

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 Editor(s) (if applicable) and The Author(s), under exclusive license to Springer Nature Switzerland AG 2023

This work is subject to copyright. All rights are solely and exclusively licensed by the Publisher, whether the whole or part of the material is concerned, specifically the rights of reprinting, reuse of illustrations, recitation, broadcasting, reproduction on microfilms or in any other physical way, and transmission or information storage and retrieval, electronic adaptation, computer software, or by similar or dissimilar methodology now known or hereafter developed.

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
May 4, 2023

Jim Reavis

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
Dallas, USA
May 2023

Jyoti Ponnappalli

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
Lisbon, Portugal
Singapore, Singapore
New York, NY, USA
Stockholm, USA

Ken Huang
Dyma Budorin
Lisa J. Y. Tan
Winston Ma
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

- 7.3 Sample Security Tools for Web3 DevSecOps 153
 - 7.3.1 Sample Security Tools Used in during the Requirement and Design Phase 154
 - 7.3.2 Sample Security Tools Used in Implementation and Testing Phase 154
 - 7.3.3 Sample Security Tools Used during Mainnet or Production Phase 155
- References 157
- 8 Web3 Security Analytics 159**
 - Carlo Parisi and Dmitriy Budorin
 - 8.1 Introduction 159
 - 8.1.1 What Is on-Chain Analytics 159
 - 8.1.2 Preventive Vs Reactive Web3 on-Chain Analytics and Monitoring 161
 - 8.1.2.1 Preventive on-Chain Analysis 161
 - 8.1.2.2 Reactive on-Chain Analysis 161
 - 8.2 Preventive on-Chain Analysis 162
 - 8.2.1 Past and Present of Preventive on-Chain Analysis. 162
 - 8.2.1.1 The Past and Present of Preventive on-Chain Analysis: Evolution and Challenges 162
 - 8.2.1.2 The Past: The Evolution of Web2 Monitoring 163
 - 8.2.1.3 The Present: An Overview of Web3 Monitoring 163
 - 8.2.1.4 The Present: Protecting End Users in Web3 164
 - 8.2.1.5 Challenges in Web3 on-Chain Monitoring 164
 - 8.2.2 Technology Stack Used for Preventive on-Chain Analysis 164
 - 8.2.3 Future of Preventive on-Chain Analysis 166
 - 8.3 Reactive on-Chain Analysis 168
 - 8.3.1 The Problem that Reactive on-Chain Analysis Solves. 168
 - 8.3.1.1 Incident Response and Forensic Analysis 169
 - 8.3.1.2 Post-Mortem Analysis and Lessons Learned 169
 - 8.3.1.3 Enhancing Preventive Measures and Proactive Security 169
 - 8.3.1.4 Regulatory Compliance and Legal Support 170
 - 8.3.1.5 Reputation Management and User Trust. 170
 - 8.3.2 The Present of Reactive on-Chain Analysis. 171
 - 8.3.2.1 Looking Ahead: The Future of Reactive on-Chain Analysis. 172
 - 8.4 On-Chain Analysis Tools 172
 - 8.5 The Future of on-Chain Analysis: Combining Preventive and Reactive Approaches 174
 - 8.5.1 Enhanced Machine Learning and AI Capabilities 174
 - 8.5.2 Cross-Chain and Interoperability 175

- 8.5.3 Privacy-Preserving on-Chain Analysis 175
- References. 176
- 9 Data Authenticity 177**
- Ken Huang
- 9.1 Types of Blockchain Oracles 178
 - 9.1.1 Input Oracles 178
 - 9.1.2 Output Oracles 179
 - 9.1.3 Cross-Chain Oracles. 180
 - 9.1.4 Compute-Enabled Oracles 181
 - 9.1.5 Other Types of Oracles. 181
- 9.2 Examples of Data Oracle Providers. 182
- 9.3 Oracle Use Cases 187
 - 9.3.1 Decentralized Finance (DeFi) 187
 - 9.3.2 Dynamic NFTs and Gaming 188
 - 9.3.3 Insurance 189
 - 9.3.4 Enterprise Supply Chain Management. 190
 - 9.3.5 Prediction Markets 190
 - 9.3.6 Sustainability 191
- 9.4 Oracle Design Considerations 192
- 9.5 Security Attacks on Oracles. 194
- 9.6 Countermeasures to Oracle Security Attacks. 196
- References. 200
- 10 Security in Permissioned Blockchain 201**
- William Zhang
- 10.1 Introduction 201
 - 10.1.1 Permission Blockchain Use Cases. 202
 - 10.1.2 Overview of the Chapter 203
- 10.2 Different Types of Permissioned Blockchain 203
 - 10.2.1 Hyperledger Fabric. 203
 - 10.2.2 R3 Corda 204
 - 10.2.3 Quorum 205
- 10.3 Top Security Vulnerabilities in Permissioned Blockchain. 206
 - 10.3.1 Compromised Node 206
 - 10.3.2 Centralization 207
 - 10.3.3 Weakness in the Permissioning Process. 207
 - 10.3.4 Software Vulnerabilities 207
 - 10.3.5 Insider Threats 208
 - 10.3.6 Smart Contract Vulnerabilities 208
 - 10.3.7 Weakness in Consensus Protocols 208
 - 10.3.8 Governance Issues 209
 - 10.3.9 Denial-of-Service Attacks 209
- 10.4 How to Achieve Security in Permissioned Blockchains 209
 - 10.4.1 Architecture Design 210
 - 10.4.2 Design Redundancy for any Single Point of Failure 210

- 10.4.3 Manage Software Supply Chain. 210
- 10.4.4 Ensure Robust Identity Management for the Whole Lifecycle of a Node 211
- 10.4.5 Adopt Strong Network Security to Minimize the Chance of a Node Compromise 211
- 10.4.6 Ensure Security Best Practices in Administration 212
- 10.4.7 Ensure Data Confidentiality, Integrity, and Availability 212
- 10.4.8 Validate the Security of Smart Contracts 212
- 10.4.9 Have a Strategy for System Upgrades 213
- 10.4.10 Patch Systems Diligently 213
- 10.4.11 Establish Monitoring and Incident Response Capabilities and Processes 213
- 10.5 Final Thoughts 213
- References. 214

Part III Financial Integrity and National Security

11 Regulation and Crypto on a Cliff Edge. 219

Winston Ma

- 11.1 FTX Collapse: Global Regulation Rising Sharply. 219
 - 11.1.1 2022: Dramatic and Difficult Year 219
 - 11.1.2 The Rise (and Fall) of FTX 219
 - 11.1.3 Three Profound Implications 221
 - 11.1.3.1 FOMO Out, DD In 221
 - 11.1.3.2 More Blockchain Technology, Less Speculative Trading 222
 - 11.1.3.3 Global Regulations Rising. 222
- 11.2 China: Crackdown on (Formerly) World’s Largest Crypto Market 223
 - 11.2.1 Unprecedented Crackdown Since 2021 223
 - 11.2.2 Three Key Factors 224
 - 11.2.2.1 Investor Protection. 224
 - 11.2.2.2 Carbon Neutrality 224
 - 11.2.2.3 Financial Stability 225
 - 11.2.3 China’s CBDC Push. 226
 - 11.2.4 Global Implication of China’s Crypto Crackdown 228
- 11.3 EU’s MiCA: First Comprehensive Crypto Regulatory Framework 228
 - 11.3.1 “Crypto-Assets” Clarified 229
 - 11.3.2 White Paper Requirement for Issuers of Crypto-Assets. 230
 - 11.3.3 Excluded (for Now): NFT, DeFi, and DAO 230
 - 11.3.4 “Passport” Perks in Europe 231
- 11.4 US: Fragmented Enforcement as Regulation. 232
 - 11.4.1 Conflict of Jurisdictions: CFTC Vs. SEC. 232

- 11.4.2 Crypto’s Howey Test: Securities and/or Commodities? 233
- 11.4.3 SEC V. Ripple Case 234
- 11.4.4 Staking under Attack: Coinbase and the Wells Notice 235
- 11.5 Stablecoin Regulation: A Rare Global Consensus. 236
- 11.6 Conclusion: Regulatory Game of Thrones. 238
- 12 Terrorist Financing, War Crimes, and Crypto Geopolitics 241**
- Winston Ma
- 12.1 Crypto and Geopolitics: Ukraine V. Russia War 241
 - 12.1.1 Crypto in Conflict. 241
 - 12.1.2 Sovereign Nations into Crypto Market 243
 - 12.1.3 Decentralized Exchanges Caught in the War 244
 - 12.1.4 Best Practices in Need 245
- 12.2 Money Laundering/Terrorism Financing on Blockchain. 245
 - 12.2.1 Unique Characteristics of Crypto Assets 245
 - 12.2.2 DeFi Tricks: DEXs, Mixers, and Liquidity Pools 246
 - 12.2.3 Case Study: Tornado Mixer and North Korea 247
- 12.3 FATF’s AML/CFT Framework and Travel Rule 248
 - 12.3.1 Are Cryptos Traceable? 248
 - 12.3.2 FATF: Unified Global Response 249
 - 12.3.3 Travel Rule. 250
- 12.4 Crypto Intelligence and Blockchain Analysis 252
 - 12.4.1 Blockchain Analysis Solutions. 252
 - 12.4.2 AI-Powered Analytics 253
 - 12.4.3 The Case of Crypto Flow and Hamas Financing 254
- 12.5 Biden Executive Order and “Responsible Development” 255
 - 12.5.1 Role of National Security in Executive Order 255
 - 12.5.2 Digital Dollar: US CBDC 256
 - 12.5.3 US Treasury: DeFi Poses a Threat to National Security 257
- 12.6 Conclusion: The US Balancing Act. 258

About the Editors and Contributors

About the Editors



Ken Huang is Chair of the Blockchain Security Working Group for Cloud Security Alliance Great China Region (CSA GCR) and the author of multiple books both in English and Chinese on blockchain and Web3. Over the past 20 years, he has worked on application security, identity, and access management, and cloud security for the fintech industry as well as federal civilian agencies. He has been certified as CISSP since 2007 and authored a book titled <<Blockchain Security Guide>> which was published by China Machine Press in 2018. As CEO of DistributedApps, he provides cyber-

security consulting services on Blockchain and AI for startup companies globally. He was a judge for AI and Blockchain startup contests organized by Google, Softbank, and Stanford in 2018. He was a member of ACM’s AI Decentralized Practitioners Board in 2018. As part of the W3C Credentials Community Group Member, he provided his comments for NIST 800-63 documents on Identity Management.

As Chair of CSA GCR, he has worked with top security experts in blockchain space to create the following white papers:

1. Digital Wallet Security Development and Application
2. Top 10 Crypto Exchange Security Risks
3. Smart Contact Security Guide
4. AML and Chain Analysis for Digital Asset Transactions.
5. DApp Security Guide
6. Decentralized Identity Security and Privacy Considerations

He was an invited speaker to numerous local and global conferences in Blockchain, AI, ChatGPT, and Security including Davos WEF, CoinDesk Consensus, IEEE, ACM, World Bank, Stanford University, UC Berkeley, Bank of China, and Huawei.

Recently he co-authored the book entitled <<Blockchain and Web3: Building the Cryptocurrency, Privacy, and Security Foundations of the Metaverse>> which was published by Wiley in September 2022 and named as one of the six must-read books in 2023 by TechTarget.



Dyma Budorin Founder & CEO at Hacken and Founder at HackenProof.

Dyma is a cybersecurity expert and crypto economy influencer with 14+ years of managerial expertise in cybersecurity as well as risks and controls audits. Dyma holds a master's degree in International Economics and an MBA from the Kyiv Institute of Investment Management. He is a certified member of the Association of Chartered Certified Accountants (ACCA).

In 2017, Dyma established Hacken, a cybersecurity consulting firm. Five years later, Hacken is trusted by the largest crypto projects; the company's portfolio includes HackenAI, HackenProof, CER, and a suite of accompanying blockchain services. Dyma's effective leadership is what transformed Hacken from a startup into a major player in Web3 cybersecurity. The story of success is only gaining momentum.

As the company's Co-Founder and CEO, Dyma is responsible for leading the team of 100+ talented specialists and providing a vision of the future. Dyma consults the Ukrainian government on the adoption of a virtual economy. He is a regular participant in major Web3 cybersecurity events as an invited speaker.



Lisa J. Y. Tan is the founder and lead economist at Economics Design, a research-focused consultancy for digital ecosystems. In the academic world, she contributes to research work in various fields like math and economics, while having practitioner exposure with startups and global businesses. She's also one of the leaders in a United Nations x Stanford University project on regulating digital currencies.

She is also the author of Economics and Math of Token Engineering and DeFi, a research-based textbook for users in the space (crypto holders and DeFi users), as well as crypto protocol projects that cover the evolution of economics, a framework for designing systems and the math around the various mechanisms. Lisa's previous work in token economy has made her a pioneer in the design and engineering of digital ecosystems. With a track record of over 30 token economies and 50 token analyses, Lisa's work is characterized by a research-focused approach and a deep understanding of the potential of blockchain

technology. As a highly sought-after speaker at conferences and forums worldwide, Lisa's expertise in token economics and DeFi has established her as a respected authority in the field of digital ecosystems.



Winston Ma, CFA & Esq, is an investor, attorney, author, and adjunct professor in the global digital economy. He is the Executive Vice Chairman of Virtual-Q, a leading cloud service and virtual desktop provider. Also, he is currently the board Chairman of Nasdaq-listed MCAA (a European tech SPAC), an advisory board member of Capgemini, and an Adjunct Professor at NYU Law School on SWF fund topics. For public services, he is an inaugural member of the Investment Advisory Board convened by UNDRR (United Nations) in 2023.

Most recently for 10 years, he was Managing Director and Head of North America Office for China Investment Corporation (CIC), China's sovereign wealth fund. Prior to that, Mr. Ma served as the deputy head of equity capital markets at Barclays Capital, a vice president at J.P. Morgan investment banking, and a corporate lawyer at Davis Polk & Wardwell LLP. He is one of a small number of native Chinese who have worked as investment professionals and practicing capital markets attorneys in both the USA and China.

A nationally certified Software Programmer as early as 1994, Mr. Ma is the author of eight books on the digital economy, SWF funds, and global tech regulations, including *The Hunt for Unicorns: How Sovereign Funds are Reshaping Investment in the Digital Economy* and most recently "Blockchain and Web3" (2022). He has been frequently interviewed by CNBC and Bloomberg TV and quoted by major financial media including WSJ, Reuters, and Financial Times. He was selected as a 2013 Young Global Leader at the World Economic Forum (WEF), and in 2014 he received the NYU Distinguished Alumni Award.



Zhijun (William) Zhang is the Technology and Innovation Adviser at the Bank for International Settlements (BIS) Innovation Hub—Nordic Centre, where he focuses on cybersecurity and resilience for future financial market infrastructure. Before joining the BIS, he was the lead information security architect at The World Bank Group (WBG), where his team is responsible for security architecture design and assessment of all technology platforms and business solutions.

His team developed WBG's enterprise security architecture reference model that serves as the security framework that guides all their design and assessment work. He also led the security and risk work for WBG's innovation lab. Before joining the WBG, William worked at The Vanguard Group, a large financial service organization in the USA, in various capacities, including user experience design,

emerging technology research, system architecture, and information security. William received his BS degree from Peking University, and his Ph.D. from the University of Maryland, both in computer science.

About the Contributors

Ostap Khalavka is a professional content writer and editor focused on Web 3.0 cybersecurity and information technologies in general. Ostap's major is international economic relations. Upon graduating from the Taras Shevchenko National University of Kyiv in 2020, Ostap joined the cybersecurity company Hacken. He has been responsible for creating research articles, blog posts, social media publications, infographics, etc. In July 2022, Ostap joined the Ukrainian Armed Forces where he has been appointed to the position of deputy commander of the battalion responsible for the psychological and moral support of the staff.

Carlo Parisi is a smart contract auditor and an Italian content creator who has been involved in the crypto industry for many years, conducting his first bitcoin transaction in 2013. He completed his bachelor's degree in Computer Science from the University of Bari Aldo Moro and has gained several years of experience working as a developer in both Java and Solidity. In 2022, he joined Hacken as a solidity smart contract auditor.

Part I

Foundational Components of Web3 Security

As the world of Web3 expands at an unprecedented pace, the need for robust security measures becomes increasingly critical. Built on the foundation of blockchain technology, Web3 promises self-sovereign information systems, value-based transactions, and a secure and decentralized ecosystem. However, ensuring the security of these systems is essential for their long-term success and adoption.

In Part I of this book, we delve into the foundational components of Web3 security, covering the CIA properties of blockchain, chain security, wallet security, smart contract security, token economics model creation and security, as well as economic exploits and risk mitigation strategies.

Chapter 1 discusses the relevance of the Confidentiality, Integrity, and Availability (CIA) triad in the context of Web3 and its application to blockchain technology. It highlights the importance of each of the CIA triad properties in protecting sensitive information and maintaining reliable systems.

Chapter 2 provides a comprehensive exploration of chain security, touching upon node security, consensus algorithm security, and network layer security. It emphasizes the importance of securing individual nodes, protecting the consensus algorithm, and safeguarding data transmitted between nodes.

Chapter 3 delves into wallet security, examining the types of wallets, their underlying technologies, and their crucial role in securing digital assets and facilitating transactions. The chapter offers valuable insights and practical advice on wallet security, focusing on risk mitigation, user education, and proactive auditing.

Chapter 4 presents an in-depth overview of smart contract security, providing a detailed security checklist for developers and auditors and analyzing the top security vulnerabilities. The chapter underscores the necessity of rigorous auditing processes and robust security practices to ensure the safety and long-term success of Web3 platforms.

Chapter 5 explores token economics, its underlying principles, and the security challenges associated with it. The chapter defines token economics, examines the interplay between Web3 security and token economics, and addresses cybersecurity risks in the context of token economics.

Chapter 6 investigates case studies related to token economics, shedding light on risks, exploits, and potential solutions. It also discusses the impact of artificial intelligence (AI) on token economics and outlines key considerations for assessing economic risk metrics in token economics.

By the end of Part I, readers will have a solid understanding of the fundamental components of Web3 security and the knowledge required to navigate the complex and rapidly evolving landscape of decentralized technologies.

Chapter 1

The C.I.A Properties of Web3 System



Ken Huang

This chapter discusses the confidentiality, integrity, and availability (CIA) triad properties of Blockchain.

From a cybersecurity perspective, the CIA triad is a fundamental concept that helps organizations protect their sensitive information. Confidentiality, integrity, and availability are the three key pillars of this triad that form the basis of effective information security measures.

Confidentiality is critical for safeguarding information from unauthorized access or disclosure. This is particularly important when dealing with sensitive data such as personal information, financial records, or intellectual property. By ensuring that only authorized individuals have access to this information, organizations can minimize the risk of data breaches and protect their reputations.

Integrity is equally important, as it ensures that information is accurate and trustworthy. When data is tampered with or modified without authorization, it can lead to errors, fraud, or other serious consequences. By maintaining data integrity, organizations can ensure that their information is reliable and can be used to make informed decisions.

Availability is the third pillar of the CIA triad and refers to the ability of authorized users to access information when they need it. Without access to critical data, organizations may struggle to carry out their day-to-day operations, resulting in lost productivity, decreased customer satisfaction, and ultimately, a negative impact on the bottom line.

Security professionals define security using the CIA triad because it provides a comprehensive framework for understanding and addressing the various aspects of information security. These principles are interdependent and must be considered together in order to effectively protect information and systems.

K. Huang (✉)
DistributedApps.AI, Fairfax, VA, USA
e-mail: Ken@Distributedapps.ai

By focusing on the CIA triad, security professionals can ensure that they are addressing all of the key elements of information security, including the protection of sensitive information from unauthorized access or disclosure, the accuracy and completeness of information, and the availability of information to authorized users. Using the CIA triad as a framework for defining security also helps security professionals to prioritize their efforts and allocate resources in a way that aligns with the most important security objectives. This can help to ensure that the security measures that are put in place are effective and efficient at protecting information and systems.

Since Web3 is a value-based and self-sovereign information system, the CIA triad still applies to Web3. At the core of Web3, blockchain technology has unique advantages and challenges in terms of the CIA triad that we will explore in detail in this chapter. But the following are the brief statements.

In terms of confidentiality, we argue that the pseudo-anonymity of native blockchain without privacy-preserving technology or protocol cannot really provide sufficient confidentiality of blockchain data.

In terms of integrity, we discuss the immutable nature of the blockchain ledger that can provide some level of integrity only if the chain can withstand a forking attack and the consensus algorithm has solid security and liveness design.

The availability of blockchain hinges upon the data replication and scalability and latency of blockchain networks as well as on-chain and off-chain data of blockchain.

1.1 The Confidentiality Property of Blockchain

The transactions on the public blockchain are transparent, but the identities of the parties involved are kept confidential. This is done through the use of pseudonyms, which are randomly generated strings of characters that are used to represent the parties involved in a transaction.

This means that each participant in the blockchain is assigned a unique identifier, or pseudonym, which is used to record and verify transactions. While this does offer a certain level of privacy, it is not actually as anonymous as many people think.

For example, it is possible for an individual's identity to be linked to their Bitcoin address in certain circumstances. If an individual uses their real name or other personally identifying information to create a Bitcoin wallet via a centralized entity or exchange, or if they conduct transactions through a centralized exchange that requires identity verification, their identity may be associated with their Bitcoin address. Additionally, if an individual engages in transactions with parties that they are personally connected to and those parties are aware of their identity, it becomes possible for others to infer the identity of the individual based on the transaction information.

Moreover, it is also important to note that law enforcement agencies and other organizations have developed methods for analyzing and tracing transactions on the

blockchain and potentially linking them to real-world identities and the transaction information associated with these identities. While this is a good feature for law enforcement, if the same technology is used by nefarious hackers, the technology can breach the basic privacy and security of end users and the transactions they have conducted on-chain. We must indeed examine the issue of lack of confidentiality of many public blockchains and explore privacy-preserving technologies that can be used to improve confidentiality for blockchain.

1.1.1 Cryptographic Primitives in Blockchain

In this section, we introduce cryptographic primitives used in the blockchain using bitcoin as an example.

1.1.1.1 What Are the ECDSA (GeeksforGeeks, 2022) and Schnorr Signature Algorithm (Boneh, 2020)

ECDSA (Elliptic Curve Digital Signature Algorithm) is a variant of the Digital Signature Algorithm (DSA) that uses elliptic curve cryptography to generate a digital signature. It involves the use of a private key, which is known only to the signer, and a public key, which is shared with the verifier.

To create a digital signature using ECDSA, the signer first hashes the message or document to be signed. The hash is then encrypted using the signer's private key, resulting in the digital signature. The verifier can then use the signer's public key to decrypt the signature and compare the resulting hash to the original message or document. If the two hashes match, it means the message or document has not been tampered with and is therefore authentic.

Since Bitcoin's inception, ECDSA has been used to secure bitcoin. ECDSA was chosen for Bitcoin for a few reasons:

- **Open Source.** ECDSA was not protected by patents or copyright, so there were no legal issues with using it for Bitcoin.
- **Well Tested.** ECDSA was widely known and applied when Bitcoin was first designed, and its security was sufficiently established by years of testing.
- **OpenSSL.** ECDSA was implemented in OpenSSL, an open-source cryptography library used by Bitcoin. This made implementing ECDSA for Bitcoin simpler.

There are several different elliptic curves that can be used with ECDSA, including secp256k1, secp256r1, and secp384r1. secp256k1 is the most commonly used curve in Bitcoin and other cryptocurrencies, as it provides a good balance between security and efficiency. It is also the curve that is used by default when generating a Bitcoin address.

However, ECDSA also has several drawbacks which Schnorr signatures improve upon. For this reason, developers have decided that Bitcoin should implement a different signature scheme, Schnorr.

Schnorr signatures are named after their inventor, Claus-Peter Schnorr, who proposed the concept in a paper published in 1991. Schnorr signatures have several properties that make them well-suited for use in Bitcoin and other cryptocurrency networks:

- They are efficient: Schnorr signatures are smaller in size compared to other types of digital signatures, which means they take up less space on the Bitcoin blockchain. This can help reduce the overall size of Bitcoin transactions and the fees associated with them.
- They are secure: Schnorr signatures are based on strong cryptographic principles and are considered to be highly secure.
- They support multi-signature (or “multisig”) transactions: With Schnorr signatures, it is possible to create transactions that require multiple parties to sign off on them before they can be broadcast to the network. This is useful for scenarios where multiple parties need to agree on a transaction before it can be completed.

1.1.1.2 What Is a Hash Algorithm and What Is SHA256 (Mycryptopedia, 2022), How SHA256 Is Used in Bitcoin

A hash algorithm is a mathematical function that takes an input (or “message”) and produces a fixed-size output (or “hash”), which is typically a string of characters. The output of a hash function is often referred to as a “hash” or a “message digests.”

The main property of a hash function is that it is a one-way function: it is easy to compute the hash of a message, but it is infeasible to recreate the original message from the hash. In other words, the hash function is used to create a fingerprint or a unique representation of the original message, but it is not possible to reverse the process and recover the original message from the hash.

SHA-256 (Secure Hash Algorithm 256-bit) is a specific type of hash function that is commonly used in the Bitcoin network. It is a cryptographic hash function that produces a fixed-size output (256 bits) for any input, regardless of the size of the input. SHA-256 is considered to be a secure and reliable hash function, and it is widely used in many different applications.

In the context of Bitcoin, SHA-256 is used in the mining process to help secure the blockchain. Miners use their computers to solve complex mathematical puzzles, and the first miner to solve the puzzle gets to add a new block to the blockchain. In order to create a new block, the miner must include the hash of the previous block in the blockchain, as well as the hash of the transactions being included in the new block. The miner must also include a nonce (a random number) in the block header, and this nonce is used to create a unique hash for the block. The miner’s goal is to find a nonce that produces a hash that meets certain criteria (e.g., it must have a certain number of leading zeros).

SHA-256 is also used in other parts of the Bitcoin network, such as in the creation of Bitcoin addresses and in the signing of transactions.

A Bitcoin address is a unique identifier that is used to send and receive Bitcoins. A Bitcoin address is derived from the public key of a user, and it is created by running the public key through a series of cryptographic hash functions, including SHA-256.

Finally, SHA-256 is used in the signing of transactions. When a user wants to send Bitcoins to another user, they must create a transaction and sign it with their private key. The signature is created by running the transaction data and the private key through a series of hash functions, including SHA-256. The signature is then included in the transaction and broadcast to the network, where it is verified by other nodes to ensure that the transaction is valid and has been authorized by the owner of the Bitcoins.

1.1.1.3 What Is Base58 (BitcoinWiki, 2022) and How It Is Used in Bitcoin?

Base58 is a way to encode data, such as addresses and private keys, in a shorter, more user-friendly format. It is commonly used in the Bitcoin network, as well as in other cryptocurrency networks.

Base58 works by representing data as a series of numbers and letters from the base58 alphabet, which consists of the following characters:

123456789ABCDEFGHJKLMNPQRSTUVWXYZabcdefghijklnopqrstuvwxyz.

The base58 alphabet excludes certain characters (such as 0, O, I, and l) that are easily confused with each other when displayed, which helps to reduce the risk of errors when inputting or displaying data.

One of the main advantages of base58 is that it is more compact than other encoding schemes, such as base64. This makes it particularly useful for encoding data that needs to be stored or transmitted in a space-efficient manner, such as addresses and private keys in the Bitcoin network.

In the Bitcoin network, base58 is used to encode a variety of data, including addresses, private keys, and script hashes. For example, a Bitcoin address is a string of characters that consists of a prefix (usually “1” or “3”) and a series of numbers and letters that represent the public key hash of the owner of the address. This address is then encoded using base58 to create a shorter, more user-friendly representation that is easier to share and type.

Private keys in the Bitcoin network are also typically encoded using base58. A private key is a secret piece of data that is used to sign transactions and prove ownership of Bitcoins. It is important to keep private keys secure, as anyone with access to a private key can potentially spend the associated Bitcoins.

1.1.1.4 How Bitcoin Address Is Generated

A Bitcoin address is a unique identifier that is used to send and receive Bitcoin transactions. It is generated using a combination of several cryptographic techniques, including the Secure Hash Algorithm (SHA) and the Elliptic Curve Digital Signature Algorithm (ECDSA).

Here is a detailed explanation of the process (See Fig. 1.1):

- The first step in generating a Bitcoin address is to create a private key. This is a secret number that is used to sign transactions and prove ownership of the Bitcoins in question. Private keys are typically generated using a cryptographically secure pseudorandom number generator (CSPRNG).
- Once the private key has been generated, it is used to create a public key using the secp256k1 elliptic curve which is a curve for ECDSA. The public key is a

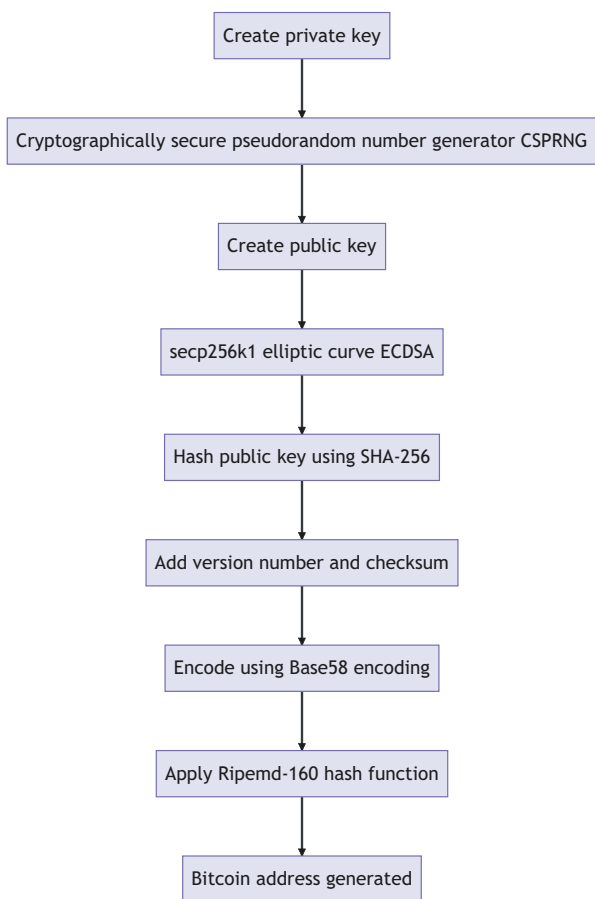


Fig. 1.1 How Bitcoin address is created

point on the curve that is derived from the private key using a set of mathematical equations.

- The public key is then hashed using the SHA-256 hash function to create a public key hash. This hash is typically represented as a string of 64 characters.
- The public key hash is then combined with a version number and a checksum and encoded using Base58 encoding to create the Bitcoin address. Base58 encoding is a way of representing data as a series of letters and numbers that is designed to be more human-readable than other encoding schemes.
- The final step in generating a Bitcoin address is to apply the Ripemd-160 hash function to the result of the Base58 encoding. This creates a shorter, 160-bit version of the address that is more resistant to errors and easier to work with.
- The process of generating a Bitcoin address using these techniques helps to ensure the security and integrity of the Bitcoin network. It also allows users to create addresses that are easy to remember and share with others, while still being virtually impossible to guess or forge.

Note that this is just one example of how a Bitcoin address can be generated, and different methods and algorithms may be used in practice. It is also worth noting that the private key should be kept secret and should not be shared with anyone, as it is used to access and control the Bitcoin associated with the address.

1.1.2 Bitcoin’s Lack of Confidential Property

While the pseudonymous nature of transactions on a public blockchain can help to maintain the confidentiality of the parties involved in the transaction, it is not always foolproof and can be used to discover the identity of the parties involved in certain circumstances.

There are several examples where the pseudonymous nature of transactions on a public blockchain has been used to discover the identity of the parties involved in the transaction. Here are a few examples:

In 2013, Ross Ulbricht, the creator of the dark web marketplace known as the Silk Road, was arrested and charged with several crimes, including money laundering and drug trafficking. Ulbricht used the pseudonym “Dread Pirate Roberts” on the Silk Road, but law enforcement was able to trace the transactions on the site back to him using blockchain analysis (Kushner & McConnell, 2014; Marric, 2021).

In the book “Tracers in the Dark: The Global Hunt for the Crime Lords of Cryptocurrency,” the author discusses how federal agents were able to use the transparent nature of the bitcoin ledger, along with tools like chainalysis.com, to track and prosecute criminals who were using bitcoin for illicit purposes. This demonstrates that while bitcoin may offer some level of anonymity, it is not completely private and can still be subject to investigation and law enforcement action (Chow, 2022).

American Bitcoin ATM operator CoinFlip’s CEO commented in June 2021, “Bitcoin transactions are more traceable than cash” and that it would be “stupid to launder dirty money using Bitcoin” (Sonnenschein, 2021).

There are several ways that a Bitcoin address can potentially be traced back to an individual’s identity:

IP address tracking: If a person uses their own device and an Internet connection to conduct a Bitcoin transaction, it is possible to track the IP address of the device used. This can potentially reveal the location and identity of the person.

Wallet software: If a person uses wallet software to manage their Bitcoin transactions, the software may require them to provide identifying information such as an email address or phone number. This information can potentially be traced back to the individual’s identity.

Exchange identification: If a person buys or sells Bitcoin on an exchange, they may be required to provide identifying information such as a government-issued ID or proof of address. This information can be used to link the individual’s identity to their Bitcoin address.

Blockchain analysis: There are specialized firms that use advanced algorithms to analyze the blockchain and potentially identify patterns or connections that can be traced back to an individual’s identity.

Law enforcement investigation: If a person is under investigation by law enforcement for illegal activities involving Bitcoin, the authorities may use a variety of techniques, including the ones listed above, to try to trace their Bitcoin address back to their identity.

The lack of complete confidentiality in bitcoin and many other public blockchains can be seen as a double-edged sword. On the one hand, the transparency of the blockchain allows law enforcement agencies to track down and prosecute individuals who use bitcoin for illegal purposes. On the other hand, the lack of complete privacy may discourage innocent individuals and businesses from using public blockchains for legitimate transactions, as they may not have full confidence in the privacy of their activities.

1.1.3 Privacy-Preserving Computation for Web3

In order for Web3 applications to be widely adopted in the real world, it will be necessary to incorporate privacy-enhancing features that protect the identities of the parties involved in transactions. This can be achieved through the use of privacy-preserving computation technologies. There are several such technologies currently under active research and development, including zero-knowledge proof, multi-party computation, homomorphic encryption, and differential privacy. These technologies aim to enable Web3 applications to provide the benefits of blockchain technology while also preserving the privacy of users.

A **zero-knowledge proof (ZKP)** is a type of cryptographic protocol that allows one party (the prover) to prove to another party (the verifier) that they possess certain information without revealing the actual information itself.

In the context of blockchain, ZKP can be used to enhance privacy and scalability. For example, a user could use zero-knowledge proof to prove that they own a certain amount of cryptocurrency without revealing their identity or the specific addresses of their wallets. This can help to protect the user's privacy, as the verifier does not need to know the user's identity or the details of their transactions in order to verify the proof.

For example, Zcash allows users to create a private transaction by providing zero-knowledge proof that their transaction is valid, without revealing any information about the sender, recipient, or amount involved. To create a zero-knowledge proof for a Zcash transaction, a user must first create a "shielded" address, which is a special kind of address that is designed to protect the privacy of its owner. The user can then create a private transaction by sending funds from a standard address to the shielded address, along with zero-knowledge proof that the transaction is valid. The zero-knowledge proof is a mathematical proof that verifies the transaction without revealing any information about it. Once the proof is verified, the transaction is added to the Zcash blockchain and the funds are transferred to the shielded address, completing the private transaction (Zcash, 2016).

Zero-knowledge proofs can also be used to improve the scalability of a blockchain by enabling the verification of transactions without the need to store or transmit the entire transaction data. This can help to reduce the amount of data that needs to be stored on the blockchain and make it more efficient (Burger, 2022).

Multi-party computation (MPC) is a type of privacy technology that allows multiple parties to jointly compute a function over their inputs without revealing their inputs to each other. MPC is based on the concept of secure multi-party computation, which involves the use of cryptographic techniques to enable multiple parties to compute a function over their inputs in a way that preserves the privacy of the inputs (Lindell, 2020).

MPC can enhance the security and privacy of blockchain-based solutions in various ways. One such use case is protecting identity wallets by using MPC to shard keys and reconstruct them dynamically with input from all parties. This makes it more difficult for a single party to compromise the transaction (Fireblocks, 2020).

MPC can also be used for high-value transactions that require the approval of multiple parties before being executed. Additionally, MPC can be utilized to maintain transaction privacy and confidentiality by offloading sensitive transactions from the blockchain and processing them through MPC, with the transaction receipt recorded on the blockchain as proof. Another example of the use of MPC and blockchain together is in reserved or sealed bid auctions, where MPC can be used to determine the highest bid while keeping bid amounts confidential. Blockchain can then be used to ensure fairness and transparency in the auction process by recording all relevant information immutably on the shared ledger (Wipro, 2020).

Another use of MPC is private key management. MPC replaces individual private keys with distributed key shares, allowing distributed parties to participate in a

signing process that is both auditable and policy-compliant. For example, Google Cloud's Confidential Space, built on their Confidential Computing platform, leverages remote attestation and Secure Encrypted Virtualization to provide a more secure environment and fast performance. This allows MPC to facilitate governance, preventing a single malicious insider from stealing assets. MPC solutions will become increasingly essential as blockchains continue to support critical infrastructure within the global financial system (Portier & Diya, 2023).

Homomorphic encryption is a type of encryption that allows mathematical operations to be performed on encrypted data as if it were unencrypted. This means that the encrypted data can be processed and analyzed without first being decrypted, which can help to protect the privacy of the data (Gillis, 2022).

Homomorphic encryption has a number of potential uses in privacy technology, including:

Secure cloud computing: Homomorphic encryption can be used to enable secure cloud computing, where sensitive data can be processed and analyzed in the cloud without the need to decrypt the data. This can help to protect the privacy of the data while still allowing it to be accessed and analyzed remotely.

Secure data sharing: Homomorphic encryption can also be used to enable secure data sharing between parties, allowing sensitive data to be shared without revealing its contents to unauthorized individuals.

Secure voting systems: Homomorphic encryption can be used to enable secure electronic voting systems, where votes can be counted and tallied without revealing the individual votes to anyone.

In the context of blockchain, homomorphic encryption can be used to enable privacy-preserving smart contracts and other applications that require the processing of sensitive data. For example, a smart contract could use homomorphic encryption to enable the processing of sensitive data without revealing the data to any of the parties involved in the contract (Hindi, 2022; Solomon & Almashaqbeh, 2021).

Differential privacy is a mathematical concept that describes a set of techniques for protecting the privacy of individuals in a dataset while still allowing the dataset to be analyzed and used for research or other purposes (Joubert, 2021).

In differential privacy, data is collected and aggregated in a way that ensures that any individual's data is not identifiable or distinguishable from the data of other individuals. This is achieved through the use of randomized perturbations, which add noise to the data in a controlled way. The noise is added in such a way that it does not significantly impact the accuracy of the overall data analysis, but it makes it difficult or impossible to identify any individual data points.

Differential privacy is used in a variety of privacy technology applications, including in the analysis of data from social media, healthcare records, and other sources.

In the context of blockchain, differential privacy can be used to protect the privacy of individuals who use the blockchain by adding noise to the data that is stored on the blockchain. For example, a blockchain-based system that is used to track medical records could use differential privacy techniques to ensure that the data is

aggregated in a way that does not reveal the identity or personal details of any individual patients (Wu, 2020).

1.2 The Integrity Property of Blockchain

Integrity refers to the accuracy and completeness of information, as well as the protection of information from unauthorized modification. In the context of blockchain, integrity is an important concept because it helps to ensure that the data stored on the blockchain is accurate and has not been tampered with.

In a traditional database, the integrity of the data is typically maintained by a central authority, such as a database administrator. However, in a decentralized blockchain system, there is no central authority to ensure the integrity of the data. Instead, the integrity of the data is maintained through the use of cryptographic techniques, such as hash functions and digital signatures, which allow users to verify the authenticity and integrity of the data.

In addition, One of the key features of a blockchain is its immutability via the consensus algorithm, which means that once data has been added to the blockchain via the consensus algorithm, it cannot be altered or deleted. This is an important aspect of maintaining the integrity of the data on the blockchain, as it ensures that the data remains accurate and complete over time.

However, it is important to note that the immutability of blockchain data is not absolute, and there are ways in which the data on a blockchain can be changed or compromised.

1.2.1 *The Integrity of the Base Layer of Blockchain*

One way in which the immutability of blockchain data can be breached is through attacking the base layer or layer 1 of the blockchain via exploiting consensus algorithms or manipulating transaction signatures.

The followings are some examples of integrity attacks on base-layer blockchain:

Finney attack: This attack is a type of double-spending attack that can be executed on blockchain networks that use a proof-of-work consensus mechanism. The attack is named after Hal Finney, the first person to receive a Bitcoin transaction from Satoshi Nakamoto. An attacker creates a new transaction that sends some cryptocurrency to a merchant or exchange and then mines a new block on the blockchain that includes the transaction. Before the merchant or exchange can confirm that the transaction is valid, the attacker creates a second transaction that sends the same cryptocurrency to a different address controlled by the attacker. The attacker then mines another block that includes the second transaction, and this block becomes the longest chain on the network. The merchant or exchange confirms the first transaction, but it is now invalid because the second transaction has been mined

into the longest chain. To prevent this kind of attack, it is highly recommended to wait for at least 6 confirmations on the Bitcoin network to consider a transaction as safe and irreversible (Bit2Me Academy, 2019).

Race attack: This attack is executed when an attacker creates two conflicting transactions. The first transaction is sent to the victim, who accepts the payment (and sends a product, for instance) without waiting for confirmation of the transaction. At the same time, a conflicting transaction returning the same amount of cryptocurrency to the attacker is broadcast to the network, eventually making the first transaction invalid (Chaudhary et al., 2015).

Vector76 attack: Vector 76 is a type of double-spending attack that combines elements of the Race and Finney attacks. In this attack, a malicious miner creates two nodes: one connected to an exchange service and the other connected to well-connected peers in the blockchain network. The attacker then creates two transactions, one high-value and one low-value. The attacker pre-mines and withholds a block containing the high-value transaction from the exchange service. Once a block is announced, the attacker quickly sends the pre-mined block directly to the exchange service, which will consider it as the main chain and confirm the transaction along with some miners. This attack takes advantage of differences in network propagation times to trick the exchange service into accepting a fraudulent transaction (Spacebot, 2021).

Transaction malleability attack: This attack allows someone to change the unique ID of a Bitcoin transaction before it is confirmed on the network. This can be used to pretend that a transaction did not happen, which can lead to double deposits or withdrawals on Bitcoin exchanges. Signature malleability is one form of this attack, where signatures are not properly encoded and can be manipulated to create new transactions (Paxful, 2020).

Nothing-at-stake attack: The nothing-at-stake problem is a theoretical security issue in proof-of-stake consensus systems in which validators have a financial incentive to mine on every fork of the blockchain that takes place, which is disruptive to consensus and potentially makes the system more vulnerable to attacks. The optimal strategy for any miner in the event of a fork is to mine on every chain, so that the miner gets their reward no matter which fork wins. This can lead to a situation where an attacker mines blocks on multiple competing chains simultaneously, potentially allowing the attacker to profit from both chains (Yaffe, 2018).

Bribe attack: A bribe attack is an attempt to change the history of a blockchain by paying miners a reward (bribing) if they create fork blocks instead of building on top of the longest chain. Typically, the attacker attempts to double-spend funds in a bribe attack. He does this by creating a fork containing bribe money freely available to any miners adopting the fork. The attacker would begin with a large pool of funds in an address and then broadcast a transaction moving all of these funds to another address and wait for it to be included in a block. The attacker would then try to introduce a fork by finding an alternate block (Hicks, 2018).

Long-range attack: A long-range attack is a theoretical attack on a blockchain that involves an attacker who creates a copy of an older version of the blockchain and then tries to convince the rest of the network to adopt it, potentially allowing the

attacker to reverse transactions or double-spend coins. In a long-range attack, instead of starting a fork 6 blocks back, the attacker starts the fork 60,000 blocks back, or even at the Genesis Block (Buterin, 2014).

51% attack: A 51% attack occurs when a group of attackers controls more than half of the computing power on a blockchain network. This allows them to potentially reverse or alter transactions on the blockchain, or even block new transactions from being added to the chain. 51% attacks have occurred on a number of different blockchain networks, including Bitcoin Gold in May 2018 (Martin, 2020) and multiple attacks in Ethereum Classic in 2020 (Voell, 2020).

Selfish mining: Selfish mining occurs when a group of miners work together to withhold blocks from the network in order to increase their own profits. This can potentially lead to a reduction in the security and integrity of the network. A selfish mining attack occurred on a Japanese cryptocurrency Monacoin in 2018 (Gutteridge, 2018).

Sybil attack: A Sybil attack occurs when a single entity creates multiple fake identities in order to gain disproportionate influence on a blockchain network. This can potentially lead to a reduction in the security and integrity of the network. In 2014, a Sybil Attack was launched against Tor, a peer-to-peer network that enables private conversations, leading to the discovery of the locations and identities of some Tor users (Goodin, 2014). The attack was carried out by an individual who controlled about 115 relays from a single IP address, giving them an undue level of influence over the network.

Eclipse attack: An Eclipse attack is a type of attack that targets a blockchain network by isolating a particular node or a set of nodes from the rest of the network. The goal of an Eclipse attack is to control the targeted node or nodes, allowing the attacker to manipulate the blockchain network's transactions and potentially execute double-spending attacks. In an Eclipse attack, the attacker floods the targeted node with a large number of fake IP addresses, making it impossible for the node to connect to legitimate peers on the network. The attacker then takes control of the node, allowing them to control the flow of information within the network. With this control, the attacker can selectively drop certain transactions, modify the order in which transactions are processed, and potentially execute double-spending attacks. To execute an Eclipse attack, the attacker needs to have a significant number of IP addresses and control over a large number of nodes in the blockchain network. The larger the network, the more difficult it is to execute an Eclipse attack successfully. Therefore, smaller blockchain networks are more vulnerable to Eclipse attacks than larger networks.

To prevent an Eclipse attack, blockchain networks can implement various security measures, such as firewalls, intrusion detection systems, and network segmentation. Additionally, peer-to-peer networks can implement mechanisms to verify the identity of nodes, such as public key cryptography or digital signatures. By verifying the identity of nodes, blockchain networks can prevent attackers from hijacking nodes and manipulating the network's transactions (Deer, 2021).

In summary, these attacks use various malicious methods to compromise blockchain integrity. It is important for developers and users of the blockchain ecosystem

to be aware of these potential attacks in order to take appropriate measures to prevent them.

1.2.2 The Integrity of Layer2 Blockchain

1.2.2.1 Bitcoin Layer 2 Lightning Network Attack

The Lightning Network, Bitcoin's layer 2 scaling protocol, has been found to have a vulnerability by researchers at the University of Illinois. In an academic paper, Cosimo Sguanci and Anastasios Sidiropoulos described a hypothetical attack that could be carried out by a collusion of node operators. They estimated that a coalition of 30 nodes could steal 750 bitcoin at the time of publication in 2022, highlighting the potential for significant losses (Protos, [2022a, b](#)).

1.2.2.2 Attacks on Ethereum Layer 2 Rollups

Rollups, such as Optimism and Arbitrum, are believed to be less secure than users may think due to their centralized sequencers and inadequate fraud-proof systems. Despite this, they are still considered acceptable as long as they move toward decentralization in the future. There are other security concerns with rollups besides centralization, as their core codebase (Ethereum-based smart contracts) can be vulnerable to hacking, just like any other blockchain-based program. This highlights the risk of smart contract security for rollup platforms. Upgrade issues can also pose a problem for rollups, as they can result in harmful upgrades, such as the Nomad bridge smart contract attack (although not directly related to the rollup smart contract) in August where a faulty upgrade of the smart contract enabled the theft of nearly \$200 million (Kovacs et al., [2022](#)). Both Optimism and Arbitrum aim to increase their upgrade safety and decentralization in the future, but it will be challenging to prevent malicious upgrades while maintaining security.

In 2022, a hacker made off with \$2 million in bug bounty after discovering a concerning vulnerability with the Ethereum network through Optimism, an Ethereum layer 2 rollup solution. The hacker, Saurik, who is known as a "grey hat," informed the Ethereum team of the vulnerability and received a substantial reward in return. In a report, Saurik explained how he found the vulnerability by examining nano payments protocols on the rollup. He discovered a weakness that could have allowed an attacker to withdraw a virtually unlimited amount of ETH from the solution (Protos, [2022a, b](#)).

1.2.2.3 Attacks on Layer 2 Bridges

A cross-chain bridge allows for the transfer of digital assets between different blockchain networks and facilitates communication and interoperability between these platforms, eliminating the need for a central intermediary. However, these bridges come with security risks such as an expanded attack surface for hackers and the lack of thorough examination of code, which could lead to hacking. Additionally, cross-chain bridges, being public and featuring smart contracts, can be vulnerable to hacking and hold large reserves of various currencies, increasing the overall risk for the bitcoin ecosystem. The following are notable attacks on layer 2 bridges:

Qubit

Qubit Finance, a DeFi platform that offers money market services, connecting borrowers and lenders and offering peripheral bridging services, was targeted by an attacker on January 27th, 2022. The attacker exploited a vulnerability in the deposit function of the Qubit bridge contract and drained crypto assets worth over \$80 million. The attacker used a null address and a large ETH amount to bypass security measures in the QBridgeHandler contract, minting 77,162 \$xETH, worth over \$185 million at the time. The tokens were then used to borrow other assets, which were eventually swapped for BNB coins, causing significant losses for Qubit (Gardner, 2022).

1.2.2.4 Wormhole Attack

Wormhole, a decentralized finance (DeFi) platform that helps users transfer cryptocurrency between the Solana and Ethereum blockchains, was targeted by an attacker on February 2nd, 2022. The attacker exploited a security flaw in Wormhole's token bridge, called Portal, and managed to steal assets worth around \$325 million. The vulnerability was found in the transfer process between Ethereum and Solana, where the attacker was able to mint 120,000 \$wETH on Solana without making a deposit on the Ethereum side. As a result, the value of \$SOL dropped by over 10%. The parent company of Wormhole, Jump Crypto, quickly took action to restore the stolen funds and offered a record-breaking bug bounty of \$10 million to the attacker (Faife, 2022).

Ronin Attack

Ronin is a network created by the creator of the popular game Axie Infinity to support its growing user base. The network uses a Proof of Authority consensus algorithm, where a select group of trusted validators stakes their identity to validate transactions. On March 23rd, 2022, a major hack occurred when the private keys for four validators managed by Sky Mavis were compromised. The attackers also obtained the signature for the fifth validator from Axie DAO through a backdoor in Sky Mavis's systems. This allowed the attackers to fraudulently approve two withdrawals from the bridge contract, one for 173,600 ETH and another for 25.5 million USDC. The total stolen amount was valued at over \$600 million, making it the

largest crypto hack ever recorded. After conducting a thorough investigation, the Ronin team, along with Chainalysis, Certik, and Verichains, determined that the infamous North Korean cybercrime group, the Lazarus Group, was behind the attack (Browne, 2022).

Nomad Attack

Nomad is a protocol that facilitates communication and transfer of digital assets between Ethereum, Avalanche, Evmos, and Moonbeam blockchains. On August 8th, 2022, the protocol suffered a major attack that resulted in the theft of nearly all of its assets, estimated at around \$190 million. The attack was triggered by a software update that introduced a critical error in the validation mechanism of the Replica smart contract. This allowed the attacker to perform small transfers of one cryptocurrency on one blockchain and receive large amounts of another cryptocurrency on another blockchain. The exploit was later repeated by other attackers (Korn, 2022).

Defense Measures for Bridge Attacks Include

Performing Rigorous Code audits:

A rigorous code audit is an important step in ensuring the security of smart contracts and the assets they manage. In the context of bridge contracts, it is especially critical as the bridge serves as a gateway for assets to move between different blockchain networks. A security audit of the smart contract code can help identify potential vulnerabilities and weaknesses in the code, which can then be fixed before the code is published on the blockchain. Smart contract security audits are typically conducted by professional smart contract auditors or security firms. These audits can range from basic code reviews to more complex security assessments that cover a variety of attack scenarios. The objective of these audits is to identify potential weaknesses and vulnerabilities in the code that could be exploited by attackers. In addition to a private security audit, companies can also conduct an extensive bounty program where they offer rewards to individuals who identify and report potential vulnerabilities in the code. This program can help incentivize the wider security community to actively participate in finding and reporting vulnerabilities, which can further strengthen the security of the code.

P2P Bridges:

P2P-based bridges provide a more secure way to facilitate inter-chain trading. Unlike traditional bridges, which rely on sophisticated smart contracts and centralized liquidity pools, P2P bridges use atomic swaps and order book mechanisms to facilitate trades between different blockchain networks. Swaps are described as “atomic” because with each order, either the trade completes and two users exchange funds or the trade does not complete and original funds are distributed back to the two users. This approach eliminates the need for intermediaries and reduces the risk of attack. In a P2P-based bridge, two users can exchange assets directly with each other, without relying on a centralized intermediary. This eliminates the need for a central party to hold and manage assets, which greatly reduces the risk of attack. Additionally, P2P bridges can be completely decentralized and trustless, which eliminates the need for users to trust a third party with their assets. Overall,

P2P-based bridges provide a more secure and efficient solution for inter-chain trading and are an increasingly popular alternative to traditional bridges.

1.2.3 Integrity of Smart Contract

Smart contracts are self-executing contracts with the terms of the agreement between buyer and seller (or any parties in a transaction) being directly written into lines of code. The integrity of a smart contract is important because it ensures that the terms of the contract are enforced accurately and consistently.

However, there are several ways in which the integrity of a smart contract could potentially be breached:

Code vulnerabilities: Like any software, smart contracts are subject to vulnerabilities and bugs that could potentially be exploited to compromise the integrity of the contract. For example, if a vulnerability is discovered in the code of a smart contract, it could potentially be exploited to alter the terms of the contract or bypass the contract's protections.

Human error: Smart contracts are only as good as the code that defines them. If there are errors or mistakes in the code, the contract may not function as intended, which could compromise its integrity.

In Chap. 4, we will discuss in more detail smart contract security.

1.3 The Availability Property of Blockchain

In the context of computer security, availability refers to the ability of authorized users to access a system or its resources when they need to. It is one of the three main pillars of information security, along with confidentiality and integrity.

Attacks on availability are designed to disrupt access to a system or its resources, often by overwhelming it with traffic or requests. Examples of attacks on availability include:

Denial of Service (DoS) attacks: These attacks flood a system with traffic or requests, overwhelming it and making it unavailable to legitimate users.

Distributed Denial of Service (DDoS) attacks: These attacks involve multiple attackers or compromised systems coordinating to flood a target with traffic or requests, making it even harder to defend against.

Ransomware attacks: These attacks encrypt a system's data and resources, making them unavailable to the victim until a ransom is paid to the attackers.

Supply chain attacks: These attacks involve compromising a system or its components as they are being manufactured or delivered, making it unavailable to users when it is deployed.

It is important to protect against attacks on availability, as they can have serious consequences for businesses, organizations, and individuals, including financial

losses, reputational damage, and the inability to access important information or services.

For blockchain, the availability issues can include the following:

- **Data availability:** This refers to the ability to access and view information stored on the blockchain network. This can include transaction history data, which is a record of all transactions that have taken place on the blockchain, events, which are actions that occur within smart contracts, and metadata of the transactions, which can include information such as the time and date of the transaction, and off-chain data, which refers to data that is not stored directly on the blockchain but is related to the transactions taking place on the blockchain.
- **Smart contract availability:** Smart contracts are self-executing contracts with the terms of the agreement between buyer and seller being directly written into lines of code. They are stored on the blockchain, and the availability of smart contracts refers to the ability to access and use these contracts. For example, in some cases, it may be necessary to pause the execution of a smart contract for maintenance or security reasons. In such cases, a pausing interface can be used to make the smart contract temporarily unavailable. Another example is the *Selfdestruct* in Ethereum smart contract which is used to remove the smart contract byte code from the blockchain. Once *Selfdestruct* is called, the smart contract becomes unavailable. This actually happened when an earlier version of the “selfdestruct” function called “suicide” is invoked against the Parity wallet library code which destroyed the contract and make the funds locked inside the contract unavailable permanently (Mueller, 2017). The security of smart contracts will be discussed in Chap. 4.
- **Non-censorship of transactions:** One of the key features of blockchain is that it is decentralized and not controlled by any single entity. This means that transactions cannot be censored or restricted in any way. This allows for greater transparency and trust in the system, as no one can interfere with or manipulate the transaction process.
- **RPC node availability:** An RPC (Remote Procedure Call) node is a server that allows external applications to interact with the blockchain network. The availability of RPC nodes refers to the ability of these external applications to connect to and communicate with the blockchain network. This is important for the functioning of decentralized applications (dApps) that rely on the blockchain for their operation.
- **Wallet service availability:** A wallet is software that allows users to interact with the blockchain network, such as sending and receiving digital assets. The availability of wallet services refers to the ability to access and use these wallets. This is important for allowing users to manage their digital assets and participate in the blockchain network.
- **Web3 dApp architecture availability:** Web3 refers to the next generation of web development, which utilizes blockchain technology. This includes front-end hosting services, middle-tier, and databases. For example, user profiles or transaction context can be stored on decentralized storage solutions like IPFS

(InterPlanetary File System), and oracle services can be used to connect smart contracts with off-chain data.

- Oracle availability: Oracles are third-party services that provide external data to smart contracts. They act as a bridge between the blockchain network and the outside world. For example, an oracle could be used to provide weather data to a smart contract that is being used to execute a weather-based insurance policy. Availability of oracle services refers to the accessibility and reliability of these third-party services.

This section focuses on data availability via replication and scaling solutions.

1.3.1 Availability via Data Replication

In a blockchain, data replication refers to the process of copying data from one node to another. This is important because it ensures that the data on the blockchain is not lost if a single node fails or becomes unavailable. Data replication also helps to improve the speed and efficiency of the blockchain, as it allows multiple nodes to access and process the data simultaneously.

At its core, a blockchain is a replicated deterministic state machine. A state machine is a mathematical model that represents a system's behavior by defining various states and transitions between them. In a blockchain, a state machine can be used to model the system's behavior and to ensure that all nodes reach a consensus about the state of the blockchain.

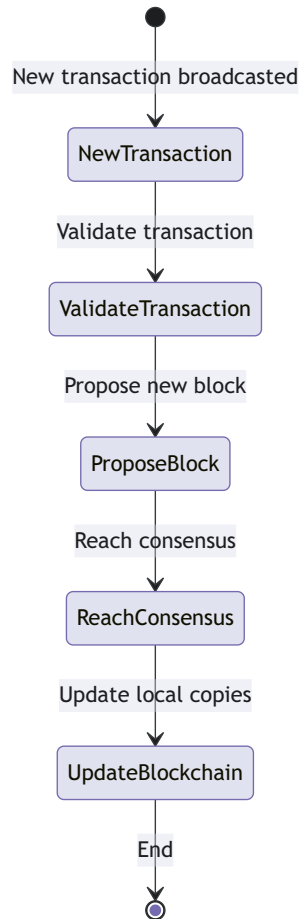
Figure 1.2 depicts blockchain data replication using State Machine with the following steps:

- New transactions are broadcasted to the network
- Nodes validate the transactions and add them to their local copy of the blockchain
- Nodes propose new blocks containing validated transactions
- The network reaches a consensus on the new block
- The new block is added to the blockchain, and nodes update their local copies

1.3.2 Availability via Scalability

Scalability technology for blockchain can be used to ensure the availability of the blockchain network by addressing one of the main challenges facing blockchain technology: the ability to handle a large number of transactions. As more users and transactions are added to a blockchain network, the number of nodes in the network increases, and the amount of data that needs to be processed and stored also increases. This can lead to slow transaction processing times and high storage costs.

Fig. 1.2 Blockchain as a State Machine



Scalability solutions aim to address this issue by increasing the capacity of the blockchain network to handle more transactions and users. Some of the most popular scalability solutions include:

Sharding: This technique involves dividing the blockchain into smaller “shards” or partitions, each of which can be processed and stored separately. This allows for parallel processing and storage of transactions, increasing the overall capacity of the network.

Off-chain transactions: This technique involves moving some of the transactions off the blockchain, reducing the number of transactions that need to be processed and stored on the blockchain itself. This can be done using payment channels or sidechains, which allow for faster, cheaper transactions that are settled on the main blockchain at a later time.

Layer-2 scaling solutions: This technique involves adding a layer on top of the blockchain to handle additional transactions, without changing the underlying blockchain protocol. An example is the lightning network for Bitcoin.

We will discuss these scaling solutions in the next sub-sections.

1.3.2.1 Sidechain VS Layer-2

Sidechain

A sidechain is a blockchain that is connected to the main one. Different sidechains have different goals, so they come in various forms with different capabilities and purposes. Each sidechain operates under its own set of rules, including potentially a different consensus mechanism from the main chain, which can lead to more efficient blockchain operations. Sidechains can enhance transaction processing by independently validating transactions and periodically updating the main chain, allowing blockchains to scale better. However, sidechains also come with their own security risks, as demonstrated by the 801,601 MATIC token theft on Polygon in December 2021 before the issue was resolved (Polygon, [2021](#)).

Layer-2

Layer-2 solutions enhance scalability and transaction processing while maintaining the security of the main blockchain. Layer-2 Rollups play a crucial role in scaling by allowing transactions to be grouped and processed off the main blockchain while still recording the transaction data on the main chain, improving transaction handling capacity. However, layer-2 also has limitations, such as exacerbating the issue of inter-chain compatibility.

ZKPs (Zero-Knowledge Proofs) in Rollups optimize efficiency through recursion, where multiple proofs are combined into a single smaller proof. Many protocols acknowledge the need for recursive ZKPs to reduce costs and improve efficiency, but the efficiency of proof schemes varies. It is important to note that the effectiveness of proof schemes can vary.

1.3.2.2 Data Availability and Layer 2 Solutions

One of the challenges with rollups or other layer 2 solutions is ensuring that all of the data associated with each transaction is available and accessible to all participants in the network. If this data is not available, it can lead to security issues and potential loss of funds.

To address this problem, several approaches have been proposed. One approach is to use fraud proofs, which allow participants to prove that certain transactions are invalid if they are not properly executed or if data is missing. Another approach is to

use data availability sampling, which involves randomly selecting a subset of nodes in the network to verify that all necessary data is available.

Other potential solutions include using cryptographic techniques like zero-knowledge proofs, which can help improve scalability while maintaining security and data availability.

Use Fraud Proof to Solve Data Availability Problems

Fraud proofs are a mechanism used to ensure that all nodes on a blockchain network have access to the same data. They work by allowing nodes to submit evidence of any missing or invalid data, which can then be used to penalize nodes that are withholding or manipulating data. This helps ensure that all nodes have access to the same data and helps prevent inconsistencies and potential security vulnerabilities.

Ethereum is an example of a mainstream blockchain project that utilizes fraud proofs, which the Optimism team has recently renamed as “fault proofs,” as part of its Optimism framework. This framework is designed to enhance scalability and lower transaction costs by creating “child chains” linked to the primary Ethereum chain. Child chains can process transactions faster and more affordably than the primary chain, but they still rely on it for security.

To guarantee that all nodes have access to the same data, Optimism utilizes fault proofs. If a node discovers any missing or invalid data on a child chain, it can submit evidence to the primary chain. The primary chain can then use this evidence to penalize any nodes found to be withholding or manipulating data on the child chain (Optimism, 2022).

Use Data Sampling to Solve Data Availability Problem

Data sampling is a technique that is used to ensure that all necessary data associated with a transaction is available and accessible to all participants in the network. This involves randomly selecting a subset of nodes in the network to verify that they have access to the data, and if not, taking steps to ensure that it is made available.

The basic idea behind data availability sampling is to use statistical methods to ensure that the probability of data unavailability is low enough that it can be considered negligible. By randomly selecting nodes in the network and verifying that they have access to the necessary data, it becomes less likely that any one node will be able to withhold or manipulate data without being detected.

Several blockchain projects are exploring the use of data availability sampling as a way to improve scalability and reduce costs. For example, Ethereum 2.0, which is currently under development, includes a feature called “data availability checks” that uses sampling techniques to ensure that all necessary data is available before processing transactions.

Other projects using similar techniques include Polkadot, which uses “fishermen” nodes to monitor for invalid transactions or missing data, and Avalanche, which uses “sub-sampling” techniques to randomly select nodes for verification.

Use Zero-Knowledge Proof (ZKP) to Solve Data Availability Problems

Zero-Knowledge Proof (ZKP) is a cryptographic method that allows nodes to generate a proof without revealing any data. In the case of data availability problems for layer 2, nodes can use ZKP to generate a proof that they have the data without revealing the

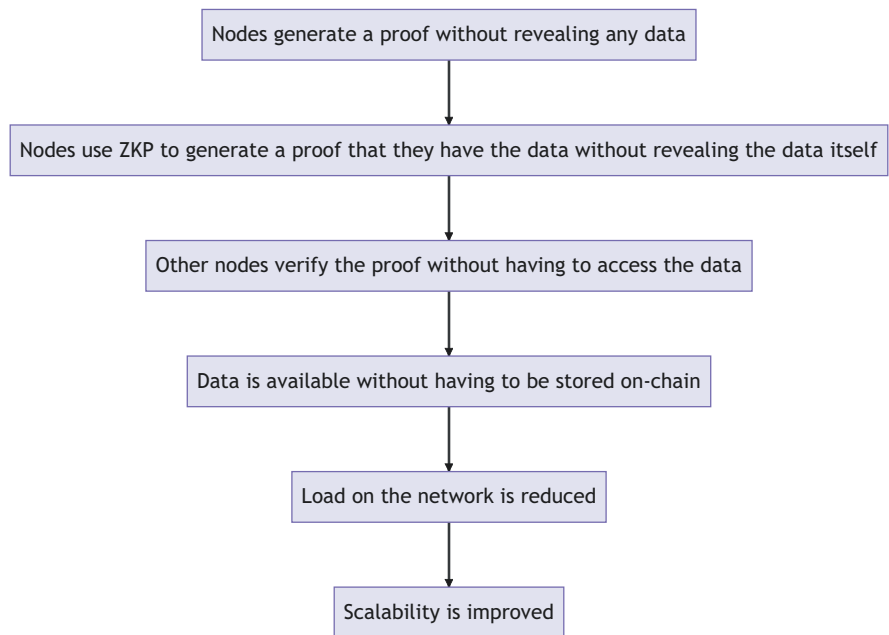


Fig. 1.3 Use ZKP for data availability

data itself. Other nodes can then verify the proof without having to access the data. This allows for data to be available without having to be stored on-chain, which can help to reduce the load on the network and improve scalability (see Fig. 1.3).

By using zero-knowledge proofs in this way, blockchain networks can ensure that all nodes have access to correct and valid data without requiring each node to store all of that data themselves. This helps improve overall network scalability and reliability while still maintaining high levels of security and privacy.

One example of a mainstream blockchain project that uses zero-knowledge proofs for addressing data availability issues is Quorum, which is an enterprise-focused version of Ethereum developed by JPMorgan Chase. Quorum uses a technique called “private state validation” which involves creating zero-knowledge proofs for private transactions on the network. These proofs allow nodes on the network to validate private transactions without having access to sensitive information about those transactions.

1.3.2.3 Bitcoin Lightning Network for Better Availability

The Lightning Network is a protocol that enables fast and low-cost transactions between two parties using Bitcoin. By creating a payment channel, users can send unlimited transactions without affecting the Bitcoin network. The channel operates like its own ledger, where one party locks in a certain amount of Bitcoin, and the

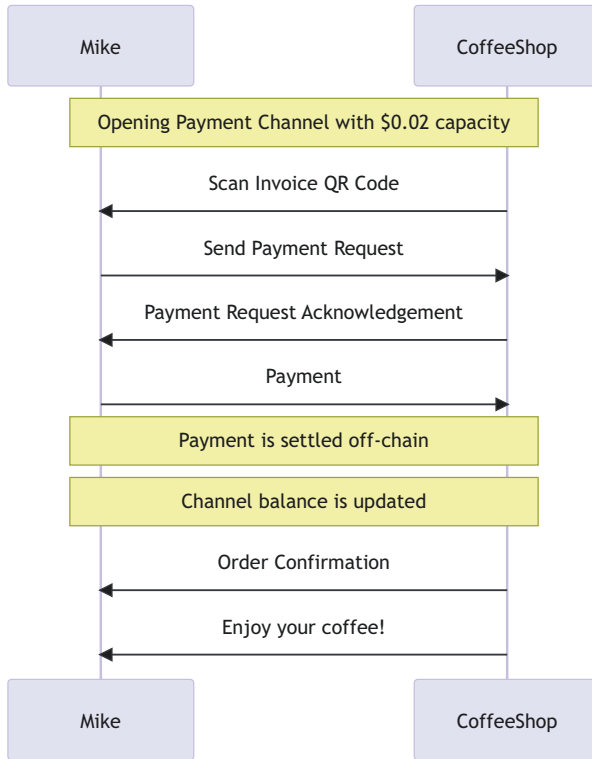


Fig. 1.4 Using lightning network for small payment

other party invoices as needed. Transactions within the channel are faster and cheaper than traditional Bitcoin transactions. When the channel is closed, the information is consolidated into one transaction and sent to the main Bitcoin network for recording. This eliminates the issue of congesting the network with small transactions. An example is a customer visiting a coffee shop and paying in Bitcoin through a Lightning Network channel, avoiding high fees and long validation times associated with small transactions on the regular Bitcoin network.

As described in Fig. 1.4, the Lightning Network allows Mike to open a payment channel with the coffee shop. This creates a smart contract between the two parties where transactions can be made instantaneously, cheaply, or even for free. These transactions are recorded within the channel and the coffee shop is still paid. When the channel is closed, all of its transactions will then be recorded to the main Bitcoin blockchain.

The Lightning Network allows for off-chain transactions that are trusted to enforce the blockchain and are automatically fulfilled once the preset requirements are met. These transactions are anonymous within the channel, with only the total transfer of value visible. The Lightning Network’s design relies on the mainchain as the arbiter of all transactions, integrating the off-chain ledger back into the mainchain.

To facilitate payments on the Lightning Network, users can create a series of HTLCs. An HTLC is a type of smart contract that enables secure off-chain transactions between parties. It is called “Hashed Time-Locked Contract” because it involves two main components: a hash function and a time-lock.

Here is how an HTLC-based transaction works on the Lightning Network:

- Alice wants to send 0.1 BTC to Bob, and they have a payment channel open between them.
- Alice generates a random secret value and creates an HTLC that includes the hash of that secret value.
- Alice sends the HTLC to Bob, along with the hash of the secret value.
- Bob receives the HTLC and verifies that the hash of the secret value matches the hash that Alice sent.
- Bob creates a new HTLC with a time-lock, which is the time period during which the funds are locked in the channel.
- Bob sends the new HTLC to Alice, along with the hash of the secret value and the time-lock.
- Alice receives the new HTLC and verifies that the hash and time-lock are correct.
- Alice reveals the secret value to Bob, which allows him to claim the original HTLC she sent.
- Bob uses the secret value to claim the original HTLC, and then sends the funds from the new HTLC back to Alice.
- The payment channel between Alice and Bob is updated with the new balances.

In this way, HTLCs allow for secure off-chain transactions between parties, while maintaining the security of the Bitcoin blockchain. If any party tries to cheat by refusing to release the secret value or by broadcasting an old channel state, the HTLCs will time-out and the funds will be returned to their original owners.

References

- Bit2Me Academy. (2019). *What is a Finney Hack or Finney attack?* Bit2Me Academy. Retrieved January 16, 2023, from <https://academy.bit2me.com/en/que-es-un-hackeo-finney-ataque-finney/>
- BitcoinWiki. (2022). *Base58 algorithm. All about cryptocurrency.* BitcoinWiki. Retrieved February 3, 2023, from <https://en.bitcoinwiki.org/wiki/Base58>
- Boneh, D. (2020, July 11). *Schnorr digital signature scheme.* <https://link.springer.com/>. Retrieved February 3, 2023, from https://link.springer.com/referenceworkentry/10.1007/978-1-4419-5906-5_154
- Browne, R. (2022, April 15). *Ronin hack: North Korea linked to \$615 million crypto heist, U.S. says.* CNBC. Retrieved March 16, 2023, from <https://www.cnbc.com/2022/04/15/ronin-hack-north-korea-linked-to-615-million-crypto-heist-us-says.html>
- Burger, E. (2022, April 15). *Decentralized speed: Advances in zero knowledge proofs.* Andreessen Horowitz. Retrieved January 2, 2023, from <https://a16z.com/2022/04/15/zero-knowledge-proofs-hardware-decentralization-innovation/>
- Buterin, V. (2014, May 15). *Long-range attacks: The serious problem with adaptive proof of work | Ethereum foundation blog.* Ethereum Foundation Blog.

- Retrieved March 16, 2023, from <https://blog.ethereum.org/2014/05/15/long-range-attacks-the-serious-problem-with-adaptive-proof-of-work>
- Chaudhary, K., Fehnker, A., van de Pol, J., & Stoelinga, M. (2015, November 13). [1511.04173] *Modeling and verification of the bitcoin protocol*. arXiv. Retrieved January 16, 2023, from <https://arxiv.org/abs/1511.04173>
- Chow, A. R. (2022, December 8). *How investigators are tracing crypto criminals | time*. TIME. Retrieved January 2, 2023, from <https://time.com/6239364/crypto-criminals-andy-greenberg/>
- Deer, M. (2021, December 11). *What is an eclipse attack?* Cointelegraph. Retrieved March 16, 2023, from <https://cointelegraph.com/explained/what-is-an-eclipse-attack>
- Faife, C. (2022, February 3). *Wormhole cryptocurrency platform hacked for \$325 million after error on GitHub*. The Verge. Retrieved March 16, 2023, from <https://www.theverge.com/2022/2/3/22916111/wormhole-hack-github-error-325-million-theft-ethereum-solana>
- Fireblocks. (2020). *MPC wallet as a service technology*. Fireblocks. Retrieved January 2, 2023, from <https://www.fireblocks.com/platforms/mpc-wallet/>
- Gardner, A. (2022, January 28). *Hackers seize \$80 million from Qubit in latest DeFi attack*. Bloomberg News. Retrieved March 16, 2023, from <https://www.bloomberg.com/news/articles/2022-01-28/hackers-seize-80-million-from-qubit-in-latest-defi-attack>
- GeeksforGeeks. (2022, November 29). *Blockchain - Elliptic curve digital signature algorithm (ECDSA)*. GeeksforGeeks. Retrieved February 3, 2023, from <https://www.geeksforgeeks.org/blockchain-elliptic-curve-digital-signature-algorithm-ecdsa/>
- Gillis, A. S. (2022). *What is homomorphic encryption?* TechTarget. Retrieved January 2, 2023, from <https://www.techtarget.com/searchsecurity/definition/homomorphic-encryption>
- Goodin, D. (2014, July 30). *Active attack on tor network tried to decoak users for five months*. Ars Technica. Retrieved March 13, 2023, from <https://arstechnica.com/information-technology/2014/07/active-attack-on-tor-network-tried-to-decloak-users-for-five-months/>
- Gutteridge, D. (2018, May 21). *Japanese cryptocurrency Monacoin hit by selfish mining attack*. Yahoo News. Retrieved March 13, 2023, from <https://www.yahoo.com/news/japanese-cryptocurrency-monacoin-hit-selfish-205031219.html>
- Hicks, A. (2018, January 23). *Smart contracts and bribes – Bentham’s gaze*. Bentham’s gaze. Retrieved March 16, 2023, from <https://www.benthams gaze.org/2018/01/23/smart-contracts-and-bribes/>
- Hindi, R. (2022, July 20). *Private smart contracts using homomorphic encryption*. Zama. Retrieved January 2, 2023, from <https://www.zama.ai/post/private-smart-contract-using-homomorphic-encryption-ethcc-2022>
- Joubert, E. (2021, June 1). *Differential privacy: How it works, benefits & use cases in 2023*. AIMultiple. Retrieved January 2, 2023, from <https://research.aimultiple.com/differential-privacy/>
- Korn, J. (2022, August 3). *Another crypto bridge attack: Nomad loses \$190 million in ‘chaotic’ hack*. CNN. Retrieved March 16, 2023, from <https://www.cnn.com/2022/08/03/tech/crypto-bridge-hack-nomad/index.html>
- Kovacs, E., Winkelvoss, L., Solomon, M., George, T., Wilson, M., & Townsend, K. (2022, August 3). *Nearly \$200 million stolen from cryptocurrency Bridge Nomad*. SecurityWeek. Retrieved March 13, 2023, from <https://www.securityweek.com/nearly-200-million-stolen-cryptocurrency-bridge-nomad/>
- Kushner, D., & McConnell, M. (2014, February 4). *The fall of internet crime Kingpin Ross Ulbricht*. Rolling Stone. Retrieved January 2, 2023, from <https://www.rollingstone.com/culture/culture-news/dead-end-on-silk-road-internet-crime-kingpin-ross-ulbrichts-big-fall-122158/>
- Lindell, Y. (2020). *Secure multiparty computation (MPC)*. Cryptology ePrint archive. Retrieved January 2, 2023, from <https://eprint.iacr.org/2020/300.pdf>
- Marric, L. (2021, March 17). *Silk road review: The true story of the dark web’s illegal drug market*. New Scientist. Retrieved January 2, 2023, from <https://www.newscientist.com/article/mg24933260-400-silk-road-review-the-true-story-of-the-dark-webs-illegal-drug-market/>

- Martin, J. (2020, January 27). *Bitcoin gold Blockchain hit by 51% attack leading to \$70K double spend*. Cointelegraph. Retrieved March 13, 2023, from <https://cointelegraph.com/news/bitcoin-gold-blockchain-hit-by-51-attack-leading-to-70k-double-spend>
- Mueller, B. (2017, November 8). *What caused the accidental killing of the parity multisig wallet & how to detect similar bugs*. Medium. Retrieved January 22, 2023, from <https://medium.com/hackernoon/what-caused-the-latest-100-million-ethereum-bug-and-a-detection-tool-for-similar-bugs-7b80f8ab7279>
- Mycryptopedia. (2022, April 24). *What is SHA-256 and how is it related to bitcoin?* Mycryptopedia. Retrieved February 3, 2023, from <https://www.mycryptopedia.com/sha-256-related-bitcoin/>
- Optimism. (2022, December 10). *Rollup protocol*. Optimism Docs. Retrieved March 16, 2023, from <https://community.optimism.io/docs/protocol/2-rollup-protocol/#fault-proofs>
- Paxful. (2020, July 26). *What is bitcoin transaction malleability & how can it affect me?* Paxful. Retrieved March 16, 2023, from <https://paxful.com/university/bitcoin-transaction-malleability-explained/>
- Polygon. (2021, December 29). *All you need to know about the recent network upgrade - Polygon*. Polygon Technology. Retrieved March 16, 2023, from <https://polygon.technology/blog/all-you-need-to-know-about-the-recent-network-upgrade>
- Portier, B., & Diya, C. (2023, January 25). *How confidential space and MPC can help secure digital assets*. Google Cloud. Retrieved March 16, 2023, from <https://cloud.google.com/blog/products/identity-security/how-confidential-space-and-mpc-can-help-secure-digital-assets>
- Protos. (2022a, February 14). *Hacker could've printed unlimited 'Ether' but chose \$2M bug bounty instead*. Protos. Retrieved March 13, 2023, from <https://protos.com/ether-hacker-optimism-ethereum-layer2-scaling-bug-bounty/>
- Protos. (2022b, August 10). *Researchers discover critical bitcoin lightning network vulnerability*. Protos. Retrieved March 13, 2023, from <https://protos.com/researchers-discover-critical-bitcoin-lightning-network-vulnerability/>
- Solomon, R., & Almashaqbeh, G. (2021). *smartFHE: Privacy-preserving smart contracts from fully homomorphic encryption*. Cryptology ePrint Archive. Retrieved January 2, 2023, from <https://eprint.iacr.org/2021/133.pdf>
- Sonnenschein, M. (2021, December 24). *Bitcoin does not make payments anonymous — Just really hard to trace*. Business Insider India. Retrieved January 2, 2023, from <https://www.businessinsider.in/investment/news/bitcoin-does-not-make-payments-anonymous-just-really-hard-to-trace/articleshow/85068905.cms>
- Spacebot. (2021, April 20). *Blockchain attacks: Vector attack 76*. Spacebot. Retrieved January 16, 2023, from <https://spacebot.group/blockchain/blockchain-attacks-vector-attack-76/>
- Voell, Z. (2020, August 29). *Ethereum classic hit by third 51% attack in a month*. CoinDesk. Retrieved March 13, 2023, from <https://www.coindesk.com/markets/2020/08/29/ethereum-classic-hit-by-third-51-attack-in-a-month/>
- Wipro. (2020). *Synergizing blockchain & multi-party computation to reimagine transactions*. Wipro. Retrieved January 2, 2023, from <https://www.wipro.com/blockchain/synergizing-blockchain-and-multi-party-computation-to-reimagine-transactions/>
- Wu, O. (2020, June 2). *Blockchain-enabled contextual online learning under local differential privacy for coronary heart disease diagnosis in mobile edge computing*. PubMed. Retrieved January 2, 2023, from <https://pubmed.ncbi.nlm.nih.gov/32750921/>
- Yaffe, L. (2018, November 30). *Thoughts about nothing at stake*. HackerNoon. Retrieved March 16, 2023, from <https://hackernoon.com/thoughts-about-nothing-at-stake-b93b13bb5d6e>
- Zcash. (2016). *Zcash basics—Zcash documentation 5.3.2 documentation*. Zcash Documentation. Retrieved January 2, 2023, from https://zcash.readthedocs.io/en/latest/rtd_pages/basics.html

Chapter 2

Chain Security: Nodes, Algorithm, and Network



Ken Huang

In this chapter, we discuss the three key tenants of chain security: node security, consensus algorithm security, and network layer security (see Fig. 2.1).

Node security is essential to ensure that individual nodes in the blockchain network are secure and not vulnerable to attacks. Nodes can be targeted by attackers who may attempt to compromise the node's security in order to manipulate transactions, alter the blockchain ledger, or disrupt the network. Node centralization, where a small number of nodes control a significant portion of the network, can also be a security risk, as it provides a single point of failure and can lead to network manipulation by malicious actors. Therefore, it is crucial to secure each node through measures such as secure hardware, strong encryption, regular updates and maintenance, and ensuring decentralization.

Consensus algorithm security is critical to validate and add new blocks to the ledger, ensuring that all nodes in the network agree on the state of the ledger and that no one can tamper with it. A flawed consensus algorithm or one that is vulnerable to attacks can compromise the security of the entire network. Therefore, it is essential to ensure that the consensus algorithm used by the blockchain is secure, well-designed, and regularly updated to prevent attacks.

Network layer security ensures that the data transmitted between nodes in the blockchain network is secure and cannot be intercepted or manipulated by attackers. The blockchain network relies on peer-to-peer communication to ensure that all nodes are in sync and have the same copy of the ledger. Therefore, it is essential to secure the network layer against some potential attacks.

The security of a blockchain system depends on the proper implementation and maintenance of these three key tenants. A failure in any one of these areas can

K. Huang (✉)
DistributedApps.AI, Fairfax, VA, USA
e-mail: Ken@Distributedapps.ai

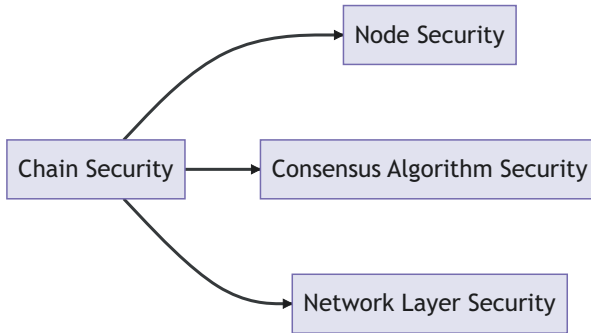


Fig. 2.1 Three key tenants of chain security

compromise the security and integrity of the entire blockchain network, making it vulnerable to attacks and manipulation.

2.1 What Is Consensus Node?

A consensus node, also known as a validator node, is a particular type of node in a blockchain network responsible for validating and confirming transactions. Consensus nodes play a crucial role in ensuring the security and integrity of the blockchain, as they are responsible for ensuring that only valid transactions are added to the ledger.

There are several types of consensus algorithms that are used in blockchain systems, each of which has its own set of rules and protocols for how transactions are validated and added to the ledger. Some common examples of consensus algorithms include Proof-of-Work (PoW), Proof-of-Stake (PoS), and Delegated Proof-of-Stake (DPoS).

In a Proof-of-Work (PoW) system, consensus nodes are typically responsible for solving complex mathematical puzzles in order to validate transactions and create new blocks. In a Proof-of-Stake (PoS) system, consensus nodes generally are chosen based on the amount of stake they hold in the network, with the ability to validate transactions and create new blocks being proportional to the amount of stake they hold. In a Delegated Proof-of-Stake (DPoS) system, consensus nodes are chosen by the community through a voting process, and they are responsible for validating transactions and creating new blocks.

Consensus nodes play a crucial role in ensuring the security and integrity of the blockchain, as they are responsible for verifying the validity of transactions and adding them to the ledger. By using a decentralized network of consensus nodes, it is possible to ensure that the blockchain remains secure and resistant to tampering or interference.

2.2 Consensus Node Configuration Security

Consensus node configuration security refers to the measures taken to ensure that the nodes participating in a blockchain network are secure and cannot be easily compromised. This is critical for the proper functioning and integrity of the network. We use Bitcoin and Ethereum node configurations as examples to discuss node configuration security. The same security practices should be applied to other types of blockchains.

2.2.1 *Bitcoin Node Security Configuration Recommendations*

If you run your own bitcoin node, please make sure the following protection measures are implemented (Fig. 2.2).

- Use Tor or a VPN: Tor is a browser that hides your IP address and browsing activity, while a VPN tunnels your traffic through a secure server. Both methods protect your privacy and security when using your Bitcoin node.
- Use a local node: Run your own node on a local network-connected device rather than relying on third-party services or cloud nodes. This provides greater control and privacy, as well as avoiding the need to give KYC data to node providers.
- Limit your hot stack: Avoid storing large amounts of Bitcoin in the hot wallet of your node. Instead, use a cold storage wallet for long-term storage and only keep a small amount in the hot wallet for day-to-day transactions.
- Secure your home WiFi: Ensure that your WiFi connection is encrypted and secure to prevent unauthorized access or interception of data.
- Use a secure password manager & 2FA: Create a long and complex password for your node and store it in an encrypted password manager. Use two-factor authentication (2FA) with an authenticator app instead of email or SMS for greater security.
- Secure your private keys: Keep a backup of your private keys offline and away from your node to prevent loss in case of a failure or disaster.
- Limit your apps: Only install apps that are necessary for Bitcoin use and come from reputable sources. Avoid adding unnecessary apps that could introduce security risks.
- Run a UPS: Use an uninterruptible power supply (UPS) to keep your node online in case of power outages or surges.
- Hide or obscure your node: Keep your node hidden from public view and secure in a location that is not easily accessible or visible.
- Avoid advertising your node: Do not advertise that you are running a node or make it known on social media to prevent being targeted by criminals.

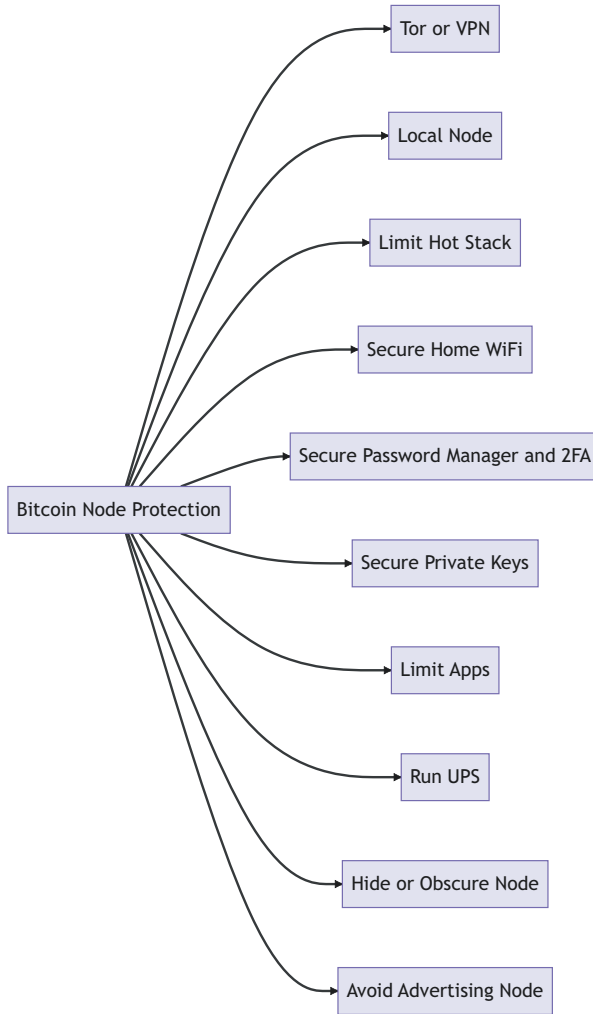


Fig. 2.2 Bitcoin Node Security Protection Recommendation

By following these recommendations, you can secure your bitcoin node which is a critical aspect of blockchain security and helps to ensure the integrity and stability of the network.

2.2.2 *Ethereum POS Validator Node Security Recommendations*

In September 2022, Ethereum switched from proof-of-work (POW) to proof-of-stake (POS) as its consensus mechanism with the “merge.” The previous POW consensus mechanism required a decentralized network of computers to solve mathematical puzzles to validate transactions but was energy-intensive. The new POS mechanism uses significantly less power and is estimated to be 99% more energy-efficient.

After the merge, the mining nodes became validator nodes. In a PoS consensus mechanism, validators are selected to validate transactions and create new blocks based on the amount of stake they hold, rather than their computational power as in a PoW consensus mechanism.

Here are some recommendations for securing Ethereum PoS validator node (Fig. 2.3):

- Create a non-root user with sudo privileges: Running your validator node as a non-root user with sudo privileges helps to prevent unauthorized access to your system. You can create a new user with the “adduser” command and give it sudo privileges.
- Disable SSH password authentication and use SSH keys only: SSH password authentication can be easily compromised by brute-force attacks, so it is recommended to disable it and use SSH keys instead. SSH keys provide better security and make it difficult for attackers to gain unauthorized access to your system.
- Disable root account: Disabling the root account adds an extra layer of security to your system. This prevents attackers from logging in as the root user, which is the most privileged account on a Linux system.
- Secure shared memory: Shared memory is a potential security risk on Linux systems. You can secure shared memory by setting the “tmpfs” filesystem to mount with the “noexec” and “nosuid” options in the /etc/fstab file.
- Install Fail2ban: Fail2ban is a popular security tool that helps prevent brute-force attacks by banning IP addresses that fail to authenticate multiple times. It can be easily installed using the package manager.
- Configure your firewall: Configuring a firewall helps to limit network access to your system. You can use the Uncomplicated Firewall (UFW) or another firewall tool to configure your firewall rules.
- Verify listening ports: Verifying the listening ports on your system helps you to identify any open ports that could be used to attack your system. You can use the “netstat” command to check for open ports.
- Keystore storage: Store the keystore in only one validator machine to minimize the risk of unauthorized access.
- Monitoring: Utilize monitoring tools such as Prometheus and Grafana to track important real-time metrics about your validator.

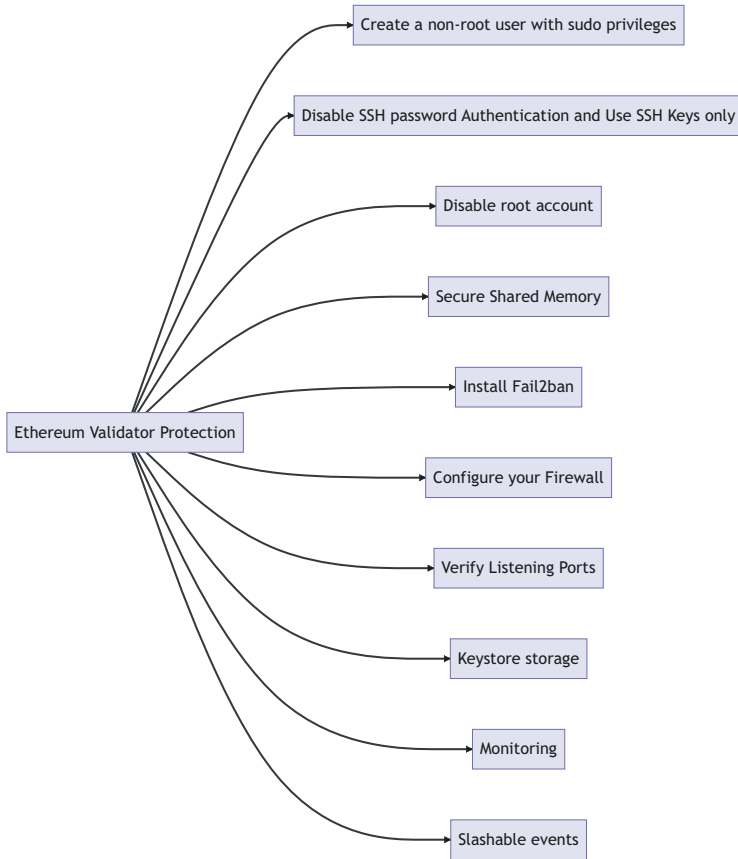


Fig. 2.3 Ethereum validator node protection

- **Slashable events:** Be aware that running your validator in multiple locations increases the risk of a slashable event, which can result in ejection from the network.

By following these security recommendations, you can help protect your Ethereum PoS validator node and minimize the risk of funds loss and contribute to the overall security of the Ethereum network.

2.2.3 Attacks on Consensus Node

Consensus nodes are an essential component of a blockchain network responsible for validating transactions and maintaining the integrity of the network. As a result, they are often targeted by attackers seeking to compromise the network’s security.

Consensus node attacks can take various forms, including denial-of-service attacks, network partitioning attacks, and attacks on node misconfigurations. These attacks can have severe consequences, including loss of funds, network instability, and reputational damage to the blockchain network. It is crucial for blockchain operators to implement appropriate security measures to protect their consensus nodes from these attacks.

The followings are some examples of attacks in the past.

EOS Remote Execution Attack (Khandelwal, 2018)

In 2018, security researchers discovered a vulnerability in the EOS blockchain platform that could allow remote hackers to take complete control over the node servers running critical blockchain-based applications. The vulnerability is due to a buffer out-of-bounds write issue in the process used by node servers to parse contracts. The attackers could upload a malicious WASM file to the server, which would execute the malicious payload on the node, potentially leading to control over the supernode in the EOS network. If the supernode is controlled, the attackers could then manipulate transactions and access financial and privacy data. The vulnerability has since been fixed by the maintainers of the EOS project.

Ethereum Eclipse Attack (Cimpanu, 2018)

In March 2018, security researchers found that Ethereum nodes are vulnerable to eclipse attacks where an attacker only needs two malicious nodes to isolate and affect another. An eclipse attack allows a malevolent party to co-opt a victim's mining power and use it to attack the blockchain's consensus algorithm or double spending and selfish mining. The attack can also fool victims into viewing incorrect Ether transaction details and delay the view of various parameters used by the smart contract's internal computations resulting in incorrect output. The research team worked with the Ethereum Foundation to silently patch the issue and recommended countermeasures that were applied in the latest software release (geth 1.8.0), which raised the number of malicious nodes needed from two to thousands but did not fully prevent eclipse attacks.

The DoS Attack on Solana (Hayward, 2021)

In September 2021, The Solana network experienced a Denial-of-Service (DoS) attack during an Initial DEX Offering (IDO) for Grape Protocol, a widely used toolset for DeFi developers on the Solana platform. The cause of the attack was the massive number of transactions generated by bots that were attempting to gain an advantage in the token offering. These transactions overwhelmed the network's distributed nodes, leading to crashes due to excessive memory usage. As a result, the network was unable to reach a consensus on the blockchain's current state, causing it to stop producing blocks. Initially, Solana attributed the downtime to "resource exhaustion."

Aptos Node Vulnerability (Numen Cyber Technology, 2022)

Numen Cyber Technology, a Singapore-based Web3 security firm, uncovered a critical vulnerability in the highly-anticipated public blockchain, Aptos. The vulnerability was discovered in the MoveVM component of Aptos and could result in

crashes and undefined behavior due to an integer overflow in the stack-based Web3 programming language. The vulnerability could also make the Aptos network susceptible to Denial-of-Service (DoS) attacks, potentially leading to a complete network shutdown and causing serious harm to the stability of the nodes. The existence of this vulnerability has been confirmed by Aptos Labs and Numen Cyber Labs has assisted the team in fixing the issue.

To prevent these types of attacks and ensure the security and integrity of a blockchain network, it is important to thoroughly test node software and configure nodes with correct and hardened settings to prevent unauthorized access and impact to the whole blockchain network.

2.3 Node Centralization and Security Concerns

Node centralization is a phenomenon that occurs when a small number of nodes control a large portion of the network in a blockchain system. This can have significant implications for the security and stability of the blockchain, as a centralized node can potentially wield a disproportionate amount of power and influence over the network.

One example of this is Lido staking nodes, which are nodes that are responsible for validating and confirming transactions on the Lido blockchain. Lido is a decentralized staking protocol for Ethereum that allows users to earn rewards on their ETH holdings by staking them on the Ethereum 2.0 network. Lido uses a liquid staking model, which means that users can stake their ETH and receive a tokenized representation of their stake (stETH) in return. This allows users to continue using their staked ETH while still earning rewards.

One potential issue with Lido is the centralization risk associated with its node operators. Lido relies on a set of node operators to validate transactions and produce blocks on the Ethereum 2.0 network. If a small number of these node operators were to collude or become compromised, they could potentially manipulate the network and compromise its security.

To mitigate this risk, Lido has implemented measures such as a decentralized governance model and a rotating set of node operators selected through a transparent process. Additionally, Lido has plans to implement additional security measures such as multi-party computation (MPC) in the future to further decentralize its operations and reduce centralization risk.

There are several other ways in which node centralization can occur in a blockchain system. One common way is through the use of the so-called supernodes, which are nodes that have a large number of resources and are able to process a large number of transactions. These nodes may be operated by large, well-funded organizations, which can give them an advantage over smaller, less well-funded nodes.

Another way that node centralization can occur is through the use of nodes that are operated by a small number of individuals or organizations. These nodes may be

controlled by a single entity, or they may be operated by a small group of individuals who are able to coordinate their efforts. In either case, this can lead to a concentration of power and a lack of decentralization.

Table 2.1 listed various examples of node centralization and security concerns as well as countermeasures.

It is worth noting that not all forms of node centralization are inherently bad. However, excessive centralization can lead to a lack of trust in the network and can undermine the key benefits of blockchain technology such as decentralization, security, and immutability.

In summary, node centralization can present a range of security concerns depending on the specific example. It is important for blockchain networks to strive for a balance between centralization and decentralization in order to maintain trust and security for all participants.

2.4 Bitcoin Security After Mining Rewards Depletion

There are a number of factors that will impact the long-term security of the Bitcoin network after mining rewards depletion in around 2140. Here are a few key considerations:

Transaction fees: After mining rewards are depleted, the primary incentive for miners will be transaction fees. If transaction fees are high enough, they can provide sufficient incentives for miners to continue securing the network.

Network decentralization: The more decentralized the network is, the more resistant it will be to attacks and other security threats. It is important for the Bitcoin network to maintain a high degree of decentralization in order to remain secure.

Hardware advancements: As technology improves, new and more efficient hardware may become available, which could potentially impact the profitability of mining and the security of the network.

Changes to the protocol: If changes to the Bitcoin protocol are made in the future, they could potentially impact the security of the network. It is important for any changes to be thoroughly tested and carefully evaluated before being implemented.

In addition, Table 2.2 listed more security measures to protect Bitcoin after mining rewards depletion.

It is worth noting that these are just a few potential security measures that could be implemented to help maintain the security of the Bitcoin network after mining rewards are depleted. The best approach will likely depend on a variety of factors, including the overall health of the network, the specific needs of users and miners, and the broader regulatory and economic landscape. Nevertheless, these measures can help provide a starting point for discussions about how to ensure the long-term viability and security of the Bitcoin network.

Table 2.1 Node centralization and security concerns

Example of node centralization	Security concerns	Countermeasures
Mining pools	Control over consensus, the potential for 51% attacks, uneven rewards distribution, centralization of hashing power	Encouraging decentralization of mining power, implementing consensus mechanisms that discourage concentrated pool formation, promoting fair rewards distribution
Full node service providers	Control over network access, the potential for censorship, lack of privacy	Encouraging the creation of more full node operators, promoting decentralized alternatives to centralized services, implementing privacy-enhancing technologies
Proof-of-stake validators	Centralization of staked assets, control over consensus, lack of decentralization, potential for economic attacks	Encouraging decentralization of staked assets, implementing mechanisms that limit the influence of large stakeholders, promoting fair distribution of rewards
Token exchanges	Control over token listings, potential for manipulation, lack of transparency	Encouraging decentralized exchanges and peer-to-peer trading, promoting transparency in listing processes, implementing measures to prevent market manipulation
Developer teams	Control over protocol updates, lack of community input, potential for malicious code	Encouraging community involvement in protocol development, promoting transparency in development processes, implementing measures to prevent malicious code from being included in updates
Cloud providers	Control over server infrastructure, potential for censorship, lack of privacy, potential for DDOS attacks	Encouraging the use of decentralized hosting solutions, promoting the use of privacy-enhancing technologies, implementing measures to prevent DDOS attacks
Hardware wallet manufacturers	Control over private key storage, potential for collusion with bad actors, lack of transparency	Encouraging the use of open-source hardware wallet solutions, promoting transparency in hardware wallet design and manufacturing processes, implementing measures to prevent collusion with bad actors
Token holders	Centralization of wealth, potential for market manipulation, lack of decentralization, potential for economic attacks	Encouraging broader distribution of tokens, implementing mechanisms to prevent market manipulation, promoting decentralization of decision-making
Mining equipment manufacturers	Control over hardware supply, potential for centralization of mining power, lack of transparency	Encouraging the creation of alternative mining equipment manufacturers, promoting transparency in hardware manufacturing processes, implementing measures to prevent centralization of mining power

(continued)

Table 2.1 (continued)

Example of node centralization	Security concerns	Countermeasures
Government-run nodes	Control over network access, potential for censorship, lack of privacy, potential for surveillance	Encouraging the creation of community-run nodes, promoting the use of privacy-enhancing technologies, implementing measures to prevent censorship and surveillance
Proof-of-authority validators	Centralization of authority, potential for collusion, lack of decentralization, potential for economic attacks	Encouraging the decentralization of authority, implementing measures to prevent collusion, promoting fair distribution of rewards
Internet service providers	Control over network access, potential for censorship, lack of privacy, potential for DDOS attacks	Encouraging the use of decentralized networking solutions, promoting the use of privacy-enhancing technologies, implementing measures to prevent censorship and DDOS attacks
Social media platforms	Control over content and access, potential for censorship, lack of transparency, potential for abuse of power	Encouraging the use of decentralized social media platforms, promoting transparency in content moderation processes, implementing measures to prevent abuse of power

Table 2.2 Bitcoin Network Security Measures after block rewards depletion

Security measure	Description
Layer 2 solutions	Implement layer 2 solutions such as the lightning network to help reduce the burden on the main blockchain network and increase transaction throughput. This can help make transactions more efficient and affordable, which in turn can help maintain network security by reducing the likelihood of spam attacks.
Alternative reward mechanisms	Consider alternative reward mechanisms such as inflationary models or “proof-of-burn” mechanisms that encourage users to burn coins rather than mine them. These mechanisms can help incentivize continued participation in the network and ensure that there are sufficient resources available to maintain security.
Decentralization	Encourages the decentralization of mining power by promoting the use of alternative mining hardware and discouraging the concentration of mining power in the hands of a few large players. This can help prevent 51% attacks and ensure that the network remains robust and secure.
Community support	Foster community support for the network by encouraging broader participation in decision-making processes and promoting education about the benefits of bitcoin and blockchain technology. This can help ensure that the network remains resilient and that users remain committed to its long-term success.

2.5 Attacks on Consensus Algorithm and Countermeasures

Consensus algorithms are used in distributed systems to ensure that all nodes agree on a common state or decision. In the context of FLP (Fischer et al., 1985) impossibility theory, consensus algorithms are subject to the fundamental problem that it is impossible for a distributed system to reach consensus in the presence of even a single faulty node (Fischer et al., 1985).

This means that in order to design a secure consensus algorithm, certain assumptions must be made about the behavior of nodes on the network. For example, many consensus algorithms assume that nodes are honest and follow the protocol as intended. Other assumptions might include limits on network latency or message loss.

By making these assumptions, consensus algorithms can be designed to achieve high levels of security and reliability despite the inherent limitations of distributed systems. However, it is important to note that these assumptions may not always hold true in practice, and as such, consensus algorithms must be continually monitored and updated to address potential vulnerabilities.

Consensus algorithm security refers to the level of protection that a blockchain network has against attacks on its consensus mechanism. The consensus algorithm is the mechanism by which nodes on a blockchain network agree on the state of the network and validate transactions. Consensus algorithm security is important because it ensures that the network remains secure and resistant to attacks.

There are several factors that contribute to consensus algorithm security, including the type of consensus algorithm used, the number and distribution of nodes on the network, and the level of decentralization. Other factors that can impact consensus algorithm security include network latency, node uptime, and the ability of nodes to communicate with each other. In order to maintain high levels of consensus algorithm security, blockchain networks must continually monitor their operations for potential vulnerabilities and take steps to address them as they arise. This can include implementing node software updates, increasing node distribution, or implementing additional security measures such as multi-party computation (MPC).

Table 2.3 lists some common consensus algorithm and associated security attacks.

2.5.1 Attacks on Proof-of-Work (PoW) and Countermeasures

Proof-of-Work (PoW) is a consensus algorithm used in blockchain technology to validate transactions and create new blocks. It is a computationally intensive process that requires miners to solve complex mathematical problems to validate transactions and create new blocks. However, PoW is vulnerable to several attacks, including:

Table 2.3 Consensus algorithm security attacks

Consensus algorithm	Description	Security attacks
Proof-of-work (PoW)	A consensus mechanism that requires nodes to perform a certain amount of computational work (finding the smallest hash value) in order to participate in the network and validate transactions.	51% attack Double-spending attack, selfish-mining attack
Proof-of-stake (PoS)	A consensus mechanism where nodes hold a stake of the network's native cryptocurrency, and the chances of a node being selected to validate transactions is proportional to the amount of stake it holds.	Nothing at stake attack, long-range attack, stake grinding attack, bribing attack.
Delegated proof-of-stake (DPoS)	A consensus mechanism where token holders vote for a set of delegates who validate transactions and produce blocks on their behalf.	"Voting" centralization attack, Sybil attack, bribery attack
Proof-of-activity (PoA)	A hybrid consensus mechanism that combines elements of proof-of-work and proof-of-stake.	51% attack Nothing at stake attack Long-range attack
Proof of elapsed time (PoET)	A consensus mechanism that uses random wait time to select nodes to validate transactions.	Clock skew attack Multiple certificate attack
Byzantine fault tolerance (BFT)	A consensus mechanism that allows nodes to agree on a single value, even in the presence of malicious nodes.	Sybil attack, man in the middle attack, denial of service attack

51% attack: A 51% attack is a scenario where a single entity or a group of entities control more than half of the computing power in a network, allowing them to manipulate the network by producing blocks faster than the rest of the network, double-spend coins, or block other transactions from being confirmed. An example of a 51% attack occurred in the Ethereum Classic network in January 2019. The attack was carried out by a single person who was able to control around 60% of the mining power, creating a longer blockchain which gave them the ability to double spend. The attack caused a loss of funds worth 219,500 ETC, roughly amounting to \$1.1 million (Clarke, 2019).

There are several ways to prevent a 51% attack, including:

50% limit on a single miner: A blockchain's protocol could ensure that no miner or a group of miners controls more than 50% of the blockchain's hashing power.

Strong network community: A strong network community can help prevent 51% attacks by ensuring that miners are incentivized to act in the best interest of the network.

Double-spending attack: A double-spending attack is a type of attack where a malicious actor attempts to spend the same digital asset twice. In a PoW network, a double-spend attack can occur if a malicious miner or attacker creates a fraudulent transaction that is accepted by the network, and then sends a conflicting transaction that spends the same digital currency to a different recipient. If the attacker can successfully have the fraudulent transaction accepted by the network, they can effectively spend the same digital currency twice.

Here is an example of how a double-spending attack can work (see Fig. 2.4):

In this example, the attacker sends a valid transaction to a merchant, which is verified by the network and approved for payment. The attacker then sends a second transaction that spends the same digital currency to a different address. The network adds the second transaction to the blockchain, effectively creating a double-spending attack.

The merchant receives notification of the second transaction but is unaware of the fraudulent nature of the attack. The merchant releases goods or services based on the first transaction, effectively losing out on the payment for the transaction.

Double-spending attacks can be mitigated through the use of transaction confirmation systems, such as requiring a certain number of confirmations before a transaction is considered valid. This can help prevent attackers from creating fraudulent transactions and spending the same digital currency multiple times.

Selfish-mining attack: A selfish-mining attack is a type of attack where a group of miners collude to mine blocks privately, keeping their blocks secret from the rest of the network, in order to gain an advantage. This type of attack can lead to reduced network security and decreased trust in the network.

Figure 2.5 shows how selfish-mining attack works.

Miner1 is attempting to perform a selfish-mining attack on the network. Initially, both Miner1 and Miner2 are mining blocks and adding them to the blockchain, following the honest mining protocol. However, when Miner1 successfully mines Block 3, instead of immediately adding it to the blockchain, they withhold it from the network and secretly continue mining on top of it to create Block 4.

Once Miner1 has successfully mined Block 4, they release Blocks 3 and 4 simultaneously to the network. Because Block 3 is the longest chain, it is added to the blockchain, and Block 4 is ignored as a duplicate. This effectively gives Miner1 an unfair advantage over other miners on the network, as they were able to mine two blocks in secret, while other miners were only aware of one.

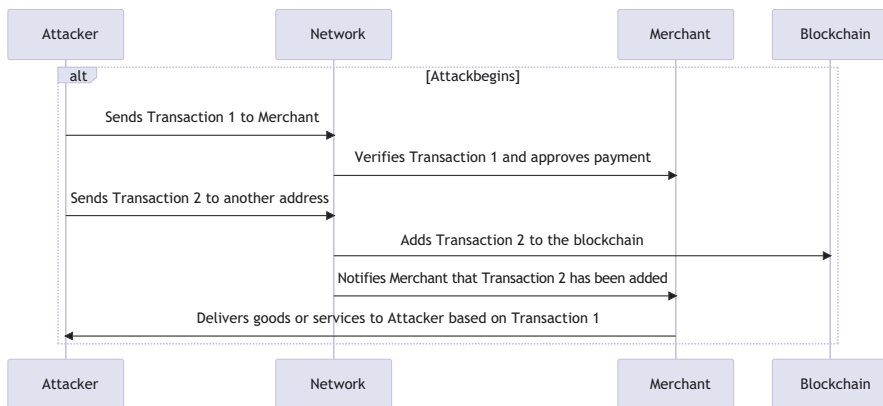


Fig. 2.4 Double-spending attack

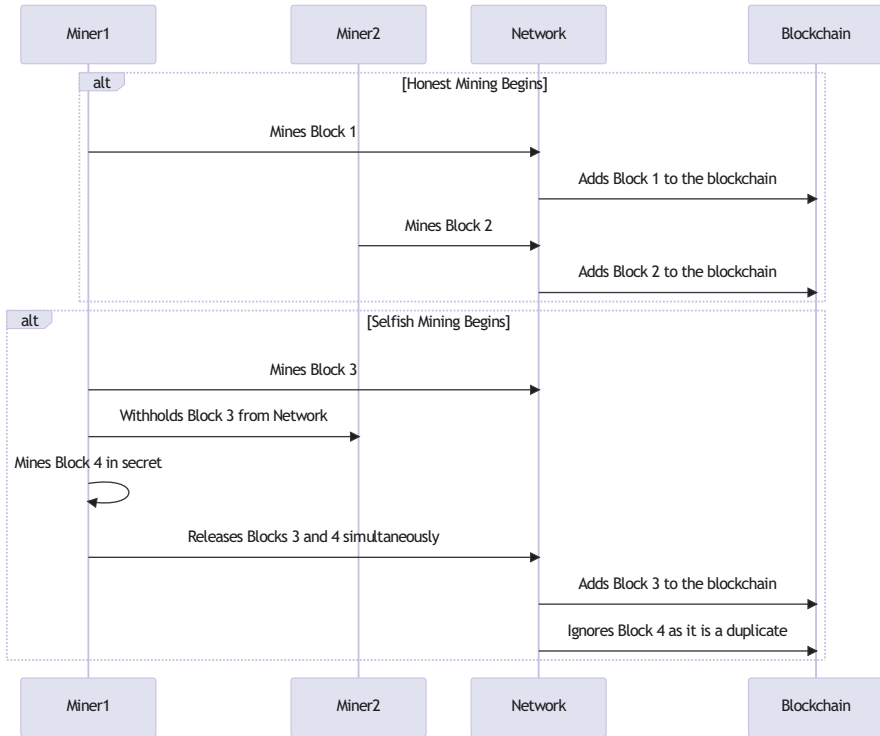


Fig. 2.5 Selfish-mining attack

Selfish-mining attacks can be difficult to prevent, but measures such as increasing the network’s hashing power, reducing block propagation times, and implementing a fair sharing reward system can help mitigate the risk of such attacks.

2.5.2 Attacks on Proof-of-Stake (PoS) and Countermeasures

Proof-of-Stake (PoS) is a consensus mechanism used in blockchain networks to validate transactions and create new blocks. In contrast to Proof-of-Work (PoW), which relies on computational power to validate transactions, PoS relies on the concept of “staking” to achieve consensus. In a PoS system, validators, also known as “stakers,” are chosen to create new blocks and validate transactions based on the amount of cryptocurrency they hold or “stake” in the network. The more cryptocurrency a staker holds, the more likely they are to be selected to validate transactions and create new blocks. This is because validators are incentivized to act in the best interest of the network, as any attempt to compromise the system would result in a loss of their staked cryptocurrency.

The process of staking involves holding cryptocurrency in a designated wallet and locking it up to participate in block validation. Validators are then randomly selected to validate transactions and create new blocks based on the amount of cryptocurrency they have staked. Validators are also rewarded with transaction fees and newly minted cryptocurrency for their participation in the network. One of the main advantages of PoS over PoW is that it consumes significantly less energy, as there is no need for expensive mining hardware and electricity to solve complex mathematical problems. PoS also provides greater security against 51% attacks, as the cost of acquiring a majority stake in a PoS network is significantly higher than in a PoW network.

Nevertheless, if designed improperly, PoS network can be susceptible for the following attacks:

Nothing at stake attack (NoS): A nothing at stake attack is a type of attack where a validator can vote for multiple conflicting chains, without incurring any costs, leading to the possibility of a network split and reduced security.

To defend against NoS attack, several measures can be taken, including:

Slashing: One of the most common defense mechanisms against NoS attacks is the implementation of a slashing mechanism. Slashing refers to the process of penalizing validators who attempt to stake on multiple chains. This can be achieved by removing a portion of their staked cryptocurrency or by disqualifying them from participating in the network.

Punitive forking: Another method of defending against NoS attacks is by using punitive forking, which involves creating a fork in the blockchain that penalizes validators who attempt to stake on multiple chains. This can involve reducing the amount of staked cryptocurrency or disqualifying them from participating in the network.

Longer validation time: Increasing the validation time for blocks can make it more difficult for validators to create multiple chains simultaneously, as they will have to wait longer to confirm their transactions on each chain. This can help prevent NoS attacks by discouraging validators from attempting to create multiple chains.

Reputation-based selection: Using a reputation-based selection process for validators can also help prevent NoS attacks, as it can discourage malicious validators from participating in the network. This can be achieved by using a reputation system that tracks the behavior of validators and rewards them based on their contribution to the network.

Long-range attack: A long-range attack is a type of attack where an attacker is able to manipulate a PoS blockchain by creating an alternative version of the blockchain's history, starting from a previous block and extending it to the present. This type of attack is possible due to the lack of a PoW mechanism in PoS consensus.

To defend against long-range attacks, several measures can be taken, including:

Checkpointing: Checkpointing involves periodically creating a snapshot of the blockchain, which is then used to verify the integrity of the blockchain at a later point in time. Checkpointing can help prevent long-range attacks by ensuring that

the blockchain is valid up to a certain point in time, even if the attacker attempts to recreate the blockchain from a much earlier point in time.

Immutable history: Another way to defend against long-range attacks is to create an immutable history for the blockchain. This can be achieved by storing the entire blockchain history, including all past blocks, and ensuring that they cannot be altered or deleted. This can help prevent attackers from recreating the blockchain from an earlier point in time, as they will not be able to modify or delete past blocks.

Consistency checks: Consistency checks can also be used to defend against long-range attacks. Consistency checks involve verifying the validity of the blockchain at different points in time, by checking for inconsistencies or errors in the blockchain data. This can help detect long-range attacks early on and prevent the attacker from overtaking the blockchain.

Stake grinding attack: A stake grinding attack is a type of attack when an attacker attempts to manipulate the selection process for validators in order to increase their chances of being selected as the next validator.

To defend against stake grinding attacks, several measures can be taken, including:

Random number generation: One of the most effective ways to defend against stake grinding attacks is to use a random number generation algorithm that is resistant to manipulation. This can make it more difficult for attackers to predict the outcome of the selection process and increase their chances of being selected.

Penalty mechanisms: Penalty mechanisms can be used to discourage attackers from attempting to manipulate the selection process. This can include penalties such as losing a portion of their staked cryptocurrency or being disqualified from participating in the network.

Shuffling: Shuffling involves periodically shuffling the selection process for validators, making it more difficult for attackers to predict the outcome of the selection process. This can be achieved by using techniques such as randomizing the order of validator selection or using a different selection algorithm.

Time-based selection: Another approach to defend against stake grinding attacks is to use a time-based selection process, where validators are selected based on the amount of time they have staked their cryptocurrency in the network. This can make it more difficult for attackers to manipulate the selection process, as they would need to hold their cryptocurrency for a longer period of time to have a greater chance of being selected.

Bribing attack: A bribing attack is a type of attack where a malicious validator attempts to bribe other validators to validate transactions that they have submitted, increasing the likelihood that their transactions will be confirmed.

To defend against bribing attacks, several measures can be taken, including:

Transparency: One of the most effective ways to defend against bribing attacks is to promote transparency in the selection process for validators or delegates. This can be achieved by making the selection process public and ensuring that it is fair and unbiased.

Random selection: Random selection of validators or delegates can help prevent attackers from targeting specific individuals for bribes. This can be achieved by

using a random number generator to select validators or delegates, making it more difficult for attackers to predict the outcome of the selection process.

Consensus-based selection: Consensus-based selection involves using a group decision-making process to select validators or delegates. This can help prevent attackers from bribing a single individual and ensure that the selection process is fair and unbiased.

Slashing: Slashing is a mechanism that can be used to penalize validators or delegates who act in a way that is detrimental to the network. This can include reducing their stake or disqualifying them from participating in the network.

Rotation of validators or delegates: Rotation of validators or delegates involves periodically rotating the individuals responsible for validating transactions and creating new blocks. This can prevent any one individual from gaining too much power or influence within the network.

2.5.3 Attacks on Delegated Proof-of-Stake (DPoS) and Countermeasures

Delegated Proof-of-Stake (DPoS) is a variation of the Proof-of-Stake (PoS) consensus mechanism, where a group of “delegates” are elected by token holders to validate transactions and create new blocks on their behalf.

In a DPoS system, token holders vote for delegates to become part of the consensus mechanism. The delegates are then responsible for validating transactions, creating new blocks, and maintaining the network. Delegates are incentivized to act in the best interest of the network, as any attempt to compromise the system would result in a loss of their reputation and the possibility of losing their position as a delegate.

One of the main advantages of DPoS over other consensus mechanisms is its scalability, as the number of delegates is typically smaller than the number of validators in other consensus mechanisms. This makes it easier to achieve consensus and reduces the likelihood of network congestion.

However, DPoS is not without its security risks. Some of the common security attacks on DPoS include:

“Voting” centralization attack: In a “voting” centralization attack, a small number of entities control a significant portion of the voting power, potentially allowing them to control the network and approve malicious transactions.

Sybil attack: A Sybil attack is a type of attack where a malicious entity creates multiple identities to increase their influence in the network, potentially allowing them to control the network.

Bribery attack: A bribery attack is a type of attack where a malicious entity bribes delegates to validate malicious transactions or blocks.

2.5.4 Attacks on Proof of Activity (PoA) and Countermeasures

Proof of Activity (PoA) is a hybrid consensus algorithm that combines two existing consensus algorithms: Proof-of-Work (PoW) and Proof-of-Stake (PoS). PoA is designed to provide the security benefits of PoW while reducing its energy consumption and environmental impact.

In PoA, the network uses PoW to generate new blocks initially, but once a certain number of blocks have been mined, the network switches to PoS. In PoS, nodes are selected to validate transactions and create new blocks based on the amount of cryptocurrency they hold.

While PoA is a relatively new consensus algorithm, there are still some attacks that can be carried out on it. Here are some of the attacks on PoA:

51% attack: A 51% attack occurs when an attacker controls a majority of the mining power in the PoW stage of the PoA algorithm. With this control, the attacker can create a longer chain of blocks and rewrite the blockchain history.

Countermeasure: PoA systems can reduce the impact of a 51% attack by increasing the difficulty of the PoW stage or by implementing checkpointing to prevent the attacker from rewriting the blockchain history.

Nothing at Stake attack: In PoS, nodes can validate transactions and create new blocks based on the amount of cryptocurrency they hold. A Nothing at Stake attack occurs when a validator creates multiple blocks on multiple forks of the blockchain, as there is no cost to doing so.

Countermeasure: PoA systems can prevent a Nothing at Stake attack by implementing penalties for validators who create blocks on multiple forks of the blockchain.

Long-range attack: In a long-range attack, an attacker creates a new blockchain from the genesis block and creates a longer chain than the existing blockchain.

Countermeasure: PoA systems can prevent long-range attacks by implementing checkpointing or by requiring validators to keep a copy of the blockchain from the genesis block.

2.5.5 Attacks on Proof of Elapsed Time (PoET) and Countermeasures

Proof of Elapsed Time (PoET) is a consensus algorithm that was developed by Intel to provide a more energy-efficient alternative to Proof-of-Work (PoW). In PoET, nodes on the network compete to be selected to create the next block, but instead of using computational power like PoW, nodes use a random waiting time. This waiting time is determined by a trusted execution environment (TEE), which is a secure hardware module built into the node's processor.

The PoET algorithm works by having each node in the network request a random wait time from the TEE. The node with the shortest wait time is then selected to

create the next block, and the wait time is broadcast to the network for verification. Once the wait time has elapsed, the node can create the next block and add it to the blockchain.

Potential attacks on PoET include Clock Skew Attack and Multiple Certificate Attack.

Clock Skew Attack is an attack that targets the accuracy of a node's system clock. In PoET, nodes use their system clock to wait for a randomly generated period of time before attempting to create a block. If an attacker can manipulate a node's system clock, they can influence the node's selection to create the next block, leading to a potential manipulation of the blockchain.

To prevent Clock Skew Attack, PoET systems can reduce the impact of a Clock Skew Attack by implementing multiple time sources and using a consensus mechanism to determine the correct time. Nodes can also be designed to detect significant clock skew and reject wait times that are too short or too long.

Multi-Certificate Attacks against PoET is an attack that exploits the ability of nodes to obtain multiple certificates from the TEE (Trusted Execution Environment) to increase their chances of being selected to create the next block in the PoET consensus algorithm. The certificates are used to attest to the identity of the node and to prove that it has waited for the required amount of time before attempting to create a block. In a Multi-Certificate Attack, a node acquires multiple certificates from the TEE, each with a different identity. The node then uses these certificates to increase its chances of being selected to create the next block. The attack is particularly effective when combined with a Sybil attack, as the attacker can create multiple identities to obtain multiple certificates.

To prevent Multi-Certificate Attacks, PoET systems can implement a number of defense measures. One possible defense measure is to limit the number of certificates that a single node can obtain from the TEE. This can be achieved by setting a cap on the number of certificates that a node can request, or by implementing a penalty mechanism that reduces a node's chance of being selected if it has multiple certificates. Another possible defense measure is to use a reputation system to assign reputation scores to nodes based on their behavior in the network. Nodes with a higher reputation score are more likely to be selected to create the next block, which reduces the effectiveness of Multi-Certificate Attacks.

2.5.6 Attacks on Byzantine Fault Tolerance (BFT) and Countermeasures

Byzantine Fault Tolerance (BFT) is a consensus algorithm that is designed to achieve fault tolerance in distributed systems. It is used to ensure that a network of nodes can reach an agreement on a transaction or decision even if some of the nodes are faulty or malicious.

Figure 2.6 gives an illustration of how BFT works, NodeA and NodeD propose new blocks, and NodeB and NodeC receive these proposals and vote on them. After the votes are counted, the block with more votes is committed by the nodes.

However, like any other consensus algorithm, BFT is susceptible to attacks. The following are typical attacks on BFT and the countermeasure to defend against the attacks.

Sybil attack: A Sybil attack occurs when a malicious actor creates multiple fake identities (known as Sybils) in a network, with the aim of controlling the network. In the context of BFT, a Sybil attack can be used to overwhelm the honest nodes in the network and force them to accept a fraudulent transaction or decision. To prevent a Sybil attack, BFT systems can employ techniques such as proof-of-work or proof-of-stake. Proof-of-work requires nodes to solve computational puzzles before they can participate in the consensus process, while proof-of-stake requires nodes to hold a certain amount of cryptocurrency or stake in the network to participate.

Man-in-the-Middle attack: In a man-in-the-middle (MITM) attack, an attacker intercepts and alters the messages being sent between nodes in the network. In the context of BFT, an MITM attack can be used to change the decision being made by the network, leading to a fraudulent transaction. To prevent a Man-in-the-Middle Attack, BFT systems can use cryptographic techniques such as digital signatures and message authentication codes (MACs) to ensure that messages are not tampered with during transmission. In addition, nodes can use encryption to protect the confidentiality of messages.

Distributed Denial-of-Service (DDoS) attack: A DDoS attack involves overwhelming a network with traffic or requests, making it inaccessible to legitimate users. In the context of BFT, a DDoS attack can be used to prevent honest nodes from participating in the consensus process, leading to a failure in the network. To prevent a DDoS attack, BFT systems can employ techniques such as rate limiting and traffic filtering to prevent DDoS attacks. Nodes can also be distributed across multiple data centers to mitigate the impact of a DDoS attack.

These are some of the possible security attacks that could occur in various consensus algorithms. It is important to note that while these attacks may be possible, they can also be mitigated through various security measures, such as network design and implementation, monitoring, and security updates.

Moreover, each consensus algorithm has its own advantages and disadvantages, and there is no perfect consensus algorithm that is invulnerable to all types of attacks. The security of a consensus algorithm depends on many factors, including the size of the network, the number of nodes, the complexity of the algorithm, and the incentives for nodes to follow the protocol.

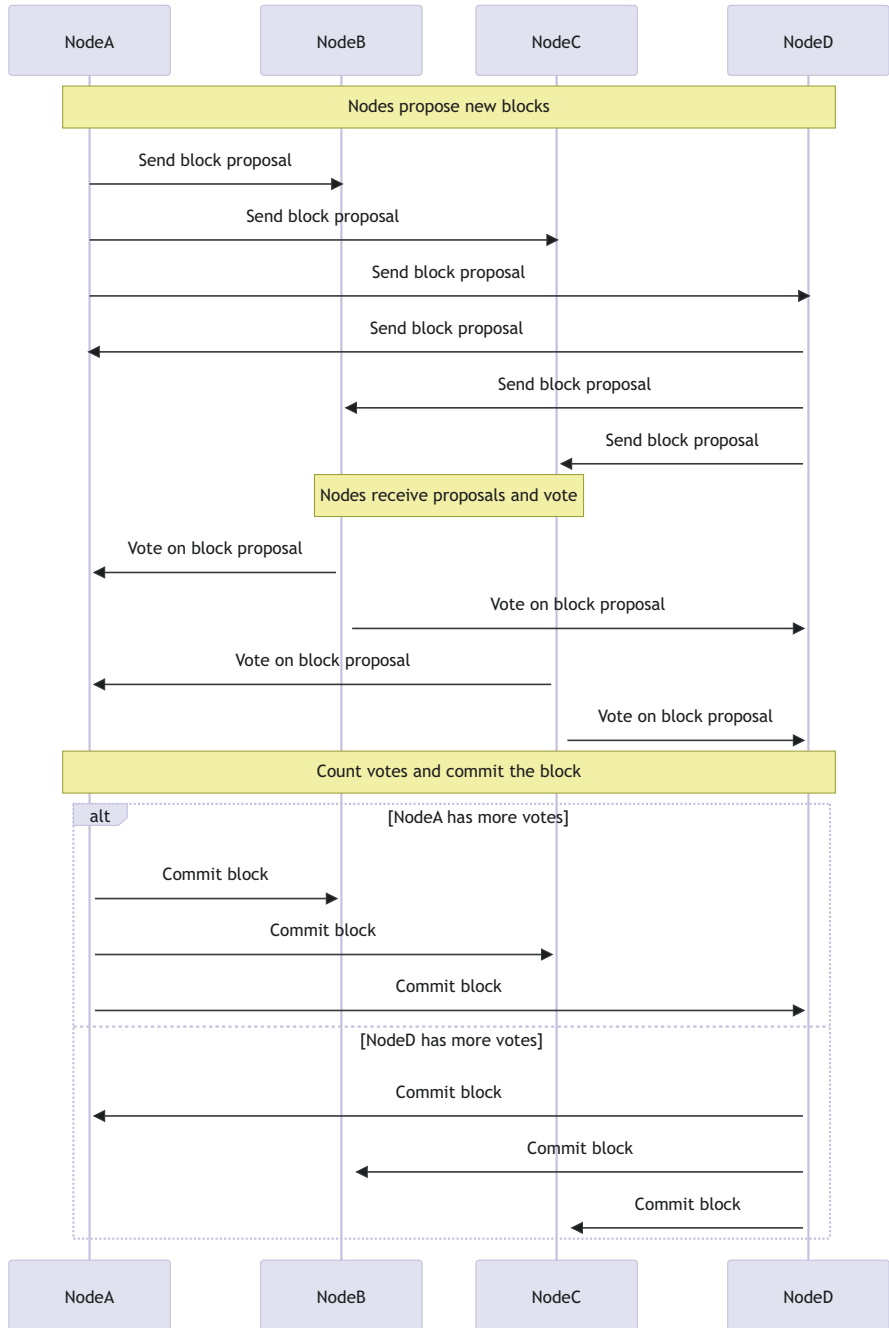


Fig. 2.6 BFT Algorithm Illustration

2.6 Attacks on Blockchain Network Layer and Countermeasures

Blockchain network is inherently a peer-to-peer network, which means that each node in the network has equal status and communicates directly with other nodes in the network, without the need for a central authority or intermediary.

In a peer-to-peer (P2P) network, computers or devices communicate directly with each other rather than through a central server. P2P networks can be used for various purposes, including file sharing, online gaming, and distributed computing.

One of the main advantages of P2P networks is that they can be more resilient and fault-tolerant than centralized networks since there is no single point of failure. However, P2P networks also have their own set of security challenges. For example

Lack of central authority: In a P2P network, there is no central authority to enforce security measures or monitor activity. This can make it more difficult to detect and prevent security breaches.

Security vulnerabilities: P2P software and protocols may have security vulnerabilities that can be exploited by attackers.

Malicious nodes: In a P2P network, any participant can potentially act as a “node,” or point of connection. This means malicious actors could join the network and engage in malicious activity, such as distributing malware or spam.

In the context of blockchain technology, P2P networks play a crucial role in maintaining the security and integrity of the blockchain. In a blockchain, P2P networks are used to distribute and validate transactions and blocks. Each participant in the network maintains a copy of the blockchain and verifies the validity of new transactions and blocks before adding them to the chain.

This decentralized approach to transaction validation helps to ensure that the blockchain is secure and resistant to tampering. However, ensuring that the P2P network is secure and that participants behave honestly and correctly is still important.

The integrity of the blockchain network layer is crucial for maintaining the security of the entire system. In recent years, there have been several attacks on the blockchain network layer that have exploited vulnerabilities in the system. This section will explore some of the previous attacks on the blockchain network layer and discuss the measures that can be taken to enhance the security and integrity of the network.

2.6.1 Time Jacking Attack and Countermeasures

Timejacking is a blockchain attack where a hacker manipulates the network time counter of a node, forcing it to accept an alternative blockchain. This attack poses a threat to blockchain security, particularly for cryptocurrencies like Bitcoin. The attack involves two stages: Fork & Isolate and Double-Spend.

In the Fork & Isolate stage, the attacker generates a “poisoned” block which the victim node rejects, while the rest of the network accepts it. The attacker manipulates the victim’s network time by adding fake peers with inaccurate timestamps, causing the victim to reject subsequent blocks from the “poisoned” block. Consequently, the victim becomes isolated from the main network.

During the Double-Spend stage, the attacker generates an alternative chain containing a transaction that transfers tokens to the victim’s wallet. The victim accepts this chain while the main network disregards it. The victim believes they have received tokens and sends goods, while the main network assumes the tokens never left the attacker’s wallet.

To prevent timejacking attacks, several measures can be taken:

- Use the node’s system time instead of network time for determining the upper limit of block timestamps and block creation.
- Restrict the node’s network time to a value within 30 minutes, reducing the maximum initial attack window.
- Require more confirmations before accepting transactions, striking a balance between expediency and reversal probability.
- Rely on trusted peers or distributed networks, although this approach does not fully resolve the global time agreement problem.
- Validate blocks through median blockchain time exclusively to prevent timestamp splits and ensure that peers cannot disagree on block validity.
- Implement delayed timestamp validation, allowing nodes to retain blocks with excessive timestamps in memory and re-check them later.

2.6.2 Tampering with Message Body and Countermeasures

Tampering with the message body is possible as a network layer attack on an earlier version of Bitcoin through the use of a technique called “transaction malleability.”

Transaction malleability is a term used to describe a flaw in the Bitcoin protocol that allows an attacker to modify the unique transaction identifier (TXID) of a Bitcoin transaction before it is confirmed in the blockchain.

Every Bitcoin transaction has a unique TXID that is generated by hashing the transaction data using the SHA-256 algorithm. Once a transaction has been broadcast to the network, the TXID is used to identify the transaction and track its progress through the blockchain.

However, due to the design of the Bitcoin protocol, it is possible for an attacker to modify certain parts of the transaction data without changing its validity. This can result in a new transaction that has a different TXID but is otherwise identical to the original transaction.

This presents a problem because Bitcoin nodes and miners use the TXID to confirm transactions and include them in the blockchain. If an attacker modifies the

TXID of a transaction, it can cause confusion among nodes and miners, leading to the possibility of double-spending and other security issues.

To address this issue, Bitcoin developers have implemented a few different solutions, including Segregated Witness (SegWit) and the Replace-By-Fee (RBF) protocol. These solutions aim to make it more difficult for attackers to modify transaction data and create new transactions with different TXIDs.

Segregated Witness (SegWit) is a protocol upgrade that was activated on the Bitcoin network in August 2017. One benefit of using this protocol is to solve the issue of transaction malleability.

SegWit works by separating the signature data from the transaction data, which allows for more efficient use of block space and reduces the size of the transaction. By doing this, the signature data is no longer included in the transaction hash, which makes it impossible for an attacker to modify the signature data without changing the transaction ID.

This means that even if an attacker attempts to tamper with the message body of a transaction that uses SegWit, they will not be able to change the transaction ID, which is the key identifier used to track transactions on the blockchain. This helps to prevent double-spending attacks and other forms of fraud that rely on modifying the transaction ID.

In addition to its security benefits, SegWit also provides other advantages, such as faster confirmation times and lower transaction fees. However, it does require some changes to the way that Bitcoin transactions are created and verified, so it may take some time for adoption to become widespread. Nonetheless, many exchanges and wallets have already implemented SegWit support, and its adoption is expected to continue to grow over time.

2.6.3 MEV Attack and Countermeasures

One big issue with most smart contract-enabled blockchains is the so-called miner maximal extractable value or MEV. To understand MEV, it is necessary to understand the concept of mempool.

When a user submits a transaction, the network will broadcast it to peer nodes. The peer nodes can decide if the transaction can be included in the upcoming block based on the incentive fees included with the transaction. So, the transaction will stay in the so-called mempool before it is included in a block. From the message integrity perspective, this message is not altered in the literal message context. However, from the economic value perspective, the miner or bots can use front-running, sandwich, or back-running to extract value from user transactions. This can happen when the ordering of the transactions impacts how much a user can get from the transaction. For example, a user's market order can be used in the so-called sandwich attack in a decentralized exchange.

In a sandwich attack, a bad actor will look for a pending transaction by another user on a blockchain network of their choice. The predatory trader will then place

one trade order just before the victim's pending transaction (front-running) and another trade order just after it (back-running). The victim's pending transaction will be sandwiched between the two new trade orders created by the attacker. If the attack is successful, the attacker will create an artificial price increase and generate a profit.

Sandwich attacks are possible because of transaction transparency in the mem-pool. If a user's transaction is a simple transfer, then the transaction value integrity is protected. However, if the transaction is more complex, such as a swap transaction with a decentralized exchange or some complex transaction with decentralized finance (for example, lending protocol liquidations), then the attacks can extract value from this transaction. The attacks can be a miner or a bot monitoring the mem-pool. This is an example of MEV.

Maximal extractable value (MEV) refers to the maximum value that can be extracted from block production in excess of the standard block reward and gas fees by including, excluding, and changing the order of transactions in a block. Beyond what's happening within blocks, MEV can have deleterious effects between blocks. If the MEV available in a block significantly exceeds the standard block reward, miners may be incentivized to re-mine blocks and capture the MEV for themselves, causing blockchain reorganization and consensus instability.

This possibility of blockchain reorganization has been previously explored on the Bitcoin blockchain. As Bitcoin's block reward halves and transaction fees make up a greater and greater portion of the block reward, situations arise where it becomes economically rational for miners to give up the next block's reward and instead re-mine past blocks with higher fees. With the growth of MEV, the same sort of situation could occur in Ethereum, threatening the integrity of the blockchain. Therefore, MEV can impact blockchain integrity by enabling malicious actors to manipulate transactions for their own.

The following are some of the countermeasures against MEV attacks on the blockchain:

Transaction batching and sorting: Protocols like Gnosis Safe use transaction batching and sorting to prevent front-running. Batching multiple transactions together and sorting them by value or time reduces the possibility of front-running and transaction reordering attacks.

Cryptographic techniques: Using cryptographic techniques like commit-reveal schemes, transactions can be hidden from miners until they are included in a block. This prevents miners from having the information they need to reorder or censor transactions based on their content.

Flashbots: Flashbots is a research organization working on improving blockchain systems by reducing the negative externalities associated with MEV. They have developed a communication channel between miners and users called MEV-Relay, which allows users to submit their transactions directly to miners, thus reducing front-running and other MEV-related issues.

Randomized transaction ordering: Implementing randomness in the transaction ordering process can reduce the predictability of transaction inclusion, making it more difficult for miners to extract MEV.

Time-delayed transactions: Introducing time delays between transaction submission and inclusion in a block can help minimize front-running and other MEV-related issues.

By implementing these countermeasures, blockchain networks can reduce the impact of MEV attacks and maintain a more secure, fair, and transparent environment for all participants.

2.6.4 Routing Attacks and Countermeasures

A routing attack is a type of attack on a blockchain network where the attacker breaks the network into multiple isolated chunks by controlling the links between these isolated chunks. By doing so, the attacker controls each chunk's view of the current state of the network.

A routing attack can have consequences on individual nodes and the overall blockchain network. An attacker alters the transactions before sending them to peers. It cannot be easily detected by the other nodes as the attacker divides the network into subdivisions by which the communication between nodes is lost.

Countermeasures against routing attacks include making peer selections routing-aware, increasing diversity in Internet paths seen by connections, use of secure routing protocols, such as the Border Gateway Protocol (BGP) and the Resource Public Key Infrastructure (RPKI), the use of blockchain-specific security mechanisms, such as the SABRE system (Apostolaki et al., 2018), monitoring the performance of connections, and implementing end-to-end encryption.

2.6.5 Fake Bootstrapping Attack and Countermeasures

This security threat arises when a new node attempts to join the network. During this process, the new node must establish a connection with an existing node, referred to as a bootstrap node, to gain access to the network's current state and peers. The bootstrap node essentially serves as the new node's entry point into the blockchain network.

If this bootstrap node happens to be malicious, it can significantly impact the network view for the newly joining node by manipulating or falsifying the information it provides. This might include presenting a distorted view of the network topology, providing incorrect blockchain data, or directing the new node to connect only with other malicious nodes.

In doing so, the malicious bootstrap node can effectively isolate the new node, creating an isolated network. In this isolated environment, the new node becomes susceptible to various attacks, such as double-spending or consensus manipulation, as it is no longer receiving accurate and up-to-date information from the rest of the network.

To mitigate this security threat, the following countermeasures can be implemented:

Use multiple trusted bootstrap nodes: Instead of relying on a single bootstrap node, the new node can establish connections with multiple trusted nodes to obtain a more accurate and diverse view of the network.

Verify blockchain data: Newly joining nodes should independently verify the blockchain data they receive from bootstrap nodes by cross-referencing with other nodes or using cryptographic proofs, such as Merkle proofs, to validate the integrity of the data.

Monitor connection quality: Continuously monitor the connection quality and response times of connected nodes to identify potential malicious behavior or inconsistencies in the information being provided.

Random peer selection: Employ a random peer selection process when joining the network to minimize the risk of connecting with a malicious bootstrap node.

By employing these countermeasures, new nodes can effectively reduce the risks associated with connecting to a malicious bootstrap node and ensure they are receiving accurate and trustworthy information from the blockchain network.

2.6.6 Eclipse Network Attack and Countermeasures

The eclipse attack is similar to the fake bootstrapping attack since both attacks involve isolating victim nodes from the network. Their methods and targets differ. A fake bootstrapping attack focuses on exploiting a new node during its initial connection to the network, whereas an Eclipse Network Attack targets existing nodes by inundating them with connections from fake nodes to sever their communication with the rest of the network.

Specifically, the eclipse attack targets a specific node by overwriting its network table and redirecting its outgoing connections to IP addresses controlled by the attacker. This can leave the victim vulnerable to double-spending attacks.

To prevent this, periodic “feeler” connections can be made to test IP addresses in the “New Nodes” section and only promote valid nodes to “Tried Nodes.” This increases the cost for the attacker by requiring them to acquire new IP addresses in order to change the data from the required sections.

In the context of the eclipse attack, the “tried nodes” are a set of Bitcoin nodes that a node has already connected to and considers reliable. The “new nodes” are a set of potential Bitcoin nodes that a node has not yet connected to.

A “feeler” connection is a periodic connection made to test the IP addresses in the “new nodes” section. If the connection is successful, the node is promoted to the “tried nodes” section. This mechanism of filtering IP addresses helps prevent an attacker from filling up “new nodes” with random addresses and only allows valid nodes to be added to “tried nodes.” This makes it difficult for an attacker to eclipse a node and change the data from the required sections.

2.6.7 *Attack on Libp2p and Countermeasures*

LibP2P is a versatile network stack designed to enable peer-to-peer communication between nodes in decentralized networks. It supports various communication types and offers security features like encryption to ensure private and secure exchanges. Several protocols are available for transmitting information between peers, including the gossip domain, which disseminates information rapidly across the network, and the request-response domain, which contains protocols for clients to request specific data from their peers.

Each peer is identified by a unique cryptographic key that enables authentication of remote peers. However, since authorization requirements can vary significantly across peer-to-peer systems, libP2P does not provide an out-of-the-box authorization framework. Despite its robust features, libP2P is not immune to malicious actors, and it is susceptible to several types of attacks, such as Sybil attacks.

One example of a potential vulnerability is the Kad-DHT protocol, a distributed hash table that offers a shared key/value storage system for all participants. This protocol is particularly prone to Sybil attacks, where an attacker creates numerous fake identities to gain control over a substantial portion of the network. By doing so, the attacker can manipulate or censor data, disrupt communication, or even launch more severe attacks.

Another vulnerability was discovered in the libp2p-core before 0.8.1 for Rust. Attackers can spoof ed25519 signatures (CVE Details, [2020](#)).

To mitigate these risks and protect against potential and actual attacks on libP2P, various countermeasures can be employed:

Regular updates and patches: Keeping the libP2P implementation up-to-date with the latest security patches and updates can help prevent known vulnerabilities from being exploited by attackers.

Limit node connections: Implementing a limit on the number of connections a node can establish can help prevent Sybil attacks by making it more difficult for an attacker to create a large number of connections with fake identities.

Reputation systems: Developing and implementing a reputation system can help identify and isolate malicious nodes based on their behavior, reducing the impact of attacks on the network.

Secure peer authentication: Ensuring proper authentication of peers using cryptographic techniques can help prevent man-in-the-middle attacks and maintain secure communication channels.

By adopting these countermeasures, libP2P users can enhance the security of their networks and protect against potential and actual attacks.

References

- Apostolaki, M., Marti, G., Müller, J., & Vanbever, L. (2018, August 19). [1808.06254] SABRE: Protecting Bitcoin against routing attacks. arXiv. Retrieved March 19, 2023, from <https://arxiv.org/abs/1808.06254>
- Cimpanu, C. (2018, March 2). *Eclipse attack plugged in Ethereum network*. Bleeping Computer. Retrieved February 4, 2023, from <https://www.bleepingcomputer.com/news/cryptocurrency/eclipse-attack-plugged-in-ethereum-network/>
- Clarke, G. (2019, January 9). *After Ethereum classic suffers 51% hack, experts consider - Will bitcoin be next?* Forbes. Retrieved March 17, 2023, from <https://www.forbes.com/sites/ginaclarke/2019/01/09/after-ethereum-classic-suffers-51-hack-experts-consider-will-bitcoin-be-next>
- CVE Details. (2020, August 24). *CVE-2019-15545: An issue was discovered in the libp2p-core crate before 0.8.1 for rust. Attackers can spoof ed25519 signatures*. CVE Details. Retrieved March 19, 2023, from <https://www.cvedetails.com/cve/CVE-2019-15545/>
- Fischer, M., Lynch, N. A., & Paterson, M. S. (1985). *Impossibility of distributed consensus with one faulty process*. Research. Retrieved March 6, 2023, from <https://groups.csail.mit.edu/tds/papers/Lynch/jacm85.pdf>
- Hayward, A. (2021, September 20). *Solana blames 'denial of service attack' for last week's downtime*. Decrypt. Retrieved February 4, 2023, from <https://decrypt.co/81375/solana-blames-denial-of-service-attack-for-last-weeks-downtime>
- Khandelwal, S. (2018, May 29). *Critical RCE flaw discovered in Blockchain-based EOS smart contract system*. The Hacker News. Retrieved February 4, 2023, from <https://thehackernews.com/2018/05/eos-blockchain-smart-contract.html>
- Numen Cyber Technology. (2022, October 12). *Critical vulnerability in Aptos MoveVM Discovered by Singapore Web3 security company*. GlobeNewswire. Retrieved February 4, 2023, from <https://www.globenewswire.com/news-release/2022/10/12/2533292/0/en/Critical-Vulnerability-in-Aptos-MoveVM-Discovered-by-Singapore-Web3-Security-Company.html>

Chapter 3

Wallet Security



Carlo Parisi, Dyma Budorin, and Ostap Khalavka

3.1 Introduction

3.1.1 Overview of Different Types of Blockchain Wallets

Blockchain wallets act as storage for users' digital assets. Cryptocurrency assets are as safe as the wallets they are stored in. Through blockchain wallets, users interact with the blockchain network. There are two main types of blockchain wallets, including software and hardware wallets, which are also referred to as "hot" and "cold" storage. In reality, blockchain wallets do not store cryptocurrencies. Instead, they generate the information needed to send and receive tokens. This information includes public and private keys.

3.1.2 Explanation of the Different Kinds of Wallets

Cold wallets and hot wallets are types of cryptocurrency wallets used for storing digital assets. Cold wallets, also known as offline or hardware wallets, are not connected to the Internet, providing higher security for long-term storage. Examples include the Ledger Nano S and paper wallets. Hot wallets, also known as online or software wallets, are connected to the Internet and are more convenient for frequent transactions. Examples include Exodus, Mycelium, and MetaMask. Cold wallets are less susceptible to hacks and cyberattacks, while hot wallets are more vulnerable due to their constant Internet connection. The choice between a cold wallet and a

C. Parisi (✉) · D. Budorin · O. Khalavka
Hacken, Lisbon, Portugal
e-mail: c.paris@hacken.io; d.budorin@hacken.io; o.khalavka@hacken.io

hot wallet depends on the user's priorities, whether it is long-term asset security or ease of access for daily transactions.

Blockchain wallets may be further divided into four big categories depending on the device or software used for their management.

Mobile wallets: These are suitable for users who frequently use cryptocurrencies for payments. Mobile wallets are apps that store users' private keys and often use Simplified Payment Verification (SPV) technology, which operates on smaller subsets of the blockchain and relies on trusted nodes in the network (Potapenko et al., 2021).

Web wallets: These store users' private keys, making them more susceptible to hacks and third-party collapses. It is essential to choose a reputable web wallet provider with robust security measures in place.

Desktop wallets: Once downloaded and installed on a user's computer, desktop wallets store private keys on the user's hard drive or solid-state drive.

Hardware wallets: These store private keys on a secure physical device, making them resistant to computer viruses. Hardware wallets are ideal for users who prioritize the long-term storage and protection of their assets.

The choice of wallet type depends on the user's digital asset management strategy. A combination of wallet type could be used, hardware wallets for assets that should be more safe and less accessible and other kinds of wallets for assets that should be more easily accessible (Sharma, 2023).

3.1.3 *Comparison of Blockchain Wallets to Traditional Banking and Financial Systems*

The traditional banking system does not eliminate major issues attributable to transactions. Namely, transactions may be slow and have to pass through an intermediary. The traditional banking system works on the Internet and uses its own software, while blockchain wallets work on the blockchain. Blockchain wallets do not process fiat money, and only crypto serves as a medium of exchange.

Unlike traditional banking, *blockchain wallets do not need centralized command to process every transaction*, and, thus, users are the only ones who can determine whether to conduct a transaction. *The other thing about blockchain wallets is that they cannot be frozen by outside parties*. In traditional banking, financial institutions can freeze a client's account or block any transactions at the request of law enforcement authorities. *Blockchain wallets do not let any party interfere with the user-network interaction chain*.

Geographical location has no bearing on blockchain wallet operations. The speed of processing does not depend on the physical distance between the cryptographic sender and receiver. The functioning of blockchain wallets is governed by smart contracts, which automate agreements. Only when certain conditions of the

agreement are met does the execution of a transaction take place. Unlike in the world of blockchain, in the financial world, transactions take more time and cost more since they are based on greater trust, requiring manuals and paper to meet legal rules and avoid possible implications.

3.1.4 Difference between Custodial and Non-custodial Wallets

There are also two broad categories of digital crypto wallets, depending on who has full control over the user's assets (Academy, 2023).

Custodial wallets: There is a third party holding and managing a private key to the user's wallet on his or her behalf and holding his or her assets in custody. An example of a custodial wallet is an account on a centralized crypto exchange. Even if a customer forgets or loses his or her cryptocurrency exchange account password, he or she will still be able to access the account and its assets by contacting a third-party customer support service.

Non-custodial wallets: Users alone have complete control over their assets. Non-custodial wallets are a good option for experienced users who know how to safely store their private keys and secret phrases. Non-custodial wallets are used for interactions with decentralized exchanges and decentralized applications. One of the best things about non-custodial wallets is that they do not charge a custodial fee. On the other hand, *the user has to take more responsibility for managing a non-custodial wallet.*

3.2 How Blockchain Wallets Work

3.2.1 Technical Explanation of How Blockchain Wallet Works

There are two main types of wallets in the crypto space: nondeterministic and deterministic.

Nondeterministic wallets, which are also called "Just a Bunch of Keys" (JBOK) wallets, make each key from a different random number. These keys have nothing in common.

On the other hand, deterministic wallets generate all keys from a single master key, known as the seed. All the keys in this type of wallet are related to each other and can be regenerated if the original seed is known (Antonopoulos, 2017). Deterministic wallets often use a hierarchical structure, like in BIP-32 (B, 2022) and BIP-44 (B, 2019).

For added security against data loss, deterministic wallets often use a mnemonic code made up of a list of words. This can be written down and used in the event of an accident, such as losing your phone. However, *it is important to keep these code*

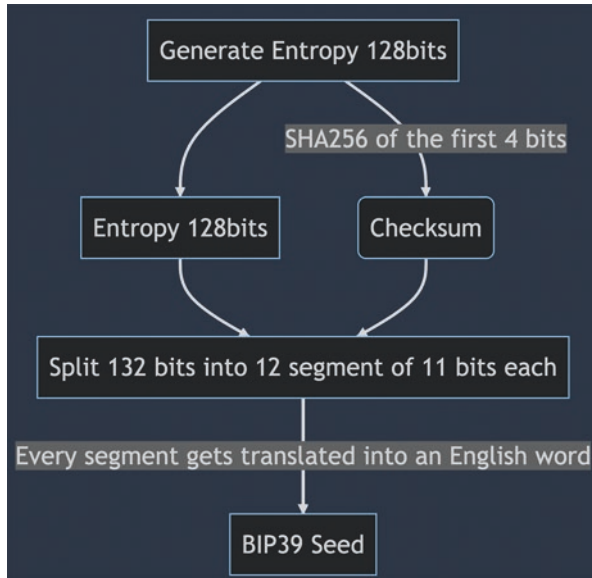


Fig. 3.1 From Entropy to BIP39 Seed

words safe, as someone with access to them can recreate your wallet and gain access to your funds. It is recommended to write them down on paper and store them in a secure location, *never storing them electronically*.

The mnemonic phrase, which is also called the “seed phrase” or “recovery phrase,” is a set of words that are made using a standard method described in BIP-39 (B, 2020) (Fig. 3.1).

The process starts by creating a cryptographically random sequence of 128 to 256 bits, known as S . A checksum is then added to this sequence by taking the first (length-of- S , 32) bits of the SHA-256 hash of S . The checksum is then appended to the end of the random sequence S . This sequence and checksum are then divided into groups of 11 bits, and each group is mapped to a word from a predefined dictionary of 2048 words. When you put these words together in the order they were made, you get the final mnemonic phrase, which is a unique, easy-to-remember phrase that can be used to restore a wallet.

3.2.2 Overview of the Use of Public and Private Key

The process of generating a private key or master key on a blockchain can vary. In a Bitcoin wallet, for example, there is a set of key pairs, each of which is made up of a private key and a public key. The private key is a randomly chosen number. Elliptic curve multiplication, which is a one-way cryptographic function, is used on

the private key to make the public key. The Bitcoin address is then created by using a one-way cryptographic hash function on the public key (Antonopoulos, 2017).

In Ethereum, the process is slightly different. There are two types of accounts: Externally Owned Addresses (EOAs) and contracts. EOAs have a public and private key pair similar to Bitcoin. Contract addresses are made when a special transaction is sent to the 0 address (20 bytes of 0s with 0x as a prefix), and the address is based on the sender's public address and their nonce (Antonopoulos & Wood, 2021).

Digital signatures, which are made with the private key, are used to get access to and control over funds in a blockchain. Transactions need a valid digital signature in order to be included in the blockchain. Anyone who knows how to get a private key can control the account and any coins or tokens that go with it. *As long as a user keeps their private key safe, digital signatures in Ethereum transactions confirm the true owner of the funds by proving ownership of the private key.*

The process of generating a public key from a private key in Bitcoin is done through elliptic curve multiplication. The private key, which is shown as a random number k , is multiplied by the generator point G , a fixed point on the curve. This results in another point on the curve, which is the corresponding public key K . The `secp256k1` standard describes the generator point, which is the same for all Bitcoin keys. The equation can be represented as:

$$K = k * G \tag{3.1}$$

Generating a public key (K) from a private key (k) where k is the private key, G is the generator point, and K is the resulting public key. *Since the generator point is the same for all users, the same private key multiplied by G will always result in the same public key.* The relationship between the private key and the public key is fixed and can only be calculated in one direction, from the private key to the public key (Antonopoulos & Wood, 2021; Antonopoulos, 2017). This is why you can share a Bitcoin address, which is based on the public key, without giving away your private key.

Using a one-way cryptographic hashing method, a Bitcoin address can be made from a public key. This process involves applying a “hash algorithm,” a one-way function that produces a unique fingerprint or “hash” of an input of any size. Cryptographic hash functions are used extensively in Bitcoin, including in the creation of Bitcoin addresses, script addresses, and the mining Proof-of-Work algorithm. The specific hash algorithms used to generate a Bitcoin address from a public key are SHA-256 and RIPEMD-160. To create a Bitcoin address, the public key K is first hashed using SHA-256, and then the result is hashed again using RIPEMD-160, resulting in a 160-bit (20-byte) number (Fig. 3.2).

$$A = \text{RIPEMD160}(\text{SHA256}(K))$$

Fig. 3.2 Generating a Bitcoin Address (A) from a private key (K)

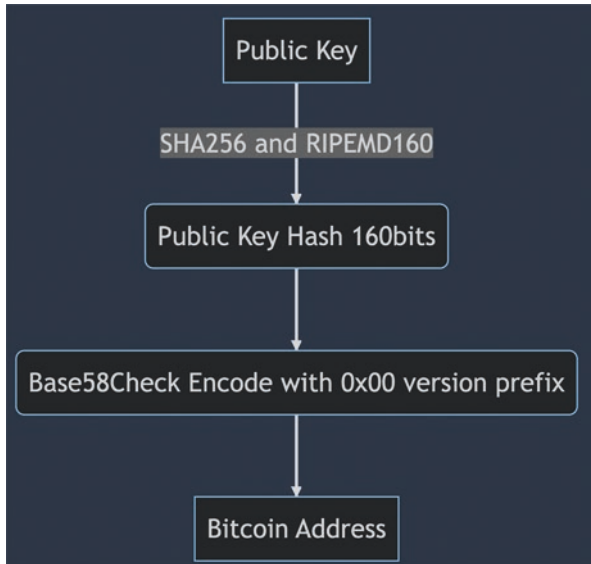


Fig. 3.3 From public key to bitcoin address

$$A(pr) = \beta_{96 \dots 255}(KEC(ECSDAPUBKEY(pr)))$$

Fig. 3.4 Generating a public/private key pair in Ethereum

Bitcoin addresses are usually encoded with Base58Check, which uses 58 characters and a checksum to make them easier to read, make them less confusing, and prevent mistakes when they are written down or typed in (Antonopoulos, 2017) (Fig. 3.3).

In Ethereum, the process of generating a public/private key pair is as follows (Fig. 3.4):

The corresponding Ethereum address, $A(pr)$, can be found by taking the 160 bits on the right of the Keccak hash of the corresponding ECDSA public key. This is done with a private key, pr . To put it simply, the process of getting a public key from a private key is similar to the process used in Bitcoin, where $K = k * G$. The public key is a 64-byte string of letters and numbers. The public address used to receive transactions can be made from the public key by using a one-way hash function (Keccak-256) to turn it into a 32-byte string, then taking the last 20 bytes and adding a 0x prefix to them. When it comes to contracts in Ethereum, there are two methods for deriving the address: the opcode CREATE and the opcode CREATE2 proposed in the Ethereum Improvement Proposal (EIP) 1014 (Proposals, 2018). The most common method is CREATE, which gets the address by taking the rightmost 160 bits of the Keccak hash of the RLP encoding of a structure that contains the sender address and the account nonce. The sender is the address that initiates the

$$\alpha = \beta 96 \dots 255 (KEC(RPL((s, \sigma[S]n - 1)))$$

Fig. 3.5 Generating a contract address with the CREATE opcode

transaction, and the nonce is a counter that tracks the number of transactions sent by an account (Antonopoulos & Wood, 2021) (Fig. 3.5).

3.2.3 *Overview of the Role of the Wallet in Public and Private Key*

A wallet is a piece of software that connects you to the blockchain and is mostly used to keep track of keys and addresses. It makes a private key by picking a number between 1 and 2^{256} at random. It does this by using a good source of entropy to make sure the number is not predictable or deterministic. As was already said, the public key and address can be figured out from the private key. The private key is used to authorize transactions and show ownership of funds, while the public key is used to get the address that is used to receive transactions or funds. Public keys and addresses can be shared publicly because the process used to derive them is one-way, and *it is computationally infeasible to determine a private key from a public key*.

3.2.4 *Smart Contract Wallets*

A smart contract wallet is a type of wallet that combines the benefits of custodial and non-custodial wallets. With custodial wallets, there is a third party who can withdraw funds from the wallet if he so desires, whereas with non-custodial wallets, the user bears a significant amount of responsibility for the security of the private key (DeCommas, 2022).

Generally, a smart contract wallet is a smart contract that acts as a wallet through account abstraction; the most famous example of a smart contract wallet are multisignature wallets.

3.2.5 *Account Abstraction*

There are currently three major challenges facing the widespread adoption of blockchain technology:

1. The complexity of the technology and the difficulty of providing a user-friendly experience
2. The management of wallets and seed phrases by companies and escrow services
3. The recovery of lost or stolen wallets due to poor operational security

Even though these problems have not been fully solved yet, many people use account abstraction (Julien Niset, 2022), multisignature wallets, and social recovery methods to deal with them.

Account abstraction aims to merge the two types of Ethereum accounts, externally owned accounts and contract accounts, into one unified contract account (Team, 2023). Transactions will also move from the blockchain to the Ethereum Virtual Machine (EVM), eliminating the need for separate account types. The main goal of this change is to make things easier for users by letting developers make better protocols and services without having to think about different types of accounts. Additionally, it will offer advanced features such as multisignature security, social recovery, rate limiting, and gasless meta-transactions.

There are currently various EIPs that aim to improve account abstraction. These include EIP-86 (Vitalik Buterin, 2017), EIP-2938 (Proposals, 2020a), EIP-3074 (Proposals, 2020b), and EIP-4337 (Proposals, 2021), which are notable proposals in this area.

When Ethereum account abstraction is finished, it will change how accounts are implemented and how users interact with them. It will also give developers the freedom to create and manage accounts however they want.

With account abstraction, developers will be able to utilize smart contract logic not just for determining transaction effects but also for fee payment and validation. This will provide important security benefits like multi-sig and smart recovery wallets and the ability to change keys without switching wallets.

Some of the use cases that account abstraction will make possible include:

Wallets: With account abstraction, users will be able to enjoy advanced security features such as multi-sig and smart recovery, as well as the convenience of changing keys without changing wallets.

Sponsored transactions: Account abstraction will let entities or their subsidiaries do things like pay fees on behalf of users and let users pay gas fees in ERC-20 tokens, which will be turned into ETH.

Meta-transactions: With account abstraction, users can receive meta-transactions (gasless) and pay for gas without having to trust a relayer.

3.2.6 Multisignature Wallets

Bitcoin is usually stored in a single-key address, which means that only the person who has the private key to that address can use the money. This means that only one key is needed to sign transactions, and anyone with the private key can transfer the coins without any authorization. *However, this system presents security issues as it*

is vulnerable to phishing attacks, and the funds are protected by a single point of failure. Additionally, this method is not ideal for businesses, as the private key would either be entrusted to a single person or multiple individuals, which is not secure.

Multi-sig wallets solve these problems by making it so that you need more than one signature, *made with different private keys*, to get to the money on an address. An example for a configuration is 2-of-3, which means that you only need two signatures to get to the money in a 3-signature address.

Multi-sig technology has a variety of potential applications; some of the most common use cases include:

- Corporate treasury management
- Escrow services
- Secure storage of digital assets
- Crowdfunding platforms
- Secure transfer of sensitive information

It is a more secure way of handling cryptocurrency funds and can be used for a variety of purposes, such as corporate treasury management, escrow services, and digital asset storage.

3.2.7 Social Recovery

To make sure a cryptocurrency wallet is safe, it should be made in a way that meets three key criteria:

1. **No single point of failure:** The wallet should not have a single point of vulnerability that can be exploited by an attacker to gain access to funds or a single point of loss that can deny access to funds.
2. **Low mental overhead:** The design should be user-friendly and not require users to learn new habits or exert mental effort to follow specific patterns of behavior.
3. **Maximum ease of transacting:** Normal activities such as transactions should not require much more effort than traditional wallets like Status or MetaMask.

One method that is gaining popularity for securing a wallet is social recovery. In this system, there is a single “signing key” that can be used to approve transactions.

There is a set of at least three “guardians” (or a higher number), and a majority of them can cooperate to change the signing key of the account.

The signing key has the ability to add or remove guardians, but only after a delay (often 1–3 days).

This method allows for a secure and user-friendly way to protect the wallet while also allowing for flexibility in case of loss or theft of the private key (Fig. 3.6).

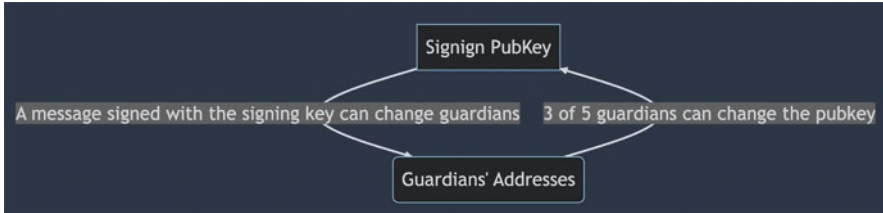


Fig. 3.6 *Signign Pubkey and Guardians' Addresses correlation*

3.2.8 MPC Wallet

MPC, or secure Multi-Party Computation, is a branch of cryptography that has been around for 30 years. It enables two or more parties to jointly compute the output of a function, without revealing their respective inputs.

For cryptocurrency wallets, MPC allows for the creation of a secure key management system without a single point of failure. Multiple parties, such as a mobile phone and a remote server, can perform cryptographic functions like key generation and transaction signatures together, while keeping their secrets confidential. In this process, there is never a single private key that is generated, split, or reconstructed (Portier & Diya, 2023; Wikipedia contributors, 2023; ZenGo, 2023).

By using MPC technology, wallets, both for consumers and institutions, can create a secure on-chain asset management system without a single private key. *This eliminates the risk of private key theft and key loss, as each party can individually back up their secret input without exposing the entire system.*

The familiarity and ease of using recovery methods such as email, trusted contacts, cloud backup, or biometric scanning make them less intimidating for most people. This is key to attracting new users to the world of crypto.

Having recovery options that are familiar to people will help them feel more comfortable using crypto. Once they are in the ecosystem, they may opt for more secure options or low-centralization risk alternatives.

Using multiple wallets for storing crypto assets is recommended. However, the biggest barrier for most people entering the crypto world is the use of seed phrases.

The idea of having a single phrase that controls the entire contents of an account can be daunting for many people. While some are willing to take full responsibility for keeping it safe, most are not.

Creating an easy entry point for new users to try crypto applications and hold assets without the worry of seed phrases is critical for attracting the next billion people to the world of Web3.

3.2.9 Most Common Attack Vectors

Attackers use a diversified portfolio of attack techniques to compromise blockchain wallets. Generally, these malicious techniques may be divided into the following broad categories:

Stealing private keys: Keys must be encrypted at the application level. Hackers can easily steal unencrypted keys in the application sandbox, clipboard, preference or external areas, SD card, etc.

Malicious devices: Hackers can gain access to the client's blockchain address by abusing common software development tools or if a device is rooted or jailbroken.

Man-in-the-Middle attacks: Malicious actors infiltrate a conversation between a user and an application to impersonate one of these parties. One of the most common ways for users to fall victim to man-in-the-middle attacks is to use unsecure public Wi-Fi networks.

Malware: Malicious actors actively utilize ads-delivered malware to drain victims' wallets. Instead of clicking on the official website, unsuspecting victims click on sponsored advertisements. This form of malware used by attackers is information-stealer that is often hidden on highly convincing phishing pages.

Phishing: Malicious techniques aimed at stealing private keys and security recovery phrases. Attackers create websites or services that appear to be genuine, such as a service to recover stolen funds. After gaining all sensitive data, an attacker can access someone's crypto wallet and exfiltrate assets. Phishing attacks are frequently disguised as attractive emails that appear to be legitimate. All these suspicious emails have the same purpose: to lure users into sharing some sensitive data or into performing actions that would lead to the loss of funds or the disclosure of data, including seed phrases (Pirus, 2020).

Threatful browser extensions: People like using browser extensions such as print screens, grammar checks, etc. However, apart from simplifying the user's life, some of these extensions, especially the ones coming from suspicious sources, may monitor and copy user's data and transfer them to hackers. That is why users should not install unverified browser extensions.

3.2.10 Wallet Security Features

Wallets for cryptocurrencies usually have more than one way to keep the user's money and private information safe. The following are a few of the most popular security features offered by cryptocurrency wallets:

- Private key management is essential to a crypto wallet since it allows users to sign transactions and gain access to their money. The majority of wallets provide solutions for managing private keys, such as hardware wallets that store the private key offline or multi-sig wallets that need several signatures to approve a transaction.

- By requiring the user to provide two forms of authentication, such as a password and a one-time code delivered to their phone, in order to access their funds, two-factor authentication (2FA) increases security.
- Cryptocurrency wallets frequently employ encryption to safeguard private keys and other sensitive data, as well as to block unauthorized access even in the event that a device or computer is lost or stolen.
- Good wallets provide backup and recovery alternatives, such as seed phrases, to help users get their money back if they lose access to their wallet.
- Software upgrades on a regular basis can shield users against threats and address any faults in the wallet program. Attack vectors are occasionally only identified years after the wallet has been released, as was the case with the fault-injection technique identified for the Trezor hardware wallet, which was subsequently patched through software updates (Zetter, 2022).

The user is ultimately the biggest weakness for the majority of wallets. So, a major security feature, along with enough randomness for key generation, strong encryption to keep the keys safe, and ways to fix software or hardware problems, is the ability to create an interface that connects the user to the blockchain in a way that is easy to use and gives them useful information.

It's important to choose a wallet with strong security features, and it's also a good idea to keep private keys and seed phrases safe, back up the wallet regularly, and keep up with the blockchain while working with it.

3.3 Past Blockchain Wallet Hacks

3.3.1 Overview of Past Relevant Wallet Hacks

3.3.1.1 “NFT God” Hacked, January 2023

On January 14, 2023, “NFT God” (real name Alex) downloaded the video streaming service OBS, but instead of the original link, he used a sponsored link on Google that contained malicious software. A few hours later, one of God’s followers alerted him that his Twitter account had been hacked. However, the account compromise was only the first in a series of attacks. All wallets belonging to “NFT God” were drained of crypto and NFTs. The attacker also hacked Alex’s Gmail, Discord, and Substack accounts and sent emails containing malicious links to more than 16K subscribers (Connor Sephton, 2023).

Alex made a costly mistake when setting up his ledger account. According to him, he entered his seed phrase in a way that no longer kept the wallet cold. Because Alex made this mistake, the hacker was able to use malware to get into his wallet.

3.3.1.2 BitKeep, December 26 2022, \$8M Lost

On December 26, 2022, some users of the BitKeep wallet reported seeing their assets drained from their wallets. The team confirmed that the attacks hijacked some Android package (APK) downloads and installed them with code. APK is the file format that allows users to install apps from third-party sources on their Android phones. This incident cost users around \$8 million.

In October of the same year, BitKeep also experienced an exploit, during which the attacker took \$1 million worth of BNB through the service enabling token swaps (Reguerra, 2022).

3.3.1.3 Deribit, November 2022, \$28M Lost

On November 2, 2022, Deribit cryptocurrency options and futures exchange informed its community of the compromise of its hot wallets. Hackers managed to get access to the exchange's hot wallet and initiate withdrawals. The attack affected hot wallets for Bitcoin, Ethereum, and USDC. The company's officials noted that 99% of all funds were stored in cold storage, which is why the incident did not have catastrophic implications for the exchange (Knight, 2022).

3.3.1.4 Solana Wallet Hacks, August 2022, \$5M Lost

The attack affected nearly 8000 Solana digital wallets. The incident affected major Internet-connected "hot" wallets such as Phantom, Slope, and TrustWallet. The attack predominantly affected mobile wallet users. The attacker managed to sign transactions on users' behalf. The trusted third-party service might have been compromised through a supply-chain attack. The bug that was used by attackers was likely in the software that several software wallets used (Quarmby, 2022).

3.3.1.5 Profanity Wallets Hack, \$3.3M Lost

Throughout 2022, Profanity wallets might have experienced hacks due to the ambiguity in the creation of vanity addresses. Profanity is the tool allowing users to create "vanity addresses"—custom crypto wallets that have identifiable names or numbers within them. Security researchers found out that the generator seeded 256-bit private keys with a random 32-bit vector. Profanity seeded the cryptographic pseudorandom number generator with an unsigned integer, thereby leaving only 4.3 billion seed values possible. Although this figure is great, it is not sufficient to let crypto wallets withstand a brute-force attack. In this case, users should be aware of the importance of using reputable and still actively supported tools for private key generation. The original creators of the Profanity vulnerability address generator

abandoned the product multiple years ago, but, unfortunately, users still turn to this tool for private key generation (Emmanuel, 2022).

3.3.1.6 Binance Hot Wallet Hack, May 2019, \$40M Lost

In May 2019, hackers broke into the Binance exchange and stole 7000 bitcoins. One of the biggest cryptocurrency exchanges, Binance, later paid back the losses using the SAFU (Secure Asset Fund for Users), a separate fund set up to protect users' money in case of theft.

Combining phishing, malware, and other methods, the breach gave the attackers access to the private keys for Binance's hot wallet. Even though Binance tried hard to keep its platform safe, the hackers were able to pull off the heist (Doug Bonderud, 2019).

3.3.1.7 MetaMask iCloud Hack, July 2021

In July 2021, there was an event known as the MetaMask iCloud hack, during which a hacker gained access to a user's MetaMask seed phrase that was kept in their iCloud account. The user's Ethereum assets that were kept in the MetaMask wallet were now accessible to the hacker. The attack happened because the user did not protect their iCloud account and MetaMask seed phrase well enough.

Not a bug in the MetaMask software, but the user's failure to follow best practices for storing and protecting their seed phrase made this type of attack possible. To avoid situations like this one, you should always save your seed phrase in a safe place, avoid storing it on cloud-based services, and turn on two-factor authentication for all of your online accounts (Toulas, 2022).

3.3.1.8 Parity Multisig Hack, November 2017, \$30M Lost

In November 2017, there was a security breach called the Parity Wallet hack. About 153,000 ETH, which was worth about \$30 million at the time, were stolen from multi-sig wallets made with Parity Technologies' Ethereum client software. A weakness in the wallet contract code made it possible for the hacker to take over the contract owner of the wallet and make transactions from it. Users who were hurt by the incident lost a lot of money, and the incident made people worry about how safe smart contract systems are. In response to the event, Parity Technologies tried to pay the users who were hurt and make its products safer (Palladino, 2020).

3.3.2 The Impact of Cyberattacks on Blockchain Wallets

Because there are so many ways to attack blockchain wallets, the projects that make them have had to add more security measures. Following a series of hot wallet compromises, exchange wallets establish special insurance funds to immediately cover potential losses. At the same time, hot wallet hacks force crypto exchanges to hold the majority of the assets they manage in cold wallets.

Mobile wallet developers implement security protections such as limiting the wallet's functionality on jailbroken or rooted devices, limiting the device's lifecycle, and ceasing support for old devices.

Also, it is a common mistake to suggest that crypto wallet developers are the best experts in cryptography. Most of the time, they are just regular web, mobile, and desktop developers who know the basics of cryptography but are not experts in how it is used. That is why the companies that develop blockchain wallets invest heavily in the education of their employees to make them more advanced specialists in cryptography.

Early detection of bugs could be critical for crime prevention. As a result, blockchain wallet developers begin to pay more attention to communication with users about flaws they notice when using their wallets.

And, in general, using best practices for secure coding, like OWASP Secure Coding Practices, is the best way to protect their products from the most common types of attacks.

3.4 The Importance of Auditing a Wallet

3.4.1 Explanation of the Importance of Auditing a Wallet

The users' trust in crypto wallets primarily depends on their security. From the developers' perspective, the crypto wallet attack area is enormous, while attackers may need to apply just a single attack vector to reach their malicious targets. Regarding the rapid speed of crypto transactions, security flaws in crypto wallets allow attackers to drain money quickly without even allowing developers to notice the attack and respond appropriately. Also, public blockchains do not have support services that can revert transactions or anti-fraud systems to timely notify a user of the susceptibility of certain actions. That is why stopping an ongoing attack targeting crypto wallets does not always bring the desired outcomes and is likely to result in an ultimate failure. For crypto wallets, attack prevention is a reasonable strategy for developers. *The most effective way to stop attacks is to audit a wallet to find bugs and fix them before attackers can see them.*

The other important reason for blockchain wallet developers to turn to security testing is related to budgeting. Pushing security from the earliest stages prevents spending on fixing exploitation outcomes and dealing with reputation damage.

Investing in security from the start saves projects valuable time that would otherwise be spent recovering wallets after an attack.

Just putting information security controls in place is not enough. Professional auditors are the only ones who can check if defenses are set up correctly and if there are any vulnerabilities that have not been found yet. Security testing of crypto wallets shows their developers what components of their products may be subject to a cyberattack, as well as pointing out expected attack scenarios.

Professional auditors not only look at specific flaws but also assess their synergies. The purpose of auditing a wallet is to ensure the wallet's cryptographic confidentiality, integrity, and availability, as well as the cryptographic assets it stores and its private keys.

Depending on the type of wallet under test and its technical peculiarities, auditors identify specific attack vectors and advise on the measures to be taken to eliminate these threats or minimize their business impact on a project.

Overall, security testing gives users more faith in their crypto wallets by showing them that their assets are well protected and that there is no chance of unauthorized interference.

3.4.2 Overview of Different Types of Audit that Can Be Performed

Crypto wallet security testing has several main forms, depending on the technical peculiarities of the product to be audited:

Threat modeling and risk assessments: This form of testing identifies the threats affecting the wallet under audit that may arise from different sources such as the attacks by cybercriminals, insider attacks, etc. The purpose of this form of testing is to assess the threats depending on their likelihood and potential impact so that a project can set priorities for their proper management and mitigation.

Penetration testing: Emulation of attack methods done by hackers to get into the targeted crypto wallet to identify vulnerabilities and point out the measures to be taken by a project to fix these flaws.

Architecture review: Validation of the presence and viability of implemented security controls. The purpose of this form of testing is to highlight any possible security risks in the wallet's architecture.

Code review: Thorough analysis of the code quality to detect incorrect functions and any flaws in dependencies that would undermine wallet's security. A special focus during code review is made on signing transactions and key generation.

The complex blockchain wallet audit process also includes identity management audits, certification and authorization audits, node security reviews, session management checks, and cryptography security audits.

3.4.3 Different Tools to Audit Wallets

Auditing a blockchain wallet, which includes cryptographic-using browser add-ons, desktop applications, hardware, and more, is a difficult operation. *It's crucial to evaluate both the cryptography part and the application element while auditing a wallet.*

Depending on the type of wallet being utilized, the application side of the wallet will differ substantially. For instance, it is important to confirm that an extension does not have any communication flaws with the browser or the Internet at large while auditing a browser wallet. This can entail performing an HTTP response header security audit, an XSS security audit, and a third-party JS assessment. It may be crucial to look at the app cache security or permission detection while auditing a desktop wallet.

As hardware and software have been audited since the invention of computers, these audits are not specific to wallets. Combining these audits with the cryptography component makes auditing wallets complicated. *A wallet must meet a number of requirements in order to be considered secure, such as producing or receiving enough entropy while generating keys.* Ensuring that your system complies with NIST SP 800-90A is one approach to doing this. A cryptographic security audit is typically required for a wallet to be deemed secure.

Some of the instruments used to conduct a cryptographic security audit include the following:

CryptCheck: A program to evaluate the effectiveness of SSL/TLS setups, including those for ciphers and certificates.

SSL Labs: An online service called SSL Labs offers a thorough examination of SSL/TLS setups and certificates.

Qualys SSL Labs: A web-based application that offers a thorough study of SSL/TLS implementations.

OpenSSL: A popular open-source SSL/TLS implementation that has a number of tools for testing and debugging encryption setups.

References

- Academy, B. (2023, February 9). *Custodial vs. Non-custodial wallets: What's the difference?* Binance Academy. Retrieved from <https://academy.binance.com/en/articles/custodial-vs-non-custodial-wallets-what-s-the-difference>
- Antonopoulos, A. M. (2017). *Mastering bitcoin: Programming the open Blockchain*. O'Reilly Media.
- Antonopoulos, A. M., & Wood, G. (2021). *Mastering Ethereum: Building smart contracts and DApps: Building smart contracts and DApps*.
- B. (2019, March 12). *bips/bip-0044.mediawiki at master · bitcoin/bips*. GitHub. Retrieved from <https://github.com/bitcoin/bips/blob/master/bip-0044.mediawiki>
- B. (2020, December 20). *bips/bip-0039-wordlists.md at master · bitcoin/bips*. GitHub. Retrieved from <https://github.com/bitcoin/bips/blob/master/bip-0039/bip-0039-wordlists.md>

- B. (2022, January 3). *bips/bip-0032.mediawiki at master · bitcoin/bips*. GitHub. Retrieved from <https://github.com/bitcoin/bips/blob/master/bip-0032.mediawiki>
- Bonderud, D. (2019, May 15). *Binance hack steals \$41 million from 'hot wallet'*. Security Intelligence. Retrieved from <https://securityintelligence.com/news/binance-hack-steals-41-million-from-hot-wallet>
- Buterin, V. (2017, February 10). *EIPs/eip-86.md at master · ethereum/EIPs*. GitHub. Retrieved from <https://github.com/ethereum/EIPs/blob/master/EIPs/eip-86.md>
- Connor Sephton. (2023, January 16). "Violated": NFT god loses "life-changing" sum of Crypto after clicking on Malware Link. CoinMarketCap Alexandria. Retrieved from <https://coinmarketcap.com/alexandria/article/violated-nft-god-loses-life-changing-sum-of-crypto-after-clicking-on-malware-link>
- DeCommas. (2022, November 8) *Smart contract wallets explained*. Retrieved from <https://decommas.io/blog/smart-contract-wallets-explained>
- Emmanuel, O. O. (2022, September 26). *Hacker exploits profanity's vanity address to steal \$950 in ETH*. crypto.news. Retrieved from <https://crypto.news/hacker-exploits-profanitys-vanity-address-to-steal-950-in-eth/>
- Knight, O. (2022, November 2). *Crypto exchange Deribit loses \$28M in hot wallet hack, pauses withdrawals*. Retrieved from <https://www.coindesk.com/business/2022/11/02/crypto-exchange-deribit-loses-28m-in-hot-wallet-hack/>
- Niset, J. (2022, March 28). *Part I: WTF is account abstraction*. argent.xyz. Retrieved from <https://www.argent.xyz/blog/wtf-is-account-abstraction>
- Palladino, S. (2020, May 19). *The parity wallet hack explained*. OpenZeppelin Blog. Retrieved from <https://blog.openzeppelin.com/on-the-parity-wallet-multisig-hack-405a8c12e8f7>
- Pirus, B. (2020, September 6). *Electrum Bitcoin wallet still plagued by known crypto phishing attack*. Cointelegraph. Retrieved from <https://cointelegraph.com/news/electrum-bitcoin-wallet-still-plagued-by-known-crypto-phishing-attack>
- Portier, B., & Diya, C. (2023, January 25). *How confidential space and MPC can help secure digital assets*. Google Cloud Blog. Retrieved from <https://cloud.google.com/blog/products/identity-security/how-confidential-space-and-mpc-can-help-secure-digital-assets>.
- Potapenko, J., Hil, A., & Voitova, A. (2021, December 13). *Crypto wallets security as seen by security engineers*. Cossack Labs. Retrieved from <https://www.cossacklabs.com/blog/crypto-wallets-security>.
- Proposals, E. I. (2018, April 20). *EIP-1014: Skinny CREATE2*. Ethereum improvement proposals. Retrieved from <https://eips.ethereum.org/EIPS/eip-1014>
- Proposals, E. I. (2020a, September 4). *EIP-2938: Account abstraction [DRAFT]*. Ethereum improvement proposals. Retrieved from <https://eips.ethereum.org/EIPS/eip-2938>
- Proposals, E. I. (2020b, October 15). *EIP-3074: AUTH and AUTHCALL opcodes [DRAFT]*. Ethereum Improvement proposals. Retrieved from <https://eips.ethereum.org/EIPS/eip-3074>
- Proposals, E. I. (2021, September 29). *ERC-4337: Account abstraction using Alt Mempool [DRAFT]*. Ethereum Improvement Proposals. Retrieved from <https://eips.ethereum.org/EIPS/eip-4337>
- Quarmby, B. (2022, August 3). *Solana-based wallet hack saw millions drained*. Cointelegraph. Retrieved from <https://cointelegraph.com/news/ongoing-solana-based-wallet-hack-has-already-seen-millions-drained>.
- Reguerra, E. (2022, December 26). *Hackers drain \$8M in assets from Bitkeep wallets in latest DeFi exploit*. Cointelegraph. Retrieved from <https://cointelegraph.com/news/hackers-drain-8m-in-assets-from-bitkeep-wallets-in-latest-defi-exploit>
- Sharma, T. K. (2023, January 25). *Types of crypto wallets explained*. Blockchain Council. Retrieved from <https://www.blockchain-council.org/blockchain/types-of-crypto-wallets-explained/>.
- Team, P. (2023, March 28). *Ethereum account abstraction: Everything you need to know!* Panther Protocol Blog. Retrieved from <https://blog.pantherprotocol.io/ethereum-account-abstraction-everything-you-need-to-know>

- Toulas, B. (2022, April 18). *Hackers steal \$655K after picking MetaMask seed from iCloud backup*. BleepingComputer. Retrieved from <https://www.bleepingcomputer.com/news/security/hackers-steal-655k-after-picking-metamask-seed-from-icloud-backup>
- Wikipedia contributors. (2023, March 27). *Secure multi-party computation*. Wikipedia. Retrieved from https://en.wikipedia.org/wiki/Secure_multi-party_computation.
- ZenGo. (2023, March 30). *MPC wallet - What is MPC? - ZenGo*. Retrieved from <https://zengo.com/mpc-wallet>
- Zetter, K. (2022, January 24). *Cracking a \$2 million crypto wallet*. The Verge. Retrieved from <https://www.theverge.com/2022/1/24/22898712/crypto-hardware-wallet-hacking-lost-bitcoin-ethereum-nft>

Chapter 4

Smart Contract Security



Carlo Parisi and Dyma Budorin

4.1 Introduction

Over time, the term “smart contract” has come to encompass a variety of concepts. Nick Szabo coined the term in the 1990s, and its original definition was:

A smart contract is a set of promises, specified in digital form, including protocols within which the parties perform on these promises (FutureLearn, 2022).

Today, however, *smart contracts are computer programs that run in the context of a blockchain and that are immutable and deterministic*, meaning that they cannot be modified once deployed and their outcomes are identical for all users, given the transaction context and the state of the blockchain. Contrary to their name, smart contracts are not legally binding, and their access is restricted to their own state, the transaction context, block information, and a few other key primitives.

There are numerous applications for smart contracts, ranging from simple agreements between individuals to more complex agreements between businesses or organizations. They can be used to automate a variety of processes, including payment settlements, supply chain management, and digital identity verification.

4.1.1 Definition of Smart Contracts in the Context of Web3 Applications

Smart contracts are essential to the development of decentralized applications (dApps) and are one of the key elements that enable the Web3 ecosystem to function in a transparent, decentralized, and trustless manner.

C. Parisi (✉) · D. Budorin
Hacken, Lisbon, Portugal

The ability of smart contracts to automate the execution of contractual agreements between parties is one of their primary advantages. *This automation eliminates the need for intermediaries and other third parties*, thereby decreasing transaction costs and boosting efficiency.

Additionally, smart contracts enable a high level of transparency and confidence in the Web3 ecosystem. It is impossible for any party to alter or manipulate the transaction history due to the fact that smart contract transactions are visible to all blockchain participants. The blockchain's transparency and immutability foster a high level of trust between parties, allowing them to conduct transactions without the need for intermediaries.

Smart contracts play a crucial role in the Web3 ecosystem, as they enable a variety of decentralized applications and promote trust and transparency between parties. As Web3 technology adoption continues to increase, it is likely that smart contracts will become even more crucial for enabling a decentralized and trustless economy.

Smart contracts are the backbone of Web3 technology, and rightly so. When a user interacts with a decentralized application, they are most likely interacting with a trustless, decentralized, and transparent smart contract.

Nevertheless, it is crucial to interact with secure smart contracts. As explained in greater detail later in this chapter, interacting with insecure smart contracts could result in the loss of funds. Given that smart contracts are immutable and operate in a decentralized manner, it is crucial to ensure the contract's security prior to interacting with it.

Smart contracts enable the development of decentralized applications and facilitate peer-to-peer transactions, making them an essential component of Web3 technology. However, caution and diligence must be exercised when interacting with smart contracts to avoid potential security risks.

4.2 Smart Contract Security Checklist

This section looks at a few typical problems with smart contracts. While some blockchain architectures may have greater relevance for these challenges than others, this list is supposed to be generic in nature. A large number of these flaws result from constraints in the Ethereum Virtual Machine (EVM) design and the long-established and widely used programming language Solidity.

This is a selection of some of the most well-known vulnerabilities that have been identified up to this point, rather than a comprehensive list of flaws to check for.

4.2.1 Gas Optimization

With gas serving as the unit of measurement for the amount of computational work necessary to do particular operations, gas optimization is the process of lowering the cost of running your smart contract code on the Ethereum network. *Gas is the cost that each Ethereum transaction needs to pay.*

Smart contracts can be made more economical and effective overall by being optimized for gas usage. Gas costs can fluctuate owing to network congestion and other causes; therefore, it is crucial to optimize for gas to guarantee that smart contracts stay cost-effective even as market conditions change.

Avoiding pointless computations and storage operations, using more effective data types, minimizing external function calls, reusing code with modifiers, and emitting information to the outside world with events rather than returning values from functions are a few things to keep in mind when optimizing for gas.

4.2.2 Compiler Version

It can be problematic to use an old compiler version, especially if the current compiler version has bugs and problems that have been made public (SWC-102 · Overview, [n.d.](#)).

4.2.3 Access Control

Some smart contract architectures that include the implementation of security measures like authentication, authorization, and accountability include access control as a key component. Any of these mechanisms can cause security breaches where attackers can take advantage of privileged access, get access to private data, issue illegal instructions, or avoid detection if they are not implemented or used properly.

Specification and enforcement are two distinct activities that might lead to access control flaws. When specifications are used, the user or the resource may have inappropriate privileges, permissions, ownership, or other access control needs that are clearly declared.

When the access control system has flaws that prevent it from correctly enforcing the given access control requirements, enforcement weaknesses exist. Enabling users to define their own privileges, for instance (CWE - CWE-284: Improper Access Control, [n.d.](#)).

4.2.4 *Check Effect Interaction*

The DAO hack, *which caused the hard fork and chain split between Ethereum and Ethereum Classic*, is likely the most well-known hack in the Ethereum community. The vulnerability in the DAO smart contract is now known as the “reentrancy attack,” and it is one of the most well-known and actively searched for vulnerabilities in smart contracts.

The check effect interaction design makes sure that all internal state changes are made before an external call to another contract is made in an effort to prevent falling victim to that vulnerability (SWC-107 · Overview, [n.d.](#)) (Fig. 4.1).

4.2.5 *SELFDESTRUCT Instruction*

Another well-known example of a flaw in the Ethereum community is the Parity Multisig contract problem. The contract had a function allowing a user with the name of “devops199” to destroy the multisig’s code, thereby rendering any money trapped inside the contract unavailable forever (ghost, [n.d.](#)).

The “I accidentally killed it” bug, as this flaw has come to be known, emphasizes the significance of *avoiding the usage of self-destruct functionality unless absolutely essential*. It is advised to design a multisig scheme so that several parties must approve the self-destruct action if there is a legitimate use case for it (SWC-106 · Overview, [n.d.](#); Wilmoth, [2021](#)) (Fig. 4.2).

4.2.6 *Denial of Service*

A Denial of Service can generally be brought on by any circumstance that could prevent a transaction from being executed. For example, external calls can fail accidentally or deliberately, and a certain quantity of gas is always required for the

Fig. 4.1 Reentrancy attack

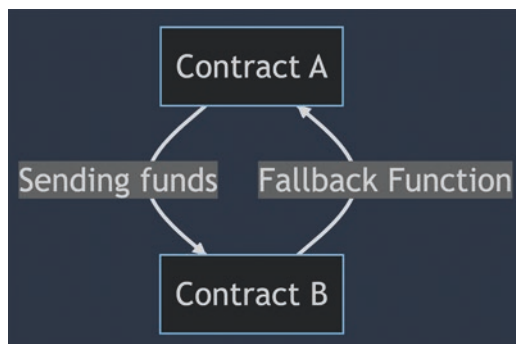




Fig. 4.2 I accidentally killed it announcement

execution of smart contract deployments and function calls within them, depending on the amount of computation involved. *The total gas used by the transactions contained in a block cannot go over the block gas limit set by the Ethereum network.*

When the cost of executing a function exceeds the block gas limit, programming patterns that are safe in centralized apps can cause Denial of Service problems in smart contracts. A Denial of Service situation like this can result from changing an array whose size is unknown and which grows over time (SWC-113 · Overview, [n.d.](#); SWC-128 · Overview, [n.d.](#)).

4.2.7 *Deprecated Functions*

There could be some deprecated functions and operators. They result in lower code quality when used. Deprecated operators and functions could have unintended consequences and compiler issues (SWC-111 · Overview, [n.d.](#)).

4.2.8 *Race Conditions*

A race-condition vulnerability occurs when code depends on the order of the transactions submitted to it.

One of the most obvious examples of a race condition is with swaps in decentralized exchanges. The transaction for the swap would be public and visible in the mempool, and an attacker could pay more gas to get his transaction included before the swap for the first user and change the outcome of the swap for that user (SWC-114 · Overview, [n.d.](#)).

4.2.9 Signature Unique ID

Because of the flexibility and improved transferability that this offers, smart contract systems frequently permit users to sign messages off-chain rather than requesting them to perform an on-chain transaction. Smart contract systems that process signed messages must build their own logic to determine the signed messages' authenticity before continuing to process them.

A secure implementation needs to protect against Signature Replay Attacks by, for example, keeping track of all processed message hashes and only allowing new message hashes to be processed. A malicious user could attack a contract without such a control, get a message hash that was sent by another user, and replay the message multiple times (SWC-117 · Overview, [n.d.](#); SWC-121 · Overview, [n.d.](#); SWC-122 · Overview, [n.d.](#); Proposals, [2017](#); Vitalik Buterin, [n.d.](#)).

4.2.10 Weak Source of Randomness

In a wide range of applications, having the ability to create random numbers is quite useful. Gambling DApps, which choose the winner using a pseudo-random number generator, are one clear example. In deterministic blockchains, it might be exceedingly difficult to generate a reliable source of randomness. For instance, using block.timestamp in Ethereum is insecure since a miner can choose to use any timestamp over a short period of time and still have his block accepted by others. As the miner controls blockhash, block.difficulty, and other fields, their use is equally risky. If the stakes are high, the miner can quickly mine a large number of blocks using rental hardware, choose the block with the requisite block hash, and dump all other blocks (SWC-120 · Overview [n.d.](#); MIT School of Engineering, [n.d.](#)).

The use of Oracles is one of the most popular solutions for this.

4.2.11 Assets Integrity and User Balance Manipulation

Smart contracts that hold user assets should not allow for the possibility of wrongfully withdrawing or manipulating users' funds.

4.2.12 *Secure Oracle Usage*

Oracles are applications that gather, validate, and send external data—that is, data kept off the blockchain—to smart contracts that are active on the blockchain. Oracles can “push” data from the blockchain to external systems in addition to “grabbing” off-chain data and broadcasting it on Ethereum.

Oracles serve as a “bridge” to link off-chain data providers with smart contracts on blockchains. Applications for smart contracts would only be allowed to access on-chain data in the absence of oracles. The use of off-chain data to activate smart contract features is made possible by an oracle.

The data source, single or numerous sources, trust mechanism, centralized or decentralized, and system design are three factors that distinguish different Oracles. We can also distinguish between oracles based on how they conduct computational activities off-chain, convey data from the blockchain to off-chain apps, or retrieve external data for use by on-chain contracts.

Because of the nature of oracles, it is important to use them correctly and have trust in them (Ethereum, 2023).

4.2.13 *Flash Loans*

A flash loan attack on smart contracts is a sort of exploit where an attacker takes advantage of the ability to borrow a sizable sum of money from a decentralized finance (DeFi) platform for one transaction. In order to their advantage, the attacker manipulates the price of an asset on a decentralized exchange or other DeFi protocol using borrowed money. The attacker repays the flash loan after the price manipulation is done and keeps the money earned.

Due to the DeFi protocols’ composability, which enables intricate interactions between several smart contracts, flash loan attacks are possible. Flash loans can be used to carry out sophisticated attacks that take advantage of DeFi’s interconnectedness, even though they are not intrinsically harmful in and of themselves.

When working with exchange rates, it is important to ensure that they are obtained from a reliable source and are not susceptible to sudden fluctuations in exchange rates that can be made possible by using flash loans. The use of oracles is advised.

4.2.14 Style Guide and Readability

While not a critical vulnerability, it is still essential to adhere to a style guide when writing code to improve its readability. Code that is too complex can be difficult to comprehend and audit, potentially resulting in undiscovered vulnerabilities for an extended period of time.

4.2.15 Requirements Compliance

Although the code itself might not be vulnerable, designing a smart contract in a specific way may prevent it from meeting desirable functional and technical requirements. Even if they are not intrinsically malevolent, disobeying these requirements could result in missing functionality or unexpected behaviors.

4.2.16 Importance of Following the Checklist to Ensure Smart Contract Security

This checklist looks at some of the most common programming mistakes made when creating smart contracts and offers fixes for some of them. *Since known vulnerabilities will be the main focus of hostile actors, avoiding them is essential.* While developing a smart contract, having a checklist of recommended practices and hazards to watch out for is quite helpful.

4.3 Top Security Vulnerabilities in Smart Contracts

4.3.1 Flash Loans

As long as the borrowed amount plus a fee is paid back before the transaction's end, flash loans are unique transactions that permit the borrowing of an asset. Users are not required to provide collateral for these transactions in order to proceed. Flash loans have no counterpart in the real world, so understanding how state is controlled within blocks in blockchains is a prerequisite.

The steps for a flash loan are as follows:

1. The borrower executes a smart contract for a flash loan
2. A flash loan contract asks the liquidity pool for the loan amount
3. The loan funds are subsequently used by the contract to carry out specified operations (e.g., trading on an exchange)

4. The borrowed money is repaid to the liquidity pool once operations are finished
5. The transaction is committed to the blockchain

Smart contracts provide us with the ability to verify that:

1. The necessary funds are present in the smart contract to carry out the flash loan's operations
2. Before the transaction is added to a new block, the loan is given and repaid
3. The operations do not cause the borrower to lose money, he just pays a fee on top of the amount received
4. The right amount owed to the lending pool is returned together with a transaction fee for using the protocol
5. As long as the lender is reimbursed for the exact amount lent, the borrower is free to do anything they choose with the money

The most common operation with flash loans is arbitrage, which is moving a token from one exchange to another with a higher value in order to benefit.

A flash loan contract must be funded before it can be executed.

The use of a flash loan as a financial tool is not inherently malevolent. However, due to the high composability of smart contracts, flash loans can become a potential source of malevolent attacks if developers fail to consider such possibilities. In the past, flash loans have been one of the most widely used methods of attack in the DeFi space (Seher Saylik, 2023).

Let us see some examples:

PancakeBunny: In this instance, the attacker used price manipulation to launch their attack on both USDT/BNB and BUNNY/BNB. Unlike many other BSC MasterChef-like farms, BUNNY had a special supply mechanism: It took 30% of the profit from the farming pools as a performance fee and redistributed them to the BUNNY Staking pool.

This meant that the attacker acquired more tokens than they “should” have when extracting value or exchanging BUNNY for BNB. As a result, the attacker had 114,631 WBNB left over after paying back the flash loan, which represents the profit from the attack (WatchPug, 2022; Behnke, n.d.-a).

Platypus Finance: This is a more complex scenario in which not only were flash loans used, but also an improper check within the smart contract enabled the \$9 million attack.

According to the blockchain data, the exploiter borrowed over \$44 million from the lending platform Aave for the flash loan, utilizing it to offer liquidity to a trading pool on Platypus and fooling smart contracts into issuing \$44 million of Platypus' LP token, LP-USDC, in return.

This occurred during the course of two transactions. These LP tokens were subsequently transferred into a Platypus staking contract, which issued 11,000 platypus (PTP) tokens as a staking payout.

As Platypus allows users to borrow USP stablecoins against their LP positions, the attacker was also able to obtain 41 million USP tokens using \$44 million in LP tokens as collateral.

At this time, the attacker invoked the “emergencywithdraw” function on Platypus’ smart contracts in order to withdraw the \$44 million that had been initially deposited into the Platypus liquidity pool. The mistake in the code’s solvency check failed to prevent this action, allowing the attacker to withdraw tokens and repay the AAVE flash loan.

Unfortunately, the system did not revoke the 41 million USP tokens that were issued, allowing the attacker to exchange them for the \$8.5 million in liquidity on Platypus at the moment.

Beanstalk: Two malicious Beanstalk proposals carried out the Beanstalk attack. Beanstalk Proposals #18 and #19 emptied the Beanstalk smart contract and delivered the stolen tokens to the address of the attacker as well as the Ukrainian contribution address.

For the proposals to be approved, the attacker has to control two-thirds of the votes for the governance protocol. Nevertheless, voting power is decided by donations to the Diamond contract of the Beanstalk protocol.

After the one-day waiting period, the attacker was able to make a substantial deposit to the Diamond contract using a flash loan. This allowed them to control 79% of the votes for the governance protocol, which is significantly more than the 2/3 required to pass the proposal. With this ability, the attacker might approve their request unilaterally via emergencyCommit.

The value contained in the Beanstalk protocol was distributed to the Ukrainian fund and the attacker, who utilized it to repay their flash loan once the fraudulent proposal was implemented. The perpetrator made a profit of \$76 million from the \$181 million stolen (Rekt - Beanstalk – REKT, 2022) (Fig. 4.3).

```

Hacker 0xc5dcd006ea787e4783f9e6021c32935a10fb4
Hacker Contract 0x79224bc0bf70ec34f0ef56ed8251619499a59def
BIP18 0xe5ecf73603d98a0128f05ed30506ac7a663dbb69

Propose BIP18 tx: 0x68cdec0ac76454c3b0f7af0b8a3895db00adf6daaf3b50a99716858c4fa54c6f
1. Hacker proposes a malicious proposal BIP with initAddress @ 0xe5ecf73603d98a0128f05ed30506ac7a663dbb69

Launch the hack tx: 0xd314668aaa9bbf8eaf1a0bd2b6553d01dd58899c508d4729fa7311dc5d33ad7
1. Flashloan 350,000,000 DAI, 500,000,000 USDC, 150,000,000 USDC, 32,425,202 BEAN, and 11,643,065 LUSD
2. Vyper_contract_bebc.add_liquidity 350,000,000 DAI, 500,000,000 USDC, 150,000,000 USDT to get 979,691,328 3Crv
3. LUSD3CRV-f.exchange to convert 15,000,000 3Crv to 15,251,318 LUSD
4. BEAN3CRV-f.add_liquidity to convert 964,691,328 3Crv to 795,425,740 BEAN3CRV-f
5. BEANLUSD-f.add_liquidity to convert 32,100,950 BEAN and 26,894,383 LUSD and get 58,924,887 BEANLUSD-f
6. Deposit 795,425,740 BEAN3CRV-f and 58,924,887 BEANLUSD-f into Diamond
7. Diamond.vote bip=18)
8. Diamond.emergencyCommit bip=18) and hacker proposed _init contract is excuted to get 36,084,584 BEAN and 0.54 UNI-V2_WETH_BEAN,
874,663,982 BEAN3CRV-f, 60,562,844 BEANLUSD-f to hacker contract
9. BEAN3CRV-f.remove_liquidity_one_coin 874,663,982 BEAN3CRV-f to get 1,007,734,729 3Crv
10. BEANLUSD-f.remove_liquidity_one_coin 60,562,844 BEANLUSD-f to get 28,149,504 LUSD
11. Flashloan back LUSD 11,795,706 and BEAN 32,197,543
12. LUSD3CRV-f.exchange to swap 16,471,404 LUSD to 16,184,690 3Crv
13. Burn 16,184,690 3Crv to get 522,487,380 USDC, 365,758,059 DAI, and 156,732,232 USDT
14. Flashloan back 150,135,000 USDT, 500,450,000 USDC, 350,315,000 DAI
15. Burn UNI-V2_WETH_BEAN 0.54 to get 10,883 WETH and 32,511,085 BEAN
16. Donate 250,000 USDC to Ukraine Crypto Donation
17. swap 15,443,059 DAI to 15,441,256 USDC
18. swap 37,228,637 USDC to 11,822 WETH
19. swap 6,597,232 USDT to 2,124 WETH
20. Profit 24,830 WETH is sent to hacker

```

Fig. 4.3 Beanstalk hack flow

4.3.2 *Front Running*

Front-running attacks fall under the category of Race Conditions attacks and are one of the most prevalent types of attacks.

When a transaction is submitted to the blockchain, it is broadcast to the mempool and waits to be included in the following block. To construct the next block, miners are searching the mempool. As they are incentivized to do so, they often include the transactions with the highest fees first in the following block. Observers of the network can view and replicate a transaction before it is included in the next block. This is called “front running.”

In general, a front-running attack happens when a valuable transaction that depends on the order of arrival is broadcast to the public mempool (SWC-114 · Overview, [n.d.](#)).

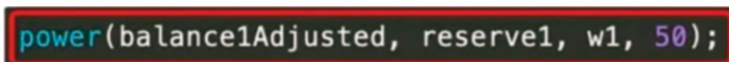
This attack became widespread with Flashbots and the introduction of MEV (Miner Extractable Value), Flashbots created a market for front-runners to collect transactions that they wanted to race and pay miners.

4.3.3 *DoS*

Defining a denial of service attack can be a challenging task as it can come across as too general. Such an attack typically hinges on the terms of a contract and occurs when a critical contract operation results in an unintended and disruptive halt.

An instance that exemplifies this is the “I accidentally killed it” bug found in the parity multisig smart contract. Due to uninitialized functions, the user “devops199” was able to gain access to the contract “0x863df6bfa4469f3ead0be8f9f2aae51c91a907b4” and carry out a SELFDESTRUCT operation, effectively terminating the contract (Wilmoth, [2021](#)).

This incident exposed several vulnerabilities, notably: funds lock, as all funds held in the parity multisig were inaccessible; access control violation, as an unauthorized user was able to take ownership of the contract; and denial of service, as the contract’s main function became inoperable once the contract was terminated (SWC-113 · Overview, [n.d.](#); SWC-128 · Overview, [n.d.](#); CWE - CWE-284: Improper Access Control, [n.d.](#)).



```
power(balance1Adjusted, reserve1, w1, 50);
```

Fig. 4.4 Invalid calculation in ValueDefi vSwap contract

4.3.4 Invalid Calculations

It can be difficult to define this vulnerability without using overly general examples. It depends primarily on the contract’s specifics and operations (SWC-101 · Overview, n.d.).

This vulnerability manifests itself when a mathematical operation yields a result that is inconsistent with the intended outcome. A recent example is the 2021 ValueDeFi vSwap contract exploit, in which approximately \$11M was lost due to the improper use of a complex exponentiation function power() in the calculation and enforcement of the weighted constant product invariant (Fig. 4.4).

An important consideration when utilizing this same power() function is that it assumes baseN must always be greater than or equal to baseD. In the ValueDeFi vSwap contract exploit, the swap() function of the pool was called with an input that violated this assumption. The consequent circumvention of the weighted constant product invariant led to the depletion of pool funds (PeckShield, 2022).

4.3.5 Token Supply Manipulation

Tokens are among the most commonly used smart contracts, with different types that may follow the ERC-20, ERC-721, ERC-1155 standards, or none at all. An essential feature of tokens is their supply, or the amount of tokens in circulation, which can range from zero to a very large number. The creators and deployers of the token should determine the logic for the supply, which must be enforced by the smart contract governing the token. Although the logic for creating and deleting the token supply may be complex in some instances, it should adhere to the specifications outlined by the smart contract deployers.

Token supply manipulation occurs when the determined logic for token supply is not followed or enforced by the smart contract governing the token.

The 2022 hack of the \$aBNBc token contract in the Ankr protocol provides a notable instance of token supply manipulation. The aBNBc token had an unlimited mint bug, whereby the mint() function was protected with onlyMinter modifier, but there was another function (with the 0x3b3a5522 function signature) that bypassed caller verification and allowed arbitrary minting (Fig. 4.5).

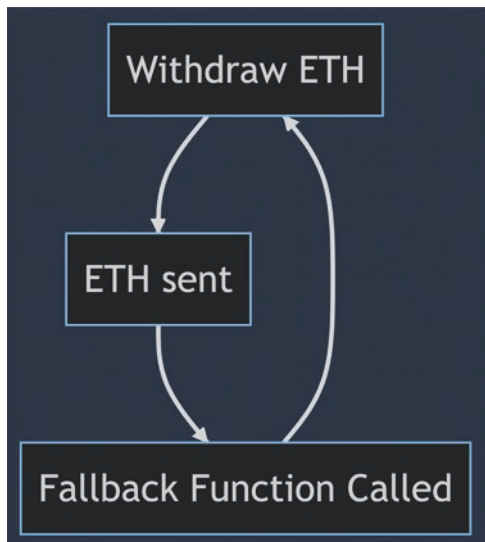


Fig. 4.5 Ankr protocol hack transaction

Input Accounts	#1 - Account0 - CxegPrfn2ge5dNiQberUrQJkHCcimeR4VXkeawcFBBka
	#2 - Account1 - ywSj8KSWAXavP8bCgjCgaLGWt4UBTF4bLBSksTzFJ3B
	#3 - Account2 - EtMw1nQ4AQaH53RjYz3pRk12rrqWjcYjPDEtPhYJzmCX
	#4 - Account3 - 2tHS1cXX2h1KBEaadprqELJ6sV9wLoaSdX68FqsrrZRd
	#5 - Account4 - Rent Program
	#6 - Account5 - 11

Fig. 4.7 Normal wormhole transaction

Fig. 4.8 Reentrancy Attack flow



4.3.7 Reentrancy Attack

The reentrancy attack has had a significant impact on the cryptocurrency landscape, resulting in numerous hacks, including the infamous 2016 DAO hack. This type of attack occurs when a contract makes an external call to an untrusted address without first modifying its state. The untrusted contract can then recursively invoke the reentrant function. For example, a withdraw function that sends ETH prior to updating the user’s balance can be exploitable if the recipient’s address is a contract with a fallback function that calls the withdraw function (Polak, 2022) (Fig. 4.8).

Utilizing a programming pattern known as the Check Effect Interaction pattern or implementing a mechanism to detect a reentrancy attack can mitigate the reentrancy attack. Public contracts, such as OpenZeppelin’s ReentrancyGuard contract, are available to help detect such attacks (SWC-107 · Overview, n.d.).

Consider a few examples to comprehend the potential of this attack’s power:

Fig. 4.9 The DAO Hack

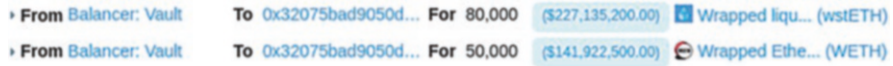
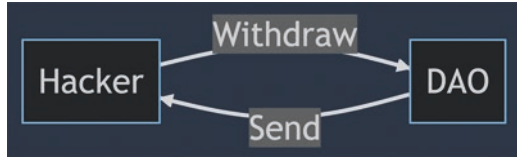


Fig. 4.10 Rari Capital Hack first borrow from Balancer

The DAO: The hacker deployed a smart contract that acted as a “investor” and then deposited ETH into The DAO. This allowed the hacker to later invoke The DAO’s smart contract’s `withdraw()` function. The DAO’s contract sent ETH to the hacker upon invoking the `withdraw()` function. However, the hacker’s smart contract omitted the `receive()` function on purpose, triggering the fallback function instead.

The fallback function, which contained malicious code, immediately re-invoked The DAO’s `withdraw()` function, initiating a loop. At this time, the first call to `withdraw()` was still executing, and it would not finish until the hacker contract’s fallback function completed executing. However, rather than concluding execution, the fallback function re-called `withdraw()`, resulting in a cycle of calls between the hacker contract and The DAO’s smart contract (Pratap, 2022) (Fig. 4.9).

Rari Capital: The attacker borrowed 50,000 WETH and 80,000 WSTETH from the Balancer vault using a flash loan. They then deposited 80,000 WSTETH into the fWSTETH-146 pool as collateral (Fig. 4.10).

Following the deposit, the attacker borrowed 2397 ETH from the fWSTETH-146 pool without updating the borrower’s record (Fig. 4.11).

The pool triggered the fallback function of the exploiter contract and sent ether to the exploit contract, at which point the attacker made a reentrant call to `exitMarket()` and withdrew 80,000 WSTETH (Fig. 4.12).

The attacker gained 2397 ETH for free and transferred it to a different address (Fig. 4.13).

The attacker repeated this procedure until, eventually, he escaped with a profit of approximately \$79 million (Abdul Sami, 2022).

4.3.8 Access Control Violation

Access control is a method used to regulate the authority of individuals within a contract to perform specific actions. Typically, these actions are essential to the safety and stability of the protocol, such as issuing new tokens, halting transfers and withdrawals, and implementing upgrades.

```

/*
 * We invoke doTransferOut for the borrower and the borrowAmount.
 * Note: The cToken must handle variations between ERC-20 and ETH underlying.
 * On success, the cToken borrowAmount less of cash.
 * doTransferOut reverts if anything goes wrong, since we can't be sure if side effects occurred.
 */
doTransferOut(borrower, borrowAmount);

/* We write the previously calculated values into storage */
accountBorrows[borrower].principal = vars.accountBorrowsNew;
accountBorrows[borrower].interestIndex = borrowIndex;
totalBorrows = vars.totalBorrowsNew;

```

Fig. 4.11 Part of the Rari Capital contract

```

function doTransferOut(address payable to, uint amount) internal {
  // Send the Ether and revert on failure
  (bool success, ) = to.call.value(amount)("");
  require(success, "doTransferOut failed");
}

```

Fig. 4.12 doTransferOut() function from the Rari Capital hacked contract

The significance of access control lies in its ability to prevent malicious parties from abusing vital contract functions. This is achieved by granting activation privileges for specific operations to designated accounts and implementing safeguards to prevent unauthorized parties from initiating restricted operations (CWE - CWE-284: Improper Access Control, n.d.).

Let us analyze an example to understand how tricky access control management can be. Mismanagement of access rights in two significant Polynetwork smart contracts, EthCrossChainManager and EthCrossChainData, led to a breach. EthCrossChainData is a highly privileged contract to which only its owners should have access. It maintains a list of the public keys of the “authenticator nodes” (keepers) that control the wallets in the underlying liquidity chains. EthCrossChainData determines who has permission to transfer large amounts of funds from Poly’s Binance wallet, Ethereum wallet, and other wallets. If an attacker had access to the correct EthCrossChainData function putCurEpochConPubKeyBytes(), they could replace a keeper’s public key with their own, allowing them to execute a high-volume transaction on the Poly network and move large sums to other wallets. This poses a serious security risk.

EthCrossChainManager is a second contract with high privileges that permits messages to be sent from another chain to the Poly chain. Anyone can call a cross-chain event by invoking the verifyHeaderAndExecuteTx() function of EthCrossChainManager and passing a Poly contract to execute as the target. However, EthCrossChainManager only calls a function with a unique “Solidity function ID” calculated by truncating to 32 bits a 256-bit Keccak hash of the string _method and a suffix. The attacker took advantage of two vulnerabilities: EthCrossChainManager is the owner of EthCrossChainData and can execute privileged functions within it, and the user-defined _method field can be used to brute-force the 32-bit value for putCurEpochConPubKeyBytes.

```
└ TRANSFER 2,392.401126398370465747 Ether From 0xfbd8aaf46ab3c2732fa930e5b... To → 0xd7f7d5c97ee01c80aa9c0ead...
└ TRANSFER 2,392.401126398370465747 Ether From 0xd7f7d5c97ee01c80aa9c0ead... To → 0x32075bad9050d4767018084f...
└ TRANSFER 50,000 Ether From Wrapped Et... To → 0x32075bad9050d4767018084f...
└ TRANSFER 50,000 Ether From 0x32075bad9050d4767018084f... To → 0xfbd8aaf46ab3c2732fa930e5b...
└ TRANSFER 50,000 Ether From 0xfbd8aaf46ab3c2732fa930e5b... To → 0x2ec06417378bdad8cf21a91d...
└ TRANSFER 50,000 Ether From 0x2ec06417378bdad8cf21a91d... To → 0x32075bad9050d4767018084f...
└ TRANSFER 50,000 Ether From 0x32075bad9050d4767018084f... To → Wrapped Et...
└ TRANSFER 2,392.301126398370465747 Ether From 0x32075bad9050d4767018084f... To → 0xe39f3c40966df56c69aa508d...
```

Fig. 4.13 Transaction from the Rari Capital Hack



Fig. 4.14 PolyNetwork hack flow

The attacker first calculated a 32-bit ID for `putCurEpochConPubKeyBytes()` and then brute-forced a string that would produce the same ID. Then, they invoked a cross-chain transaction from Ethereum to Poly by addressing `EthCrossChainData` and passing their own Ethereum wallet’s public key as a parameter. This prompted `EthCrossChainManager` to invoke the `putCurEpochConPubKeyBytes()` function in `EthCrossChainData` and register the attacker’s public key as a Keeper. With this status, the attacker transferred tokens from Poly’s Ethereum wallet to their own wallet using the corresponding secret key (Gagliardoni, 2021; Oleh Malanii, 2023) (Fig. 4.14).

4.3.9 Replay Attacks

A signed replay attack in a smart contract is a type of security vulnerability in which an attacker intercepts a validly signed message and then later replays it to the contract. The message is typically signed with a private key and contains executable instructions for the smart contract. By replaying the message, an attacker can trick the smart contract into executing the same instructions again, which can result in undesirable behavior or even financial loss.

Consider, for instance, a smart contract that enables users to withdraw funds from their account by submitting an authorized, signed message. An attacker could intercept a valid withdrawal message from a legitimate user and then replay that message later. Even though the context has changed, the smart contract would assume that the signed message is still valid because it has been digitally signed. This could allow the attacker to withdraw funds from the user’s account.

To prevent signed replay attacks, developers of smart contracts can implement various security measures, including the use of unique message IDs and the addition

of time-based restrictions to the validity of signed messages (SWC-117 · Overview, [n.d.](#); SWC-121 · Overview, [n.d.](#); SWC-122 · Overview, [n.d.](#); Proposals, 2017; Vitalik Buterin, [n.d.](#)).

4.3.10 *Weak Source of Randomness*

Due to the deterministic nature of the system, it is impossible to generate truly random numbers in the context of the blockchain.

The emphasis on determinism is required because it ensures that the smart contract code returns the same result regardless of where it is executed.

A weak source of randomness in a smart contract is one that enables an attacker to predict or manipulate the results of the contract's operations. Some smart contracts frequently rely on random values to make crucial decisions, such as choosing a lottery winner or assigning tasks to participants in a decentralized system.

An attacker can manipulate the outcome of a contract if the source of randomness is not truly random or is easily predictable. For instance, an attacker may be able to generate a large number of contract interactions in a short amount of time by exploiting the predictable nature of the randomness to increase their odds of winning a lottery or being selected for a task.

This can result in unfair outcomes and undermine confidence in the contract and blockchain system underlying them. To avoid these vulnerabilities, it is essential that smart contracts utilize robust and at least pseudo-random sources, such as trusted external oracles (SWC-120 · Overview, [n.d.](#); MIT School of Engineering, [n.d.](#)).

4.3.11 *Incorrect Oracle Usage*

In blockchains, “incorrect oracle usage” refers to a situation in which an oracle is misused, resulting in the injection of inaccurate or malicious data. An oracle is a trusted third-party service that supplies external data to a blockchain-based smart contract. Inappropriate use of oracles can result in a variety of issues, including improper execution of smart contracts, security flaws, and financial losses for users (Ethereum, 2023).

Incorrect oracle usage occurs when an oracle is not properly authenticated or verified, resulting in the smart contract receiving inaccurate or manipulated data. Another instance is when a smart contract relies on a single oracle source, leading to a single point of failure and vulnerability to manipulation. In addition, an oracle may be incentivized to provide false data to the blockchain, either as a result of a malicious attack or a design flaw.

To avoid incorrect oracle usage, it is essential to carefully design and verify the oracle service, as well as to use multiple, independent oracle sources to supply the blockchain with data. In addition, it is essential to properly authenticate and verify

the oracle sources and implement security measures to prevent malicious data from being added to the blockchain.

Due to the protocol's inadequate handling of slippage checks for leveraged trading, which relied on a single oracle to determine asset prices, Vee Finance was compromised. This is a common error in DeFi that is exploited by adversaries to manipulate pricing information.

In this instance, the attacker took advantage of this vulnerability by creating multiple new trading pairs on the exchange and executing trades between them, thereby distorting the prices displayed on a decentralized exchange. By manipulating token prices on the decentralized exchange, the attacker was able to circumvent Vee Finance's slippage checks.

Due to incorrect pricing information and errors in price calculation, Vee Finance approved transactions that should have been rejected, allowing the attacker to steal approximately \$34 million in tokens from the protocol (Behnke, [n.d.-b](#)).

4.4 Importance of Smart Contract Audits in Web3 Applications

A smart contract audit is the process of examining the code of a smart contract in order to identify and address any potential security flaws, errors, or inefficiencies. The objective of an audit of a smart contract is to ensure that the contract functions as intended, is secure, and adheres to industry standards and best practices.

Audits of smart contracts are typically conducted by firms or individuals with expertise in blockchain technology, smart contract development, and security. Code review, vulnerability testing, penetration testing, and functional testing may be included in the auditing procedure.

Typically, the results of a smart contract audit are presented in a report that details any identified issues and corresponding recommendations. In addition to a summary of the contract's design and functionality, the audit report may also include a summary of any potential risks and restrictions.

Overall, a smart contract audit is crucial for ensuring the security and validity of a smart contract. By conducting a thorough audit, developers and stakeholders can identify and address any potential vulnerabilities prior to deploying the contract, thereby reducing the risk of security breaches, financial losses, and other adverse outcomes.

Given the immutability of smart contracts, auditing them prior to deployment is a crucial step in securing the Web3 environment. Although the presence of one or more audits does not guarantee that the code is completely secure, it reduces the likelihood of vulnerabilities significantly.

It is essential to remember that new vulnerabilities will always be discovered in the future, such as in cryptography and digital signatures, and that best practices will continue to evolve over time. However, ensuring the security of a smart contract at the time of deployment can significantly reduce the risk of attacks and

vulnerabilities. In other words, auditing a smart contract is not a one-time activity but rather an ongoing procedure to maintain its security and trustworthiness in the dynamic Web3 ecosystem.

Importantly, some of the vulnerabilities discussed in this chapter are unique to blockchain and smart contracts. For example, the deterministic nature of blockchains and the difficulty of producing pseudo-random numbers can present unique challenges for Web2 developers accustomed to working in a more forgiving environment.

Even experienced developers with a solid background in conventional software development may be unaware of all the distinctions between the two worlds. Here, the knowledge of professional auditors can prove invaluable. Having a team of professionals whose sole responsibility is to check smart contracts for vulnerabilities can significantly mitigate this issue.

In addition to identifying potential vulnerabilities, auditors can offer a fresh perspective on the problem and approach that the smart contract is attempting to solve. This can assist developers in refining and enhancing their code, resulting in more secure and resilient smart contracts.

4.5 Final Thoughts

In this chapter, we analyzed the biggest and most well-known smart contract vulnerabilities, focusing mainly on Solidity and Ethereum. We presented a checklist for vulnerable scenarios and a list of vulnerabilities with real-world examples. We also emphasized the importance of auditing the code. However, it is crucial to keep in mind that even when the smart contract is entirely safe, there could be other vulnerabilities outside of the code that pose a risk to user funds.

For example, in the access control section, we explained that only trusted addresses should be able to call certain functions. However, this assumption is based on the belief that a trusted address will not be compromised. In the Meerkat Finance hack, the attacker modified the logic of the smart contract from the Meerkat deployer account, indicating that Meerkat was either compromised or there were malicious intentions.

Moreover, the user experience in the crypto world could be improved to avoid problems. Even when the contract is perfectly safe and has perfect logic, phishing attacks could pose a vulnerability for user funds, as was the case with Badger DAO. Additionally, since most blockchain transactions have financial implications, there are financial risks associated with smart contract use, as seen in the Mango Markets hack. While checking the code's security is important, it is not sufficient to ensure that funds are safe.

References

- Abdul Sami, J. (2022, May 7). *Rari capital hack analysis & POC - BlockApex - Medium*. Medium. Retrieved from <https://blockapex.medium.com/rari-capital-hack-analysis-poc-3f0328e555d9>
- Behnke, R. (n.d.-a). *Explained: The PancakeBunny protocol hack (May 2021) - Halborn Blockchain security firm: Ethical hackers, Infosec & pen tests*. Halborn. Retrieved from <https://www.halborn.com/blog/post/explained-the-pancakebunny-protocol-hack-may-2021>
- Behnke, R. (n.d.-b). *Explained: The Vee Finance Hack (September 2021) - Halborn Blockchain security firm: Ethical hackers, Infosec & pen tests*. Halborn. Retrieved from <https://www.halborn.com/blog/post/explained-the-vee-finance-hack-september-2021>
- Buterin, V. (n.d.). *EIPs/eip-155.md at master · ethereum/EIPs*. GitHub. Retrieved from <https://github.com/ethereum/EIPs/blob/master/EIPS/eip-155.md>
- CWE - CWE-284: Improper Access Control (4.10). (n.d.). Retrieved from <https://cwe.mitre.org/data/definitions/284.html>
- Ethereum. (2023, March 16). *Oracles | ethereum.org*. ethereum.org. Retrieved from <https://ethereum.org/en/developers/docs/oracles/>
- Extropy. (2022, May 10). *Solana's Wormhole hack post-mortem analysis - Extropy. IO - Medium*. Medium. Retrieved from <https://extropy-io.medium.com/solanas-wormhole-hack-post-mortem-analysis-3b68b9e88e13>
- FutureLearn. (2022, October 25). *Updates, insights, and news from FutureLearn | online learning for you*. FutureLearn. Retrieved from <https://www.futurelearn.com/info/courses/defi-exploring-decentralised-finance-with-blockchain-technologies/0/steps/251885#:~:text=A%20smart%20contract%20is%20a,parties%20perform%20on%20these%20promises>
- Gagliardoni, T. (2021, August 12). *The Poly Network Hack explained*. Kudelski Security Research. Retrieved from <https://research.kudelskisecurity.com/2021/08/12/the-poly-network-hack-explained/>
- ghost. (n.d.). *Anyone can kill your contract · Issue #6995 · openethereum/parity-ethereum*. GitHub. Retrieved from <https://github.com/openethereum/parity-ethereum/issues/6995>
- MIT School of Engineering | » *Can a computer generate a truly random number?* (n.d.). MIT Engineering. Retrieved from <https://engineering.mit.edu/engage/ask-an-engineer/can-a-computer-generate-a-truly-random-number/#:~:text=%E2%80%9COn%20a%20completely%20deterministic%20machine.same%20algorithm%20to%20generate%20them>
- Oleh Malanii. (2023, February 24). *Biggest crypto hacks & their causes*. Hacken. Retrieved from <https://hacken.io/discover/crypto-hacks/>
- PeckShield. (2022, January 6). *ValueDeFi Incident: Incorrect weighted constant product invariant calculation*. Medium. Retrieved from <https://peckshield.medium.com/valuedefi-incident-incorrect-weighted-constant-product-invariant-calculation-1bbaa220a02b>
- Polak, K. (2022, January 17). *Hack solidity: Reentrancy attack*. HackerNoon. Retrieved from <https://hackernoon.com/hack-solidity-reentrancy-attack>
- Pratap, Z. (2022, September 5). *Reentrancy attacks and the DAO hack*. Chainlink Blog. Retrieved from <https://blog.chain.link/reentrancy-attacks-and-the-dao-hack/>
- Proposals, E. I. (2017, September 12). *EIP-712: Typed structured data hashing and signing*. Ethereum Improvement Proposals. Retrieved from <https://eips.ethereum.org/EIPS/eip-712>
- Rekt - Beanstalk - REKT. (2022, April 18). Rekt. Retrieved from <https://rekt.news/beanstalk-rekt/>
- Saylık, S. (2023, February 23). *Smart contract vulnerabilities*. Hacken. Retrieved from <https://hacken.io/discover/smart-contract-vulnerabilities/>
- SWC-101 · Overview. (n.d.). Retrieved from <https://swcregistry.io/docs/SWC-101>
- SWC-102 · Overview. (n.d.). Retrieved from <https://swcregistry.io/docs/SWC-102>
- SWC-106 · Overview. (n.d.). Retrieved from <https://swcregistry.io/docs/SWC-106>
- SWC-107 · Overview. (n.d.). Retrieved from <https://swcregistry.io/docs/SWC-107>
- SWC-111 · Overview. (n.d.). Retrieved from <https://swcregistry.io/docs/SWC-111>
- SWC-113 · Overview. (n.d.). Retrieved from <https://swcregistry.io/docs/SWC-113>
- SWC-114 · Overview. (n.d.). Retrieved from <https://swcregistry.io/docs/SWC-114>

- SWC-117 · Overview. (n.d.). Retrieved from <https://swcregistry.io/docs/SWC-117>
- SWC-120 · Overview. (n.d.). Retrieved from <https://swcregistry.io/docs/SWC-120>
- SWC-121 · Overview. (n.d.). Retrieved from <https://swcregistry.io/docs/SWC-121>
- SWC-122 · Overview. (n.d.). Retrieved from <https://swcregistry.io/docs/SWC-122>
- SWC-128 · Overview. (n.d.). Retrieved from <https://swcregistry.io/docs/SWC-128>
- Team, C. (2023, January 30). *[UPDATED 1/30/23] lessons from the wormhole exploit: Smart contract vulnerabilities introduce risk: Blockchains' transparency makes it hard for bad actors to cash out.* Chainalysis. Retrieved from <https://blog.chainalysis.com/reports/wormhole-hack-february-2022/>
- WatchPug. (2022, January 6). *The PancakeBunny Bunny performance fee minting incident analysis.* Medium. Retrieved from <https://watchpug.medium.com/the-pancakebunny-bunny-pool-incident-analysis-71fb67c1536e>
- Wilmoth, J. (2021, March 4). *'I accidentally killed it': Parity wallet bug locks \$150 million in ether.* CCN.com. Retrieved from <https://www.ccn.com/i-accidentally-killed-it-parity-wallet-bug-locks-150-million-in-ether>

Chapter 5

Token Economics Model Creation and Security



Lisa J. Y. Tan

Token economy an emerging and intricate. Well-designed token economics, with rules and incentives, can define the long-term outcomes of token ecosystems. Poorly designed economics can lead to the collapse of the ecosystem.

While the study of token economics is enthralling and relatively new its foundational principles have roots in traditional economic theories. We see fundamental elements of it in classical economics like the works of Adam Smith, Elinor Ostrome's take on public goods, and behavioural patterns in sociology. If this is nothing new then, why are there so many new books and articles relating to this topic? To get started, we need to understand what token economy is and why token economics is an important topic.

5.1 Tokens vs Economy

Tokens play a crucial role in the digital asset economy, which can be built on distributed ledger technology (DLT). To fully grasp the significance of tokens, it is essential to understand the nature of this economy as a public common good used by relevant economic agents. With advancements in technology, we now have the opportunity to design and create this economy from scratch.

Digital assets, which are items of value represented digitally through tokenization, can be anything from financial assets like cash and bonds to real assets such as artwork and property. Deployed on distributed ledgers like blockchains, these digital assets can also be referred to as crypto assets. The combination of tokenization

L. J. Y. Tan (✉)
Economics Design, Singapore, Singapore

and distributed ledgers unlocks transformative economic potential by enabling anything of value to be represented digitally and stored on a secure, immutable ledger.

The digital asset economy is an economy governed by rules and incentives. This extends beyond just rules and incentives of how individual transact with each other in the ecosystem, but also rules and incentives programmed in the token. The economy supports various use cases that can potentially facilitate efficient transactions, enhance financial inclusion, and unlock economic value. Within this economy, cryptocurrencies act as the native currency of the distributed ledger, serving as a medium of exchange or store of value for the network. At a blockchain level, tokens are often used to pay transaction fees or incentivize users to maintain the network's security. At an application layer, tokens can be used to represent an intrinsic value of the ecosystem, like a token to facilitate the trade of two separate tokens in an autonomous market maker (AMM), or a store of intrinsic value to signal trust and security in a project, like a decentralised insurance protocol.

Tokens are an integral part of the digital asset economy built on DLT, serving as the foundation for a public good that can be designed and created from scratch. By understanding the digital asset economy, we can better design robust economies and address the economic risks associated with the incentive mechanisms.

5.2 Economy Design of Tokens Is Not New

In the physical world with countries and international organizations, we design similar economies with a shared environment that accommodates the diverse incentives and behaviors of various economic agents (Hardin, 1968). It is important to design proper economies that foster collaboration and sustainable use of assets in the economy, while addressing the unique challenges and conflicting interests that often arise in such settings.

In today's rapidly evolving technological landscape, the management of public goods and ecosystems extends beyond merely analyzing risks within existing market structures. We must also consider risks when creating new mechanisms and incentives for the economy. This forward-thinking approach enables us to establish innovative rules and structures tailored to specific situations, rather than relying solely on traditional market models. By proactively addressing risks, we can better align stakeholder incentives and ensure that newly created ecosystems are both sustainable and resilient in the face of change (Bruce and Buck, 1997).

An important point in token economy is the critical role of governance structures, monitoring, and enforcement in managing public goods and ecosystems. By establishing a robust governance framework, we can effectively navigate the challenges and risks inherent in shared ecosystems. Governance structures, such as DAOs, provide a foundation for decision-making and coordination among diverse stakeholders. Monitoring and enforcement mechanisms are equally crucial, as they ensure compliance with agreed-upon rules and regulations, fostering trust and accountability among stakeholders.

5.3 Why Is this Important

Economics is split into two primary domains: macroeconomics and microeconomics. In recent years, the domain of “behavioral economics” has also risen in significance. There are also competing schools of thought which influence the fundamentals of how one decides economic policies (De Benedictis & Di Maio, 2016). But at its core, economics is three simple things:

- Incentives
- Disincentives
- Behaviours



















Token economics is an important topic because of the growing ecosystems that come into the market. Looking at the top market capitalization of companies in 2001 vs 2021 (Table 5.1 and 5.2, respectively), we have moved from supply-side production to ecosystems development. In 2001, companies like Cisco, Exxon Mobil, Ford, General Electric, and Royal Dutch Shell are constrained by supply-side production. The companies have to produce goods and services and balance them with production constraints like barrels of oil extractable per day or cars made per month. On the other hand, in 2021, we see a new trend of business models, where the companies are not producing anything, but rather, their main business lies in the ecosystem they build. For example, Amazon, Alphabet, Meta, Tencent and Alibaba Group. These are ecosystem-based business models that produce some goods and services, but value proposition (hence intrinsic value) lies in the prosumer ecosystem they have built.

In the last 20 years, we moved toward multi-sided ecosystems, where businesses focus on building the ecosystem and allowing buyers and sellers to produce and consume goods. It is no longer constrained by supply-side production limits. This is

Table 5.1 List of public corporations by market capitalization (Wikipedia, 2021)

Rank	Name	Country	Primary industry	Market value (USD million)
1	General Electric	United States	Conglomerate	▲477,406
2	Cisco Systems	United States	Networking hardware	▼304,699
3	ExxonMobil	United States	Oil and gas	▲286,367
4	Pfizer	United States	Health care	263,996
5	Microsoft	United States	Software industry	▼258,436
6	Walmart	United States	Retail	▼250,955
7	Citigroup	United States	Banking	250,143
8	Vodafone	United Kingdom	Telecommunications	227,175
9	Intel	United States	Computer hardware	▼227,048
10	Royal Dutch Shell	Netherlands United Kingdom	Oil and gas	206,340

Table 5.2 List of public corporations by market capitalization (Financial Times, 2021)

Rank	First quarter		Second quarter		Third quarter		Fourth quarter	
		Value		Value		Value		Value
1		Apple ▼ 2,050,000		Apple ▲ 2,286,000		Apple ▲ 2,339,000		Apple ▲ 2,913,000
2		Microsoft ▲ 1,778,000		Microsoft ▲ 2,040,000		Microsoft ▲ 2,119,000		Microsoft ▲ 2,525,000
3		Amazon ▼ 1,558,000		Amazon ▲ 1,735,000		Alphabet ▲ 1,777,000		Alphabet ▲ 1,922,000
4		Alphabet ▲ 1,395,000		Alphabet ▲ 1,680,000		Amazon ▼ 1,664,000		Amazon ▲ 1,691,000
5		Meta ▲ 838,720		Meta ▲ 985,920		Meta ▼ 956,890		Tesla ▲ 1,061,000
6		Tencent ▲ 766,970		Tencent ▼ 721,460		Tesla ▲ 776,850		Meta ▼ 935,640
7		Tesla ▼ 641,110		Tesla ▲ 654,780		Berkshire Hathaway ▼ 619,950		Nvidia ▲ 732,920
8		Alibaba Group ▼ 615,010		Berkshire Hathaway ▲ 637,280		TSMC ▼ 579,030		Berkshire Hathaway ▲ 668,630
9		TSMC ▲ 613,410		TSMC ▲ 623,160		Tencent ▼ 574,460		TSMC ▲ 623,930
10		Berkshire Hathaway ▲ 590,050		Alibaba Group ▲ 615,140		Nvidia ▲ 517,900		Tencent ▼ 559,900

the new digital economy. Using a simple example, that means ecosystems need to be efficient at matching homemade pastry chefs with dessert-loving consumers (ecosystem) as opposed to a supply chain of making all the cakes, optimizing marginal cost per cake, and balancing demand forecast with cake production (supply-side production).

5.3.1 Risks

This is an important topic now because ecosystems today are not centrally managed but decentralized. In addition, the execution of these trades is done by machines and executed automatically based on the rules embedded in the rules of trade. That brings about two risks here.

Firstly, the risk is in the creation of these rules that govern the trade and transaction between consumers and producers in the ecosystem. How do we define these rules? How do we create anti-fragile rules? Who decides who decides? How do we create fair rules or universal constraints, in which we can update the rules that are suitable for the ecosystem at that time? For example, when the Web3 market cap is 100 M, the risk management of lending protocols was more relaxed than when the market cap is 100B. There are more inherent and systematic risks, and hence more rules and constraints will need to be created as the macro market grows and evolves.

Secondly, the risk is the execution of these rules. The rules of transaction between economic participants in this economy need to be defined. But who makes sure these rules are executed? How can this be done? Who updates the rules as the market structure changes? The execution of these rules needs to be facilitated by machines or code instead of people. It is no longer the board of Facebook or Amazon making changes to how the ecosystem functions. Today, users of the ecosystem get a say in it.

The importance of designing common goods and ecosystems with the varied incentives and behaviors of stakeholders in mind, addressing risks in both existing market structures and newly created mechanisms, and emphasizing the crucial role of governance structures, monitoring, and enforcement in managing shared resources. By considering these key factors, we can work toward building resilient, sustainable, and inclusive ecosystems that benefit all stakeholders involved.

5.4 What Is Token Economics

What then, is token economics, if that is so important? Token economics is the study of **designing incentives** for the system to **encourage economic transactions** with the goal of **coordinating and collaborating** between agents in the system. This can include a metaverse, blockchain game, complex system or an exchange to allow a swap between Token A and Token B.

Designing incentives includes designing the incentives and rules to govern economic transactions and coordinate in a network. That is different from embedded incentives that cannot be changed, because the types of economic transactions could change with time. Thus, the incentives need to be constantly updated to reflect the current state of the economic transactions. This is similar to government policies. For example, the policies (incentives) that worked in Singapore 50 years ago under the leadership of Lee Kuan Yew might not work in Singapore right now. These rules of the economic transactions can be defined in smart contracts like trades in Uniswap, mint DAI on Maker protocol, battle-winning payoff in games, and meta-verse token payment to travel.

Economic transactions are defined by each ecosystem. It refers to the type of interaction between participants of the market ecosystem. Encouraging economic transactions is key, because in a platform, value creation comes from users interacting with each other (Cong et al., 2021). An Instagram or Facebook page with just your pictures is not an app you will download, whereas the ability to look at other people's pictures, like and comment creates value for the Instagram or Facebook user. This is the *raison d'être* for an ecosystem or market.

Coordinating and collaborating are the new addition to economics. Previously, in a centralized market or ecosystem, the core governance body (e.g., board of directors at Facebook or Amazon) defines how the ecosystem is structured and governed. Now in a decentralized market or ecosystem, we collectively govern the economic transactions available and collectively agree on the distribution and potential production of resources in the market. This new level of social coordination requires the design of the right incentives.

When it comes to tokens, tokens can take different forms—for example, a way to facilitate transactions amongst users, or tools as a coordination mechanism for decentralized economic agents to vote on economic mechanism changes via a DAO. The token could evolve and create new utility for internal economy usage as the economic transactions and/or incentives change as the market structure changes.

Token economics is still a new field. The coordination of people to engage in economic transactions is enforced by rules of transaction (think of them as rule of law with more flexibility because code is not always law, Lessig, 2000). These rules can be a protocol, a set of steps to follow when engaging in a transaction, embedded in a smart contract. This field of economics include market design, mechanism design, monetary policy, financial economics, and allocation mechanism, just to name a few. It combines both micro- and macro-economics.

The platform layer's goal is to increase economic transactions as that is a proxy for value creation. The economics is to maintain the right incentives and allocation of resources. Here, like a country, a platform can go through economic busts and booms, recessions, financial crises, and hyperinflation.

We want to design a system that is sufficiently robust, while continuously maintaining and upgrading it to be anti-fragile. Like a country, we need to define, measure, and improve the value creation in the system. Token economics *could* be changed, as a reflection of market structure changes.

The goal of token economics is to answer: given these constraints and goals, what kinds of economic transactions and resources can we design to achieve the

coordination properties we want? Going back to ecosystems that we talked about in the first part of this chapter, we need to design the economic incentives and rules for this ecosystem to thrive, for it to be self-financing, self-sustaining, and self-organizing.

5.5 Web3 Security and Token Economics

In token economics, a very important aspect we need to talk about is Web3 security. In Web2, companies and institutions create rules and regulations of how they work together. These usually are known as the standard operating procedures and they are the operational rules of how to behave, act, and interact in this institution. In Web3, where everyone can participate instead of going through an interview process to join a company, we need new ways of creating rules and regulations to enforce the behaviors we want or do not want to do. In Web3, this new way is the use of tokens as incentive mechanisms. Tokens are the mechanisms to coordinate the actions and behaviors of users in this ecosystem. The future is about the logic of what the smart contract executed because that is defined by the economic rules. This is operational efficiency.

Web3 security is not just about code, but also about finance and economics. As discussed, token economics defines the rules of the ecosystem. The rules are then codified and executed by smart contract. The aspect of code-based security is absolutely important, because a bug or hack can cause the ecosystem to crumble. At the same time, when analyzing security from a token economics perspective, we need to take a step back and look beyond what we usually analyze: post event. Security in token economics here is a pre-event analysis. That could be exploits like leveraging a low market cap token with low liquidity. For example, you could open an Aave lending pool by using the token with a low market cap as collateral and borrowing USDC. With the USDC, you can buy more of the token with the low market cap and borrow more USDC. Since that pushes token prices up due to the low liquidity, you can borrow more USDC. When the amount of USDC is more than the initial value you added in, you can default on the payment and the insurance pool of Aave will have to repay it. This results in a security risk that is due to the flaw in the economy design. To resolve this, there needs to be more consideration on the risk parameter of that borrowing pool. For instance, instead just enabling a borrowing ratio (e.g., depositing 1000 USDC to borrow 70% of that value in another token, ABC), there also needs to be additional parameters like “secondary market liquidity ratio.” In the example, the other token, ABC needs to have at least 50% liquidity in the secondary market to reduce the financial risk in the borrowing pool.

5.5.1 Ponzinomics

An example of Web3 economic security is the design of what is known as Ponzinomics. Ponzinomics is a combination of ponzi-scams and economics, where someone creates a ponzi-scam wrapped in a protocol and markets it as economics.

It is essentially a trait in projects where the primary motivation for a lot of participants is financial gain. Here, the creators are not so much about caring about the underlying activity of the game as it is about making money off of the project. In doing so, having that experience of financial motivation be the main driver, means that the value added to the game is driven by all these users coming in. So we end up with a zero or negative economy. After all, if someone's making money, it is because somebody else is buying in, rather than there being any real value generated by the project.

To put it simply, we can identify ponzinomics when the value creation is not in the value created (e.g., facilitating swaps in an AMM, gameplay in a game, or social interaction in a metaverse). Rather, the value is about making money off new players in the ecosystem. That means, there is no value generated by the economy, except to get new value from users coming in. An example of such design flaw and thus economic security risk is the early case of Axie Infinity, a video game. They encourage users to join the game by giving away tokens that can be traded in the open market, and thus have a market price. This financial reward becomes too attractive for players to focus on playing the game and growing the marketplace, resulting in a crash in the economy, since players were solely there to extract value.

5.6 How Web3 Compares with Existing Economic Structures?

Abstracting the idea of economic rules of a game, we see similar models in Web2, primarily in companies and countries. In a company, it is similar to that of the executive team optimizing either operations for the company's internal ecosystem or ecosystem team (be it games, social media, or an ecosystem) to increase the engagements within its ecosystem. In a country, it is similar to that of the government who sets the laws in place.

In a company, the company sets the rules of engagement. For example in a game, the company sets what you can or cannot do, the ways to interact with another player, the reward points and strategies available for your character to move about in the game. These rules underline the entire gameplay and game design. These rules are economic rules. We create the constraints for users to behave independently and freely, to incentivize certain behaviors and actions from them.

From a country's perspective, the government sets the rule of law in the country. They define what can or cannot be done in the jurisdiction, the rules of engagement, and constraints of the individual. For example, income tax in Singapore is different to that of the USA, France, and Qatar. Even in the USA, there are different taxation rules in each state. These rules did not appear random. Instead, they support the functioning of a well-organized country. The economic rules and laws help to create a self-financing, self-sustaining, and self-organizing economy.

With that being said, who does the checks and balances? Typically, the protocol operators (e.g., core developers, operations team of the protocol), Web3 ecosystem participants like the user of the protocol, stakeholders like VCs who invest in the growth of the protocol, smart contract auditors who are paid to do an independent audit, bug bounty participants, regulators or even key opinion leaders who are promoting certain protocols. In any case, this is deemed as token economics security.

Token economics deals with coordination of people in economic transactions using smart contracts. It aims to optimize incentives and resource allocation in the ecosystem and ensure its security. It encompasses multiple sub-fields and as the ecosystem evolves, the risk and security of the ecosystem will also change.

Macro perspective: To get started with token economics, it is first necessary to define the value proposition of the ecosystem. After all, the ecosystem exists to provide value to the producers and consumers, then encourage them to trade in your ecosystem. The value proposition is what makes the economy different from its competitors. This basically asks why should people choose to participate in your economy over others like it.

Middle perspective: Understanding the value proposition leads us to defining the market, the rules of the trade, and the reason for trade between producers and consumers in your ecosystem. Security comes in the form of the appropriate rules, regulations, and constraints of what a person can or cannot do in the economy.

Micro perspective: The micro-economy here refers to the assets of trade, the security, stability, and structure of trade. We need to understand the assets and how the assets behave, then create rules to constrain their behaviors to allow the assets to act in certain ways. For example, an asset should not be traded and should only be used for internal accounting purposes in this specific economy.

5.7 What Does Token Economics Entail

The truth is that there is no one size fits all solution. Instead, we can use a framework to share how such economies make sense and how to begin designing the economic mechanisms (Tan, 2019).

The **Economics Design Framework** (Fig. 5.1) considers the parameters of an economy when designing an ecosystem. It falls into 3 key pillars: market design, mechanism design, and token design.

Market design defines this environment through design and engineering. This ensures that users of the ecosystem trade within the environment. Trade in this context could mean exchange of tokens or data.

Mechanism design develops the rules participants must follow to play in the market, including governance, non-financial incentives, and structures to update these rules as needed.

Token design refers to the rules of how tokens act within an ecosystem. This can include whether there is a single versus a dual token model. The type of token distribution used in a game determines who receives tokens. If staking is an included

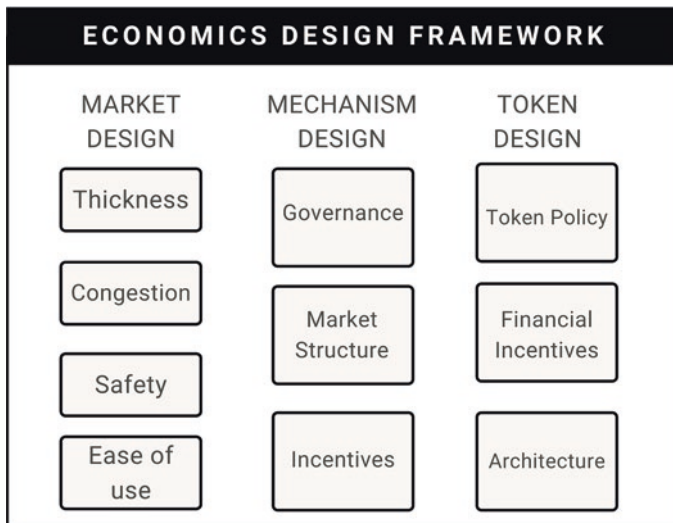


Fig. 5.1 Economics Design Framework

feature of that protocol, if there is a tax on buying and selling Non-Fungible Tokens (NFTs), and where that revenue is directed toward, etc., (Cong et al., 2022). These rules can be defined with code in the smart contract. They can change as the system grows, or as the ecosystem integrates new forms of transactional activities. The tokens capture the intrinsic value of this ecosystem, and by designing the tokens, we can better understand where value is being captured and where value is being created, and how value is distributed amongst the users in this ecosystem.

Designing the economy and token is not a one-stop shop. There will be more creative and unique ways of design that are relevant to the ecosystem itself. This means, while token economics involve market, mechanism, and token design, there is no one ideal model that is likely to be widely adopted because the token value capture and creation is different for different economies. There are likely to be several different variations and mechanisms of creative design applied to each project, and that is because not all economies are the same. Therefore, it is important to have the right design that fits the particular version and underlying goals.

Going back to the companies and countries analogy above, each company and country is different in its operations, production, and skillsets of the team or citizens. Each country has its own unique set of resources within its economy. There is no single solution to meeting the needs of every country. The mechanisms created to balance one economy must be dependent on the resources present, the political landscape, and every agent that is present inside the economy. This is similar to token-based ecosystems (Cong et al., 2020). Economists would have a few models to base their economies on. However, it is up to them what mechanisms they configure within their economy to help them balance it.

5.7.1 Economics Design Framework

The economics design framework was developed to allow economists, creators, and designers to focus on the important aspects when developing a sustainable and working economy.

Market design are the parameters initially decided by the economist, game designer, and ecosystem developer. This is important to limit the effectiveness of the mechanism design and token monetary policy designs moving forward. Mechanism design defines the rules of transaction between agents, both interaction with smart contract and interactions with each other. When comparing the various industries in Web3 (e.g., DeFi vs games), instead of a market structure in DeFi, we have a revenue model in games. Revenue model includes direct, rental, employee (scholarship), and asset utilization. These are important rules that affect token design next. This is why economy design is different for each ecosystem. Some token business models not are also crucial when it comes to value creation under market design. Token design translates the value created, through the market and rules of the economy, into real value earned by the users. The important part is to balance the monetary policy of resources with the value creation cycle.

5.7.2 Value Creation

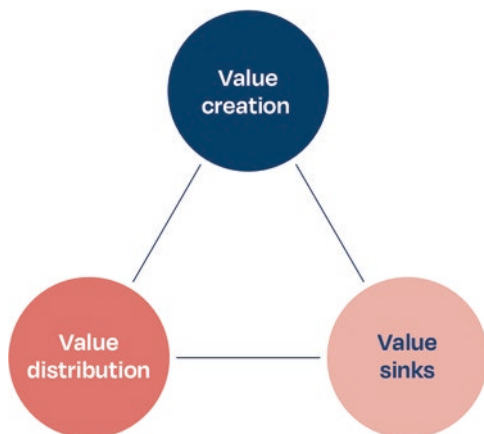
Markets exist by adding value to the users in the market by reducing transaction cost. Markets tap into the economics of agglomeration and bring more value by increasing the ability to match and transact, define the economic rules to trade, and reduce the opportunity cost to find the right agent to trade with.

Value is created when matching is done right. Matching means matching the right person or resource to transact with. That includes trading resources (sell Axie in a market) or fight in a battle (PvP battles). This is important to have both parties feel like their value is optimized when trading, instead of a mismatch. If a market is unable to match users right, the user can trade outside of the market (sell Axie via OTC) or leave the market as it fails to generate value for the user (spend more time playing another game instead).

Value is realized when there is a reduced cost to search for matching transactions. If matching is that important, the value is truly realized when there is a reduction of cost to search for the person to transact with. The searching cost, in terms of time, energy, and effort, increases the cost to transact. This can be seen as opportunity cost. If it is easy to find the right person or resource to transact with, it becomes much cheaper to transact, which increases value to users of the market.

Value is retained when market rules are defined and respected. Even if the market is thick to increase matching ability, less congested to reduce search cost, the final value retention is to enable the trade to be executed. Here, the market is an important coordination tool. That is to define and enforce for rules to be respected. If legal

Fig. 5.2 Value Creation Cycle



contracts are not obeyed, the market finds it hard to grow since trades rules are not respected. We see this with emerging markets, where the value of legal contracts is less high than in developed markets.

5.7.3 Value Creation Cycle

The value creation cycle (Fig. 5.2) consists of 3 components, creation (inflation), distribution, and sinks (deflation). When new value is created, the new resources can be deployed for a specific persona for new economic activities like cashing out or other personas, entering the ecosystem and interacting with other assets like NFT, tokens, smart contracts, or non-tradable tokens.

While most projects focus on creation and distribution, value sinks essential to create a healthy balanced economy. In any market, the key asset of transfer is value. Value can be captured in forms of goods (barter trade), common currency (sovereign currency), or internal tokens (in-game currency, digital representation of assets). It is an art to balance between value being transacted and the assets that represent such value. Successful game design has its value strategies tied to the token policy that balances between boom and bust cycles of value creation.

The value cycle components represent various mechanisms in the economy. Value creation is about long-term productivity growth and structural transformation. Value distribution focuses on short-term balance of economic growth and asset inflation. Value sinks refer to the real value growth of the active player class, coming from supply reduction of asset. The important thing is to balance between the 3 value forces by managing the monetary policy.

Incentives and rules play a critical role in shaping the behavior of economic agents within the value cycle. By aligning incentives with the desired outcomes, token economists and protocol operators can encourage sustainable value creation, equitable value distribution, and effective value sinks. Rules and regulations, on the

other hand, set boundaries for economic activities, ensuring that the actions of individuals and organizations contribute positively to the overall value cycle.

Economic security is a vital aspect of the value cycle, as it ensures stability and confidence in the system. A secure economy fosters trust among participants, enabling them to engage in value creation, distribution, and sink processes without fear of disruption or loss. Security can be achieved through a combination of robust governance structures, risk management strategies, and transparency in the rules and incentives that guide economic behavior. By promoting economic security, policymakers can support a resilient and thriving value cycle that benefits all participants and contributes to the long-term well-being of the economy.

5.8 Token Economics Stress Test vs Economics Risk Monitoring

Agent-based simulation is a useful method for stress testing economic models, as it allows researchers to examine the behaviors of individual agents within an economy in response to various incentive mechanisms. By simulating the interactions between agents under different scenarios, policymakers and analysts can evaluate the robustness of their economic designs and identify potential risks or weaknesses. Tools such as Python-based agent modeling and artificial intelligence can be employed to create realistic simulations of agent behavior. One relevant paper that demonstrates the use of generative agents to simulate human behavior is “Generative Agents: Interactive Simulacra of Human Behavior.”

Another approach to stress testing economic models involves using Excel-based financial modeling, which can help researchers develop a first principles understanding of the relationships between individual behaviors and their impact on the macro economy. By building comprehensive financial models that capture the key dynamics of the economy, analysts can test the sensitivity of their assumptions and evaluate the potential consequences of various policy choices or market conditions.

Stress testing is a valuable tool for designing and evaluating new economies during their initial phases, such as “go-to-market,” defining “product-market fit,” and “initial user acquisition.” However, once the market and ecosystem are established with a user base, the focus should shift from stress testing to economic risk monitoring, that includes updating economic incentives for user retention. In this stage, it is crucial to identify emerging economic risks and address them using real historical data, rather than relying solely on simulated data. By staying adaptive and responsive to changing market conditions, policymakers and economists can better ensure the long-term stability and success of the economy.

5.9 Cyber Security Risks Come In

So far, we have discussed how to design and create a working economy. Cyber security comes in the form of risks of the economy design. For example, execution of these economic policies in smart contract, exploits in economic model, exploits in code—e.g. over-leverage or Aave structure, or bugs in the smart contract.

It is important to understand the risks because it provides undisputed proof of responsibility and care toward the community, developers, investors, and users alike. Communities will grow with the assurance that there are no hidden risks. Since the key difference in Web3 is the design of the economy, as compared to Web2, token economy risks are the best way to discover and address risks before the protocol suffers substantial losses.

Since the economic rules are executed with code, cyber security enters to discuss the importance of well-written code. As discussed in Chap. 7, DevSecOps, it goes into detail about how DevSecOps evolve in the Web3 space.

5.10 Summary and Ongoing Work on Tokenomics

In this chapter, we have explored the principles of designing an economy across various domains, including games, interactive media (metaverse), finance (DeFi, ReFi, SoFi), and infrastructure (L1, L2, oracles) projects. The foundational principles of creating a functional and robust economy are in 3 pillars: market design, mechanism design, and token design.

The foundational pillars for creating an economy remain the same across these diverse industries, emphasizing the importance of understanding the underlying dynamics and mechanisms that drive value creation, distribution, and retention.

However, the implementation of these principles can vary significantly depending on the specific context and industry. Factors such as governance structure, monitoring and enforcement of rules, and the design of token monetary policy must be tailored to the unique characteristics and requirements of each domain. As the token economy continues to evolve and expand, industries such as games, interactive media (metaverse), finance (DeFi, ReFi, SoFi), and infrastructure (L1, L2, oracles) projects will increasingly rely on well-designed economic systems to ensure their long-term success and sustainability. By understanding and applying the principles discussed in this chapter, practitioners can create robust, adaptable, and thriving economies that cater to the distinct needs of their respective industries.

In the next chapter, we will discuss economic risk, now that we have learnt how to design a robust economy.

References

- Bruce, A., & Buck, T. (1997). Executive reward and corporate governance. K. Keasey, S. Thompson and M. Wright, *Corporate Governance: Economic, Management and Financial Issues*, 80-102.
- Cong, L. W., Li, Y., & Wang, N. (2020). *Token-based platform finance no. w27810*. National Bureau of Economic Research.
- Cong, L. W., Li, Y., & Wang, N. (2021). Tokenomics: Dynamic adoption and valuation. *The Review of Financial Studies*, 34(3), 1105–1155.
- Cong, L. W., He, Z., & Tang, K. (2022). *Staking, token pricing, and crypto carry*. Available at SSRN.
- De Benedictis, L., & Di Maio, M. (2016). Schools of thought and economists' opinions on economic policy. *Eastern Economic Journal*, 42(3), 464–482.
- Hardin, G. (1968). The Tragedy of the Commons. *Science*, 162(3859), 1243–1248. <http://www.jstor.org/stable/1724745>
- Financial Times. (2021). FT500 - Global 500 data. *Financial Times*. Retrieved from <http://specials.ft.com/ft500/may2001/FT36H8Z8KMC.html>
- Lessig, L. (2000). Lawrence Lessig on the increasing regulation of cyberspace. *Harvard Magazine*. Retrieved from <https://www.harvardmagazine.com/2000/01/code-is-law-html>
- Tan, L. (2019). Token economics framework. *Other Economics Research eJournal*.
- Wikipedia. 2021. *List of public corporations by market capitalization*. Wikipedia. Retrieved January 11, 2023, from https://en.wikipedia.org/wiki/List_of_public_corporations_by_market_capitalization#2021

Chapter 6

Economic Exploits and Risk Mitigation Strategies



Lisa J. Y. Tan

Following our chapter in Chap. 5, we will now dive deeper into the case studies of economic risks and exploits. While there are currently no token-as-a-new-commodity-class regulation in place nor are there token-based working groups working on such protective regulation, it is important to understand that such risks exist as part of the security of Web3. The other chapters in the book cover technical and code-based risks, which are important in the age of a digital code-based world. That being said, the final users are humans at the end of the day, and there are risks that exist even when we could technically mitigate all possible technological security risks.

Economic exploit and security risk are similar to that of “legal loopholes.” For example, creating shell companies in tax havens to pay zero taxes or sophisticated arbitrage in the financial market. It is not a new security risk. However, just because such risks exist in the traditional world does not mean that as we evolve and build better systems, we should carry these risks over. Thus, to build better systems, we need to first understand the flaws and security risks in the systems we build today. Then, we can build better economic models.

In this chapter, we will focus on understanding 3 case studies and how these protocols are created from an economic perspective. Then, we will look at the flaws of the protocols. We will dive into 3 areas of security risks, Economic Exploit, Economic Incentive Design, and Bonding Curve Exploits. To have a diverse understanding of the impact, we will give a DeFi example, GameFi example, and CeFi example that is linked to DeFi.

L. J. Y. Tan (✉)
Economics Design, Singapore, Singapore

6.1 Case Study 1: Economic Exploit Through Financial Engineering

Aave is a lending and borrowing protocol. Users deposit TokenA and borrow TokenB. There is a ratio to measure the financial macroeconomic risk of the protocol as a whole, the loan-to-value (LTV) ratio. This case study is specifically about an economic exploit that happened in Aave, due to how the protocol is structured and liquidity of a low capitalization token.

6.1.1 Case Study

In November, Avi Eisenberg attempted an audacious attack on the Aave decentralized finance (DeFi) protocol by exploiting the CRV token in a loop-borrow and trade pattern. Eisenberg, known for draining around \$110 million from the Solana-based lending protocol Mango Markets (Sandor, 2022), deposited USDC as collateral on Aave, borrowed CRV tokens, and sold them for USDC, which he then deposited back into Aave. This caused the CRV price to plummet, and traders initially expected that Eisenberg would liquidate one of Curve's founders, who had deposited a substantial amount of CRV into Aave as collateral.

However, the CRV price rallied, and traders speculated that Eisenberg was trying to force a massive short squeeze, pushing Aave's liquidation mechanism to acquire large amounts of CRV. Curve's release of its crvUSD whitepaper also contributed to the price rally. The attack left Aave with 2.68 million CRV (approximately \$1.6 million) in bad debt.

Aave, governed by a decentralized autonomous organization (DAO) and AAVE token holders, responded to the situation by voting to procure the necessary CRV tokens through the ParaSwap decentralized exchange aggregator. The acquisition of CRV tokens eliminated the bad debt resulting from Eisenberg's botched exploit. This action was taken before the activation of a major tech upgrade called Aave v3.

This case highlights the importance of effective liquidation mechanisms in DeFi borrowing, as liquidations depend on dynamic decentralized exchange (DEX) liquidity. In the case of crvUSD, a mechanism called LLAMMA (Lending Liquidity AMM Algorithm) is employed to smooth out the volatility of the collateral and minimize liquidations. The entire episode underscores the need for protocols to have stability mechanisms in place to handle such exploit attempts and ensure the security of their users' assets.

6.1.2 *The Exploit*

Avraham Eisenberg, a notorious crypto trader known for exploiting \$114 million from Mango Markets, attempted a similar exploit on Aave, a decentralized lending platform. Eisenberg borrowed 40 million Curve (CRV) tokens (valued at \$20 million) from Aave, using \$40 million in USDC stablecoin as collateral. He then transferred the CRV tokens to the OKEx crypto exchange, presumably to build a short position and profit from a price decline (Sandor, 2023).

However, after a series of wild price fluctuations, Eisenberg's position was liquidated, leaving Aave with \$1.6 million in bad debt, a relatively insignificant amount compared to the \$6 billion total value locked on the protocol. Eisenberg's exploit attempt ultimately failed due to insufficient initial capital to execute the "profitable trade."

This case study highlights the risks associated with decentralized finance (DeFi) protocols and the importance of implementing security measures to prevent potential exploits by malicious actors.

6.1.3 *Solution: Risk Adjustment*

The short-term solution is to temporarily freezing specific markets on Aave V2 ETH, including YFI, CRV, ZRX, MANA, 1inch, BAT, sUSD, ENJ, GUSD, AMPL, RAI, USDP, LUSD, xSUSHI, DPI, renFIL, and MKR, to derisk Aave V2 and encourage migration to V3. This is a broader approach to reduce risks associated with insolvency, price manipulation, traders using Aave to avoid high slippage costs, high utilization impeding atomic liquidations, and replicating the CRV situation. The decision stems from several factors, including the community's lower risk tolerance, the recent CRV exploit, and the impending migration toward V3 (Aave, 2022).

It is important to analyze the risk profile of specific assets, their intrinsic utility and usage, and the impact in the macro market. The community's risk tolerance may affect the decision to pause borrowing for assets like LINK and UNI, which are considered lower risk. Meanwhile, low-usage assets like ENJ and USDP are included in the proposal due to their ambivalent benefits in V2.

The other solution is to disable borrowing instead of freezing the assets for borrowing. These are all solutions to mitigate short-term risks spurred by insufficient liquidity and vulnerable parameters, with the latter offering a more lenient yet risk-aware solution.

In addition, following an exploit attempt on rival lending platform Aave, Compound Finance, another decentralized lending protocol, has taken proactive measures to reduce risk on its platform. The community voted to introduce or lower the maximum borrowing amount for 10 cryptocurrencies, including wBTC, LINK, and UNI. By setting borrowing caps, Compound aims to avoid high-risk attack

vectors while maintaining capital efficiency and allowing for organic borrow demand (Compound, 2022).

6.2 Case Study 2: Incentive Mechanism Design Risk

The gaming economy is an original concept that creates an emerging market for in-game items and assets. The market is based on supply and demand for these items. The price of items fluctuates over time depending on various factors such as the popularity of the game, the rarity of the item, and the demand for it. The economics behind P2E gaming business models are based on supply and demand. In-game assets are in short supply, which creates scarcity and increases their value. This scarcity is achieved through several methods, such as limiting the number of assets that can be minted. This is done by making them difficult to acquire or restricting their availability through time-limited events or promotions (Martin, 2022a, b).

Demand for in-game assets is driven by players who intend to use them in-game or sell them for real money. Players who want to use in-game purchases in gameplay may be willing to pay a premium to acquire them quickly. On the other hand, players who want to sell in-game assets for real money may be willing to accept a lower price to make a quick sale. P2E gaming business models also rely on network effects. The more players participate in the ecosystem, the more valuable the assets become. This is because a larger player base increases asset demand, which drives up their price. Additionally, more players in the ecosystem mean more potential buyers for in-game purchases, which creates liquidity and a more efficient market.

One popular example of P2E games is Axie Infinity. It is a blockchain-based game where players can earn crypto by breeding, battling, and trading virtual creatures called “Axies.” The game’s economy is governed by the game’s native tokens called Axie Infinity Shards (\$AXS) and Smooth Love Potion (SLP), which can be traded for other cryptocurrencies or fiat currencies on various online exchanges. Players can earn significant amounts of money playing the game. It has become particularly popular in Southeast Asian countries, such as the Philippines, where players turn to the game as a source of income.

Axie Infinity was the game that put the blockchain gaming industry on the map as it was arguably the first successful gaming project that allowed gamers to earn from interacting with their ecosystem. At the peak of its success, the price of its governance token, Axie Infinity Shards (\$AXS) hit an all-time high of \$164.9, and the game had roughly 2.7 million users. The numbers took a turn for the worse since then as the economic model proved to be unsustainable. The economy crashed as demand for assets could not keep up with the overwhelming increase in supply, which ultimately led to the start of the project’s misfortunes.

6.2.1 Case Study

Axie Infinity, a popular blockchain-based game, has managed to create a thriving economy by attracting a diverse set of personas, including players, builders, developers, investors, and NFT collectors. The game's economy is based on several key aspects, such as market design, mechanism design, token design, and user-generated content (UGC). The main value creation activities within the game include player-versus-player (PvP) and player-versus-environment (PvE) gameplay, breeding Axies, and earning Smooth Love Potion (SLP) and experience (EXP) through various tasks and gameplay.

To maintain a sustainable economy, Axie Infinity must balance user growth with inflationary asset pressures. The game's economy relies on the value created by fun gameplay, which retains users and encourages the use of SLP or Axie Infinity Shards (AXS) for further value creation. The game's developers must manage levers of monetary and fiscal expansion and contraction, with the ambition of fostering long-term growth.

Long-term growth strategies for Axie Infinity include increasing the usability of SLP, managing the supply of Axies to support breeding, and implementing land mechanics correctly to avoid an extraction-focused incentive for landowners. Short-term growth strategies include increasing daily active users (DAUs), managing daily SLP minting, and reducing botting or exploitable loopholes. To ensure actual users' playability, Axie Infinity should allow Axies to retire, manage the supply of Axies by affecting breeding rates, and focus on users who appreciate gameplay.

6.2.2 The Exploit

Axie Infinity faces challenges in focusing on user-base growth and attracting users who are more interested in economics than gameplay. The game's economy may exhibit Ponzi-like behavior, where value is created mainly by new players entering the space due to a lack of value sinks.

The initial idea of using token rewards as an incentive mechanism for in user acquisition. However, this resulted in attracting the users who are more excited by the prospect of earning tokens through gameplay than playing the game itself. This led to an overinflation of tokens, especially when a large number of users join the ecosystem back in 2021.

The problem with this approach is that it often attracts the wrong kind of users, who are more interested in the financial incentives than actually engaging with the game. As a result, these users tend to dump their tokens in the secondary market once they accumulate a significant amount, leading to a negative feedback spiral. The continuous dumping of tokens devalues the in-game currency, making it less attractive for players to earn tokens and ultimately leading to even more dumping.

To mitigate these issues, it is essential for Axie to evolve and update their incentive mechanisms. While using tokens as incentives can be effective for initial user acquisition, it is crucial to also incorporate retention strategies that focus on creating long-term value for users. This way, the platform can maintain a healthy balance between attracting new players and ensuring existing users remain engaged and committed to the game's long-term success.

6.2.3 Solution: Economy Parameter Adjustment

To counteract these issues, Axie Infinity should increase token utility, reduce token supply, focus on attracting new entrants, and emphasize long-term value creation. This can be achieved by tuning various parameters within the game. For SLP, energy requirements, EXP acquisition, and daily quests can be adjusted to balance skill and participation incentives. For Axies, growth of the user-base, supply of Axies, and breeding rates should be carefully managed to ensure a healthy economy. AXS usage can be diversified by promoting user-generated content through land mechanics and implementing taxes paid in AXS (Martin, 2022a, b).

In conclusion, the Axie Infinity economy is a live system that requires constant adjustment and balancing of various forces, including resources, assets, and value creation activities. By growing these elements proportionally and maintaining a focus on both short-term and long-term growth, Axie Infinity can continue to thrive as a popular blockchain-based game with a sustainable and dynamic economy.

6.3 Case Study 3: Bancor's Insurance Mechanism and Celsius' Exploitation

Decentralized finance (DeFi) has experienced tremendous growth in recent years, bringing forth various innovative solutions and financial tools. However, with this innovation comes challenges in the form of exploits and unforeseen consequences. This essay will examine the case of Bancor's insurance mechanism and how Celsius, a crypto lending platform, exploited it.

6.3.1 Case Study

Bancor (now known as Carbon) is a decentralized liquidity protocol that enables users to convert tokens without the need for an order book or a counterparty. Bancor introduced the concept of a "bonding curve," which is a mathematical formula used to determine the price of a token in relation to its supply. In the Bancor system, the

bonding curve ensures that the price of a token will automatically adjust based on its supply and demand, providing continuous liquidity for users.

The Bancor bonding curve is instrumental in maintaining a fair and transparent pricing mechanism for tokens. It allows for instant token swaps and reduces slippage, which is the difference between the expected price of a trade and the actual price at which the trade is executed.

Bancor V2.1 and Impermanent Loss Insurance

To address the issue of impermanent loss, Bancor launched its V2.1 upgrade (Bancor, 2021), which introduced an insurance pool against impermanent loss. Impermanent loss occurs when the price of tokens in a liquidity pool changes relative to each other, leading to a potential loss for liquidity providers when they withdraw their tokens from the pool.

Bancor's insurance mechanism aimed to compensate liquidity providers for potential impermanent losses by allocating a portion of the swap fees generated by the protocol. This innovative solution was designed to attract more users to provide liquidity to Bancor pools and reduce the risks associated with impermanent loss.

6.3.2 *The Exploit*

Celsius is a centralized crypto lending platform that allows users to earn interest on their crypto assets by lending them out to borrowers. Celsius identified a potential exploit in Bancor's insurance mechanism and attempted to take advantage of it (Peckshield, 2022). The exploit involved leveraging the insurance pool mechanism and attempting to short the system, essentially profiting from the impermanent loss insurance provided by Bancor.

This exploitation was possible through a composite economic building block that combined elements of both DeFi and CeFi (centralized finance). Celsius aimed to profit from the difference between the interest rates on their platform and the impermanent loss compensation provided by Bancor, essentially creating a risk-free arbitrage opportunity.

6.3.3 *Solution: Bancor's Response to the Exploit*

In response to Celsius' exploitation of the insurance mechanism, Bancor took swift action to protect its users and the integrity of its platform (Nagarajan, 2022). Bancor paused the insurance pool and shifted to a new economic model to prevent further exploitation. This move demonstrated Bancor's commitment to addressing unforeseen challenges and adapting its protocol to ensure the security and stability of its ecosystem.

The new economic model employed by Bancor sought to address the shortcomings of the previous model and prevent bad-faith behavior from actors like Celsius. By adjusting the insurance mechanism and implementing additional security measures, Bancor aimed to provide a more robust and secure environment for its users.

The case study of Bancor's insurance mechanism and Celsius' exploitation highlights the challenges faced by DeFi protocols in the rapidly evolving world of decentralized finance. While Bancor's innovative approach to addressing impermanent loss was commendable, it also exposed vulnerabilities that were exploited by Celsius.

Bancor's response to the exploit showcases the resilience and adaptability of DeFi protocols in addressing unforeseen challenges.

6.4 Opportunities and Threats with AI

Artificial Intelligence (AI) has transformed various industries and sectors, and the field of economics is no exception. Chatgpt might not be ready not to design and create a robust economy system, but it sure has the potential to revolutionize the way we understand, analyze, and mitigate economic risks. However, with these advancements come potential threats that need to be considered.

6.4.1 Opportunities

1. Data-driven recommendations for token allocation: AI models can analyze market trends and historical data to provide accurate and efficient recommendations for token allocation. This can lead to better decision-making in token investment and distribution, maximizing returns and minimizing risks.
2. Recommendations for economy design: AI models can analyze historical data and market trends to suggest improvements in economic designs. By employing game theory, AI can identify optimal strategies for economic actors, leading to a more efficient and stable economy.
3. Goal-oriented recommendations: AI models can provide data-driven recommendations to achieve specific goals based on historical data and market trends. Predictive analytics capabilities allow AI to forecast potential future outcomes, enabling decision-makers to make more informed choices and mitigate risks proactively.
4. Pattern recognition and prediction: With the vast amount of data available on-chain, AI can identify user behavioural patterns and predict possible upcoming economic events. This proactive approach allows for early identification of potential risks and the implementation of preventive measures to minimize their impact.

6.4.2 *Threats*

1. Qualitative and cultural norms in the economy: AI models may struggle to account for qualitative and cultural factors that influence economic decisions. While AI training on data can improve over time, it may not always accurately capture the intricacies of human behavior and decision-making processes.
2. Bots exploiting systems: AI-driven bots can exploit vulnerabilities in economic systems, leading to unintended consequences and potentially destabilizing the economy. This is evident in games, and in the wider context of financial legos in DeFi, that can be dangerous. This threat highlights the importance of robust security measures and constant monitoring to protect against malicious AI-driven activities.
3. Over-reliance on AI: As AI continues to improve and provide more accurate recommendations, there is a risk that human decision-makers may become overly reliant on AI-driven insights. This over-reliance could lead to complacency, reducing the ability of decision-makers to think critically and independently, which is essential in effectively managing economic risks.
4. Bias in AI models: AI models are trained on historical data, which can be inherently biased. If not properly addressed, these biases can be perpetuated and even amplified in AI-driven recommendations, leading to unfair and potentially harmful economic outcomes.
5. Concentration of power: The development and deployment of AI technologies are often dominated by large token holders who vote on economic decisions based on how it can benefit them. This concentration of power may result in an unequal distribution of benefits, exacerbating existing inequalities and posing a threat to the overall stability of the economy.
6. Lack of transparency: The complexity of AI algorithms can make it difficult for users and regulators to understand how AI-driven recommendations are generated. This lack of transparency can lead to a loss of trust in AI-driven insights and pose a barrier to the widespread adoption of AI in economic risk management.
7. Misinterpretation of AI-driven insights: The insights generated by AI models can be complex and challenging to interpret. Decision-makers may misinterpret these insights, leading to suboptimal decisions and increased economic risks. This can be dangerous when large token holders skew the votes toward their preferences.
8. Insufficient regulation: The rapid pace of AI development may outstrip the ability of regulators to develop appropriate oversight mechanisms. This could result in unforeseen negative outcomes ranging from financial instability to biased decision making by AI systems. In the absence of a regulatory framework, malicious actors can exploit vulnerabilities in the system for personal gain which undermines trust and integrity of the system. A simple regulation could take the form of mandatory financial audit for public companies. In the same vein, mandatory economic audits can be enforced as a checkpoint to understand the current state of growth of both the specific economy and overall macro token-based economy.

6.5 10 Economic Risk Metrics Considerations

With the availability of comprehensive and transparent data thanks to validation on blockchain, it becomes possible to measure the health of an economy using a wide range of metrics. Here are ten such possible metrics that can be developed.

1. **Total Transaction Volume:** This metric measures the total value of all transactions within the token economy over a given period. It provides insights into the overall activity and usage of the token, indicating the level of economic activity in the system. A healthy token economy will show consistent or increasing transaction volume over time.
2. **Number of Active Addresses:** This metric calculates the total number of unique addresses that have participated in transactions within a given period. A high number of active addresses indicates a diverse and engaged user base, which is a positive sign of a healthy token economy.
3. **Token Circulation:** Token circulation measures the movement of tokens through the economy, taking into account factors such as transaction volume, token velocity, and token age. A high token circulation implies that tokens are being actively used, exchanged, and held by participants, which is indicative of a healthy token economy.
4. **Network Value to Transaction (NVT) Ratio:** The NVT ratio compares the market capitalization of a token to its transaction volume. A low NVT ratio suggests that the token is undervalued relative to its usage, while a high NVT ratio may indicate overvaluation. A stable or decreasing NVT ratio over time can be a positive sign of a healthy token economy.
5. **Wallet Gini Coefficient:** The Gini coefficient measures income or wealth distribution within an economy, with values ranging from 0 (perfect equality) to 1 (perfect inequality). A low Gini coefficient indicates a more equal distribution of tokens, which can be a sign of a healthy and inclusive token economy.
6. **Token Velocity:** Token velocity measures the rate at which tokens are exchanged within the economy. A high token velocity implies that tokens are being actively used for transactions, which can be indicative of a healthy and vibrant token economy. Conversely, a low token velocity may suggest that tokens are being hoarded or not being used effectively.
7. **Token Utility Ratio:** This metric compares the utility value of a token (i.e., its use in transactions, staking, or governance) to its speculative value (i.e., its market price). A high token utility ratio indicates that the token is being primarily used for its intended purpose, which can be a sign of a healthy token economy.
8. **Inflation Rate:** The inflation rate measures the rate at which new tokens are issued or created in the economy. A moderate and predictable inflation rate can contribute to a healthy token economy by encouraging spending and investment while preventing deflationary spirals.
9. **User Retention Rate:** The user retention rate measures the percentage of users who continue to participate in the token economy over a given period. A high

user retention rate indicates that users find value in the ecosystem and are likely to continue using the token, contributing to the long-term health of the token economy.

10. **Decentralization Index:** The decentralization index measures the distribution of power and influence within the token economy, taking into account factors such as the concentration of token holdings, the number of validators or nodes, and the distribution of governance power. A high decentralization index suggests that the token economy is resistant to centralized control and manipulation, which can be a sign of a healthy and resilient ecosystem.

These are just simple and basic metrics that can be used to glimpse an insight of how healthy the economy of the protocol is.

In conclusion, the advent of Web3 economies has provided us with unparalleled access to transparent and public data, allowing for more accurate and insightful analysis of token economies. As a result, we can now evaluate the health of these economies using a range of metrics that capture various aspects of their functioning. By analyzing metrics such as total transaction volume, number of active addresses, token circulation, and user retention rate, we can gain insights into the overall activity, engagement, and stability of a token economy.

Furthermore, the analysis of metrics such as the Gini coefficient, token utility ratio, and decentralization index can provide valuable information about the inclusivity, resilience, and distribution of power within the token economy. These factors contribute significantly to the long-term health and sustainability of a token ecosystem. It is crucial to continually monitor and assess these metrics to identify potential issues and take corrective actions as needed.

Additionally, understanding the potential threats and opportunities of AI in analyzing token economy health can help stakeholders make informed decisions. AI models can provide data-driven recommendations, predictive analytics, and pattern recognition that can help identify potential problems before they escalate. However, it is essential to be aware of the potential risks associated with AI, such as the exploitation of systems through bots or the misinterpretation of qualitative and cultural norms.

In this new era of transparent, data-driven economies, it is vital for stakeholders to remain vigilant and adaptive to maintain the health and integrity of token economies. By leveraging the available data, employing AI models responsibly, and closely monitoring key metrics, we can foster the growth and development of robust, sustainable token economies that benefit all participants. Ultimately, the success of Web3 economies will depend on our ability to harness the power of data and technology while prioritizing the needs and interests of the diverse users that make up these ecosystems.

6.6 Why Should We Care

The security of a token economy is essential to the success of the system. Tokens that are poorly designed can cause a death spiral and can quickly lead to chaos and undermine the entire system. This chapter uses case studies in DeFi, games, and CeFi to discuss the risks associated with the token economy.

We care about token economics because it provides the operating manual of how this economy works. From there, we can identify how to best secure this economy, and where security should be enhanced. As mentioned excessively in this chapter, token economics defines the rules of this economy and the ecosystem of how people should behave and who should join. This is absolutely important as it is the first layer of security pre-event happening, to understand the risks and protect against the downside.

The rules of the economy also include rules of how trade and transaction work. Trade and transact assets that represent value. We call them tokens. When it comes to the assets in the economy, whether tradeable or not, we call them tokens. Tokens are anything that capture value. We define the rules in which these tokens should follow.

Token economics is a new field in economics that looks into the incentive design and mechanisms of tokens based ecosystems. It is defined by the general framework used to design the incentives of the system. A token represents the intrinsic value of the ecosystem. When it is traded on secondary markets, it undergoes price discovery to determine the extrinsic value. The goal of token economics is to define, design, and build the intrinsic value. While it is possible to use the token economics framework in Layer 1 and Layer 2, we primarily focus on its use in the Dapp layer. The focus of the economic design of the token is around the environment and rules in which the economic agents, tokens, and institutions will interact and transact by. Once we know how rules are designed, we can better improve, maintain, or change the economic rules and potential exploits.

References

- [ARC] Repay excess debt in CRV market for Aave V2 ETH. (2022). *Aave - Governance forum*. Retrieved from <https://governance.aave.com/t/arc-repay-excess-debt-in-crv-market-for-aave-v2-eth/10779>
- Bancor. (2021). *Bancor v2.1 staking guide*. Bancor. Retrieved from <https://blog.bancor.network/bancor-v2-1-staking-guide-749e5cc4326a?gi=1ce3fb3a12c9>
- Compound | Proposal Detail #135. (2022). *Compound finance*. Retrieved from <https://compound.finance/governance/proposals/135>
- Martin, L. (2022a). *How Web3 Blockchain gaming formalized informal Web2 gaming trade mechanisms*. Economics Design Newsletter. Retrieved from <https://www.newsletter.economicsdesign.com/p/how-web3-blockchain-gaming-formalized>

- Martin, L. (2022b). *Axie infinity mechanism design: Before and after*. Economics Design Newsletter. Retrieved from <https://www.newsletter.economicsdesign.com/p/axie-infinity-mechanism-design-before-and-after>.
- Nagarajan, S. (2022). *Bancor uses 'emergency powers' to fight 'hostile antagonist'*. Blockworks. Retrieved from <https://blockworks.co/news/bancor-describes-hostile-antagonist-behind-impermanent-loss-defense>
- Peckshield. (2022). Retrieved from <https://twitter.com/PeckShieldAlert/status/1541604014248169473>
- Sandor, K. (2022). *Mango exploiter's funds get liquidated after roiling Aave using \$20M of borrowed curve tokens*. CoinDesk. Retrieved from <https://www.coindesk.com/markets/2022/11/22/mango-exploiter-gets-liquidated-after-roiling-aave-using-20m-of-borrowed-curve-tokens/>
- Sandor, K. (2023). *DeFi protocol Aave clears bad CRV token debt from exploit attempt*. CoinDesk. Retrieved from <https://www.coindesk.com/markets/2023/01/26/defi-protocol-aave-clears-bad-crv-token-debt-from-exploit-attempt/>

Part II

Security Concerns for Enterprise Web3 Application Development

The adoption of Web3 technology in enterprise applications necessitates the highest level of security and robustness. To achieve this, enterprises must embrace DevSecOps, utilize advanced data analytics and monitoring tools, ensure data authenticity, and explore the unique security concerns associated with permissioned blockchains. Part 2 of this book delves into these crucial areas, providing a comprehensive understanding of the security concerns associated with enterprise Web3 application development.

Chapter 7 discusses the essential role of DevSecOps in Web3 application development, highlighting the integration of development, security, and operations. The chapter emphasizes the need for higher security standards in Web3 applications and provides practical insights into introducing DevSecOps into Web3 development.

Chapter 8 offers a comprehensive overview of on-chain analytics and monitoring in the Web3 ecosystem, discussing both preventive and reactive approaches to security and risk management. It explores key concepts, techniques, and principles of on-chain analysis, emphasizing the importance of balancing proactive and responsive strategies in a decentralized digital economy.

Chapter 9 provides an in-depth exploration of data authenticity in the Web3 ecosystem using blockchain oracles. It discusses various types of blockchain oracles, use cases, design considerations, and security attacks, along with their countermeasures. This chapter is an invaluable resource for understanding the importance of oracles in blockchain networks and how to design and secure them effectively.

Chapter 10 delves into the unique security concerns associated with permissioned blockchains, which are commonly used in enterprise applications. It covers architecture design considerations, strategies for onboarding new nodes, node verification, and removal processes. This chapter also emphasizes the importance of securing individual nodes, communication between nodes, and synchronizing on software and smart contract upgrades.

By the end of Part II, readers will have a deep understanding of the security concerns associated with enterprise Web3 application development. Armed with this knowledge, they will be better equipped to navigate the complexities of

decentralized technologies, ensuring the security, resilience, and success of their enterprise Web3 applications.

Chapter 7

DevSecOps for Web3



Ken Huang

DevSecOps stands for development, security, and operation. DevSecOps is an evolving application development methodology and process used by many BigTech companies, FinTech companies, and government agencies such as the US Department of Defense (DoD, 2019a, 2019b). In fact, recent Gartner research indicated that DevSecOps is no longer a consideration—it is a necessity (Gartner Research, 2022).

What DevSecOps has to do with Web3? There are a few reasons why DevSecOps is very important for Web3 applications.

First, the Web3 application with public blockchain as a backend enjoys real-time transaction settlement and immutability which requires a financial system level of security before any transactions can be sent to the blockchain. In the traditional financial system, there is a “charge-back” possibility. “Charge-back” means reversing a transaction if the transaction is proven to be fraudulent. There is no “charge-back” possibility for transactions recorded on the chain. This calls for the Web3 development team to adopt higher security standards than the traditional financial system.

Web3 application team can benefit from the DevSecOps process to identify security during the early stage of Web3 application development and continue the process during the development phase using automated security tools and application build pipelines to identify security bugs during the build phase and also using good analytics and monitoring tools to alert fraudulent on-chain activities.

Second, the DevSecOps process is unfortunately not widely used among Web3 projects due to a lack of awareness of this process and the lack of skill set of DevSecOps professionals.

K. Huang (✉)
DistributedApps.AI, Fairfax, VA, USA
e-mail: Ken@Distributedapps.ai

Third, Web3 still leverages a lot of Web2 technologies. For example, the front end of Web3 applications is mostly developed with React.js and hosted in a cloud provider environment such as AWS cloud. The middle-tier server to process the front-end request before sending it to the blockchain using either.js framework may also be hosted in a centralized cloud environment. Some of these Web3 applications may even have a user database to record user profiles for various reasons such as custom relationship management, “Know Your Customer” requirements, targeted advertising, etc. These centralized databases will still get attacks from hackers. The fact that there is a blockchain backend does not eliminate the need for DevSecOps, instead as stated before, this requires higher security standards than traditional financial systems.

For example, security researchers have already found many security vulnerabilities in the decentralized version of Twitter called Mastodon. The attack involved abusing Chrome’s autofill feature to steal users’ stored credentials by getting the targeted user to click on a malicious element on a page and a vulnerability that allows a remote attacker to gain unauthorized access to sensitive information (Kovacs, 2022).

This chapter will discuss what DevSecOps is and how to introduce DevSecOps into Web3 application development and some sample security tools for getting the level of automation needed for successful DevSecOps for Web3.

7.1 What Is DevSecOps?

From a broad perspective, DevSecOps combines methodologies, analysis, philosophies, cultures, practices, and tools that enhance the security and reliability of applications and implement applications at a faster pace than using traditional software development processes.

It should be noted that DevSecOps also provides greater flexibility for development teams, IT security teams, and operation teams who work together on operational activities throughout the entire process. At the core of the DevSecOps approach, the IT security team plays an essential role in adding security controls into the application development life cycle leveraging security requirements gathering, security architecture, security design, security engineering, and security monitoring elements.

By integrating security early into the development process (also called the “security shift to the left” process), the project team can catch security vulnerabilities early and fix them before they become a problem. This increases the security of the application and reduces the chances of a security breach.

DevSecOps can help the project team to improve the efficiency of the development process by automating tasks and speeding up the development process. Moreover, DevSecOps can reduce costs by integrating security early into the development process. Indeed, DevSecOps can reduce the cost of fixing security vulnerabilities (reduced security debt) and improve the overall security of your application.

In some legacy IT companies, IT activities and responsibilities are somewhat segmented. For example, developers are responsible for programming applications while infrastructure is responsible for taking care of systems environments and deploying them in production. Security, on the other hand, is delegated to another specific team that acted alone in the final stage of development.

This legacy development process (or waterfall development process where each development stage is sequential and isolated) made it difficult to mitigate a problem in the production environment. That is because developers typically did not have direct access to it. Infrastructure analysts often did not have the slightest knowledge about applications. And security only had visibility of possible vulnerabilities practically at the end of the process and usually without knowing any context related to the role that application has within the company’s business. Therefore, due to these factors, it was difficult to resolve problems that were often basic and could be easily solved or minimized if there was greater transparency and unity between the areas.

With the DevSecOps process (one example is the process adopted by the US Department of Defense in Fig. 7.1), the project team can have effective implementation guarantees fast, secure, and frequent development cycles, often lasting weeks or days, where the focus is to deliver products in an optimized, transparent, and collaborative way. In this way, when working with incremental deliveries, development teams are able to deliver products faster and more securely.

As shown in Fig. 7.1, DevSecOps is a continuous and circular development process that is different from legacy waterfall development processes. Security is introduced early in the planning phase and requirement phase of the development process. Security scanning tools are used during the development process, and security monitoring tools are used during the operation stages. The process is agile and iterative, allowing fast feedback loops and uncovering security vulnerabilities early in the development process.

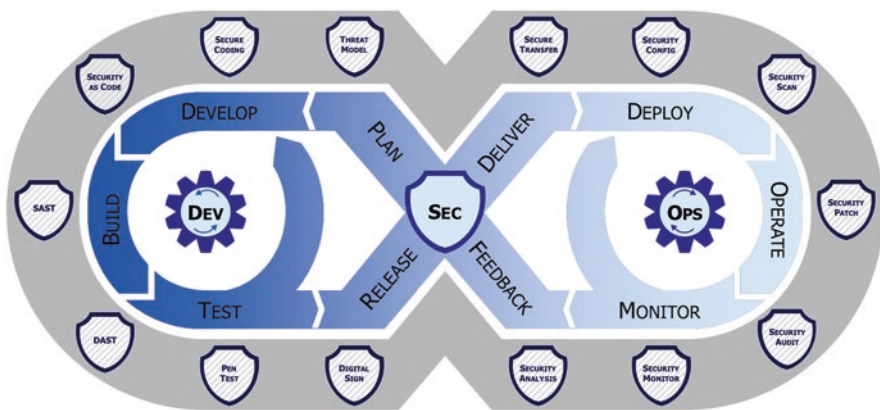


Fig. 7.1 DevSecOps. Source: DoD DevSecOps Unclassified (DoD, 2019a, 2019b)

So DevSecOps means thinking about application and infrastructure security from the beginning, throughout the entire development cycle. It also means automating some security activities to avoid slowing down the development process.

There are different ways to incorporate security into DevSecOps, such as implementing security tools in an integrated development environment (IDE), in application build *pipelines* with the option to break the build to disallow the code commit which may have highly vulnerable code. However, effective security in DevSecOps requires more than new tools: it must build on the cultural changes which integrate security into all stages of application development.

7.2 How to Integrate DevSecOps into Web3

The speed of innovation in Web3 is astonishing and this can be echoed with many IT workers leaving BigIT to join Web3 startups and contentious project development in DeFi and NFT as well as layer 2 roll-up technology in the Ethereum ecosystem.

Unfortunately, the security and the important process of DevSecOps are missing from most Web3 startups and projects.

In this section, we will highlight some steps needed for integrating DevSecOps into the Web3 application development process.

Web3 DevSecOps contains security activities ensuring that the best practice of discovery, remedy, and prevention is an ongoing circular process for security posture. This ongoing circular process is composed of 4 intertwined phases. As shown in Table 7.1, each process has its set of security activities that need to be conducted for overall Web3 application security postures.

Table 7.1 Web3 DevSecOps Phases and Key Security Activities

Web3 DevSecOps Phases	Key Security Activities
Requirement and design phase	Security requirement gathering Technical threat model DataFlow model Token economic model Financial security model
Implementation phase	CI/CD pipeline integration with SAST, SCA, secret scanning, DAST IDE tool extension Security code review
Testing and external validation phase (testnet phase)	Formal verification Third-party security auditing (not just Solidity code, must include all code) Bug Bounty
Production (mainnet) phase	Continuous Bug Bounty Logging/auditing Monitoring/alerting

These four phases are iterative and not sequential in the traditional waterfall process. So, we can alternatively use the term “component” instead of “phase.” But for the sake of simplicity, we will continue to use the term “phase.” Readers need to keep in mind that these phases are intertwined and iterative.

7.2.1 DevSecOps during Requirement and Design Phase

During the Requirement and Design Phase, the security activities include one or all of the following:

- Security requirement gathering
- Technical Threat Model
- DataFlow Model
- Token Economic Model
- Financial Security Model

In order to perform these security activities, the participants must include project owner, technical team leader, security architect, and business functionality analyst.

There are two documents that must be provided as input to the security activities.

7.2.1.1 Web3 Product Description and Requirement Document

Product documents describe the main functionality and user stories of the Web3 product, including the integration with third-party APIs. For example, for a decentralized exchange(DEX) aggregator application, the product document can describe a DEX aggregator as the product which sources liquidity from different DEXs and thus offer users better token swap rates than they could get on any single DEX. DEX aggregators have the ability to optimize slippage, swap fees, and token prices which, when done right, offer a better rate for users. The document must describe which DEXs the aggregator uses to get liquidity and price quotes and which APIs are used to get price quotes. The product document also needs to specify if there is a utility token or governance token.

Usually, the Web3 project team can use a white paper as a product description document if the document specifies the third-party APIs and on-chain access logic since these are very important for the security.

7.2.1.2 Web3 Architecture Document

Web3 architecture documents should describe the high-level architecture of the product, as well as the security requirements and controls.

The following is the list of security controls that must be explained in this architecture document:

Authentication

Which authentication protocol is used? For example, use walletconnect.com to connect the user's wallet to your product. A pure Web3 product should only need to authenticate the user using the decentralized nature of authentication without adding a user to a centralized database. But, if you have the business needs and justification to add the user into a centralized database, you need to describe how the user is added into what kind of database and what information you will gather from the users. If you collect Personal Identifying Information (PII), you may have to encrypt them in transit and at rest to meet security compliance requirements such as PCI/DSS and SOC2 (Reciprocity, 2020) down the road.

Authorization

Does the Web3 application support different levels of access for different users? Who is responsible for managing who has access? How do users grant and revoke access? How do we ensure that users only have access to data that they should (e.g., not data from other customers)?

For example, your Web3 application may leverage smart contracts for access control. The smart contract can specify who is the owner of the contract, and who is the administrator who can modify access for the external address. Who can pause the contract in emergency cases? Who can change parameters or configuration settings of the Web3 application such as the staking rate, interest rate, insurance prime, adding or removing liquidity pools, etc.? These all depend on the nature of your Web3 application. Also, it is very possible that your Web3 application has a Decentralized Autonomous Organization (DAO) to manage the Web3 application and its access control via on-chain or off-chain governance. If so, the DAO mechanism must be fully documented and the decision-making process (such as using quadratic voting) (Forbes, 2018) should be transparent and accessible to all stakeholders.

Auditing, Logging, Monitoring, and Alerting

Using Ethereum blockchain as examples. For each transaction, an event can be emitted so the transaction can trigger other workflow processes within your Web3 application and also allow third-party analytic tools to analyze the events. As shown in Fig. 7.2, events are not stored in the transaction nor on the blockchain. They are stored within the transaction receipt. TX receipts are stored in the Receipts Trie by the node. Further, the root of the receipts tree is stored on-chain in the block header.

Web3 applications can use both transaction data and events data for auditing and logging purposes. If your Web3 application also contains a centralized front-end or middle-tier user profile database, you will need to add additional layers of logging and auditing which will be helpful if there are any security incidents.

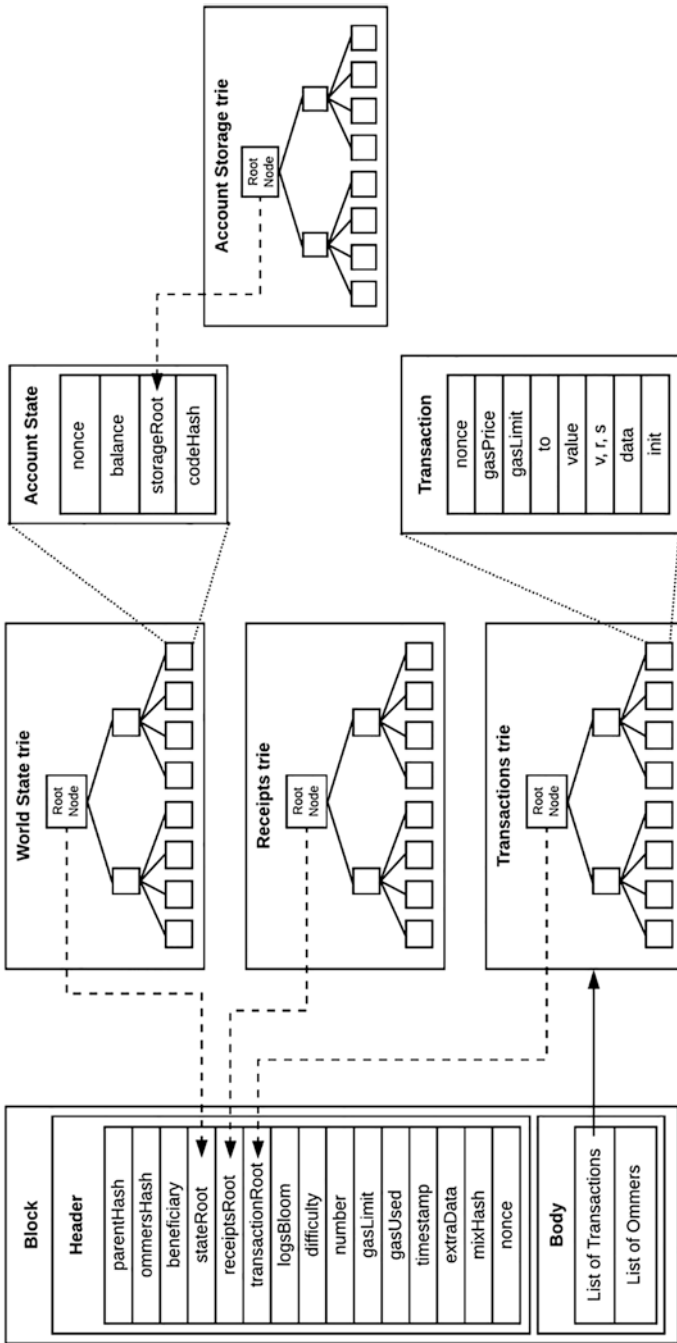


Fig. 7.2 Block, transaction, account state objects, and Ethereum tries (Saldanha, 2018)

Web3 project team can also leverage third-party products such as Chainalysis, Nansen, or Elliptic.co for additional capabilities in security monitoring and compliance.

Web3 API Security

Web3 applications mostly will leverage Rest API or GraphQL API to access on-chain or off-chain data or even use API to initiate on-chain transactions. It is important to make sure there is security validation logic and output encoding logic to avoid some of the top ten security risks documented by the Open Web Application Security Project in terms of API vulnerability. The following figure illustrates the top 10 API security risks. As you can see, access control at the data object level is the top security risk. For more details, please refer to the website: <https://owasp.org/www-project-api-security> (Fig. 7.3).

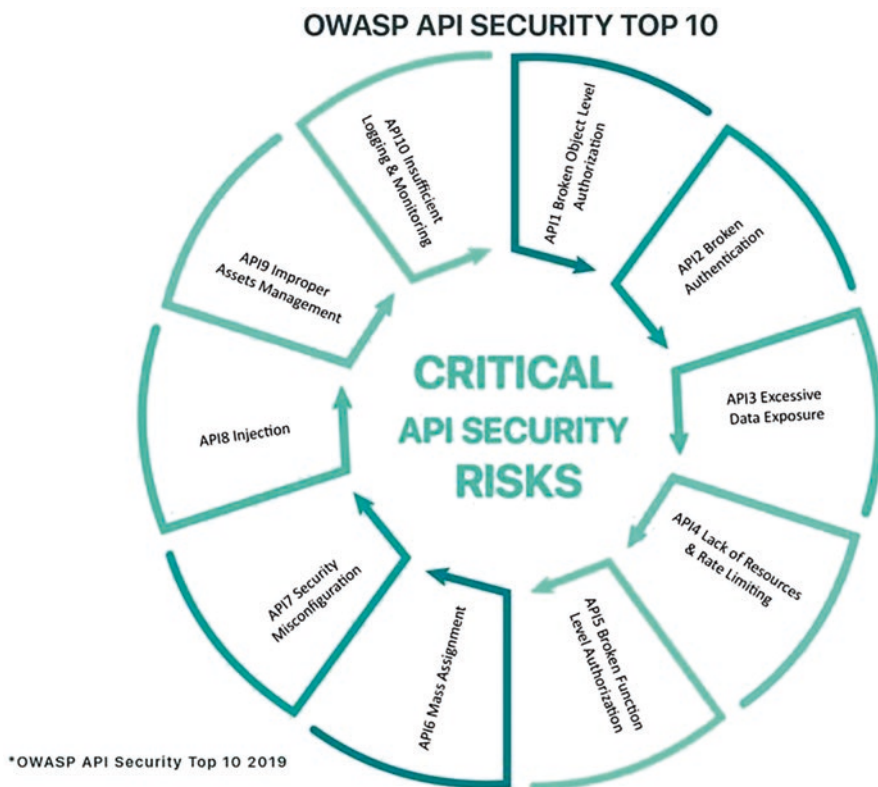


Fig. 7.3 OWASP API Security Top 10

The architecture document should include the approaches used to enhance API security such as using API gateway, enforcing fine-grained access control, and encryption of sensitive data.

7.2.1.3 Security Requirement Gathering

This is an ongoing process. The “shift to left” security culture emphasizes the initial involvement of security requirements at an early stage of the Web3 application development and then continues through the DevSecOps process.

With the input from the production description document and the architecture document, the security requirements can be collected with the main focus on authentication, authorization, auditing, monitoring, alerting, and data encryption. This will give an initial list of security requirements. To continue gathering more security requirements, it is necessary to conduct technical threat modeling exercises which we will discuss next.

7.2.1.4 Technical Threat Modeling

When performing a security review of a Web3 application one of the most important steps is threat modeling. There is a great deal of documentation on how to perform threat modeling from the existing enterprise IT world and we can leverage these methodologies with some modifications for Web3. The following are a number of different techniques that can be used.

- [OWASP Threat Risk Modelling](#)
- <https://docs.microsoft.com/en-us/learn/modules/tm-introduction-to-threat-modeling/1-introduction>
- [NIST Risk Management Guide](#)

For example, we can use STRIDE (see Table 7.2), which is a [Microsoft threat modeling tool](#).

7.2.1.5 Data or Capital Flow Diagram

Data flow diagram describes how data flows within each component of the application and the security boundary with external systems. In the Web3 application, the data is usually represented by the capital or funds from users to smart contract pools and then back to users. For example, Fig. 7.4 is the capital flow for a Yield Farm application.

This yield farm application has two types of users: Lenders and Borrowers. Of course, due to the peer to peer nature of a Web3 application, a user can be both types of users if he/she wishes. The lender deposits crypto assets and gets the deposit interests. The borrower can request a loan with collateral and if the borrower’s

Table 7.2 STRIDE Threat Modeling Web3 Examples

Threat	Definition	Question	Threat example
Spoofing	Attacker pretends to be someone or something else	Are both sides of the communication authenticated?	The attacker hacked the user's wallet extension to pretend to be someone to trick the victim to send the funds to the hacker. (Godbole, 2020) and (Biggs, 2018)
Tampering	Attacker changes data without authorization	How do I know someone can't change data in transit, in use, or at rest?	Similar to the previous example, the hacker can change the address or transaction amount and steal users' funds. This usually happens when the Web3 transactional API is not secured. (Franceschi, 2021)
Repudiation	Attacker claims to not have done something	Can every action be tied to an identity?	With the pseudonymous nature of blockchain, repudiation attacks on DeFi, DAO, and NFT are a big problem. Using verifiable credentials is a possible solution. (Strack & Martin, 2022)
Information disclosure	Attacker sees data they aren't supposed to see	How do I know someone can't see data in transit, in use, or at rest?	If your Web3 application collects off-chain data, you need good access control for this data. Also, if you want to keep on-chain data security private, you need to use privacy preserving technology.
Denial of service	Attacker brings your system down	Are there areas in the system where resources are limited?	Flooding the Web3 application with requests. (Deka, 2022)
Elevation of privilege	Attacker has unauthorized access to data	How do I know someone is allowed to take this action?	Hackers may explore the "approve" function of smart contracts to steal funds from victims. (Clark, 2021)

collateral is too low, a liquidation process can happen. So, the capital can follow from the Lender to the DeFi smart contract to the Borrower and then back to the lender. The security analysis and threat modeling should look into the crypto flow and find the potential vulnerabilities and attack surfaces. More about threat modeling is in the previous section of this chapter.

7.2.1.6 Token Economic Model

The Web3 application can design many different token security models with a single token or multiple tokens. The security of the token model has to do with the economics, legal, and game theory aspects of token design. The main goal for security is to have a token model which is sustainable and conducive to ecosystem

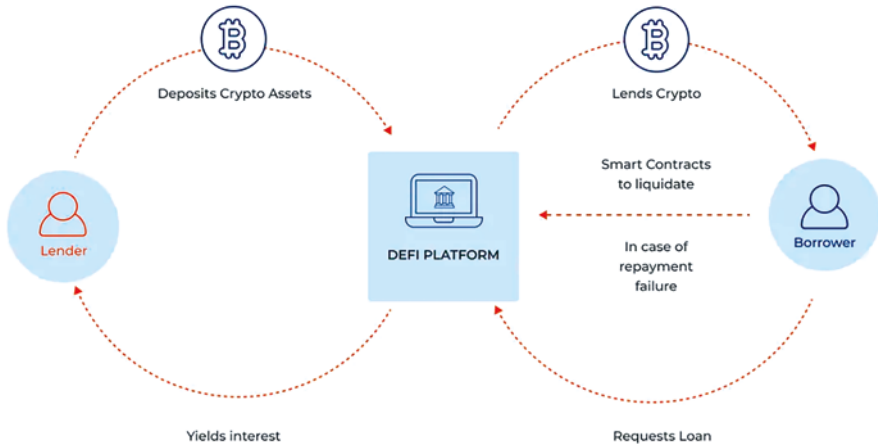


Fig. 7.4 Yield Farm DeFi application Capital Flow Diagram

development. Any token model which is based on the Ponzi scheme is not sustainable and thus is not secure. We have discussed this in more detail in Chaps. 5 and 6.

7.2.1.7 Financial Security Model

Financial security has to do with liquidity mining mechanism, flashloan attack resistance, DAO incentive model, duration management for the fixed-income asset, diversity of investment and staking mechanism, etc.

We will use the liquidity mining mechanism and flashloan attack resistance as examples:

In terms of the liquidity mining mechanism, it is strongly suggested to use it only as an initial marketing and user acquisition phase, it can allow an initial high yield for the early phase of the project to incentivize the user to participate. The Web3 project should notify the user upfront about the liquidity mining mechanism and the overall return over a period of time with reduced yield for late participants. For example, the project team can use Bitcoin’s half schedule to reduce the yield after a certain number of years so the total amount of awards to be distributed can converge to a capped amount instead of a risky amount of issuance which can cause systemic risk for the Web3 application in question.

The application also needs to be designed with flash loan attack resistance. A flash loan is an unsecured loan, where the whole lending and returning process occurs within a single block on the blockchain. The loan does not need collateral and guarantors provided that the principal and interests are returned to the pool within a single transaction block. If this fails to occur, the whole transaction is reversed with no penalty except the gas fees used in the transaction. This guarantees the safety of the funds in the reserve pool.

Flash loan attacks are relatively common because they are easy for a hacker to perform and low-risk due to the fact that the hacker needs a relatively small amount of funds and can remain anonymous during the attack. Flashloan attack includes manipulating asset prices in order to take advantage of arbitrage opportunities on DeFi services that would not otherwise have existed. In short, due to the theoretically infinite size of the loan, the attacker is able to “increase demand” and raise the price. They can make a trade just like any other arbitrage opportunity, then pay off the loan and keep the profits.

To design a flashloan attack-resistant application, we suggest the following:

1. Make your smart contract simple and verify all external calls

Complexity comes with risk. While developing a large smart contract or building a dApp it is difficult to pinpoint loopholes. Therefore, all external calls should be located, and explore if these could serve as a path for the malicious actors in the contracts.

2. Use a decentralized oracle

Oracle manipulations are the biggest cause of flash loan attacks. Smart contracts heavily rely on oracles which provide an effective interface between the contracts and the external source to push the required data. Decentralized Oracles like Chainlink gather data about prices from multiple sources, which reduces the likelihood of a single data point influencing the oracle. If a platform relies solely on the data of one particular DEX, then its data is at risk of being flawed. Hackers could directly manipulate the price of the singular DEX.

7.2.2 *Implementation Phase*

During the implementation phase, we suggest using some level of automation consisting of using tools and techniques that can ensure continuous code integration. This process, along with continuous delivery, allows development teams to spend less time on manual activities so they can focus on other important activities.

Some of the notable tools used in the DevSecOps include the following categories (Table 7.3):

7.2.2.1 **CI/CD Pipeline Security Tools Integration**

What Is a CI/CD Pipeline?

Continuous integration and continuous deployment (CI/CD) pipeline is a series of steps that must be performed in order to deliver a new version of the software. CI/CD pipelines are a practice focused on improving software delivery throughout the software development life cycle via automation.

Table 7.3 Security Tools used during Web3 Application Implementation Phase

Tool category	Description
SAST (Static application security testing)	Scan source code to find vulnerabilities
DAST (Dynamic analysis security testing)	Scan and find security vulnerabilities in web applications while they are running in production.
IAST (Interactive application security testing)	Deploy agents and sensors in running applications and continuously analyzing all application interactions initiated by manual tests, automated tests, or a combination of both to identify vulnerabilities in real-time
Secret scanning	Automatic scanning hard coded secrets in the code or configuration files so they can be managed by a centralized secret management tool.
SCA (Software composition analysis)	A software composition analysis tool is used to track open-source components, identify potential security and license compliance threats, and give security and development teams a path to remediation before problems have negative reputational, IP, or monetary impact.

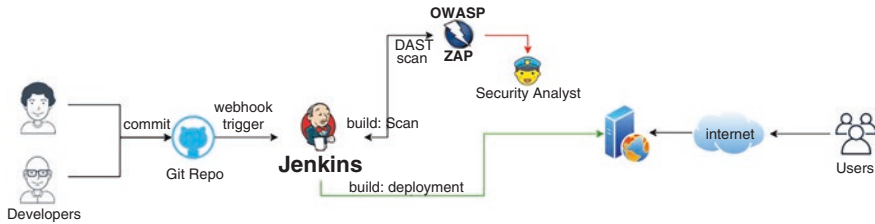


Fig. 7.5 Sample CI/CD Pipeline integration with Security Tools

There are many different ways of integrating security tools with CI/CD pipelines depending on the repository tool and integration tools used. The following diagram (Fig. 7.5) is one such example using open-source security tool ZAP as DAST tool and Jenkins as the build tool to scan the code in the GitHub repository. In addition to the ZAP tool, we can add any number of SAST, DAST, Secret Scanning, and SCA tools. For example, we can add open-source Solidity static security scanning tools such as Slither, Securify, and Mythx.

7.2.2.2 IDE Tool Extension

Most Web3 developers use Visual Studio Code (VSC) or the on-line Remix tool. But tools support static security scanning as an extension and will report potential security vulnerabilities. Developers can choose to fix the vulnerabilities or mark them as false positives. The following is an example of Solidity Smart Contract Static security scanning tool extension in VSC.

This extension was written in Python 3 and can scan a suite of vulnerabilities and annotate potentially dangerous code and suggested fixes. Additional features of the extension include:

- Analyze open workspaces
- Explore results in a custom tree, sorted by issue type or severity
- View results as native Visual Studio Code information/warnings/errors
- See annotations for relevant source code for each issue
- Print detailed issue descriptions and recommendations
- Filter issues by type (per workspace configuration)
- Specify custom solc path (per workspace configuration)
- Solidity Syntax Highlighting

Keep in mind that in addition to the Slither extension for VSC, there are many other Solidity security scanning extensions that developers can find via the VSC extension tool. Other commonly used VSC extensions for Solidity security and visualization include Solidity Visual Developer, Surya, Solgraph, Sol2UML, and Sol Function Profiler.

Using an IDE security extension can increase the security awareness of developers and fix some vulnerabilities at the early stage of code development. Web3 project shall investigate time early in the implementation phase to incorporate security extensions and integrate them into coding.

7.2.2.3 Security Code Review

A security code review is a process where an in-house security expert examines your code for potential vulnerabilities. This can help to identify issues that could be exploited by hackers and help to ensure that your Web3 application is as secure as possible before deploying to the mainnet.

The benefits of a security code review include:

- Identifying and fixing vulnerabilities before they can be exploited
- Reducing the risk of wrong access control logic which can lead to disclosure or modification of critical data
- Preventing financial losses and other damages

Security code review is an ongoing process and any major source code update will require source code review manually by a security expert.

7.2.3 Testing and External Validation Phase (Testnet Phase)

When a Web3 project is implemented, the project team can choose a blockchain to deploy the code. The blockchain that is used for deploying testing code should be the blockchain testnet instead of the mainnet. In this phase, we can conduct code

formal verification, hire an external auditor to conduct a security review of the code, and launch a bug bounty program.

7.2.3.1 Formal Verification

This is a technique used to mathematically prove the correctness of a program. This is a valuable tool, as it can help to detect and fix potential errors in a program before it is deployed. In Web3 application development, formal verification of smart contract code is an important security activity that needs to be conducted.

Formal verification needs a formal model to generate formal specification that can be verified.

A formal model is a mathematical description of a computational process. Programs are abstracted into mathematical functions (equations), with the model describing how outputs to functions are computed given an input. Formal models provide a level of abstraction over which analysis of a program's behavior can be evaluated. The existence of formal models allows for the creation of a formal specification, which describes desired properties of the model in question.

A formal specification is a technical requirement that a particular system must satisfy. In programming, specifications represent general ideas of what the program should do.

In the context of smart contracts, formal specifications refer to properties—formal descriptions of the requirements that a contract must satisfy. Such properties are described as “invariants” and represent logical assertions about a contract's execution that must remain true under every possible circumstance, without any exceptions.

Thus, we can think of a formal specification as a collection of statements written in formal language that describes the intended execution of a smart contract. Specifications cover a contract's properties and define how the contract should behave in different circumstances. The purpose of formal verification is to determine if a smart contract possesses these properties (invariants) and that these properties are not violated during execution.

Formal specifications are critical in developing secure implementations of smart contracts. Contracts that fail to implement invariants or have their properties violated during execution are prone to vulnerabilities that can harm functionality or cause malicious exploits.

Using Solidity smart contract as an example and specifically the function `transfer()` or `transferFrom()` in ERC-20 token contracts, one important specification is that “A sender's balance should be greater than the number of tokens to be sent.” This natural-language description of a contract invariant can be translated into a formal (mathematical) specification, which can then be rigorously checked for validity.

There are various techniques for the formal verification of smart contracts, the following are some examples.

Model Checking

Model checking often uses the state-transition system to evaluate temporal properties. For example, a security property related to access control (e.g., Only the owner of the contract can call the pool Withdraw method) can be written in formal logic. Thereafter, the model-checking algorithm can verify if the contract satisfies this formal specification. Model checking involves constructing all possible states of a smart contract and attempting to find reachable states that result in property violations. However, this can lead to an infinite number of states (known as the “state explosion problem”), hence model checkers rely on abstraction techniques to make an efficient analysis of smart contracts possible.

Theorem Proving

Theorem proving is a method of mathematically proving the correctness of programs. It involves transforming the model of a contract’s system and its specifications into mathematical formulas or logic statements. A theorem prover can prove a smart contract’s model precisely matches its specifications. Theorem proving may need manual work due to the fact that it can handle the analysis of infinite-state systems and an automatic theorem proving may not reach a deterministic result.

Symbolic Execution

Symbolic execution can be used to find errors in a smart contract, including errors that are not detectable by other formal verification methods.

Symbolic execution involves executing a program (often statically) using symbolic input values instead of concrete values. Because symbolic values can represent multiple concrete values, it is possible to explore multiple execution paths of a smart contract without needing to go through them one by one.

Although formal verification of smart contracts is important and necessary and can find some vulnerabilities. There are a few drawbacks.

The verification of formal models is a complex and time-consuming task. The main problem is that the verification process is very error-prone, and the slightest mistake can easily lead to a wrong conclusion.

Another problem is that formal verification is very difficult to use, and it is often not possible to verify complex smart contracts. Furthermore, the verification process is often not possible to detect all vulnerabilities. If specifications are poorly written, violations of properties—which point to vulnerable executions—cannot be detected by the formal verification audit.

So, in addition to formal verification, third-party security auditing and bug bounty are also necessary and important security activities in the DevSecOps process.

7.2.3.2 Third-Party Security Auditing (Not Just Solidity Code, Must Include all Code)

Many Web3 projects adopted a formal process of engaging a few external auditors to review smart contracts. If Web3 also has the code for centralized front-end and middle-tier components, the best practice is to have these code to be reviewed as well.

Notwithstanding what we said in the previous paragraph, this section will focus on smart contract third-party auditing. This boils down to one important question:

How to Choose a Smart Contract Auditor?

When looking for a smart contract auditor, you should keep in mind the auditor's experience with the blockchain of your choice and the smart contract language. For example, Ethereum and Solidity are the most used blockchain and smart contract languages. Other blockchains such as Solana and Rust are less frequently used. Smart Contract auditor may have good experience and skill set with one blockchain and one smart contract language but not other blockchains or smart contract languages. It is important that the auditor has a deep understanding of the language and the blockchain and more importantly if any of the previous auditings they have worked on has been exploited. Also, the size/popularity of the projects they have audited will help determine whether the auditor is worth hiring as larger projects with good security track records usually hire good auditors.

You may also need to know the methodology and approach taken by the audit firm. You can review their previous audit reports to see what kind of security checks they perform, what kind of security scanning tools they use, the scope of auditing, and how many people are involved in the auditing. Also, the quality of audit reports is another factor to look for in a good auditor. A good report should include a detailed description of all the issues that were found during the course of the investigation. It is also very important to note if the findings of the audit have been addressed by the project and the project team can work with the auditor to decide if there is any false positive in the findings or if a project team is willing to accept the risks for some low vulnerability findings.

Even while smart contract audits are crucial, they should not be seen as a panacea to stop all hacks. Instead, they ought to be seen as an ongoing activity in DevSecOps especially if there are significant code changes to your Web3 application. Developers should continue to put in the effort after an audit to make sure that the findings are fixed to reduce the likelihood of security vulnerabilities.

7.2.4 Bug Bounty

Following a security audit, it is critical to maintain an active Bug Bounty program. Instead of depending on a single security expert, Bug Bounty programs draw security specialists from all over the world with various backgrounds and levels of

competence to enhance the underlying security. Encouraging a global network of professionals to extensively examine your smart contracts for flaws means that all assets under scope are carefully examined.

So, how to run a good Bug Bounty program?

Decide the Correct Incentive Mechanism

The first and most crucial requirement is that incentives be of adequate size. It is crucial to remember that many security researchers view bug bounties as a full-time profession. If rewards are too low, it is highly unlikely that such researchers will spend hours auditing an asset for a potential small payout. Instead, by providing appropriately sized financial incentives, you can be sure that researchers won't divert their valuable time to competing programs and will instead have a strong incentive to spend quality time on your targets in search of high-impact vulnerabilities.

Rewards should also be based on impact. To put it another way, if the security finding can be measured in the amount of funds to be stolen, then regardless of what methods are used in finding the security bugs, the rewards should be the same based on the impact. You can set the rewards by threat level with a higher threat level getting more rewards.

Define the Right Scope

You should clearly define the scope of the bug bounty. For example, for smart contracts, you need to provide the addresses of these smart contracts in scope. If you have front-end code or middle-tier code or database code, you also need to specify the code location in GitHub. You also need to define the items which are out of scope. For example, if the code is not deployed to the mainnet, then it is out of scope, and a denial of service attack should also be out of scope.

Use a Reputable Bug Bounty Program

Instead of running your own platform for bug bounty, you can leverage some mature platforms for your bug bounty program to reach out to more hackers worldwide. For example, immunefi.com and hackerproof.

Allow Public Disclosure

Both project owners and security researchers benefit from transparency as does the disclosure policy. We strongly recommend a “coordinated disclosure” strategy that allows project owners to share mutually accepted vulnerability information with researchers when the fix to the vulnerability is tested and implemented.

7.2.5 *Production (Mainnet) Phase*

7.2.5.1 Continuous Bug Bounty

During the production or mainnet phase, the Web3 project is actually in use and the real money changes hands with smart contract transactions. It is very important to continue the Bug Bounty program as there is no 100% security in smart contract code or any programming code. You may also want to extend the Bug Bounty to other programming codes or components used in your Web3 application and reward the white hat hackers who find the security vulnerabilities.

7.2.5.2 Monitoring/Alerting

A real-time smart contract monitoring system (RCSM) is a system that monitors the execution of a smart contract to ensure that it is proceeding as expected. The system can also provide alerts if any problems or fraudulent transactions occur.

An RCSM is important for two reasons. First, it can help to ensure the accuracy and reliability of the smart contract. Second, it can help to prevent or mitigate the security incidents that may occur.

The RCSM monitors the smart contract in real-time, meaning that it updates its status by subscribing to the events emitted from smart contract execution. If it detects problematic transactions, the RCSM can provide alerts to help prevent or mitigate the effects of the problem. For example, get a notification if a Smart Contract gets called from an address that is not whitelisted.

There are some existing RCSM tools such as tenderly.co or open-source tools such as Smart Contract Watch at <https://github.com/Neufund/smart-contract-watch>

7.3 Sample Security Tools for Web3 DevSecOps

In order to conduct successful DevSecOps, we need to leverage a set of tools which can add automation in the process and increase the probability of finding security issues in the process. This section will highlight some of the tools from Web2 application development which will be still useful for Web3 application development. We will also highlight some of the new security tools designed just for Web3 application development.

There are many good tools either in commercial versions or open-source versions, this section only provides a sample list with URLs for readers' further reading and reference. The tool list is not exhaustive. Due to the size limit of this chapter, we only provide a high-level description of each tool, readers are encouraged to follow the URL to find more information about the relevant tools.

Table 7.4 Sample threat modeling tools

Sample threat modeling tool	Description
IriusRisk https://www.irusrisk.com/	It is an open threat model platform that can create threat models and manage security risks throughout the DevSecOps process using a template-based approach. IriusRisk applies security standards such as OWASP ASVS.
ThreatModeler https://threatmodeler.com/	It is an automated threat modeling solution that helps to identify, predict, and define threats. It features automation, integration, and collaboration to determine where to apply most efforts.
OWASP Threat Dragon https://owasp.org/www-project-threat-dragon/	OWASP Threat Dragon is an open-source threat modeling tool from OWASP, which uses it to create threat model diagrams, possibly record threats, and decide mitigations. Its features include system diagramming and a rule engine to auto-generate threats and their comforts.

7.3.1 *Sample Security Tools Used in during the Requirement and Design Phase*

With the product description documentation and architecture document as input, we can leverage traditional threat modeling tools to refine security requirements for both Web3 and Web2 applications.

The three sample tools used for threat modeling in identifying, defining, and mitigating the threats are as follows (Table 7.4):

These tools can be leveraged for threat modeling of both Web2 and Web3 applications.

There are some academic research on applying different threat modeling methodologies that reader may be interested for further reading (Cuppens et al., 2020; Almashaqbeh, 2019).

7.3.2 *Sample Security Tools Used in Implementation and Testing Phase*

During the development and testing phase, there are some sample tools which can be integrated into CI/CD pipelines or used independently to improve the security posture of your applications. Table 7.5 listed these sample tools. We provide the URLs in the table for users to get more information about the tool. Some of these tools are open source (such as Mythx, Slither, Mythril) or commercial versions of tools with free tier usage support such as Synk, Veracode, and Checkmarx.

Table 7.5 Sample security tools during Web3 implementation phase

Tool Category	Sample Web2 security tools and URLs	Sample Web3 security tools and URLs
SAST (Static application security testing)	Synk.io Veracode.com Checkmarx.com	MythX.io Slither.io Mythril: https://github.com/ConsenSys/mythril
DAST (Dynamic analysis security testing)	Invicti.com Indusface.com Acunetix.com	Mythx.io Mythril: https://github.com/ConsenSys/mythril Manticore: https://github.com/trailofbits/manticore
IAST (Interactive application security testing)	VeraCode.com Invicti.com Acunetix.com	Not exist yet
Secret scanning	Snyk.com Cyccode.com GitLeaks.io	Can use the same Web2 tools for secret scanning Web3 source code such as Solidity
SCA (Software composition analysis)	Synk.io VeraCode.com GitLab.com	Guardrails.io Snyk.io
Formal verification tool	Frama-C.com JavaPathfinder: https://software.nasa.gov/software/ARC-17487-1 BLAST: http://goto.ucsd.edu/~rjhala/blast.html	Scribble—Scribble transforms code annotations in the Scribble specification language into concrete assertions that check the specification. Dafny—Dafny is a verification-ready programming language that relies on high-level annotations to reason about and proves the correctness of code. Solidity SMTChecker—Solidity’s SMTChecker is a built-in model checker based on SMT (Satisfiability modulo theories) and Horn solving. It confirms if a contract’s source code matches specifications during compilation and statically checks for violations of safety properties.

7.3.3 Sample Security Tools Used during Mainnet or Production Phase

After functional testing, security penetration testing, and performance and load testing as well as third-party security auditing (and the vulnerabilities identified during the audit are fixed or the risks are accepted), the Web3 application can be deployed to the mainnet for users to interact with. The security activities do not stop in this phase. We need to continue to monitor the application and get alerts for abnormal transactions.

Since blockchain is the key building block in Web3 applications, we need to at least collect information and monitor the following:

Addresses Information

To ensure the validity and authenticity of a given blockchain address, monitoring tools map blockchain addresses to real-world entities. One of the primary ways

Table 7.6 Sample security tools used during Mainnet or production phase

Tool category	Sample Web2 tools and URL	Sample Web3 tools and URL
Logging and monitoring tool	Extrahop.com Datadog (Datadoghq.com) Sumologic.com	Metrika.co Forta.org
Alert tools	Dynatrace.com PagerDuty.com Amazon SNS (https://aws.amazon.com/sns/)	Metrika.co Forta.org
Dashboard tool	Grafana.com Kibana (https://www.elastic.co/kibana)	Dune.com Nansen.ai Messari.io

monitoring and analysis tools do this is through techniques such as clustering algorithms, statistical analysis, fraud database monitoring, dust attacks, and web scraping. The clustering algorithm method used in blockchain monitoring tools can identify cryptographic services and associated transactions, making it easier to associate transactions with real-world entities.

Transaction Information

The Web3 project can assess the risks associated with any kind of transaction made on the blockchain platform. For example, monitoring the blockchain ecosystem can help Web3 application owners track the origin of funds, track the flow of funds, reveal the identity and history of senders, wallet details of recipients, etc., useful for identifying specific addresses. One of the primary ways monitoring tools assess risk is through the development and use of risk models integrated with machine learning techniques. Such risk models are created based on certain parameters such as transaction amount, funding source, etc., and machine learning algorithms assign a specific risk score to each blockchain transaction.

Transactions and Addresses Correlation

Blockchain ecosystem monitoring also provides visualization tools to understand and examine the nature of blockchain transactions, including blockchain addresses. Most of the tools include a graphical user interface with transaction graphs and charts showing associations between various transactions and addresses.

In a world of escalating financial crime and fraudulent activities, the need for Web3 monitoring and analysis becomes essential. Securing Web3 transactions from financial fraud and theft will be essential before Web3 is adopted on a large scale. Web3 monitoring tools can be very useful in detecting and preventing fraudulent activity via blockchain, enabling individuals and businesses to enjoy the long-term benefits and sustainability of the Web3 network.

In addition to monitoring, the alert features need to be integrated so the Web3 project team can get notified in real-time of potentially fraudulent activities or hack activities and use a good incident response plan to deal with the issues alerted.

Table 7.6 gives a sample security tools list for the monitoring and alerting of both Web2 and Web3 applications.

References

- Almashaqbeh, G. (2019). *ABC: A cryptocurrency-focused threat modeling framework*. IEEE INFOCOM 2019 - IEEE Conference on Computer Communications Workshops (INFOCOM WKSHPS). Retrieved November 26, 2022, from <https://ieeexplore.ieee.org/abstract/document/8845101>
- Biggs, J. (2018, July 3). New malware highjacks your Windows clipboard to change crypto addresses. TechCrunch. Retrieved November 25, 2022, from <https://techcrunch.com/2018/07/03/new-malware-highjacks-your-windows-clipboard-to-change-crypto-addresses>
- Clark, M. (2021, October 13). OpenSea fixes vulnerabilities that could let hackers steal crypto with malicious NFTs. The Verge. Retrieved November 25, 2022, from <https://www.theverge.com/2021/10/13/22723092/opensea-nft-vulnerability-gift-security-researchers-wallet-hack>
- Cuppens, N., Lambrinouidakis, C., Pallas, F., Kalloniatis, C., Gritzalis, S., Sasse, A., Cuppens, F., Pohle, J., Furnell, S., Antón, A., Mylopoulos, J., Garcia-Alfaro, J., Katsikas, S., & Meng, W. (Eds.). (2020). *Computer security: ESORICS 2019 International Workshops, CyberICPS, SECPRE, SPOSE, and ADIoT, Luxembourg City, Luxembourg, September 26–27, 2019 revised selected papers*. Springer International Publishing. https://doi.org/10.1007/978-3-030-42048-2_13
- Deka, L. (2022, 6 6). Home. YouTube. Retrieved November 25, 2022, from <https://www.tron-weekly.com/ddos-attacks-web3-app-stepn>
- DoD. (2019a). *DoD Enterprise DevSecOps Reference*. DoD Enterprise DevSecOps reference. https://dodcio.defense.gov/Portals/0/Documents/DoD%20Enterprise%20DevSecOps%20Reference%20Design%20v1.0_Public%20Release.pdf
- DoD. (2019b, August 12). DoD Enterprise DevSecOps reference design. DoD CIO. Retrieved December 15, 2022, from https://dodcio.defense.gov/Portals/0/Documents/DoD%20Enterprise%20DevSecOps%20Reference%20Design%20v1.0_Public%20Release.pdf
- Forbes. (2018). Quadratic Voting. Quadratic voting: A New Way to Govern Blockchains for Enterprises. Retrieved November 21, 2022, from <https://www.forbes.com/sites/sherman-lee/2018/05/30/quadratic-voting-a-new-way-to-govern-blockchains-for-enterprises/?sh=773c60ca6ef8>
- Franceschi, L. (2021, December 2). Hackers steal \$119M from ‘Web3’ crypto project with old school attack. VICE. Retrieved November 25, 2022, from <https://www.vice.com/en/article/pkpp4n/hackers-steal-dollar119m-from-web3-crypto-project-with-old-school-attack>
- Gartner Research. (2022). Critical capabilities for application security testing. Gartner Research. Retrieved November 26, 2022, from <https://www.gartner.com/en/documents/4014084>
- Godbole, O. (2020, 12 12). *Nexus Mutual's CEO, Hugh Karp, lost the tokens after an attacker gained remote access to his computer*. CEO of DeFi insurer nexus mutual hacked for \$8M in NXM tokens. Retrieved November 25, 2022, from <https://www.coindesk.com/markets/2020/12/14/ceo-of-defi-insurer-nexus-mutual-hacked-for-8m-in-nxm-tokens>
- Kovacs, E. (2022, November 21). Security researchers looking at mastodon as its popularity soars. SecurityWeek. Retrieved November 25, 2022, from <https://www.securityweek.com/security-researchers-looking-mastodon-its-popularity-soars>
- Reciprocity. (2020, November 23). *SOC 2 vs. PCI Compliance: What's the Difference?* Reciprocity. Retrieved November 25, 2022, from <https://reciprocity.com/resources/soc-2-vs-pci-compliance-whats-the-difference/>
- Saldanha, L. (2018). Merkle tree and Ethereum objects - Ethereum yellow paper walkthrough. Article blockchain. Retrieved November 25, 2022, from <https://www.lucassaldanha.com/ethereum-yellow-paper-walkthrough-2>
- Strack, B., & Martin, S. (2022, October 26). JPMorgan exploring applications of digital identity. Blockworks. Retrieved November 25, 2022, from <https://blockworks.co/news/jpmorgan-exploring-applications-of-digital-identity>

Chapter 8

Web3 Security Analytics



Carlo Parisi and Dmitriy Budorin

8.1 Introduction

8.1.1 *What Is on-Chain Analytics*

On-chain analysis is the study and examination of data generated by the activities and transactions that occur on a blockchain network. It provides valuable insights into various aspects of the network, including user behavior, market trends, and the overall health of the ecosystem. By analyzing on-chain data, stakeholders can make more informed decisions about their investments, security practices, and future developments. In this section, we will explore the fundamentals of on-chain analysis and its importance in the Web3 space (Nansen Team, 2022; Roy, 2022).

Blockchain networks, such as Bitcoin and Ethereum, are decentralized systems that rely on distributed ledger technology to record and verify transactions. The ledger, or blockchain, is a transparent and immutable record of all transactions that have ever occurred on the network. As new transactions are added to the ledger, they are grouped into blocks, which are then linked together in a sequential and chronological order. This creates a transparent, traceable, and tamper-proof history of all network activities.

On-chain analysis involves the examination and interpretation of this data to derive meaningful insights and patterns. There are various types of on-chain data that can be analyzed, including:

Transaction Data This includes information about the sender, receiver, amount, and timestamp of each transaction. By analyzing transaction data, one can identify trends in user behavior, such as the frequency and volume of transactions, as well as the distribution of wealth among network participants (McGinn et al., 2016).

C. Parisi (✉) · D. Budorin
Hacken, Lisbon, Portugal

Address Data Blockchain addresses are unique identifiers that represent the ownership of assets on the network. By studying address data, analysts can track the movement of assets between addresses, identify clusters of addresses that may be controlled by a single entity, and uncover patterns in the usage of specific addresses.

Smart Contract Data On platforms like Ethereum, smart contracts are self-executing agreements that run on the blockchain. They enable various decentralized applications (dApps) and use cases, such as decentralized finance (DeFi) and non-fungible tokens (NFTs). Analyzing smart contract data allows researchers to understand the behavior and usage of these dApps, as well as identify potential vulnerabilities and security risks.

Network Data This encompasses information about the overall state and health of the blockchain network, such as block size, block time, and transaction fees. By analyzing network data, one can gain insights into network performance, scalability, and potential bottlenecks or congestion.

On-chain analysis is a crucial tool for a wide range of stakeholders in the Web3 ecosystem, including investors, developers, security teams, and regulators. It offers several benefits, such as:

Identifying Market Trends By analyzing on-chain data, investors can gain insights into market trends, such as shifts in user behavior, the popularity of specific dApps, and the overall sentiment of the market. This can help them make more informed investment decisions and identify potential opportunities.

Enhancing Security On-chain analysis can help security teams identify and prevent potential threats, such as suspicious transactions, malicious smart contracts, and unusual network activity. By detecting these anomalies early, they can mitigate risks and protect the integrity of the network.

Informing Development Developers can use on-chain analysis to understand how their dApps and smart contracts are being used, identify areas for improvement, and optimize their applications for better performance and user experience.

Supporting Regulation Regulators can leverage on-chain analysis to monitor the activities of blockchain networks, ensure compliance with relevant laws and regulations, and identify potential cases of fraud or other illicit activities.

Summary

In conclusion, on-chain analysis is a powerful tool for understanding the complex dynamics of blockchain networks and the Web3 ecosystem. By examining the rich trove of data generated by these networks, stakeholders can gain valuable insights that can inform their decisions, enhance security, and drive innovation in the space.

8.1.2 *Preventive Vs Reactive Web3 on-Chain Analytics and Monitoring*

In the context of on-chain analytics, preventive and reactive analysis represent two distinct approaches to monitoring and securing blockchain networks. Each approach has its own set of objectives, methodologies, and tools, and they can often complement each other in providing a comprehensive view of the network's security and health. In this section, we will delve into the differences between preventive and reactive on-chain analysis and their significance in the Web3 ecosystem.

8.1.2.1 Preventive on-Chain Analysis

Preventive on-chain analysis focuses on identifying potential threats and vulnerabilities before they can be exploited, thereby mitigating risks and safeguarding the network and its participants. This proactive approach involves monitoring the blockchain for unusual or suspicious activities, analyzing smart contracts for potential security flaws, and tracking the movement of funds to detect possible fraud or money laundering. Some key aspects of preventive on-chain analysis include:

Anomaly Detection By analyzing historical on-chain data, preventive analytics can establish baseline patterns of normal network behavior. This allows for the identification of anomalies or deviations from these patterns, which may indicate potential threats or vulnerabilities. Examples of anomalies include unusually large transactions, rapid movements of funds between addresses, or sudden spikes in network activity (Gu et al., 2022).

Smart Contract Auditing Preventive analysis involves the examination of smart contracts for potential security flaws, bugs, or vulnerabilities that could be exploited by malicious actors. This is achieved through a combination of automated tools, such as static analysis and formal verification, and manual review by security experts. By identifying and addressing these issues before they can be exploited, preventive analytics helps to maintain the integrity of the network and protect users' assets.

Risk Profiling Preventive on-chain analysis can also involve assessing the risk associated with specific addresses, contracts, or transactions. This can be achieved through a combination of factors, such as the reputation of the involved parties, historical transaction patterns, and known associations with malicious actors. By understanding the risk profiles of network participants, preventive analytics can help inform decision-making and enhance security for users and protocols.

8.1.2.2 Reactive on-Chain Analysis

Reactive on-chain analysis, on the other hand, focuses on responding to and mitigating the impact of security incidents that have already occurred on the blockchain network. This involves monitoring for signs of ongoing attacks, tracing the

movement of funds following a breach, and conducting forensic investigations to identify the perpetrators and understand the root cause of the incident. Key aspects of reactive on-chain analysis include:

Incident Detection Reactive analytics involves monitoring the blockchain for indicators of compromise, such as unauthorized transactions, suspicious smart contract interactions, or signs of network congestion. By detecting these incidents in real time, reactive analysis can help initiate a rapid response and minimize the potential damage caused by an attack.

Asset Tracing Following a security breach, reactive on-chain analysis can be used to trace the movement of stolen funds across the blockchain. This can help identify the addresses and entities involved in the attack, as well as provide valuable information for law enforcement and recovery efforts.

Forensic Investigation Reactive on-chain analysis also involves conducting in-depth forensic investigations to understand the root cause of a security incident and identify any potential vulnerabilities that may have been exploited. This can help inform future preventive measures and strengthen the overall security posture of the network.

Summary

In summary, preventive and reactive on-chain analysis are complementary approaches to securing blockchain networks and protecting users' assets. While preventive analysis focuses on proactively identifying and mitigating potential threats, reactive analysis deals with responding to and learning from security incidents that have already occurred. By combining these two approaches, stakeholders in the Web3 ecosystem can gain a comprehensive understanding of the security landscape and make informed decisions to enhance the safety and resilience of the network.

8.2 Preventive on-Chain Analysis

8.2.1 *Past and Present of Preventive on-Chain Analysis*

8.2.1.1 **The Past and Present of Preventive on-Chain Analysis: Evolution and Challenges**

The history of monitoring and security solutions has come a long way, from the early days of the internet with network intrusion systems to modern Web3 platforms. In this section, we'll delve deeper into the past and present of preventive on-chain analysis and discuss some of the challenges faced by the industry.

8.2.1.2 The Past: The Evolution of Web2 Monitoring

Digital surveillance in the Web2 era dates back to the infancy of the internet. In 1995, Zeek created a network intrusion system that established the foundation for intrusion detection systems. However, these systems didn't reach widespread adoption due to their noisy character and the difficulty associated with maintaining them.

In 2011, the tech industry shifted its focus to prevention, investing heavily in firewalls and anti-virus software to secure organizations. The emergence of cloud computing was a turning point, allowing security firms to collect and process data centrally, thereby generating threat intelligence and delivering warnings of greater quality.

In the beginning, endpoint detection and response (EDR) systems largely depended on heuristics, which permitted accurate warnings with little data needed. Unfortunately, heuristics suffer from low recall and generalizability. When more data from the real world became available, security firms began investing in data science, supervised machine learning models, and anomaly detection to improve their solutions.

These EDR solutions provided complete protection against assaults by assessing data at the network, endpoint, and cloud levels. However, they discovered problems with noise, volume, explainability, and the ability to respond to attacks. These obstacles frequently came from scalability restrictions and a dearth of security specialists on incident response teams (Forta., 2022).

8.2.1.3 The Present: An Overview of Web3 Monitoring

Web3 monitoring contrasts starkly with Web2 monitoring. Web2 attacks typically unfold at a slower rate, and it can be more difficult to quantify the consequences of a successful attack. Web3, on the other hand, focuses heavily on user funds and data accessibility.

A major proportion of Web3 attacks occur swiftly, demanding extremely precise alerts prior to the theft of cash. The effectiveness of machine learning algorithms in producing these warnings has been shown, but the general adoption of automated incident response procedures via smart contract operational services such as Chainlink Keepers and OZ's Defender remains restricted.

Yet, some Web3 attacks may last for hours or even days. In such situations, monitoring and manual analysis by specialists become crucial. As was the case with Web2, investments in ranking, clustering, explainability, and investigation tools are required to reduce the strain on incident responders and security operation personnel (Forta., 2022).

8.2.1.4 The Present: Protecting End Users in Web3

End-user security in the Web3 ecosystem is contingent on the availability of large data and cloud capabilities. To guarantee effective protection, a detection strategy with multiple layers is required, which includes:

1. Rapid heuristics and indications curated by a team of specialists who manage ongoing attacks and develop detection coverage.
2. Models of machine learning that are trained persistently on data and labels to generalize beyond specific attacks.

The financial incentives and adversarial nature of the environment drive attackers to constantly attempt to evade these barriers, notwithstanding the success of this strategy. Due to concerns about user friction created by false positives, the concept of zero trust has been presented but has not been implemented successfully. (Forta., 2022).

8.2.1.5 Challenges in Web3 on-Chain Monitoring

While data is generally accessible in Web3, restrictions such as zero-knowledge (ZK) and Dapp data can limit the effectiveness of monitoring systems.

The rapid nature of Web3 assaults requires rapid alarms and responses, which can be challenging to design and maintain.

A lack of security experience in the Web3 domain creates difficulties for incident response teams and security operation centers, which may result in gaps in monitoring and protection.

As the Web3 ecosystem grows, security solutions must scale to support the increasing number of users, assets, and possible attack routes.

The widespread use of on-chain analytics and monitoring integration with smart contract operational services for automated issue response has not yet occurred, allowing potential for improvement in proactive protection.

Continually decreasing false positives and boosting the signal-to-noise ratio is an ongoing problem in Web3 monitoring.

In a financially motivated environment, attackers continually alter their methods and strategies to circumvent security systems, necessitating constant awareness and adaptation by security personnel. (Forta., 2022).

8.2.2 Technology Stack Used for Preventive on-Chain Analysis

Preventive on-chain analysis relies on a diverse range of technologies and tools to monitor, analyze, and secure blockchain networks. These technologies are designed to work in concert, providing a comprehensive view of the network's health and

potential risks. In this section, we will explore some of the key components of the technology stack used in preventive on-chain analysis.

Data Collection and Storage The foundation of preventive on-chain analysis is the collection and storage of vast amounts of blockchain data. This involves ingesting raw transaction data, smart contract interactions, and other on-chain events from various blockchain networks. To achieve this, analysts employ:

Blockchain nodes Running full or archive nodes on different blockchain networks enables the collection of complete transaction histories, smart contract data, and other relevant information.

APIs and data providers Leveraging APIs and data providers, such as Infura or QuickNode, can streamline access to blockchain data without having to maintain nodes in-house.

Data storage solutions Storing and organizing the collected data in databases (e.g., PostgreSQL, MongoDB) or distributed storage systems (e.g., Apache Cassandra, Amazon S3) allows for efficient querying and analysis.

With the collected data in hand, analysts apply various processing and analysis techniques to extract insights and identify potential threats or vulnerabilities. Some key components in this process include:

ETL (Extract, Transform, Load) pipelines ETL pipelines facilitate data transformation and enrichment, preparing raw blockchain data for analysis by converting it into structured formats, aggregating data points, and generating relevant metrics.

Analytics engines Specialized analytics engines, such as Apache Spark, Elasticsearch, or GraphDB, enable high-performance querying and analysis of large-scale blockchain data, allowing analysts to uncover patterns, trends, and anomalies.

Data visualization tools Tools like Tableau, Grafana, or D3.js help visualize complex on-chain data, making it more accessible and understandable to analysts and decision-makers.

Detecting unusual or suspicious activities on the blockchain is a critical aspect of preventive on-chain analysis. To this end, analysts employ various anomaly detection techniques and machine learning models, such as:

Statistical methods Techniques like standard deviation, clustering, or control charts help identify data points that deviate significantly from established patterns or trends, potentially signaling malicious activities or vulnerabilities.

Machine learning models Supervised and unsupervised learning algorithms, such as decision trees, neural networks, or clustering algorithms, can be used to create models that recognize complex patterns and flag potential threats or anomalies in real time.

Feature engineering Crafting relevant features from raw blockchain data is essential for training effective machine learning models. This may involve calculating transaction frequencies, identifying network centrality measures, or extracting patterns from smart contract code.

Analyzing smart contracts for potential security flaws or vulnerabilities is a vital component of preventive on-chain analysis. Some key technologies and tools in this area include:

Static analysis tools Tools like Mythril, Slither, or Securify can automatically scan smart contract code for known vulnerabilities, coding mistakes, or other security issues, providing a preliminary assessment of potential risks.

Formal verification Techniques such as model checking or theorem proving can be used to mathematically prove the correctness of smart contract code, ensuring that it behaves as intended under all possible conditions.

Fuzz testing Fuzz testing involves executing a smart contract with a wide range of inputs and attempting to trigger unexpected behavior or crashes that may indicate underlying vulnerabilities.

Risk-scoring models Leveraging machine learning algorithms, statistical methods, or expert-driven rules to calculate risk scores for blockchain entities based on factors such as transaction history, smart contract vulnerabilities, or connections to known malicious actors.

Reputation systems Implement systems that track the trustworthiness of addresses, contracts, or users over time based on their on-chain activities and interactions with other entities.

Dashboarding and reporting Providing real-time dashboards and reporting interfaces that allow analysts and decision-makers to track key metrics, trends, and alerts related to on-chain security and risk management.

Summary

In summary, the technology stack used in preventive on-chain analysis comprises a diverse range of tools and techniques, spanning data collection and storage, data processing and analysis, anomaly detection and machine learning, smart contract analysis, risk assessment and scoring, and real-time monitoring and alerting. By leveraging these technologies, analysts can gain a deep understanding of the blockchain ecosystem, identify and mitigate potential threats, and contribute to the overall security and stability of the Web3 landscape.

8.2.3 *Future of Preventive on-Chain Analysis*

As the Web3 ecosystem expands and matures, the future of preventative on-chain analysis will need to adapt and change to accommodate the problems and possibilities that occur. These are some significant areas where preventative on-chain analysis will likely concentrate in the future:

Monitoring Tradeoff Web3 end-user protection may be divided into negative and positive reputation services. Negative reputation services safeguard users by detecting and banning harmful EOAs, contracts, and compromised contacts, while positive reputation services only enable interactions with recognized, trustworthy

companies. Finding the correct balance between these techniques is critical for successful end-user security as the Web3 area expands.

Standardizing Actionable Negative Signals Creating standardized, actionable negative signals using heuristics is critical for safeguarding end users and protocols in the Web3 environment. Reducing alarm fatigue via alert grouping, rating, and investments in data science and sophisticated machine learning models may improve the accuracy of negative signals, making them more useful in detecting and managing assaults.

Automated Incident Response Creating and implementing automated incident response systems for protocols is a vital field that requires major effort. Improving alert accuracy and collaborating with smart contract libraries and operational systems may make automated incident response more dependable and effective. This entails establishing cross-chain intelligence as well as positive reputation systems for end users and on-chain protocols.

Wallet Provider Security Wallet providers are critical in protecting users' money and guaranteeing their security. Companies must accept responsibility for user safety by adding security features such as scam warning prompts, firewalls, and other safeguards.

Interoperability and Cross-Chain Security With various blockchain networks and rising cross-chain interactions, preventative on-chain analysis must adapt and broaden its scope to encompass monitoring and protection across many blockchains. This entails creating cross-chain intelligence and security solutions to handle the particular issues provided by cross-chain assaults.

Decentralized Security Solutions Decentralized security solutions, including decentralized oracles and smart contract insurance, may become increasingly widespread, adding levels of safety and confidence to the Web3 ecosystem. These technologies may supplement existing preventative on-chain analysis approaches and contribute to a more secure environment for users and protocols.

Cooperation and Information Sharing Improved Web3 ecosystem security will need more collaboration and information sharing across various initiatives, security teams, and researchers. Working together and sharing expertise allows the sector to create more effective preventative on-chain analysis solutions and stay ahead of possible problems.

Regulatory Frameworks As the Web3 ecosystem obtains mainstream attention, regulatory frameworks must emerge to assure the ethical and lawful conduct of preventative on-chain analyses. This may include creating industry standards and best practices as well as rules and legislation controlling the usage of these approaches in the Web3 area.

Integrating Privacy-Preserving Technologies As user privacy becomes more important, privacy-preserving technologies such as zero-knowledge proofs and private computing will play a larger role in preventative on-chain analyses. Incorporating these technologies into monitoring and security systems enables on-chain data analysis and danger detection without jeopardizing user privacy.

Advancing AI and ML Techniques As data science and machine learning methods evolve, their applications in preventative on-chain analysis are projected to

extend and improve. Using cutting-edge AI and ML approaches may improve security solutions' accuracy, efficiency, and effectiveness in identifying and blocking attacks in the Web3 ecosystem.

Education and Awareness As the Web3 ecosystem expands, user education and knowledge of security best practices and possible threats become more important. Raising security awareness and providing users with information and means to defend themselves may supplement preventative on-chain analysis with a more knowledgeable user base better prepared to recognize and avoid dangers.

Customization and Personalization Future preventative on-chain analysis solutions may become more configurable and customized to meet the particular demands of diverse users and protocols. Enabling customers to customize security solutions to their individual needs may improve the efficiency of preventative on-chain analysis for diverse use cases and risk profiles.

Real-Time and Proactive Attack Detection As the pace and complexity of assaults in the Web3 ecosystem grow, the necessity for real-time and proactive threat detection becomes increasingly vital. Future preventative on-chain analysis solutions will most likely concentrate on recognizing and reducing risks as they develop rather than simply depending on historical data and post-attack analysis.

To summarize, the future of preventative on-chain analysis will be formed by continual innovation, cooperation, and adaptability in response to the ever-changing Web3 context. By concentrating on these critical areas and adopting new technologies and techniques, the industry can collaborate to build a more secure and resilient ecosystem that benefits all stakeholders, from end users to protocols and developers. As the Web3 area evolves and grows, preventative on-chain analysis must adapt and develop with it, tackling growing difficulties and capturing new possibilities to improve the security and stability of the blockchain ecosystem. (Forta., 2022).

8.3 Reactive on-Chain Analysis

8.3.1 *The Problem that Reactive on-Chain Analysis Solves*

Reactive on-chain analysis is a critical component of a comprehensive approach to blockchain security and risk management. In contrast to preventive on-chain analysis, which aims to identify and mitigate potential threats before they materialize, reactive on-chain analysis focuses on responding to incidents and attacks after they have occurred. By conducting in-depth investigations and forensic analysis of on-chain data, reactive on-chain analysis helps to understand the root cause of incidents, trace the flow of stolen funds, and identify potential vulnerabilities or loopholes that can be addressed to prevent similar attacks in the future. In this section, we will explore the key problems that reactive on-chain analysis solves and discuss the importance of this approach in the broader context of Web3 security.

8.3.1.1 Incident Response and Forensic Analysis

One of the primary functions of reactive on-chain analysis is to support incident response and forensic analysis efforts following a security breach, hack, or other malicious activity on the blockchain. By thoroughly examining on-chain data, transactions, and smart contract interactions, reactive on-chain analysis can help to:

- Determine the root cause of an incident, such as a smart contract vulnerability, a phishing attack, or a compromised private key.
- Identify the attackers or malicious entities involved by tracing transactions and connections to known bad actors or suspicious addresses.
- Analyze the attack vectors, techniques, and patterns used, which can inform the development of new detection methods or countermeasures for future attacks.
- Track the flow of stolen funds or assets, providing valuable intelligence for law enforcement, recovery efforts, or legal proceedings. (OfficerCIA.eth, 2022).

8.3.1.2 Post-Mortem Analysis and Lessons Learned

In addition to supporting incident response and forensic investigations, reactive on-chain analysis plays a crucial role in conducting post-mortem analysis and extracting valuable lessons learned from past incidents. By identifying the factors that contributed to an attack or vulnerability, reactive on-chain analysis can help to:

- Evaluate the effectiveness of existing security measures, risk management practices, and monitoring systems in detecting and preventing incidents.
- Identify gaps, weaknesses, or areas for improvement in the blockchain ecosystem's overall security posture, which can guide future investments, research, or development efforts.
- Inform the design and implementation of new security controls, best practices, or policies aimed at reducing the likelihood or impact of similar incidents in the future.

8.3.1.3 Enhancing Preventive Measures and Proactive Security

Reactive on-chain analysis also plays a vital role in informing and enhancing preventive measures and proactive security efforts in the Web3 space. By analyzing past incidents and understanding the tactics, techniques, and procedures (TTPs) employed by attackers, reactive on-chain analysis can contribute to the development of more effective detection methods, risk-scoring models, and countermeasures. For example:

- Machine learning models used in preventive on-chain analysis can be trained on historical data from past attacks, enabling them to better identify and flag similar patterns or anomalies in real time.

- Heuristic-based detection rules or indicators of compromise (IoCs) can be refined and updated based on insights gleaned from reactive on-chain analysis, improving the accuracy and coverage of threat detection.
- Risk assessment methodologies, scoring systems, and reputation models can be informed by the outcomes of reactive on-chain analysis, allowing for more accurate and targeted risk mitigation strategies.

8.3.1.4 Regulatory Compliance and Legal Support

As the regulatory landscape surrounding cryptocurrencies and blockchain technology continues to evolve, reactive on-chain analysis can play a critical role in ensuring compliance with relevant laws, regulations, and industry standards. By providing detailed insights into on-chain activities, transactions, and risk factors, reactive on-chain analysis can help organizations to:

- Demonstrate compliance with anti-money laundering (AML), counter-terrorism financing (CTF), or know-your-customer (KYC) requirements, by conducting thorough due diligence and monitoring of on-chain activities (Kocegarovas, 2022).
- Support legal proceedings, investigations, or enforcement actions related to blockchain-based fraud, theft, or other illicit activities, by providing evidence, expert testimony, or forensic analysis of on-chain data (Grigg, 2022).
- Facilitate cooperation and information sharing between blockchain projects, regulators, law enforcement agencies, and other stakeholders, to collectively address the challenges posed by malicious actors and cyber threats in the Web3 space (Kaur, 2022).

8.3.1.5 Reputation Management and User Trust

Maintaining a strong reputation and user trust is essential for any blockchain project or platform, especially in the highly competitive and rapidly evolving Web3 ecosystem. Reactive on-chain analysis can contribute to reputation management and user trust by:

Demonstrating a commitment to security, transparency, and accountability, through the thorough investigation and disclosure of incidents, vulnerabilities, or risks.

Communicating the lessons learned and corrective actions taken following an incident, to reassure users, partners, and investors that the project is taking steps to prevent similar issues in the future.

Providing ongoing updates and insights into the security landscape and threat environment, to educate users and stakeholders about the risks, challenges, and best practices associated with blockchain technology and digital assets.

Summary

In summary, reactive on-chain analysis is an essential component of a comprehensive approach to blockchain security and risk management. By focusing on responding to incidents and attacks after they have occurred, reactive on-chain analysis helps to understand the root cause of incidents, trace the flow of stolen funds, and identify potential vulnerabilities or loopholes that can be addressed to prevent similar attacks in the future. The insights gained from reactive on-chain analysis can inform and enhance preventive measures, proactive security efforts, regulatory compliance, legal support, and reputation management, ultimately contributing to the long-term success and sustainability of the Web3 ecosystem.

8.3.2 *The Present of Reactive on-Chain Analysis*

Reactive on-chain analysis currently involves a combination of manual investigation and automated tools to analyze incidents, track fund movements, and inform preventive measures. Some key aspects of the present state of reactive on-chain analysis are:

Manual Investigation Security professionals and researchers often rely on manual investigation techniques, such as examining transaction data, reviewing smart contract code, and analyzing on-chain behavior, to understand the nature of an incident and its root cause.

Analytics Tools Several analytics tools and platforms are available to facilitate reactive on-chain analysis, including blockchain explorers, data visualization tools, and specialized forensic analysis platforms. These tools enable researchers to track fund movements, analyze transaction patterns, and identify potentially malicious addresses or contracts involved in an incident.

Collaboration with Law Enforcement Reactive on-chain analysis often involves working with law enforcement agencies to share information and intelligence about security incidents. This collaboration is crucial for recovering stolen funds and holding malicious actors accountable for their actions.

Collaboration with Exchanges and Other Stakeholders When tracking stolen funds or attempting to recover assets, reactive on-chain analysis may require collaboration with cryptocurrency exchanges, wallet providers, and other stakeholders in the blockchain ecosystem. These stakeholders can help by providing additional data, freezing accounts, or assisting with asset recovery.

Community-Driven Efforts The blockchain community plays a significant role in reactive on-chain analysis. Security researchers, developers, and enthusiasts often collaborate on forums, social media, and other platforms to share information, analyze incidents, and develop solutions to address security challenges.

Education and Awareness As part of reactive on-chain analysis efforts, security professionals and researchers often engage in education and awareness campaigns

to inform users about potential threats and best practices for securing their assets. This can include blog posts, webinars, and workshops to share insights and lessons learned from security incidents.

8.3.2.1 Looking Ahead: The Future of Reactive on-Chain Analysis

The future of reactive on-chain analysis is likely to be shaped by several key developments:

Advanced Analytics Platforms As the field of on-chain analysis evolves, we can expect the development of more advanced analytics platforms that integrate machine learning and AI techniques to automate the investigation process and detect patterns and anomalies more efficiently.

Decentralized Incident Response Decentralized incident response solutions leveraging blockchain technology may emerge, enabling trustless collaboration among different stakeholders in the ecosystem to address security incidents and recover stolen assets more effectively.

Cross-Chain Forensics As the blockchain ecosystem becomes more interconnected and multi-chain solutions become more prevalent, cross-chain forensics will be essential to track fund movements and analyze incidents that span across different networks.

Integration with DeFi Protocols As decentralized finance (DeFi) continues to grow, reactive on-chain analysis solutions will need to be tightly integrated with DeFi protocols to help address security incidents and protect users from risks such as smart contract exploits, rug pulls, and other types of fraud.

Enhanced Privacy-Preserving Techniques The increasing adoption of privacy-preserving technologies like zero-knowledge proofs and confidential transactions will require reactive on-chain analysis to adapt and develop new approaches to investigate incidents while preserving user privacy.

Summary

In conclusion, the field of on-chain analysis is continually evolving, with preventive and reactive approaches playing crucial roles in securing the blockchain ecosystem. As technology and the blockchain landscape advance, we can expect further developments in analytics tools, machine learning techniques, and collaboration among stakeholders to address security challenges and maintain trust in the blockchain ecosystem.

8.4 On-Chain Analysis Tools

On-chain analysis tools are an essential part of the blockchain ecosystem, providing valuable insights into the behavior, trends, and patterns within various blockchain networks. These tools come in different forms and offer a wide range of features,

catering to specific use cases and requirements. Some common types of on-chain analysis tools include transaction analysis, OSINT (Open Source Intelligence), querying, and more (Bederov, 2022; Argonyte, 2021; Giacomo Giallombardo, n.d.).

Transaction analysis tools primarily focus on monitoring, tracking, and analyzing transactions and addresses on blockchain networks. They help identify patterns, detect anomalies, and uncover suspicious activities. These tools are particularly useful for compliance, risk assessment, and fraud detection purposes.

OSINT tools leverage publicly available data sources to gather intelligence about blockchain networks, projects, and users. They collect data from sources like social media, news, forums, and other online platforms to provide insights into market sentiment, trends, and user behavior.

Querying tools allow users to access and analyze raw blockchain data using custom queries or predefined templates. They offer a powerful way to explore blockchain data and derive meaningful insights based on specific research questions or interests. These tools are particularly useful for developers, researchers, and data analysts who require granular control over the data they analyze.

There are also visualization tools that help users better understand blockchain data by presenting it in an intuitive and visually appealing format. These tools often provide interactive charts, graphs, and maps that enable users to explore data in a more engaging and accessible way.

Another category of on-chain analysis tools is focused on DeFi (Decentralized Finance) and NFT (Non-Fungible Token) ecosystems. These tools provide specialized metrics, insights, and analytics for the rapidly growing sectors of the blockchain industry.

Please note that the following list is not comprehensive, but it serves to give the reader an idea of the range of tools available. The industry is rapidly growing, and more tools are created and updated every day.

Nansen Nansen is an analytics platform that provides insights into Ethereum blockchain data, including DeFi and NFTs. It offers various features like smart alerts, whale tracking, wallet profiling, and more (Igwe, 2023; Oladotun, 2023).

Dune Analytics Dune Analytics is a user-friendly platform that allows users to create, share, and explore Ethereum data dashboards using SQL queries. It supports various DeFi protocols and offers a wide range of pre-built dashboards to get started (Igwe, 2023; Oladotun, 2023).

Glassnode Glassnode is an on-chain market intelligence platform that provides data-driven insights into the behavior of various blockchain networks like Bitcoin, Ethereum, and others. It offers various metrics, charts, and analytical tools to help users better understand the underlying economics of these networks (Oladotun, 2023).

TokenAnalyst TokenAnalyst focuses on providing data and insights for various digital assets. It offers an API for on-chain data and real-time metrics, including transaction volumes, user activity, and token flows.

IntoTheBlock IntoTheBlock is an analytics platform that offers a wide range of on-chain indicators and insights for various cryptocurrencies. It provides features like address activity, token flows, transaction patterns, and more (Oladotun, 2023).

DeFiLLama DeFiLLama is a popular decentralized finance (DeFi) analytics platform that provides comprehensive and up-to-date information about various

DeFi protocols, projects, and tokens across multiple blockchain networks. The platform aggregates data from various sources to offer users a holistic view of the DeFi ecosystem. Users can access metrics such as Total Value Locked (TVL), market data, trading volumes, and liquidity pools, among others (Shift, 2023).

Bubblemaps Bubblemaps is an online platform for creating interactive, customizable bubble maps to visualize various types of data. The maps can be customized to display different data types, sizes, colors, and other visual elements, helping users better understand and interpret the information being presented.

Summary

In conclusion, on-chain analysis tools are a diverse and vital component of the blockchain landscape, catering to different use cases and requirements. They enable users to better understand the complex dynamics of blockchain networks, uncover valuable insights, and make informed decisions in the world of digital assets. As the blockchain ecosystem continues to evolve, these tools will undoubtedly play an increasingly important role in navigating the ever-changing landscape of blockchain technology.

8.5 The Future of on-Chain Analysis: Combining Preventive and Reactive Approaches

As the Web3 ecosystem continues to evolve, on-chain analysis will play an increasingly important role in ensuring the security, transparency, and trustworthiness of blockchain networks, platforms, and applications. Looking ahead, the future of on-chain analysis will likely involve a more holistic, integrated approach, combining both preventive and reactive strategies to address the multifaceted challenges and opportunities presented by the decentralized digital economy.

8.5.1 *Enhanced Machine Learning and AI Capabilities*

One of the key drivers of innovation in on-chain analysis will be the ongoing development of advanced machine learning (ML) and artificial intelligence (AI) technologies. *ML and AI have already proven to be valuable tools for detecting and analyzing complex patterns, anomalies, and trends in large-scale, high-dimensional blockchain data.* In the future, these capabilities will likely become even more sophisticated and powerful, enabling on-chain analysis solutions to:

- Identify new attack vectors, vulnerabilities, and threats in real time, as they emerge or evolve, with greater accuracy and speed.

- Automatically generate and update heuristics, rules, or IoCs based on the latest threat intelligence and historical data, to improve the effectiveness of preventive monitoring and detection systems.
- Leverage advanced analytics and predictive modeling techniques to assess the potential impact, likelihood, or severity of different types of incidents or risks, allowing for more informed decision-making and resource allocation.

8.5.2 Cross-Chain and Interoperability

Another important trend shaping the future of on-chain analysis is the increasing emphasis on cross-chain and interoperable blockchain technologies. As more and more projects and platforms adopt multi-chain, cross-chain, or bridge solutions to connect different blockchain networks and facilitate the seamless transfer of assets and data, *on-chain analysis will need to adapt and expand its scope to cover these interconnected environments*. This could involve:

- Developing new methodologies, tools, or protocols for tracking, tracing, or analyzing cross-chain transactions, asset flows, or smart contract interactions.
- Establishing common standards, data formats, or APIs for exchanging and sharing on-chain analytics, threat intelligence, or risk assessment information across different blockchain networks or platforms.
- Collaborating with other stakeholders, such as bridge operators, multi-chain wallet providers, or interoperability-focused projects, to jointly address the security and risk management challenges associated with cross-chain operations and infrastructure.

8.5.3 Privacy-Preserving on-Chain Analysis

As concerns around data privacy, user anonymity, and confidentiality grow in importance within the blockchain space, on-chain analysis will need to strike a balance between providing effective security and risk management solutions and respecting the privacy rights and preferences of users. This may involve:

Implementing privacy-preserving techniques, such as zero-knowledge proofs, secure multi-party computation, or homomorphic encryption, to enable on-chain analysis without revealing sensitive or personally identifiable information (PII).

Designing on-chain analysis systems and processes that adhere to data protection regulations and principles, such as data minimization, purpose limitation, or data subject rights, while still maintaining their effectiveness and utility.

Collaborating with privacy-focused blockchain projects, organizations, or research institutions to develop and promote best practices, guidelines, or standards for conducting ethical, responsible, and privacy-conscious on-chain analysis.

Summary

In conclusion, the future of on-chain analysis will likely involve a more integrated, adaptive, and forward-looking approach that combines preventive and reactive strategies, leverages cutting-edge technology, and addresses the evolving needs, priorities, and challenges of the Web3 ecosystem. By staying ahead of the curve and embracing these emerging trends and opportunities, on-chain analysis can help to ensure the ongoing security, resilience, and success of the decentralized digital economy.

References

- Argonyte. (2021, December 26). How to use OSINT in cryptocurrency investigations? - RIXED_LABS - *Medium*. Medium. <https://medium.com/ax1al/using-osint-to-investigate-cryptocurrency-transactions-7229f64c671a>
- Bederov, I. S. (2022, August 19). Ethereum (ETH) OSINT investigations tools - Igor S. Bederov - *Medium*. Medium. https://medium.com/@ibederov_en/ethereum-eth-osint-investigations-tools-7d1ec5deable.
- Forta. (2022, November 23). *The past, present, and future of monitoring* - Forta network. Forta Network. <https://forta.org/blog/the-past-present-and-future-of-monitoring/>
- Giacomo Giallombardo. (n.d.). GitHub - aaarghhh/awesome_osint_crypto_web3_stuff: A list of useful crypto resources for OSINT investigation. GitHub. https://github.com/aaarghhh/awesome_osint_crypto_web3_stuff#metaverse
- Grigg, G. (2022, July 22). Blockchain analysis for national security and law enforcement agencies: A *Primer*. Chainalysis. <https://blog.chainalysis.com/reports/blockchain-analysis-national-security-law-enforcement/>.
- Gu, Z., Lin, D., & Wu, J. (2022). On-chain analysis-based detection of abnormal transaction amount on cryptocurrency exchanges. *Physica D: Nonlinear Phenomena*, 604, 127799. <https://doi.org/10.1016/j.physa.2022.127799>
- Igwe, P. (2023, January 19). Blockchain analytics and its use cases - Coinmonks - *Medium*. Medium. <https://medium.com/coinmonks/blockchain-analytics-and-its-use-cases-d084f8f69f2b>.
- Kaur, G. (2022, March 17). How do crypto monitoring and blockchain analysis help avoid cryptocurrency fraud? *Cointelegraph*. <https://cointelegraph.com/explained/how-do-crypto-monitoring-and-blockchain-analysis-help-avoid-cryptocurrency-fraud>
- Kocegarovas, G. (2022, March 16). *Crypto anti-money laundering: How to prevent each step in a 3-step process*. - PSP Lab. PSP Lab. <https://psplab.com/crypto-anti-money-laundering-preventing-3-step-process/>
- McGinn, D., Birch, D. G., Akroyd, D., Molina-Solana, M., Guo, Y., & Knottenbelt, W. J. (2016). Visualizing dynamic bitcoin transaction patterns. *Big Data*, 4(2), 109–119. <https://doi.org/10.1089/big.2015.0056>
- Nansen Team (2022, December 7). *What is on chain analysis, and why is it useful for crypto traders?* (n.d.). <https://www.nansen.ai/guides/what-is-on-chain-analysis-and-why-is-it-useful-for-crypto-traders>
- OfficerCIA.eth. (2022, May 1). *Blockchain forensics, how to investigate crypto hacks*. (n.d.). <https://officercia.mirror.xyz/BFzv17UwH6QG4q711NALjtSiP8eKR17daLjTdmAgbHw>
- Oladotun, A. (2023, February 28). 8 best on-chain analysis tools in 2023. *BeInCrypto*. <https://beincrypto.com/learn/on-chain-analysis-tools/>
- Roy, R. (2022, August 3). All you want to know about on-chain analytics - WazirX Blog. *WazirX Blog*. <https://wazirx.com/blog/all-you-want-to-know-about-on-chain-analytics/>.
- Shift, C. (2023, March 10). Comprehensive list of Crypto Research & Analytics Tools – Collective Shift. *Collective Shift*. <https://collectiveshift.io/tools/crypto-analytics-tools/>

Chapter 9

Data Authenticity



Ken Huang

Data authenticity is a critical security concern for web3 applications that utilize real-world data with on-chain smart contracts. When the data upon which a smart contract relies is inaccurate or tampered with, it can have serious unintended consequences. This is an especially daunting challenge since smart contracts operate automatically and cannot independently verify the accuracy or integrity of the data they receive. As a result, security vulnerabilities and loss of trust in the system are likely outcomes.

Fortunately, several companies, including Chainlink, Band Protocol, UMA, Nest Protocol, and API3, have stepped up to address this issue by providing decentralized data feeders or decentralized oracles to smart contracts.

These decentralized oracles provide a secure and reliable way to connect smart contracts to off-chain data sources, ensuring that the data they receive is accurate and trustworthy. By utilizing a decentralized network of data providers, these oracles ensure that data is verified and validated through a consensus mechanism, reducing the risk of manipulation or malicious attacks.

This chapter discusses different types of data oracles; examples of data oracle providers; oracle use cases in DeFi, NFT, Insurance, Enterprise, prediction market, and even sustainability; oracle design considerations, and security attacks on oracles and the countermeasures.

K. Huang (✉)
DistributedApps.AI, Fairfax, VA, USA
e-mail: Ken@Distributedapps.ai

9.1 Types of Blockchain Oracles

Different types of oracles are needed for smart contracts because the requirements for external data and computation can vary widely between different contracts. For example, some contracts may need real-time data from external sources, while others may be able to work with delayed data. Some contracts may require data from multiple sources, while others may only need data from one specific source.

Additionally, the level of security required for the data can also differ between contracts. Some contracts may be designed to handle sensitive financial or personal data and therefore require a higher level of security, while others may not require such stringent measures.

To meet these diverse requirements, different types of oracles are designed to handle specific tasks. For example, some oracles are specialized in fetching data from a specific type of source, while others are designed to perform computations on the data before delivering it. These different types of oracles allow smart contracts to be tailored to meet the specific needs of each use case, which is essential for their functionality and success.

9.1.1 Input Oracles

The input oracle is the most well-known type of oracle in use today, and it plays a crucial role in enabling smart contracts to interact with the real world. As its name suggests, the input oracle fetches data from off-chain sources and delivers it to the blockchain network for consumption by smart contracts.

In Fig. 9.1, the input data oracle is represented by the rectangle labeled “Input Data Oracle,” while the smart contract is represented by the rectangle labeled “Smart Contract.” The arrow indicates that the input data oracle sends input data to the smart contract.

One of the most popular applications of input oracles is in powering Chainlink Price Feeds. These feeds provide DeFi (Decentralized Finance) smart contracts with on-chain access to financial market data, such as cryptocurrency prices or exchange rates. This data is crucial for the functioning of many DeFi applications, such as lending platforms, stablecoins, and derivatives trading platforms.

For example, consider a DeFi lending platform that uses an input oracle to retrieve real-time cryptocurrency prices. When a user deposits their crypto assets as collateral, the platform’s smart contract uses the price data from the oracle to calculate the value of the collateral and determine the maximum loan amount that can be

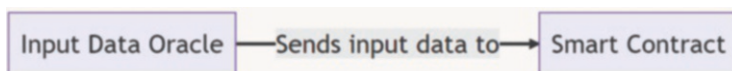


Fig. 9.1 Input Data Oracle

issued. If the price of the collateral drops below a certain threshold, the smart contract will automatically trigger a liquidation event to repay the loan and protect the lender’s funds.

In this scenario, the input oracle serves as a trusted source of financial market data, enabling the smart contract to operate securely and autonomously. This is just one of many examples of how input oracles are used to bring real-world data into the blockchain and power the next generation of decentralized applications.

9.1.2 Output Oracles

Output oracles serve as the opposite of input oracles, as they allow smart contracts to communicate with the real-world (off-chain) systems and trigger them to perform specific actions. These actions can range from simple tasks, such as sending a notification, to more complex processes, such as executing a financial transaction or controlling a physical device.

Output oracles are used **after** smart contract execution to provide data and to trigger real-world events while input oracles are used **before** smart contract execution to provide real-world data to trigger smart contract execution.

In Fig. 9.2, the smart contract is represented by the rectangle labeled “Smart Contract,” the output data oracle is represented by the rectangle labeled “Output Data Oracle,” and the real-world application is represented by the rectangle labeled “Real-World Application.” The arrows indicate that the smart contract sends the execution result to the output data oracle, and the output data oracle sends the output data to the real-world application.

For example, consider a smart contract that manages car rentals on a blockchain network. Once a user makes an on-chain payment for a rental, the smart contract can send a command to an output oracle, which then pings an IoT (Internet of Things) system to unlock the car door. This type of output oracle provides a secure and automated way for the smart contract to communicate with the off-chain world and execute the rental process.

Another example is a smart contract that manages payments for a cloud storage service. The smart contract can use an output oracle to send a command to the storage provider, instructing them to store the specified data. This eliminates the need for manual intervention, reduces the risk of human error, and provides a more efficient and secure way to manage the storage service.

Output oracles play an important role in enabling smart contracts to interact with the real-world systems and perform a wide range of tasks. By providing a secure and automated way to communicate with off-chain systems, output oracles help to

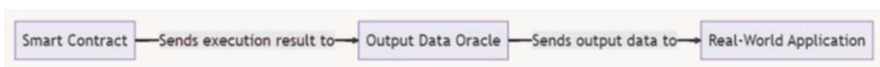


Fig. 9.2 Output Data Oracle

bring the benefits of blockchain technology to a wider range of use cases and industries.

9.1.3 Cross-Chain Oracles

Cross-chain oracles are a type of oracle that enable communication and transfer of information and assets between different blockchain networks. They play a crucial role in enabling interoperability across different blockchains, making it possible to move data and assets between them.

In Fig. 9.3, there are two chains—Chain A and Chain B, represented by the rectangles labeled “Chain A” and “Chain B,” respectively. The cross-chain data oracle is represented by the rectangle labeled “Cross-Chain Data Oracle,” and the real-world application is represented by the rectangle labeled “Real-World Application.” The arrows indicate that Chain A sends a request to the cross-chain data oracle, which fetches the data from Chain B and sends it to both Chain A and the real-world application.

For example, consider a decentralized exchange that operates on a blockchain network. The exchange uses a cross-chain oracle to retrieve data from another blockchain network, such as the current price of an asset. This allows the exchange to offer trading in assets that are native to different blockchains, making it possible for users to trade assets across different networks.

Another example is a decentralized finance (DeFi) platform that operates on one blockchain network, but allows users to use assets from another blockchain network. The DeFi platform uses a cross-chain oracle to bridge assets between the two networks, making it possible for users to use their assets in the DeFi platform, even though they were originally issued on a different blockchain network.

Cross-chain oracles play a critical role in promoting blockchain interoperability and helping to advance the decentralized finance ecosystem. By enabling seamless communication and transfer of information and assets between different blockchains, cross-chain oracles help to break down barriers and create a more connected and interoperable blockchain landscape.

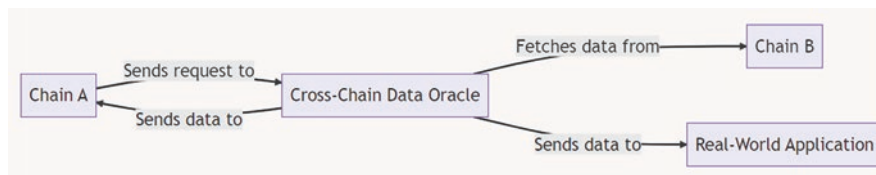


Fig. 9.3 Cross-Chain Oracles

9.1.4 Compute-Enabled Oracles

Compute-enabled oracles are an emerging type of oracle that is gaining popularity in smart contract applications. These oracles use secure off-chain computation to offer decentralized services that may be impractical or impossible to perform on-chain due to technical, legal, or financial limitations.

In Fig. 9.4, the smart contract is represented by the rectangle labeled “Smart Contract,” the Chainlink node is represented by the rectangle labeled “Chainlink Node,” the compute-enabled oracle is represented by the rectangle labeled “Compute-Enabled Oracle,” and the external API is represented by the rectangle labeled “External API.” The arrows indicate the flow of data and computation. The smart contract requests data from the Chainlink node, which routes the request to the compute-enabled oracle. The compute-enabled oracle uses data from the external API to perform computation and sends the result back to the Chainlink node, which then sends the result to the smart contract.

For instance, Chainlink Automation uses compute-enabled oracles to trigger smart contracts execution based on predefined real-world events, automating complex processes and eliminating the need for manual intervention. This approach enhances efficiency and security in smart contract execution.

Another example is the use of zero-knowledge proofs, a form of secure computation that enables privacy-preserving computations. Compute-enabled oracles can perform these proofs off-chain, providing smart contracts with a secure way to access private data without exposing it to the public.

Additionally, compute-enabled oracles can run verifiable randomness functions, which are critical for decentralized applications such as gaming and lotteries. These oracles offer a tamper-proof and provably fair source of randomness to smart contracts, ensuring that they operate in a transparent and equitable manner.

9.1.5 Other Types of Oracles

In addition to oracles listed above in this chapter, there are other types of oracles that can provide valuable services to smart contracts. These include:

- Trusted Computing Environment (TEE) is a technology that is increasingly used to protect sensitive data. For high-end sensors or servers, the TEE can be used to

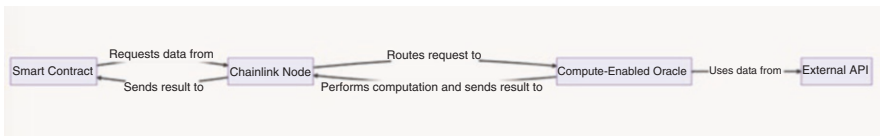


Fig. 9.4 Compute-Enabled Oracle

digitally sign collected data, ensuring that data cannot be tampered with during transmission. The TEE physically protects the private key used for signing, making the key invalid without the physical subject. This guarantees that only authorized parties can access the data and that any unauthorized changes to the data will be unsuccessful. Other similar technologies that can be used for protection include Secure Element Physical UnclonableFunction (PUF) and other technologies. Estonia is an excellent example of how TEE can be used to protect authenticity of voters record. The country allows citizens to vote electronically using their national ID cards, which contain a TEE that ensures the private key is physically protected and cannot be used without the physical ID card. This makes it virtually impossible for anyone to hack the voting system or tamper with votes during transmission (Lohrmann, 2020).

- On-chain asset tracking is another way to ensure data authenticity. This technology is used for assets with unique physical properties that can be measured. For instance, Everledger uses the unique physical properties of diamonds to create a chain of custody for precious stones, preventing the circulation of fake diamonds (Williams & Kaplan, 2017). This technology ensures that the data about the asset is stored in a distributed ledger that is tamper-proof, making it difficult for fraudsters to manipulate the data.
- Artificial intelligence and machine learning can also be used to increase the authenticity of data. These technologies can be used to identify and filter out fake data, making it easier to verify the authenticity of uplinked data. By analyzing large volumes of data, these technologies can detect patterns and anomalies, helping to identify fake data.
- Video surveillance and other security controls are another important component of data authenticity. These technologies can be used to monitor assets and provide additional security to prevent fraud or theft. For example, video surveillance can be used to monitor the movement of assets and identify any suspicious activities. Other security controls can be used to restrict access to data, making it more difficult for unauthorized parties to gain access.

9.2 Examples of Data Oracle Providers

There are several ways to ensure the authenticity of data provided by a data oracle, including:

Cryptographic techniques: Data oracles can use cryptographic techniques, such as digital signatures and hash functions, to ensure the integrity and authenticity of the data being provided.

Decentralization: Data oracles can be implemented as decentralized networks, which can help to ensure the authenticity of the data by making it harder for a single entity to control or manipulate the data.

Governance: Data oracles can use decentralized governance models to ensure the authenticity of the data by aligning the interests of oracle operators with those of the network.

Reputation: Data oracles can use reputation systems to ensure the authenticity of the data by incentivizing oracle operators to provide accurate and reliable data.

Ensuring the authenticity of data provided by a data oracle is important for the integrity and trustworthiness of a blockchain application, as it helps to ensure that the smart contract is executing correctly and producing reliable results.

This section highlights several oracle providers which used cryptographic techniques, decentralization, governance, and reputation to improve data authenticity.

Chainlink

Chainlink is a decentralized oracle network that allows smart contracts to access external data and off-chain resources. It uses a network of independent oracle nodes to fetch data from external sources and feed it into the blockchain via secure and transparent mechanisms. Chainlink has been widely adopted by a number of blockchain projects and has partnerships with major companies and organizations.

Band Protocol

Band Protocol is a decentralized oracle platform that allows developers to build their own oracles and use them to access external data and information. It uses a decentralized governance model to ensure the integrity and trustworthiness of the oracles on the platform. Band Protocol has been used in a number of decentralized applications (DApps) and has partnerships with major companies and organizations.

UMA

UMA (Universal Market Access) is a decentralized financial contracts platform that uses data oracles to provide real-time pricing data to smart contracts. It allows users to create and trade synthetic assets that track the value of real-world assets, such as stocks, commodities, and currencies. UMA uses a decentralized governance model to ensure the integrity and reliability of its oracles.

Nest Protocol

Nest Protocol is a decentralized oracle platform that allows developers to build their own oracles and use them to access external data and information. It uses a decentralized governance model and a system of incentives to ensure the integrity and trustworthiness of the oracles on the platform. Nest Protocol has been used in a number of decentralized applications and has partnerships with major companies and organizations.

Table 9.1 compares each oracle provider based on publicly available sources. Cryptographic techniques used by these projects may vary depending on specific use cases and implementations. The degree of decentralization is subjective and may change over time. Governance models can also change as projects evolve. Reputation technologies can be either on-chain or off-chain.

Each of the data oracles listed in the table has a unique approach to solving the data authenticity problem in web3 applications. For example, Chainlink utilizes

threshold signatures as a consensus mechanism to ensure that data is verified by a network of trusted data providers.

Band Protocol, on the other hand, utilizes a delegated proof of stake consensus mechanism, which allows token holders to elect validators to provide data.

UMA takes a different approach, relying on economic incentives to encourage data providers to submit accurate data.

Nest Protocol utilizes a unique nesting consensus mechanism that combines multiple sources of data to arrive at a consensus, while API3 uses a community-driven governance approach to ensure the accuracy and reliability of data.

Overall, the architecture, consensus mechanisms, and incentives used by each data oracle differ significantly, and developers must carefully evaluate the pros and cons of each solution when selecting a data oracle for their project. By doing so, they can ensure that their smart contracts have access to reliable and trustworthy data, improving the security and functionality of their web3 applications.

The following provides further analysis of the benefits and drawbacks of each data oracle approach, with a focus on scalability, reliability, and cost-effectiveness:

1. Chainlink:

- Benefits:
 - Decentralized architecture provides high security and reliability.
 - Threshold signatures consensus mechanism ensures data accuracy and tamper-proofing.
 - LINK tokens incentivize data providers to submit accurate data.
- Drawbacks:

Table 9.1 Data oracle providers comparison

Project	Cryptographic Techniques	Degree of Decentralization	Governance	Reputation
Chainlink	Elliptic curve cryptography, hash functions, digital signatures	Highly decentralized	Decentralized governance	On-chain reputation
Band protocol	Multi-party computation, threshold signatures, hash functions	Moderately decentralized	DAO governance	On-chain reputation
UMA	Zero knowledge proofs, hash functions, digital signatures	Moderately decentralized	Tokenholder governance	On-chain reputation
Nest protocol	Elliptic curve cryptography, hash functions, digital signatures	Moderately decentralized	DAO governance	On-chain reputation
API3	Hash functions, digital signatures, threshold signatures	Highly decentralized	DAO governance	Off-chain reputation

- Requires a large number of trusted data providers to achieve a high level of decentralization, which may limit scalability.
- Cost may be a factor for small-scale projects, as the use of LINK tokens may be expensive.

2. Band Protocol:

- Benefits:
 - Delegated proof of stake consensus mechanism provides fast and efficient verification of data.
 - BAND tokens incentivize data providers to submit accurate data.
 - Decentralized architecture provides high security and reliability.
- Drawbacks:
 - The use of delegated proof of stake may limit decentralization and reduce security.
 - The need for token holders to elect validators may limit scalability.

3. UMA:

- Benefits:
 - Economic incentives incentivize data providers to submit accurate data.
 - Decentralized architecture provides high security and reliability.
 - Allows for customizable data feeds.
- Drawbacks:
 - Economic incentives may be expensive and may not be sustainable in the long term.
 - The need for users to hold UMA tokens may limit adoption and scalability.

4. Nest Protocol:

- Benefits:
 - The nesting consensus mechanism provides a high level of accuracy and reliability.
 - NEST tokens incentivize data providers to submit accurate data.
 - Hybrid architecture provides scalability and decentralization.
- Drawbacks:
 - The nesting consensus mechanism may be complex and difficult to implement.
 - The need for NEST tokens may limit adoption and scalability.

5. API3:

- Benefits:

- Community-driven governance provides high transparency and accountability.
- Hybrid architecture provides scalability and decentralization.
- API3 tokens incentivize data providers to submit accurate data.
- Drawbacks:
 - Community-driven governance may be slow and cumbersome.
 - The need for API3 tokens may limit adoption and scalability.

In addition to the oracle providers listed above, there are other oracle providers used in various business uses cases:

Witnet

Witnet is a decentralized oracle network where nodes earn or lose reputation based on their correct or incorrect fulfillment of data requests, as determined by a consensus algorithm. Nodes are randomly chosen for jobs and mining blocks based on their network reputation, making majority attacks more difficult. Reputation is constantly redistributed at each block to prevent centralization and exit scams, using a demurrage function. Witnet is a separate blockchain that provides decentralized oracle services via bridge nodes, offering a scalable solution with reduced on-chain operation fees and the ability to fix critical vulnerabilities as a last resort. More information can be found at <https://witnet.io> or in their whitepaper.

Oraclize

Oraclize is a London-based cybersecurity company offering a centralized solution to blockchain oracles. While it is available on multiple blockchain platforms (Bitcoin, Ethereum, Monax, Rootstock, Corda, and private networks), the majority of their customers are working on Ethereum.

Their approach is to leverage all TEE environment providers to minimize vulnerability. This is what they call sandboxing. Oraclize leverages the products of IT providers and manufacturers (including Amazon's EC2, Google's SafetyNet, Qualcomm's QSEE, Ledger's Nano S and Intel's SGX) as key components of its own core service (the Oraclize technology). They are physically grouped within a unique environment and leveraged together: Oraclize has designed ad-hoc custom applications as well as a software layer connection for all of TEEs to make them interoperable. By collecting the data from multiple TEEs, even if one technology were to be compromised by a vulnerability such as Spectre for Intel's SGX, the overall aggregation of value would still ignore the compromised data point (assuming the vulnerability was architecture specific, and not a generic one hitting all processors).

To achieve distributed trust and the integrity of their data, Oraclize has been relying on TLS-Notary to digitally sign TLS data from https websites. This comes at cost: Oraclize can in theory only deliver data as shown on the website with no post-processing off-chain, but this already covers many use cases. The main risk here remains that if too many data sources are compromised, there is no way to prevent

wrong data from being propagated, but this risk is also present in the more “decentralized” solutions.

Town Crier

Town Crier acts as a bridge between smart contracts on any blockchain and https-enabled websites with TLS layer handling handshakes for secure communication to deliver source-authenticated data. The approach taken is different to TLS-notary (security at software level only), allowing for more customizable data relaying.

The data is collected by nodes running on Intel’s SGX (security at both software and hardware level). This authenticated data feed is delivered from enclave to the blockchain, solely relying on the SGX protection to testify the node is indeed running the software as expected.

To protect confidentiality, messages are only decrypted inside the Trusted Execution Environment’s enclave, which can thus be used not only for safe data transfer but also for ingesting encrypted user credentials (e.g., private API). In addition, custom requests are supported for potentially multiple web-scraping target.

Their approach to tackle single points-of-failure is to aggregate both data source and data oracles on multiple SGX platforms. The software has proven to be relatively scalable with throughputs of 15–65 transactions/sec.

9.3 Oracle Use Cases

As the world becomes increasingly digital, the need for reliable and accurate data has never been more important. In the realm of Web3, this is where data oracles come in. The importance of data oracles cannot be overstated, as they are essential for ensuring trust, security, and transparency in various industries, including DeFi, NFTs, insurance, enterprise supply chain management, prediction markets, and sustainability initiatives. In this section, we will explore the different use cases of data oracles in each of these areas and discuss some examples. By the end of this section, you will have a better understanding of the critical role data oracles play in the Web3 ecosystem and how they can be leveraged to transform various industries.

9.3.1 Decentralized Finance (DeFi)

A large portion of the decentralized finance (DeFi) ecosystem requires oracles to access financial data about assets and markets. For example, decentralized lending protocol uses price oracles to determine users’ borrowing capacity and check if users’ positions are undercollateralized and subject to liquidation. Similarly, synthetic asset platforms use price oracles to peg the value of tokens to real-world assets and automated market makers (AMMs) use price oracles to help concentrate liquidity at the current market price to improve capital efficiency.

There are numerous examples of successful implementations of oracle data in DeFi. Here are a few notable examples:

Aave: Aave is a lending platform that uses oracles to determine the value of collateral. This allows the platform to adjust loan-to-value ratios based on changes in the value of the collateral.

Synthetix: Synthetix is a platform that allows users to trade synthetic assets. Oracles are used to provide price feeds for these assets, allowing users to trade them with confidence.

There are a variety of technologies and formulas used in the collection and analysis of oracle data in DeFi. Here are a few examples:

Linear interpolation: Linear interpolation is a technique used to estimate a value between two known values. This is commonly used in price feeds, where the price of an asset may not be available at a specific point in time.

Weighted average: Weighted average is a technique used to calculate an average based on the importance or weight of each data point. This is commonly used in price feeds, where the price of an asset may be based on multiple exchanges or data sources.

Time-weighted average price (TWAP): TWAP is a formula used to calculate the average price of an asset over a specified period of time. This is commonly used in price feeds to provide a more accurate representation of the true value of an asset.

Oracle data plays a critical role in the DeFi ecosystem, providing reliable, accurate data for a variety of applications. By following best practices and using trusted, decentralized oracles, DeFi platforms can ensure that.

9.3.2 Dynamic NFTs and Gaming

Oracles enable dynamic NFTs (Non-Fungible Tokens that can change in appearance, value, or distribution based on external events like the time of day or the weather). Additionally, compute oracles are used to generate verifiable randomness that projects then use to assign randomized traits to NFTs or to select random lucky winners in high-demand NFT drops. On-chain gaming applications also use verifiable randomness to create more engaging and unpredictable gameplay experiences like the appearance of random loot boxes or randomized matchmaking during a tournament. The following are example projects:

Dynamic NFTs: An example of a project that uses oracles for dynamic NFTs is Ether Cards, which is a platform that allows users to create and collect customizable NFT cards with dynamic traits. Ether Cards uses Chainlink VRF (Verifiable Randomness Function) to generate random traits for the cards, such as discounts, access rights, royalties, etc. Ether Cards also uses Chainlink API calls to enable the cards to change based on external events, such as sports scores, crypto prices, social media trends, etc.

Verifiable randomness for NFT traits: The “CryptoPunks” NFT collection is an example of NFTs that use verifiable randomness generated by oracles. Each

CryptoPunk has a randomized set of traits (e.g., punk hair, accessories, facial features) that were assigned using a verifiable randomness function. This ensures that no two CryptoPunks are identical and creates scarcity and uniqueness within the collection.

Randomized gameplay experiences: The on-chain game “Axie Infinity” uses oracles to generate verifiable randomness for various gameplay elements. For example, the appearance of random loot boxes that contain valuable in-game items is determined by an oracle-generated random number. Additionally, randomized matchmaking during tournaments ensures that players are paired up in a fair and unpredictable way, creating a more engaging and challenging gameplay experience.

9.3.3 Insurance

Insurance smart contracts use input oracles to verify the occurrence of insurable events during claims processing, opening up access to physical sensors, web APIs, satellite imagery, and legal data. Output oracles can also provide insurance smart contracts with a way to make payouts on claims using other blockchains or traditional payment networks.

The following is the examples of oracle use in insurance.

Arbol: Arbol uses IoT sensors to monitor weather conditions, such as temperature, rainfall, and wind speed, in real time. The data collected by the sensors is then fed into smart contracts, which automatically trigger payouts to policyholders if certain predefined conditions are met. For example, if the temperature in a certain area drops below a certain threshold, a smart contract could automatically initiate a payout to farmers who have taken out weather-related insurance policies (Arbol, 2021).

Etherisc: Etherisc uses oracles to access external data sources, such as flight information APIs, to determine whether a policyholder’s flight has been delayed or cancelled. When a delay or cancellation occurs, the smart contract automatically triggers a payout to the policyholder based on the terms of their insurance policy (Cuenca, 2022).

AIG and Standard Chartered: AIG, IBM, and Standard Chartered completed a pilot project in 2017 that used smart contracts and oracles to automate trade finance transactions, including insurance coverage. The project involved using smart contracts to automatically trigger insurance payouts when certain conditions were met, such as when goods were delivered to a certain location. Oracles were used to provide external data, such as shipping information, to the smart contracts (BusinessWire, 2017).

9.3.4 *Enterprise Supply Chain Management*

Supply chain management is the process of planning, coordinating, and executing the flow of materials, products, and information from suppliers to customers in an efficient and effective way. Data oracles are used to connect blockchain-based smart contracts to external data sources, such as sensors, APIs, databases, or other blockchains. Data oracles can provide information such as temperature, location, quality, quantity, and status of goods along the supply chain to smart contracts. This can enable automation, verification, and optimization of supply chain processes. Some examples of companies using data oracles in their supply chain management are ADNOC, De Beers, Walmart, Zara, and Everledger (Sharma, 2022).

Abu Dhabi National Oil Company (ADNOC): ADNOC has partnered with IBM to use blockchain to track, validate, and execute transactions across its oil and gas value chain. The blockchain platform uses smart contracts and IoT devices to automate the accounting and reconciliation processes, reduce operational costs, and increase transparency.

De Beers: De Beers has developed a blockchain platform called Tracr to trace the provenance and quality of diamonds from mine to retail. The platform uses smart contracts and digital certificates to verify the authenticity and ethical sourcing of diamonds, as well as to prevent fraud and theft.

Walmart: Walmart has collaborated with IBM and other partners to use blockchain to improve food safety and traceability. The blockchain platform uses smart contracts and IoT sensors to record data such as temperature, location, and expiration date of food products along the supply chain. This enables Walmart to quickly identify and recall contaminated products, as well as to reduce waste and spoilage.

Zara: Zara has implemented a blockchain solution called Loomia to enhance its fast fashion supply chain. The solution uses smart contracts and RFID tags to track the movement of garments from production to distribution to retail. This helps Zara optimize its inventory management, reduce costs, and increase customer satisfaction.

Everledger: Everledger is a company that uses blockchain to create digital passports for wine bottles. The digital passports contain information such as grape variety, vintage, origin, quality, and ownership history of each bottle. The blockchain platform uses smart contracts and NFC tags to verify the authenticity and provenance of wine bottles, as well as to prevent counterfeiting and fraud.

9.3.5 *Prediction Markets*

Decentralized prediction markets are platforms that allow users to create and trade on the outcome of events, such as political elections, sports games, or even the weather. These markets operate using a decentralized network of participants, who

buy and sell shares in various outcomes based on their predictions of the event's outcome.

To participate in a prediction market, users must first buy shares in the possible outcomes of the event. For example, in a prediction market for a political election, users might buy shares in the candidates they think will win. The price of these shares fluctuates based on supply and demand, with the price of the winning outcome eventually settling at 1 and the price of the losing outcome settling at 0.

In order to determine the final outcome of the event and settle the market, prediction markets rely on oracles. Oracles are trusted sources of off-chain data that are used to determine the outcome of the event. For example, in a prediction market for a sports game, an oracle might be used to provide the final score of the game.

Augur and Gnosis, two popular decentralized prediction market platforms, each use their own unique oracle systems.

Augur uses a decentralized network of oracles, which are selected by Augur token holders based on their reputation and accuracy in reporting outcomes. Once an outcome is determined, the oracles report the result to the Augur smart contract, which automatically settles the market and pays out winnings to the users who correctly predicted the outcome.

Gnosis, on the other hand, uses a centralized oracle system called the Gnosis Olympia Oracle. The Olympia Oracle is a consortium of trusted data providers who are responsible for reporting the outcome of events to the Gnosis platform. Once an event is resolved, the Gnosis smart contract uses the Olympia Oracle's data to determine the final outcome and automatically settle the market.

9.3.6 Sustainability

In recent years, there has been a growing interest in using blockchain technology and smart contracts to support environmental initiatives, such as carbon offsetting and sustainable land management. Oracles play a critical role in these efforts by providing smart contracts with environmental data from a variety of sources, including sensors, satellite imagery, and advanced machine learning computation. This data can then be used to automatically trigger rewards, verify the effectiveness of environmental projects, and support the creation of new forms of carbon credits. Here are some examples of companies and projects that are using oracles to support these efforts:

Supplying Smart Contracts with Environmental Data

Ocean Protocol: Ocean Protocol is a decentralized data exchange that allows individuals and organizations to share and monetize their data. The platform uses oracles to securely connect data sources, such as sensors and satellite imagery, with smart contracts. This allows the data to be used for a variety of applications, including tracking environmental metrics and supporting sustainable practices.

ClimateTrade: ClimateTrade is a carbon offset marketplace that uses blockchain and smart contracts to automate the purchase and verification of carbon offsets. The platform uses oracles to gather environmental data, such as carbon emissions data from industrial sources, and feed it into smart contracts. These smart contracts then automatically initiate the purchase and transfer of carbon offsets to buyers, providing a more transparent and efficient way to offset carbon emissions.

ClimateCHECK: ClimateCHECK is a software platform that helps companies track, measure, and report their carbon emissions. The platform uses oracles to gather environmental data from a variety of sources, such as energy usage data and transportation data, and feed it into smart contracts. These smart contracts then automatically calculate the company's carbon emissions and provide recommendations for reducing them.

Supporting New Forms of Carbon Credits

Nori: Nori is a marketplace for carbon removal credits that uses blockchain and smart contracts to automate the purchase and verification of carbon removal services. The platform uses oracles to gather environmental data, such as soil carbon levels and tree growth rates, from a network of trusted data providers. This data is then used to verify the effectiveness of carbon removal projects and provide a more transparent and trustworthy way to buy and sell carbon removal credits.

9.4 Oracle Design Considerations

Oracles play a critical role in the blockchain ecosystem by providing off-chain data to smart contracts. However, designing an oracle requires careful consideration of several factors to ensure the accuracy, reliability, and security of the data provided to the smart contract. The design considerations for oracles include correctness, availability, incentive compatibility, data quality, security, scalability, and cost transparency. Correctness involves ensuring the authenticity and integrity of the data provided to the smart contract to prevent state changes based on invalid information. Availability is essential to enable smart contracts to access off-chain data without delay or interruption. Incentive compatibility incentivizes off-chain data providers to submit accurate information, enabling rewards or penalties based on information quality. Data quality is crucial to ensuring the accuracy of the smart contract's execution, and the oracle should source data from multiple trusted sources and verify the accuracy of the data. Security measures such as encryption, authentication, and authorization must be integrated into the oracle design to prevent malicious actors from manipulating the data. Scalability is also critical, and the oracle must be designed to handle a high number of requests per second and manage data storage and retrieval efficiently. Lastly, the cost of using the oracle should be transparent and cost-effective. In this article, we will explore each of these design considerations in detail and discuss best practices for designing oracles that meet the needs of the blockchain ecosystem.

Correctness: An oracle should provide valid off-chain data that does not cause smart contracts to execute state changes based on invalid information. This requires the authenticity and integrity of data, meaning that it was obtained from the correct source and not tampered with before being sent on-chain. For example, Certified Origins is using the Oracle Blockchain Platform (OBP) to verify the authenticity of its Italian extra virgin olive oil and to streamline billing and purchase orders (Shaw, 2020).

Availability: An oracle should ensure that smart contracts can access off-chain data without delay or interruption, enabling them to execute actions and trigger state changes promptly. For example, Chainlink oracle networks aggregate data from a number of decentralized ChainLink nodes to remove any single point of failure in the delivery of data to the blockchain. This provides strong guarantees to users around the availability, accuracy, and the tamper-proof nature of sourcing off-chain data and delivering it on-chain.

Incentive Compatibility: An oracle should incentivize off-chain data providers to submit accurate information to smart contracts. This involves attributability and accountability, allowing for the correlation of external information to its provider and the bonding of data providers to the information they provide, enabling rewards or penalties based on information quality.

Data Quality: The quality of data provided by the oracle must be high to ensure the accuracy of the smart contract's execution. The oracle should source data from multiple trusted sources and have a mechanism to verify the accuracy of the data.

Security: The oracle must be secure to prevent malicious actors from manipulating the data provided to the smart contract. The oracle should be designed with security features such as encryption, authentication, and authorization.

Scalability: The oracle must be scalable to handle the large volume of data required by Web3 applications. The oracle should be designed to handle a high number of requests per second and have a mechanism to manage data storage and retrieval efficiently.

Cost: The cost of using the oracle should be considered when designing the oracle. The oracle should be cost-effective, and the cost of using the oracle should be transparent to the users.

In addition to the previously mentioned oracle design patterns, there are two other commonly used patterns that depend on the specific use case: request-response and publish-subscribe. The request-response pattern allows client contracts to request specific data that may be too large to store on the blockchain, while the publish-subscribe pattern provides a data feed that can be read by multiple smart contracts.

Publish-subscribe Oracles

An oracle service based on a publish-subscribe mechanism exposes a “data feed” which other contracts can regularly read for information. The data in this case is expected to change frequently, so client contracts must listen for updates to the data in the oracle's storage. An excellent example is an oracle that provides information on the latest ETH-USD price to users.

Request-response Oracles

Request-response oracles are an alternative oracle design pattern that allows smart contracts to request arbitrary data that is not provided by a publish-subscribe oracle. This design pattern is particularly useful when the dataset is too large to be stored on the blockchain or when users only need a small part of the data at any given time. In a request-response setup, the oracle has an on-chain component that receives data requests from client contracts and passes them to an off-chain node for processing. However, users initiating data queries must cover the cost of retrieving information from the off-chain source. Additionally, the client contract must provide funds to cover the gas costs incurred by the oracle contract in returning the response via the callback function specified in the request.

9.5 Security Attacks on Oracles

As the use of smart contracts and blockchain technology continues to grow, the importance of data oracles in facilitating communication between off-chain data sources and on-chain smart contracts cannot be overstated. However, data oracles are vulnerable to a range of potential attacks that can compromise the integrity and security of the system. These attacks include oracle spoofing, tampering, censorship, denial of service, front-running, bribery, extortion, and insider attacks. In order to ensure the reliability and accuracy of data oracles, it is crucial to implement strong security protocols and cryptographic techniques, as well as secure key management practices to protect against these types of attacks.

1. Oracle manipulation: This attack involves a malicious actor altering or manipulating the data provided by a data oracle, potentially leading to incorrect execution of a smart contract.
2. Oracle spoofing: This is a type of attack that involves a malicious actor presenting false or fraudulent data to a data oracle, potentially leading to incorrect execution of a smart contract. For example, an attacker could manipulate the data that is being fed into the smart contract, causing it to execute in a way that benefits the attacker. This could be done by presenting false data to the oracle, which would then be used to execute the smart contract. The attacker could then use this to their advantage, potentially causing financial harm to the victim.
3. Oracle censorship: This attack involves a malicious actor preventing a data oracle from accessing or providing certain data, potentially disrupting the execution of a smart contract.
4. Oracle Denial of Service (DoS): This attack involves overwhelming a data oracle with traffic or requests, making it unavailable to legitimate users and potentially disrupting the execution of a smart contract.
5. Oracle front-running: This attack involves a malicious actor manipulating the data provided by a data oracle to gain an unfair advantage in a smart contract execution.

6. Oracle bribery: This attack involves a malicious actor attempting to bribe or coerce a data oracle operator to provide false or fraudulent data, potentially leading to incorrect execution of a smart contract.
7. Oracle extortion: This attack involves a malicious actor threatening to disrupt or manipulate the data provided by a data oracle unless the operator pays a ransom or performs a specific action.
8. Oracle insider attack: This attack involves an insider (e.g., an employee or contractor) at a data oracle provider intentionally providing false or fraudulent data, potentially leading to incorrect execution of a smart contract.

It is important to protect against these types of attacks on data oracles, as they can have serious consequences, including financial losses, reputational damage, and the loss of trust in the system. This can be achieved through the use of secure cryptographic techniques, secure key management practices, and strong security protocols. We will discuss the countermeasures to prevent these attacks in the next section.

The following are some real-world examples of attacks on data oracles that have been reported:

Oracle Manipulation Attack: According to a report from Chainalysis, hackers stole \$386.2 million from DeFi protocols in 2022 using “oracle manipulation” attacks. This type of attack involves artificially inflating the trading volume of a low-liquidity token on a DeFi protocol to spike its price. The hackers then use flash loans to secure the initial capital needed to inflate the token’s trading volume, trade the designated token for a more stable crypto asset after pumping up the price, and leave the DeFi protocol insolvent. Chainalysis outlines the case of Avraham Eisenberg, who used \$10 million worth of USDC to short 488 million MNGO (Mango governance token) and artificially inflate its price, leading to losses for Mango Markets.

(Devitt, 2023)

Other example includes Synthetix, a synthetic asset issuance platform built on Ethereum, which experienced an oracle manipulation attack which netted the attacker over 37 million sETH (Synthetic Ether) in June 2019. The true dollar value is difficult to calculate given the relative illiquidity of sETH on secondary markets. The attack was carried out by exploiting a vulnerability in the oracle used by Synthetix to manipulate the price of a synthetic asset and profit from the resulting arbitrage opportunity. The attack resulted in losses of approximately \$1 million (Todd, 2019).

Oracle spoofing attack: In 2020, an attacker exploited a vulnerability in the oracle used by the decentralized exchange (DEX) bZx to manipulate the price of a synthetic asset and profit from the resulting arbitrage opportunity. The attack resulted in losses of approximately \$8 million. Although bZx was able to recover the funds, the reputation damage to the project is significant (Balakrishnan, 2020).

As oracles play more significant roles in the Web3 ecosystem, we expect more attacks and different and even new attacks on oracle. Web3 users and developers

need to be vigilant to get informed and Web3 project teams need to implement better oracle solutions to counter attacks.

9.6 Countermeasures to Oracle Security Attacks

As we discussed in the last sections, oracles are a potential weak point in the security of blockchain systems, as they can be susceptible to various types of attacks, such as spoofing, tampering, censorship, denial of service (DoS), front-running, bribery, extortion, and insider attacks. To address these security concerns, various countermeasures can be implemented.

Oracle manipulation: One potential countermeasure to prevent oracle manipulation is to use cryptographic techniques such as digital signatures and hash functions. Digital signatures can be used to authenticate the data provided by the oracle, ensuring that it has not been altered in transit. When the oracle signs the data, it produces a unique digital signature that can be verified by the smart contract to ensure that the data has not been tampered with.

Hash functions can be used to provide data integrity. A hash function takes an input and produces a fixed-length output, which is a unique representation of the input data. If the input data changes, even slightly, the resulting hash value will also change. By storing and verifying the hash value of the data provided by the oracle, smart contracts can ensure that the data has not been altered.

For example, consider a smart contract that executes based on the current temperature of a particular location. An oracle provides this data to the smart contract. To prevent oracle manipulation, the oracle can digitally sign the temperature data, and the smart contract can verify the digital signature. Additionally, the oracle can provide a hash value of the temperature data, and the smart contract can verify that the hash value matches the data provided by the oracle, ensuring data integrity.

Oracle spoofing: To prevent oracle spoofing, one potential countermeasure is to use multiple data sources and require consensus among them before allowing a smart contract to execute. By using multiple sources, the probability of all sources being spoofed simultaneously decreases. Consensus among the sources is then required to ensure that the data provided by the oracle is accurate and reliable.

There are several ways to implement this countermeasure. One way is to use a decentralized oracle network where multiple oracles provide data to the smart contract. The smart contract can then require a majority or consensus of the oracles to ensure the accuracy of the data. For example, Chainlink is a decentralized oracle network that provides decentralized data feeds to smart contracts and uses multiple oracles to ensure the accuracy of the data.

Another way to implement this countermeasure is to use multiple independent data sources outside of the blockchain network, such as API services or trusted third-party data providers. The smart contract can then compare the data provided by the different sources and require consensus among them before executing. For example, a smart contract that executes based on the current market price of a

particular asset can use multiple independent data sources, such as several financial data providers or exchanges, to ensure the accuracy of the price data.

Furthermore, blockchain networks can use different consensus algorithms to ensure the accuracy of the data provided by oracles. For example, Proof of Authority (PoA) consensus algorithm can be used to establish a set of trusted authorities, who then validate the data provided by the oracle. If a majority of the authorities agree on the data, the smart contract can execute.

Oracle censorship: To prevent oracle censorship, one potential countermeasure is to use decentralized oracle networks that are resistant to censorship, such as those based on peer-to-peer protocols. Decentralized oracle networks remove the need for centralized authorities to provide data to smart contracts, making them less susceptible to censorship. In a peer-to-peer network, nodes can communicate directly with each other, eliminating the need for intermediaries, and allowing nodes to act as both providers and consumers of data.

There are different ways to implement this countermeasure. One way is to use a blockchain network that includes a built-in decentralized oracle system. For example, Chainlink uses a decentralized oracle network that uses a combination of cryptographic proofs, reputation systems, and market incentives to ensure that the data provided to smart contracts is accurate and tamper-proof. In this system, data providers and consumers can interact directly without the need for intermediaries, making it resistant to censorship.

Another way to implement this countermeasure is to use a distributed oracle network that uses a consensus algorithm to validate the data provided by the oracles. In such a system, data providers can form consensus on the data they provide to smart contracts, eliminating the need for centralized authorities to validate the data. For example, Oraclize is a distributed oracle network that provides a trusted source of data to smart contracts by using a consensus mechanism that involves multiple oracles.

Additionally, blockchain networks can use peer-to-peer protocols, such as IPFS (InterPlanetary File System), to store and distribute the data used by oracles. IPFS allows data to be stored and accessed by nodes on the network, removing the need for centralized authorities to provide the data. By using peer-to-peer protocols, blockchain networks can ensure that the data used by oracles is resistant to censorship.

Oracle Denial of Service (DoS): To prevent Oracle DoS attacks, one potential countermeasure is to use distributed oracle networks that are resistant to DoS attacks, such as those that use redundant nodes or use sharding techniques to distribute the load. Distributed oracle networks have multiple nodes that can provide data to smart contracts, making them more resilient to DoS attacks. In a redundant system, if one node fails or is overloaded, the other nodes can take over and continue to provide data to smart contracts.

There are different ways to implement this countermeasure. One way is to use a blockchain network that includes a distributed oracle system with redundant nodes. In this kind of system, if one node fails or is attacked, the other nodes can continue to provide data, making it resistant to DoS attacks.

Another way to implement this countermeasure is to use sharding techniques to distribute the load. Sharding involves breaking down data into smaller, more manageable pieces and distributing them across multiple nodes. By doing so, the workload is distributed among multiple nodes, making it harder for an attacker to overwhelm any one node. For example, Augur, a decentralized prediction market platform, uses sharding to distribute the load across multiple oracles to ensure the accuracy of its predictions.

Additionally, blockchain networks can use a variety of DoS protection mechanisms, such as rate limiting, IP blocking, and anomaly detection, to detect and mitigate DoS attacks. These mechanisms can detect abnormal behavior and limit the amount of traffic a node can receive, preventing it from being overwhelmed.

Oracle front-running: One potential countermeasure to prevent oracle front-running is to use smart contract designs that are resistant to front-running. One such design is the use of randomness in smart contracts. By using randomness, it becomes difficult for an attacker to predict the outcome of a transaction and execute a similar transaction with a higher gas price. This makes it harder for the attacker to manipulate the outcome of the original transaction.

Another countermeasure is the use of commit-reveal schemes. In this approach, the transaction details are first committed to the blockchain without revealing them, and then the details are revealed later. This approach makes it difficult for an attacker to front-run the transaction because they cannot see the details of the transaction until it is too late to execute a similar transaction with a higher gas price.

Oracle bribery: One potential countermeasure to prevent oracle bribery is to use decentralized oracle networks that are resistant to bribery. These networks rely on multiple nodes to provide data to the smart contract, making it difficult for any single node to manipulate the data. Decentralized oracle networks can use different mechanisms to resist bribery, such as decentralized governance models or incentives to align the interests of oracle operators with those of the network.

Decentralized governance models involve the selection of trustworthy nodes based on a reputation system. The reputation of nodes is based on their past performance and the value of the data they provide. This ensures that only reliable nodes are selected to provide data to the smart contract. Additionally, nodes can be incentivized to provide accurate data by staking a certain amount of cryptocurrency as collateral. This incentivizes them to provide accurate data, as they risk losing their stake if they provide inaccurate data.

Another countermeasure is to align the interests of oracle operators with those of the network. This can be achieved by providing incentives to oracle operators to provide accurate data. For example, oracle operators can earn a portion of the fees generated by the smart contract. This incentivizes them to provide accurate data and ensures that they have a stake in the success of the smart contract. If an oracle operator provides inaccurate data, they risk losing their reputation score and their ability to earn fees in the future.

Oracle extortion: One important defense mechanism is monitoring of oracle nodes. This involves closely monitoring the activity and performance of each oracle node to detect any unusual behavior or signs of compromise. This can be done

through regular audits, security checks, and vulnerability scans. If any node is found to be compromised or at risk of compromise or extortion, it can be removed from the network to prevent it from providing inaccurate data to smart contracts.

Decentralized node operations can also be used as a defense mechanism against oracle extortion. In a decentralized network, multiple nodes are responsible for providing data to smart contracts, making it difficult for an attacker to gain control of the majority of nodes. This reduces the risk of a single point of failure and makes it more difficult for an attacker to manipulate the data provided to smart contracts.

Node governance is another defense mechanism that can be used to prevent oracle extortion. This involves implementing a governance model that ensures the oracle nodes are operated in a fair and transparent manner. This can include mechanisms for selecting trustworthy node operators, implementing staking or bonding mechanisms to incentivize accurate data provision, and regular audits and security checks to ensure that nodes are not compromised.

Oracle insider attack: To prevent such attacks, several defense mechanisms can be implemented. Here are some defense methods for preventing Oracle insider attacks:

Data Access Controls: One of the ways to prevent Oracle insider attacks is to implement data access controls that restrict the amount of data that an insider can access. By restricting the access to data, it reduces the potential for malicious actors to manipulate the data.

Regular Auditing and Security Checks: Regular auditing and security checks can be conducted to monitor the behavior of insiders and detect any signs of malicious activity. This can include checking for changes in access patterns or monitoring data requests to detect any unusual or unauthorized access.

Multi-party Computation: Multi-party computation (MPC) is a technique that allows multiple parties to compute a function or algorithm without revealing their inputs to each other. This can be used to prevent insider attacks by allowing multiple data providers to compute the final output of a smart contract without any one provider having access to all the data. This technique can make it difficult for an insider to manipulate the data without being detected.

Decentralized Oracle Networks: Decentralized oracle networks can help prevent insider attacks by relying on multiple data providers to supply data to the smart contract. This reduces the dependence on any single provider and makes it more difficult for insiders to manipulate the data.

Background Checks: Conducting background checks on employees or contractors who have access to sensitive data can help prevent insider attacks. By conducting a thorough background check, it is possible to identify any past criminal activity or questionable behavior that could indicate a potential insider threat.

In summary, the data oracle space has deficiencies and security risks and is open for new developments and players to enter. Decentralization is a core value for Web3 and blockchain applications and is the key for defense against oracle attacks. Innovative oracle and blockchain providers are expected to enter the space to meet market demand.

References

- Arbol. (2021, January 12). Businesses and farmers can now hedge weather risk through the Arbol platform and Chainlink data. Arbol. Retrieved March 14, 2023, from <https://arbolmarket.medium.com/businesses-and-farmers-can-now-hedge-weather-risk-through-the-arbol-platform-and-chainlink-data-d6f36506146c>
- Balakrishnan, A. (2020, September 14). bZx recovers \$8.1M lost in third exploit. Crypto Briefing. Retrieved March 16, 2023, from <https://cryptobriefing.com/bzxs-third-exploit-2020-ends-with-8-million-lost/>
- BusinessWire. (2017, June 15). AIG, IBM, standard chartered deliver first multinational insurance policy powered by Blockchain. Business Wire. Retrieved March 14, 2023, from <https://www.businesswire.com/news/home/20170615005586/en/AIG-IBM-Standard-Chartered-Deliver-First-Multinational-Insurance-Policy-Powered-by-Blockchain>
- Cuenca, O. (2022, January 21). Etherisc launches automated blockchain travel insurance. ITIJ. Retrieved March 14, 2023, from <https://www.itij.com/latest/news/etherisc-launches-automated-blockchain-travel-insurance>
- Devitt, C. (2023, March 10). Crypto hackers stole \$386,200,000 from DeFi protocols via 'Oracle manipulation attacks' in 2022: Chainalysis. The daily Hodl. Retrieved March 29, 2023, from <https://dailyhodl.com/2023/03/10/crypto-hackers-stole-386200000-from-defi-protocols-via-oracle-manipulation-attacks-in-2022-chainalysis/>
- Lohrmann, D. (2020, September 25). Could Estonia be the model for secure online voting? Government technology. Retrieved March 29, 2023, from <https://www.govtech.com/blogs/lohrmann-on-cybersecurity/could-estonia-be-the-model-for-secure-online-voting.html>
- Sharma, S. (2022, September 8). *5 examples of Blockchain in supply chain management*. OyeLabs. Retrieved March 14, 2023, from <https://oyelabs.com/examples-of-blockchain-in-supply-chain-management/>
- Shaw, J. (2020, January 27). Making smart contracts a reality with Blockchain technology. Oracle Blogs. Retrieved March 14, 2023, from <https://blogs.oracle.com/blockchain/post/making-smart-contracts-a-reality-with-blockchain-technology>
- Todd, R. (2019, June 24). Synthetix suffers oracle attack, more than 37 million synthetic ether exposed. The Block. Retrieved March 29, 2023, from <https://www.theblock.co/linked/28748/synthetix-suffers-oracle-attack-potentially-looting-37-million-synthetic-ether>
- Williams, A. D., & Kaplan, R. P. (2017, December 22). Diamonds on the Blockchain: Building a global digital ledger for valuable assets. DEEP Centre. Retrieved March 29, 2023, from <https://deepcentre.com/wordpress/wp-content/uploads/2019/10/DEEP-Centre-Diamonds-on-the-Blockchain-December-2017.pdf>

Chapter 10

Security in Permissioned Blockchain



William Zhang

10.1 Introduction

Permissioned blockchains have been used by enterprises and government organizations for use cases from trade finance, and supply chain tracking, to central bank digital currencies. Even though they also have a chain of blocks, permissioned blockchains are different from their permissionless counterparts in that there is typically not a large number of nodes in the network. On the other hand, people typically assume that each node can be trusted, as permissioned blockchains require authorization and identity validation before a node can join the network. Therefore, the risk profile is similar to other distributed financial systems.

As a permissioned blockchain can hold a large amount of value, it is subject to cyberattacks. As the number of nodes in a permissioned blockchain is typically much smaller, compromising one could cause significant damage.

Permissioned blockchain nodes typically run within an enterprise computing environment, they can benefit from the security measures established in such environments, including identity and access management, network security, security hardening and patching, logging and monitoring, etc. It could also benefit from enterprise security measures around application security such as threat modeling (Shostack, 2014), security architecture reviews, and DevSecOps.

Security pitfalls that need special attention about permissioned blockchains include the lack of robustness of the consensus protocol when considering the limited number of nodes in the network and security around smart contracts. Another

Views presented in this book chapter are the author's own and do not represent the official position of the Bank for International Settlements (BIS) or the BIS Innovation Hub.

W. Zhang (✉)

Bank for International Settlements Innovation Hub - Nordic Centre, Stockholm, Sweden

area that is quite different from the permissionless blockchain is that there are often only a few copies of the ledger across the whole network (some protocols only keep two copies in production, one copy for each of the two parties involved in the transaction). Data backup becomes important in this case as the platform does not intrinsically provide enough data redundancy.

10.1.1 Permission Blockchain Use Cases

Some enterprises have chosen to use permissioned blockchain within their own organization or with their business partners to build DLT-based applications.

- JP Morgan Chase developed its internal blockchain, using Quorum, with JPMCoin as the token representing assets held at the bank (Morgan, 2022).
- Project Ubin has gone through multiple phases, experimenting with various permissioned blockchain technologies (Monetary Authority of Singapore, 2022).¹
- In 2018, the World Bank launched the world's first blockchain-based bond, using a permissioned blockchain based on Ethereum (World Bank, 2018).

The following are reasons that businesses may choose to use permissioned blockchains vs. public ones:

- **Privacy:** Permissionless blockchains such as Bitcoin allow anyone to join, including anonymous and pseudonymous users. However, businesses such as financial services institutions and healthcare providers work under stringent privacy requirements. They cannot allow just anyone to see sensitive information recorded on the ledger.
- **Scalability:** Most permissionless blockchains have low scalability because all the nodes on the network are required to process transactions and consensus takes minutes or tens of minutes to reach. This results in low transaction throughput.
- **Upgradability of smart contracts:** On permissionless blockchains, smart contracts cannot be changed once deployed and their execution results are irreversible. Businesses need ways to ensure they are bug-free before deploying these.
- **Storage efficiency:** Since every full node stores all the data on a typical permissionless blockchain, storage requirements are duplicated across all nodes and continually increase over time. This excessive storage redundancy is not practical for businesses.
- **More efficient consensus algorithm:** Bitcoin and Ethereum use the proof of work (POW) or proof of stake (POS) algorithms, which require lots of computing power or staking of a lot of value. For POW, as time passes, the processing power and energy requirements increase making it impractical in the business

¹ Similar projects include Jasper, Stella, and Khokha.

context. For POS, the amount of value being staked and the complexity of the incentive mechanism creates inefficiency.

- **Better governance:** Permissionless blockchains are often controlled by a developer community or a small group of people through a decentralized automated organization (DAO), who make decisions on improvements and changes. This process can be ad hoc and has been compromised by malicious players. Businesses need sufficient governance to run blockchain effectively over the long term.

10.1.2 Overview of the Chapter

After discussing the different use cases for permissioned blockchain, this chapter will go over the architecture and security features of three popular permissioned blockchain networks, namely Hyperledger Fabric, Corda, and Quorum, with Hyperledger Fabric being elaborated more as the other two have similar properties. Next, the chapter will highlight the security measures that are most important for such platforms, covering the different layers of these solutions.

10.2 Different Types of Permissioned Blockchain

10.2.1 Hyperledger Fabric

Hyperledger Fabric (Hyperledger Foundation, 2023), sometimes referred to as Fabric in the text below, is an open-source framework to implement permissioned blockchains. Digital Asset and IBM were the two companies that built the initial version of Fabric.

One can build a permissioned blockchain network using Fabric by forming a consortium of organizations, each of which would run one or more Fabric nodes. Here are some features of Fabric:

- In theory, it supports a plug-and-play model for consensus algorithms. In practice, RAFT has been adopted as the de facto consensus algorithm for Fabric.
- It uses a membership service for node onboarding and lifecycle management. A membership service provider (MSP) is the certificate authority that issues and revokes digital certificates to member nodes.
- Smart contracts in Fabric are called “chaincodes,” which are hosted using the container technology.
- It supports transaction privacy using channels.
- An ordering service is used to deliver transactions to “peers,” i.e., a group of nodes responsible for committing the transactions in the ledger.

- Endorsement policy is used to determine how many peer endorsement is required for a transaction to be validated and added to the ledger.

In a Fabric blockchain network, a node can assume one or more of the following roles:

1. Client: invokes transactions;
2. Orderer: updates transaction data;
3. Peer: receives updates from orderer and commits transactions in the ledger;
4. Endorser: a kind of peer that validates transaction authenticity.

In Fabric, transaction validation mirrors how a transaction workflow operates in normal enterprise and works as follows:

1. The transaction processing has 3 separate phases:
 - (a) Distributed logic processing and agreements involving chaincodes;
 - (b) Transaction ordering;
 - (c) Transaction validation and commit.
2. This ensures fewer levels of trust and validation across different types of nodes, thus reducing overhead;
3. A transaction lifecycle is as follows:
 - (a) A requester submits a transaction proposal to an endorser;
 - (b) The endorsement policy specifies the number and combination of endorsers required for this transaction;
 - (c) The endorser executes chaincodes to simulate the proposal to the peers through a “read/write set”;
 - (d) The endorser sends back the signed proposal responses, also called “endorsements”;
 - (e) The client submits a transaction to the orderer with digital signatures;
 - (f) The orderer creates a block of transactions and sends it to the peers;
 - (g) The peer checks whether endorsement policy was met and checks for conflicting transactions. When both checks are successful the peer commits the block in the ledger.

10.2.2 R3 Corda

The Corda distributed ledger technology is developed by R3, which is an alliance of large banks, insurers, exchanges, law firms, financial technology providers, etc. It focuses on financial applications, even though the technology can also be used for other use cases (R3, 2023).

Corda’s architecture does not consist of a chain of blocks, but rather uses a distributed database to maintain the ledger. It borrows the UTXO idea from bitcoin, and smart contract from Ethereum.

A Corda blockchain network can have the following types of nodes:

1. **Notary:** It can be one or multiple nodes, which are responsible for validating and timestamping transactions. They act as a decentralized and impartial third-party to ensure that transactions are valid and not fraudulent, including that the transaction has a valid digital signature, is not a replay of a transaction that has been executed and that the input UTXO has not been spent before. Once notarized, transactions are ready for validation and execution.
2. **Full nodes:** Full nodes are responsible for storing a copy of the ledger and verifying transactions that involve them. Full nodes have a complete record of all transactions that have occurred on the network, and they can validate transactions and check that they conform to the rules set out in smart contracts.
3. **Oracle nodes:** Oracle nodes are responsible for providing external data to the network. They act as a bridge between the Corda network and external systems, providing data such as exchange rates or stock prices. Oracle nodes can also be used to verify the authenticity of data before it is used in a transaction.

For data privacy, Corda only stores transactions on nodes that are involved in the transaction, in many cases, only the two parties who have sent or received the digital asset. CorDapps offers programmability in the Corda network, using the Kotlin programming language.

10.2.3 *Quorum*

Quorum is an enterprise blockchain platform based on Ethereum, with a focus on privacy and scalability. It ensures that participants only see the data they are allowed to, using a set of technologies collectively referred to as Tessera.

A Quorum blockchain network may have the following types of nodes:

1. **Permissioning node:** a special node that is responsible for managing the access control list (ACL) of the network. It allows network administrators to set permissions and access controls for other nodes on the network.
2. **Blockchain node:** This is the main type of node in a Quorum network. It is responsible for storing a copy of the ledger and verifying transactions that involve it. Blockchain nodes can be either regular nodes or validating nodes, depending on their role in the network.
3. **Bootnode:** This is a type of node that acts as an entry point for new nodes joining the network. It provides a list of addresses for other nodes on the network and helps new nodes to find and connect to them.

Besides using Constellation nodes to ensure the privacy of communications, Quorum uses the following technologies to ensure the privacy of transactions and computation:

1. **Private Transactions:** a private transaction manager (PTM) enables private transactions between selected parties on the network. This feature allows transactions to be executed and validated without being visible to all participants on the network.
2. **Private Smart Contracts:** Only selected parties will execute and validate such smart contracts without making them visible to other participants on the network. With private smart contracts comes a private state, as only selected parties will store and access data related to private smart contracts.
3. **Constellation:** It is responsible for managing the secure communication layer for the Quorum network. It uses an encrypted communication protocol to ensure that all messages sent between nodes are secure and private.
4. **Zero-Knowledge Proofs (ZKPs):** Quorum also supports ZKPs to ensure privacy and confidentiality. ZKPs are mathematical proofs that allow one party to prove to another that they have knowledge of a specific piece of information, without revealing the information itself. This can be used to verify the validity of a transaction without disclosing any sensitive information.
5. **Enclave Computing:** Quorum uses enclave computing to protect the privacy of transactions. Enclave computing involves running specific parts of the application code in a secure, isolated environment, such as an Intel SGX enclave. This ensures that sensitive data and processes are kept separate from other processes running on the network, further enhancing privacy and security.

10.3 Top Security Vulnerabilities in Permissioned Blockchain

Permissioned blockchains restrict access to a set of nodes that have gone through a validation process to join the network. In this regard, the nodes in a permissioned blockchain tend to be more trustworthy. Such a blockchain network could have its nodes running within an enterprise's network, or could have nodes running independently. Permissioned nodes do not necessarily mean secure nodes at the network level. The following are some potential security vulnerabilities for a permissioned blockchain network, with the caveat that not all vulnerabilities apply to a specific type of permissioned blockchain platform.

10.3.1 *Compromised Node*

Unlike a permissionless blockchain, which may have thousands of nodes, a permissioned blockchain often only has a small (often single-digit) number of nodes. This means that each node tends to have a higher level of impact within the network. It also means that if one of the nodes is compromised, the security of the entire network can be at risk. Because permissioned blockchains typically do not have strong protection against rogue nodes at the protocol level, a compromised node can

potentially manipulate the data or transactions within the blockchain. Therefore, it is essential to ensure that each node is well protected. Additionally, regular monitoring and auditing of the nodes can help detect and address any potential security breaches in a timely manner.

10.3.2 Centralization

Permissioned blockchains are more centralized than public blockchains, which means that they are more susceptible to attacks against a single entity. If the controlling node or entity is compromised, the entire blockchain network may be at risk.

Some of the functions in a permissioned blockchain (e.g., the notary node in Corda) is performed by one logical node. It is important to understand the nature of the permissioned blockchain and understand that the compromise of a small number of (sometimes even one) nodes could lead to issues with the integrity of data or transactions. It is also essential to have contingency plans in place in case of a security breach, such as data backups and disaster recovery procedures.

10.3.3 Weakness in the Permissioning Process

The integrity of a permissioned blockchain relies on the honesty of its member nodes. The process of granting access to nodes or entities that can participate in the network and validate transactions is called permissioning. If the permissioning process is weak or compromised, it can allow unauthorized or unverified nodes or entities to gain access to the network, which can lead to a network compromise. An attacker could run a rogue node and join the network through weak permissioning and manipulate the data or transactions within the blockchain.

10.3.4 Software Vulnerabilities

Same as any other software, software for permissioned blockchain platforms can have vulnerabilities, which can be exploited by attackers to compromise the security of the network. Once such vulnerabilities are made public, if not addressed in a timely manner, they can potentially allow attackers to manipulate or steal the data or assets within the blockchain.

If not managed well, software vulnerabilities can also lead to unexpected downtime or disruptions in the network, which can be costly for businesses and organizations that rely on the blockchain for their operations.

As an example, there have been three reported vulnerabilities for HyperLedger Fabric ([CVE-2022-31121](#), [CVE-2022-36023](#), [CVE-2022-45196](#)) (MITRE, 2023),

two of which were about a malformed request causing the orderer to crash, and one about repeated request of certain nature causing a denial-of-service of the blockchain network.

10.3.5 Insider Threats

Since only specific entities or nodes have access to the blockchain network, insider attacks can easily cause damage. Malicious insiders could take over a node, alter the blockchain's ledger, or access sensitive information, depending on their access privileges and motivations. When a permissioned blockchain is used to support financial transactions, the incentive for an insider to compromise the network can be quite high.

If the sensitive information being handled by the blockchain is valuable, an insider could observe what's happening in the blockchain, and benefit from either monetizing the confidential information or front-running a financial transaction that has been submitted to the blockchain but not yet executed.

10.3.6 Smart Contract Vulnerabilities

Smart contracts are an integral part of many permissioned blockchains. However, they may contain vulnerabilities that can be exploited by attackers to gain access to the blockchain network or to manipulate data. Smart contracts that are used to hold values, create values (e.g., as in cross-chain bridges), and pay automated payments are especially attractive to attackers. A compromise of such a smart contract could lead to a significant loss of funds.

10.3.7 Weakness in Consensus Protocols

For a permissioned blockchain, the consensus protocol often only takes into consideration a technical failure of the nodes but not a potential malicious behavior by them. Knowing this nature, a small group of nodes could collude to control the network and potentially manipulate transactions. This can be particularly problematic in permissioned blockchains as the number of nodes is limited and predetermined.

To mitigate this issue, a permissioned blockchain should consider whether it should employ a Byzantine Fault Tolerance (BFT) consensus protocol that is robust even if a certain percentage of nodes have become rogue. Additionally, regular node rotation and strict access controls can help prevent collusion and protect the integrity of the network.

10.3.8 Governance Issues

Permissioned blockchains are often governed by a consortium or a group of entities. The governance mechanism establishes the rules and procedures for decision-making and ensures that the network operates effectively and transparently. With permissioned blockchains, given the small number of nodes involved, there is a risk that governance decisions may be made without the input or agreement of other stakeholders, potentially leading to disagreements and conflicts, which can compromise the security and integrity of the blockchain network and damage trust in the network.

To address this issue, a permissioned blockchain could employ a multi-stakeholder governance model, which allows for a diverse range of participants to have a say in the decision-making process. This can include regulators, industry experts, and representatives from different sectors of the economy, who can run nodes that do not submit transactions but participate in governance decisions. By promoting inclusivity and transparency, multi-stakeholder governance can help to ensure that permissioned blockchains operate in a fair and accountable manner.

10.3.9 Denial-of-Service Attacks

Denial-of-service (DoS) attacks are a significant risk for permissioned blockchains. These attacks can take many forms, including flooding the network with large numbers of transactions or overwhelming individual nodes with requests, which can lead to delays, network congestion, and even a network failure.

In a permissioned blockchain, where the number of nodes is limited and predetermined, a successful DoS attack can effectively bring the entire network to a halt, compromising the availability and even integrity of the ledger.

To mitigate the risk of DoS attacks, permissioned blockchains can employ various measures, such as authentication, rate limiting, firewalls, and load balancing, to manage network traffic and prevent unauthorized access.

10.4 How to Achieve Security in Permissioned Blockchains

Permissioned blockchains are typically hosted by enterprises and can benefit from the security measures implemented and maintained by the hosting organizations. The following are areas that could help achieve security of a permissioned blockchain network.

10.4.1 Architecture Design

The overall architecture design, with a combination of consensus algorithms, number of nodes, and ownership of nodes, should ensure that one party (which may host multiple nodes) compromised or experiencing outage should not compromise the integrity of the whole blockchain network.

Here, one should not only consider the owning parties of blockchain nodes. Hosting platforms should also be considered. For example, if some nodes are hosted in the cloud, having multiple nodes hosted in the same region of the same cloud provider should consider what happens when the region goes down. A table-top exercise should be run to play out these scenarios and ensure that the architecture design is robust against such failure scenarios.

10.4.2 Design Redundancy for any Single Point of Failure

Besides the overall architecture design, single points of failure in the network need to be identified, such as certificate authority or notary node. Redundancy needs to be established so that if such a component has an outage, the backup component can be activated either automatically or manually.

10.4.3 Manage Software Supply Chain

Landmark security incidents in recent years such as SolarWinds (Kumar, 2023) and Log4j (UK National Cyber Security Centre, 2021) highlight the magnitude of software supply chain risks. To mitigate such risk, it is essential that the consortium of a permissioned blockchain network regularly audits its major software suppliers to ensure that they follow all the security best practices and can demonstrate that they have a program to manage their own software supply chain by adopting, as an example, the software bill-of-material (SBOM) program (CISA, 2022). The consortium needs to have a program to keep track of the other software components used in the network and use a risk-based approach to perform due diligence, e.g., use the SBOM method, on these software modules.

10.4.4 Ensure Robust Identity Management for the Whole Lifecycle of a Node

In a permissioned blockchain network, it is crucial to have robust identity management to ensure that only authorized nodes can participate in the network and access its resources. Therefore, the blockchain network must have a robust node onboarding process. This could include strong identity proofing before a digital certificate is issued to the node. This unique digital certificate should contain the node's identity information, such as organization name, the public key, and other relevant details. The certificates should be managed by a trusted certificate authority that verifies and validates the identity of the nodes.

From then on, all communications from the node to the network should be authenticated using this digital certificate. The identity in the certificate should then be used to enforce access control policies, which define the rules and permissions for each node in the network.

It is also important to have a mechanism in place for removing a node from the network and revoking the digital certification of a node in case of a security breach or business reasons.

10.4.5 Adopt Strong Network Security to Minimize the Chance of a Node Compromise

Network security works side by side with identity management to ensure a secure access layer. There are two sides of network security. One is the internet-facing access points for communications from the Internet to come through. Here, adopting DDoS protection, advanced firewalls, IDS/IPS, etc. would help secure the blockchain network. Feeding these engines with real-time threat intelligence, e.g., in the form of STIX (OASIS, 2023), is a key component of ensuring that a network is well protected against the imminent threats.

The other side of network security is to reduce the chance that enterprise employees get compromised and provide a backdoor for malicious actors to get into the network. Here adopting the zero-trust security principles (CISA, 2023) would help. This includes disabling access to enterprise networks by regular employees, granular network segmentation, and behavior-based anomaly detection, etc.

Regular security audits and vulnerability assessments should be performed to identify and address potential weaknesses in the network.

10.4.6 Ensure Security Best Practices in Administration

One of the most important steps in secure administration is to enforce multi-factor authentications. Nowadays, given the well-known attacks against SMS (MailSafi, 2022), and man-in-the-middle attacks against some of the other authentication mechanisms, hardware-based authentication such as FIDO tokens (Identity Automation, 2023) is strongly recommended for administrators. Following the zero-trust security principle, minimize the need for manual administration, and when required, use just-in-time authorization when possible, with comprehensive logging and correlation with change tickets.

10.4.7 Ensure Data Confidentiality, Integrity, and Availability

The selection of the blockchain technology and the design of the architecture should ensure that the on-chain data is protected per business requirements, in terms of confidentiality and integrity. When it comes to availability, permissioned blockchains may not have the built-in data redundancy as in public blockchains, backing up data likely becomes a requirement.

Blockchain platforms often store data off-chain, e.g., in a database. Such off-chain data must also be properly secured using proper access control, data encryption, and logging and monitoring. Such databases should also be protected against attacks such as SQL injection (OWASP, 2023) by input validation before passing any requests to the database.

10.4.8 Validate the Security of Smart Contracts

Ensuring the security of smart contracts is crucial for blockchain applications as they handle the transfer of valuable assets among other transaction types. Smart contract flaws were the root cause of numerous large-value DeFi hacks (Cybavo, 2023).

Code reviews, testing, and scanning of smart contract code would help find and correct security vulnerabilities introduced in the development process. Some smart contract languages such as Solidity for Quorum have more security tools available (Delb, 2023) as compared to others such as Chaincode for HyperLedger or Kotlin for Corda.

Detective controls such as monitoring must also be established to trigger alerts when the blockchain transactions initiated by smart contracts are behaving strangely, using behavior analysis.

10.4.9 Have a Strategy for System Upgrades

As nodes in a permissioned blockchain network are often operated by different organizations, software upgrades, including smart contract upgrades, require careful planning and coordination. The consortium in the network should decide beforehand whether the network should be designed to allow system outages in order to support software patching and upgrades.

The consortium should also include the need for rollback as part of their upgrade strategy, as a system upgrade may encounter unexpected issues or errors.

10.4.10 Patch Systems Diligently

It is also essential to keep the software and firmware up-to-date with the latest security patches and updates to prevent exploitation of known vulnerabilities. Subscribing to security alerts and having a risk-based strategy and timeline for patching vulnerabilities are essential for ensuring the integrity and security of the permissioned blockchain network and its data.

10.4.11 Establish Monitoring and Incident Response Capabilities and Processes

When it comes to security, prevention is ideal, but detection is a must. As many permissioned blockchain networks are used for financial applications, any delay in detecting a security breach could mean additional financial loss.

Besides having a well-established security operations center within each organization, supported by a security information and event management (SIEM) system, the consortium running the permissioned blockchain network should establish a channel to share threat information and any indications of attacks with each other and leverage the security capability of each consortium members.

10.5 Final Thoughts

From the security perspective, a permissioned blockchain network has its advantages and disadvantages as compared to public blockchains, and the two share the same issues in some areas.

Given a much smaller number of nodes in a permissioned blockchain network, it does not have the same strength as public blockchains in terms of strong data

integrity, intrinsic data redundancy, and protection against cyberattacks on individual nodes.

The areas where permissioned blockchain has potential advantages include a mechanism for node onboarding and lifecycle management, the ability to leverage enterprise security controls, and the possibility of having scheduled downtime for system upgrades and updates.

Smart contract security is an area that is common between public and permissioned blockchains.

A hidden gem in security for permissioned blockchain is the prospect of combining the security forces from different organizations of the blockchain consortium, to jointly perform security tasks of the overall blockchain network, such as designing and reviewing the security architecture, validating the security of smart contracts, detecting potential attacks against the blockchain network, and responding to security incidents, etc. Given the shortage of cybersecurity talent across the globe, this provides an added benefit when organizations combine their technical capabilities to secure the chain.

References

- CISA. (2022). *Software Bill of Materials (SBOM)*. CISA. Retrieved April 22, 2023, from <https://www.cisa.gov/sbom>
- CISA. (2023). Zero trust maturity model.
- Cybavo. (2023, February 6). Year in review: Top 10 DeFi hacks of 2022. CYBAVO. Retrieved April 22, 2023, from <https://www.cybavo.com/blog/year-in-review-top-defi-hacks-2022/>
- Delb, B. (2023). *Home*. YouTube. Retrieved April 22, 2023, from <https://cryptodevops.academy/overview-of-the-main-solidity-smart-contracts-security-tools-51475460ba19>
- Hyperledger Foundation. (2023). A Blockchain Platform for the Enterprise — hyperledger-fabricdocs main documentation. Retrieved April 22, 2023, from <https://hyperledger-fabric.readthedocs.io/en/release-2.5/>
- Identity Automation. (2023). FIDO U2F Tokens FIDO U2F Tokens. Identity Automation. Retrieved April 22, 2023, from <https://www.identityautomation.com/iam-platform/rapididentity-access-management/authentication/fido-u2f-tokens/>
- Kumar, B. (2023, February 28). SolarWinds Attack & Details you Need to Know about it. Simplilearn. Retrieved April 22, 2023, from <https://www.simplilearn.com/tutorials/cryptography-tutorial/all-about-solarwinds-attack>
- MailSafi. (2022, January 28). How SIM-SWAP fraud affects your SMS-based 2-FA. MailSafi. Retrieved April 22, 2023, from <https://mailsafi.com/blog/sim-swap-fraud-sms-2fa/>
- MITRE. (2023). CVE - CVE. Retrieved April 22, 2023, from <https://cve.mitre.org/>
- Monetary Authority of Singapore. (2022, December 15). *Project Ubin: Central Bank Digital Money using Distributed Ledger Technology*. Monetary Authority of Singapore. Retrieved April 22, 2023, from <https://www.mas.gov.sg/schemes-and-initiatives/Project-Ubin>
- JP Morgan. (2022). Coin systems | onyx by J.P.Morgan. J.P. Morgan. Retrieved April 22, 2023, from <https://www.jpmorgan.com/onyx/coin-system.htm>
- OASIS. (2023, February 15). Introduction to STIX. Retrieved April 22, 2023, from <https://oasis-open.github.io/cti-documentation/stix/intro>
- OWASP. (2023). *OWASP top ten*. OWASP foundation. Retrieved April 22, 2023, from <https://owasp.org/www-project-top-ten/>

- R3. (2023). R3 Documentation - Home. Retrieved April 22, 2023, from <https://docs.r3.com/>
- Shostack, A. (2014). *Threat modeling: Designing for security*. Wiley.
- UK National Cyber Security Centre. (2021, December 14). *What the Log4j vulnerability is, who is affected* - NCSC.GOV.UK. National Cyber Security Centre. Retrieved April 22, 2023, from <https://www.ncsc.gov.uk/information/log4j-vulnerability-what-everyone-needs-to-know>
- World Bank. (2018, August 23). World Bank prices first global Blockchain bond, raising a\$110 million. World Bank. Retrieved April 22, 2023, from <https://www.worldbank.org/en/news/press-release/2018/08/23/world-bank-prices-first-global-blockchain-bond-raising-a110-million>

Part III

Financial Integrity and National Security

In this part of the book, we delve into the intricate relationship between Web3 security, financial integrity, and national security. As we witness the digital asset landscape undergoing a seismic shift, it's imperative to grasp the profound implications this evolution brings along. From regulatory changes to potential geopolitical ramifications, this section illuminates how Web3 security intersects with broader socio-economic and political aspects.

The year 2022 was marked by significant incidents that drastically altered institutional investors' attitudes toward crypto assets, culminating in the collapse of the FTX exchange. The tremors from these events accelerated regulatory efforts globally, particularly in the three largest markets: China, the USA, and the EU. While China has curtailed private crypto markets in favor of a sovereign digital currency, the EU and USA are forging paths toward more comprehensive frameworks for crypto regulation.

These regulatory developments have far-reaching implications for the crypto community, necessitating a closer scrutiny of these changes and an adaptation to this evolving "new normal." Furthermore, the ongoing Russia-Ukraine war underscores the potential geopolitical implications of the cross-border crypto ecosystem, emphasizing the need for robust compliance mechanisms and best practices for crypto-based fundraising, sanctions compliance, and anti-financial-crime controls.

Finally, it's crucial to dispel the myth of crypto assets being "non-traceable." In reality, the primary vulnerability arises from non-compliance with AML/CFT and sanctions obligations by DeFi services. With the international community rallying behind enforcement powers like the Financial Action Task Force (FATF), coupled with new blockchain analysis technologies, we are at the cusp of a new era in crypto intelligence. This section invites readers to explore these pressing issues in greater depth, gaining a holistic understanding of the role of Web3 security in the larger global context.

Chapter 11

Regulation and Crypto on a Cliff Edge



Winston Ma

11.1 FTX Collapse: Global Regulation Rising Sharply

11.1.1 2022: Dramatic and Difficult Year

The year 2022 brought a series of damaging events for some significant parts of the digital assets sector, as shown in Table 11.1. Crypto-asset prices peaked in November 2021 and fell by roughly two-thirds of total crypto market capitalization (about \$2 trillion), over the course of 2022. This price decline, and the corresponding reduction in players and investors' activities, is referred to as a "Crypto Winter."

The calamities of the past year revealed major flaws in the business models and practices of many crypto ventures, notably in the exchange and lending spaces. The collapse of FTX, one of the world's biggest cryptocurrency exchanges, in November 2022 put a capstone on a terrible year of failures and lost market value in the world of digital assets. The FTX failure further led to a new set of falling dominoes, with other crypto service providers declaring bankruptcy as well.

11.1.2 The Rise (and Fall) of FTX

Sam Bankman-Fried was once known as the face of cryptocurrency. As recent as early 2022, FTX, among the highest profile crypto exchanges in the world, was valued as recently as January at \$32 billion in a fundraising round from investors including Singapore SWF Temasek, Canadian pension Ontario Teachers' Pension Plan Board (OTPP), SoftBank Vision Fund (partly backed by SIFs' LP capital), and

W. Ma (✉)
NYU School of Law, New York, NY, USA

Table 11.1 Critical market events of 2022

Time	Event	Description
May, 2022	Terra LUNA collapse	UST loses peg to the dollar and collapses, along with stabilization token LUNA, erasing over \$50 bln in value
July, 2022	LUNA contagion	Plunge in crypto liquidity and prices trigger collapse of Celsius network, voyager digital, and three arrows capital
August, 2022	Activity collapse	Assets locked in DeFi protocols falls by over half in two months; crypto companies begin layoffs
November	FTX and alameda fail	Bahamas-based exchange FTX and its trading arm, alameda, collapse as concerns about its finances trigger investor outflows
December	Contagion spreads	Crypto lenders BlockFi and genesis file for bankruptcy because of exposures to other failed firms and tokens

many well-known VC firms such as Tiger Global and Sequoia Capital, according to news reports.

But FTX melted down in November 2022. In a matter of days, FTX went from a \$32 billion valuation to bankruptcy as liquidity dried up, customers demanded withdrawals, and rival exchange Binance walked away from a nonbinding agreement to buy the company. In December 2022, Sam was arrested on wire fraud, securities fraud, and money laundering charges from the Bahamas. The US Securities and Exchange Commission has alleged that Sam defrauded FTX investors and raised \$1.8 billion in equity.

As a result, two prominent institutional investors in the global markets, Temasek and OTPP announced, with excuses in public statements, that they had, respectively, fully written down their \$275 million and \$75 million investments in the crypto exchange. The Silicon Valley firm Sequoia Capital and SoftBank, the Japanese tech conglomerate, also declared their stakes worthless (\$213 million and \$100 million).

In a terse statement, OTPP wrote down the entire investment in FTX citing “potential fraud.” “We will be writing down our investment in FTX to zero at our year end ... We are disappointed with the outcome of this investment, take all losses seriously and will use this experience to further strengthen our approach,” OTPP said, “Naturally, not all of the investments in this early-stage asset class perform to expectations.”

For Singapore’s Temasek, its public announcement was much longer. Temasek’s investments in early-stage companies amount to about 6% of the portfolio. Its direct investments in blockchain “are not a significant part” of that exposure, it said. Writing down the investment “will not have significant impact on our overall performance,” Temasek said, but Temasek treats “any investment losses seriously and there will be learnings for us from this.”

As a result, an internal unit at Temasek will conduct the review separately from the team that decided to invest in FTX and will report directly to the board. (Such reviews have been triggered by Temasek before by other investments that were written off or permanently impaired.) The government won’t rule out calling for an external private auditor or engaging the auditor general if it suspects negligence,

fraud, or misconduct, Singapore's deputy prime minister and Minister for Finance, Lawrence Wong, said to the parliament.

11.1.3 Three Profound Implications

11.1.3.1 FOMO Out, DD In

FTX was not the first crypto token company that went to bankruptcy and consequently SIFs had to write off their investment. The Caisse de Depot et Placement du Quebec (CDPQ) pension fund of Quebec, Canada in the fall of 2021 invested US\$150 million in Celsius, a (then) major crypto lender. "Blockchain technology has the potential to disrupt several sectors of the traditional economy. As digital assets grow in adoption, we intend to capture the right opportunities, while working with our partners towards a regulated industry," Alexandre Synnett, executive vice-president and chief technology officer at Caisse said at the time.¹

Merely 9 months later, Celsius suspended withdrawals on its platform on June 12, citing liquidity issues arising from the crypto market downturn. The firm [filed for bankruptcy](#) in New York one month later. A court document showed the firm has [\\$5.5 billion in liabilities](#) and a \$170 million cash balance. In August 2022 CDPQ decided to write off its investment in the bankrupt firm, and during a webcast discussing the firm's mid-year results, Caisse CEO Charles Emond said the fund "arrived too soon in a sector which was in transition."

And it's likely that FTX would not be the last crypto-related investments that would hit SIF investors. Celsius, FTX, and a few more high profile failures of crypto firms in 2022 have shaken the market confidence and led to significant asset contagion risks in the crypto world. It is quite likely that more bankruptcies would come in 2023, and more investment positions may be wiped out.

But all these should not come as a big surprise. Just like traditional VC firms, who are otherwise smart investors but would do dumb things any time there is a boom cycle like this—because they see their pals and peers piling in and worry that they will be left out, SIF investors are not immune from FOMO (fear of missing out) and would also invest in companies of stretched valuation in the hunt for unicorns.

Most importantly, it can be expected that in the future, institutional investors will NOT embrace an "inspiring leader" instead of Due Diligence (DD). It was well summarized by Marcelo Claire, the former SoftBank executive who helped lead the Japanese tech conglomerate's (former) investment in FTX. "I have been reflecting personally on the whole FTX fiasco and it taught me one more time that we should NEVER invest because of FOMO and we should always 100% understand what we are investing in. I totally failed here on both," he tweeted. The investor community

¹ Sinclair, Sebastian. "Celsius initiates bankruptcy proceedings to 'stabilize' its business," July 13, 2022. <https://blockworks.co/news/celsius-to-file-for-bankruptcy-imminently-report>

probably will agree. We are still at the very beginning of Web3, so take a pause and do your due diligence.

11.1.3.2 More Blockchain Technology, Less Speculative Trading

So, how will the sovereign wealth funds and pension funds adjust their investment approach to this new space, after an “egg on the face” (term used by Madam Ho Ching, ex-Chairwoman of Temasek, in a Facebook post that the write down of Temasek’s full investment in FTX)?

Temasek said, in its FTX-related public announcement, that it continues to recognize the potential of blockchain applications and decentralized technologies “to transform sectors and create a more connected world. But recent events have demonstrated what we have identified previously — the nascency of the blockchain and crypto industry and the innumerable opportunities as well as significant risks involved.”

Temasek added that there have been “misceptions” that the FTX exposure was “an investment into cryptocurrencies.” Actually, “To clarify, we currently have no direct exposure in cryptocurrencies.” Instead, its investment will focus on tech investing, as VC funds typically do historically. Its blockchain investment activity focuses on “financial market service providers to the digital asset space providing protocol agnostic and market neutral exposure” and technology infrastructure such as wallets, developer tools, metaverse, and gaming infrastructure.

This kind of shifting strategy probably will be seen across the institutional investor space. They will shift their focus toward infrastructural aspects of blockchain, the so-called picks and shovels of the industry. Instead of pure financial applications, so-called hard technology innovations will be in favor. They tend to be technical in nature, requiring a high level of expertise; also, they take longer to build out and realize, which matches well with the patient, long-term capital of sovereign wealth funds and pension funds.

(It’s worth noting that this bifurcated approach—more focus on the tech aspect of blockchain, less focus on the financial aspect of crypto-assets—is quite similar to the Chinese government’s policy approach to this space. Reference to Winston Ma’s 2021 book: *The Digital War—How China’s Tech Power Shapes the Future of AI, Blockchain and Cyberspace.*)

11.1.3.3 Global Regulations Rising

FTX collapse highlighted risks from crypto-assets that lack basic protections. This has brought immediate sharp focus to regulators, both on the fallout among FTX retail investors and its knock-on effects throughout the greater financial landscape. The risk to market integrity demonstrates the need for a rapid and comprehensive global regulatory policy approach and supervisory framework.

As a result, financial regulators worldwide will keep their attention on two places at once. As one eye stays firmly on precluding terrorism funding (next Chap. 12), the other is on the protection of retail investors and the overall financial market's stability (this chapter). This chapter will focus on the regulatory approaches from the three biggest markets: China, USA, the EU.

11.2 China: Crackdown on (Formerly) World's Largest Crypto Market

11.2.1 Unprecedented Crackdown Since 2021

Before China's State Council's Financial Stability Committee vowed to [crack down on the cryptocurrency's mining and trading activities](#) in May 2021, few people—even among global financial professionals—realized that China accounts for more than 70% of the world's bitcoin and other cryptocurrencies' supply. Because [the majority of global cryptocurrencies were mined](#) and traded in China, Chinese regulations in this new industry have had profound global implications.

The 2021 crackdown was not the first time China has strengthened regulation of cryptocurrencies. China issued similar bans first in 2013, and then in 2017, when [China accounted for 90% of global bitcoin trading](#). The 2017 rule issued by China's central bank, the People's Bank of China (PBOC), and other ministries, essentially shut down local cryptocurrency exchanges, forcing major exchanges including Binance and Huobi to relocate overseas.²

Nevertheless, onshore Chinese investors could still trade cryptocurrencies on platforms owned by overseas exchanges. As the price of bitcoin jumped multiple times since late 2020, Chinese trading activities also heated up.

As such, the May 2021 crackdown was viewed by the cryptocurrency market as just another rule announcement without serious enforcement. For example, [Hong Kong's Bitcoin Association said in a tweet](#) in response to China's reiterated ban: "For those new to bitcoin, it is customary for the People's Bank of China to ban bitcoin at least once in a bull cycle."

But this time is different. Coming from the State Council's Financial Stability Committee, the highest level financial regulator of China led by then vice premier, the latest cryptocurrency crackdown was a significant upgrade of existing regulations. Furthermore, it was the first time the State Council has explicitly targeted cryptocurrency mining activities, which indicated a determination to crack down cryptocurrency trading from its origin, as China was the largest cryptocurrency mining field in the world.

²CGTN. "China bans financial, payment institutions from crypto business amid price volatility," May 19, 2021. <https://news.cgtn.com/news/2021-05-19/China-bans-financial-payment-institutions-from-crypto-business-10og4diN0t2/index.html>

11.2.2 Three Key Factors

The Chinese government has suggested that investor protection, carbon neutrality, and financial stability are the three key factors for the new regulations. The regulatory development of China, the largest cryptocurrency mining field and trading market in the world, will be an important reference case for other countries that start developing regulations for the cryptocurrency mining and trading activities.

11.2.2.1 Investor Protection

Investor protection—cutting off the cash flow channel between uneducated investors and offshore exchanges—is a motivation for new regulations. For the Chinese regulators, bitcoin and other cryptocurrencies are not investment tools, rather, they are speculative instruments with high volatility. China has a clear record of cracking down on all kinds of products for fear that bubbles will eventually burst and lead to riots of disgruntled retail investors—whether it is in beans, garlic, tea, or the more recent, peer-to-peer loans.

Since the State Council’s decision in May 2021, three Chinese financial associations—the National Internet Finance Association of China, the China Banking Association, and the Payment and Clearing Association—issued a new rule to ban [financial institutions from cryptocurrency-related businesses](#). The rule was designed to make it more difficult for individuals to buy cryptocurrencies using various payment channels. The associations have reminded investors that virtual currencies “are not supported by real value.”

To ensure all the rules will be seriously enforced, the PBOC (China’s Central Bank) summoned representatives of multiple institutions, including state-owned commercial banks and Alipay, and told them to “strictly implement” recent notices and guidelines from authorities on curbing risks tied to cryptocurrency transactions. As China-focused exchanges that are registered overseas allow Chinese individuals to open accounts online, and cryptocurrency transactions by Chinese individuals can be made through banks, or online payment channels such as Alipay or WeChat, the financial firms were also instructed to go through their systems to investigate and identify customers with accounts in virtual currency exchanges, in which case the institutions have to cut off the accounts’ ability to send or receive money for transactions.

11.2.2.2 Carbon Neutrality

Another motivation for new cryptocurrency regulations is China’s goal toward carbon neutrality. China’s new environmental policy is a key factor in the mining crackdown and was not part of previous cryptocurrency regulations. President Xi Jinping, in a [speech](#) last November to the UN General Assembly—months before

the cryptocurrency crackdown—pledged to have the nation’s carbon emissions peak before 2030 and realize carbon neutrality by 2060.

The carbon neutrality policy cuts back coal power, which has been a major energy source for the country. According to London-based climate data provider [TransitionZero](#), China needs to halve its carbon dioxide emissions from coal-based power plants by 2030 to achieve the policy. To meet climate targets, cryptocurrency mining is one of the focus areas as it is one of the many high energy consumption industries in China. Additionally, members of the Financial Stability Committee include the National Development and Reform Commission, the national energy regulator.

After the central government initiated the cryptocurrency crackdown campaign in May, major coal-based power producers such as Inner Mongolia and Xinjiang, which were previously the top two cryptocurrency mining hubs in China, have been among the first regions that quickly developed local rules to clean up mining businesses.

Furthermore, China’s carbon neutrality policy created an energy shortage within the country due to its drastic reduction in coal-fired power, which means that even mining with renewable energy like hydropower is subject to new regulations. Sichuan and other provinces also had to shut down all mining businesses in June, whether they were powered by coal or hydro.

11.2.2.3 Financial Stability

A third motivating factor for cryptocurrency regulation is to maintain financial stability as well as to push forward China’s central bank digital currency. On July 16, the PBOC [issued a white paper](#) on its development of China’s digital currency, the e-CNY. China has taken the lead in the digital currency push, and it is likely to be the first major economy to introduce a sovereign digital currency. Since 2020, China has been steadily expanding its digital yuan pilot programs, given the country’s rapid development of internet industries such as e-commerce and social network platforms that provide a myriad of application scenarios.³

In its white paper, the PBOC cited the rapid growth in cryptocurrencies as a driver for research and development of the e-CNY and said that “cryptocurrencies are mostly speculative instruments, and therefore pose potential risks to financial security and social stability.” This is the first time that the PBOC, in an official document, linked its sovereign digital currency issuance with cryptocurrencies’ potential challenges to the international monetary system. According to the PBOC, “cryptocurrencies’ lack of intrinsic value, acute price fluctuations, low trading efficiencies and huge energy consumption make them unfit for use in daily economic activities.”

³PBOC. “Progress of Research & Development of E-CNY in China,” July 2021. <http://www.pbc.gov.cn/en/3688110/3688172/4157443/4293696/2021071614584691871.pdf>

11.2.3 China’s CBDC Push

Although China has cracked down on cryptocurrencies (details in the following section), shutting down all domestic crypto exchanges and banning all ICOs (initial coin offerings), the government recognizes blockchain technology itself as a revolutionary development. In an October 2019 speech, Chinese President Xi Jinping declared blockchain would play “an important role in the next round of technological innovation and industrial transformation.” That marked the first major world leader to issue such a strong endorsement of the widely hyped—but still unproven—distributed ledger technology (DLT). (By contrast, most governments in the West have been far more cautious.)

Calling for blockchain to become a focus of national innovation, President Xi’s speech detailed the ways the Chinese government would support blockchain research, development, and standardization. China’s leadership position in the global competition of central bank digital currency (CBDC) is the prime example. (At the beginning, Chinese CBDC was referred to as DCEP, meaning “digital currency, electronic payment.”)

Unlike bitcoin and other cryptocurrencies built on the excitement regarding “decentralization,” China’s CBDC, which is called e-CNY by the People’s Bank of China (PBOC), China’s central bank (CNY is the English synonym of the Chinese currency, the yuan), is run on a centralized database; nevertheless, e-CNY is built with blockchain and cryptography, and it has incorporated blockchain’s key concepts such as peer-to-peer payment, traceability, and tamper-proof-ness.

The e-CNY’s timeline began years after the development of bitcoin and other cryptocurrencies (see Fig. 11.1). The first publicized PBOC effort on digital currency occurred four years after the first bitcoin transaction in May 2010, in the form of the establishment of an in-house digital currency research group. Starting 2017, PBOC accelerated its efforts and first established the Digital Currency Research Institute in January 2017, then followed with December 2017’s call for Chinese commercial banks and payment institutions to collaborate in efforts in digital currency. Further acceleration of e-CNY testing was broadly viewed as a reaction to

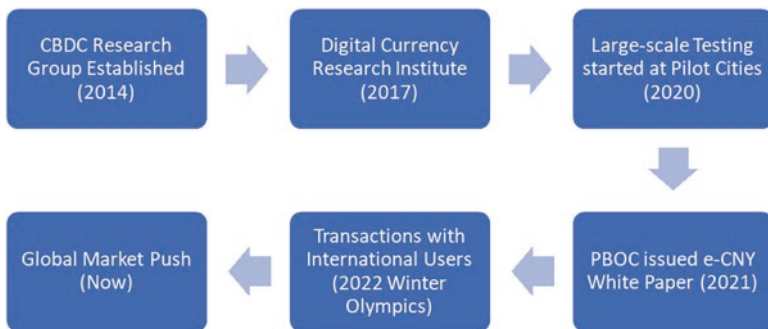


Fig. 11.1 Timeline of China’s Digital RMB. Data Source: PBOC Public Reports

Facebook's announcement in 2019 that it intended to launch *Libra*, Facebook's planned blockchain-based digital currency (see detailed discussion later in this chapter).

The large-scale testing occurred in 2020 at numerous major cities amid the Covid-19 pandemic. In those pilot zones, e-CNY has been formally adopted into the cities' monetary systems, with some government employees receiving their salaries in the digital currency from May 2020. People can create an e-CNY wallet in their commercial banks' mobile app and use the national digital currency for things like transportation, education, healthcare, and other consumer goods and services. Starbucks, McDonald's, and Subway chains in China, for example, were named on the central bank list of firms to test the digital currency.

In July 2021, the PBOC issued a white paper detailing the current workings of the digital yuan, also referred to as the e-CNY, which is the first comprehensive disclosure of its plans. The release of the white paper probably marked the near end of the testing phase for the digital currency's "2C" retail payment. The digital yuan wallet supports several functions, including scan to pay, top-ups, and money transfers. According to the white paper, as of June 2021, participants have spent 34.5 billion digital yuan (\$5.3 billion) in trials. Uses included paying utility, dining, transportation, shopping, and government services. In January 2022, the eCNY wallet was the most downloaded app in Apple and Xiaomi App stores within just a week of formal launching.

The new digit yuan would allow users to spend it even without an internet connection, and it will bring convenience to foreigners, too. "Foreign residents temporarily traveling in China can open an e-CNY wallet to meet daily payment needs without opening a domestic bank account," said the white paper. That means even foreigners traveling in China can have access to the digital yuan without a domestic bank account. This is a particular benefit given the difficulties that foreigners have had using mobile payment apps like WeChat Pay (of Tencent) and Alipay (of Alibaba), because those apps must be linked to banking accounts.

In February 2022, the Beijing Winter Olympics became a major milestone for China's digital currency because it was the first test for the digital yuan with international users. It was also like a stress test for the digital currency infrastructure because the system handled the exchange of foreign currencies from numerous countries. For example, global athletes and visitors could put their own money, from different countries, into ATM machines and then get a debit card in Chinese digital yuan, converted from the foreign money. With the debit card, they could go to restaurants and go shopping nearby, without needing a banking account in China.

Of course, the profound impact of e-CNY is likely to be more than China's retail markets. Most likely, e-CNY would make China the first major economy to adopt a native digital currency. Many believe the e-CNY will bolster Chinese currency's global status and eventually challenge the US dollar's preeminent position as the world's reserve currency. For example, the e-CNY could bypass Western-operated cross-border payment networks, such as SWIFT, which the USA has used to enforce sanctions.

11.2.4 Global Implication of China's Crypto Crackdown

China's new regulations have already made significant impact in the global cryptocurrency markets. First, China's mining crackdown has forced a [seismic shift](#) in bitcoin mining patterns. By July 2021, bitcoin's network hash rate, a measure of its computational horsepower, had [dropped about 50% since its peak level in May 2021](#).⁴

Second, from a cryptocurrency trading perspective, China's tightened regulations and enforcement have contributed to bitcoin's price dropping about 50% from its all time high price within a few months.

Finally, and probably most importantly, China's new regulatory framework may influence many countries' cryptocurrency-related regulations going forward. The regulatory development in China is giving the rest of the world a sense of urgency, especially for those governments that have been slow to act on the rapid expansion of cryptocurrencies.

While broad bans might be viewed as disproportionate, China is not alone. [Containing user risks](#) will be difficult for authorities around the world given the rapid evolution in crypto, and some countries are taking similar drastic steps.

For example, sub-Saharan Africa, the smallest but fastest growing region for crypto trading, nearly a fifth of countries have [enacted bans](#) of some kind to help reduce risk, according to IMF reports. Six countries—Cameroon, Ethiopia, Lesotho, Sierra Leone, Tanzania, and the Republic of Congo—have banned crypto. Zimbabwe has ordered all banks to stop processing transactions and Liberia directed a local crypto startup to cease operations (implicit bans).⁵

11.3 EU's MiCA: First Comprehensive Crypto Regulatory Framework

On 20th April 2023, the European Parliament approved the new Markets in Crypto-Assets Regulation ("MiCA"), making it the first major jurisdiction in the world to introduce a comprehensive crypto law. "We are putting safeguards in place that would prevent companies active on the EU market from engaging in some of the practices that led certain crypto-asset operators to collapse. As we have seen in recent months, stringent rules and supervision are very much needed because we've had the collapse of projects such as FTX, Terra Luna, Celsius, and Voyager," said

⁴Kiderlin, Sophie. "A 'seismic shift' in Chinese crypto mining is underway and bitcoin could slide further as a result: Glassnode," June 23, 2021. <https://markets.businessinsider.com/currencies/news/bitcoin-mining-china-price-crypto-regulation-glassnode-2021-6-1030547552?miRedirec=1>

⁵IMF blog. "Africa's Growing Crypto Market Needs Better Regulations," November 22, 2022. <https://www.imf.org/en/Blogs/Articles/2022/11/22/africas-growing-crypto-market-needs-better-regulations>

Mairead McGuinness, the European Commissioner for Financial Stability, Financial Services, and the Capital Markets Union.⁶

Among other things, MiCA imposes restrictions on the issuance and use of stablecoins. MiCA regulates primary market activities (issuance/public offerings) and access to the secondary market (listings) as well as the provision of certain crypto-related services.

11.3.1 “Crypto-Assets” Clarified

MiCA regulates activities involving “crypto-assets.” The term crypto-asset is broadly defined as any “digital representation of a value or a right which may be transferred and stored electronically, using distributed ledger technology or similar technology” (Art. 3 (1) No. (2) MiCA). MiCA introduces three sub-categories of crypto-assets that are subject to different requirements adjusted to the risks they entail:

- “**Electronic money tokens**” or “**e-money tokens**” (EMTs) are crypto-assets that purport “to maintain a stable value by referencing to the value of one official currency.” Like traditional e-money, EMTs are electronic surrogates for coins and banknotes and are likely to be used for payment purposes.
- “**Asset-referenced tokens**” (ARTs) aim “to maintain a stable value by referencing to any other value or right or a combination thereof, including one or more official currencies.” For example, ARTs could be backed by a basket of different fiat currencies, commodities, or crypto-assets.
- The third sub-group is a catch-all category for **all other crypto-assets** that are not EMTs or ARTs, which thus covers a wide variety of crypto-assets, including non-pegged payment tokens (*i.a.*, cryptocurrencies like Bitcoin or Ether) and utility tokens. MiCA lays down a few specific rules for utility tokens, defined as “a type of crypto-asset which is only intended to provide access to a good or a service supplied by the issuer of that token.”

Both EMTs and ARTs are variants of “stablecoins,” which are subject to stricter rules due to related concerns regarding financial stability and monetary sovereignty. That will be covered in more detail in the later section on Stablecoins.

In short, MiCA establishes three distinct, but interrelated, regulatory regimes, namely, (i) a regime for issuers of stablecoins (ARTs and EMTs), (ii) a regime for issuers of non-stablecoins (other crypto-assets), and (iii) a regime for entities providing services in respect of crypto-assets, who are referred to as crypto-asset service providers (“CASP”).

⁶Browne, Ryan. “EU lawmakers approve world’s first comprehensive framework for crypto regulation,” April 20, 2023. <https://www.cnbc.com/2023/04/20/eu-lawmakers-approve-worlds-first-comprehensive-crypto-regulation.html>

11.3.2 White Paper Requirement for Issuers of Crypto-Assets

One core obligation under MiCA is that issuers of all three types of crypto-assets must issue white papers—a sort of prospectus for crypto-assets, informing potential holders of the characteristics of the issued crypto-asset—before they may offer a token to the public or list it on a trading platform. MiCA introduces minimum standards for these white papers in order to achieve a (so far lacking) standardization and reliability.

Under MiCA, white papers must include information on not only, *i.a.*, the issuer, the crypto-asset project or token, risks and the rights and obligations attached to the crypto-asset but notably also the adverse environmental and climate-related impacts of the consensus mechanism used to issue the crypto-asset.

Any entity (an individual or a financial institution), which wishes to offer crypto-assets to the public or admit crypto-assets to a trading platform, must draft a white paper in respect of those crypto-assets containing mandatory disclosures and other information. The contents of the whitepaper will vary depending on the type of crypto-asset, but all whitepapers must contain information including information on the issuer, information on the crypto-asset, information on the underlying technology, and the associated risks. Advertising and marketing communications should be consistent with the contents of the white paper.

Unlike a corporate stock offering with a prospectus, there is no general requirement for a competent authority to approve the whitepaper. For crypto-assets other than ARTs or EMTs, MiCA mainly stipulates disclosure, transparency, and governance rules. Offering such crypto-assets to the public or listing them on a trading platform does not require prior authorization. Rather, issuers only need to notify and publish the white paper up front.

MiCA will require issuers of asset-referenced tokens to maintain robust governance arrangements. This is stated to include (a) a clear organizational structure with well-defined, transparent, and consistent lines of responsibility; (b) effective processes to identify, manage, monitor, and report the risks to which the issuer is or might be exposed; and (c) adequate internal control mechanisms, including sound administrative and accounting procedures.

11.3.3 Excluded (for Now): NFT, DeFi, and DAO

MiCA does not apply to crypto-assets captured by existing financial services legislation (e.g., security tokens qualifying as financial instruments under MiFID II). Further, it does not apply to crypto-assets that are unique and not fungible with other crypto-assets (Art. 2 (2a) MiCA; so-called Non-Fungible Tokens (NFTs)). However, NFTs that are issued “in a large series or collection” may be considered fungible and thereby covered by MiCA. Fractional parts of NFTs also do not fall under the exclusion.

Since crypto-asset services that “are provided in a fully decentralized manner without any intermediary” and crypto-assets without an identifiable issuer also do not fall within the scope of MiCA (recital 12a), the regulation does not capture Decentralized Finance (DeFi) and operations of Decentralized Autonomous Organizations (DAO)—so long as control of the operations is truly decentralized.

In other words, there are still many “gaps” under the MiCA. In April 2023, just days before the EU vote on MiCA, European Central Bank (ECB) supervisory board member Elizabeth McCaul raised her concerns, by publishing a blog on the media section of the ECB’s official website, that the upcoming MiCA does not provide adequate supervision for crypto exchanges, among several gaps that must be addressed in the existing framework.

She contends that MiCA lacks the necessary measures to supervise exchanges using quantitative metrics, thereby limiting its effectiveness in promoting transparency and accountability in the sector. The top examples used was Binance, the world’s largest crypto exchanges. Talking about Binance she said that while Binance didn’t have an exact physical office or headquarters, there should be no leniency in the policies it must adhere to as a global company. In its current iteration, the MiCA bill would not have considered Binance a “significant” crypto-asset service provider (CASP), despite having between 28 and 29 million global customers.

11.3.4 “Passport” Perks in Europe

In spite of these uncovered areas, MiCA represents the first attempt by a leading global jurisdiction to regulation digital assets and the greater crypto ecosystem. Legislation is not a static process. It can be expected that there will be reviews and improvements. The European Commission would review the implementation of obligations and consider feedback from government supervisors and industry participants, and the initial impact of MiCA.

MiCA will apply in two parts. The first part dealing with stablecoins should apply after 12 months (Q2 2024), while the second part dealing with CASPs should apply after 18 months (Q4 2024). In the meantime, the European Banking Authority and European Securities Markets Authority will develop technical standards and guidelines to complement MiCA.

MiCA will ensure a harmonized regime across member states. It is expected that in 2023 a growing number of CASPs will seek to register in Europe to take advantage of one MiCA’s benefits, which allows entities registered in one EU member state to “passport” their services around Europe without having to obtain approval from regulators in all member states.⁷

⁷Schickler, Jack. “EU Parliament Approves Crypto Licensing, Funds Transfer Rules,” April 20, 2023. <https://www.coindesk.com/policy/2023/04/20/eu-parliament-approves-crypto-licensing-funds-transfer-rules/>

11.4 US: Fragmented Enforcement as Regulation

After MiCA, the US crypto industry leaders are increasingly making the trans-Atlantic juxtaposition to argue for clearer regulations as US regulators have been enforcing decades-old rules for trading and banking in the crypto world. The US Congress has not been able to craft a federal standard for crypto-assets, so the federal agencies of Biden Administration are creating crypto rules through their enforcement actions (See Fig. 11.2.)

As a result, current US regulatory interpretations can cause digital assets to simultaneously fall under multiple legal classifications by different federal agencies (e.g., as both a commodity and a security). This may complicate which federal regulators have oversight of an individual crypto-asset, and it can also make it difficult for crypto projects to develop compliance and operational standards.⁸

11.4.1 Conflict of Jurisdictions: CFTC Vs. SEC

Regulation of the crypto markets in the USA is fragmented, and the key is on whether a crypto-asset fits within the definition of a “security” under the US securities laws. In the beginning, crypto currencies such as bitcoin (BTC) or ether (ETH) dominated the overall crypto markets, and they were generally considered to be undefined assets that were not subject to any existing regulatory schemes. But as the crypto markets gained more size and attention, the US regulators, especially the Securities and Exchange Commission (SEC) and the Commodity Futures Trading Commission (CFTC), began to assert their jurisdiction over crypto-assets.

Most notably, the SEC (the regulator of securities markets) began classifying certain crypto-assets as “investment contracts,” which is a catch-all term under the definition of “security.” Meanwhile, CFTC, the regulator charged with overseeing

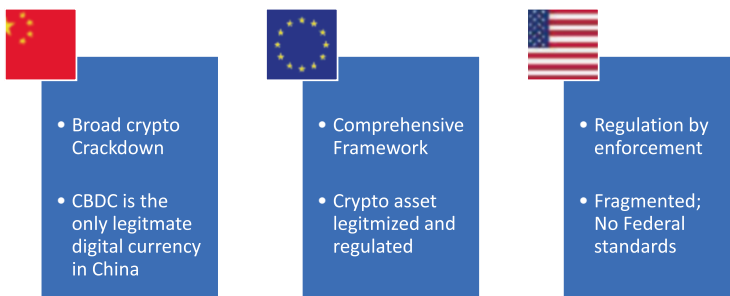


Fig. 11.2 Three different models (China US EU)

⁸Parker, Emily. “Keep Crypto in America,” March 2, 2023. <https://www.coindesk.com/consensus-magazine/2023/03/02/lack-of-regulatory-clarity-puts-crypto-in-the-united-states-at-risk/>

commodities and commodities derivative transaction, stated (for example, in CFTC’s civil lawsuit against FTX and its founder Sam Bankman-Fried) that they consider the stable token Tether (USDT), in addition to BTC and ETH, to be a commodity.

Whether a digital asset is a “security” or a “commodity” under US law can have far-reaching consequences for the viability of the crypto-assets, as well as the related projects. A security—unless it is subject to an exception or exemption—must be publicly registered—before it can be offered to the public investors. Furthermore, once a security is issued to the public, it can only trade through regulated entities, undergo certain record-keeping, and fulfill continuous disclosure requirements. In general, commodities spot transactions are considered simpler to perform than securities transactions.

To make it more complex, it is possible that the CFTC and SEC both claim jurisdiction over one same asset in what colloquially referred to as a “turf war.” The CFTC has [stated](#) its belief that all digital assets are commodities, but such a classification does not foreclose the possibility that a digital asset is also a security. Therefore, it is instructive to look at statements made by all government agencies when considering a digital asset’s classification as a security, commodity, or otherwise.

Because enforcement based on securities laws has more profound impact on the crypto markets and the related projects than CFTC regulation, this chapter will focus on the securities law related enforcement actions by the SEC.⁹ CFTC’s enforcement actions, such as its 2023 lawsuit against Binance, the world’s largest crypto exchange, will be discussed in Chap. 12 (relating to the national security issues).¹⁰

11.4.2 *Crypto’s Howey Test: Securities and/or Commodities?*

Currently, the process for determining whether a digital asset is a “security” in the US market requires interpreting statute, court precedent, and statements by government officials. The Securities Act of 1933 and the Securities Exchange Act of 1934 provide the definition of “security” that the markets use when determining how securities laws apply to a particular asset or transaction. The statutory definition of “security” is comprised of a long list of assets, including well-known securities like stocks, notes, and bonds, and it also includes the reference to “investment contract,” which is undefined by statute.

⁹Andersen, Derek. March 15, 2023, Cointelegraph report, “Gensler suggests staking token operators should ‘seek to come into compliance,’” <https://cointelegraph.com/news/gensler-suggests-staking-token-operators-should-seek-to-come-into-compliance>

¹⁰CFTC release. “CFTC Charges Sam Bankman-Fried, FTX Trading and Alameda with Fraud and Material Misrepresentations,” December 13, 2022. <https://www.cftc.gov/PressRoom/PressReleases/8638-22>

To determine whether a digital asset is an investment contract, one must apply the *Howey* Test articulated by the Supreme Court in *SEC v. W.J. Howey Co.* In that case, the Supreme Court stated that something is an investment contract if all four of the following prongs are satisfied:

1. There is an investment of money;
2. In a common enterprise;
3. With the reasonable expectation of profits;
4. Based on the efforts of others.

From the current SEC perspective, a crypto-asset can be deemed an investment contract, and therefore a security subject to SEC oversight, if the asset meets the “Howey test.” This resulted in the SEC asserting its jurisdiction through various enforcement actions against crypto market participants and issuers. Over time, the SEC has alleged that several digital assets are investment contracts under the Howey Test, including [XRP](#) of Ripple, which will be discussed in detail below.

11.4.3 *SEC V. Ripple Case*

A business named Ripple Labs first appeared on the fintech landscape in 2012 with a promise to provide financial institutions with low cost and speedy clearance of cross-border money transfers. To make it happen, the business created the RippleNet network on which transactions in the form of a [cryptocurrency called XRP](#) can be settled and cleared in real time.

Over several years, however, [XRP](#) grew outside of the stated application. The Ripple founders used XRP as digital assets to raise funds in 2013. As a result, the SEC alleged in 2020 that Ripple Labs and two of its executives raised more than \$1.3 billion in 2013 via an unregistered security offering of XRP. According to the SEC complaint, Ripple raised funds by selling XRP tokens in unregistered security offerings to investors in the USA and around the world. Additionally, Ripple offered billions of XRP in exchange for non-cash services like market-making and labor.¹¹

Typically, instead of going to trial, the SEC settles most of its lawsuits—whether crypto-related or more broad capital market enforcement actions. Individual companies often submit to the SEC’s demands and pay penalties in order to be released. In the Ripple case, however, the company management went all the way and engaged the SEC in a full legal battle.¹²

Therefore, the Ripple vs. SEC litigation conclusions concern more than simply the Ripple community. The case will decide if crypto-assets are commodities or securities, with the latter falling inside a legal framework with much more existing

¹¹ SEC. “SEC Charges Ripple and Two Executives with Conducting \$1.3 Billion Unregistered Securities Offering,” December 22, 2020. <https://www.sec.gov/news/press-release/2020-338>

¹² Forkast. “Ripple expects SEC ruling in first half, clearer global regulations for digital assets in 2023,” January 4, 2023. <https://forkast.news/ripple-expects-sec-ruling-in-first-half/>

regulations. According to Ripple executives' media interview in 2023, the Judge's decision is expected to occur in the first half of 2023. Aside from XRP holders, the verdict of Ripple case will become a milestone legal precedent, which will have broad consequences to everyone participating in the crypto industry including the exchanges, investors, and startup founders.

11.4.4 Staking under Attack: Coinbase and the Wells Notice

In a March 2023 tweet, Coinbase CEO Brian Armstrong said the company had received a "Wells Notice" from the SEC regarding an unspecified portion of our listed digital assets. Also, SEC is investigating Coinbase's staking practices, whereby customers can stake or pledge their current crypto holdings and receive passive income in return, usually in the form of additional crypto.

A Wells notice is the way that SEC staff tells a company that they are recommending that the SEC take enforcement action for possible violations of securities laws. A Wells notice is typically one of the final steps before the SEC formally issues charges. It generally lays out the framework of the regulatory argument and offers the potentially accused an opportunity to rebut the SEC's claims. It is not a formal charge or lawsuit, but it can lead to one.

Indeed, the SEC has given staking companies several warnings that their programs may violate US security registration requirements, including the SEC's [February 2023 action against Kraken](#). To settle the SEC's charges, the two Kraken entities agreed to immediately cease offering or selling securities through crypto-asset staking services or staking programs and pay \$30 million in disgorgement, prejudgment interest, and civil penalties.¹³

Just like the Ripple case, the Coinbase management team seems to be determined to carry out the legal battle with the SEC. (Coinbase CEO Brian Armstrong told CNBC at a fintech event the company is prepared for a "years-long" legal battle with the SEC.) Thus, the outcome of future SEC actions against Coinbase will also become an important case precedent for the crypto industry.¹⁴

Furthermore, it's worth noting that Coinbase is the first and only SEC-registered major crypto exchange, and the SEC actions against Coinbase indicates that the SEC is setting a high bar for registered crypto exchanges, let alone unregistered, decentralized crypto exchange (DEX).¹⁵ Brian Armstrong said separately in a talk

¹³SEC. "Kraken to Discontinue Unregistered Offer and Sale of Crypto Asset Staking-As-A-Service Program and Pay \$30 Million to Settle SEC Charges," February 9, 2023. <https://www.sec.gov/news/press-release/2023-25>

¹⁴Coinbase blog. "We asked the SEC for reasonable crypto rules for Americans. We got legal threats instead," March 22, 2023. <https://www.coinbase.com/blog/we-asked-the-sec-for-reasonable-crypto-rules-for-americans-we-got-legal>

¹⁵De, Nikhilesh. "Crypto Exchange Bittrex Violated Federal Laws, SEC Charges in Lawsuit," Apr 17, 2023. <https://www-coindesk-com.cdn.ampproject.org/c/s/www.coindesk.com/pol->

on stage that the USA “has the potential to be an important market in crypto” but right now is not delivering regulatory clarity. If this goes on, he said, then Coinbase would consider options of investing more abroad, including relocating from the USA to elsewhere.

In short, the US regulatory landscape in the near term is mostly defined by the SEC enforcement actions, and that’s not very promising for the cryptocurrency enthusiasts. In fact, SEC chair Gensler in 2023 confirms “everything other than Bitcoin” is a security. (Interestingly, he believes that Bitcoin is not a security but a commodity under the Commodity Futures Trading Commission (CFTC) purview.¹⁶ This conclusion is probably based on the belief that Bitcoin has no “common enterprise,” which is linked to the PoW (Proof-of-Work) mechanism of Bitcoin.)

11.5 Stablecoin Regulation: A Rare Global Consensus

The USA and China don’t agree on much these days. But there’s one issue on which both superpowers see eye to eye: the regulation of “stablecoins,” a special type of crypto-assets that pegs its value to conventional money.

On July 16, 2021, US treasury secretary Janet Yellen called on the President’s Working Group (PWG) to develop a regulatory framework for cryptocurrencies. Specifically, Yellen pushed financial regulators to [draft stablecoin rules](#), due to its “potential risks to end-users, the financial system, and national security.” The PWG meeting was promptly held on July 19, the following Monday, and it announced the plan to [issue recommendations about stablecoin regulations within the next few months](#). “The secretary underscored the need to act quickly to ensure there is an appropriate US regulatory framework in place,” the Treasury reported.¹⁷

It may be a coincidence but on the same July 16, the People’s Bank of China (PBOC, China’s central bank) [issued a white paper](#) on its development of China’s digital currency (e-CNY), where the PBOC cited the rapid growth in cryptocurrencies, especially global stablecoins, as a driver for its research and development of e-CNY. (Globally, China has taken the lead in digital currency push, and it is likely to be the first major economy to introduce a sovereign digital currency.)

“Some commercial institutions even plan to launch global stablecoins, which will bring risks and challenges to the international monetary system, payment and clearing system, monetary policies, cross-border capital flow management, etc.,”

[i c y / 2 0 2 3 / 0 4 / 1 7 / crypto-exchange-bittrex-violated-federal-laws-sec-charges-in-lawsuit/?outputType=amp](#)

¹⁶Lian, Anndy. “SEC chair Gensler confirms ‘everything other than Bitcoin’ is a security: Implications and analysis,” February 28, 2023 <https://cryptoslate.com/sec-chair-gensler-confirms-everything-other-than-bitcoin-is-a-security-implications-and-analysis/>

¹⁷De, Nikhilesh. “Presidential Advisory Group Promises Stablecoin Recommendations,” July 19, 2021. <https://www.coindesk.com/markets/2021/07/19/presidential-advisory-group-promises-stablecoin-recommendations/>

said PBOC in the white paper. This is the first time that China's Central Bank, in an official document, links its sovereign digital currency issuance with stablecoins' potential risks and challenges to the international monetary system.

Why are stablecoins so important? For a comparison, Bitcoin is exciting: its price swoops and dives. Such volatility has made Bitcoin well known to the public. But the stablecoins are the opposite, which are crypto tokens pegged or linked to the value of fiat currencies. Because they are boring, they are equally useful: these stablecoins are embedded in crypto trading and lending platforms. How do people trade paper dollar for crypto-assets (or crypto-to-crypto)? Usually, they use stablecoins as the medium. For example, in that July 2021, [nearly three-quarters of trading](#) on all crypto trading platforms occurred between a stablecoin and some other token, according to the data from The Block.

Stablecoins can be a bridge between two worlds that weren't designed to mix—crypto-assets and traditional finance. They make it easier to move funds in traditional currency onto crypto exchanges. Many exchanges don't have the relationships with banks needed to offer regular currency deposits or withdrawals, but they can and do accept stablecoins such as Tether, also known as USDT.

For example, Tether is especially useful in the China crypto market, because it is the critical link for onshore Chinese investors, whose funding in Chinese RMB (CNY) is separate by Chinese regulators from the offshore USD market, to trade cryptocurrencies on platforms owned by overseas exchanges.

Because stablecoins are at the center of the global crypto ecosystem, the corresponding regulation is equally important. US Treasury Department actions and China PBOC white paper are echoed by SEC [Chairman Gary Gensler in his speech](#) at the Aspen Security Forum in August 2021. Chairman Gensler said cryptocurrency markets were “rife with fraud, scams and abuse” and called on Congress to give his agency new regulatory powers. He also singled out stablecoins and explained the necessity of regulation from financial security and securities law perspectives (which also explains why the crypto talk happened at Aspen Security Forum).¹⁸

First, from the financial security (and national security) perspective, “the use of stablecoins on these platforms may facilitate those seeking to sidestep a host of public policy goals connected to our traditional banking and financial system: anti-money laundering, tax compliance, sanctions, and the like,” said Gensler. The worry here is that the growing size of stablecoins has created a situation where huge amounts of US dollar-equivalent coins are being exchanged without touching the US financial system.

Second, from the securities regulation perspective, “these stablecoins also may be securities and investment companies.” To the extent they are, the SEC “will apply the full investor protections of the Investment Company Act and the other federal securities laws to these products.”

¹⁸SEC. “Remarks Before the Aspen Security Forum by Chair Gary Gensler,” August 3, 2021. <https://www.sec.gov/news/speech/gensler-aspen-security-forum-2021-08-03>

A **third** consideration, which has more to do with the US Treasury and Federal Reserve, is the stability (or the lack of) of the balance sheet of those stablecoins' issuers. Lawmakers and regulators have expressed alarm that retail investors are not fully protected, should one of the stablecoin firms not have the backing they purport to have.

A useful comparison is with money-market funds, which were created in the 1970s to circumvent rules limiting the interest banks could pay depositors. After promising to maintain the value of their shares at a dollar, money-market funds blew up in 2008 in the global financial crisis. American taxpayers stepped in to forestall a fire sale of their assets and a crash in the market for commercial paper, on which the real economy depends. A collapse of stablecoins could look similar according to banking industry experts.

In summary, it may be stablecoins' turn in the regulatory spotlight. Given the common focus on stablecoins by the US Treasury department, Federal Reserve, the SEC, and the legislature, the regulation of stablecoins may emerge soon in the USA. Meanwhile, EU's MiCA also put stablecoins under more stringent regulations than general crypto-assets. Stablecoins like USDT and Circle's USDC will be required to maintain ample reserves to meet redemption requests in the event of mass withdrawals. Stablecoins that become too large also face being limited to 200 million euros (\$220 million) in transactions per day.

Given the rare consensus on stablecoin regulations by China, EU, and the USA, the global crypto market may see serious enforcement actions to occur soon. But that may be a constructive development for the broad crypto market. Since stablecoins are the fundamental infrastructure for the entire digital asset industry, their complete and transparent disclosure is critical.

11.6 Conclusion: Regulatory Game of Thrones

The year 2023 is the start of a new crypto world, after consumers, businesses, and investors around the world lost nearly \$2 trillion in the digital assets market in the year before. Many regulators across the globe have either enacted regulatory schemes for dealing in crypto-assets or are on the brink of doing so.

While China develops its own sovereign digital currency (CBDC) and put a full stop on the private crypto transactions, EU's MiCA, the world's first comprehensive framework for crypto regulation, is a paradigm shift to both support and regulate the crypto space. Just like EU's GDPR (General Data Protection Regulation) has been the model law on data privacy protection for many jurisdictions, MiCA is likely to become a template that many other countries look to when developing their own crypto-asset regulatory frameworks.

Now all eyes are on the USA. Amid FTX debacle and a series of crypto bankruptcy cases following that, on January 27, 2023, the Biden administration released a strong statement ("Road Map to Mitigate Cryptocurrencies' Risk"), indicating its continued focus on cracking down on perceived abuses in crypto markets, and

calling for Congress to move more swiftly to strengthen legal frameworks. However, the US legislature is quite divided on crypto issues, therefore the US crypto law may take some time to materialize and before that, the US regulatory landscape will remain fragmented.¹⁹

Globally, different countries may follow different approaches from China, EU, and the USA. While regulatory timelines are not in all cases set, the direction of travel is clear. With global regulation rising, the crypto community must pay close attention to such developments and adapt to the “new normal.” Firms involved in digital assets must be prepared for higher standards than those in place today. The bar is rising to bring digital asset firms in line with traditional financial services obligations, such as corporate governance, regulatory compliance, and risk management.

To conclude, the coming years may be the most tumultuous yet in terms of coming storms and how crypto businesses will keep themselves dry—and solvent. The remaining viable players in the crypto industry must work hard to regain market trust, particularly among regulators and policymakers. The global shift in crypto oversight is “a regulatory Game of Thrones” for crypto projects—where you comply (live), or you die.

¹⁹The White House. “The Administration’s Roadmap to Mitigate Cryptocurrencies’ Risks,” January 27, 2023. <https://www.whitehouse.gov/nec/briefing-room/2023/01/27/the-administrations-roadmap-to-mitigate-cryptocurrencies-risks/>

Chapter 12

Terrorist Financing, War Crimes, and Crypto Geopolitics



Winston Ma

12.1 Crypto and Geopolitics: Ukraine V. Russia War

12.1.1 *Crypto in Conflict*

For the vast majority of those watching the rapid rise of cryptocurrency (with blockchain), its emergence has been something of a curious novelty. The Russia–Ukraine war that started in February 2022 unexpectedly shines a spotlight on cryptocurrency, illustrating distract concepts like fast payment, decentralized network, and non-fungible token (NFT) in live, dramatic contexts.¹

In a March 2022 news article, Yahoo Finance noted that the Ukrainian government and nongovernmental organizations supporting the Ukrainian military effort have collectively raised \$59.2 million from crypto donations. Alex Borynyakov, Ukraine’s Deputy Minister of Digital Transformation, stated that crypto donations are crucial, especially due to the fast turnaround time: “In times like these, response time is crucial. Crypto is playing a role to give us flexibility to respond really quickly to deliver the army’s required supplies.” Crypto donations to Ukraine’s government began to spike when Mykhailo Fedorov, Ukraine’s vice prime minister, posted a Bitcoin and Ethereum wallet address via his Twitter, soliciting crypto donations worldwide (see Fig. 12.1).

¹Chainalysis. “Cryptocurrency Brings Millions in Aid to Ukraine, But Could It Also Be Used for Russian Sanctions Evasion?,” March 28, 2022. <https://blog.chainalysis.com/reports/cryptocurrency-ukraine-russia-sanctions/>

W. Ma (✉)
NYU School of Law, New York, NY, USA



Fig. 12.1 Ukraine’s Vice PM Tweeted Crypto Wallet Addresses for Donations

Crypto donations like Bitcoins and Ethereum tokens (including NFTs, i.e., Non-Fungible Tokens) have helped Ukrainians in a massive way by providing a source of monetary support in a secure fashion, from anywhere in the world to Ukrainians in urgent need. In March 2022, Ukraine government legalized the crypto sector as digital currency donations continue to pour in. It passed a law that creates a legal framework to allow foreign and Ukrainian cryptocurrencies exchanges to operate legally. Banks will be allowed to open accounts for crypto companies. Although Ukraine did not make any cryptocurrency legal tender, “virtual assets” become legal assets.

On crypto-based donations, Tom Robinson, blockchain analytics firm Elliptic’s chief scientist, noted in a March 2022 CNBC article that cryptocurrencies also have the advantage of being suited toward international fundraising, due to their decentralized nature: “Cryptocurrency is particularly suited to international fundraising because it doesn’t respect national boundaries and it’s censorship-resistant—there is no central authority that can block transactions, for example, in response to sanctions.”

12.1.2 Sovereign Nations into Crypto Market

“No central authority”? Maybe. After the war broke out, US Treasury Secretary Janet Yellen announced that US would monitor cryptocurrencies as a channel (for Russia) to evade sanctions from the US and Western nations. The International Monetary Fund warned in a report that bitcoin could allow countries such as Russia to monetize energy resources, “some of which cannot be exported due to sanctions.” The European Commission has clarified that all of its preexisting financial sanctions measures apply to activity conducted in crypto assets.

In April 2022, the US Treasury Department began to take action against companies in Russia’s virtual currency mining industry, because “these companies help Russia monetize its natural resources.” (According to data from Cambridge University, Russia is the world’s third-biggest destination for bitcoin mining.) Furthermore, officials and oligarchs are attempting to use crypto in an effort to conceal their wealth from the Office of Foreign Assets Control (OFAC) and other highly effective global sanctions regimes.²

Since the war broke out, the US has undertaken numerous actions targeting Russia that have implications for crypto space, including:

- **February 2022:** the US imposed restrictions on dealings with the Donetsk and Luhansk regions of Ukraine, where pro-Russian separatist groups have been identified soliciting donations in Bitcoin.
- **March 2022:** the US Treasury’s Financial Crimes Enforcement Network (FinCEN) issued an alert on red flags of Russian sanctions evasion. This includes red flags related to crypto activity, including the potential for virtual asset service providers (VASPs) located in high-risk jurisdictions to facilitate sanctions evasion.
- **April 2022:** the US Treasury’s Office of Foreign Assets Control (OFAC) imposed targeted sanctions on the Russian dark web marketplace Hydra and on Garantex, an Estonian-registered crypto exchange service involved in laundering funds on behalf of Russian cybercriminals. OFAC listed over 100 crypto asset addresses belonging to these entities on the Specially Designated Nationals and Blocked Persons List (SDN List), prohibiting US persons from dealing with those or other addresses controlled by Hydra and Garantex. In the same month, OFAC sanctioned the Russian Bitcoin mining company BitRiver.
- **September 2022:** OFAC sanctioned Task Force Rusich for its paramilitary activities in Ukraine, including crypto addresses belonging to the group on the SDN List.

Nevertheless, pro-Russian fundraising and donations still exist. According to Ecliptic’s report in 2023, pro-Russian crypto activity poses significant sanctions and anti-financial crime compliance risks to virtual asset services. Over 10% of

²CSIS. “Cryptocurrencies and U.S. Sanctions Evasion: Implications for Russia,” December 20, 2022. <https://www.csis.org/analysis/cryptocurrencies-and-us-sanctions-evasion-implications-russia>

pro-Russian donations originate from illicit sources, including dark web markets, sanctioned entities, and stolen credit card vendors. Many entities raising crypto have also openly advocated and glorified potential war crimes and crimes against humanity.

12.1.3 Decentralized Exchanges Caught in the War

Decentralized? We will see. Whereas Ukraine’s vice prime minister tweeted crypto wallet addresses for donations, he also urged crypto exchanges to block the addresses of Russian users. “It’s crucial to freeze not only the addresses linked to Russian and Belarusian politicians but also to sabotage ordinary users,” he tweeted (see Fig. 12.2).

One crypto exchange, DMarket, quickly responded to the calling. According to Axios reports, DMarket is a Ukrainian startup that sells NFTs and virtual items for games such as Counter-Strike: Global Offensive. DMarket soon blocked new user registration from Russian and Belarus on its platform as a manner of protest against Russian invasion, even though approximately 30% of DMarket’s customers are from these two countries. Besides the ban on new user registration, DMarket has also frozen assets of Russian and Belarusian users and prohibited transactions involving the Russian ruble.

The crypto community, however, regarded this as a controversial move. Many were greatly displeased with DMarket’s actions, expressing via Twitter that Russian users have become the scapegoat caught in the middle of a war they did not cause. Other users have commented that DMarket’s move to freeze Russian and Belarusian assets on their platform is stealing value from innocent users who are merely



Fig. 12.2 Ukraine’s Vice PM Urged Crypto Exchanges to Sabotage Russian Users

targeted due to their nationality. Furthermore, Twitter users have commented that DMarket's move is a violation of the idea of cryptocurrency and Web3, which heralds decentralization as a core value.

12.1.4 Best Practices in Need

As the war between Russia and Ukraine rages on, it has brought into focus cryptocurrencies and their use—and related debates. Both sides have used blockchain technology to aid their respective efforts. Many campaigns have sought to harness core developments in the crypto ecosystem to aid their fundraising. The ongoing war highlights the rising participation of sovereign nations in the cross-border crypto ecosystem, as well as the profound implications for private players—ranging from sanctions concerns to complicity with potential war crimes.³

As a result, the international crypto markets must develop best practices for crypto-based fundraising, sanctions compliance, and anti-financial-crime controls, in the wake of a rapidly changing crypto regulatory landscape.

12.2 Money Laundering/Terrorism Financing on Blockchain

12.2.1 Unique Characteristics of Crypto Assets

Cryptocurrencies pose challenges to national security because they make it possible to hold and transfer money without a central authority, like SWIFT or PayPal, that can shut down accounts and freeze funds. Anyone in the world can create a Bitcoin address and begin receiving digital tokens without even providing a name or an address.

Crypto assets, particularly Bitcoin, have become the most common form of payment for drug dealing, human trafficking, and ransomware attacks increasingly targeting businesses and public services, because it allows the **nefarious actors** behind these attacks to receive large amounts of money quickly and anonymously. Some of their unique characteristics make them appealing for conducting illegal activities:

1. Transactions do not have to be conducted in person;
2. Decentralized, unsupervised by any government or central bank, and therefore, like cash, preserve a high degree of anonymity; and.
3. Virtual, and therefore generally unbounded by geographical borders.

³Elliptic. "Sanctions Compliance in Cryptocurrencies 2023," April 18, 2023. <https://www.elliptic.co/resources/elliptic-guide-to-sanctions-compliance-in-crypto-2023>

12.2.2 *DeFi Tricks: DEXs, Mixers, and Liquidity Pools*

Furthermore, the development of DeFi (Decentralized Finance) provides more sophisticated tools for illicit actors to abuse DeFi services and launder illicit proceeds. While there is currently no generally accepted definition of DeFi, the term broadly refers to protocols of crypto assets that allow some form of automated peer-to-peer transactions, by using self-executing code known as “smart contracts” based on blockchain technology.

Bad actors may use a variety of DeFi techniques and services for their global money transfers, including exchanging virtual assets for other virtual assets that are easier to use in the virtual asset industry or less traceable (sometimes using cross-chain bridges to exchange virtual assets for others that operate on other blockchains); sending virtual assets through mixers; and placing virtual assets in liquidity pools as a form of layering.

These laundering methods can create challenges for investigators attempting to trace illicit proceeds, and many actors may mix more than one of these techniques:

- **DEXs and Cross-Chain Bridges:** Illicit actors can use DeFi services, such as a DEX (decentralized exchanges), to convert one virtual asset into a different virtual asset. They do this for a variety of reasons, including to exchange into a more liquid asset that has higher trading volumes and is easier to cash out into fiat currency, or into another currency that allows them to evade government sanctions. They may choose to exchange their illicit proceeds for several different assets, sometimes using different DEXs to obtain better conversion rates and diversify their laundering methods.
- Illicit actors can also chain-hop, exchanging virtual assets on one blockchain for virtual assets on another, which could be done through a DEX or aggregator or by interacting directly with a cross-chain bridge. Such “chain-hopping” can make it more difficult for authorities to trace financial transactions or for service providers to detect if incoming funds are tied to illicit activity. This is especially true if actors are using specific assets or blockchains that are more difficult to trace given current limits on blockchain analysis.
- **Mixers:** Bad actors also use virtual asset mixers to functionally obfuscate the source, destination, or amount involved in a transaction. Mixers can accomplish this through a variety of ways, including pooling or aggregating virtual assets from multiple individuals, wallets, or accounts into a single transaction or transactions; splitting an amount into multiple amounts and transmitting the virtual assets as a series of smaller independent transactions; or leveraging code to manipulate the structure of the transactions. (See the Case Study of “Tornado Mixer” below.)
- **Liquidity Pools:** A liquidity pool is a digital pile of cryptocurrency locked in a smart contract. A major component of a liquidity pool is the [automated market makers](#) (AMMs), which is a protocol that uses liquidity pools to allow digital assets to be traded in an automated way rather than through a traditional market

of buyers and sellers. Liquidity pools are designed to incentivize users of different crypto platforms, called liquidity providers (LPs), by awarding them with liquidity provider tokens (LPTs). LP tokens can then be used in different ways on a DeFi network.

- Illicit actors can place criminals' proceeds in a DeFi service's liquidity pool, and as liquidity providers they may receive a portion of fees or some other type of return created through the DeFi service. (For compliance-sensitive financial institutions, sometimes they demand DeFi protocols that allow liquidity pools to add permissioning, meaning both lenders and borrowers must be approved by a central body of "whitelisters," adding a centralized component to the decentralized protocol.)

12.2.3 Case Study: Tornado Mixer and North Korea

Pariah states use cryptocurrencies, and the anonymity that they grant, to evade sanctions and launder money. Before US government's sanction on the decentralized crypto-mixing service Tornado Cash for linkage with Democratic People's Republic of Korea (DPRK), it has [spent years](#) warning that crypto mixers may be illegal or aid in illegal activity.

For users of Tornado Cash, new funds deposited into Tornado Cash are placed into a "pool" of other users' tokens. From here, users can withdraw their funds to another address while concealing where they came from originally. Tornado Cash says it is non-custodial, meaning users always maintain complete control of their funds—even if those funds are technically in one of Tornado's pools.

According to the US [Treasury Department](#) and the Office of Foreign Asset Control (OFAC), its sanctions watchdog, Tornado Cash has been a key tool for the Lazarus Group, a North Korean hacking group tied to the [\\$625 million March hack](#) of Axie Infinity's Ronin Network, among others. [OFAC sanctioned Tornado Cash](#) in August 2022, claiming North Korean hackers had laundered hundreds of millions of dollars' worth of crypto through the mixer since its launch. (According to Elliptic's research, Tornado Cash has enabled criminals to launder more than \$1.5 billion in criminal proceeds, including funds associated with North Korea's crypto-enabled sanctions evasion.)

Because of the OFAC order, all U.S. persons and entities [are prohibited](#) from interacting with Tornado Cash or any of the Ethereum wallet addresses tied to the protocol. Those who do may face criminal penalties. As would be expected, the crypto industry has opposed the move, pointing to the fact that OFAC does not normally sanction "software" and the fact that Tornado Cash does not have any central operator.

In November 2022, OFAC redesignated Tornado Cash for its role in enabling malicious cyber activities that ultimately support the DPRK's WMD (weapons of mass destruction) program. OFAC stated that sanctions were applied to the entity

known as Tornado Cash and that Tornado Cash uses computer code known as “smart contracts” to implement its governance structure, provide mixing services, offer financial incentives for users, increase its user base, and facilitate the financial gain of its users and developers.

OFAC also explained that Tornado Cash’s organizational structure consists of: (1) its founders and other associated developers, who together launched the Tornado Cash mixing service, developed new Tornado Cash mixing service features, created the Tornado Cash DAO, and actively promoted the platform’s popularity in an attempt to increase its user base; and (2) the Tornado Cash DAO, which is responsible for voting on and implementing new features created by the developers.

It should be noted that in response to the sanctions, the advocacy group Coin Center filed lawsuits against the Treasury Department and OFAC. The complaint alleged that sanctioning Tornado Cash was “unprecedented and unlawful,” in part, due to privacy concerns over crypto transactions. The ruling of the Coin Center lawsuits may provide more guidance for the crypto community regarding sanction-related compliance.

12.3 FATF’s AML/CFT Framework and Travel Rule

12.3.1 Are Cryptos Traceable?

Despite regulatory enforcement, bad actors can exploit vulnerabilities, including the fact that many DeFi services, which have anti-money laundering and countering the financing of terrorism (AML/CFT) obligations, fail to implement them. Today, pariah states, terrorist organizations, and cybercriminals are still using DeFi services to transfer and launder their illicit proceeds.

Like many people, terrorists may have thought that crypto, especially bitcoin, is untraceable and is primarily used for nefarious purposes, but that’s a huge misconception.

For example, in January 2019, the Al-Qassam Brigades, the military wing of Hamas, began a fundraising campaign. This group is a designated terrorist organization by many countries, including the USA, Israel, and the European Union. They began the campaign by requesting that funds be sent to a static donation address listed on their website. Approximately \$4000 worth of cryptocurrency donations were received. The organization also introduced a fundraising platform that assigns distinct donation addresses to every visitor. This method, often employed by ransomware, presents a greater obstacle for external parties attempting to monitor contributions and track their destinations. Nevertheless, a blockchain data analytic firm, Elliptic, was able to identify a group of addresses employed to receive donations within this campaign. This accomplishment entailed conducting network analysis on transactions associated with prior campaigns executed by the same individual or group (Wilder 2019). That’s because blockchain, the technology that underpins

bitcoin, is a public ledger of activity. It's therefore possible to track the movements of funds from one account to another. In other words, in the cryptocurrency ecosystem, coins have a story, tracked in the unchangeable blockchains underpinning their economy. ("Blockchain Analytics" will be discussed in detail later in this chapter.)

Therefore, crypto assets are not "non-traceable." In fact, the primary vulnerability that illicit actors exploit stems from non-compliance by DeFi services with AML/CFT and sanctions obligations. DeFi services at present often do not implement AML/CFT controls or other processes to identify customers, allowing layering of proceeds to take place instantaneously and pseudonymously, using long strings of alphanumeric characters rather than names or other personally identifying information. The challenges in the cross-border context is even worse.

As such, the international community has developed a comprehensive, multinational response with enforcement power, the Financial Action Task Force (FATF).⁴

12.3.2 FATF: Unified Global Response

The FATF is the international watchdog responsible for coordinating the global fight against money laundering, terrorism financing, and nuclear proliferation. It is a proactive and robust organization that enjoys tremendous professional credibility and global influence over both member and non-member countries. The FATF is composed of thirty-nine member countries (including most of the G20 countries) and regional organizations, and together with its nine associated FATF-Style Regional Bodies (FSRBs), it encompasses over 200 jurisdictions.

The FATF has defined financial standards, called "Recommendations," which are in fact mandatory measures that all countries and jurisdictions must implement into their national legal systems. The FATF and FSRBs conduct ongoing monitoring to review and evaluate the level of compliance of countries with these Recommendations. All jurisdictions, regardless of their membership status, must adopt the FATF Recommendations into their legal framework and implement them in an efficient manner or risk being cut off from the global financial system.

When the FATF finds that a jurisdiction has a substantial deficiency or non-cooperation with the evaluation process, it may list that jurisdiction on its "gray list" (under "increased monitoring") or "blacklist" ("high-risk" jurisdiction). These lists are powerful signaling tools that put severe pressure on the listed jurisdictions to quickly meet FATF Recommendations. Jurisdictions on the gray lists will see their respective financial sectors' ability to participate in the global market becoming limited. A place on the blacklist practically abolishes financial activities between the blacklisted country and other jurisdictions.

⁴Sanction Scanner. "Financial Action Task Force (FATF) Travel Rule," 2023. <https://sanctionscanner.com/blog/financial-action-task-force-fatf-travel-rule-140>

In 2014, FATF identified the risks associated with cryptocurrency. The cryptocurrency is covered by the broader realm of “virtual assets,” a term used by the FATF to cover digital representations of value that can be digitally traded or transferred and can be used for payment or investment purposes, but do not include digital representations of fiat currencies, securities, and other financial assets.

In 2018, the FATF revised its standards to explicitly apply similar rules for virtual assets and VASPs as those in existence for other kinds of financial services providers. Since then, the FATF has been leading coordinated implementation efforts around the world.

The FATF’s response was the first global, coordinated regulatory response to cryptocurrency risks. The FATF has continued to be responsive to impending challenges by publishing clarifications and updates related to the application of the FATF Recommendations to the cryptocurrency industry. The latest development is the “Travel Rule,” which has proven to be one of the most significant and complex facets of the cryptocurrency industry for Virtual Asset Service Providers (VASPs).

12.3.3 Travel Rule

Financial Action Task Force (FATF) recently published its updated recommendations, one of which now requires VASPs and financial institutions engaged in virtual asset (VA) transfers to collect and share personal data of a transaction’s sender and recipient. This is stated in Recommendation 16, commonly referred to as the Travel Rule. (Initially, this requirement only applied to financial institutions; however, in 2019, the FATF expanded its recommendation to include VASPs, or platforms that provide cryptocurrency services.)

The Travel Rule for crypto states that all crypto companies—such as exchanges, banks, OTC desks, hosted wallets, and other financial institutions—must screen, record, and communicate the information of both sender and recipient (relevant originator and beneficiary information) for crypto transactions that exceed \$1000 or a certain amount designated by FATF member states. Because the personal data of the transacting parties “travels” with their transfers, the regulation was dubbed the “Travel Rule,” which is like the standard that US banks are required to abide by for wire transfers under the Bank Secrecy Act (BSA).

In short, a company needs to introduce two solutions to stay compliant: one for collecting data and the other for sharing it. This requirement means many challenges for VASPs, such as finding the safest way (“data privacy”) to collect and share user data, without exposing it to hackers or data brokers (“data security”).

To protect users’ assets and personal information, VASPs must detect VASP-to-VASP payments and ensure that sensitive transaction data is shared only with legitimate counterparties (i.e., other Travel Rule-compliant institutions that are not out to steal someone’s personal information), while also checking for sanctions violations and money-laundering red flags.

Can Barely Buy an AK-47 with 600 Bucks

According to three blockchain analytics firms and CoinDesk's own analysis, Izz ad-Din al-Qassam Brigades, the militant wing of Hamas, received up to \$100,000 in bitcoin since the beginning of 2021—with a spike in donations in May, when Israel and Hamas exchanged multiple rocket attacks, resulting in hundreds of casualties. According to CoinDesk's reports in 2021, on-chain data showed that Hamas collected generous [bitcoin](#) donations and sent them through Binance as violence escalated in Gaza.

In March 2023, the Commodity Futures Trading Commission (CFTC) of the US [brought a civil enforcement action](#) against Binance, seeking punishments including fines and permanent trading bans. Filed in a federal court in Chicago, the CFTC lawsuit covered many aspects of the Binance operation, including its dealings with the Islamic militant group Hamas.

[The CFTC claims Binance knew](#) it had facilitated potentially illegal activity, and the US regulator accuses Binance executives of joking in internal office chats about illegal transactions that terrorists and criminals could have made on their crypto platform.

The complaint says Samuel Lim, then-chief compliance officer for Binance, had received information in February 2019 “regarding Hamas transactions” on Binance and told a colleague that terrorists usually send “small sums,” as “large sums constitute money laundering.” Lim’s colleague replied: “Can barely buy an AK47 with 600 bucks.”

In another chat about certain Binance customers (probably from Russia), Samuel Lim said in February 2020: “Like come on. They are here for crime.” Binance’s money laundering reporting officer agreed that “we see the bad, but we close 2 eyes,” per the CFTC complaint.

The complaint said Lim described a Binance compliance audit as a “half assed individual sub audit on geo(fencing)” to “buy us more time.”

“I HAZ NO CONFIDENCE IN OUR GEOFENCING,” the Money Laundering Reporting Officer wrote to Lim during this audit, per the complaint. She also wrote that she would “need to write a fake annual MLRO report to Binance board of directors wtf.”

“Yea its fine I can get mgmt to sign,” Lim responded, per the CFTC’s complaint.

“Lim’s internal discussions with compliance colleagues illustrate that Binance has tolerated Binance customers’ use of the platform to facilitate ‘illicit activity,’” said the CFTC’s complaint.

Of course, the FAFT recommendations must be translated into domestic laws to be fully enforceable. As discussed in the previous Chap. 11, the major economies like the US and EU are developing comprehensive crypto regulatory framework, during which process more serious AML/CFT laws are expected to occur as well.

Furthermore, VASP's non-compliance is the primary weakness during the process, no matter how many new laws and regulations can be enacted.

What's promising is that the latest enforcement actions taken by FTFA member states would accelerate the travel rule adoption and enforcement. Regulators have pursued cases against DeFi services operating in the US that failed to register with the appropriate regulators and failed to implement the requisite AML/CFT program. Among them, the CFTC's lawsuit against Binance, the world's largest crypto exchange, is a major milestone. (See **“Can Barely Buy an AK-47 with 600 Bucks.”**)

Meanwhile, these regulatory requirements call for reliable, interoperable authentication and encryption technology—advanced solutions that can help VASPs make certain that every transaction is seamless and safe, which will be discussed in the following section.

12.4 Crypto Intelligence and Blockchain Analysis

As the crypto ecosystems and transactions become increasingly complex, all stakeholders—financial institutions, government agencies, crypto exchanges, trading firms, individual customers, and all Virtual Asset Service Providers (VASPs)—must have technological tools to navigate the complex data that blockchain networks generate and make informed decisions. They need “crypto intelligence” to monitor, detect, and investigate crypto fraud and financial crime.

12.4.1 *Blockchain Analysis Solutions*

To that end, blockchain analytics companies, such as Chainalysis, CipherTrace, Elliptic, and TRM Labs, are the new key players in the cryptocurrency systems. They blend blockchain data with advanced analytics to help financial institutions and governments fight fraud, money laundering, and financial crime. Their blockchain analysis software can help AML and sanctions compliance at scale (See Table 12.1), by processing tens of thousands of crypto transactions in real time with capabilities that reveal the movement of assets as they pass through different blockchains and assets.

Using in-depth analysis and pattern recognition across thousands of interactions, it may be possible to identify nefarious users that legitimate players should avoid doing business with. It is the equivalent of credit checks on a credit card, making sure that the actions are legal and genuine. Furthermore, the software may develop new insights from raw blockchain data, providing players with real-time notifications about high-risk activities. They are indispensable for VASPs to comply with global regulations and trace the movement and risk of crypto funds.

Table 12.1 Key compliance checks by blockchain analysis

Compliance Check	Blockchain Analysis
Crypto wallet screening	<ul style="list-style-type: none"> • Assess the risk of crypto wallets. • Obtain accurate insights with minimal effort. • Understand the counterparty to comply with sanctions regulations and reduce fraud.
Crypto transaction monitoring	<ul style="list-style-type: none"> • Screen your crypto transactions for risk. • Automating AML/CFT and sanctions checks. • Empower your compliance team to spend their time where it's needed most.
VASP screening	Understand the risk profile of virtual asset service providers (VASPs), such as crypto exchanges, when evaluating them as customers or counterparties.
Crypto investigations	<ul style="list-style-type: none"> • Create detailed network visualizations of wallets and the transactions between them. • Gain new insights. • Develop reports and communicate the findings.

12.4.2 AI-Powered Analytics

Lately, AI (artificial intelligence) technology is added to blockchain analytics to enable additional security and trust to the digital ecosystem. For example, in late 2022 Mastercard debuted a new software called Crypto Secure, which uses artificial intelligence algorithms to determine the risk of crime associated with crypto exchanges on the Mastercard payment network.

Crypto Secure combines insights and technology from Mastercard's existing blockchain analytics with related proprietary information to develop insights, such that card issuers may stay compliant with the complex regulatory landscape of the digital assets sector. The platform allows them to better assess the risk profile of crypto exchanges or other VASPs and decide which purchases of cryptocurrency to approve.

On the Crypto Secure platform, banks and other card issuers are shown a dashboard with color-coded ratings representing the risk of suspicious activity, with severity of risk ranging from red for "high" to green for "low." Crypto Secure doesn't make a judgment call on whether to turn away a specific crypto merchant, which is down to the card issuers—like the technology used to prevent fraud in fiat currency transactions.

However, as artificial intelligence and natural language processing are increasingly employed to analyze vast amounts of financial data, privacy concerns become more pressing than ever. In 2023, OpenAI's AI chatbot (ChatGPT) took the world by the storm. With all eyes on AI, in the blockchain space, several AI startups are developing tools related to blockchain analytics, creating a new generation of analytics companies, such as Blocktrace, Arkham, and Nansen.

Take the Austin, US-based startup Blocktrace, for example. Originally established in 2018 as something like blockchain forensics firm Chainalysis by a

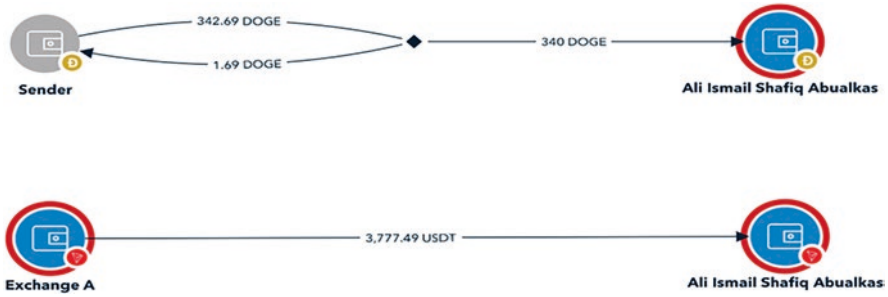


Fig. 12.3 TRM tool enabled investigation into Hamas Financing. Source: TRM (Graph does not reflect the full scope of detail available in the TRM platform)

software engineer previously served as the head of training at Chainalysis. Recently, Blocktrace has created an AI chatbot called Robby the Robot that interacts with Bitcoin blockchain data. This AI chatbot enables users to engage with a virtual assistant-like feature by posing questions in natural language, which is enhanced by an AI layer.

By leveraging AI chatbots and NLP (natural language processing) technology, these startups simplify blockchain transaction tracking and data analysis, offering users valuable insights. However, because AI-powered blockchain analytics are increasingly employed to analyze vast amounts of financial data, privacy concerns become more pressing than ever. As these services become more widely available to the public, it becomes imperative to address privacy in the crypto space.

12.4.3 The Case of Crypto Flow and Hamas Financing

Now we go back to Hamas case mentioned earlier in this chapter. Because cryptocurrency is not truly anonymized but rather “pseudo-anonymous,” governments and analysts can follow illicit funds to find not just bad actions but also bad actors, who need to move assets between addresses or entities. Just like counter-terror investigators may use cell phone records, for example, to discover the ties between bad actors, in the crypto world blockchain analytics can scrutinize the activity of wallets, represented as nodes in the graph database, to achieve a similar outcome.⁵

Below Fig. 12.3 shows the on-chain flow occurring between addresses associated with Hamas on the Tron and Dogecoin blockchains.

Understanding how those nodes are connected represents the digital equivalent of the link analysis activities with which law enforcement and national defense are

⁵TRM. “Hamas and Cryptocurrency: The Evolution of Terror Financing and the Global Effort to Stop It,” July 8, 2021. <https://www.trmlabs.com/post/hamas-cryptocurrency-financing-campaign-a-continuing-evolution>

familiar with. Bad actors may use a range of tools to disguise their illegal activity—for example, using non-compliant exchanges to move funds or running multiple wallets to cover their tracks—analytics can peer deeply into such activity to surface a clear picture for investigators.

12.5 Biden Executive Order and “Responsible Development”

For the topic of this chapter, US lawmaking and enforcement probably is the most important. US President Biden’s March 9, 2022, Executive Order “on Ensuring Responsible Development of Digital Assets” asserts that technological advances and the rapid growth of crypto markets “necessitate an evaluation and alignment of the United States Government approach to digital assets.” The order mandates multiple reports and studies, and it tasks more than twenty government agencies with responsibility for the effort.⁶

The Web3 industry had long been waiting for this executive order, yet it arrived unexpectedly in March 2022. Probably driven by the concern of sanctions-dodgers, the executive order showed that the government have begun to go further than merely arm-twisting exchanges to comply with existing anti-laundering guidelines—a policy tightening that the war has clearly accelerated.

12.5.1 *Role of National Security in Executive Order*

President Biden’s Digital Asset Executive Order mandates multiple reports and studies focused around six principal themes:

- Protecting U.S. consumers, investors, and businesses.
- Protecting U.S. and global financial stability and mitigating systemic risk.
- Mitigating illicit finance and national security risks posed by misuse of digital assets.
- Reinforcing U.S. leadership in the global financial system and in technological and economic competitiveness.
- Promoting access to safe and affordable financial services.
- Supporting technological advances that promote responsible development and use of digital assets.

The order tasks numerous government agencies with responsibility for the effort, which will be led directly out of the White House. Thirteen of 23 Cabinet

⁶The White House. “Executive Order on Ensuring Responsible Development of Digital Assets,” March 9, 2022. <https://www.whitehouse.gov/briefing-room/presidential-actions/2022/03/09/executive-order-on-ensuring-responsible-development-of-digital-assets/#:~:text=The%20United%20States%20should%20ensure,contribute%20to%20human%20rights%20abuses>.

departments (including Treasury, Justice, State and Homeland Security), all major financial services regulators, several science and technology offices, economic and policy officials, the intelligence community, and the EPA (Environment Protection Agency) will all play a role. A key takeaway from the order is that the Administration is not handing over responsibility for national crypto policy to the banking, securities, and other financial services regulators.

By giving a seat at the table to agencies such as the State Department, the Domestic Policy Council, the Council of Economic Advisers, the Office of Science and Technology Policy, the Office of Information and Regulatory Affairs and the National Science Foundation, the order signals that the US government may consider the potential impact of crypto technology on the US economy, national security and global leadership to be so profound that the legacy regulatory structures need to be modernized by a broader frame of reference.

Indeed, the Assistant to the President for National Security Affairs and the Assistant to the President for Economic Policy are responsible for coordinating the work for the executive agencies required by the order. Ukraine-Russia war-related sanction concern probably was an important catalyst for the order, even though the order called for a comprehensive crypto regulatory framework broader than money laundering.

12.5.2 Digital Dollar: US CBDC

Similar national security considerations can be found in the Biden Administration placing “the highest urgency on research and development efforts into the potential design and deployment” of a US central bank digital currency (CBDC). This is a clear statement of support from the Administration and to accelerate the Federal Reserve’s ongoing work on CBDC design and technological research.

Workstreams specific to CBDCs, mostly directed to the Federal Reserve Bank, include a report on potential design choices and implications; US participation in international efforts and pilot projects; a strategic plan for potential implementation and launch from the Federal Reserve; and a proposal for dollar CBDC legislation to be developed by the Attorney General in consultation with Treasury and the Federal Reserve.

What’s in the backdrop is that the US Fed is tech-ready if it pushes the digital dollar forward. Maybe a coincidence—when China started the international testing of its CBDC (eCNY) at the Winter Olympics in February 2022, [Boston Fed and MIT released a report](#) on the open-source code that they have developed and could be used as the groundwork for a CBDC. Because the US dollar is the global reserve currency and trade settlement currency for most nations, the digital US dollar may become the most important link between crypto assets and fiat currencies in the future, which is of strategic importance to the US.

12.5.3 *US Treasury: DeFi Poses a Threat to National Security*

Pursuant to the Executive Order, the US Treasury Department published its “Action Plan to Address Illicit Financing Risks of Digital Assets” in September 2022. The Illicit Finance Action Plan states that addressing weaknesses in AML regulation, supervision, and enforcement in foreign jurisdictions is a priority for the U.S. government. To support this work, the U.S. government will continue to work through the FATF to promote the effective implementation of measures related to digital assets. Supporting actions include:

1. Partnering with G7 countries to urge foreign jurisdictions to implement the FATF standards for virtual assets and VASPs;
2. Engaging bilaterally with countries that the U.S. government assesses will be receptive to engagement and have high illicit financing risks related to virtual assets to encourage and support implementation of the FATF standards for virtual assets and VASPs;
3. Working with Congress to secure funding requested in the 2023 Budget to support efforts to support the implementation of the FATF standards for virtual assets and VASPs abroad; and.
4. Sharing information with partner nations, as appropriate, to support international investigations and prosecutions on the abuse of digital assets.

Months later in April 2023, the Treasury Department published the 2023 DeFi Illicit Finance Risk Assessment, the first illicit finance risk assessment conducted on decentralized finance (DeFi) in the world. Its analysis comes as international standard-setters for anti-money laundering and counter-terrorist financing (AML/CFT), such as the FATF, focus increasing attention on the impact of innovation in the DeFi space, as discussed earlier in this chapter.

“Risk assessments play a foundational role in promoting understanding of the illicit finance risk environment and more effectively protecting the integrity of the U.S. financial system,” said, Under Secretary of the Treasury for Terrorism and Financial Intelligence Brian E. Nelson. “Our assessment finds that illicit actors, including criminals, scammers, and North Korean cyber actors are using DeFi services in the process of laundering illicit funds. Capturing the potential benefits associated with DeFi services requires addressing these risks. The private sector should use the findings of this assessment to inform their own risk mitigation strategies and to take clear steps, in line with AML/CFT regulations and sanctions obligations, to prevent illicit actors from abusing DeFi services.”⁷

Interestingly, in this report the Treasury cited data from Elliptic’s [State of Cross-Chain Crime Report](#), which notes that ransomware gangs laundered at least \$50

⁷U.S. Department of the Treasury. “Illicit Finance Risk Assessment of Decentralized Finance,” April 6, 2023. <https://home.treasury.gov/news/press-releases/jy1391>. Wilder, Heidi. 2019. “Tracing Bitcoins from a Hamas Terrorist Fundraising Campaign.” Elliptic. <https://www.elliptic.co/blog/tracing-bitcoin-terrorism>.

million through a single cross-chain bridge in the first half of 2022. The Treasury's highlighting of these risks also underscores the importance of blockchain analytics solutions—from Elliptic and its peers (as discussed in the previous section)—that are used to identify cross-chain laundering.

12.6 Conclusion: The US Balancing Act

As can be said of Biden Executive Order itself, the Treasury's DeFi Illicit Finance Risk Assessment Report reflects the fact that the digital assets sector has increasingly shifted from an area of interest for regulators to one of primary concerns. The Treasury's DeFi risk assessment marks an important development in anti-financial crime efforts in the crypto space, in that it stresses the need for regulated businesses to take proactive steps to identify related risks and complete compliance requirements.

More importantly, the risk assessment by the Treasury is typically the first step toward formal regulations. Therefore, some formal regulations on DeFi may be enacted soon by the US government before a comprehensive cryptocurrency regulatory framework can be put in place.

However, the US is careful in balancing innovation and compliance, the two sides of the “responsible development” coin. The same Treasury Department, in its 2022 Illicit Finance Action Plan, says that the US government is committed to supporting the pace of innovation while also combatting emerging illicit finance risks. Supporting Actions include:

1. Considering ways to modernize the U.S. payments infrastructure;
2. Working with interagency partners and Congress to implement recommendations stemming from the [President's Working Group on Financial Markets on Stablecoins](#); and
3. Supporting U.S. companies' collective pursuit of developing new financial technologies through regulatory and supervisory guidance, symposia, tech sprints, and FinCEN Innovation Hours.

Indeed, the Biden Executive Order itself carefully balanced the two aspects:

“We must support technological advances that promote responsible development and use of digital assets. The technological architecture of different digital assets has substantial implications for privacy, national security, the operational security and resilience of financial systems, climate change, the ability to exercise human rights, and other national goals.

The USA has an interest in ensuring that digital asset technologies and the digital payments ecosystem are developed, designed, and implemented in a responsible manner that includes privacy and security in their architecture, integrates features and controls that defend against illicit exploitation, and reduces negative climate impacts and environmental pollution, as may result from some cryptocurrency mining.”

In summary, blockchain technology and digital currencies are driving tremendous innovation that has the potential to make the global economy more efficient. But they may also pose various national security issues and financial threats. The US government, as well as many countries, will tighten cryptocurrency regulations out of national security concerns. This will be a “new normal” risk factor for Web3 innovation going forward.

Amid the rapidly changing geopolitical landscape, it is critical that crypto asset businesses and financial institutions prepare for an ever-tightening sanctions compliance environment. At the same time, blockchain-driven technology innovation is still encouraged, and the compliance challenges can also be managed by more technological development of blockchain analytics.