# Integrated platforms for blockchain enablement

**Chapter** *in* Advances in Computers · January 2019

DOI: 10.1016/bs.adcom.2019.01.001



**5 authors**, including:

Md. Sadek Ferdous
Shahjalal University of Science and Technology
**47** PUBLICATIONS **189** CITATIONS
SEE PROFILE

Kamanashis Biswas
Australian Catholic University
**41** PUBLICATIONS **309** CITATIONS
SEE PROFILE

Mohammad Jabed Morshed Chowdhury
La Trobe University
**16** PUBLICATIONS **47** CITATIONS
SEE PROFILE

Niaz Chowdhury
The Open University (UK)
**16** PUBLICATIONS **34** CITATIONS
SEE PROFILE

# Integrated Platforms for Blockchain-Enablement

Md Sadek Ferdous[a,b,*], Kamanashis Biswas[c,*], Mohammad Jabed Morshed Chowdhury[d], Niaz Chowdhury[e], Vallipuram Muthukkumarasamy[f]

[a]*Shahjalal University of Science and Technology, Sylhet, Bangladesh*
[b]*Imperial College London, UK*
[c]*Australian Catholic University, Australia*
[d]*Swinburne University of Technology, Australia*
[e]*Open University, UK*
[f]*Griffith University, Australia*

**Abstract**

The Internet of Things (IoT) is experiencing an exponential growth in a wide variety of use-cases in multiple application domains, such as healthcare, agriculture, smart cities, smart homes, supply chain and so on. To harness its full potential, it must be based upon a resilient network architecture with strong support for security, privacy and trust. Most of these issues still remain to be addressed carefully for the IoT systems. Blockchain technology has recently emerged as a breakthrough technology with the potential to deliver some valuable properties such as resiliency, support for integrity, anonymity, decentralisation and autonomous control. A number of blockchain platforms are proposed that may be suitable for different use-cases including IoT applications. In such, the possibility to integrate the IoT and blockchain 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 blockchain platform for a particular application satisfying its underlying requirements. This chapter aims to achieve this goal by describing an evaluation framework which can be utilised to select a suitable blockchain platform for a given IoT application.

*Keywords:* IoT, Blockchain, Healthcare, Supply Chain, Smart Home, Smart City

## 1. Book Chapter

**This chapter is the author's abridged version. The full chapter is to be published as a book chapter in Elsevier Advances in Computer (ADCOM) Volume 115: Role of Blockchain Technology in IoT Applications.**

*Corresponding author
*Email addresses:* s.ferdous@imperial.ac.uk (Md Sadek Ferdous), kamanashis.biswas@acu.edu.au (Kamanashis Biswas), mjchowdhury@swin.edu.au (Mohammad Jabed Morshed Chowdhury), niaz.chowdhury@open.ac.uk (Niaz Chowdhury), v.muthu@griffith.edu.au (Vallipuram Muthukkumarasamy)

The book can be purchased from the following location:
https://www.elsevier.com/books/role-of-blockchain-technology-in-iot-applications/kim/978-0-12-817189-9

## 2. Requirements, Comparison & Evaluation Framework

In this chapter, we have selected four IoT application domains: Healthcare, Supply chain , Smart city and Smart home. Each of these application domains and their corresponding use-cases have been analysed to identify several functional, security and privacy requirements. The functional requirements are:

- **F1 - Scalability:** Scalability refers to the ability to grow in size and functionalities without degrading the performance of the original system.
- **F2 - Multiple Sources:** The systems must be able to handle data generated from multiple heterogeneous sources and transmit such data with minimal to no latency.
- **F3 - Data Sharing:** All the stakeholders within each application should be able to exchange and share information, generated by heterogeneous data sources, internally within the organisation as well as externally to other entities without any intermediary.
- **F4 - Inter-operability:** A system developed for a particular application should be inter-operable among a wide range of stakeholders of the application.
- **F5 - Identity Management:** Every IoT devices and other human entities must be properly identified within the systems. Therefore, a proper identity management framework must be embedded into the systems of every use-case within an application.
- **F6 - Transparency:** Systems for these applications should be able to create an auditable chain of custody/activities from the data producer to the data consumer to ensure transparency in supply chain and healthcare systems.
- **F7 - Traceability:** For supply chains, traceability has become increasingly important due to the growth in consumers' interest about the origin of the products or services.
- **F8 - External Interface:** Systems in a particular application domain should expose an external interface by which it can be connected to the entities of other application domains so as to enable novel business cases.
- **F9 - Payment Mechanism:** Some application domains such as supply chain will inherently require a payment system built into its system. Whereas, the support of payment will enable additional business cases in other application domains.
- **F10 - Performance:** Systems for these applications should maintain certain level of performance in terms of response time, available storage or capacity so that they have the capability to process high volume and high frequency data generated by plethora of IoT devices.

- **F11 - Reliability:** The reliability requirement of an application ensures the availability of the system, up-do-date and accurate information as well as consistent flow of information among all entities in the system.

The identified security requirements (denoted with *S*) and privacy requirements (denoted with *P*) are

- **S1 - Secure Transmission:** Data generated in an application must be transmitted, both internally and externally, securely - that is with appropriate crypto mechanisms.
- **S2 - Fine-grained Access Control:** Among these applications, healthcare and smart home system would require authorising the right user and providing the appropriate access to the data. Hence, a fine-grained access control mechanism would be mandatory.
- **S3 - Data Provenance and Integrity:** The provenance and integrity of data generated from a specific source must be guaranteed.
- **S4 - Fault Detection and Patching:** There must be mechanisms to identify and trace every faulty IoT device in the system.
- **P1 - Privacy Protection:** Systems must protect the privacy of users and organisations with appropriate mechanisms.

Next, based on our analysis, we summarise the requirements for different IoT applications in Table 1. As per the table, we differentiate between explicit and implicit requirements which denote the mandatory and optional requirements respectively for a particular application.

Table 1: Summary of functional requirements for different applications

| Application | Explicit Requirement | Implicit Requirement |
|---|---|---|
| Healthcare | F1-F6, F11 | F7-F10 |
| Supply chain | F1-F7, F9-F11 | F8 |
| Smart city | F1-F5, F10, F11 | F6-F9 |
| Smart home | F1-F5, F11 | F6-F10 |

Similarly, we summarise the security and privacy requirements for different applications in Table 2. In the table, the symbol '✓✓' is used to denote that a specific requirement is crucial for an application whereas a single '✓' is used to denote that the requirement is desirable but not mandatory for the corresponding application.

Recently, we have experienced the emergence of different blockchain platforms, specifically to support different IoT applications. To identify the suitability of these platforms for our selected application domains, we need to analyse if these platforms satisfy the requirements presented above. The selected blockchain platforms are: Waltonchain (https://www.waltonchain.org/), OriginTrail (https://origintrail.io/), IOTA (https://www.iota.org/), Slock.it (https://slock.it/), IBM Watson (https://www.ibm.com/watson) Moeco (https://moeco.io/) and NetObjex (https://www.netobjex.com/).

Table 2: Summary of security and privacy requirements for different applications

| Application | S1 | S2 | S3 | S4 | P1 |
|---|---|---|---|---|---|
| Healthcare | ✓✓ | ✓✓ | ✓✓ | ✓ | ✓✓ |
| Supply chain | ✓✓ | ✓ | ✓✓ | ✓✓ | ✓✓ |
| Smart city | ✓✓ | ✓ | ✓✓ | ✓✓ | ✓✓ |
| Smart home | ✓✓ | ✓✓ | ✓✓ | ✓✓ | ✓✓ |

Next, we have evaluated these blockchain platforms using a set of properties. The result of the evaluation and the set of properties used are presented in Table 3. We have used the '✓' to indicate a certain property is satisfied and the 'x' to indicate the property is not supported by the respective platform. The '-' is used to signify that the property is not applicable for the platform. Moreover, the term '+Eth' is used to indicate that the respective platform inherits the values of the properties from Ethereum (a public smart-contract blockchain platform, https://www.ethereum.org/). Finally, numerical values or textual explanations, where appropriate, have been provided for other properties for corresponding platforms.

Since there are a number of blockchain 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 analysed to evaluate the suitability of different blockchain platforms for different IoT application scenarios. Our analysis has resulted in an evaluation framework which is presented in Figure 1.

The evaluation framework serves two main purposes:

- it can be used to identify which requirements are satisfied by which platforms and
- it can be used to choose (a) suitable platform(s) satisfying different requirements.

However, we propose to use the Performance requirement in a tie-break situation among several platforms. For example, if an application needs to support Scalability, Data Sharing capability with payment support, there are a few options to choose from: IOTA, OriginTrail, Waltonchain and NetObjex. In such cases, we propose to use the Performance requirement (based on TPS) to select the best one from these. This mechanism also provides additional flexibilities. We can even consider different quantitative consensus characteristics as part of the Performance requirement to impose other quantitative selection criteria to select the best platform for an application.

## 3. Conclusion

This chapter has explored four different IoT applications: Healthcare, Supply chain, Smart city and Smart home. For each of these applications, different use-cases have been analysed. Based on this, several functional, security and privacy requirements have been identified. Next, seven IoT-focused blockchain platforms have been examined to identify their inherent properties. Finally, combining the requirements of the IoT applications and properties of the selected blockchain platforms, an evaluation framework has been created which is presented as a figure (Figure 1). The graphical representation provides an intuitive visualisation to identify the suitable blockchain platform(s) for a particular application under certain requirements.

Table 3: Comparison of blockchain platforms using relevant properties

| Properties | IOTA | Walton chain | Origin Trail | Slock.It | Moeco | IBM Watson | NetObjex Platform |
|---|---|---|---|---|---|---|---|
| Public | ✓ | ✓ | ✓ | ✓ | ✓ | x | ✓ |
| Private | x | ✓ | x | x | x | ✓ | ✓ |
| Transaction Speed | 500-800 TPS | 100 TPS [? ] | +Eth | +Eth | +Eth | 160-3,500 | Platform dependent |
| Fee | x | ✓ | ✓ | ✓ | ✓ | x | Platform dependent |
| Block creation time | - | 30sec | ✓ | +Eth | +Eth | Variable | Platform dependent |
| Consensus | Tangle | WPoC | PoW | +Eth | +Eth | PBFT. However, other algorithms can be plugged in | Platform dependent |
| Network Size | Large | Large | +Eth | +Eth | +Eth | small to medium | Platform dependent |
| Block Size | - | 225 | +Eth | +Eth | +Eth | can be configured using BatchTimeout and BatchSize | Platform dependent |
| Smart Contract | ✓ | ✓ | +Eth | +Eth | +Eth | ✓ | Platform dependent |
| Secure Channel | x | x | x | x | x | ✓ | x |
| Verified identity | - | ✓(For private network) | ✓ | x | x | ✓ | ✓ |

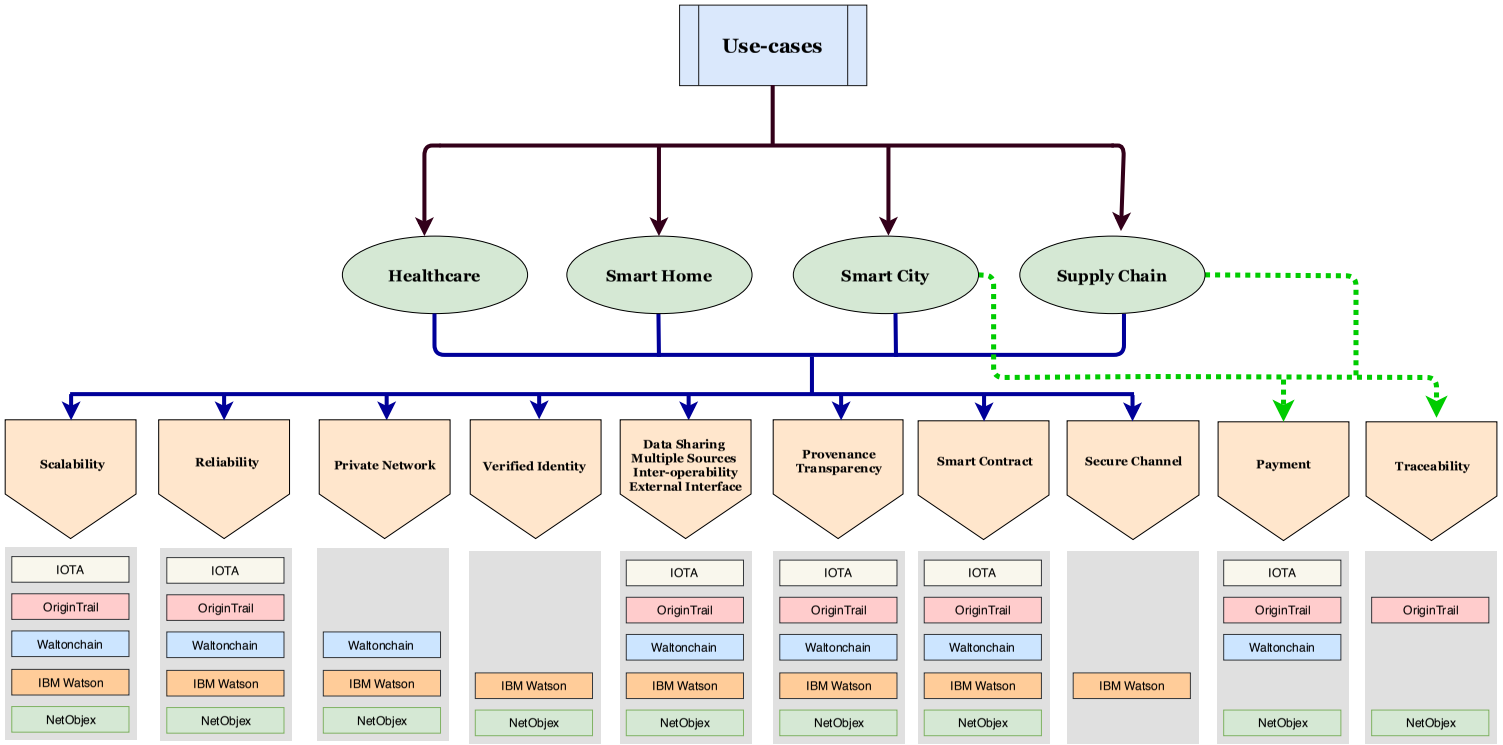


Figure 1: Blockchain platform