IoT devices. Although a number of studies showed that it is possible to integrate powerful Class II IoT devices with public blockchains, either by using a base station as a blockchain node or using remote trusted blockchain nodes, a proper integration with lower powered devices is yet to be seen. Therefore, based on the analysis conducted in this paper, a list of characteristics was proposed that would potentially enable the use of Class I IoT devices with public blockchains. Furthermore, key aspects of IoT node design, that should be accounted for, are specified. These aspects include, but may not be limited to hardware accelerators, private key storage solutions, and software upgradeability via OTA. Further, a future trend of the existing public blockchains that target IoT networks was analyzed. Sharding techniques, shift to PoS consensus algorithms, and zero-knowledge schemes were identified to be the most popular approaches to solve the existing challenges mentioned above.

Future work will concentrate on the analysis of consensus algorithms suitable for use with resource-constrained IoT devices to achieve better interoperability. Furthermore, a detailed analysis of DAG suitable for resource-constrained IoT devices will be done to achieve a balance of security and computational requirement.

ACKNOWLEDGEMENT

This work was supported by Malaysian Ministry of Higher Education (MOHE) under Grant No. FRGS/1/2018/ICT04/ USMC/02/1.

REFERENCES

[1] M. S. Ali, M. Vecchio, M. Pincheira, K. Dolui, F. Antonelli, and M. H. Rehmani, "Applications of Blockchains in the Internet of Things: A Comprehensive Survey," *IEEE Communications Surveys & Tutorials,* vol. 21, no. 2, pp. 1676-1717, 2019, doi: 10.1109/COMST.2018.2886932.

[2] W. Viriyasitavat, L. D. Xu, Z. Bi, and D. Hoonsopon, "Blockchain Technology for Applications in Internet of Things—Mapping From System Design Perspective," *IEEE Internet of Things Journal,* vol. 6, no. 5, pp. 8155-8168, 2019, doi: 10.1109/JIOT.2019.2925825.

[3] M. A. Ferrag, M. Derdour, M. Mukherjee, A. Derhab, L. Maglaras, and H. Janicke, "Blockchain Technologies for the Internet of Things: Research Issues and Challenges," *IEEE Internet of Things Journal,* vol. 6, no. 2, pp. 2188-2204, 2019, doi: 10.1109/JIOT.2018.2882794.

[4] T. M. Fernández-Caramés and P. Fraga-Lamas, "A Review on the Application of Blockchain to the Next Generation of Cybersecure Industry 4.0 Smart Factories," *IEEE Access,* vol. 7, pp. 45201-45218, 2019, doi: 10.1109/ACCESS.2019.2908780.

[5] A. Panarello, N. Tapas, G. Merlino, F. Longo, and A. Puliafito, "Blockchain and IoT Integration: A Systematic Survey," (in eng), *Sensors (Basel),* vol. 18, no. 8, p. 2575, 2018, doi: 10.3390/s18082575.

[6] M. Wu, K. Wang, X. Cai, S. Guo, M. Guo, and C. Rong, "A Comprehensive Survey of Blockchain: From Theory to IoT Applications and Beyond," *IEEE Internet of Things Journal,* vol. 6, no. 5, pp. 8114-8154, 2019, doi: 10.1109/JIOT.2019.2922538.

[7] H. Dai, Z. Zheng, and Y. Zhang, "Blockchain for Internet of Things: A Survey," *IEEE Internet of Things Journal,* vol. 6, no. 5, pp. 8076-8094, 2019, doi: 10.1109/JIOT.2019.2920987.

[8] K. Christidis and M. Devetsikiotis, "Blockchains and Smart Contracts for the Internet of Things," *IEEE Access,* vol. 4, pp. 2292-2303, 2016, doi: 10.1109/ACCESS.2016.2566339.

[9] Y. Sun, L. Zhang, G. Feng, B. Yang, B. Cao, and M. A. Imran, "Blockchain-Enabled Wireless Internet of Things: Performance Analysis and Optimal Communication Node Deployment," *IEEE Internet of Things Journal,* vol. 6, no. 3, pp. 5791-5802, 2019, doi: 10.1109/JIOT.2019.2905743.

[10] S. K. Lo *et al.*, "Analysis of Blockchain Solutions for IoT: A Systematic Literature Review," *IEEE Access,* vol. 7, pp. 58822-58835, 2019, doi: 10.1109/ACCESS.2019.2914675.

[11] W. Viriyasitavat, T. Anuphaptrirong, and D. Hoonsopon, "When blockchain meets Internet of Things: Characteristics, challenges, and business opportunities," *Journal of Industrial Information Integration,* vol. 15, pp. 21-28, 2019/09/01/ 2019, doi: https://doi.org/10.1016/j.jii.2019.05.002.

[12] S. Voulgaris, N. Fotiou, V. A. Siris, G. C. Polyzos, M. Jaatinen, and Y. Oikonomidis, "Blockchain Technology for Intelligent Environments," *Future Internet* vol. 11, no. 10, 2019.

[13] S. Aggarwal, R. Chaudhary, G. S. Aujla, N. Kumar, K.-K. R. Choo, and A. Y. Zomaya, "Blockchain for smart communities: Applications, challenges and opportunities," *Journal of Network and Computer Applications,* vol. 144, pp. 13-48, 2019/10/15/ 2019, doi: https://doi.org/10.1016/j.jnca.2019.06.018.

[14] J. Xie *et al.*, "A Survey of Blockchain Technology Applied to Smart Cities: Research Issues and Challenges," *IEEE Communications Surveys & Tutorials,* vol. 21, no. 3, pp. 2794-2830, 2019, doi: 10.1109/COMST.2019.2899617.

[15] P. P. Ray, D. Dash, K. Salah, and N. Kumar, "Blockchain for IoT-Based Healthcare: Background, Consensus, Platforms, and Use Cases," *IEEE Systems Journal,* pp. 1-10, 2020, doi: 10.1109/JSYST.2020.2963840.

[16] L. Lao, Z. Li, S. Hou, B. Xiao, S. Guo, and Y. Yang, "A Survey of IoT Applications in Blockchain Systems: Architecture, Consensus, and Traffic Modeling," *ACM Comput. Surv.,* vol. 53, no. 1, p. Article 18, 2020, doi: 10.1145/3372136.

[17] Y. Mezquita *et al.*, "Blockchain Technology in IoT Systems: Review of the Challenges," *Annals of Emerging Technologies in Computing,* vol. 3, no. 5, 2019.

[18] N. Kshetri, "Can Blockchain Strengthen the Internet of Things?," *IT Professional,* vol. 19, no. 4, pp. 68-72, 2017, doi: 10.1109/MITP.2017.3051335.

[19] N. Herbaut and N. Negru, "A Model for Collaborative Blockchain-Based Video Delivery Relying on Advanced Network Services Chains," *IEEE Communications Magazine,* vol. 55, no. 9, pp. 70-76, 2017, doi: 10.1109/MCOM.2017.1700117.

[20] S. Huh, S. Cho, and S. Kim, "Managing IoT devices using blockchain platform," in *2017 19th International Conference on Advanced Communication Technology (ICACT)*, 19-22 Feb. 2017 2017, pp. 464-467, doi: 10.23919/ICACT.2017.7890132.

[21] E. Karafiloski and A. Mishev, "Blockchain Solutions for Big Data Challenges: A Literature Review," in *17th International Conference on Smart Technologies*, Ohrid, 2017, pp. 763-768.

[22] W. Xin, T. Zhang, C. Hu, C. Tang, C. Liu, and Z. Chen, "On Scaling and Accelerating Decentralized Private Blockchains," in *3rd International Conference on Big Data Security on Cloud*, Beijing, 2017, pp. 267-271.

[23] A. Hankin. "JPMorgan's Digital Currency Runs On A Private Blockchain - Here's What Makes It Different From Public Blockchains." MarketWatch. https://www.marketwatch.com/story/jpmorgans-digital-currency-runs-on-a-private-blockchain-heres-what-makes-it-different-from-public-blockchains-2019-02-19 (accessed.

[24] CBInsights. "The March of Financial Services Giants Into Bitcoin And Blockchai Startups In One Chart." CBInsights. https://www.cbinsights.com/research/financial-services-corporate-blockchain-investments/ (accessed.

[25] T. L. A. Members, "Libra White Paper," Libra Association, 2020. [Online]. Available: https://libra.org/en-US/white-paper/

[26] Dragonchain, "Dragonchain Commercial Platform," Dragonchain, 2017, vol. 6. [Online]. Available: https://whitepaper.io/document/58/dragonchain-whitepaper

[27] XinFin, "The XDC Protocol," XinFin Organization, 2017. [Online]. Available: https://www.xinfin.org/docs/whitepaper-tech.pdf

[28] D. Puthal and S. P. Mohanty, "Proof of Authentication: IoT-Friendly Blockchains," *IEEE Potentials,* vol. 38, no. 1, pp. 26-29, 2019, doi: 10.1109/MPOT.2018.2850541.

[29] M. Sidorov, M. T. Ong, R. Vikneswaran, J. Nakamura, R. Ohmura, and J. H. Khor, "Ultralightweight Mutual Authentication RFID Protocol for Blockchain Enabled Supply Chains," *IEEE Access,* pp. 1-1, 2019, doi: 10.1109/ACCESS.2018.2890389.

[30] A. Chauhan, O. P. Malviya, M. Verma, and T. S. Mor, "Blockchain and Scalability," in *2018 IEEE International Conference on Software Quality, Reliability and Security Companion (QRS-C)*, 16-20 July 2018 2018, pp. 122-128, doi: 10.1109/QRS-C.2018.00034.

[31] L. S. Sankar, M. Sindhu, and M. Sethumadhavan, "Survey of consensus protocols on blockchain applications," in *2017 4th International Conference on Advanced Computing and Communication Systems (ICACCS)*, 6-7 Jan. 2017 2017, pp. 1-5, doi: 10.1109/ICACCS.2017.8014672.

[32] D. Schwartz, N. Youngs, and A. Britto, "The Ripple Protocol Consensus Algorithm," *Ripple Labs Inc,* 2014.

[33] B. Ş and G. İnce, "Blockchain-based Framework for Customer Loyalty Program," in *2018 3rd International Conference on Computer Science and Engineering (UBMK)*, 20-23 Sept. 2018 2018, pp. 342-346, doi: 10.1109/UBMK.2018.8566642.

[34] P. Aublin, S. B. Mokhtar, and V. Quéma, "RBFT: Redundant Byzantine Fault Tolerance," in *2013 IEEE 33rd International Conference on Distributed Computing Systems*, 8-11 July 2013 2013, pp. 297-306, doi: 10.1109/ICDCS.2013.53.

[35] K. Salah, N. Nizamuddin, R. Jayaraman, and M. Omar, "Blockchain-Based Soybean Traceability in Agricultural Supply Chain," *IEEE Access,* vol. 7, pp. 73295-73305, 2019, doi: 10.1109/ACCESS.2019.2918000.

[36] M. Sidorov, M. T. Ong, R. V. Sridharan, J. Nakamura, R. Ohmura, and J. H. Khor, "Ultralightweight Mutual Authentication RFID Protocol for Blockchain Enabled Supply Chains," *IEEE Access,* vol. 7, pp. 7273-7285, 2019, doi: 10.1109/ACCESS.2018.2890389.

[37] P. K. Sharma, N. Kumar, and J. H. Park, "Blockchain-Based Distributed Framework for Automotive Industry in a Smart City," *IEEE Transactions on Industrial Informatics,* vol. 15, no. 7, pp. 4197-4205, 2019, doi: 10.1109/TII.2018.2887101.

[38] M. A. Rahman, M. M. Rashid, M. S. Hossain, E. Hassanain, M. F. Alhamid, and M. Guizani, "Blockchain and IoT-Based Cognitive Edge Framework for Sharing Economy Services in a Smart City," *IEEE Access,* vol. 7, pp. 18611-18621, 2019, doi: 10.1109/ACCESS.2019.2896065.

[39] M. Fan and X. Zhang, "Consortium Blockchain Based Data Aggregation and Regulation Mechanism for Smart Grid," *IEEE*

Access, vol. 7, pp. 35929-35940, 2019, doi: 10.1109/ACCESS.2019.2905298.

[40] C. Liu, K. K. Chai, X. Zhang, E. T. Lau, and Y. Chen, "Adaptive Blockchain-Based Electric Vehicle Participation Scheme in Smart Grid Platform," *IEEE Access,* vol. 6, pp. 25657-25665, 2018, doi: 10.1109/ACCESS.2018.2835309.

[41] D. C. Nguyen, P. N. Pathirana, M. Ding, and A. Seneviratne, "Blockchain for Secure EHRs Sharing of Mobile Cloud Based E-Health Systems," *IEEE Access,* vol. 7, pp. 66792-66806, 2019, doi: 10.1109/ACCESS.2019.2917555.

[42] J. Xu *et al.*, "Healthchain: A Blockchain-Based Privacy Preserving Scheme for Large-Scale Health Data," *IEEE Internet of Things Journal,* vol. 6, no. 5, pp. 8770-8781, 2019, doi: 10.1109/JIOT.2019.2923525.

[43] *An Introduction to Hyperledger*, Hyperledger, 2018.

[44] *Hdac: Transaction Innovation - IoT Contract & M2M Transaction Platform based on Blockchain*, HdacTech, 2017.

[45] *The Tangle*, S. Popov, 2017.

[46] *Vechain: Development Plan and White Paper*, Vechain, 2018.

[47] *Waltonchain White Paper V.1.0.4*, Waltonchain, 2018.

[48] O. Novo, "Blockchain Meets IoT: An Architecture for Scalable Access Management in IoT," *IEEE Internet of Things Journal,* vol. 5, no. 2, pp. 1184-1195, 2018, doi: 10.1109/JIOT.2018.2812239.

[49] *MultiTech Conduit - Programmable Gateway for the Internet of Things*, Multitech, 2019. [Online]. Available: https://www.multitech.com/documents/publications/data-sheets/86002198.pdf

[50] *Cisco Wireless Gateway for LoRaWAN*, Cisco, 2019. [Online]. Available: https://www.cisco.com/c/en/us/products/collateral/se/internet-of-things/datasheet-c78-737307.pdf

[51] *InGateway902 Series Industrial Edge Computing Gateway*, I. Networks, 2020. [Online]. Available: https://www.inhandnetworks.com/upload/attachment/202009/01/InHand%20Networks_InGateway902%20Edge%20Gateway_Prdt%20Spec_V2.1.pdf

[52] *CC2652P SimpleLink™ Multiprotocol 2.4 GHz Wireless MCU With Integrated Power Amplifier*, T. Instruments, 2020. [Online]. Available: https://www.ti.com/lit/ds/symlink/cc2652p.pdf?ts=1599062566695&ref_url=https%253A%252F%252Fwww.ti.com%252Fwireless-connectivity%252Fsimplelink-solutions%252Fbluetooth-low-energy%252Fproducts.html

[53] *SARA-R5 series: LTE-M / NB-IoT modules with secure cloud*, Ublox, 2020. [Online]. Available: https://www.u-blox.com/sites/default/files/SARA-R5_ProductSummary_%28UBX-18051286%29.pdf

[54] *Introduction to Bluetooth Low Energy*, Bluetooth, 2019. [Online]. Available: https://cdn-learn.adafruit.com/downloads/pdf/introduction-to-bluetooth-low-energy.pdf

[55] *ZigBee Specification*, Z. Alliance, 2012. [Online]. Available: http://www.zigbee.org/wp-content/uploads/2014/11/docs-05-3474-20-0csg-zigbee-specification.pdf

[56] J. H. Khor, W. Ismail, M. I. Younis, M. K. Sulaiman, and M. G. Rahman, "Security Problems in an RFID System," (in English), *Wireless Pers Commun,* vol. 59, no. 1, pp. 17-26, Jul 2011, doi: 10.1007/s11277-010-0186-2.

[57] A. LoRa, "LoRaWAN Specification 1.0," 2015, doi: https://www.lora-alliance.org/portals/0/specs/LoRaWAN%20Specification%201R0.pdf.

[58] X. Xiong, K. Zheng, R. Xu, W. Xiang, and P. Chatzimisios, "Low power wide area machine-to-machine networks: key techniques and prototype," *IEEE Communications Magazine,* vol. 53, no. 9, pp. 64-71, 2015, doi: 10.1109/MCOM.2015.7263374.

[59] "SIGFOX - The Global Communications Service Provider for the Internet of Things (IoT)," ed.

[60] Ingenu. "RPMA vs Competition." (accessed.

[61] Weightless. Weightless - Setting the Standard for IoT [Online] Available: http://www.weightless.org/

[62] L. Li, J. Ren, and Q. Zhu, "On the Application of LoRa LPWAN Technology in Sailing Monitoring System," in *2017 13th Annual Conference on Wireless On-demand Network Systems and Services (WONS)*, 21-24 Feb. 2017 2017, pp. 77-80, doi: 10.1109/WONS.2017.7888762.

[63] C. Edwards, "Over the hills & far away [Communications Sensors]," *Engineering & Technology,* vol. 11, no. 6, pp. 60-63, 2016, doi: 10.1049/et.2016.0605.

[64] M. Sidorov, P. V. Nhut, A. Okubo, Y. Matsumoto, and R. Ohmura, "TenSense: Sensor Node for the Remote Tension Measurement of a Bolted Joint," in *2019 IEEE International Conference on Pervasive Computing and Communications Workshops (PerCom Workshops)*, 11-15 March 2019 2019, pp. 364-366, doi: 10.1109/PERCOMW.2019.8730699.

[65] M. Sidorov, P. V. Nhut, Y. Matsumoto, and R. Ohmura, "LoRa-Based Precision Wireless Structural Health Monitoring System for Bolted Joints in a Smart City Environment," *IEEE Access,* vol. 7, pp. 179235-179251, 2019, doi: 10.1109/ACCESS.2019.2958835.

[66] S. O'Dea, "mart city IoT active connections in the EI 2016,2019, 2022, and 2025," Statista, 2019. [Online]. Available: https://www.statista.com/statistics/691843/smart-city-iot-active-connections-in-the-eu/

[67] A. Palai, M. Vora, and A. Shah, "Empowering Light Nodes in Blockchains with Block Summarization," in *2018 9th IFIP International Conference on New Technologies, Mobility and Security (NTMS)*, 26-28 Feb. 2018 2018, pp. 1-5, doi: 10.1109/NTMS.2018.8328735.

[68] Blockchain, "Blockchain Size," 2020. [Online]. Available: https://www.blockchain.com/charts/blocks-size.

[69] Etherscan. "Ethereum Full Node Sync (Archive) Chart." https://etherscan.io/chartsync/chainarchive (accessed.

[70] Algorand. "Algorand Network." https://algorand.foundation/network (accessed.

[71] NEM, "NEM Technical Reference," NEM, 2018, vol. Version 1.2.1. [Online]. Available: https://nem.io/wp-content/themes/nem/files/NEM_techRef.pdf

[72] A. Banafa. "IoT and Blockchain: Challenges and Risks." Datafloq. https://datafloq.com/read/iot-and-blockchain-challenges-and-risks/3797 (accessed.

[73] *The Zilliqa Techinical Whitepaper*, Zilliqa, 2017. [Online]. Available: https://docs.zilliqa.com/whitepaper.pdf

[74] Elrond, "Elrond - A Highly Scalable Public Blockchain via Adaptive State Sharding and Secure Proof of Stake," 2018. [Online]. Available: https://elrond.com/files/Elrond_Whitepaper_EN.pdf

[75] *A Scalable Vaue Transfer Protocol for The Digital Economy*, Elrond, 2018. [Online]. Available: https://elrond.com/files/Elrond_Deck_EN.pdf

[76] Zilliqa, "The Zilliqa Technical Whitepaper," Zilliqa, 2017, vol. 1. [Online]. Available: https://docs.zilliqa.com/whitepaper.pdf

[77] A. Back *et al.*, "Enabling Blockchain Innovations with Pegged Sidechains," 2014. [Online]. Available: https://blockstream.com/sidechains.pdf

[78] S. D. Lerner, "RK-Bitcoin Powered Smart Contracts," 2019. [Online]. Available: https://www.rsk.co/wp-content/uploads/2019/02/RSK-White-Paper-Updated.pdf

[79] E. B. Sasson *et al.*, "Zerocash: Decentralized Anonymous Payments from Bitcoin," in *2014 IEEE Symposium on Security and Privacy*, 18-21 May 2014 2014, pp. 459-474, doi: 10.1109/SP.2014.36.

[80] C. Hannon and D. Jin, "Bitcoin Payment-Channels for Resource Limited IoT Devices," presented at the Proceedings of the International Conference on Omni-Layer Intelligent Systems, Crete, Greece, 2019.

[81] B. W. Nyamtiga, J. C. S. Sicato, S. Rathore, Y. Sung, and J. H. Park, "Blockchain-Based Secure Storage Management with Edge Computing for IoT," *Electronics,* vol. 8, 2019. [Online]. Available: https://www.mdpi.com/2079-9292/8/8/828/pdf-vor.

[82] J. Poon and T. Dryja. (2016). The Bitcoin Lightning Network: Scalable Off-Chain Instant Payments.

[83] Raiden. "Raiden Network Specification." https://raiden-network-specification.readthedocs.io/en/latest/ (accessed.

[84] J.-P. Buntinx. "Pro's and Con's on Bitcoin Block Pruning." Bitcoin.com. https://news.bitcoin.com/pros-and-cons-on-bitcoin-block-pruning/ (accessed.

[85] J. Ehrenhofer. "Monero Adds Blockchain Pruning and Improves Transacion Efficiency." Monero. https://ww.getmonero.org/2019/02/01/pruning.html (accessed.

[86] J. Cech. "IRI 1.6.0 With Local Snapshots Out Now." IOTA. https://blog.iota.org/iri-1-6-0-with-local-snapshots-out-now-fc4d991faba8 (accessed.

[87] S. Seth. "Proof of Assignment(PoA)." Investopedia. https://www.investopedia.com/terms/p/proof-assignment-poa.asp (accessed.

[88] A. F. Zorzo, H. C. Nunes, R. C. Lunardi, R. A. Michelin, and S. S. Kanhere, "Dependable IoT using Blockchain-based Technology," in *2018 Eighth Latin-American Symposium on Dependable Computing*, Foz do Iguaçu, 2018. [Online]. Available: http://repositorio.pucrs.br/dspace/bitstream/10923/15221/2/Dependable_IoT_using_Blockchain_based_Technology.pdf. [Online]. Available: http://repositorio.pucrs.br/dspace/bitstream/10923/15221/2/Dependable_IoT_using_Blockchain_based_Technology.pdf

[89] J. Eberhardt and J. Heiss, "Off-chaining Models and Approaches to Off-chain Computations," presented at the Proceedings of the 2nd Workshop on Scalable and Resilient Infrastructures for Distributed Ledgers, Rennes, France, 2018.

[90] M. Lohstroh, H. Kim, J. C. Eidson, C. Jerad, B. Osyk, and E. A. Lee, "On Enabling Technologies for the Internet of Important Things," *IEEE Access,* vol. 7, pp. 27244-27256, 2019, doi: 10.1109/ACCESS.2019.2901509.

[91] E. Greve. "Relaunching the PoWBox." IOTA. https://blog.iota.org/relaunching-the-powbox-d392236b6939 (accessed.

[92] L. Daly. "AWS Lambda and IOTA FTW!" A Medium Corporation. https://medium.com/vessels/a-little-while-back-i-worked-on-little-demo-of-performing-iota-proof-of-work-on-aws-lambda-40195974ded7 (accessed.

[93] F. Xu, F. Yang, C. Zhao, and C. Fang, "Edge Computing and Caching based Blockchain IoT Network," in *2018 1st IEEE International Conference on Hot Information-Centric Networking (HotICN)*, 15-17 Aug. 2018 2018, pp. 238-239, doi: 10.1109/HOTICN.2018.8606001.

[94] HPB, "High Performance Blockchain Whitepaper," HPB, 2018. [Online]. Available: https://hpb.io/HPB_WhitePaper_en.pdf

[95] *Zynq UltraScale+ MPSoC Data Sheet: Overview*, Xilinx, 2019. [Online]. Available: https://ro.mouser.com/datasheet/2/903/ds891-zynq-ultrascale-plus-overview-1662253.pdf

[96] A. Hedding. "What Do “7nm” and “10nm” Mean for CPUs, and Why Do They Matter?" How-To Geek. https://www.howtogeek.com/394267/what-do-7nm-and-10nm-mean-and-why-do-they-matter/ (accessed.

[97] R. Simar, "Chasing Moore’s Law with 90-nm:More Than Just a Process Shrink," Texas Instrument, 2004. [Online]. Available: https://www.ti.com/lit/wp/spry054/spry054.pdf

[98] Xilinx, "UltraSCALE+ Multiplying the Value of 16nm - Staying a Generation Ahead," Xilinx, 2015. [Online]. Available: https://www.xilinx.com/support/documentation/product-briefs/multiplying-the-value-of-16nm.pdf

[99] E. Sperling. "Evolution Of The MCU." Semiconductor Engineering. https://semiengineering.com/evolution-of-the-mcu/ (accessed.

[100] C. Hayes. "Microcontroller balancing act demands a new process." Electronic Specifier. https://www.electronicspecifier.com/products/power/microcontroller-balancing-act-demands-a-new-process (accessed.

[101] B. Bailey. "The MCU Dilemma." Semiconductor Engineering. https://semiengineering.com/the-mcu-dilemma/ (accessed.

[102] STMicroelectronics, "STMicroelectronics - Semi Annual Report 2020," STMicroelectronics, 2020. [Online]. Available: https://investors.st.com/static-files/601d353d-aa59-46b3-ad3d-2009db640a12

[103] N. Semiconductors, "NXP Semiconductors N.V. - Annual Report 2019," NXP Semiconductors N.V., 2019. [Online]. Available: https://investors.nxp.com/static-files/398f8e55-7a29-4e52-9587-2de67897e26d

[104] Xilinx, "Xilinx - Annual Report," Xilinx, 2020. [Online]. Available: https://investor.xilinx.com/static-files/0fbbc50e-a1ed-4629-bd4f-de693d465629

[105] I. Cutress. "AMD Clarifies Comments on 7nm / 7nm+ for Future Products: EUV Not Specified." AnandTech. https://www.anandtech.com/show/15589/amd-clarifies-comments-on-7nm-7nm-for-future-products-euv-not-specified (accessed.

[106] AMD. "AMD "Zen 3" Core Architecture." AMD. https://www.amd.com/en/technologies/zen-core-3 (accessed.

[107] Samsung. "Show All Processors." Samsung. https://www.samsung.com/semiconductor/minisite/exynos/products/all-processors/ (accessed.

[108] Qualcomm, "Qualcomm Snapdragon 855+ Mobile Platform," ed: Qualcomm, 2020.

[109] Qualcomm, "Qualcomm Snapdragon 730 Mobile Platform," Qualcomm, 2020. [Online]. Available: https://www.qualcomm.com/media/documents/files/snapdragon-730-mobile-platform-product-brief.pdf

[110] A. Garreffa. "NVIDIA will shift over to TSMC for new 7nm Ampere GPUs in 2021." TweakTown. https://www.tweaktown.com/news/75679/nvidia-will-shift-over-to-tsmc-for-new-7nm-ampere-gpus-in-2021/index.html (accessed.

[111] S. Ahmad *et al.*, "Xilinx First 7nm Device: Versal AI Core (VC1902)," in *2019 IEEE Hot Chips 31 Symposium (HCS)*, 18-20 Aug. 2019 2019, pp. 1-28, doi: 10.1109/HOTCHIPS.2019.8875639.

[112] TSMC. "Logic Technology." TSMC. https://www.tsmc.com/english/dedicatedFoundry/technology/logic (accessed.

[113] R. Evans and J. Gao. "DeepMind AI Reduces Energy Used for Cooling Goole Data Centers by 40%." Google. https://blog.google/outreach-initiatives/environment/deepmind-ai-reduces-energy-used-for/ (accessed.

[114] B. Technologies. "The Convergence of Blockchain and AI: Beginning of a new Era." A Medium Corporation. https://medium.com/@BangBitTech/the-convergence-of-blockchain-ai-beginning-of-a-new-era-efcd45ed91a2 (accessed.

[115] N. M. Smith and R. Poornachandaran, "Blockchain System with Nucleobase Sequencing as Proof of Work," United States, 2016.

[116] A. Dovbnya. "Meet Velas: When Artificial Intuition Boosts Blockchain Capabilities." U.Today. https://u.today/meet-velas-when-artificial-intuition-boosts-blockchain-capabilities (accessed.

[117] F. Unlu and L. Wawla, "Energy Harvesting Technologies for IoT Edge Devices," Electronic Devices & Networks Annex, 2018.

[118] M. Shirvanimoghaddam *et al.*, "Towards a Green and Self-Powered Internet of Things Using Piezoelectric Energy Harvesting," *IEEE Access,* vol. 7, pp. 94533-94556, 2019, doi: 10.1109/ACCESS.2019.2928523.

[119] J. Bito, R. Bahr, J. G. Hester, S. A. Nauroze, A. Georgiadis, and M. M. Tentzeris, "A Novel Solar and Electromagnetic Energy Harvesting System With a 3-D Printed Package for Energy Efficient Internet-of-Things Wireless Sensors," *IEEE Transactions on Microwave Theory and Techniques,* vol. 65, no. 5, pp. 1831-1842, 2017, doi: 10.1109/TMTT.2017.2660487.

[120] O. B. Akan, O. Cetinkaya, C. Koca, and M. Ozger, "Internet of Hybrid Energy Harvesting Things," *IEEE Internet of Things Journal,* vol. 5, no. 2, pp. 736-746, 2018, doi: 10.1109/JIOT.2017.2742663.

[121] S. Du, Y. Jia, C. Zhao, G. A. J. Amaratunga, and A. A. Seshia, "A Nail-Size Piezoelectric Energy Harvesting System Integrating a MEMS Transducer and a CMOS SSHI Circuit," *IEEE Sensors Journal,* vol. 20, no. 1, pp. 277-285, 2020, doi: 10.1109/JSEN.2019.2941180.

[122] J. Xiong, P. S. Lee, and M.-F. Lin, "Wearable Triboelectric Generator for Energy Harvesting," Patent Appl. PCT/SG2018/050150, 2018.

[123] A. A. Chlaihawi, M. Z. Atashbar, B. J. Bazuin, S. Emamian, and B. B. Narakathu, "Printed Magneto-electric Energy Harvester," United States Patent Appl. US 2018/0351479 A1, 2018.

[124] *Gemini Thermoelectric Generator Harvester*, M. Industries, 2019.

[125] R. Amen, "Energy Harvesting With Thin-Film GaAs Solar Cells," in *Energy Harvesting Industry Session at APEC 2017*, 2017: PSMA Energy Efficiency Committee.

[126] *AEM30940 RF Energy Harvesting*, e.-P. Semiconductors, 2018. [Online]. Available: https://e-peas.com/product/aem30940/

[127] A. Soundararajan. "10 Blockchain and New Age Security Attacks You Should Know." Aruba. https://blogs.arubanetworks.com/solutions/10-blockchain-and-new-age-security-attacks-you-should-know/ (accessed.

[128] BitcoinCash. "Peer-to-Peer Electronic Cash." BitcoinCash. https://www.bitcoincash.org/ (accessed.

[129] P. Gazi, A. Kiayias, and D. Zindros, "Proof of Stake Sidechains," Cardano, 2018. [Online]. Available: https://eprint.iacr.org/2018/1239.pdf

[130] B. Lim *et al.*, "On/Off-Chain Hybrid Exchange System," Yosemite X, 2017. [Online]. Available: https://yosemitex.com/documents/YOSEMITE_Hybrid_Exchange_Technical_White_Paper_20170731a.pdf

[131] E. F. Jesus *et al.*, "A Survey of How to Use Blockchain to Secure Internet of Things and the Stalker Attack," *Security and Communication Networks,* vol. 2018, p. 27, 2018, Art no. 9675050, doi: 10.1155/2018/9675050.

[132] E. Heilman, A. Kendler, A. Zohar, and S. Goldberg, "Eclipse attacks on Bitcoin's peer-to-peer network," presented at the Proceedings of the 24th USENIX Conference on Security Symposium, Washington, D.C., 2015.

[133] Y. Marcus, E. Heilman, and S. Goldberg, "Low-Resource Eclipse Attacks on Ethereum's Peer-to-Peer Network," *Cryptology ePrint Archive,* 2018. [Online]. Available: https://eprint.iacr.org/eprint-bin/cite.pl?entry=2018/236.

[134] Q. Jing, A. V. Vasilakos, J. Wan, J. Lu, and D. Qiu, "Security of the Internet of Things: perspectives and challenges," *Wireless Networks,* journal article vol. 20, no. 8, pp. 2481-2501, November 01 2014, doi: 10.1007/s11276-014-0761-7.

[135] D. Canellis. "TRON Suffered From A Critical Bug That Could Crashed Its Entire Blockchain." TheNextWeb. https://thenextweb.com/hardfork/2019/05/06/tron-blockchain-dos-attack-vulnerability-hackerone-cryptocurrency-trx/ (accessed.

[136] M. Apostolaki, A. Zohar, and L. Vanbever, "Hijacking Bitcoin: Routing Attacks on Cryptocurrencies," in *2017 IEEE Symposium on Security and Privacy (SP)*, 22-26 May 2017 2017, pp. 375-392, doi: 10.1109/SP.2017.29.

[137] A. Reyna, C. Martín, J. Chen, E. Soler, and M. Díaz, "On Blockchain and Its Integration With IoT. Challenges and Opportunities," *Future Generation Computer Systems,* vol. 88, pp. 173-190, 2018/11/01/ 2018, doi: https://doi.org/10.1016/j.future.2018.05.046.

[138] J. Kelly, M. Lauer, R. Prinster, and S. Zhang, "Investigation of Blockchain Network Security - Exploration of Consensus Mechanisms and Quantum Vulnerabilities," *Semantic Scholar,* 2018.

[139] D. Dasgupta, J. M. Shrein, and K. D. Gupta, *A Survey of Blockchain From Security Perspective*. 2019.

[140] B. Rodenburg and S. P Pappas, *Blockchain and Quantum Computing*. 2017.

[141] L. K. Grover, "A fast quantum mechanical algorithm for database search," presented at the Proceedings of the twenty-eighth annual ACM symposium on Theory of Computing, Philadelphia, Pennsylvania, USA, 1996.

[142] P. Waterland, "Quantum Resistant Ledger," Quantum Resistant Ledger, 2016. [Online]. Available: https://www.cryptunit.com/documents/34/QRL_whitepaper.pdf

[143] E. Heilman *et al.*, "Cryptanalysis of Curl-P and Other Attacks on the IOTA Crytocurrency," *IACR Cryptol. ePrint Arch,* vol. 344, 2019.

[144] H. C. Hudde, "Development and Evaluation of a Code-based Cryptography Library for Constrained Devices," Master Master, Ruhr-Universitat, 2013.

[145] A. Petzoldt, M.-S. Chen, J. Ding, and B.-Y. Yang, "HMFEv - An Efficient Multivariate Signature Scheme," Cham, 2017: Springer International Publishing, in Post-Quantum Cryptography, pp. 205-223.

[146] J. Suomalainen, A. Kotelba, J. Kreku, and S. Lehtonen, "Evaluating The Efficiency of Physical and Cryptographic Security Solutions for Quantum Immune IoT," *Cryptography,* vol. 2, no. 5, 2018.

[147] R. J. McEliece, "A Public-Key Cryptosystem Based on Algebraic Coding Theory," in "The Deep Space Network Progress Report " Jet Propulsion Laboratory, 1978, vol. 4244.

[148] T. M. Fernández-Caramès and P. Fraga-Lamas, "Towards Post-Quantum Blockchain: A Review on Blockchain Cryptography Resistant to Quantum Computing Attacks," *IEEE Access,* vol. 8, pp. 21091-21116, 2020, doi: 10.1109/ACCESS.2020.2968985.

[149] T. Oder, T. Pöppelmann, and T. Güneysu, "Beyond ECDSA and RSA: Lattice-based digital signatures on constrained devices," in *2014 51st ACM/EDAC/IEEE Design Automation Conference (DAC)*, 1-5 June 2014 2014, pp. 1-6.

[150] P. Czypek, S. Heyse, and E. Thomae, "Efficient Implementations of MQPKS on Constrained Devices," Berlin, Heidelberg, 2012: Springer Berlin Heidelberg, in Cryptographic Hardware and Embedded Systems – CHES 2012, pp. 374-389.

[151] F. Shahid, A. Khan, and G. Jeon, "Post-quantum distributed ledger for internet of things," *Computers & Electrical Engineering,* vol. 83, p. 106581, 2020/05/01/ 2020, doi: https://doi.org/10.1016/j.compeleceng.2020.106581.

[152] J. H. Phoon, W. K. Lee, D. C. K. Wong, W. S. Yap, B. M. Goi, and R. C. W. Phan, "Optimized IoT Cryptoprocessor Based on QC-MPDC Key Encapsulation Mechanism," *IEEE Internet of Things Journal,* vol. 7, no. 9, pp. 8513-8524, 2020, doi: 10.1109/JIOT.2020.2991334.

[153] K. Shim, C. Park, N. Koo, and H. Seo, "A High-Speed Public-Key Signature Scheme for 8-b IoT-Constrained Devices," *IEEE Internet of Things Journal,* vol. 7, no. 4, pp. 3663-3677, 2020, doi: 10.1109/JIOT.2020.2974264.

[154] H. Seo, P. Sanal, A. Jalali, and R. Azarderakhsh, "Optimized Implementation of SIKE Round 2 on 64-bit ARM Cortex-A Processors," *IEEE Transactions on Circuits and Systems I: Regular Papers,* vol. 67, no. 8, pp. 2659-2671, 2020, doi: 10.1109/TCSI.2020.2979410.

[155] S. Ebrahimi, S. Bayat-Sarmadi, and H. Mosanaei-Boorani, "Post-Quantum Cryptoprocessors Optimized for Edge and Resource-Constrained Devices in IoT," *IEEE Internet of Things Journal,* vol. 6, no. 3, pp. 5500-5507, 2019, doi: 10.1109/JIOT.2019.2903082.

[156] O. M. Guillen, T. Pöppelmann, J. M. B. Mera, E. F. Bongenaar, G. Sigl, and J. Sepulveda, "Towards post-quantum security for IoT endpoints with NTRU," in *Design, Automation & Test in Europe Conference & Exhibition (DATE), 2017*, 27-31 March 2017 2017, pp. 698-703, doi: 10.23919/DATE.2017.7927079.

[157] T. Güneysu and T. Oder, "Towards lightweight Identity-Based Encryption for the post-quantum-secure Internet of Things," in *2017 18th International Symposium on Quality Electronic Design (ISQED)*, 14-15 March 2017 2017, pp. 319-324, doi: 10.1109/ISQED.2017.7918335.

[158] J. Lee, D. Kim, H. Lee, Y. Lee, and J. H. Cheon, "RLizard: Post-Quantum Key Encapsulation Mechanism for IoT Devices," *IEEE Access,* vol. 7, pp. 2080-2091, 2019, doi: 10.1109/ACCESS.2018.2884084.

[159] Z. Liu, H. Seo, S. Sinha Roy, J. Großschädl, H. Kim, and I. Verbauwhede, "Efficient Ring-LWE Encryption on 8-Bit AVR Processors," in *Cryptographic Hardware and Embedded Systems -- CHES 2015*, Berlin, Heidelberg, T. Güneysu and H. Handschuh, Eds., 2015// 2015: Springer Berlin Heidelberg, pp. 663-682.

[160] M. Sidorov, J. H. Khor, P. V. Nhut, Y. Matsumoto, and R. Ohmura, "A Public Blockchain-Enabled Wireless LoRa Sensor Node for Easy Continuous Unattended Health Monitoring of Bolted Joints: Implementation and Evaluation," *IEEE Sensors Journal,* vol. 20, no. 21, pp. 13057-13065, 2020, doi: 10.1109/JSEN.2020.3001870.

[161] L. Hang and D.-H. Kim, "Design and Implementation of an Integrated IoT Blockchain Platform for Sensing Data Integrity," *Sensors,* vol. 19, no. 10, p. 2228, 2019. [Online]. Available: https://www.mdpi.com/1424-8220/19/10/2228.

[162] M. Pincheira and M. Vecchio, "Towards Trusted Data on Decentralized IoT Applications: Integrating Blockchain in Constrained Devices," in *2020 IEEE International Conference on Communications Workshops (ICC Workshops)*, 7-11 June 2020 2020, pp. 1-6, doi: 10.1109/ICCWorkshops49005.2020.9145328.

[163] M. Pincheira, M. Vecchio, R. Giaffreda, and S. S. Kanhere, "Exploiting constrained IoT devices in a trustless blockchain-based water management system," in *2020 IEEE International Conference on Blockchain and Cryptocurrency (ICBC)*, 2-6 May 2020 2020, pp. 1-7, doi: 10.1109/ICBC48266.2020.9169404.

[164] A. Singla and E. Bertino, "Blockchain-Based PKI Solutions for IoT," in *2018 IEEE 4th International Conference on Collaboration and Internet Computing (CIC)*, 18-20 Oct. 2018 2018, pp. 9-15, doi: 10.1109/CIC.2018.00-45.

[165] T. Okada. "Handle Smart Contract on Ethereum with Arduino or ESP32." Medium. https://medium.com/@takahirookada/handle-smart-contract-on-ethereum-with-arduino-or-esp32-1bb5cbaddbf4 (accessed.

[166] J. Huang, L. Kong, G. Chen, M. Wu, X. Liu, and P. Zeng, "Towards Secure Industrial IoT: Blockchain System With Credit-Based Consensus Mechanism," *IEEE Transactions on Industrial*

Informatics, vol. 15, no. 6, pp. 3680-3689, 2019, doi: 10.1109/TII.2019.2903342.

[167] C. Ward. "Sharding Roadmap." Ethereum Wiki. https://eth.wiki/en/sharding/sharding-roadmap (accessed.

[168] L. Kamel. "IOTA: Using Scylla for Distributed Storage of The Tangle." Scylla. https://www.scylladb.com/2020/08/13/iota-using-scylla-for-distributed-storage-of-the-tangle/ (accessed.

[169] CoinMarketCap. "New Cryptocurrencies Recently Added." CoinMarketCap. https://coinmarketcap.com/new/ (accessed.

[170] Ethos. "The Beacon Chain Ethereum 2.0 explainer you need to read first." Ethos.dev. https://ethos.dev/beacon-chain/ (accessed.

[171] A. Bouguera. "How Will Quantum Computing Affect Blockchain?" Consensys. https://consensys.net/blog/blockchain-development/how-will-quantum-supremacy-affect-blockchain/ (accessed.

[172] HPB. "HPB 2.0 Technology Strategy/Governance Roadmap." HPB Foundation. https://www.hpb.io/post-387 (accessed.

[173] H. Vasconcelos. "The Cost of Running a DApp on a EOS Blockchain." DEV. https://dev.to/heldervasc/the-cost-of-running-a-dapp-on-a-eos-network-9j1 (accessed.

[174] R. Millman. "What is Ethereum 2.0 and Why Does It Matter?" Decrypt. https://decrypt.co/resources/what-is-ethereum-2-0 (accessed.

[175] F. Conti, D. Palossi, A. Marongiu, D. Rossi, and L. Benini, "Enabling the heterogeneous accelerator model on ultra-low power microcontroller platforms," in *2016 Design, Automation & Test in Europe Conference & Exhibition (DATE)*, 14-18 March 2016 2016, pp. 1201-1206.

[176] T. Instruments, "Low-Energy Accelerator (LEA) Frequently Asked Questions (FAQ)," Texas Instruments, 2016. [Online]. Available: https://www.ti.com/lit/an/slaa720/slaa720.pdf

[177] Microchip. "SmartFusion2 SoC." Microchip. https://www.microsemi.com/product-directory/soc-fpgas/1692-smartfusion2#overview (accessed.

[178] *ATECC508A Summary Data Sheet*, Microchip, 2017. [Online]. Available: https://ww1.microchip.com/downloads/en/DeviceDoc/20005928A.pdf

[179] *ATECC608A CryptoAuthentication™ Device Summary Datasheet*, Mirochip, 2018. [Online]. Available: https://ww1.microchip.com/downloads/en/DeviceDoc/ATECC608A-CryptoAuthentication-Device-Summary-Data-Sheet-DS40001977B.pdf

[180] L. Lunesu. "A Tale of Two Curves." Enuma Technologies. https://blog.enuma.io/update/2016/11/01/a-tale-of-two-curves-hardware-signing-for-ethereum.html (accessed.

[181] E. Heilman *et al.*, "Cryptanalysis of Curl-P and Other Attacks on the IOTA Cryptocurrency," *IACR Transactions on Symmetric Cryptology,* vol. 2020, no. 3, pp. 367-391, 09/28 2020, doi: 10.13154/tosc.v2020.i3.367-391.

[182] I. Korotkyi and S. Sachov, "Hardware Accelerators for IOTA Cryptocurrency," in *2019 IEEE 39th International Conference on Electronics and Nanotechnology (ELNANO)*, 16-18 April 2019 2019, pp. 832-837, doi: 10.1109/ELNANO.2019.8783449.

[183] I. L. R. Azevedo, A. S. Nery, and A. d. C. Sena, "A SHA-3 Co-Processor for IoT Applications," in *2020 Workshop on Communication Networks and Power Systems (WCNPS)*, 12-13 Nov. 2020 2020, pp. 1-5, doi: 10.1109/WCNPS50723.2020.9263759.

[184] T. Pototschnig. "PiDiver 1.3 Documentation." GitLab. https://gitlab.com/microengineer18/pidiver1.3/-/wikis/home (accessed.

[185] T. Pototschnig. "Welcome to The ICCFPGA-Core Wiki." Gitlab. https://gitlab.com/iccfpga/iccfpga-core/-/wikis/home (accessed.

[186] MicroEngineer. "IOTA Crypto Core FPGA — 1st Progress Report." MicroEngineer. https://medium.com/@punpck/iota-crypto-core-fpga-1st-progress-report-caebe1dac579 (accessed.

[187] MicroEngineer. "IOTA Crypto Core FPGA — 2ndProgress Report." MicroEngineer. https://medium.com/@punpck/iota-crypto-core-fpga-2ndprogress-report-c3fbf8715ea1 (accessed.

[188] *ESP32 Series Datasheet*, E. Systems, Shanghai, 2020. [Online]. Available: https://www.espressif.com/sites/default/files/documentation/esp32_datasheet_en.pdf

[189] *NXP® 180 MHz 32-bit MCUs with Integrated Security* NXP, 2016. [Online]. Available: https://www.nxp.com/docs/en/fact-sheet/LPC18SXXLF.pdf

[190] Renesas. "MCU Solutions for IoT Security." Renesas. https://www.renesas.com/us/en/application/technologies/iot-security/mcu-iot-security-solutions (accessed.

[191] *ATSHA204A Microchip CryptoAuthentication Data Sheet*, Microchip, 2018. [Online]. Available: https://ww1.microchip.com/downloads/en/DeviceDoc/ATSHA204A-Data-Sheet-40002025A.pdf

JINGHUEY KHOR is an Assistant Professor at the University of Southampton Malaysia and a visiting academic at the University of Southampton, UK. She joined the university as a lecturer in 2014 and currently she teaches different subjects that include Digital Systems, Electronic Engineering Design, and Advanced Programming Modules. Starting 2021 she is a visiting researcher at Yonsei University under the International Scholar Exchange Fellowship (ISEF) Program of the Chey Institute for Advanced Studies. During her early research career, she has focused on designing lightweight cryptographic protocols for RFID systems. Starting the year of 2016, she has been actively designing privacy preserving protocols for communication between IoT devices and blockchain, designing new consensus algorithms and decentralized application for IoT purposes. She has served as a technical committee member for several international conferences, and as a reviewer for IEEE and Elsevier journals.

MICHAIL SIDOROV is a Research Fellow at the Toyohashi University of Technology (TUT), Japan working in the field of IoT. He has received his B.Sc degree in Informatics from Coventry University, UK in 2009, B.Sc Degree in Informatics Engineering from Klaipeda University, Lithuania in 2010, a joined M.Sc degree in Embedded Computing Systems (EMECS) from Norwegian University of Science and Technology (NTNU), Norway and University of Southampton (UoS), UK in 2013, and Ph.D in Computer Science and Engineering from TUT in 2020. He was a Teaching Fellow and Laboratory Officer for the period of 2013 – 2017 at the University of Southampton Malaysia. His current research interests include energy harvesting sensor network design, LPWAN, and blockchain technology for IoT.

PEH YEE WOON joined University of Southampton Malaysia (UoSM) as a teaching assistant in 2017. She is a MEng Electrical and Electronic Engineering graduate from University of Southampton. Her interests include machine learning, statistical modelling, and blockchain.