Chapter 45
Perspectives of Blockchain in Cybersecurity:
Applications and Future Developments

Muath A. Obaidat
Center for Cybercrime Studies, City University of New York, USA

Joseph Brown
City University of New York, USA

ABSTRACT

In recent years, blockchain has emerged as a popular data structure for use in software solutions. However, its meteoric rise has not been without criticism. Blockchain has been the subject of intense discussion in the field of cybersecurity because of its structural characteristics, mainly the permanency and decentralization. However, the blockchain technology in this field has also received intense scrutiny and caused to raise questions, such as, Is the application of blockchain in the field simply a localized trend or a bait for investors, both without a hope for permanent game-changing solutions? and Is blockchain an architecture that will lead to lasting disruptions in cybersecurity? This chapter aims to provide a neutral overview of why blockchain has risen as a popular pivot in cybersecurity, its current applications in this field, and an evaluation of what the future holds for this technology given both its limitations and advantages.

INTRODUCTION

As an emergent technology, blockchain has been a crux of discussion and experimentation in many fields. One among these is cybersecurity - a fast-moving, ever-changing industry which is constantly at the mercy of changing norms. The blockchain technology did not emerge with cybersecurity solely in mind, but rather as a means of decentralizing data while maintaining trust between users. However, as blockchain grew in notability, its purpose expanded to academia and commerce, where it quickly

DOI: 10.4018/978-1-6684-7132-6.ch045

developed in the cybersecurity area as well because of its intrinsic characteristics, commonly cited as immutability and decentralization.

Cybersecurity is a field which demands evolution at a more frequent rate than its constituent industries. As other technological norms evolve in tandem, cybersecurity must evolve at a relative rate in order to ensure the safety of - or alternatives to - such norms. To adhere to both the ever-changing norms of technology as well as the constant race for improved soundness and convenience for security, cybersecurity remains a field which is constantly evolving. As new architectures and protocols enter the public consciousness, such concepts always find their way into the sphere of cybersecurity discussion and research. Can these concepts be utilized to improve security? What implications do such concepts have for the field? One of these concepts is blockchain. The spur in discussion and research about blockchain has largely been fueled by both a desire for innovation as well as changing logistical cybersecurity structures which have already been considered as standard, such as the client-server or third-party authentication models. Blockchain stands as a contrast to historical architectures and security methodologies, and thus has brought some renewed hopes for researchers and businesses for the future, while others remain skeptical of its applicability.

The introduction of any elements considered ground-breaking or game-changing into a field, brings its own problems. These elements do exist in isolation, but alongside an omnipresent race for innovation, notability, or attracting the attention of investment without care for the integrity of proposed solutions. In the past few years, blockchain has shifted from a once curious concept into a pivotal discussion point in the fields of software, computer science, and cybersecurity. The exponential growth in popularity of blockchain has drawn rigorous debate; some voices purport blockchain to be a universal solution for filling prior gaps in historical fields, while others believe blockchain is simply a passing fad. As mentioned above, in cybersecurity especially, blockchain has remained a hot button yet also a controversial topic.

This chapter aims to present an investigation into the place of blockchain within the current field of cybersecurity, and evaluate its possible presence in the field in the future. The organization of this chapter is broken into three sections as follows. The first section outlines the characteristics of blockchain as they pertain to cybersecurity, discussing both the advantages of the blockchain architecture as well as the limitations and liabilities that its implementation could propose. The second section uses the first as a springboard to both discuss and evaluate the most popular currently discussed applications of blockchain within the cybersecurity field. The third section discusses the future implications of what impact blockchain will have on the cybersecurity field; it discusses both what opportunities blockchain has created which may continue to be influential in the future, as well as what issues a blockchain-centric future for cybersecurity may create.

CHARACTERISTICS OF BLOCKCHAIN

The usages of blockchain within cybersecurity and other perpendicular fields such as finance, typically lean on the core architectural traits of blockchain rather than more tangential extrapolations of its functionalities. Possible usages of blockchain within the field which have been promoted both by studies and private firms have included digital identity management, including digital signatures which is a direct derivative of the inherent functionality of the data structure. There are typically five core architectural characteristics of blockchain: *decentralized, immutable, anonymous, cryptographically encrypted,* and