Blockchain for Distributed Systems Security

Edited by Sachin Shetty, Charles Kamhoua, and Laurent Njilla, Wiley-IEEE Computer Society Press, April 2019, ISBN 978-1-119-51960-7, hardcover, 352 pages

Reviewer: Mubashir Husain Rehmani

Historically, ledgers have been used to record transactions among different parties. These transactions contain information ranging from financial transactions to buying and selling of goods. Later, with the advent of computers, ledgers were automated and transactions were recorded using record keeping software such as databases and spread sheets. With the evolution of the Internet and related technologies, ledgers were made available online. However, traditionally, trusted third parties, like banks and intermediaries, are required to maintain these ledgers and to establish trust among different parties. Blockchain, in the absence of trusted third parties, permits communicating parties to interact with each other. Blockchain is a distributed and decentralized public ledger system used for maintaining the transactions record over several computers (Blockchain nodes). Blockchain has made its place in different application areas such as crypto currencies, supply chain management, and energy sectors, just to name a few.

This book on Blockchain for distributed systems security is one of the timely books available on this topic. It summarizes the research efforts done in the area of distributed systems security with particular emphasis on Blockchain. Experienced researchers who have vast experience in distributed systems security edited this book. Researchers who are working in this area of Blockchain security including post-graduate students will find this book useful. The topics covered in this book are interesting for readers in the area of Blockchain security and privacy. The main feature of this book is that it contains three chapters (chapters 4, 5, and 8) that are in fact top voted Blockchain research papers. These papers were voted at the Blockchain Connect Conference in 2019.

> This book on Blockchain for distributed systems security is one of the timely books available on this topic. It summarizes the research efforts done in the area of distributed systems security with particular emphasis on Blockchain.

This book has 14 chapters that are organized into four parts. The first part covers the basic topic of Blockchain. There are three chapters in this part. The first chapter introduces Blockchain, highlighting few Military Cyber Operations use cases. Consensus protocols serve as the heart of Blockchain. Considering their importance, a dedicated chapter discusses consensus protocols. The editors then move to the main theme of the book and provide the basics of attack surfaces in Blockchain. These three chapters build sufficient knowledge to the reader who is not acquainted with the knowledge of Blockchain and the basics of attacks in Blockchain.

In the second part of this book, the focus is on presenting Blockchain solutions for distributed systems security. In this part of the book, four chapters are included. The first chapter in this part (chapter 4) presents Blockchain-based cloud data provenance. In the second chapter in this part (chapter 5), Blockchain security and privacy in the context of automotive was discussed. In the next chapter (chapter 6), Internet of Things (IoT) security protection is considered by focusing on Blockchain based dynamic key management. The last chapter in this part (chapter 7) presents an information-sharing framework for Blockchain-enabled cyber security.

The third part of this book discusses Blockchain security. This part contains four chapters. Chapter 8 presents Blockchain security analysis. Chapter 9 discusses privacy in permissioned and permissionless Blockchain. Chapter 10 then presents distributed denial of service (DDoS) attacks and their countermeasures. The last chapter of this part, chapter 11, discusses a reputation-based paradigm to prevent digital currency misuse to launch attacks against mining pools.

The last part of this book, part four, discusses Blockchain implementation. This part of the book has three chapters. The first chapter in this part (chapter 12) presents private Blockchain configuration for improved IoT security. Chapter 13 discusses Blockchain evaluation platforms. An interesting aspect of this chapter is the Hyperledger Fabric example exercise, supported by example code available on github. Finally, chapter 14 provides the summary and discusses future works.

One of the main drawbacks of this book is the presence of redundant material, which reduces the readability of the book. For instance, part one of this book covers Blockchain introduction and basics. Later in other chapters, Blockchain basics are repeatedly provided (cf. chapter 10). In my opinion, the editors should have made some effort to remove this redundant material so that the presented material becomes more coherent and organized. Another drawback of this book is that the future directions mentioned in chapter 14 are not discussed in detail. Being a researcher in Blockchain, I was expecting more detail on future research directions. In my opinion, this book is more suitable for researchers and may not be suitable as a textbook alone. Another minor issue is that by looking at the metadata available on the publisher's website, we can find that there are 352 pages mentioned; however, the hardcopy of the book has 324 pages, which is not consistent with the information provided online. Nevertheless, these shortcomings do not undermine the timely contribution made by the editors in this active area of research.