



A survey on blockchain-based platforms for IoT use-cases

MOHAMMAD JABED MORSHED CHOWDHURY¹, MD SADEK FERDOUS^{2,3} ,
KAMANASHIS BISWAS⁴ , NIAZ CHOWDHURY⁵ and VALLIPURAM
MUTHUKKUMARASAMY⁶

¹*La Trobe University, VIC, Australia*
e-mail: m.chowdhury@latrobe.edu.au

²*Shahjalal University of Science and Technology, Sylhet, Bangladesh*
e-mail: sadek-cse@sust.edu

³*Imperial College London, London, UK*
e-mail: s.ferdous@imperial.ac.uk

⁴*Australian Catholic University, NSW, Australia*
e-mail: kamanashis.biswas@acu.edu.au

⁵*Open University, Milton Keynes, UK*
e-mail: niaz.chowdhury@open.ac.uk

⁶*Griffith University, QLD, Australia*
e-mail: v.muthu@griffith.edu.au

Abstract

The Internet of Things (IoT) has recently emerged as an innovative technology capable of empowering various areas such as healthcare, agriculture, smart cities, smart homes and supply chain with real-time and state-of-the-art sensing capabilities. Due to the underlying potential of this technology, it already saw exponential growth in a wide variety of use-cases in multiple application domains. As researchers around the globe continue to investigate its aptitudes, a collective agreement is that to get the best out of this technology and to harness its full potential, IoT needs to sit upon a flexible network architecture with strong support for security, privacy and trust. On the other hand, blockchain (BC) technology has recently come into prominence as a breakthrough technology with the potential to deliver some valuable properties such as resiliency, support for integrity, anonymity, decentralization and autonomous control. Several BC platforms are proposed that may be suitable for different use-cases, including IoT applications. In such, the possibility to integrate the IoT and BC technology is seen as a potential solution to address some crucial issues. However, to achieve this, there must be a clear understanding of the requirements of different IoT applications and the suitability of a BC platform for a particular application satisfying its underlying requirements. This paper aims to achieve this goal by describing an evaluation framework which can be utilized to select a suitable BC platform for a given IoT application.

1 Introduction

The Internet of Things (IoT) has gained massive acclaim in recent time. It is no exaggeration that this technology has become a part of modern society where people, knowingly or unknowingly, regularly use it in their day-to-day activities. In IoT, physical objects such as home appliances, vehicles, logistic items and infrastructure components can sense the environment around them and adaptively interact with each other in real time. Smart objects in IoT systems are usually heterogeneous and work under an administrative domain that is unique in nature; hence, establishing trust and maintaining security in the realm of IoT is often regarded as a challenging chore (Liu *et al.*, 2012). IoT devices depend on a variety of underlying network infrastructure which is vulnerable to attacks as evident in several recent cyberattacks

(Biggs, 2016; IoT Attacks, 2018). Furthermore, security and privacy of the data in IoT networks is also a significant concern.

Recently, Blockchain (BC) technology has come into prominence and gained popularity across a wide range of industries. Due to its capabilities to bring into play properties such as resiliency, support for integrity, anonymity, decentralization and autonomous control, this technology is viewed as a game changer by many experts and researchers around the globe have been trying to explore its strengths and weaknesses for various domains.

Although cryptocurrency is the most widely used application of BC technology, the number of other useful applications beyond token-values is emerging. Over the past few years, the utilization of BC has expanded steadily, ranging from domains like identity management, governance, IoT networks, financial services to healthcare. Among these applications, the juxtapositions of BC and IoT networks hold enormous potentials in the area of IoT device identification, authentication, sensor data storage and secure data transfer. The possibility of this convergence has driven the enthusiasm among the researchers, academia and industry practitioners to disrupt several IoT applications as well as to address issues prevailing in IoT systems mentioned earlier.

In order to accomplish this goal, several BC platforms for IoT systems have come into existence in recent time. This includes IOTA (2018), Waltonchain (2019) and OriginTrail (2018), with the focus on different IoT application domains. Similarly, some researchers are exploring the applicability of BC platforms for different IoT applications such as supply chain, healthcare, smart city, smart home, financial services, automated smart contracts, and quality control and regulation. Understandably, this diverse set of IoT applications have different requirements. For example, requirements in smart cities are different from that of the wearable fitness tracking in healthcare or goods tracking system in supply chain management. It is often challenging to identify a suitable BC platform for a particular IoT application satisfying all its requirements. To the best of the authors' knowledge, little work has been done investigating this aspect leaving a gap in this domain for an evaluation framework which could be utilized to select an appropriate BC platform for a given IoT application considering its specific requirements. This paper addresses this issue where motivations are two-fold: (i) to formulate a comprehensive set of requirements for different categories of IoT applications and (ii) to develop an evaluation framework to verify the suitability of a given BC platform for a particular type of application according to its identified requirements.

With this urge in mind, the paper provides comprehensive coverage as to how to support IoT devices and networks using BC technology focusing on the platforms and their suitability to fit into specific IoT applications.

This paper is an extension of our previous work presented at the 2nd Symposium on Distributed Ledger Technology, 2018 (Chowdhury *et al.*, 2018) with the following additions:

- We have expanded the background section with an enlarged discussion of BC, along with its properties and advantages and BC-based IoT.
- We have identified and provided detail discussion about different IoT use-cases and their functional and non-functional requirements.
- We have analyzed different BC solutions to meet the identified requirements of IoT-based system.

All in all, with these additional contributions, the current version has been extended more than 70% from our previous work. The paper begins with a brief discussion on the background of the relevant technologies and their relationship towards integration in Section 2. The paper then concentrates on various BC-enabled IoT use-cases and their functional and non-functional requirements in Section 3 followed by a comprehensive survey on the available BC platforms in Section 4. It presents a brief discussion in Section 5 and conclusion in Section 6.

2 Background

The juxtaposition of IoT and BC opens up new opportunities that were previously either not possible or difficult to achieve individually. Nonetheless, to realize how these two disruptive technologies can work

closely to integrate applications with extended supports, understanding their background is essential. In this section, we briefly describe the characteristics of IoT (Section 2.1), BC (Section 2.2) and the convergence of IoT and BC (Section 2.3).

2.1 Internet of Things

The IoT is the network of connected objects that are discoverable using standard communication protocols. IoT encompasses everything having connectivity and ability to communicate. The ‘things’ can be anything from sensors to electronic devices, to appliances and to vehicles. The concept of IoT is motivated by the idea that objects of our world will talk to each other and hence, form a network of devices where each object might have the communication ability as well as some ‘sensing’ and ‘actuating’ capabilities.

The IoT technology can be one of three types: internet-oriented that acts as a middleware, things-oriented that provides sensing ability and semantic-oriented that enables accessing knowledge. The suitability of a specific type depends on the working principles of a particular application. A combination of multiple types or just a standalone IoT can be used to build such smart applications aiming at solving critical problems in our daily life (Atzori *et al.*, 2010).

2.2 Blockchain technology

Evolving from the Bitcoin BC, a new breed of BC platforms has emerged which facilitates the deployment and execution of computer programmes, known as smart contracts, on top of the respective BC. Such smart contracts enable the creation of so-called decentralized applications (DApps), which are autonomous programmes operating without relying on any human intervention. Being part of the BC, smart contracts and their executions become immutable and irreversible, a sought-after property having a wide-range of applications in different domains.

BC platforms generally demonstrate some common characteristics. Among, the distributed consensus is arguably one of the key features that play a huge role in the maintenance and security of its data. Immutability and irreversibility of the BC state are two other essential traits that almost all BC exhibit. Furthermore, cryptographic mechanisms guarantee data provenance of transactions that, in turn, helps BC to ensure the accountability and transparency of its data and actions. Equipped with these characteristics, BC platforms offer significant advantages over traditional systems for many application domains. Among them, in this paper, we only explore IoT-focused applications. Depending on the application domains, different BC deployment strategies can be pursued (Chowdhury, 2019).

2.3 Future of blockchain-based IoT

During the last decade, the IoT has significantly increased its reach and a large number of devices are interconnected through the Internet, enabling them to send and receive data. It has been predicted that by 2019, 20% of all IoT deployments will be BC-enabled according to the IDC report (MacGillivray *et al.*, 2016).

Today, over 5 billion IoT devices all around the world produce massive amount of geographic and demographic data and exchange them on the Internet. These data have the risk of being exploited and misused in the absence of appropriate security measures leading to compromising the confidentiality, integrity and authenticity of the contents. BC-based decentralization can play a pivotal role in this regard (Chowdhury *et al.*, 2020). Storing data on BC platforms are inherently decentralized ruling out the potential influence of centralized entities responsible for managing the conventional infrastructure such as the host of a data warehouse. The immutability trait of those platforms also removes the chances of data alteration. Data confidentiality can also be achieved by putting data on a decentralized distributed storage such as InterPlanetary File System or solid with complete users’ control and a hash of each data on the BC to verify the integrity (Ramachandran *et al.*, 2020).

Furthermore, vulnerable connected devices such as surveillance cameras can be of interests to attackers wishing to facilitate malicious activities. As such, each device in an IoT network can be a potential point of failure and can be exploited to launch various cyberattacks, including botnets and distributed denial of service attacks (Panarello *et al.*, 2018). The use of BC in managing access to data from IoT devices can potentially supplement an additional layer of security to the networks leading to overcoming the single-point-of-failure problem.

Nevertheless, due to the lack of sufficient computing and communication power, it has been a challenge for IoT devices to participate in the BC network directly. Besides, BC platforms are secured by their cryptographic mechanisms. Any human error in coupling these two emerging technologies would lead to further security vulnerabilities instead of solving the existing ones.

Despite some technological hurdles and implementation factors as stated above, the consensus among the scholarly community is the convergence of BC and IoT has opened doors of opportunities for many applications operating with areas such as supply chains, logistics, smart cities and manufacturing industries. The inherent properties of BC and the self-execution capabilities of the smart contract have fostered the potential large-scale adoption of this technology to IoT applications where the interconnected devices can interact with each other and make decisions without any human intervention.

3 Blockchain-enabled IoT use-cases

The convergence of IoT and BC technology is set to transform the traditional way of transaction for many industrial and home applications. This includes financial sector, health sector, logistics, manufacturing, energy, smart home, smart vehicles and smart cities. This section discusses four BC-enabled IoT application domains as follows.

3.1 Smart industry

According to the World Economic Forum, the fourth industrial revolution (Industry 4.0) will be driven by three disruptive technologies: BC, artificial intelligence (AI) and IoT. Among these, BC will play the mediating role by proving a new way for securing trust, transferring value and storing data. In particular, it would represent a technology capability platform to support industry applications, for example, supply chain and trade across manufacturing, food, pharmaceuticals, automobile and creative industries (Sniderman *et al.*, 2016). This section describes some use-cases, characteristics, functional and non-functional requirements of a smart industry.

Food safety. Food safety has become a key concern now-a-days as it leads to a number of issues such as spread of food-borne illness, unnecessary waste and economic burden of recalls. According to the 2016 Label Insight Food Revolution Study, 'it is important to 94% of consumers that the brands and manufacturers they purchase products from are transparent about what is in their food and how it is made' (Insight, 2016). To quickly identify food safety issues, improve product recalls and ensure end-to-end visibility, 10 of the world's biggest companies including Walmart Inc., Nestle SA and Unilever NV are developing a BC-based solution called *food trust BC*.

Drug safety. In this era of globalization, poor quality drugs pose a serious risk to public health worldwide. The report of World Health Organization (WHO) shows that at least 72 000 children die of pneumonia and 69 000 people die of malaria each year as a result of falsified or substandard medicines (World Health Organisation, 2017). BC and IoT can play a vital role in increasing drug safety by ensuring traceability and security in pharmaceutical industries. In particular, manufacturing, distribution and dispensing of perishable goods such as vaccines and chemicals can be monitored and traced through BC to detect potential fraud and failures. Mediledger (2019), LifeCrypter (Schöner *et al.*, 2017) and Vaccichain (Biswas *et al.*, 2017) are some examples of BC projects that aim to leverage the power of BC and IoTs to combat fake medicines.

3.2 Requirement analysis: smart industry

Industries have become automated and more complex in the recent years due to the growth of digital economy and technological evolution. Companies are trying to capture and store everything without properly analyzing the functional requirements, data utility and effective information management schemes. First, we identify the main characteristics of a complex industrial system that would help to determine both functional and non-functional requirements. The smart industry should possess the following capabilities:

- *Ever-ready*—It should be always operational so that sensors and other location-based tools can continuously sense and transmit data to provide integrated views of multiple facets of the network with minimal to no latency.
- *Shared platform*—All the stakeholders, suppliers, manufacturers, distributors, partners and customers, would be able to exchange and share information without any difficulties.
- *Cross-functional capability*—A smart industry should have transformative capabilities and thus would be able to combine and link cross-functional data (e.g. production, inventory and shipment) from various sources.
- *End-to-end transparency*—It should be capable of unifying information and processes to enable end-to-end transparency and more efficient collaboration.
- *Intelligent decision making*—In a smart industry, machines and human should be able to work together and share information that would help in intelligent decision making.

3.2.1 Functional requirements

On the basis of above characteristics of a smart industry, we have identified a number of functional and non-functional requirements. The functional requirements describe the basic operations and activities that define what a system supposed to do, as illustrated below.

- **Totality**—A smart industry should incorporate all internal and external activities such as manufacturing, distribution, procurement, payment and invoicing to provide a holistic view of the system.
- **Traceability**—The need for an effective product-traceability system is increasing globally as it improves product quality and reduces risks. It also helps to quickly identify, isolate and prevent defected products reaching consumers in the event of a product recall.
- **Transparency**—Transparency is considered as a critical factor in building consumer trust in a brand or product. A smart industry should be able to create an auditable chain of custody to provide its users easy access to reliable information about a product.

3.2.2 Non-functional requirements

Unlike functional requirements, non-functional requirements specify external constraints that a system must satisfy. The following are the non-functional requirements identified for a smart industry.

- **Performance**—Every smart industry should maintain certain level of performance in terms of response time, available storage or processing capacity.
- **Flexibility**—Flexibility mainly combines two basic functional operations: (i) adaptability, adaptable to the changes in business strategies, products and technologies and (ii) agility, the ability to quickly respond to short-term changes.
- **Scalability**—Scalability refers to the ability to scale in size and functionalities without deteriorating the performance of the original system.
- **Privacy and security**—One of the key challenges in smart industries is protecting privacy of shared data among multiple entities. Privacy-preserving mechanisms such as data anonymization can be used to remove identifiable personal information from the shared data sets. In addition to privacy issues,

security has become a big concern due to the increased level of complexity in industrial operations. From the perspective of basic security services, it should maintain the following requirements:

Confidentiality—Only legitimate users should have access to sensitive information such as intellectual property, contacts and business strategy.

Integrity—Integrity of exchanged information among different parties should be preserved to ensure the correctness of the system.

Availability—Availability ensures uninterrupted services to the users. All entities including physical systems should be available when and where they are needed.

3.3 Smart health

BC technology has the potential to transform traditional healthcare by placing the patient at the centre of the healthcare ecosystem and increasing the security, privacy and interoperability of health records. This technology could provide a new model for health information exchanges by making electronic medical records more efficient, disintermediated and secure. Xia *et al.* (2017) have designed a system for sharing medical data among medical big data custodians in a trustless environment. The system provides data provenance, auditing and control for shared medical data in cloud repositories among big data entities. Similarly, Nugent *et al.* (2016) have used BC to improve the transparency in clinical trials. Apart from these, BC-based system shows promising solutions for interoperability (Brodersen *et al.*, 2016; Peterson *et al.*, 2016; Zhang *et al.*, 2017), which is a major challenge for current healthcare systems. Other than sharing and interoperability, it can also be applied to specific healthcare-related applications (Angraal *et al.*, 2017; Kuo *et al.*, 2017; Dubovitskaya *et al.*, 2017).

Data sharing platform. At present, the stakeholders of healthcare systems are working as isolated entities in silos rather than as a part of an integrated system. With an integrated system, information would be available for use by legitimate third parties, hospitals, clinics, researchers, practitioners and patients as necessary. In addition to traditional information systems, IoT devices are also gaining popularity in health sectors. Therefore, integrating different IoT devices and exchanging data among them has become a big challenge. BC could be a perfect match to provide interoperability support for such high-level of heterogeneous data sources.

Claims management. Medical claims management involves billing, filing, updating and processing of medical claims related to patient diagnosis, treatments and medications. Since maintaining patient records, interacting with health insurers and issuing invoices for medical services are time consuming, many hospitals and clinics outsource those tasks to medical claims management firms. Without effective medical claims management, patients would not know what they owe and medical facilities would not receive the funds due for patient services.

Open research data. Another IoT-supported BC use-case is collecting open research data for clinical trials. The main objective of this is to improve the clinical trials. The BC initiative will help clinical personals to collaborate worldwide and do population health research.

3.4 Requirement analysis: smart health

In this section, we discuss different types of functional and non-functional requirements that are important to realize the use-cases stated above. However, it is often useful to identify the key characteristics of these applications in order to formulate different requirements. Next, we present some of those characteristics for smart health use-cases.

- *Data sharing capability*—Smart health systems must enable a common platform where the stakeholders can easily exchange data among themselves. This is very crucial for emergency situations where doctors need to access patients past records immediately.

- *Real-time monitoring and control*—Data from wearable devices are used to monitor the health condition of the patients. Therefore, availability of real-time data is very important in a smart health system. In addition, patients would have full control of their data.
- *Multi-facet data sources*—There has been a proliferation in the number of wearable and portable devices for monitoring personal health and wellness. Different companies develop their custom-made devices and use their own data formats. The smart health system must be capable of operating in a heterogenous network.
- *Payment system*—Both healthcare providers and patients are benefited from efficient payment processes. A BC-based payment system can significantly improve the payment systems in healthcare by eliminating the intermediary.
- *Identity management*—Medical data are private and sensitive. It is very important to ensure that only the legitimate entities can access the data. To achieve that we should have a proper identity management system. In addition to human being, IoT devices should also be under the identity management system to track which device is generating which data.

3.4.1 Functional requirements

The functional requirements for smart health use-cases are presented as follows:

- **Patient-centric design**—Today's healthcare systems are provider-centric instead of patient-centric, thereby preventing patients from taking control of their own health records and having knowledge of what is done to their data or who has accessed their data.
- **IoT support**—As the research will progress, new IoT devices will emerge to provide more accurate and real-time health data. Therefore, the systems need to be able to easily integrate new IoT devices.
- **Interoperability**—Patients visit different health centre for different types of services. Every organization keeps record of the individuals. However, often two different organizations cannot exchange patients' information due to the interoperability issue, like data format mismatch. Therefore, it is the most important requirement for the future healthcare system.

3.4.2 Non-functional requirements

The following are the non-functional requirements identified for a smart health system:

- **Security issues:** Security of the healthcare systems is very critical. The system should meet the following security requirements:
 - *Availability*—The patient information should always be available for treatment or other medication-related purposes. Adopting a distributed system architecture can help to reduce the risk of attacks on availability.
 - *Access control*—Authenticating the right user and providing right kind of access to the data are critical for healthcare system. Therefore, the system should have fine-grained access control mechanisms to provide access to only specific required data rather than a general access right.
- **Privacy issues:** As health data are privacy sensitive data, there are several privacy requirements as follows:
 - *Consent management*—The patients should be at the centre of decision-making process when their data will be shared among different parties. They should be able to change their consent from time to time.
 - *Anonymity*—The system should provide anonymization services to the patient data. If a patient wants to share her data anonymously, the system should support that.

3.5 Smart city

The concept of a smart city has numerous definitions depending on the context and meaning of the word *smart*. Sometimes it refers to being intelligent while occasionally it indicates the ability to generate and

exchange real-time data. In general, a smart city incorporates people, IoT devices, technology and data to provide better services and living experiences for its citizens (Cocchia, 2014). Real-time data from these devices and immutable historical data on BC are jointly going to open up vast opportunities for the researchers who would get an extra edge to look at the smart city use-cases from a new perspective called data-to-decision which ties up sensor data with AI in making real-time decisions (Miller & Mork, 2013). In the following, we discuss how an IoT-integrated BC platform can play a vital role in different smart city use-cases:

Transportation. Managing the transportation system has been a great challenge for any modern city. A BC-based and IoT-integrated transport system management could play a pivotal role in addressing this challenge. Such a system would enable continuous sensing of passengers and vehicles to facilitate many applications and services in various areas such as designing timetables for metro trains and public buses, anticipating commuters demand in different parts of the city, assigning drivers shifts, sharing rides and even managing autobiography of smart vehicles (Ferdous *et al.*, 2020).

Utility services. Power and water management has been one of the most important elements of a smart city. This includes smart grid, smart water supply and their administration at both stakeholder and consumer end. The growing awareness in favour of using renewable energy at households and usage of the zero-emission electric vehicle for commuting introduce potentials for BC and IoT to play a crucial role together.

Citizen engagement. A smart city helps to improve citizens' lifestyle by engaging them in activities and recreations. Public parks, libraries, museums, sports, cinemas, shopping centre, etc. are various forms of citizen engagement commonly found in modern cities. The real-time data could be collected using IoT-enabled sensors installed at these public spaces while BC would provide the backbone of historical information that aids machine learning or similar methods to make recommendations.

3.6 Requirement analysis: smart city

This section discusses different types of functional and non-functional requirements that are essential to apprehend the smart city use-cases. The attempt, however, first identifies the system characteristics of the use-cases that, in turn, creates the ground for recognizing the requirements.

- *Tracking*—The smart city applications depends on the tracking of human and non-human elements of the urban areas. This tracking characteristic may involve technological hurdles and legal red tapes that must be taken into account before developing any application.
- *Connectivity*—IoT applications typically require a seamless connection to exchange data. While operating in a smart city context, these applications often become intolerant to delay, and their performance profoundly depends on the connectivity of the devices.
- *Privacy*—Tracking of both human and non-human elements involves privacy issue. While tracking human, whether or not tracking their faces is a matter of debate. It is also a challenge as to how to identify individuals to provide them with tailored services. Tracking of non-human elements, such as scanning a car registration plate, can also cause serious privacy concern.
- *Reliability*—This is an essential characteristic as most smart city applications are used in automation. Without a high degree of reliability, running such applications in the city is not safe and even may cause harm to the people if malfunctioned to a great extent.

3.6.1 Functional requirements

Based on the characteristics outlined above, we identify the following functional requirements of a smart city:

- **Location-based tracking**—Many smart city applications require location-based tracking to capture accurate data. To fulfil this requirement, the use of sensors and sometimes access to smartphone network data is useful.

- **Real-time decision making**—People mostly use smart city applications to obtain real-time services. Naturally, real-time service requires real-time decision making.
- **Interoperability**—Smart city applications access data from a wide range of sources including sensors, BC and database, and operate over multiple platforms. It is, therefore, an essential requirement that they have interoperability capabilities.

3.6.2 Non-functional requirements

The followings are the non-functional requirements for the smart city use-cases:

- **Privacy preservation**—Smart city applications interact with users very closely utilizing their personal and location data. This nature of the use-cases makes them popular targets for a variety of security attack looking for personal data and hence, requires privacy-preserving data storage and communication.
- **Securing the system**—The system needs security to avoid potential threats that may launch attacks not only on the users but also on the smart city infrastructures.
- **Ensuring trust**—Trust is an important element that needs to be taken care of. To obtain seamless service, people are likely to register their bank cards, connect their email and social network sites and give access to their phone location. These are all sensitive information-required trustworthy services.

3.7 Smart home

The revolution in the world of IoT and device-to-device communication has made smart homes or home automation one of the most lucrative IoT applications in recent years. With the introduction of different types of hardware, scalable infrastructure and mobile applications, the use of home automation has rapidly increased worldwide and this will continue to grow in future. Fundamentally, a smart home is a network of devices with built-in connectivity that can communicate with each other through the use of communication protocols. It provides home owners the ability to remotely monitor and manage every single electronic device at home via a centralized interface. However, the chaotic growth of IoT devices has also introduced a number of challenges such as interoperability, scalability, security and privacy. BC could play a vital role in improving data security, privacy, trust and traceability in a smart home. In this section, we present several use-cases to illustrate the usefulness of a smart home.

Smart appliances. Smart appliances are IoT-enabled appliances used in our daily life such as fridge, thermostat, air conditioner and security alarms. Recent research has revealed that the global market of smart home tools and services will be around US\$ 98 billion by the end of 2025 (TMR, 2019). It is also anticipated that every single piece of home appliance will be integrated with IoT capabilities in future. These capabilities will be leveraged to create novel applications in order to provide a greater level of control and comfort for everyone in the home. These will facilitate smart home residents to monitor and control any home appliances from anywhere in the world.

Well-being and convenience. The ultimate goals of all the features described above are to ascertain the well-being and convenience of the residents of a smart home. Equipped with the required smart devices, a smart home should be able to monitor the well-being and overall health of its residents. This is particularly crucial for a smart home in which there is at least one old resident. If any health monitoring equipment senses any danger for any resident, it should raise alarms to the emergency health services.

3.8 Requirement analysis: smart home

Home automation is receiving a lot of attention these days, and the big companies like Samsung, Google, Amazon and Apple are all racing to capture this billion dollar smart home gadgets market. To leverage the maximum benefits of smart homes, we need to understand their basic characteristics. First, we describe the key characteristics of a smart home that would help us to formulate the functional and non-functional requirements.

- *Unified control*—Most of the smart home systems unify all smart devices in a home under the control of one interface. This unified control enables the end users to manage and monitor their home devices or home environments using a simple website or mobile application.
- *Intelligent*—Smart homes are intelligent in the sense that they are capable of identifying abnormal or unexpected events and triggering alerts to the residents when necessary.
- *Heterogeneity*—Usually, smart homes or home automation systems have the ability to tie diverse electronic devices together so that they can work in a cohesive way.
- *Threat protection*—A smart home is expected to monitor its residents and environment in an unprecedented manner. Since it will collect a huge amount of personal information, it is imperative that a smart home is built around a carefully thought security and privacy requirements.

3.8.1 Functional requirements

Based on the characteristics described above, we formulate functional and non-functional requirements of a smart home. First, we identify the core set of requirements that are fundamental for realizing the outlined use-cases. The functional requirements are presented below.

- **Context awareness**—A smart home with its integrated sensors and devices should be context-aware and intelligent. It should be able to identify its residents so that it can apply their preference to detect when someone is at home or not and then act accordingly.
- **Real-time monitoring**—A smart home monitors the performance of the registered devices and raises alarms to the residents in case a device malfunctions.
- **Responsiveness**—It should be able to detect different (allowed) actions of its residents and raise alarms to the appropriate authorities in case it senses danger.

3.8.2 Non-functional requirements

Non-functional requirements are also as critical as functional requirements and they play an important role in overall system design and evaluation. The following are key non-functional requirements identified for smart home systems:

- **Interoperability**—A smart home should provide interoperability among a wide range of devices. One of the ways to achieve this is to establish a common standard by which different heterogeneous devices interact with each other.
- **Flexibility**—Home automation systems should provide the flexibility to add new devices or services at any time if required.
- **Safety and security**—Security is a key concern in smart homes since they collect and monitor sensitive information. A smart home must be able to implement standard cryptographic schemes to ensure safety and security of the system.

4 IoT-supported blockchain platforms

In this section, we explore different BC platforms that have recently emerged to support different IoT applications. The selected BC platforms are Waltonchain (briefly discussed in Section 4.1), OriginTrail (Section 4.2), Slock.it (Section 4.3), Moeco (Section 4.4), IOTA (Section 4.5), IBM Watson (Section 4.6) and NetObjex (Section 4.7).

It is to be noted that, among these platforms, IOTA theoretically is not a BC platform, rather it represents a distributed ledger platform. However, because of its relevance to the scope of this paper, we have included it in our analysis. A brief description of each platform is presented next.

4.1 Waltonchain

Waltonchain is a new BC platform for the IoT industry (Waltonchain, 2019). The platform is named thus in order to commemorate and recognize the contribution of Charles Walton, the inventor of RFID (radio frequency identification) technology and to advance his vision for the ubiquitous deployment of the RFID technology in the form of IoT. With this motivation, Waltonchain would like to disrupt the current IoT industries by integrating the transparency, accountability and provenance properties of the BC with RFID-enabled IoT hardware. Indeed, the core platform consists of RFID hardware (both RFID tags and reader), the Waltonchain public BC platform and the software platform that interfaces the hardware with the BC.

Architecture. The Waltonchain platform has a layered architecture consisting of six layers with different layers having different functionalities. The functionalities of each layer are briefly discussed below.

- **Object layer:** The object layer consists of the hardware required for the Waltonchain ecosystem. The hardware includes RFID devices, different sensors, different storage, computing and network devices. The Waltonchain ecosystem introduces novel RFID and computing devices to ensure the authenticity and reliability of data in its source.
- **Base layer:** The base layer encompasses the network primitives for a BC ecosystem. It consists of the P2P network and different types of nodes providing distributed computing and storage facilities in order to maintain a public BC system.
- **Core layer:** The core layer provides the public BC overlay, confusingly also called *Waltonchain*. It is regarded as the *Parent* chain in the Waltonchain ecosystem and defines the required BC primitives such as block structure, consensus mechanisms and smart contract facility.
- **Extension layer:** The extension layer enables the deployment of business application logic for a particular application consisting of different organizations.
- **Service layer:** The service layer is aimed towards exposing several interfaces, probably in the form of APIs (application programming interfaces) and libraries for the application layer.
- **Application layer:** The application layer is where the business applications will be developed targeting different use-cases.

Node and network. Waltonchain presumably (as not explicitly specified in their whitepaper) will consist of two types of network: public and private. A public network controls the parent public BC whereas there could be different public/private child chains for maintaining different child chains, each for a specific industry or use-case. The private chain can set their own access control rules which will govern which entity can access such a chain.

Blockchain. As mentioned earlier, the Waltonchain platform supports the simultaneous existence of different types of BCs. The parent BC, the Waltonchain, is a public BC allowing anyone to participate in the consensus mechanism or to assume any role in the BC after certain criteria are fulfilled. This public BC maintains similar properties of other public BC systems such as Bitcoin and Ethereum. A block in Waltonchain can consist of up to 255 transactions where each transaction either transfers a value in the form of Waltonchain cryptocurrency called *Waltoncoin* or encodes certain commands for creating or interacting with a smart contract or creating a child chain.

Consensus and reward. The Waltonchain platform introduces a hybrid consensus algorithm called WPoC (Waltonchain proof of contribution). WPoC is a combination of three different consensus algorithms: proof of work (PoW), proof of stake (PoS) and proof of labour (PoL) (Waltonchain, 2019). PoW is similar to what is used in Bitcoin where a special type of node, called miner, in the network tries to solve a computationally intensive cryptographic puzzle. The solution is then included in the block of Bitcoin as a proof. All miner nodes within the network compete with one another to solve the puzzle where only one succeeds. The effect of this competition is the huge wastage of electricity and hence, many do not consider PoW a sustainable long-term solution. PoS is a new type of consensus algorithm which has been proposed to replace PoW by offering a solution which arguably provides the same level of

Table 1 Waltonchain properties

Type	Speed	Consensus	Block size	Smart contract	Fee	Token
Public and Private	100 TPS	WPoC	225 TX	Yes	Yes	WTC

security as PoW without consuming any significant electricity (QuantumMechanic, 2011). Unlike PoW, PoS generally relies on a mechanism in which special types of nodes called *staking nodes* participate in the block creation competition by staking their share of the underlying cryptocurrency. If they do not behave as intended, they lose their share, whereas honest behaviour would be rewarded. It is expected that Ethereum will switch to a hybrid PoW–PoS solution in near future (Proof of Stake FAQ, 2018). PoL, on the other hand, has been described as a brand new consensus algorithm for cross-chain data transmission and token exchange in the whitepaper (Waltonchain, 2019). Waltonchain has specified different types of reward mechanisms for different nodes and different consensus mechanisms (wtcReward, 2018). Table 1 summarizes the properties of Waltonchain.

4.2 OriginTrail

OriginTrail is a decentralized, permissionless BC platform that facilitates data sharing in a multi-organizational environment (OriginalTrail, 2018). This platform incorporates BC technology with digital supply chains to provide data integrity. The key idea is to ensure product standards and safety of the consumers by employing a standard BC-based solution through an incentivized protocol. OriginTrail addresses two key disrupting factors in data collection and sharing in supply chains.

Data fragmentation—Different data storage structures across the supply chain lead to data silos and low data interoperability in both single and multi-organizational supply chains.

Data centralization—Most of the existing supply chains rely on a trusted intermediary or central authority that provides information on product authentication and provenance.

Architecture. OriginTrail implements a layered, extensible and modular framework across the entire structure known as Electronic Product Code Information Service (EPCIS) framework. The network and data layers are two system layers that implement an off-chain decentralized peer to peer network known as OriginTrail Decentralized Network (ODN) on top of the blockchain layer. The functionalities of each layer are described below.

- BC layer—OriginTrail provides data integrity in supply chains by incorporating BC technology as a data sharing platform. All information in the system are stored on immutable ledgers in the form of data fingerprints at the time of arrival.
- ODN data layer—This layer is mainly responsible to perform all data management and connectivity functionalities among different data sets across the supply chain. To leverage data relationships in an effective way, ODN incorporates a decentralized graph database which provides the most efficient solution for interconnected data in terms of interoperability, performance and availability.
- ODN network layer—The ODN network layer consists of network nodes that contain part of the decentralized database as well as graph database.
- Decentralized applications—On top of the network layer, a number of DApps work as an interface between the users and the system to provide data input facilities.

Node and protocol. The nodes in ODN can be classified into two types according to their interaction with the supply chain: (i) data creators (DC) and (ii) data holders (DH). DC nodes are mainly responsible for incorporating supply chain data into the network and replicating it over a particular number of DH nodes, whereas DH nodes must ensure the immutability and storage of the corresponding data. To defend

Table 2 OriginTrail properties

Type	Speed	Consensus	Block size	Smart contract	Fee	Token
Public	Eth + ODN	PoW	Eth	Yes	Write and Read	TRAC

against collusion attack, for each n DC nodes in a supply chain, an additional number of at least $n + 1$ DH nodes have to be selected to store the replicated data. Since a DC node is a DH node as well, the minimum ODN replication factor is $2n + 1$ in this case. OriginTrail implements a data distribution protocol within the ODN.

Consensus and reward. The current version of OriginTrail implements PoW which runs on top of the Ethereum BC. The consensus mechanism works in three steps: (i) to maintain chain of accountability, each stakeholder has to be approved by the previous and the following supply chain stakeholder, (ii) matching would be done to verify dynamic batch information including batch identifiers, timestamps, transactional compliance and sensor data and (iii) data could also be verified by the auditing and compliance organizations by providing their confirmations. Table 2 summarizes the properties of OriginTrail.

4.3 Slock.it

Slock.it (2018) is an IoT platform on top of Ethereum BC. Its vision is to establish a truly decentralized sharing economy which will enable a direct interaction between a producer/owner and a consumer of IoT smart objects. The principle of sharing economy is to allow people share their unused or less-used physical or virtual resources, such as rooms or flats, cars, electricity or even time, for financial incentives. The traditional approach requires a lot of human intervention with a big issue of trust and transparency. The existing applications of sharing economy such as Uber and Airbnb are not decentralized. They rely on their monopolistic centralized providers which charge a considerable fee, yet the security, trust and transparency issues are prevalent in such applications. Slock.it (2015) aims to address these issues by providing a platform consisting of IoT smart objects, software and BC.

Architecture. The core architecture of Slock.it consists of IoT smart devices and Slock software platform and smart contract-supported Ethereum BC. In this platform, each IoT object will interact with each other via a smart contract (or a set of smart contracts) deployed in the Ethereum BC. A person can interact with each IoT object using any preferred device such as his mobile phone. The smart contract will provide several functionalities: to set up access control rules for a specific object, to facilitate automated contract execution when a certain condition meets and possibly for financial transactions between respective entities.

Node. One of the core challenges faced by Slock.it is how to seamlessly connect IoT objects to the Ethereum network. Such IoT object understandably will have less powerful processing and storage capabilities. However, to function properly, it is essential that such IoT objects are connected to the Ethereum network in a continuous fashion and are fully synced with the BC. This becomes impractical as the size of the BC starts to grow. To remedy this situation, Slock.it has considered several types of the following nodes (Jentzsch, 2018):

- **Full node:** A full node has the full version of the BC and it requires a huge amount of storage. Hence, it is impractical for any IoT device.
- **Pruned full node:** A pruned full node is a lighter version of the full node. It only stores a certain amount of recent states (blocks) of the BC, ignoring other previous ones. Even so, it will be impractical for any IoT object.
- **Light node:** A light node will need to store around 50 MB of data consisting of only block headers. Even though it requires a considerable less storage, it is also impractical for IoT devices with limited storage capability.

Table 3 Slock.it properties

Type	Speed	Consensus	Block size	Smart contract	Fee	Token
Public	Eth	Eth	Eth	Yes	Yes	IOU

Table 4 Moeco properties

Type	Speed	Consensus	Block size	Smart contract	Fee	Token
Public	Eth	Eth	Eth	Yes	Yes	MOE

- **Remote node:** A remote node relies on a trusted full node and interacts with the full node to validate any transaction or to interact with the BC. Thus, it introduces a trust issue as it will cease to function properly if the remote full node misbehaves.

Considering all these, Slock.it introduces a novel concept called INCUBED (IN^3) (Jentsch, 2018). INCUBED is a trustless incentivized network of remote nodes. For every correct response, each remote node will be rewarded while it will face monetary punishment when it misbehaves.

Consensus and reward. Unlike Waltonchain or OriginTrail, Slock.it does not have its own BC. Instead, it utilizes Ethereum as its underlying BC platform. Hence, it relies on the Ethereum's current consensus mechanism, rewarding process and other properties. Table 3 summarizes the properties of Slock.it.

4.4 Moeco

Moeco (2018) is a BC platform envisioned by its creator as the 'DNS of things'. This platform integrates several network standards and offers connectivity to billions of devices globally through participating gateways. It is particularly built to suit IoT technology in a cost-efficient way.

BC overview. Moeco uses crowdsourcing approach to enable existing networks and private gateway owners in its infrastructure. Anyone having the communication connectivity can become a gateway service provider. For example, someone having a wireless router at home or a smartphone with the internet connectivity can join as a gateway provider and start serving vendors, who are business providers owning sensor devices, to facilitate their sensor devices looking for connectivity. The permissionless decentralized architecture makes Moeco convenient for its users, both gateway owners and vendors. The platform takes care of payment and billing processes and ensures data delivery.

Technical characteristics. The goal of the Moeco BC system is to deliver data packages. As a decentralized system, there is no central authority ensuring the payment against any service provided by the gateway owners; hence, the need for a BC transpired.

This system utilizes two BCs, namely transport BC and invoice BC. The data package transportation and payment validation are both taking place in the Moeco network based on the Exonum BC framework while the payment is arranged using ERC 20 Ethereum Moeco tokens in the Ethereum network. Table 4 enlists the properties of Moeco.

4.5 IOTA

IOTA (2018) is a special type of cryptocurrency and a distributed ledger designed for the IoT. It provides secure communications and payments between IoT devices and a smart contract like service called Qubic.

Table 5 IOTA properties

Type	Speed	Consensus	Block size	Smart contract	Fee	Token
Public	500–800 TPS	Tangle	Qubic	Yes	No fee	IOTA

Unlike using the PoW and building blocks, IOTA uses the Tangle, consensus-building data structure made of directed acyclic graph. Its transactions are fast, free of cost and scalable.

BC overview. The communication between two IoT devices in IOTA is called machine-to-machine communication. IOTA uses Tangle to solve the double spending problem alongside solving both the scalability and transaction fee issues faced by most cryptocurrency including Bitcoin. By requiring the sender in a transaction to perform a PoW like approval of two transactions, IOTA turns its users into miners; hence, the acts of making a transaction and verifying transactions are coupled in this platform. There is no dedicated miners rather those making transactions are the actors affecting the system.

Technical characteristics. The Tangle is a consensus-building system where the machine submitting a new transaction must first verify two other transactions on the network, meaning the consensus is reached out of a web of verification. Instead of using a BC, Tangle enables IOTA verifying the transactions and reaching the consensus (Chowdhury *et al.*, 2019). It also removes the need for miners and data blocks on the platform. Each network member (machine) willing to execute a transaction must actively participate in the network consensus by approving two past transactions. This way each transaction links to this two transactions it verified, and over time, it will be linked to future transactions that verify it.

Unlike BC platforms driven by the *Hashcash*-like consensus mechanism that are vulnerable if someone can accumulate 51% of the total computing power on the network, IOTA is less secure and requires only 34% or higher than one-third of the network's computing power to launch an attack on its platform. Although implementing a 34% attack using Tangle is complicated, as the attacker still has to discover the next verified transactions of the network before leveraging the 34% advantage, in a small network launching such an attack is relatively easy. The IOTA being a new distributed ledger, its network is not still big enough to avoid this attack; hence, it uses a coordinator in its initial implementation to combat this threat and ensure the early Tangles are not compromised. IOTA plans to eliminate the coordinator once the network becomes strong enough in future. Table 5 summarizes the properties of IOTA.

4.6 IBM Watson

IBM Watson IoT Platform Blockchain Service is an add-on to IBM Watson IoT Platform (Waltonchain, 2019). The service allows IoT devices to send data and respond to business events through a private BC ledger shared by different business network. It is an integrated service of IBM Watson platform and its Hyperledger BC project. It can capture data in real-time process by using IoT devices. It also provides data analytics and visualization services.

The Hyperledger project is a collaborative effort between IBM and Linux Foundation to create an enterprise-grade, open-source distributed ledger framework and code base. The idea is to realize a cross-industry open standard platform for distributed ledgers. There are several active projects are going on under the umbrella of Hyperledger project, namely Burrow, Fabric, Sawtooth, Iroha and Indy. Fabric is the most popular platform from this group. It is a permissioned BC infrastructure with modular architecture which enables to configure different types of consensus algorithms. It also supports execution of smart contracts (called 'chaincode' in Fabric) and membership services.

The Burrow platform provides Ethereum virtual machine support in Hyperledger project, whereas the Iroha project is mainly focused on mobile applications. Sawtooth is another platform contributed by Intel, and it includes a dynamic consensus feature enabling hot swapping consensus algorithm in a running network. Among the consensus options, a novel consensus protocol known as 'Proof of Elapsed Time', a lottery-design consensus protocol is optionally built on trusted execution environments provided

Table 6 IBM Watson properties

Type	Speed	Consensus	Block size	Smart contract	Fee	Token
Private	160–3500 TPS	SOLO, Kafka	Configurable	Yes	No fee	None

by Intel's software guard extensions. The Indy platform supports independent identity on distributed ledgers.

Architecture. As an umbrella project, Hyperledger does not have a single architecture. However, all Hyperledger projects follow a design philosophy that includes a modular extensible approach, interoperability, a token-agnostic approach with no native cryptocurrency, and ease-of-use. The Hyperledger architecture has the following BC components:

1. **Consensus layer**—Responsible for generating an agreement on the order and confirming the correctness of the set of transactions that constitute a block.
2. **Smart contract layer**—Responsible for processing transaction requests and determining if transactions are valid by executing business logic.
3. **Communication layer**—Responsible for peer-to-peer message transport between the nodes that participate in a shared ledger instance.
4. **Data store abstraction**—Allows different data-stores to be used by other modules.
5. **Crypto abstraction**—Allows different crypto algorithms or modules to be swapped out without affecting other modules.
6. **Identity services**—Enables the establishment of a root of trust during set-up of a BC instance, the enrollment and registration of identities or system entities during network operation, and the management of changes like drops, adds and revocations. It also provides authentication and authorization.
7. **Policy services**—Responsible for management of various policies specified in the system, such as the endorsement policy, consensus policy or group management policy. It interfaces and depends on other modules to enforce various policies.
8. **APIs**—Enables clients and applications to interface with BCs.

Node and network. In Hyperledger Fabric, there are three types of nodes. Each node is a process running on some machines (perhaps in a container) and communicates with other nodes in the network. The nodes are orderer node, peer node and client node. Each node is correlated with some organizations and has its own certificate and private key. The client node acts on behalf of an end-user and creates and thereby invokes transactions.

Transaction, block and blockchain. In Hyperledger, developers can control block size with *BatchTimeout* and *BatchSize* parameters in the configuration file based on the use-cases. Developers can also use *Max Message Count* to control the maximum number of transactions/messages to permit in block.

Consensus and reward. We have already discussed that Hyperledger uses modular architectural design that supports different consensus mechanisms to be plugged-in. However, currently, Fabric, the most popular platform supports only two consensus mechanisms: SOLO and Kafka. Sawtooth supports a novel consensus protocol known as 'Proof of Elapsed Time'. The validating peers are responsible for running consensus, validating transactions and maintaining the ledger.

In terms of rewarding system, currently it does not provide any mechanism for cryptocurrencies. However, token can be generated and used in this platform. Table 6 summarizes the properties of the IBM Watson platform.

Table 7 NetObjex properties

Type	Speed	Consensus	Block size	Smart contract	Fee	Token
Private	Variable	Variable	Variable	Yes	Yes	IoToken

4.7 NetObjex platform

NetObjex is a decentralized digital asset management platform that provides services for four major market segments, namely supply chain and logistics, manufacturing industry, smart city and automotive industry (NetObjex, 2018). The platform integrates both IoT and BC for data acquisition and dissemination purposes and supports a wide range of communication protocols such as cellular, mid-range protocols (LoRA, Sigfox and NB-IoT), Wifi, Ethernet, BLE and specialized protocols (DSRC). In addition, it also provides the flexibility to enforce business rules through smart contracts.

Architecture. The NetObjex platform integrates a number of big data repositories, distributed ledger technologies and edge devices with its core BC middleware component. This architectural design ensures interoperability and cross-communications among different entities of a complex system. The following are the key components through which NetObjex ensures a flexible, plug and play and programmable environment.

- Edge devices—Edge devices are responsible to collect data from IoT devices and process it before sending to the NetObjex platform. The devices are capable of implementing data encryption mechanisms and can be remotely monitored through the healthcheck API.
- NetObjex platform—The NetObjex platform also known as BC middleware platform provides supports for multiple database engines (e.g. MongoDB, Cassandra and Elasticsearch), AI engines (e.g. SparkML and MachineBox) and rules engine in addition to remote actuation of edge devices, notification and marketing services. This unit is responsible for providing the following BC-specific features: (i) code generation for smart contracts for various decentralized networks, (ii) inter-chain communications, (iii) search across heterogenous networks and (iv) data aggregation across BCs.
- Distributed ledgers—A number of distributed ledger technologies including Ethereum, Hyperledger, IOTA and NEM are supported by the NetObjex platform. Data can be added and retrieved from multiple distributed ledgers through a single seamless API. One key feature of this platform is distributed ledger query language which is designed for high level language support for managing distributed ledgers.
- Enterprise systems—Enterprise systems contain a number of standard applications such as Jira, Redmine, SugarCRM and CiviCRM. These applications are connected to the BC middleware platform through an enterprise gateway that facilitates the information exchange between enterprise APIs and the platform.

IoToken. The NetObjex platform implements a new mechanism, IoToken, to globally interact smart devices with each other. To communicate between digital assets owned by different organizations within a single ecosystem, the platform introduces a technology fabric through this IoToken mechanism. In addition, the platform provides supports for IoToken native cryptocurrency for inter-device transactions. Table 7 presents a summarized view of the NetObjex platform.

5 Discussion

Since there are a number of BC platforms designed to provide different functionalities, it is important to evaluate their applicability with respect to the identified requirements of the selected IoT applications. This core set of requirements are then analyzed to evaluate the suitability of different BC platforms

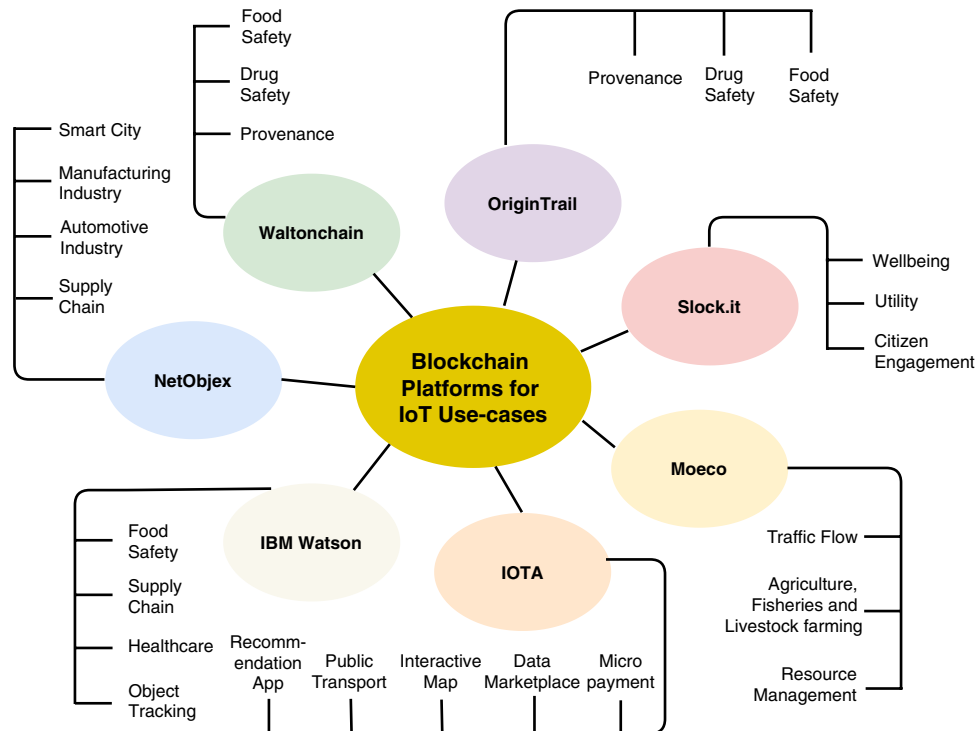


Figure 1 Different blockchain platforms and their supported IoT use-cases

for different IoT application scenarios. Our analysis has resulted in an evaluation framework which is presented in Figure 1.

In Waltonchain data are generated by RFID tags. These RFID tags are attached with the original items, which enable individuals to properly track the items. This tracking capability of the Waltonchain makes it a good solution to trace the source of food items and the supply chain of the drug. The traceability of the food items enhances the safety and builds the confidence among the consumers. RFID tags can be also used in the drug supply chain to check if it is produced by a legitimate pharmaceutical company and to check the date of expiry. Secondly, Waltonchain allows side-chains which allows to process and store data of millions of food items and drug. As data are stored in the public BC, anyone can easily verify the data along with their source, thereby providing provenance.

IBM Watson has already been used in the food chain of the giant food chain, namely Walmart Inc. (Smith, 2018). The private channels in Watson allow different food suppliers to communicate privately. This enables the buyers and sellers to buy/sell products at different prices without revealing the actual price to other competitors. In addition, as Watson is a private BC, it can process a large number of transactions. In terms of drug safety, Watson allows the participating parties in the drug supply chain to privately communicate data, similar to the food chain. In addition, the identity platform allows flexible access control mechanism, which is critical for healthcare system.

Slock.it can be utilized to facilitate the interactions between different physical resources equipped with Slock.it software and hardware and their users. A prime example of such resource is Slock.it powered smart objects within a smart home with the features to track the well-being of its residents. Such Slock.it powered smart objects can also be attached with the utility network such as electricity and gas and utilized to track the actual consumption of different utilities and facilitate autonomous payments based on the consumption. In addition, other such smart objects, for example, smart locks, can be utilized to lock and unlock physical resources (e.g. flats, houses, vehicles and so on) based on the access control rule within the corresponding smart contract in an automatic fashion. This will facilitate a new model of sharing economy which eventually will increase citizen engagements in a more efficient and secure way.

NetObjex is a middleware solutions that allows integrate solutions in different leading BC platforms such as Ethereum, Hyperledger and other. This platforms combines IoT, AI and machine learning to

provide a complete solutions. The data are captured by the edge devices. These particular features make it suitable for distributed and federated service such as transport and smart cities. It can also be used for supply chain management such as in food safety and drug.

OriginTrail is a public BC platform that can provide the data provenance and help to share the data with multiple parties. The EPCIS framework in OriginTrail provides interoperability among different systems/organization working in a supply chain. The off-chain storage in OriginTrail allows to store large amount of data in the BC.

Moeco is a gateway providing the connectivity required for IoT sensors. As explained in Section 4.4, this platform is not designed to store or share data instead offers the marketplace for vendors looking for the network connections to transfer their remote data end-to-end basis. Individuals having mobile phones or broadband can participate as gateway providers for interested vendors.

This platform suits well those uses-cases involving the public. As such, sensors on roads, shopping malls, offices, campuses, fields and similar locations where public gatherings are frequent can benefit from using the mobile phone or broadband networks of the participating providers. For instance, in a smart city, the tracking of locations of vehicles and people can be enabled using roaming people's mobile phone networks. Similarly, in vast agricultural fields, broadband connections from a limited number of people would allow everyone to use them as gateways to exchange IoT data. Offices, campuses, shopping malls, community centres, etc. can also use the shared networks for transferring resource management data collected from various sensors.

IOTA, on the contrary to Moeco, is a distributed ledger designed to work with IoT devices. It allows users to store and share their data that can be utilized by others or the contributors later. It does not charge users to share their data on the platform; however, the users require to validate at least two other transactions considered to be the *cost of IOTA*. This nature of IOTA makes the platform attractive to users interested in sharing their location data, social posts and information from the mobile phone that are not of privacy threat. In addition to the platform, its cryptocurrency can be of an added benefit too.

This platform is suitable for developing applications using public information coming from mobile phones, fitness trackers and other forms of IoT devices. Because of having the ability to share information on the platform at free of cost, both developers and users can form a win-win trade through mutual benefits using IOTA. For instance, applications providing public transport information, including road traffic congestions and traffic flow, interactive maps showing public movements in shopping malls, libraries, stadia, etc. and recommendation apps suggesting restaurants, tourists' locations and shopping places can benefit from using the platform. Furthermore, IOTA has a lot more to offer than just playing the role of a sharing platform. In the presence of IOTA cryptocurrency, which is a proper fit for making micro-payments, the platform can be turned into a data marketplace. As of 2017, it allows vendors to store data and create live streams for potential customers securely (Harbor, 2019). Kochava.com is an example of such a market powered by IOTA.

Table 8 presents a comparative view of different IoT-enabled BC platforms with respect to a number of qualitative and quantitative attributes. The first seven rows of the table summarize several key properties of BC platforms described in Section 4, whereas the next five rows compare the platforms in terms of energy consumption, privacy, identity and governance mechanisms, and upgradation supports. It can be seen that IOTA consumes very low energy as the platform is specially designed to support IoT devices. Similarly, Waltonchain consumes low energy whereas the consumption is moderate for both OriginTrail and NetObjex as they support many cross-layer functionalities. In contrast, Slock.It and Moeco consume a significant amount of energy. In terms of privacy and identity, IBM Watson provides strong privacy supports and PKI-based identification for the users, where all other platforms implement pseudonymous identity and privacy. One interesting observation to be noted that all platforms support open source code-base which provides everyone the opportunity to contribute in the further development of the platform. However, the development teams are ultimately responsible for any new implementation or upgradation of the platforms.

Table 8 A comparative view of different IoT-enabled blockchain platforms

Properties	Waltonchain	OriginTrail	Slock.it	Moeco	IOTA	Watson	NetObjex
Type	Public and private	Public	Public	Public	Public	Private	Private
Speed	100 TPS	Eth + ODN	Depends on Eth	Depends on Eth	500–800 TPS	160–3500 TPS	Variable
Consensus	WPoC	PoW	Depends on Eth	Depends on Eth	Tangle	Kafka, SOLO	Variable
Block size	225 Tx	Depends on Eth	Depends on Eth	Depends on Eth	Qubic	Configurable	Variable
Smart Contract	Yes	Yes	Yes	Yes	Yes	Yes	Yes
Fee	Yes	Yes	Yes	Yes	No	No	Yes
Token	WTC	TRAC	IOU	MOE	IoToken	No	IoToken
Energy	Low	Moderate	High	High	Very Low	Low	Moderate
Privacy	Pseudonymous	Pseudonymous	Pseudonymous	Pseudonymous	Pseudonymous	Strong privacy support using virtual channels	Pseudonymous
Identity	Pseudonymous	Pseudonymous	Pseudonymous	Pseudonymous	Pseudonymous	PKI-based identification.	Pseudonymous
Governance	Open source code-base and governed by Waltonchain	Open source code-base and governed by OriginalTrail	Open source code-base and governed by Slock.it	Open source code-base and governed by Moeco	Open source code-base and governed by the IOTA Foundation.	Open source code-base and governed by the Hyperledger foundation.	Open source code-base and governed by NetObject
Upgradation	Waltonchain development team	OriginalTrail development team	Slock.it development team	Moeco development team	IOTA development team.	Fabric committee member	NetObject development team

6 Conclusion

IoT and BC are two emerging technologies that are expected to have immense impacts in the society around the world. Each of these technologies has their own sets of applications and some significant shortcomings. Combining these two technologies, however, might address many of these shortcomings. Not only that, this combination opens up doors of opportunities for novel applications with additional advantages. This paper aims to explore this avenue. In particular, this principal motivation of this chapter has been to create an evaluation framework which can be utilized to evaluate different BC platforms for their suitability in different IoT applications.

Towards this aim, this paper has explored different IoT applications: healthcare, smart industries, smart city and smart home. For each of these applications, different use-cases have been analyzed. Based on this, several functional, security and privacy requirements have been identified. Next, seven IoT-focused BC platforms have been examined to identify their inherent properties. Finally, combining the requirements of the IoT applications and properties of the selected BC platforms, an evaluation framework has been created which is presented as a figure (Figure 1). The graphical representation provides an intuitive visualization to identify the suitable BC platform(s) for a particular application under certain requirements.

There are still a lot of challenges that need to be tackled before these two emerging technologies can be successfully merged. One major challenge will be to identify a suitable BC platform for a particular use-case (e.g. cold chain monitoring) within an application domain (e.g. supply chain). The current evaluation framework in this paper has this limitation that it can only identify suitable platforms for a generic IoT application domain. We aim to address this in our future work. Even with this limitation, we believe our effort presented in this paper will represent a step forward towards addressing this challenge effectively for researchers and practitioners in this domain.

References

- Angraal, S., Krumholz, H. M. & Schulz, W. L. 2017. Blockchain technology: applications in health care. *Circulation: Cardiovascular Quality and Outcomes* **10**(9). doi: [10.1161/CIRCOUTCOMES.117.003800](https://doi.org/10.1161/CIRCOUTCOMES.117.003800).
- Atzori, L., Iera, A. & Morabito, G. 2010. The internet of things: a survey. *Computer Networks* **54**, 2787–2805.
- Biggs, J. Hackers release source code for a powerful ddos app called mirai, TechCrunch.
- Biswas, K., Muthukumarasamy, V. & Tan, W. L. 2017. Vacci-chain: a safe and smarter vaccine storage and monitoring system. In *Symposium on Distributed Ledger Technology - SDLT '17*.
- Brodersen, C., Kalis, B., Leong, C., Mitchell, E., Pupo, E., Truscott, A. & Accenture, L. 2016. Blockchain: Securing a New Health Interoperability Experience. Ed: Accenture LLP.
- Chowdhury, N. 2019. *Inside Blockchain, Bitcoin, and Cryptocurrencies*. CRC Press, Taylor & Francis.
- Chowdhury, M. J. M., Ferdous, M. S. & Biswas, K. 2018. Blockchain platforms for IoT use-cases. In *2nd Symposium on Distributed Ledger Technology (SDLT)*.
- Chowdhury, M. J. M., Ferdous, M. S., Biswas, K., Chowdhury, N., Kayes, A. S. M., Alazab, M. & Watters, P. 2019. A comparative analysis of distributed ledger technology platforms. *IEEE Access* **7**, 167930–167943.
- Chowdhury, N., Ramachandran, M., Third, A., Mikroyannidis, A., Bachler, M. & Domingue, J. 2020. Towards a blockchain-based decentralised educational landscape. In *Proceedings of the Twelfth International Conference on Mobile, Hybrid, and On-line Learning, Valencia, Spain*.
- Cocchia, A. 2014. *Smart and digital city: a systematic literature review*. In *Smart City: How to Create Public and Economic Value with High Technology in Urban Space*, Dameri, R. P. & Rosenthal-Sabroux, C. (eds). Springer, Ch. 2, 13–43.
- Dubovitskaya, A., Xu, Z., Ryu, S., Schumacher, M. & Wang, F. 2017. How blockchain could empower eHealth: an application for radiation oncology. In *VLDB Workshop on Data Management and Analytics for Medicine and Healthcare*. Springer, 3–6.
- Ferdous, M. S., Chowdhury, M. J. M., Biswas, K., Chowdhury, N. & Muthukumarasamy, V. 2020. Immutable autobiography of smart cars leveraging blockchain technology. *Knowledge Engineering Review* **35**. doi: [10.1017/S0269888920000028](https://doi.org/10.1017/S0269888920000028).
- Global Smart Homes Market to Leverage Advancement of IoT and Improvement in Consumer Acceptance Spurring Demand. <https://www.transparencymarketresearch.com/pressrelease/smart-homes-market.htm> (accessed 10 June 2019).
- Harbor, C. Iota Data Marketplace. <https://data.iota.org/> (accessed 25 April 2020).

- Insight, L. 2016. How consumer demand for transparency is shaping the food industry. https://www.labelinsight.com/hubfs/Label_Insight-Food-Revolution-Study.pdf (accessed 25 April 2020).
- IOTA White Paper. https://iota.org/IOTA_Whitepaper.pdf (accessed 25 April 2020).
- Jentsch, C. Slock.it IoT Layer. <https://blog.slock.it/slock-it-iot-layer-f305601df963> (accessed 25 April 2020).
- Kuo, T.-T., Kim, H.-E. & Ohno-Machado, L. 2017. Blockchain distributed ledger technologies for biomedical and health care applications. *Journal of the American Medical Informatics Association* **24**(6), 1211–1220.
- Liu, L., Liu, X. & Li, X. 2012. Cloud-based service composition architecture for internet of things. In *Internet of Things*. Springer, 559–564.
- MacGillivray, C., Turner, V., Lamy, L., Prouty, K., Segal, R., Siviero, A., Torchia, M., Vesset, D., Westervelt, R. & Yesner, R. 2016. IDC FutureScape: Worldwide Internet of Things 2017 Predictions.
- Medilegger. <https://www.medilegger.com/network> (accessed 25 April 2020).
- Miller, H. G. & Mork, P. 2013. From data to decisions: a value chain for Big Data. *IT Professional* **15**(1), 57–59.
- Moeco, 2018. *Moeco Whitepaper*. Technical report v 0.9, [Moeco.io](https://moeco.io). (accessed 25 April 2020).
- NetObjex Platform. <https://www.netobjex.com/> (accessed 25 April 2020).
- Nugent, T., Upton, D. & Cimpoesu, M. 2016. *Improving Data Transparency in Clinical Trials Using Blockchain Smart Contracts*. F1000Research 5.
- OriginalTrail White Paper. <https://origintrail.io/storage/documents/OriginTrail-White-Paper.pdf> (accessed 25 April 2020).
- Panarello, A., Tapas, N., Merlino, G., Longo, F., & Puliafito, A. 2018. Blockchain and IoT integration: a systematic survey. *Sensors* **18**(8). doi:10.3390/s18082575.
- Peterson, K., Deeduvanu, R., Kanjamala, P. & Boles, K. 2016. A blockchain-based approach to health information exchange networks. In *Proceedings of NIST Workshop Blockchain Healthcare*, **1**, 1–10.
- Proof of Stake FAQ. <https://github.com/ethereum/wiki/wiki/Proof-of-Stake-FAQ> (accessed 25 April 2020).
- QuantumMechanic, Proof of Stake Instead of Proof of Work. <https://bitcointalk.org/index.php?topic=27787.0> (accessed 25 April 2020).
- Ramachandran, M., Chowdhury, N., Third, A., Domingue, J., Quick, K. & Bachler, M. 2020. Towards complete decentralised verification of data with confidentiality: different ways to connect solid pods and blockchain. In *Proceedings of the ACM Web Conference, Taipei, Taiwan*.
- Schöner, M. M., Kourouklis, D., Sandner, P., Gonzalez, E. & Förster, J. 2017. *Blockchain Technology in the Pharmaceutical Industry*. Frankfurt School Blockchain Center.
- Slock.it — Decentralizing the Emerging Sharing Economy, 2015. <https://blog.slock.it/slock-it-decentralizing-the-emerging-sharing-economy-cf19ce09b957> (accessed 25 April 2020).
- Slock.it Platform. <https://slock.it/> (accessed 25 April 2020).
- Smith, M. In Wake of Romaine *E. coli* Scare, Walmart Deploys Blockchain to Track Leafy Greens. <https://news.com/2018/09/24/in-wake-of-romaine-e-coli-scare-walmart-deploys-blockchain-to-track-leafy-greens> (accessed 25 April 2020).
- Sniderman, B., Mahto, M. & Cotteler, M. J. 2016. *Industry 4.0 and Manufacturing Ecosystems*. Deloitte Industry Report.
- Trending: IoT Malware Attacks of 2018. <https://securingtomorrow.mcafee.com/consumer/mobile-and-iot-security/top-trending-iot-malware-attacks-of-2018/> (accessed 25 April 2020).
- Waltonchain White Paper, V2.0. https://waltonchain.org/templates/default/doc/Waltonchain-whitepaper_EN_20180525.pdf (accessed 25 April 2020).
- Waltonchain Progressive Mining Reward Program. <https://github.com/ethereum/wiki/wiki/Proof-of-Stake-FAQ> (accessed 25 April 2020).
- World Health Organisation Report, 2017. A study on the public health and socioeconomic impact of substandard and falsified medical products. https://www.who.int/medicines/regulation/ssffc/publications/SE-Study_EN_web.pdf?ua=1 (accessed 25 April 2020).
- Xia, Q., Sifah, E. B., Asamoah, K. O., Gao, J., Du, X. & Guizani, M. 2017. Medshare: trust-less medical data sharing among cloud service providers via blockchain. *IEEE Access* **5**, 14757–14767.
- Zhang, P., White, J., Schmidt, D. C. & Lenz, G. 2017. Applying software patterns to address interoperability in blockchain-based healthcare apps. arXiv preprint [arXiv:1706.03700](https://arxiv.org/abs/1706.03700).