Chapter 52
Blockchain Technology for the Internet of Things Applications in Apparel Supply Chain Management

Kamalendu Pal
https://orcid.org/0000-0001-7158-6481
City, University of London, UK

ABSTRACT

Adoption of the internet of things (IoT) and blockchain technology opens new opportunities of business process automation in apparel supply chain management. The IoT technology helps to capture real-time information from different aspects of garment manufacturing activities by using radio frequency identification (RFID) tags and sensors. Blockchain technology is an emerging concept of computing that enable the decentralized and immutable storage of business transactions. In combination with IoT, blockchain technology can enable a broad range of application scenarios to enhance business value and trust. This chapter presents some of the blockchain-based IoT technology applications in apparel business processes. Moreover, the chapter provides a classification of threat models, which are considered by blockchain protocols in IoT networks. Finally, the chapter provides a taxonomy and a side-by-side comparison of the state-of-the-art methods towards secure and privacy-preserving blockchain technologies concerning the blockchain model, specific security goals, performance, and limitations.

INTRODUCTION

Apparel (i.e. textile and clothing) industry is an integral part of the world economy and society (Pal & Ul-Haque, 2020) (Pal, 2020). In recent decades, global apparel manufacturing businesses are inclined to worldwide activities due to the economic advantage of the globalization of product design and development (Pal, 2020a). In a typical textile and clothing supply chain is the sequence of organizations – their facilities, functions, and activities – that involved in producing and developing a product or service.

DOI: 10.4018/978-1-6684-7132-6.ch052

The sequence begins with raw materials purchase from selective suppliers and products are made at one or more manufacturing plants (Pal, 2019). Then these products are moved to intermediate collection points (e.g., warehouse, distribution centers) to store temporarily to move to next stage of supply chain and ultimately deliver the products to intermediate-users or retailers or customers (Pal, 2017) (Pal, 2019). The path from supplier to the customer can include several intermediaries – such as wholesalers, warehouse, and retailers, depending on the products and markets. Also, global apparel supply chains becoming increasingly heterogeneous and complicated due to a growing need for inter-organizational and intra-organizational connectedness, which is enabled by advances in modern technologies and tightly coupled business processes. Hence, information has been an important strategic asset in apparel business operational management. The apparel business networks are also using the information systems to monitor the supply chain activities ((Pal & Ul-Haque, 2020).

As a result, many global textile and clothing businesses are investing in new information and communication technology (ICT) to harness the smooth information sharing ability in supply chain operations (Pal & Ul-Haque, 2020). With the recent progress in Radio Frequency Identification (RFID) technology, low-cost wireless sensor hardwires, and world wide web technologies, the Internet of Things (IoT) advance has attracted attention in connecting global apparel business activities and sharing operational business information. These technologies promise to reshape the modus operandi of modern supply chains through enhanced data collection as well as information sharing and analysis between collaborating supply chain stakeholders. In this way, IoT technology supports the capability to connect and integrate both digital and physical business world. The process is quite simple: (i) collect data from real-world objects, (ii) communicate and aggregate those data into information, and (iii) present clear results to systems or users so that decisions can be made or object behaviour adapted.

Different research groups analysed IoT technology deployment-related issues in SCM and logistics (Atzori et al., 2018) (Gubbi et al., 2013). Particularly, a group of researchers reviewed the energy management in smart factories and concluded that IoT powered manufacturing can improve supply chain competitiveness through more effective tracking of the flow of materials, and leading to improvements in the effectiveness and efficiencies of important business processes (Shrouf et al., 2014). The other important characteristics of IoT-based systems (e.g. sharing precise and timely information related to production, quality assurance, distribution, and logistics) are also reported in the context of multi-party supply chains (Chen et al., 2014) (Cui, 2018) (Yan-e, 2011). Also, the use of IoT applications inside the production plant can increase the visibility of parts and processes, and by extension, using IoT devices along the supply chain can help to boost productivity, reduce operational costs, and enhance customer satisfaction (Deloitte, 2017).

Despite the increasing applicability of IoT applications in supply chains, there are many challenges for the use of this technology. For example, IoT-related technical issues experienced when operating at the ecosystem level, such as security, authenticity, confidentiality, and privacy of all stakeholders (Tzounis et al., 2017). Academics and practitioners consider privacy and security issues are mainly related to the vulnerability of IoT system applications. Existing security solutions are not well suited because current IoT devices may consume huge amounts of energy and often these devices need substantial information processing overhead (Dorri et al., 2017). Besides, problems such as physical tampering, hacking, and data theft might increase trust-related issues within apparel network information exchange business partners (Kshetri, 2017). Therefore IoT applications must be secure against external security attacks, in the perception layer, secure the aggregation of data in the network layer and offer particular protections that only authorized entities can access and change data in the application layer.