Mastering Zero-knowledge Proofs

Practical study of security, scalability, and privacy in blockchain and modern systems

Dr. Amit Dua

Gaurav Kumar

www.bpbonline.com

First Edition 2024

ISBN: 978-93-55519-733

LIMITS OF LIABILITY AND DISCLAIMER OF WARRANTY

The information contained in this book is true to correct and the best of author's and publisher's knowledge. The author has made every effort to ensure the accuracy of these publications, but publisher cannot be held responsible for any loss or damage arising from any information in this book.

All trademarks referred to in the book are acknowledged as properties of their respective owners but BPB Publications cannot guarantee the accuracy of this information.

Dedicated to

My dear wife ***Nivedita*** *and my darling daughter* ***Dhriti***
The time I spent writing the book was meant for them
— Amit Dua

My beloved parents:
Anand Kumar *and* ***Sweta Kumar***
and my sister ***Riya Kumar***
— Gaurav Kumar

About the Authors

- **Dr. Amit Dua** is an Associate Professor in the Computer Science and Information Systems Department at BITS Pilani. He earned his Ph.D. from Thapar University, Patiala in 2014, specializing in Vehicular Ad hoc Networks and their security. Over the past eight years at BITS Pilani, Dr. Dua has taught courses on Blockchain Technology and Computer Networks to both undergraduate and postgraduate students.

  Dr. Dua has extensively researched both practical and fundamental topics, resulting in approximately 50 research publications in international journals and conferences. He holds a joint copyright for developing code that connects electronic health records on the Solana Network using homomorphic encryption.

  With support from the BITS Pilani incubation center, Dr. Dua founded Yushu Excellence Technologies Pvt Ltd in 2021. The company developed a ZKP-based solution, Pramaan, which provides authentication to maintain data privacy and holds an Indian patent for this innovation.

  Passionate about education, Dr. Dua works extensively with NGOs and schools to enhance the effectiveness of the education system. A seasoned writer, he has authored books on machine learning and its applications in education.

- **Gaurav Kumar** holds a degree in Computer Science from BITS Pilani, Pilani Campus. With multiple years of experience in the field of Blockchain, Gaurav has established himself as a proficient and knowledgeable professional in this rapidly evolving domain. In addition, he has specialized experience in the field of Zero-knowledge Proofs, which has become a focal point of his research and professional endeavours.

  Gaurav's contributions to the field are noteworthy. He has published a research paper in the field of blockchain, demonstrating his commitment to advancing knowledge and understanding of this transformative technology. His expertise and practical insights make him a valuable resource for anyone looking to delve deeper into the intricacies of blockchain and Zero-knowledge Proofs.

  Gaurav's passion for technology and innovation drives him to continuously explore new frontiers in digital security and privacy. This book is a testament to his dedication and expertise, aimed at providing readers with a comprehensive understanding of Zero-knowledge Proofs and their applications.

About the Reviewers

- **Anurag Dashputre** is a Certified Blockchain Solution Architect from Blockchain Training Alliance. He is an accomplished Solution Architect with 18 years of experience in the IT industry.

  He has extensive experience in handling complex projects in domains such as AI/ML, Blockchain, Healthcare, Network Management, and Storage Virtualization, working alongside teams spread across the USA, UK, France, China and India.

  He enjoys working as an educator and contributes to open-source projects in his free time. He currently works with Reliance Jio as a Senior Blockchain Solution Architect.

- **Dr. Jagreet Kaur** is a leading figure in data science, with a distinguished career spanning over 18 years. Currently, she serves as the Chief Operating Officer at Xenonstack, while holding dual leadership roles as Chief AI Officer and Chief Operating Officer at Akira AI.

  Dr. Kaur's expertise encompasses a wide range of fields, including Database Security, Data Warehousing, Data Science, and Artificial Intelligence. Her academic journey began with a B.Tech degree and culminated in a Ph.D. focused on "**Artificial Intelligence Based Analytical Platform for Predictive Analysis in Health Care**." Driven by a passion for research, she actively contributes to the field through publications in renowned journals like Springer and participation as a reviewer.

  Throughout her career, Dr. Kaur has held esteemed positions at academic institutions like Khalsa College for Women, Guru Nanak Dev Engineering College, Punjab University, and Chandigarh College of Engineering and Technology. She is a prolific author, having published over 18 research papers and two books on AI and Hyperautomation.

  Dr. Kaur's dedication extends beyond technical expertise. She champions ethical and responsible applications of Generative AI, exploring its potential in medical image synthesis, creative content generation, natural language processing, and anomaly detection. Her commitment to pushing the boundaries of this technology is evident in her ongoing efforts to solve real-world challenges with innovative solutions.

Acknowledgements

We are deeply grateful to many people who contributed to the completion of this book on Mastering Zero-knowledge Proofs.

First and foremost, we would like to extend our heartfelt thanks to BPB Publications for believing in this project and bringing it to fruition. Their support and dedication were instrumental in the successful completion of this book.

I, Dr. Amit Dua, wish to sincerely thank my parents, Bharat Bhushan Dua and Anita Dua, for their endless patience, understanding, and support. Your love and encouragement have been my pillars of strength.

My heart is filled with gratitude for Mr. Ashish Taneja and Vishal, who have worked with me to develop practical solutions using Zero-knowledge Proof. The discussion with them gave me more profound clarity about topics associated with ZKP.

I, Gaurav Kumar, would like to express my deepest gratitude to my parents, Anand Kumar and Sweta Kumar, and my sister, Riya Kumar, for their unwavering support and encouragement throughout this journey. Your belief in me has been a constant source of inspiration.

Thank you all for your contributions and support.

Preface

In the ever-evolving landscape of digital technology, security and privacy have become paramount concerns. **Zero-knowledge Proofs (ZKP)** have emerged as a groundbreaking solution, enabling the verification of information without revealing the information itself. This revolutionary concept holds immense potential for transforming various sectors, from blockchain and cryptography to identity verification and decentralized finance.

We, Dr. Amit Dua and Gaurav Kumar, are excited to present this comprehensive guide on Zero-knowledge Proofs, a field where we have established our authority through extensive research and practical experience. This book is crafted to serve as a definitive resource for entrepreneurs, researchers, and professionals who seek to deepen their understanding of security and privacy in the digital age.

The contents of this book are meticulously structured to take you on a journey from the foundational principles of blockchain technology to the cutting-edge developments in Zero-knowledge Proofs. Here is a glimpse of what you can expect:

Chapter 1: Introduction to Blockchain Technology – Explore the basics of blockchain technology, its components, and its significance in the digital world.

Chapter 2: Introduction to Zero-knowledge Proofs – Delve into the fundamental concepts of Zero-knowledge Proofs, including their history, importance, and basic types.

Chapter 3: Introduction to SNARKS – Understand the concept of Succinct Non-Interactive Arguments of Knowledge (SNARKs) and their role in ZKP.

Chapter 4: SNARK Construction: Non-interactive Proof Building – Learn the initial steps in constructing SNARKs, focusing on the theoretical framework and mathematical foundations.

Chapter 5: Advanced SNARK Paradigms and Techniques – Continue the construction process with practical examples and detailed explanations of SNARK implementation.

Chapter 6: SNARK versus STARK – Compare SNARKs with Scalable Transparent Arguments of Knowledge (STARKs), highlighting their differences, advantages, and use cases.

Chapter 7: SNARKs In-depth and PLONK – Dive into the details of PLONK, a universal SNARK, and understand its significance and applications.

Chapter 8: Zero-Knowledge Virtual Machines – Explore the concept of **Zero-Knowledge Virtual Machines (ZKVMs)** and their potential to revolutionize computation and privacy.

Chapter 9: ZK-Rollups: Scalability Meets Privacy – Scalability Meets Privacy- Learn about ZK-Rollups, a layer 2 scaling solution for blockchains, and how they enhance scalability while maintaining privacy.

Chapter 10: Conceptualizing ZK-EVM in Ethereum – Discover the integration of Zero-knowledge Proofs with the **Ethereum Virtual Machine (EVM)** and its implications for smart contracts.

Chapter 11: ZK Swaps: Revolutionizing Decentralized Exchanges – Understand how ZK Swaps leverage ZKP to improve privacy and security in decentralized exchanges.

Chapter 12: Zero-Knowledge Identity – Examine the application of Zero-knowledge Proofs in identity verification and management systems.

Chapter 13: Challenges and Limitations of Zero-knowledge Proofs – Acknowledge the current challenges and limitations of implementing Zero-knowledge Proofs in various contexts.

Chapter 14: Ongoing Research and Development in Zero-knowledge Proofs – Stay updated on the latest research and advancements in the field of Zero-knowledge Proofs.

Chapter 15: Real-world Applications of Zero-knowledge Proofs – Explore various real-world applications of ZKP, showcasing its potential across different industries.

Our goal is to equip you with not only the theoretical knowledge but also the practical insights necessary to leverage ZKP in real-world applications. Whether you are an entrepreneur looking to implement cutting-edge security measures, a researcher delving into advanced cryptographic techniques, or a professional in the tech industry aiming to stay ahead of the curve, this book is designed with your needs in mind.

Published by BPB Publications, this book is the culmination of our dedication and passion for advancing the field of Zero-knowledge Proofs. We hope that it will serve as a valuable tool in your professional journey and inspire further innovations in the realm of digital security and privacy.

Thank you for embarking on this journey with us. We look forward to the advancements and breakthroughs that you, our readers, will achieve with the knowledge and insights gained from this book.

Coloured Images

Please follow the link to download the
Coloured Images of the book:

https://rebrand.ly/18a93f

We have code bundles from our rich catalogue of books and videos available at **https://github.com/bpbpublications**. Check them out!

Errata

We take immense pride in our work at BPB Publications and follow best practices to ensure the accuracy of our content to provide with an indulging reading experience to our subscribers. Our readers are our mirrors, and we use their inputs to reflect and improve upon human errors, if any, that may have occurred during the publishing processes involved. To let us maintain the quality and help us reach out to any readers who might be having difficulties due to any unforeseen errors, please write to us at :

errata@bpbonline.com

Your support, suggestions and feedbacks are highly appreciated by the BPB Publications' Family.

Piracy

If you come across any illegal copies of our works in any form on the internet, we would be grateful if you would provide us with the location address or website name. Please contact us at **business@bpbonline.com** with a link to the material.

If you are interested in becoming an author

If there is a topic that you have expertise in, and you are interested in either writing or contributing to a book, please visit **www.bpbonline.com**. We have worked with thousands of developers and tech professionals, just like you, to help them share their insights with the global tech community. You can make a general application, apply for a specific hot topic that we are recruiting an author for, or submit your own idea.

Reviews

Please leave a review. Once you have read and used this book, why not leave a review on the site that you purchased it from? Potential readers can then see and use your unbiased opinion to make purchase decisions. We at BPB can understand what you think about our products, and our authors can see your feedback on their book. Thank you!

For more information about BPB, please visit **www.bpbonline.com**.

Join our book's Discord space

Join the book's Discord Workspace for Latest updates, Offers, Tech happenings around the world, New Release and Sessions with the Authors:

https://discord.bpbonline.com

Table of Contents

Chapter 1
Introduction to Blockchain Technology

Introduction

A blockchain is a distributed database that keeps track of a growing list of ordered records known as blocks. Each block has a timestamp and a link to the previous block, forming a chain of blocks. This structure enables the database to be securely shared among multiple parties without needing centralized authority.

The data on a blockchain is typically organized into a ledger, which is a record of all transactions that have occurred on the network. Each transaction is a digitally signed record of the transfer of value between two or more parties.

One of the most important characteristics of a blockchain is that it is decentralized, which means it is not controlled by a single authority. Instead, the network is maintained by a network of participating nodes, each of which holds a copy of the entire ledger. This decentralized structure provides greater security and transparency because it is much more difficult for a single entity to manipulate or censor the data on the blockchain.

Structure

This chapter will cover the following topics:

- An overview of Blockchain
- The history

- Types of Blockchain networks
- Basic introduction to cryptography and ledger technology
- Why do we need Blockchain
- Components of Blockchain
- How does Blockchain function
- Benefits of Blockchain

Objectives

The objective of this chapter is to provide readers with a comprehensive introduction to blockchain technology. It covers the fundamental concepts of blockchain, including its definition, the role of cryptography and ledger technology, and the difference between centralized and decentralized computing. The chapter also explores the components of blockchain, its functioning, and the historical background. Furthermore, it discusses various types of blockchain networks, such as public, private, and permissioned, along with real-life examples. By the end of this chapter, readers will have a solid understanding of the key principles and components of blockchain technology.

An overview of Blockchain

A blockchain is a distributed software network that functions as both a digital ledger and a means of transferring assets in a secure and direct manner. Blockchain is a technology that allows for the digital exchange of units of value, much like the internet is a technology that allows for the flow of information online. On a blockchain network, anything, including money, real estate, and votes, can be tokenized, stored, and exchanged.

The Bitcoin blockchain, a secure and censorship-resistant peer-to-peer electronic payment system, was the first application of blockchain technology to appear in 2009. Since anyone can access Bitcoin, it is an example of an open or permissionless blockchain.

Blockchain technology is available in a variety of forms today. Some blockchains have been designed to meet the needs of a small number of users with restricted network access. These are examples of permissioned or private blockchains.

Blockchain technology provides a single version of the truth—a network state that is entirely transparent and displayed in real-time for the benefit of all participants—along with the secure transfer of value and a permanent forensic record of transactions.

Whatever blockchain protocol is used, it has the potential to transform centuries-old corporate practices, pave the way for greater levels of government legitimacy, and open up new opportunities for ordinary people.

Blockchain is a game-changing technology that has the potential to transform the way we do business, interact with one another, and even govern ourselves. It is a distributed database that enables multiple parties to securely store and transfer data without the need for a centralized authority or intermediary.

The concept of a *distributed ledger* is pivotal to Blockchain. A database that is maintained and updated by a network of computers as opposed to a single central entity. This means that the ledger's information is decentralized, transparent, and immutable.

The use of cryptographic techniques to secure the information on the ledger is a key feature of blockchain. These techniques enable the parties involved in a transaction to validate the information's authenticity and integrity without revealing the underlying data itself. This is *Zero-knowledge Proof*.

We will provide a brief overview of blockchain technology and its potential applications in this chapter. We will also discuss the concept of Zero-knowledge Proof and its role in enabling secure and private blockchain transactions.

Blockchain is a new technology, so there is still a lot to learn and understand about its capabilities and limitations. In this chapter, we'll delve deeper into the technical details of blockchain and Zero-knowledge Proof, as well as look at some of the technology's potential applications and challenges.

The distributed nature of blockchain is one of its most important characteristics. Instead of relying on a central authority or intermediary to manage and maintain the ledger, the ledger is distributed across the blockchain network of computers. This means there is no single point of failure, and the ledger is impervious to tampering or censorship.

The network uses a consensus mechanism to agree on the state of the ledger in order to maintain its integrity. This usually entails a complex process of verifying transactions and adding them to the ledger in a difficult-to-reverse manner. This ensures that once a transaction has been added to the ledger, it cannot be changed or deleted without the network's approval.

Another important aspect of blockchain is the use of cryptography to secure the data on the ledger. This entails using digital signatures, hash functions, and other cryptographic techniques to validate the authenticity and integrity of the information without revealing the underlying data.

This is where proof of zero knowledge comes in. A Zero-knowledge Proof is a cryptographic technique that allows one party (the prover) to demonstrate to another (the verifier) that they have certain information without revealing the information itself. This allows the parties involved in a transaction to verify the transaction's authenticity and integrity without revealing the underlying data to each other or a third party.

One of the potential applications of blockchain and Zero-knowledge Proof is in the financial industry. It is possible to create a secure and transparent system for transferring value between parties without the need for a central authority or intermediary by utilizing a distributed ledger and cryptographic techniques. This has the potential to lower the cost and complexity of financial transactions while also increasing their security and privacy.

Another possible use for blockchain is in supply chain management. Using a distributed ledger, it is possible to create a transparent and immutable record of the provenance and movement of goods throughout the supply chain. This could improve supply chain operations' efficiency and transparency while lowering the risk of fraud and counterfeiting.

However, there are drawbacks and limitations to using blockchain and Zero-knowledge Proof. Scalability is one of the most difficult challenges. As the network grows and more transactions are added to the ledger, maintaining the distributed nature of the ledger and network security becomes increasingly difficult. Researchers and developers are currently working on this issue, but it remains a significant challenge.

Another issue is regulatory compliance. Governments and regulators are struggling to keep up with the evolution of blockchain and Zero-knowledge Proof technology and develop appropriate frameworks to govern their use. This is an ongoing process, and it is likely that debate and discussion about the appropriate role of regulation in the blockchain space will continue.

To summarize, blockchain and Zero-knowledge Proof are promising technologies that have the potential to revolutionize the way we do business and interact with one another. While there are challenges and limitations to their use, there is no doubt that these technologies have the potential to benefit a wide range of industries and applications. We can expect to see continued growth and development in this exciting area of technology in the coming years.

In recent years, blockchain technology has made headlines as a revolutionary new way to securely and transparently manage digital transactions. A blockchain, at its core, is a distributed database that allows multiple parties to securely add and verify data without needing central authority.

One of the most important characteristics of blockchain technology is its ability to provide verifiable, tamper-evident transaction records. This is made possible through the use of cryptographic techniques such as digital signatures and hashes, which allow each network participant to validate the authenticity and integrity of the data on the blockchain.

We will provide a high-level overview of blockchain technology and its key components in this chapter. We will also discuss some of the challenges and limitations of existing blockchain systems, as well as how **Zero-knowledge Proof** (**ZKP**) can help to address these issues.

Figure 1.1 summarizes the above discussion on the overview of blockchain technology:

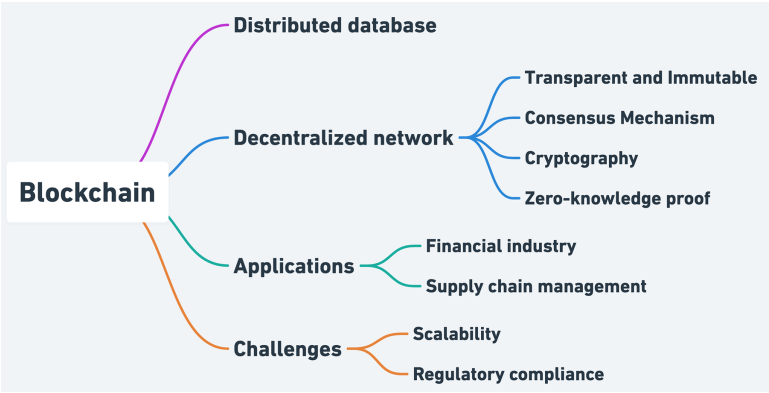

Figure 1.1: *Overview of Blockchain Technology*

The history

Blockchain's history is both fascinating and complex. It all started in 2009, when a person or group of people using the pseudonym *Satoshi Nakamoto* created the first cryptocurrency, Bitcoin.

Prior to Bitcoin, several attempts were made to create digital currencies, but they all ran into the same issue: the so-called **double spending** problem, in which a digital currency could be easily copied and spent multiple times.

Bitcoin addressed this issue by recording transactions on a decentralized ledger known as the Blockchain. This ledger is kept up to date by a network of computers known as nodes, each of which has a copy of the entire transaction history.

When a new transaction is made, the network's nodes validate it and add it to the blockchain. This ensures that each transaction can only be used once and eliminates the need for a central authority to monitor the process.

Because of Bitcoin's success, many other cryptocurrencies have been created, and the use of blockchain technology has expanded beyond just currencies. It's now used in a wide range of industries, including supply chain management, voting systems, and even music and art.