# Blockchain for 5G and IoT: Opportunities and Challenges

Tharaka Hewa*, Anshuman Kalla†, Avishek Nag‡, Mika Ylianttila§, Madhusanka Liyanage¶
*§¶Centre for Wireless Communications, University of Oulu, Finland
†School of Computing and Information Technology, Manipal University Jaipur, India
‡School of Electrical and Electronic Engineering, University College Dublin, Ireland
§School of Computer Science, University College Dublin, Ireland
Email: *§¶[firstname.lastname]@oulu.fi, ‡anshuman.kalla@jaipur.manipal.edu, §avishek.nag@ucd.ie, ¶madhusanka@ucd.ie

***Abstract*—Hitherto, the evolution of mobile networks have fulfilled the increasing demands for enhanced performance, availability, portability, elasticity, and energy efficiency posed by the ever growing network services. In line with the progression, 5G depicts the next generation of mobile networks that further promises remarkable performance improvements as well as creation of new value chain. In parallel with 5G, the Internet of Things (IoT) has also emerged as new paradigm for interconnection of massive communication-capable heterogeneous smart objects. 5G is envisaged to broaden IoT's scope and fields of applicability. However, since current mobile networks and also more general IoT systems are based on centralized models thus it is anticipated that they will face tremendous challenges to meet-up the requirements of future 5G-enabled-IoT use cases. To solve these inevitable issues blockchain stands out as a promising technology. Some of the offerings of Blockchain technology are immutability, non-repudiation, proof of provenance, integrity, privacy, etc. Blockchain's combination with 5G and IoT still requires essential insights with respect to concrete application domains, scalability, privacy issues, performance, and potential financial benefits. The paper aims to elaborate and emphasize the key aspects of the use of Blockchain for 5G and IoT.**

***Index Terms*—Blockchain, Cyber Physical Systems (CPS), Internet of Things (IoT), Industrial Internet**

## I. Introduction

Last couple of decades have witnessed remarkable evolution both in the space of Internet as well as mobile communications. Looking at the evolution of the Internet, the journey so far is marked by five different phases [1]. It emanated from local computer networking aimed at sharing of expensive resources to WWW (World Wide Web) which enabled sharing of soft information, globally. Then came the phase of mobile-Internet which opened the use of mobile networks to access Internet while connected devices are on the move. Next arrived the phase of social networks where people started making use of Internet to stay connected and share their stories. The current phase is of the Internet-of-Things (IoT) that provides means to connect almost all kind of physical objects to the Internet. Today, IoT is swiftly penetrating the global network space by enabling connectivity of devices ranging from tiny consumer-devices to heavy industrial machines. Thus, IoT has the potential to radically transform the way automation is perceived at the (physical) object level. IoT offers exciting new avenues especially for industries, since it intrinsically supports the much required Machine-to-Machine (M2M) Communications. Standardization bodies are eagerly looking into such kind of M2M communications [2].

The evolution of mobile networks marked its inception in the year 1980 as first generation (1G) that merely supported voice communication. With 2G, digital systems hit the market and thus the services like text message were introduced. It was the 3G which provided mobile broadband services with improved level of security. 4G, by and large the current generation, enhanced the date rate, security and QoS whereas reduced the latency. The mobile communication industry are not ready for 5G.

The advancements in IoT and the soon arrival of 5G, have popularized the development of 5G-enabled-IoT applications. Such applications pose stringent requirements such as high capacity, assured privacy & security, scalability of heterogeneous applications, ultra low latency, optimized use of network resources, efficient energy management and low OPEX[3]. Despite the fact that the security architectures that are currently being used for mobile networks and generic IoT systems match the required expectations, they are in principle centralized [4], [5], [6]. Using such centralized security solutions for 5G and 5G-enabled-IoT applications will lead to various impediments like increased cost due to inherent heterogeneity, complex and static security management procedures, over-utilization of network resources, creation of bottleneck in the network, single point-of-failures, high OPEX, etc. Thus, continuing the use of centralized security solutions for 5G and IoT driven applications will not only struggle to meet the demands but will also adversely affect the projected visions of 5G and IoT.

In this context, blockchain technology turns out to be a promising building block as it can provide solution to all security related issues in a unified and decentralized way. To appreciate the possible business value that can be achieved with the underpinning of Blockchain technology for 5G and IoT, it is worth looking at their estimated individual business values. On the one hand, IoT's global market is estimated to reach at $457 billions by 2020 [7], and IIoT exclusively will add $14.2 trillion value by 2030 [8]. On the other hand, 5G will add business-to-business value of $700 billion by 2030 [9]. Whereas, a recent Gartner study predicts that $3.1 trillion of business value will be created by Blockchain by 2030 [10].

Thus, it is worth exploring the opportunities and challenges pertinent to the use of Blockchain as decentralized security and privacy solution for both 5G and IoT.

The rest of the paper is organised as follows. Section II provides a quick overview on the 5G, IoT, and the Blockchain. Section III explains the significant challenges in the 5G and IoT contexts. Section IV illustrates the values that Blockchain brings in for 5G and IoT. Section V elaborates the new challenges in the Blockchain and IoT integration, with some related works to address these challenges. Section VI concludes the paper.

## II. Background

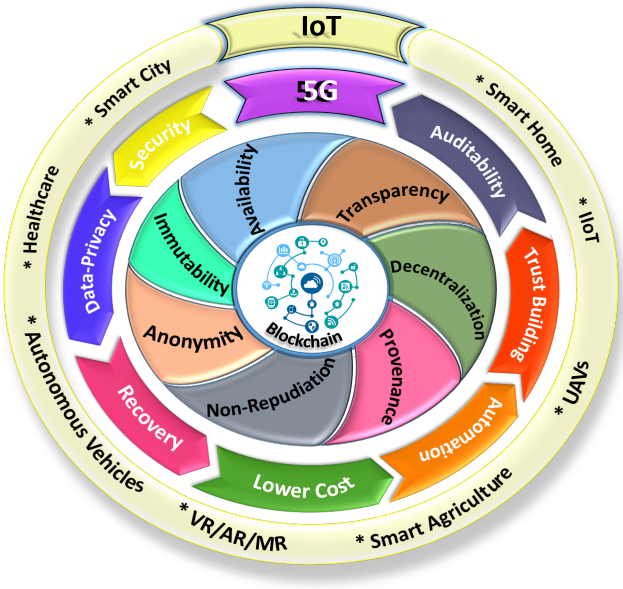


Fig. 1. Overview of the blockchain and its impact on 5G

### A. 5G

The next generation of the mobile networks to be rolled-out is 5G. ITU-R (Radio-communication Sector), which is one of the three sectors of International Telecommunication Union (ITU), has defined three broad services for 5G as eMBB (enhanced Mobile BroadBand), mMTC (massive Machine Type Communication), and URLLC (Ultra Reliable and Low Latency Communications) [11]. To support such varied kind of services, 5G is characterised by ultra low round-trip latency (of order of 1 ms), high data rate (of order of 10 Gbps), high scalability (of the order of 100x connected devices), etc. The key enabling technologies for 5G are Network Slicing (NS), SDN (Software-Defined Networking), MEC (Multi-access Edge Computing), NFV (Network Function Virtualization), mmWave communications, massive MIMO, Device-to-Device (D2D) connectivity, etc. Evidently, IoT is going to be one of the prominent use cases of 5G which would make use of mMTC and URLLC types of services.

### B. IoT

Undoubtedly, IoT is transmogrifying the way physical objects are connected; from proprietary way of locally-connected devices to standardised way of globally connected objects. IoT has fueled the intercommunication of massive number of heterogeneous and resource-constrained physical objects at Internet scale. With IoT, connectivity is feasible among anyone and anything using any network for any available service irrespective of time and place. IoT involves (tele) sensing, monitoring, and exchange of data using M2M and/or M2H communication, followed by efficient data storing and processing (using technologies like Cloud Computing, MEC[12] along with Artificial Intelligence (AI) and Big Data analytics), and finally making decisions and effectuating actions leading to higher degree of automation.

Two broad categories, widely talked about IoT are massive IoT and mission critical IoT. The former, needs more consideration primarily on scalability, while, the later has stringent demands in terms of ultra low latency and very high reliability [13]. Smart city, smart agriculture, smart home, gaming, etc. are some of the examples of massive IoT, whereas, Industrial IoT (IIoT), remote surgery, IoT enabled autonomous vehicles, tactile internet, etc. are the examples of mission critical IoT[14].

### C. Blockchain

Blockchain, a distributed ledger technology enables users to interact and transact (store and retrieve data) with ensured data authenticity, immutability, and non-repudiation. The distributed nature of Blockchain allows the industrial entities and various 5G/IoT devices to exchange data, to and from their peers, eliminating the centralized operational requirement. The Blockchain-assisted 5G ecosystem is capable of establishing accountability, data provenance, and non-repudiation for every user. The first block in a blockchain is referred to as the genesis block, which does not contain any transaction. Each block thereafter contains a number of validated transactions and is cryptographically linked with previous block. Figure 1 projects the role of blockchain and related contexts in 5G. Figure 1 project the real world use cases in 5G in different application domains.

## III. General Challenges of 5G IoT

### A. Scalability

Both 5G and IoT rely on some cloud-based architecture for their control and management. More specifically, a centralised cloud infrastructure processes the data generated by the network nodes (or sensors) and sends control signals back to the network nodes to implement some action like fault management, resource (re)allocation, traffic engineering, routing, etc. However, with the increasing number of these devices and the enormous amount of data they are generating it would be an impending task for the centralised cloud servers to scale up their capacity and computing power. Furthermore, both for the IoT and 5G scenarios, the devices connect to the cloud through a gateway (or an edge) node and series of

networks termed as fronthaul, midhaul, and backhaul. With the number of devices trying to connect to the cloud, often the links in the fronthaul, midhaul, and backhaul networks immediately adjacent to gateway nodes become congested.

### *B. Lack of Auditability and Control over data sharing/usage*

In an IoT network a huge amount of data is generated from devices that are proprietary to several enterprises. Most of the times such data is therefore not under the control of all the intermediate parties involved. Here the intermediate parties refer to all equipment vendors whose hardware form a network node, or all service providers who share a common physical network infrastructure or all users who share a common cloud platform. Thus, it is difficult to manage and audit such data in terms of who owns them, where from they are generated and how they can be processed.

### *C. Data Silos*

As discussed in the previous subsection, the data generated in the networks have different ownership and are highly non-coherent, hence, hard to trace and audit. Sometimes, there are no common standards and protocols defined for these data to be exchanged between different devices owned by different entities. Moreover, because of trust issues, even within the different units of an enterprise, data could either be locked in or may not be inter-operated because of different communication standards and protocols. Sometimes similar types of data, for example, let us say, weather and climatic data, collected by different organisations are also not shared or inter-processed to come up with an unified decision.

### *D. Security and privacy*

In both 5G and IoT domains, the end-devices are usually handheld lightweight devices with low power and form factor. For some IoT application scenarios, the devices are extremely resource-constrained and are powered by tiny batteries. Because of this, sometimes security of these devices are at serious risk [15]. These devices have low to nil security features embedded into them. Furthermore, because of fierce competition of deployment, both equipment vendors and network service providers compromise the security aspect. Therefore, home sensors, ambient-assisted-living sensors, healthcare monitors, and any other devices that contain location information can easily be compromised and sensitive users' data can go to malicious third parties. Furthermore, when the data generated by millions of devices send their data to the cloud for storage and processing, the 'locality of information' gets lost and there is always a chance of that information getting compromised from shared cloud servers.

### *E. Heterogeneity in device resources*

In a 5G/IoT context, depending on the application and the segment of the network, the nodes can have variable computational powers with some nodes having a few watts of power driven by a battery and a few megabytes of memory. This is a problem because some devices may prove to be a bottleneck in terms of its operating lifetime. For example, a sensor network might be totally out of function if one node near the gateway is deprived of resources to process huge data or is out of battery.

### *F. Complex interactions of different OS/software stacks/hardware*

The devices in an 5G/IoT network are part of different technology standards with different air interfaces, with different signalling schemes, different PHY and MAC layer protocols, data rates, modulation and coding schemes etc. They also run on different operating systems. With these plethora of protocols and standards coexisting, it is been difficult to define a common communication standard between all the devices. It is also difficult to build a system and program it that consists of a variety of devices with different communication protocols and OS. Sometimes, this aspect limits the application scenarios for devices and also limits the range of device types to be used for a particular use case.

## IV. What Blockchain can bring to IoT

### *A. Trust Building*

The establishment of trust is one of the most significant requirements in most of the industries. The stakeholders including the hosts and consumers of a particular service such as electronic financial ecosystem or healthcare management system require trust in different dimensions. The criteria of the trust is defined as regulatory enforcement and globally shared in most of the industries. For instance, Payment Card Industry-Data Security Standards (PCI-DSS) in finance context, Health Information Portability and Accountability Act (HIPAA) in medical context, and General Data Protection Regulation (GDPR) in personal data context, are the examples of the regulations for the establishment of trust. The smart contracts are identifiable as the trust representatives of the regulatory definitions in action. The smart contracts can be defined as software codes enforcing the regulatory criteria and make them transparently available.The smart contracts entirely depend on transparency and consistent integrity of all member nodes. The consistency is an indispensable fact for the sake of the trust establishment within the network. Through transparency of smart contracts, the trust is decentralized without being a "Black Box" in operations. In context of IoT, the deployment of smart contracts makes the nodes trustworthy and compliant in the specific business ecosystem. Kuo et. al [16] explained the benefits of the usage of blockchain-based smart contracts in the healthcare domain. Dagher et al. [17] and Yue et al. [18] explained the application of blockchain for the access control of healthcare data. Yu et al. [19] described the establishment of trust in the IoT ecosystem using the blockchain. Bahga and Madisetti [20] presented a blockchain-based platform for the Industrial Internet of Things (IIoT) to be utilized for manufacturing.

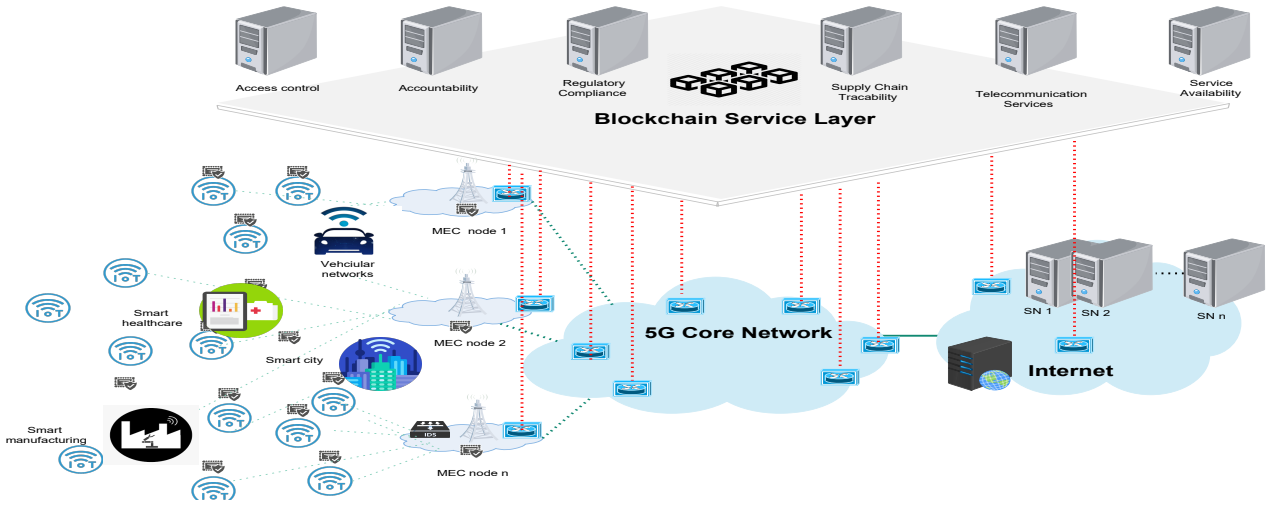


Fig. 2. Blockchain service capabilities in 5G IoT context

### B. Accelerated Data Change

The accelerated data change with higher throughput and minimal latency is an indispensable requirement of the emerging IoT ecosystems. The performance of the entire system depends on the accelerated operation of data change in the IoT nodes. The distributed nature of blockchain and smart contracts transform the data change landscape towards decentralization by elevating the performance features. For instance, the centralized validation of a particular data can be replaced by decentralized validation with the used of smart contracts deployed on the IoT node itself or near the IoT nodes such as the edge or the fog-computing nodes which act as blockchain network tenants. Thus, the request-response round trip lead time corresponding to data validation, manipulation or access can be drastically diminished using blockchain. Manzooe et al. [21] proposed a blockchain platform which supports automated IoT data exchange. Androulaki et al. [22] presented the performance elevation capability up to 3500 transactions per second with lower latency in Hyperledger Fabric along with multiple techniques.

### C. Lower Costs

The operational costs of an IoT ecosystem can be minimized in multiple aspects when the Blockchain and smart contracts are utilized. The decentralized operation of smart contracts and the ledger eliminate the requirement of deploying expensive high-end computing infrastructure such as multi-core cloud computing nodes for concurrent transaction processing. Furthermore, the centralized data storage can be eliminated by the utilization of the distributed ledger instead of centralized databases. The data transmission overheads for the request round trips to the centralized nodes such as cloud instances in the centralized systems can be eliminated in the Blockchain-based smart contracts associated ecosystems. The efficient data usage is a vital requirement in any IoT-based system including the solutions connected to 5G. However, the IoT system incurs some data overhead for the synchronization between the nodes. Ibba et al. [23] illustrated the applicability of Blockchain in the smart city scenario and discussed the cost saving capabilities of such applications. Clauson et al. [24] explained a few use cases of Blockchain highlighting the cost-cutting benefits.

### D. Improved Security

Confidentiality, Integrity, and Availability are the principal model of information security which is also known as the CIA triad. Keeping the confidentiality aside, the integrity and availability are the key features in the Blockchain-based smart contracts by design. The Blockchain-based smart contracts ensure the integrity by applying hashing and extending to the digital signatures to the individual transaction and maintaining the chain of trust entirely within the Blockchain. Furthermore, the Blockchain technology utilizes cryptographic techniques such as Merkle trees to ensure the consistent integrity over the network. Yu et al. [25] investigated the typical security and privacy issues in the IoT context and also elaborated by devloping a framework for the integration of Blockchain and IoT for the assurance of various functionalities including authentication and scalability. Khan et. al [26] explains the significant security issues in the IoT and how the Blockchain can address these issues. The availability is ensured by the distributed operational nature of the Blockchain network. For instance, Denial-of-Service attacks (DoS) attackers who attempt to conquer the Blockchain network have to overcome computationally difficult hurdles such as hijacking 51 percent of the mining power of the network and so on.

The privacy is an optional feature for the Blockchain-based smart contracts. The smart contracts highly focused on the transparency of the ledger. However, there are different privacy enforcement mechanisms that exist in the smart contract applications. For IoT, the smart contracts have versatile applicability to the privacy enforcement mechanisms such as efficient dynamic key exchanges and so on. Rodrigues et al. [27] proposed a design to mitigate Distributed-Denial-of-

Service (DDoS) attacks applying Blockchain technology and smart contracts. Ouddah et al. [28] explained FairAccess, and Pinno et al.[29] presented access control applications for IoT using Blockchain. Dorri et al. [30] explained the elimination of DDOS attacks and linking attacks using Blockchain on the smart home IoT use case. Rahulamathavan [31] proposed a privacy-preserving Blockchain architecture utilizing attribute-based encryption techniques.

Blockchain's strong protection against data tampering helps prevent a rogue device from disrupting synergy of communication systems involving home, factory or transportation system by injecting or relaying pernicious information. Thus, the Blockchain technology holds the potential to securely unlock the business and operational values of 5G networks to support common tasks, such as sensing, processing, storing, and communicating information. Ayoade et al. [32] proposed a way to utilze the Blockchain to access control the IoT data and store the raw encrypted data in Intel SGX secure enclaves. Dwivedi et al. [33] proposed a novel framework to enable features such as access control and enforce privacy for the IoT devices and medical data in the healthcare context. Kravitz and Cooper[34] explained the use of Blockchain technology for the identity management in IoT. Minoli and Occhiogrosso [35] presented a broad explanation of Blockchain in different contexts including the enforcement of IoT security. Ramani et al. [36] proposed a secured and efficient data accessibility mechanism for healthcare data.

### *E. Ensure the Accountability*

Accountability is one of the key strengths of Blockchain-based smart contracts. The distributed ledger provides capability to transparent record keeping of the events logged and the ledger is protected against alterations with the utilization of digital signatures. Some Blockchain platforms consider faster retrieval of the event log as a major requirement and optimize the retrieval operations further to ensure the compatibility of IoT ecosystems. The ledger is accessible with reduced overheads from either the IoT node itself or the edge-computing node which also acts as the Blockchain node with minor overheads. However, the accountability, guaranteed integrity, and the local invocation of the ledger elevates the value of Blockchain rather than the ordinary database systems in the IoT domain. Li et al. [37] explained the applicability of Blockchain for the IoT data storage and accountability. Liang et al. [38] explained the application of public Blockchain with a cloud server to ensure the data integrity of drone systems. Boudguiga et al. [39] investigated the utilization of Blockchain for the enforcement of the security services including accountability.

### *F. Immutability*

The immutability is regarded as a principal strength of the Blockchain-based smart contracts. The distributed ledger as well as the smart contracts are computationally infeasible to alter according to the Blockchain design principles. For an intruder or a group of intruders, it requires to vanquish more than 51 percent of the computing power to manipulate the ledger, transactions or blocks. The 51 percent taking over the block generation power is either computationally or financially harder depending on the Blockchain network. (Some Blockchain platforms such as Ethereum charge for the computational power consumed). This attack is called as 51-percent attack or majority attack in the Blockchain terminology. In the IoT perspective, the risk level is comparably low for the majority attacks due to the computational power limitations of the IoT infrastructure.

### *G. A More Efficient Supply Chain*

The contribution of the Blockchain-based smart contracts to the supply chain data provenance is important in the IoT context. Brody [40] projects some high-level insights of the application of Blockchain and its revolutionary impact to the supply chain industry while Petersen et al. [41] illustrates a comprehensive review on the opportunistic scope of the Blockchain in the supply chain and logistics context. Kshetri [42] explained the applicability of Blockchain to achieve the supply chain management objectives such as reduced cost, improved quality, and risk reduction. Saberi et al. [43] critically examined the Blockchain and smart contracts with the potential in the supply chain management. The distributed ledger can be utilized as the transparent record which indicates the significant milestones in delivery chain of a particular commodity. The more concrete examples are supply chain of frozen foods, special commodities such as gemstones, and aircraft components. The main value of the integration of Blockchain for the supply chain is that the end consumer is capable of verification of the delivery of a particular commodity to ensure the compliance. For instance, in the frozen food supply chain, the IoT devices with temperature sensors are deployable to transmit the data corresponding to the temperature condition of the frozen products. The consumer is capable of retrieving the ledger upon the purchase and make sure whether the supply chain of the product is compliant with the temperature requirement. The integration of IoT for the supply chain makes the operation more efficient and transparent with improved value to the supply chain. Abeyratne and Monfared [44] proposed application of Blockchain for the manufacturing supply chain. Madhwal and and Panfilov [45] explained the applicability of Blockchain for the improved reliability of aircraft spare parts supply chain traceability.

### *H. Automation via Smart Contracts*

The Blockchain with IoT is ideal for the automation requirements in the future industry. The smart contracts execute automatically when the conditions have reached to the executable state without intervention of any other party. The Blockchain and smart contracts deployed in the IoT devices are capable of executing the smart contracts and log the events in the distributed ledger. For instance, the temperature adjustments of the perishable cargo can be executed through the smart contracts based on the external temperature. Furthermore, the location-based customs duty calculation is operable through

the smart contracts. Griggs et al. [46] proposed a system which utilizes private Ethereum Blockchain and master-slave modeled medical device deployment model to operate IoT powered medicine actuators accurately. Gallo et al. [47] introduced BlockSee, which is a Blockchain-based video surveillance system to validate and ensure the immutability of camera settings as well as the surveillance videos in the smart cities.

### *I. Decentralization*

The decentralized operation is a core feature of Blockchain. The Blockchain operates with the decentralized transaction validation and approval mechanism. Furthermore, the transaction ledger is decentralized and each node contains a copy of the ledger. In contrast with the centralized storage and validation systems, the intruders require more effort to take over the control of decentralized validation systems and the decentralized ledger. The blocks of transactions are cryptographically linked and it is hard to alter them due to the decentralization. Huang et al. [48] proposed a decentralized solution for trusted data exchange using Blockchain for IoT and evaluated a prototype using the Ethereum Blockchain platform. The IoT ecosystems can ensure the service availability by utilizing the decentralized Blockchain systems.

## V. Challenges in Blockchain and IoT Integration

### *A. Storage capacity and scalability*

The consistent storage of transactions and blocks is a primary requirement of the Blockchain technology. Theoretically, each node must contain a copy of the ledger which is growing with the transactions. From a scalability perspective, the impact on storage for the IoT ecosystem will affect the functionality of the entire system. Especially, the evolving transactions with scaling up the system requires significant storage.

### *B. Processing Power and Time*

There are a few computational-resource-intensive operations on the Blockchain ecosystem. These operations include transaction verification and block generation, which include few cryptographic operations. Due to the resource restricted nature of IoT, there are certain limitations in computation which will lead security risks. Therefore, application of the less resource intensive alternatives require to be applied specifically when the Blockchain is applied in IoT context. The Elliptic Curve Cryptography (ECC) related technologies are one of the significant alternatives, which incurs less computational overheads to the resource restricted IoT hardware. The cryptographic operations in the restricted hardware will occur performance limitations when scaling up the system.

### *C. Security*

The integrity, availability, and access control are the primary security concerns in any system. However, the Blockchain enforces integrity and availability inherently by design. Each transaction is verified with the digital signature and the blocks of transactions linked with verifying digital signatures. The transaction verification is a resource intensive operation due to the limitations of IoT computing infrastructure. The transaction verification and block generation will have scalability limitations in cryptographic operations on Blockchain implementation. Kumar and Mallick [49] described the security and privacy issues in IoT and whhat is the significance of Blockchain in this context. Shafagh et al. [50] introduced a primary design of a distributed, secure data-storage system developed for IoT with moderated overhead in the system. The system enforces fine-grained access control and sharing of time-series sensor data in the IoT applications. Novo et al. [51] proposed a Blockchain-based access management architecture for IoT. The proposed architecture eliminates the communication overheads and improves scalability. Sharma et al. [52] proposed a Blockchain-based distributed cloud architecture to address the issues such as high availability, real-time data delivery, resilience, and low latency. The proposed solution incorporated Software-Defined Networking (SDN), fog computing, and Blockchain to enable low-cost and low-latency access to the data in a secured manner. Yinning et al. [53] presented a delay tolerant Ethereum blockchain-based payment scheme for rural areas.

### *D. Privacy*

The massive volume of IoT devices is typical in modern deployment models. The IoT devices expose broader threat surfaces and significant limitations in privacy enforcement due to the resource-restricted hardware. Especially, when the Blockchain is considered, the data privacy is not in-built since the transactions are appended to the ledger publicly upon verification. Privacy preservation is a significant challenge with widely used encryption techniques. However, the lightweight cryptographic mechanisms developed for the resource-restricted computational infrastructure will be the ideal solution to enforce data privacy in the IoT context. Zhou et al. [54] proposed BeeKeeper, which utilizes homomorphic computation on the data without revealing any insights into the users who access data. The system was evaluated on the Ethereum Blockchain platform. Cha et al. [55] proposed Blockchain-connected gateways, which act as mediators between the IoT devices and the users.

### *E. Throughput*

Besides the scalability problem of Blockchain, the throughput is another problem that is hard to tackle. The transaction throughput and latency are under consistent challenges, and as the size of transactions increases, in general, which are the hard problems that IoT system can not handle. While theoretical analysis of a platform may provide an idea about its performance, only practical implementation can provide a real-world use analysis. We can analyze the applicability of Blockchain systems based on the target use by considering the number of transactions necessary to be served in a target time frame. In the case of IoT devices, private Blockchains may be suitable, as the number of measurements for any single device will be small. Nonetheless, as we scale to larger IoT-based

TABLE I
SUMMARY OF 5G IOT USE CASES, APPLICABILITY OF BLOCKCHAIN AND PERTINENT CHALLENGES

| Application | Description | Applicability of Blockchain | Challenges |
|---|---|---|---|
| Smart City | Smart cities are the implementation of advanced modern techniques in the urbanization to improve the quality of human life. | The Blockchain is ideal to enable the services such as payments, e-Governance, security, and surveillance of the smart cities. | The computational power requirement for mining is a significant drawback in the Blockchain for IoT in the smart cities. |
| Smart Home | The smart homes essentially need to automate the entire home environment comprising of home appliances and devices | Blockchain powered 5G IoT can fuel different use cases such as smart home monitoring, remote accessing, energy optimization, surveillance and so on. | Data privacy is a major problem. Hijacking the smart contracts require to eliminate since it will expose the smart home into vulnerability. |
| Healthcare | All sorts of medical healthcare (preventive, diagnostic, rehabilitation, etc.) demands monitoring for detecting symptoms leading to early diagnosis, logging privately medical history, sharing securely medical documents, etc. | Blockchain can enable secure and trusted medical automation systems for monitoring, treatments and healthcare data access control. | A malicious attacker can take over all mining nodes and this can be disastrous. |
| Autonomous Vehicles | Fully automated (level-5) vehicles require accurate sensing and processing with ultra low latency which is indeed aligned with the promise of 5G IoT. | Blockchain can play significant role for different use cases like secure and personalized ambient in electric vehicles, automated toll calculation, and other services. | The security and access control mechanisms require to eliminate session hijacks and requires to ensure data privacy of individual users. |
| AR/VR | The interactivity, the experience of immersiveness and practical application of AR/VR can be enhanced several folds with the combined visions of 5G and IoT. | Integration of blockchain and AR/VR can revolutionize business processes and enhance gaming and entertainment activities. | The interoperability of Blockchain and the existing VR IoT applications is a significant requirement. |
| Industrial IoT | IIoT can revolutionize the way industrial manufacturing, supervision, resource management, etc. are carried out. | Plethora of applications pertaining to industrial 5G IoT, including smart manufacturing, automated maintenance, warehousing, etc., can be made secure with blockchain. | The scalability, data privacy, and data storage overheads are significant challenges in the industrial 5G IoT context. |
| Smart Agriculture | To increase the agricultural productivity while minimizing the cost need continuous ambient parameter acquisition, smart aggregation, and processing of large volume of date is required. | Leveraging blockchain for smart agriculture enables the lifecycle transparency, autonomous management, and establish regulatory requirements of agri foods. | The data integrity is highly important aspect of the agri foods which requires a special attention on the ledger. |
| UAV | On the one hand, UAVs can create wide range of applications leveraging 5G IoT and on the other hand, from infrastructure viewpoint UAVs can assist expansion of 5G | Keeping in mind the applications of UAVs such as surveillance, imaging, environmental analysis, etc the use of blockchain can be key enabler. | The operational overheads of Blockchain may affect the airtime of UAVs. The communication issues may cause physical damages to the devices. |

smart-world systems serving massively distributed devices, or big data systems that act on an unprecedented number of data items, the ability to apply Blockchain becomes more difficult. Gorenflo et al. [56] identified the performance bottlenecks in the consensus mechanisms and proposed architectural changes which reduces computational and other overheads to improve the throughput up to 20,000 transactions per second. In [57] some interesting new architecture and analytical studies are proposed to enhance the throughput and transaction latency of the Bitcoin Blockchain, however significant research still needs to be done to migrate that concept to the IoT/5G domains.

## VI. CONCLUSION

With the evident popularity of IoT and the soon roll out of 5G technology, the paper brings to the lime light the challenges (some evident and some hidden) which will arise with the integration of the two. In the midst of other possible solutions, the paper expounds the use of Blockchain to mitigate many of those issues in the realm of 5G IoT. Table 1 summarized the 5G IoT use cases with the applicability in blockchain. In particular, we emphasized on the opportunities and challenges that exist (and will show up in near future) with the use of Blockchain for the popular 5G-enabled-IoT uses case.

## ACKNOWLEDGEMENT

This work is party supported by European Union in RESPONSE 5G (Grant No: 789658), Academy of Finland in 6Genesis Flagship (grant no. 318927) and Secure Connect projects.

## REFERENCES

[1] P. Porambage, J. Okwuibe, M. Liyanage, M. Ylianttila, and T. Taleb, "Survey on Multi-access Edge Computing for Internet of Things Realization," *IEEE Communications Surveys & Tutorials*, vol. 20, no. 4, pp. 2961–2991, 2018.

[2] "ETSI," Accessed: 24.11.2019, uRL: https://www.etsi.org/technologies/internet-of-things.

[3] M. Liyanage, I. Ahmad, A. B. Abro, A. Gurtov, and M. Ylianttila, *A Comprehensive Guide to 5G Security*. John Wiley & Sons, 2018.

[4] W. Al-Saqaf and N. Seidler, "Blockchain Technology for Social Impact: Opportunities and Challenges Ahead," *Journal of Cyber Policy*, vol. 2, no. 3, pp. 338–354, 2017.

[5] M. T. Hammi, B. Hammi, P. Bellot, and A. Serhrouchni, "Bubbles of Trust: A Decentralized Blockchain-based Authentication System for IoT," *Computers & Security*, vol. 78, pp. 126–142, 2018.

[6] I. Mistry, S. Tanwar, S. Tyagi, and N. Kumar, "Blockchain for 5G-enabled IoT for Industrial Automation: A Systematic Review, Solutions, and Challenges," *Mechanical Systems and Signal Processing*, vol. 135, p. 106382, 2020.

[7] "MARKET PULSE REPORT, INTERNET OF THINGS (IoT)," Accessed: 30.11.2019, uRL: https://growthenabler.com/flipbook/pdf/IOT%20Report.pdf.

[8] P. Daugherty and B. Berthon, "Winning with the Industrial Internet of Things: How to Accelerate the Journey to Productivity and Growth," *Dublín: Accenture*, 2015.

[9] "Ericsson 5G report: Industry Digitalization Could be a USD 700 Billion Market by 2030," Accessed: 4.12.2019, uRL: https://www.ericsson.com/en/news/2019/10/ericsson-5g-for-business-a-2030-market-compass.

[10] "Gartner The CIO's Guide to Blockchain," Accessed: 30.11.2019, uRL: https://www.gartner.com/smarterwithgartner/the-cios-guide-to-blockchain/.

[11] P. Popovski, K. F. Trillingsgaard, O. Simeone, and G. Durisi, "5G Wireless Network Slicing for eMBB, URLLC, and mMTC: A communication-theoretic View," *IEEE Access*, vol. 6, pp. 55 765–55 779, 2018.

[12] P. Ranaweera, A. D. Jurcut, and M. Liyanage, "Realizing Multi-Access Edge Computing Feasibility: Security Perspective," in *2019 IEEE Conference on Standards for Communications and Networking (CSCN)*. IEEE, 2019, pp. 1–7.

[13] G. mobile Suppliers Association *et al.*, "The Road to 5G: Drivers, applications, requirements and Technical Development," *Global Mobile Suppliers Association*, 2015.

[14] H. Malik, A. Manzoor, M. Ylianttila, and M. Liyanage, "Performance Analysis of Blockchain based Smart Grids with Ethereum and Hyperledger Implementations," in *IEEE International Conference on Advanced Networks and Telecommunications Systems 2019*. IEEE, 2019, pp. 1–5.

[15] M. Liyanage, A. Braeken, P. Kumar, and M. Ylianttila, *IoT Security: Advances in Authentication*. John Wiley & Sons, 2020.

[16] T.-T. Kuo, H.-E. Kim, and L. Ohno-Machado, "Blockchain Distributed Ledger Technologies for Biomedical and Health Care Applications,"

*Journal of the American Medical Informatics Association*, vol. 24, no. 6, pp. 1211–1220, 2017.

[17] G. G. Dagher, J. Mohler, M. Milojkovic, and P. B. Marella, "Ancile: Privacy-preserving Framework for Access Control and Interoperability of Electronic Health Records using Blockchain Technology," *Sustainable cities and society*, vol. 39, pp. 283–297, 2018.

[18] X. Yue, H. Wang, D. Jin, M. Li, and W. Jiang, "Healthcare Data Gateways: Found Healthcare Intelligence on Blockchain with Novel Privacy Risk Control," *Journal of medical systems*, vol. 40, no. 10, p. 218, 2016.

[19] B. Yu, J. Wright, S. Nepal, L. Zhu, J. Liu, and R. Ranjan, "IoTChain: Establishing Trust in the Internet of Things Ecosystem using Blockchain," *IEEE Cloud Computing*, vol. 5, no. 4, pp. 12–23, 2018.

[20] A. Bahga and V. K. Madisetti, "Blockchain Platform for Industrial Internet of Things," *Journal of Software Engineering and Applications*, vol. 9, no. 10, p. 533, 2016.

[21] A. Manzoor, M. Liyanage, A. Braeke, S. S. Kanhere, and M. Ylianttila, "Blockchain based Proxy Re-encryption Scheme for Secure IoT Data Sharing," in *2019 IEEE International Conference on Blockchain and Cryptocurrency (ICBC)*. IEEE, 2019, pp. 99–103.

[22] E. Androulaki, A. Barger, V. Bortnikov, C. Cachin, K. Christidis, A. De Caro, D. Enyeart, C. Ferris, G. Laventman, Y. Manevich *et al.*, "Hyperledger Fabric: A Distributed Operating System for Permissioned Blockchains," in *Proceedings of the Thirteenth EuroSys Conference*. ACM, 2018, p. 30.

[23] S. Ibba, A. Pinna, M. Seu, and F. E. Pani, "CitySense: Blockchain-oriented Smart Cities," in *Proceedings of the XP2017 Scientific Workshops*. ACM, 2017, p. 12.

[24] K. A. Clauson, E. A. Breeden, C. Davidson, and T. K. Mackey, "Leveraging Blockchain Technology to Enhance Supply Chain Management in Healthcare," *Blockchain in Healthcare Today*, 2018.

[25] Y. Yu, Y. Li, J. Tian, and J. Liu, "Blockchain-based Solutions to Security and Privacy Issues in the Internet of Things," *IEEE Wireless Communications*, vol. 25, no. 6, pp. 12–18, 2018.

[26] M. A. Khan and K. Salah, "IoT Security: Review, blockchain solutions, and Open Challenges," *Future Generation Computer Systems*, vol. 82, pp. 395–411, 2018.

[27] B. Rodrigues, T. Bocek, A. Lareida, D. Hausheer, S. Rafati, and B. Stiller, "A blockchain-based Architecture for Collaborative DDoS Mitigation with Smart Contracts," in *IFIP International Conference on Autonomous Infrastructure, Management and Security*. Springer, Cham, 2017, pp. 16–29.

[28] A. Ouaddah, A. Abou Elkalam, and A. Ait Ouahman, "FairAccess: A New Blockchain-based Access Control Framework for the Internet of Things," *Security and Communication Networks*, vol. 9, no. 18, pp. 5943–5964, 2016.

[29] O. J. A. Pinno, A. R. A. Gregio, and L. C. E. De Bona, "ControlChain: Blockchain as a Central Enabler for Access Control Authorizations in the IoT," in *GLOBECOM 2017 - 2017 IEEE Global Communications Conference*, Dec 2017, pp. 1–6.

[30] A. Dorri, S. S. Kanhere, R. Jurdak, and P. Gauravaram, "Blockchain for IoT Security and Privacy: The Case Study of a Smart Home," in *2017 IEEE international conference on pervasive computing and communications workshops (PerCom workshops)*. IEEE, 2017, pp. 618–623.

[31] Y. Rahulamathavan, R. C.-W. Phan, M. Rajarajan, S. Misra, and A. Kondoz, "Privacy-preserving Blockchain based IoT Ecosystem Using Attribute-based Encryption," in *2017 IEEE International Conference on Advanced Networks and Telecommunications Systems (ANTS)*. IEEE, 2017, pp. 1–6.

[32] G. Ayoade, V. Karande, L. Khan, and K. Hamlen, "Decentralized IoT data Management using Blockchain and Trusted Execution Environment," in *2018 IEEE International Conference on Information Reuse and Integration (IRI)*. IEEE, 2018, pp. 15–22.

[33] A. D. Dwivedi, G. Srivastava, S. Dhar, and R. Singh, "A Decentralized Privacy-preserving Healthcare Blockchain for IoT," *Sensors*, vol. 19, no. 2, p. 326, 2019.

[34] D. W. Kravitz and J. Cooper, "Securing User Identity and Transactions Symbiotically: IoT Meets Blockchain," in *2017 Global Internet of Things Summit (GIoTS)*. IEEE, 2017, pp. 1–6.

[35] D. Minoli and B. Occhiogrosso, "Blockchain Mechanisms for IoT Security," *Internet of Things*, vol. 1, pp. 1–13, 2018.

[36] V. Ramani, T. Kumar, A. Bracken, M. Liyanage, and M. Ylianttila, "Secure and Efficient Data Accessibility in Blockchain based Healthcare Systems," in *2018 IEEE Global Communications Conference (GLOBECOM)*. IEEE, 2018, pp. 206–212.

[37] R. Li, T. Song, B. Mei, H. Li, X. Cheng, and L. Sun, "Blockchain for Large-Scale Internet of Things Data Storage and Protection," *IEEE Transactions on Services Computing*, vol. 12, no. 5, pp. 762–771, Sep. 2019.

[38] X. Liang, J. Zhao, S. Shetty, and D. Li, "Towards Data Assurance and Resilience in IoT using Blockchain," in *MILCOM 2017-2017 IEEE Military Communications Conference (MILCOM)*. IEEE, 2017, pp. 261–266.

[39] A. Boudguiga, N. Bouzerna, L. Granboulan, A. Olivereau, F. Quesnel, A. Roger, and R. Sirdey, "Towards Better Availability and Accountability for IoT Updates by Means of a Blockchain," in *2017 IEEE European Symposium on Security and Privacy Workshops (EuroS&PW)*. IEEE, 2017, pp. 50–58.

[40] P. Brody, "How Blockchain is Revolutionizing Supply Chain Management," *Digitalist Magazine*, pp. 1–7, 2017.

[41] M. Petersen, N. Hackius, and B. von See, "Mapping the Sea of Opportunities: Blockchain in Supply Chain and Logistics," *it-Information Technology*, vol. 60, no. 5-6, pp. 263–271, 2018.

[42] N. Kshetri, "1 Blockchain's Roles in Meeting Key Supply Chain Management Objectives," *International Journal of Information Management*, vol. 39, pp. 80–89, 2018.

[43] S. Saberi, M. Kouhizadeh, J. Sarkis, and L. Shen, "Blockchain Technology and its Relationships to Sustainable Supply Chain Management," *International Journal of Production Research*, vol. 57, no. 7, pp. 2117–2135, 2019.

[44] S. A. Abeyratne and R. P. Monfared, "Blockchain Ready Manufacturing Supply Chain using Distributed Ledger," 2016.

[45] Y. Madhwal and P. B. Panfilov, "Industrial Case: Blockchain on Aircraft's Parts Supply Chain Management," in *American Conference on Information Systems 2017 Workshop on Smart Manufacturing Proceedings*, vol. 6, 2017.

[46] K. N. Griggs, O. Ossipova, C. P. Kohlios, A. N. Baccarini, E. A. Howson, and T. Hayajneh, "Healthcare Blockchain System using Smart Contracts for Secure Automated Remote Patient Monitoring," *Journal of medical systems*, vol. 42, no. 7, p. 130, 2018.

[47] P. Gallo, S. Pongnumkul, and U. Q. Nguyen, "BlockSee: Blockchain for IoT Video Surveillance in Smart Cities," in *2018 IEEE International Conference on Environment and Electrical Engineering and 2018 IEEE Industrial and Commercial Power Systems Europe (EEEIC/I&CPS Europe)*. IEEE, 2018, pp. 1–6.

[48] Z. Huang, X. Su, Y. Zhang, C. Shi, H. Zhang, and L. Xie, "A Decentralized Solution for IoT Data Trusted Exchange based-on Blockchain," in *2017 3rd IEEE International Conference on Computer and Communications (ICCC)*. IEEE, 2017, pp. 1180–1184.

[49] N. M. Kumar and P. K. Mallick, "Blockchain Technology for Security Issues and Challenges in IoT," *Procedia Computer Science*, vol. 132, pp. 1815–1823, 2018.

[50] H. Shafagh, L. Burkhalter, A. Hithnawi, and S. Duquennoy, "Towards Blockchain-based Auditable Storage and Sharing of IoT Data," in *Proceedings of the 2017 on Cloud Computing Security Workshop*. ACM, 2017, pp. 45–50.

[51] 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.

[52] P. K. Sharma, M.-Y. Chen, and J. H. Park, "A Software Defined Fog Node based Distributed Blockchain Cloud Architecture for IoT," *IEEE Access*, vol. 6, pp. 115–124, 2017.

[53] Y. Hu, A. Manzoor, P. Ekparinya, M. Liyanage, K. Thilakarathna, G. Jourjon, and A. Seneviratne, "A Delay-tolerant Payment Scheme based on the Ethereum Blockchain," *IEEE Access*, vol. 7, pp. 33 159–33 172, 2019.

[54] L. Zhou, L. Wang, Y. Sun, and P. Lv, "Beekeeper: A Blockchain-based IoT System with Secure Storage and Homomorphic Computation," *IEEE Access*, vol. 6, pp. 43 472–43 488, 2018.

[55] "Privacy-aware and blockchain connected gateways for users to access legacy iot devices."

[56] C. Gorenflo, S. Lee, L. Golab, and S. Keshav, "Fastfabric: Scaling hyperledger fabric to 20,000 transactions per second," *arXiv preprint arXiv:1901.00910*, 2019.

[57] L. Yang, V. Bagaria, G. Wang, M. Alizadeh, D. Tse, G. Fanti, and P. Viswanath, "Prism: Scaling Bitcoin by 10,000x," 2019.