Chapter 58
Issues and Challenges (Privacy, Security, and Trust) in Blockchain-Based Applications

Siddharth M. Nair
Vellore Institute of Technology, Chennai, India

Varsha Ramesh
Vellore Institute of Technology, Chennai, India

Amit Kumar Tyagi
https://orcid.org/0000-0003-2657-8700
Vellore Institute of Technology, Chennai, India

ABSTRACT

The major issues and challenges in blockchain over internet of things are security, privacy, and usability. Confidentiality, authentication, and control are the challenges faced in security issue. Hence, this chapter will discuss the challenges and opportunities from the prospective of security and privacy of data in blockchain (with respect to security and privacy community point of view). Furthermore, the authors will provide some future trends that blockchain technology may adapt in the near future (in brief).

1. INTRODUCTION

Blockchain introduced the world's most famous cryptocurrency concept, bitcoin (Tomov, 2019). It is an improvement on the ideals of a peer to peer network and creates a universal data set which can be trusted by all users despite the fact that they do not trust each other. It creates a database or a record of transactions that are shared, trusted and protected, where stable and encrypted copies of data are saved on every node in the system. Financial incentives like native network tokens are applied onto the system to make it more immune to faults and collision.

DOI: 10.4018/978-1-6684-7132-6.ch058

Blockchain has been useful in other sectors of technology. For example, it has been implemented in IoT to improve security and efficiency of IoT based devices. For example, in the agriculture industry, research shows that Blockchain allows food to be tracked from farms to supermarkets in a few seconds. So, it helps in reducing illegal harvesting and shipping scams (Hackernoon, n.d.a). It is also used to keep tabs on overflowing commodities. This works on the principle that data tampering cannot take place using Blockchain, thereby making hacking difficult. Using Blockchain in IoT has its own issue. Data mining in Blockchain needs a large amount of computation and processing power. Most IoT devices do not have the required power to do so.

Blockchain is also hinted to be able to improve security and efficiency in cyber physical systems. For example, studies show that Blockchain can be used in autonomous automobile industry. A Blockchain based database can be used to store the identity information of newly created vehicles (Dorri, Steger, Kanhere et al, 2017). Thus, the information of newly created vehicles can be stored securely in an E-wallet. The data stored cannot be tampered with and will be cryptographically verified. This will enable the vehicle to communicate with a number of networks and thus pay bills, tolls, fines autonomously.

Blockchain technology has been used in social media and networks, to fix many issues. On social media, fake news spreads as quickly as good content. Blockchain helps in fighting fake news using its ledger system. Content and identification can be verified at any time. This also makes collection of data a lot simpler. Blockchain also makes it possible to track data and monitor user interaction with the content. This helps social media channels estimate the likes, shares and views more accurately.

In recent times, the popularity of crowdsourcing systems has increased massively despite the certain privacy issues and challenges faced by it. Blockchain based crowdsourcing systems were employed to solve the problem of small value transactions in crowdsourcing (Li et al., 2019). Similarly, the acquisition and computation of data using some sensing devices to share the gathered data, also known as crowdsensing has been growing in popularity in recent times. Blockchain, being a distributed database in which data cannot be tampered, has the right characteristics to improve the security of crowdsensing applications.Another important where Blockchain is used is the cloudlet (Xu et al., n.d.). Cloudlet is a group of computer systems designed to swiftly render cloud computing resources to the users to enhance the performance of multimedia applications. The security and integrity of the offloaded data that are processed by cloudlets have to be preserved especially with the increasing user requirements of migrating tasks. The characteristics of Blockchain prove to be favorable in these circumstances.

Blockchain is also used to improve security and trust in fog, edge and cloud computing. Fog computing is a decentralized computing foundation in which data, computation, storage and applications are placed some place between the cloud and the source of data. Fog computing has a distributed architecture and requires a technique to protect network resources and transactions. Similarly, edge is a distributed structure in which data is computed at the edge of the network where generation of data takes place instead of computing it in a centralized data processing repository.Cloud computing, is a technology that makes computing services like database, storage, software and analytics available on the internet. For these purposes, an equally distributed security structure is required. Blockchain is a distributed ledger in which data cannot be tampered. So, it creates distributed trust and security.

Note that many useful/ possibleapplications of blockchain have been discussed in **(Sawal et al., 2019)**. Hence, now the remaining part of this chapter is organized as:

- Section 2 discusses related work Blockchain technology and Blockchain enabled applications