Future of Business and Finance

Ken Huang · Dyma Budorin ·
Lisa JY Tan · Winston Ma ·
Zhijun William Zhang *Editors*

A Comprehensive Guide for Web3 Security

From Technology, Economic and Legal Aspects

Springer

Future of Business and Finance

The Future of Business and Finance book series features professional works aimed at defining, analyzing, and charting the future trends in these fields. The focus is mainly on strategic directions, technological advances, challenges and solutions which may affect the way we do business tomorrow, including the future of sustainability and governance practices. Mainly written by practitioners, consultants and academic thinkers, the books are intended to spark and inform further discussions and developments.

Ken Huang • Dyma Budorin •
Lisa JY Tan • Winston Ma •
Zhijun William Zhang
Editors

A Comprehensive Guide for Web3 Security

From Technology, Economic and Legal Aspects

Springer

Editors
Ken Huang
DistributedApps.AI
Fairfax, VA, USA

Dyma Budorin
Hacken
Lisbon, Portugal

Lisa JY Tan
Economics Design
Singapore, Singapore

Winston Ma
CloudTree Ventures
New York, NY, USA

Zhijun William Zhang
BIS Innovation Hub Nordic Centre
Stockholm, Sweden

ISSN 2662-2467 ISSN 2662-2475 (electronic)
Future of Business and Finance
ISBN 978-3-031-39287-0 ISBN 978-3-031-39288-7 (eBook)
https://doi.org/10.1007/978-3-031-39288-7

The use of general descriptive names, registered names, trademarks, service marks, etc. in this publication does not imply, even in the absence of a specific statement, that such names are exempt from the relevant protective laws and regulations and therefore free for general use.
The publisher, the authors, and the editors are safe to assume that the advice and information in this book are believed to be true and accurate at the date of publication. Neither the publisher nor the authors or the editors give a warranty, expressed or implied, with respect to the material contained herein or for any errors or omissions that may have been made. The publisher remains neutral with regard to jurisdictional claims in published maps and institutional affiliations.

This Springer imprint is published by the registered company Springer Nature Switzerland AG
The registered company address is: Gewerbestrasse 11, 6330 Cham, Switzerland

Paper in this product is recyclable.

This book is devoted to all those who dare to explore the uncharted territories of the digital world—the pioneers, innovators, and visionaries whose passion and tenacity are shaping the evolution of the Web3 landscape.
Web3 security is not just an optional element; it is a fundamental necessity in this digital age. It is the backbone that supports the integrity, trust, and resilience of our evolving digital ecosystem. Hence, this book is dedicated to all those who understand the importance of this critical field and are committed to enhancing it—the developers, researchers, policymakers, and educators.
To every reader who picks up this book to deepen their understanding of Web3 security, may the insights you gain empower you to safeguard our shared digital space and contribute to a secure, trustworthy digital future for all.
Finally, this work pays homage to the spirit of collaboration and shared knowledge that is integral to the growth of the Web3 community. In an era marked by rapid technological advancement, let us continue to learn from each other, challenge each

other, and together, shape the future of the Internet. May this book serve as a beacon on that journey. We would like to end this dedication with the following poem

To pioneers and innovators, bold and bright,
In the realm of Web3, you ignite the light.
Security at its core, a vital creed,
To protect and serve, in every deed.
Readers, may this book guide your flight,
In the digital world, vast and bright.
Together we learn, in this shared space,
Shaping the Internet, at our own pace.

Foreword 1

As the Co-founder and Chief Executive Officer of the Cloud Security Alliance, I am delighted to introduce this comprehensive and insightful book on Web3 security, authored by Ken Huang and his esteemed editorial team, who have brought together their wealth of knowledge and experience in the rapidly evolving world of blockchain and digital assets. I have had the pleasure of knowing Ken for many years, and I am well aware of his contributions to the blockchain industry, including his work on authoring and reviewing several blockchain-related white papers for the Cloud Security Alliance publication such as Crypto Asset Exchange Guides, Blockchains in the Quantum Era, and The Use of Blockchain in Healthcare.

In the era of Web3, security is of paramount importance as we witness a fundamental shift in how the internet operates and how value is exchanged. The decentralized nature of Web3 technologies brings new opportunities for innovation, collaboration, and economic growth. However, it also introduces new challenges and potential risks that must be addressed to ensure the safety and success of this digital revolution.

Web3 security is essential because it protects the underlying infrastructure that supports decentralized applications, digital assets, and user data. Ensuring the integrity, confidentiality, and availability of these systems is vital to building trust and fostering widespread adoption. As more individuals, businesses, and governments rely on Web3 technologies for various use cases, the need for robust security measures becomes increasingly critical. A failure to prioritize security could lead to significant financial losses, reputational damage, and a setback in the progress of the Web3 movement.

This book is an essential read for anyone involved in the development, implementation, or management of Web3 applications, as it thoroughly explores the foundational components of Web3 security, the specific concerns for enterprise Web3 application development, and recent Web3 project debacles and legal implications. The authors have meticulously examined various aspects of blockchain security, including the C.I.A properties of Blockchain, chain security, wallet security, smart contract security, tokenomics model creation, token economy security, DevSecOps for Web3, Web3 security analytics, data authenticity, and permissioned blockchain security.

As we continue to witness the growing adoption of blockchain technologies and the expansion of the Web3 ecosystem, it is imperative to prioritize security and ensure that new applications and systems are developed with a strong foundation. I am confident that this book will contribute significantly to the understanding and implementation of robust security measures in the Web3 space and help drive the industry forward.

I commend Ken Huang and his team for their dedication and expertise in creating this comprehensive guide to Web3 security, and I am certain that it will be an indispensable resource for all stakeholders in the blockchain and digital asset community.

CEO, Cloud Security Alliance Jim Reavis
May 4, 2023

Foreword 2

As the Vice President of The Hong Kong University of Science and Technology and the Chief Scientific Advisor of the Institute of WEB3 Hong Kong, the authoritative organization representing Web3 in the region, I am delighted to present "A Comprehensive Guide for Web3 Security: Exploring Technology, Economic, and Legal Aspects," masterfully edited by Ken Huang and his distinguished editorial team. This book emerges as a crucial and all-encompassing resource amid the intricacies and challenges of Web3 security, marking a pivotal moment in the evolution of the Internet's next generation.

The advent of Web3 signifies a transformative shift in the way we interact with the online world, reimagining business models and unlocking unprecedented value for the global economy. Recognizing the immense potential of Web3, Hong Kong established the Institute of WEB3 in April 2023. Our mission is to collaborate with local government and businesses to accelerate technological innovation, attract top talent, and firmly establish Hong Kong as a premier hub for Web3 development. By harnessing the power of blockchain technology, smart contracts, and decentralized applications, Web3 has the potential to reshape industries and empower individuals with greater control over their digital identities and assets.

The authors of "A Comprehensive Guide for Web3 Security" have meticulously assembled an impressive collection of chapters, drawing upon their vast experience and expertise in the field. By addressing the multifaceted aspects of Web3 security, they provide readers with an in-depth understanding of the technological, economic, and legal dimensions at play. Their thorough analysis and practical insights will not only benefit professionals and researchers but also serve as a vital resource for policymakers, entrepreneurs, and enthusiasts seeking to navigate the complex world of Web3. The book is thoughtfully structured into three parts, each addressing a different dimension of Web3 security.

In the first part, the authors delve into the foundational components that underpin Web3 security. Through a thorough examination of topics such as the C.I.A. (Confidentiality, Integrity, and Availability) properties of the blockchain, chain security, wallet security, smart contract security, and token economics model creation, readers will gain a solid understanding of the building blocks that constitute a secure Web3 environment.

Transitioning to the second part of the book, the focus shifts toward the unique security concerns enterprises face when developing Web3 applications. The authors explore critical subjects such as DevSecOps for Web3, Web3 security analytics, data authenticity, and permissioned blockchain security, making this section indispensable for businesses navigating the complex landscape of Web3 application security.

In the final part of the book, the authors examine the intersection of Web3 security with financial integrity and national security. Through engaging crypto legal case studies and discussions on terrorist financing, war crimes, and crypto geopolitics, this section shines a light on the broader implications of Web3 security on the global stage.

The diverse and accomplished group of contributors to this book brings together a unique blend of expertise in the realm of Web3 security, offering readers a comprehensive and multidisciplinary perspective on this complex and rapidly evolving subject.

In today's world, where digital technologies are transforming industries and reshaping societies, the importance of understanding and securing the Web3 landscape cannot be overstated. This book is an invaluable resource for developers, entrepreneurs, policymakers, and anyone with an interest in the future of the Internet.

As we embark on this exciting journey into the next generation of the Internet, I am confident that "A Comprehensive Guide for Web3 Security: From Technology, Economic, and Legal Aspects" will serve as a trusted guide for all who seek to navigate the challenges and opportunities that lie ahead. The insights and knowledge contained within these pages are an essential addition to the literature on Web3 security and will undoubtedly contribute to the growth and success of this promising new frontier.

VP and Professor, The Hong Kong University of
Science and Technology
Institute of WEB3 Hong Kong
Hong Kong, Hong Kong, China
May 15, 2023

Wang Yang

Foreword 3

The rapid growth of the decentralized digital economy, powered by Web3, blockchain technology, and digital assets, is transforming how we interact with our financial systems. However, high-profile failures and substantial financial losses have highlighted the need for a comprehensive understanding of the security challenges and concerns that accompany these technologies. “A Comprehensive Guide for Web3 Security: From Technology, Economic and Legal Aspects” brings together expert knowledge from various disciplines to provide a holistic perspective on the multifaceted security challenges in the world of Web3 and digital assets.

By combining theoretical knowledge with real-world examples and case studies, the book presents a comprehensive and accessible resource for readers of all backgrounds and levels of expertise.

As digital assets become an integral part of the global financial landscape, it is essential to ensure the security, stability, and trustworthiness of the underlying technologies and platforms. “A Comprehensive Guide for Web3 Security: From Technology, Economic and Legal Aspects” serves as a testament to the importance of collaboration, innovation, and vigilance in fostering a secure, trustworthy, and vibrant digital asset ecosystem. I invite you to join the authors in this exciting and transformative journey while exploring the world of Web3 security and contributing to the ongoing development of a secure, resilient, and prosperous Web3 ecosystem.

CISO, World Bank
Washington, DC, USA

Clay Lin

Foreword 4

I am honored to write the foreword for the upcoming book “A Comprehensive Guide for Web3 Security: From Technology, Economic, and Legal Aspects,” edited by Ken Huang and his team of esteemed co-editors. During my tenure at DTCC, I had the pleasure of working with Ken on the Cloud Security Alliance white paper on Crypto-Asset Exchange Security Guidelines in 2021 which affords me the opportunity to attest to his expertise in the field of blockchain security. I also had the pleasure of reading Ken Huang’s previous book on “Blockchain and Web3,” which has been named one of the six must-read books of 2023 by TechTarget. This further attests to Ken’s expertise and thought leadership in the field of blockchain technology and Web3 security. I am excited to see how Ken and his team of esteemed co-editors have expanded on this knowledge in their latest work, “A Comprehensive Guide for Web3 Security: From Technology, Economic, and Legal Aspects.” With the rapid evolution of Web3 technology and the growing need for secure and decentralized applications, this book is sure to be an invaluable resource for anyone interested in this exciting field. As a chief editor, Ken has gathered an impressive group of experts to provide a comprehensive overview of Web3 security. With chapters covering topics such as DevSecOps for Web3, wallet security, token economic security, smart contract security, data authenticity, and legal and regulatory concerns, this book offers practical advice and thought-provoking inspirations and advice to help readers navigate the complex world of Web3 security. The readers will gain a holistic understanding of the Web3 landscape and the challenges and opportunities that lie ahead.

As someone who has been involved in the blockchain space for several years across multiple industries that include fintech, energy, banking, and supply chain, I believe that this book is an essential resource for anyone looking to stay ahead of the curve when it comes to Web3 security. With contributions from some of the most respected experts in the field, this book is sure to provide invaluable insights and actionable advice.

I highly recommend “A Comprehensive Guide for Web3 Security: From Technology, Economic, and Legal Aspects” to anyone looking to deepen their understanding of this rapidly evolving field. Whether you are a developer, investor, or simply interested in the potential of blockchain technology, this book is sure to be an indispensable resource.

SVP, Head of Innovation Strategy & Research, Truist Bank Jyoti Ponnapalli
Dallas, USA
May 2023

Preface

In the wake of the dramatic implosion of cryptocurrency exchange FTX, crypto trading company Alameda Research, and numerous other high-profile failures within the blockchain and Web3 sectors in 2022, the security and regulation of Web3, cryptocurrency, and blockchain projects have taken center stage. Over $3 billion in losses were attributed to hacks alone, while other incidents led to cumulative losses of well over $44 billion. These alarming figures underscore the pressing need for a comprehensive, in-depth analysis of the security issues surrounding these technologies.

Meanwhile, the rapidly evolving world of decentralized finance and digital assets is profoundly reshaping the way we interact, transact, and engage with our financial systems. As blockchain technology matures and Web3 applications gain traction, there is a growing need for comprehensive understanding and guidance on the various aspects of this complex ecosystem. Recognizing these shifts, the necessity of this book lies in its aim to provide a holistic perspective on the multifaceted security challenges and concerns that arise in the world of Web3 and digital assets, offering valuable insights, practical solutions, and forward-looking discussions.

By addressing the security concerns that have arisen from high-profile failures and their subsequent massive financial losses, this book seeks to create a solid foundation for stakeholders to better understand the risks and complexities involved in Web3 and digital asset technologies. The goal is to empower developers, investors, regulators, and end-users with the knowledge and tools needed to navigate the rapidly changing landscape of decentralized finance and contribute to the ongoing development of a secure, resilient, and prosperous Web3 ecosystem.

In an era where digital assets are increasingly becoming an integral part of the global financial landscape, it is essential to ensure the security, stability, and trustworthiness of the underlying technologies and platforms. To that end, this book brings together expert knowledge from various disciplines, including cryptography, software development, regulatory compliance, and risk management, to provide a comprehensive resource for all stakeholders in the Web3 and digital asset space.

The book is structured into three parts: Part I: Web3 Security Essentials, Part II: Security Concerns for Enterprise Web3 Application Development, and Part III:

Financial Integrity and National Security. Each part delves into the critical aspects of Web3 security, addressing the unique challenges and opportunities associated with this new paradigm.

Part I: Web3 Security Essentials
The first part of the book provides an essential foundation for understanding the security challenges in the Web3 ecosystem. It covers a wide range of topics, including the core principles of blockchain security, smart contract security, wallet security, and the role of decentralized identity in the Web3 space. Additionally, the section discusses the security risks associated with DeFi applications and the importance of on-chain governance for ensuring the stability and resilience of decentralized platforms.

Part I serves as a solid foundation for readers who are new to the world of Web3, as well as those who are already familiar with the space but wish to deepen their understanding of the fundamental security principles and best practices.

Part II: Security Concerns for Enterprise Web3 Application Development
As Web3 applications increasingly find their way into the enterprise realm, the need for robust security practices becomes even more critical. Part II of the book addresses the specific security concerns related to enterprise Web3 application development, including the adoption of DevSecOps, the role of on-chain security analytics and monitoring, ensuring data authenticity through blockchain oracles, and the unique security considerations of permissioned blockchains.

Part II offers valuable insights for enterprise decision-makers, developers, and security professionals who are tasked with implementing Web3 solutions within their organizations. It provides practical guidance on how to navigate the complex landscape of enterprise Web3 security, and it equips readers with the tools and knowledge needed to build secure, resilient, and trustworthy applications.

Part III: Financial Integrity and National Security
The final part of the book explores the complex intersection of cryptocurrency, financial integrity, and national security. It examines the implications of major legal case studies, terrorist financing, war crimes, and crypto geopolitics in the world of digital assets. This section emphasizes the importance of understanding and adapting to the rapidly changing regulatory landscape, as well as the need for best practices in crypto-based fundraising, sanctions compliance, and anti-financial-crime controls.

As the world of digital assets becomes increasingly intertwined with global finance and geopolitics, it is vital for all stakeholders in the crypto space to stay informed and prepared for the challenges that lie ahead. Part III provides readers with a comprehensive understanding of the issues surrounding financial integrity and national security in the context of Web3 and digital assets, enabling them to navigate the evolving landscape with confidence and foresight.

Throughout the book, the authors draw on their extensive experience and expertise in the field of Web3 security, offering valuable insights, practical solutions, and thought-provoking discussions. By combining theoretical knowledge with real-world examples and case studies, the book presents a comprehensive and accessible resource for readers of all backgrounds and levels of expertise.

This book is more than just a guide to the technical aspects of Web3 security; it is a testament to the importance of collaboration, innovation, and vigilance in fostering a secure, trustworthy, and vibrant digital asset ecosystem. As we move forward into the era of decentralized finance and Web3 applications, it is crucial for all stakeholders—including developers, investors, regulators, and end-users—to embrace a culture of security, transparency, and responsibility.

In conclusion, this book is a vital resource for anyone interested in understanding the complex landscape of Web3 security and its implications for the future of the digital economy. Whether you are a seasoned professional in the field of blockchain technology or a curious newcomer seeking to learn more about the world of digital assets, this book provides a comprehensive and engaging exploration of the challenges and opportunities that lie ahead.

As you embark on this journey through the world of Web3 security, we hope you will find the information, insights, and guidance provided in this book to be both informative and inspiring. Our goal is to empower you with the knowledge and tools needed to navigate the rapidly evolving landscape of decentralized finance and digital assets and to contribute to the ongoing development of a secure, resilient, and prosperous Web3 ecosystem.

We are confident that by working together, sharing our expertise, and embracing the principles of collaboration, innovation, and responsible stewardship, we can build a brighter future for the decentralized digital economy. And we invite you to join us in this exciting and transformative journey.

To enhance the discussion and provide additional resources related to the topics covered in this book, a companion website has been developed. I strongly recommend bookmarking the website: https://distributedapps.ai/web3-security/. This platform will serve as an invaluable resource, providing more in-depth information, updates, and the opportunity to engage with authors of this book. Continue your exploration of Web3 security with this useful tool at your fingertips, and join us in advancing knowledge in this critical area of the digital world.

Fairfax, VA, USA	Ken Huang
Lisbon, Portugal	Dyma Budorin
Singapore, Singapore	Lisa J. Y. Tan
New York, NY, USA	Winston Ma
Stockholm, USA	Zhijun William Zhang

Short Recommendations

Recommendations 1

As the Chairman of the Cloud Security Alliance (CSA) Greater China Region, I am thrilled to recommend "A Comprehensive Guide for Web3 Security: From Technology, Economic, and Legal Aspects."

In this rapidly digitalizing world, as we venture into the uncharted territories of the Internet's next generation, Web3, the significance of understanding its security dimensions cannot be overstated. This book, edited by Ken Huang and his adept editorial team, is an impressive and crucial resource that provides a comprehensive exploration of Web3 security from multiple perspectives. From the foundational components of Web3 security to the unique security concerns for enterprise Web3 application development, and finally, the intersection of Web3 security with financial integrity and national security, this guide covers it all. This comprehensive coverage makes it a must-read for developers, entrepreneurs, policymakers, and anyone interested in the future of the Internet. The diverse backgrounds and unique insights of the authors breathe life into this complex subject, making the intricate world of Web3 security accessible and understandable. Whether you are a seasoned professional or a newcomer to the field, this book will provide valuable insights and deepen your understanding of Web3 security. I wholeheartedly recommend this book to anyone striving to navigate the challenges and opportunities in the exciting new world of Web3.

Prof. Yale Li, Chairman, Cloud Security Alliance Greater China Region (CSA GCR)

Recommendations 2

A Comprehensive Guide for Web3 Security is a tour de force by Ken Huang and his accomplished team of editors. Providing an in-depth exploration of the security challenges and solutions in the Web3 ecosystem, this book is a must-read for anyone involved in blockchain technology, digital assets, and their associated security concerns. Don't miss out on this invaluable resource that covers a diverse range of topics and concerns associated with Web3 Ecosystems.

Xi Chen, Professor NYU

Recommendations 3

This book provides a comprehensive and in-depth discussion of information security in the Web3.0 era, which is highly beneficial for both academia and industry

Yao Qian, the first director of the Chinese Central Bank's Digital Currency (CBDC) Program and now Director of the Science and Technology Supervision Bureau of the China Securities Regulatory Commission

Recommendations 4

A crucial resource for staying up-to-date on the latest advancements in Web3 security, this book offers practical guidance, case studies, and invaluable insights from Ken Huang and his team of expert editors. The book covers a diverse range of topics, from technology to economics and legal aspects, making it a must-read for anyone involved in the space.

Feng Zhu, Professor of Business Administration at the Harvard Business School

Recommendations 5

A meticulous analysis of the challenges and solutions surrounding Web3 security, Ken Huang and his skilled team of editors have crafted a book that is a vital resource for anyone looking to understand and address the complexities of this emerging technology. From foundational components to advanced topics, this book has it all.

Youwei Yang, Chief Economist, BIT Mining Limited

Recommendations 6

A comprehensive and insightful exploration of Web3 security, Ken Huang and his respected team of editors have created a book that covers a wide range of topics, from foundational blockchain security concepts to advanced topics covering many aspects of web3 security. This book is a must-read for anyone interested in securing the future of blockchain and digital assets.

Fang Zhang, Professor, Dept of Computer Science, Yale University

Recommendations 7

It brings me great pleasure to highly recommend "A Comprehensive Guide for Web3 Security: From Technology, Economic, and Legal Aspects," a remarkable and thorough guide to the security challenges and concerns surrounding the exciting world of Web3 and digital assets. Edited by the exceptional Ken Huang and his team of esteemed editors, this book is an invaluable resource for anyone looking to navigate the complex and ever-evolving landscape of Web3 and decentralized finance.

As someone who has worked in the Web3 and cybersecurity industry for many years as a university professor and also an industry practitioner, I understand the importance of staying informed about the latest threats and vulnerabilities. I can attest to the importance of staying informed about the latest threats and vulnerabilities in the Web3 and cybersecurity industry. With over $3 billion in losses attributed to hacks alone in 2022, it's clear that security is a critical issue in the world of digital assets. This book offers a wealth of knowledge, insights, and practical solutions for individuals and enterprises looking to deepen their understanding of Web3 security and digital asset management. With its comprehensive approach and expert contributors, "A Comprehensive Guide for Web3 Security: From Technology, Economic, and Legal Aspects" is an essential read for anyone interested in this rapidly growing field. Whether you're a seasoned expert or just starting to explore the world of Web3, this book will undoubtedly provide you with invaluable guidance and expertise, enabling you to navigate the complex and ever-changing landscape of digital assets and Web3 with confidence.

David (Kuo Chuen) Lee, Professor, Singapore University of Social Sciences

Recommendation 8

What sets this book apart is the wealth of knowledge and experience brought forth by the editor and contributors. As a graduate of the Harvard Kennedy School of Government Cybersecurity program, I had the privilege of attending the same program as Ken Huang back in 2021. Through our shared educational journey and subsequent experiences in the cybersecurity field, I can attest Ken Huang's deep understanding of the subject matter and his commitment to advancing the field of Web3 security.

"A Comprehensive Guide for Web3 Security: From Technology, Economic, and Legal Aspects" is a comprehensive resource that covers a wide range of topics relevant to cybersecurity in the digital era. From blockchain security, Web3 DevSecOps, and smart contract security to token economics and regulatory concerns, the book offers insights and strategies that will empower you to navigate the intricate world of Web3 security. It presents these concepts in an accessible manner, making it suitable for readers with varying levels of expertise.

In addition to its comprehensive coverage, “A Comprehensive Guide for Web3 Security: From Technology, Economic, and Legal Aspects” stands out for its practical approach. The book provides real-world examples, case studies, and best practices that highlight the relevance and applicability of the concepts discussed. Whether you are an aspiring Web3 professional, a technology enthusiast, or simply someone seeking to enhance your understanding of the Web3 digital landscape, this book will equip you with the knowledge and tools needed to protect yourself and your digital assets.

Aditi Joshi, Security and Privacy Engineering at Google Cloud

Acknowledgment

As the chief editor of this book, I am deeply grateful to all those who contributed their invaluable expertise, knowledge, and time to make this publication a reality.

First and foremost, I must acknowledge the exceptional work of my fellow editors Dyma Budorin, Lisa JY Tan, Winston Ma, and Zhijun (William) Zhang. Their dedication, insight, and collaboration have been indispensable in shaping the content and structure of this book, and I am truly grateful for the opportunity to work alongside such esteemed professionals, each of whom brought a unique perspective and depth of understanding to the table.

I also extend my heartfelt thanks to two contributors of this book, Carlo Parisi and Ostap Khalavka, who shared their expertise and research in three chapters of this book. Their commitment to providing accurate, up-to-date information and insightful analysis on the complex world of Web3, blockchain, and digital asset security has been demonstrated in the book.

Special mention goes to our publisher Springer Nature and the editorial and project teams, including Ms. Jianlin Yang, Ms. Poongothai Chockalingam, Ms. Lala Glueck, and many other members of the Springer Nature team. Their unwavering support and guidance throughout the publication process have been exceptional, and we are grateful for their patience, professionalism, and meticulous attention to detail, which have been instrumental in ensuring the outstanding quality of this book.

I also wish to express my appreciation to the numerous industry experts, academics, and professionals who have reviewed, critiqued, and provided feedback on the various chapters. Your input has greatly contributed to the overall rigor and value of this book.

The original impetus for editing this book came from my conversation with Igor Bershadsky, who was the director of business development at Hacken Cyber Security Service when we were both invited by the Busan Municipal Government and spoke about digital asset security at Busan Blockchain Week in November 2022. I would like to personally thank Igor for this.

Lastly, I thank my family and friends for their constant encouragement and support during the demanding process of editing this book. Your understanding and reassurance have been a source of strength and motivation.

In closing, I am truly honored to have had the opportunity to collaborate with such a remarkable group of individuals in the creation of this book. I believe that our collective efforts have resulted in a valuable resource for anyone interested in understanding and addressing the security challenges and concerns in the ever-evolving world of Web3, blockchain, and digital assets.

DistributedApps LLC
Fairfax, VA, USA

Ken Huang

Contents

Part I Foundational Components of Web3 Security

1 The C.I.A Properties of Web3 System 3
Ken Huang
1.1 The Confidentiality Property of Blockchain 4
1.1.1 Cryptographic Primitives in Blockchain 5
1.1.1.1 What Are the ECDSA (GeeksforGeeks, 2022) and Schnorr Signature Algorithm (Boneh, 2020) 5
1.1.1.2 What Is a Hash Algorithm and What Is SHA256 (Mycryptopedia, 2022), How SHA256 Is Used in Bitcoin 6
1.1.1.3 What Is Base58 (BitcoinWiki, 2022) and How It Is Used in Bitcoin? 7
1.1.1.4 How Bitcoin Address Is Generated 8
1.1.2 Bitcoin's Lack of Confidential Property 9
1.1.3 Privacy-Preserving Computation for Web3 10
1.2 The Integrity Property of Blockchain 13
1.2.1 The Integrity of the Base Layer of Blockchain 13
1.2.2 The Integrity of Layer2 Blockchain 16
1.2.2.1 Bitcoin Layer 2 Lightning Network Attack 16
1.2.2.2 Attacks on Ethereum Layer 2 Rollups 16
1.2.2.3 Attacks on Layer 2 Bridges 17
1.2.2.4 Wormhole Attack 17
1.2.3 Integrity of Smart Contract 19
1.3 The Availability Property of Blockchain 19
1.3.1 Availability via Data Replication 21
1.3.2 Availability via Scalability 21
1.3.2.1 Sidechain VS Layer-2 23
1.3.2.2 Data Availability and Layer 2 Solutions 23

1.3.2.3 Bitcoin Lightning Network for Better Availability 25
References 27

2 Chain Security: Nodes, Algorithm, and Network 31
Ken Huang
2.1 What Is Consensus Node? 32
2.2 Consensus Node Configuration Security 33
2.2.1 Bitcoin Node Security Configuration Recommendations 33
2.2.2 Ethereum POS Validator Node Security Recommendations 35
2.2.3 Attacks on Consensus Node 36
2.3 Node Centralization and Security Concerns 38
2.4 Bitcoin Security After Mining Rewards Depletion 39
2.5 Attacks on Consensus Algorithm and Countermeasures 42
2.5.1 Attacks on Proof-of-Work (PoW) and Countermeasures 42
2.5.2 Attacks on Proof-of-Stake (PoS) and Countermeasures 45
2.5.3 Attacks on Delegated Proof-of-Stake (DPoS) and Countermeasures 48
2.5.4 Attacks on Proof of Activity (PoA) and Countermeasures 49
2.5.5 Attacks on Proof of Elapsed Time (PoET) and Countermeasures 49
2.5.6 Attacks on Byzantine Fault Tolerance (BFT) and Countermeasures 50
2.6 Attacks on Blockchain Network Layer and Countermeasures 53
2.6.1 Time Jacking Attack and Countermeasures 53
2.6.2 Tampering with Message Body and Countermeasures 54
2.6.3 MEV Attack and Countermeasures 55
2.6.4 Routing Attacks and Countermeasures 57
2.6.5 Fake Bootstrapping Attack and Countermeasures 57
2.6.6 Eclipse Network Attack and Countermeasures 58
2.6.7 Attack on Libp2p and Countermeasures 59
References 60

3 Wallet Security 61
Carlo Parisi, Dyma Budorin, and Ostap Khalavka
3.1 Introduction 61
3.1.1 Overview of Different Types of Blockchain Wallets 61
3.1.2 Explanation of the Different Kinds of Wallets 61
3.1.3 Comparison of Blockchain Wallets to Traditional Banking and Financial Systems 62
3.1.4 Difference between Custodial and Non-custodial Wallets 63
3.2 How Blockchain Wallets Work 63
3.2.1 Technical Explanation of How Blockchain Wallet Works 63
3.2.2 Overview of the Use of Public and Private Key 64

3.2.3 Overview of the Role of the Wallet in Public and Private Key . . . 67
3.2.4 Smart Contract Wallets . . . 67
3.2.5 Account Abstraction. . . . 67
3.2.6 Multisignature Wallets . . . 68
3.2.7 Social Recovery . . . 69
3.2.8 MPC Wallet . . . 70
3.2.9 Most Common Attack Vectors . . . 71
3.2.10 Wallet Security Features . . . 71
3.3 Past Blockchain Wallet Hacks . . . 72
3.3.1 Overview of Past Relevant Wallet Hacks. . . . 72
3.3.1.1 "NFT God" Hacked, January 2023 . . . 72
3.3.1.2 BitKeep, December 26 2022, $8M Lost . . . 73
3.3.1.3 Deribit, November 2022, $28M Lost . . . 73
3.3.1.4 Solana Wallet Hacks, August 2022, $5M Lost . . . 73
3.3.1.5 Profanity Wallets Hack, $3.3M Lost . . . 73
3.3.1.6 Binance Hot Wallet Hack, May 2019, $40M Lost . . . 74
3.3.1.7 MetaMask iCloud Hack, July 2021 . . . 74
3.3.1.8 Parity Multisig Hack, November 2017, $30M Lost . . . 74
3.3.2 The Impact of Cyberattacks on Blockchain Wallets . . . 75
3.4 The Importance of Auditing a Wallet. . . . 75
3.4.1 Explanation of the Importance of Auditing a Wallet . . . 75
3.4.2 Overview of Different Types of Audit that Can Be Performed. . . . 76
3.4.3 Different Tools to Audit Wallets . . . 77
References. . . . 77

4 Smart Contract Security . . . 81
Carlo Parisi and Dyma Budorin
4.1 Introduction . . . 81
4.1.1 Definition of Smart Contracts in the Context of Web3 Applications . . . 81
4.2 Smart Contract Security Checklist. . . . 82
4.2.1 Gas Optimization . . . 83
4.2.2 Compiler Version . . . 83
4.2.3 Access Control. . . . 83
4.2.4 Check Effect Interaction . . . 84
4.2.5 SELFDESTRUCT Instruction . . . 84
4.2.6 Denial of Service . . . 84
4.2.7 Deprecated Functions. . . . 85
4.2.8 Race Conditions . . . 85
4.2.9 Signature Unique ID . . . 86
4.2.10 Weak Source of Randomness. . . . 86
4.2.11 Assets Integrity and User Balance Manipulation. . . . 86

4.2.12 Secure Oracle Usage 87
4.2.13 Flash Loans 87
4.2.14 Style Guide and Readability 88
4.2.15 Requirements Compliance 88
4.2.16 Importance of Following the Checklist to Ensure Smart Contract Security 88
4.3 Top Security Vulnerabilities in Smart Contracts 88
4.3.1 Flash Loans 88
4.3.2 Front Running 91
4.3.3 DoS 91
4.3.4 Invalid Calculations 92
4.3.5 Token Supply Manipulation 92
4.3.6 Deprecated Functions 93
4.3.7 Reentrancy Attack 94
4.3.8 Access Control Violation 95
4.3.9 Replay Attacks 97
4.3.10 Weak Source of Randomness 98
4.3.11 Incorrect Oracle Usage 98
4.4 Importance of Smart Contract Audits in Web3 Applications 99
4.5 Final Thoughts 100
References 101

5 Token Economics Model Creation and Security 103
Lisa J. Y. Tan
5.1 Tokens vs Economy 103
5.2 Economy Design of Tokens Is Not New 104
5.3 Why Is this Important 105
5.3.1 Risks 107
5.4 What Is Token Economics 107
5.5 Web3 Security and Token Economics 109
5.5.1 Ponzinomics 109
5.6 How Web3 Compares with Existing Economic Structures? 110
5.7 What Does Token Economics Entail 111
5.7.1 Economics Design Framework 113
5.7.2 Value Creation 113
5.7.3 Value Creation Cycle 114
5.8 Token Economics Stress Test vs Economics Risk Monitoring 115
5.9 Cyber Security Risks Come In 116
5.10 Summary and Ongoing Work on Tokenomics 116
References 117

6 Economic Exploits and Risk Mitigation Strategies 119
Lisa J. Y. Tan
6.1 Case Study 1: Economic Exploit Through Financial Engineering 120
6.1.1 Case Study 120

6.1.2 The Exploit. 121
6.1.3 Solution: Risk Adjustment 121
6.2 Case Study 2: Incentive Mechanism Design Risk 122
6.2.1 Case Study 123
6.2.2 The Exploit. 123
6.2.3 Solution: Economy Parameter Adjustment 124
6.3 Case Study 3: Bancor's Insurance Mechanism and Celsius' Exploitation 124
6.3.1 Case Study 124
6.3.2 The Exploit. 125
6.3.3 Solution: Bancor's Response to the Exploit 125
6.4 Opportunities and Threats with AI. 126
6.4.1 Opportunities 126
6.4.2 Threats 127
6.5 10 Economic Risk Metrics Considerations 128
6.6 Why Should We Care. 130
References. 130

Part II Security Concerns for Enterprise Web3 Application Development

7 DevSecOps for Web3. 135
Ken Huang
7.1 What Is DevSecOps? 136
7.2 How to Integrate DevSecOps into Web3 138
7.2.1 DevSecOps during Requirement and Design Phase 139
7.2.1.1 Web3 Product Description and Requirement Document 139
7.2.1.2 Web3 Architecture Document. 139
7.2.1.3 Security Requirement Gathering. 143
7.2.1.4 Technical Threat Modeling 143
7.2.1.5 Data or Capital Flow Diagram 143
7.2.1.6 Token Economic Model 144
7.2.1.7 Financial Security Model 145
7.2.2 Implementation Phase 146
7.2.2.1 CI/CD Pipeline Security Tools Integration 146
7.2.2.2 IDE Tool Extension. 147
7.2.2.3 Security Code Review. 148
7.2.3 Testing and External Validation Phase (Testnet Phase) 148
7.2.3.1 Formal Verification 149
7.2.3.2 Third-Party Security Auditing (Not Just Solidity Code, Must Include all Code) 151
7.2.4 Bug Bounty 151
7.2.5 Production (Mainnet) Phase. 153
7.2.5.1 Continuous Bug Bounty 153
7.2.5.2 Monitoring/Alerting 153