Blockchain: Fundamentals, Data Structures and Algorithms for Data Science

Akcora, Kantarcioglu and Gel

The latest version can be downloaded from:
`https://cakcora.github.io/book`

Contents

Preface

The famous author Douglas Adams remarked that technologies invented between the ages of fifteen and thirty-five are exciting and revolutionary, and that you can probably build a career in them. He also added that anything in the world when you are born is normal and ordinary, and is just a natural part of the way the world works. We first started studying blockchain in our thirties, and we found it new and exciting. Meanwhile, Bitcoin and its underlying technology, blockchain, have continued to gain popularity across a range of applications, from finance and insurance to clinical trials. A decade later, we now teach it to the youth with the solemn conviction that it's part of the natural order of things, and everyone should know the basics of blockchain.

Originally designed to facilitate a secure distributed platform without central authorities, blockchain was heralded as a paradigm that would be as powerful as Big Data, Cloud Computing, and Machine Learning. Expectations around blockchain have ebbed and flowed, but its importance can not be belittled. Daily blockchain trading volumes have surged past 120 billion USD [113], making blockchain a major financial avenue.

Blockchain brought together ideas from various fields, such as public key encryption and distributed systems. As such, early readers often studied resources that explained blockchain technology from only a narrow perspective, leaving them with more questions than clarity.

In this book, we offer a holistic view of blockchain. Table 0.1 gives a compact tour of the blockchain landscape, where coins and platforms differ in structure, purpose, and ideology. Starting with a brief historical overview, we discuss the building blocks of blockchain and systematically explain their interactions. We also devote a section to the next generation of blockchain and explain such extensions as Decentralized Autonomous Organizations. As graph mining plays an important role in blockchain, we elaborate on how graph theoretical aspects can be used in blockchain technology and data analytics.

	Data Structure			Functionality		System Properties		
	UTXO	Account	DAG	Platform	Cryptocurrency	Privacy-enabled	Permissioned	Public
Bitcoin	✓				✓			✓
Litecoin	✓				✓			✓
ZCash	✓				✓	✓		✓
Dash	✓				✓	✓		✓
Monero	✓				✓	✓		✓
Ripple		✓			✓		✓	
Ethereum		✓		✓	✓			✓
IOTA			✓	✓	✓		semi	✓

Table 0.1 *Blockchain systems grouped by data structure, functionality, and system properties. Privacy-enabled indicates support for optional or default privacy features. Permissioned means validator participation is restricted, as in Ripple. Ethereum is permissionless, as any node can stake 32 ETH and become a validator. "semi" denotes transitional or partially centralized designs.*

We adopt a chronological approach to teaching technology, where chapters follow the historical progression of developments rather than their technical complexity. For example, in the context of scalability, we first introduce layer one advancements, such as Proof of Stake, before moving to earlier solutions like segregated witness (a layer zero solution). This mirrors the actual sequence of events in the field, as people did not first develop layer zero solutions and then progress to higher layers. By teaching in this order, we offer students a clearer understanding of how the field has evolved and where it is headed, allowing them to contextualize current and future innovations.

Blockchains involve multiple disciplines, such as graph theory, finance, and game theory. To fully grasp blockchain, it must be considered as a concept that interacts with the world. In this sense, we follow the Annales School methodology [81], examining not only the technology itself but also the broader ecosystem in which it operates. By taking this comprehensive, world-context view, we aim to provide students with a deeper understanding of blockchain's development and its wide-reaching impact.

Without assuming any prior reader's expertise, we aim to provide a concise but complete description of blockchain technology and its capabilities.

Roadmap for This Book

Figure 0.1 shows an example reading order for the book. Chapters 1 to 2 introduce the origins of digital money and Bitcoin. Readers seeking a foundational understanding of money, financial systems, and the motivations behind Bitcoin

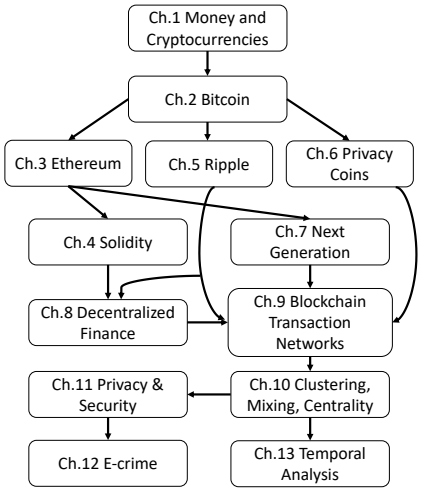

Figure 0.1 Suggested reading flow through the chapters. Arrows indicate conceptual or technical dependencies.

should begin here. Chapter 3 teaches Ethereum as a programmable blockchain, detailing accounts, gas mechanics, and data structures. Chapter 4 focuses on Solidity and smart contract development. It assumes familiarity with Ethereum concepts, so readers without coding experience might wish to skim rather than study it deeply at first. Chapter 5 explains Ripple and its architecture as a bridge currency and trust-based ledger. Chapter 6 teaches Dash, Monero, and Zcash privacy coins. Chapter 7 expands into next-generation technologies such as alternative consensus mechanisms, scalability, and blockchain interoperability. It provides valuable foresight for students focused on research or system-level design. Chapter 8 introduces Decentralized Finance, including tokens, exchanges, lending protocols, and DAOs. This section is best read after mastering Ethereum. Chapters 9 takes a graph-theoretical approach, describing the blockchain as transaction networks. Chapter 10 shows how addresses can be clustered, how important nodes can be discovered and how address influence can be measured. Readers interested in analytics, data science, or network theory will find Chapters 9 and 10 particularly useful. Chapters 11 and 12 focus on privacy and security and the use of blockchains in e-crime. These are especially relevant for students in cybersecurity or digital forensics. Chapter 13 introduces temporal analysis, useful for advanced blockchain research and time-aware systems.

Each chapter concludes with questions to prompt reflection and enable self-assessment.

The book is designed to stand as both a course textbook and a reference work. Whether used in a university classroom or for independent study, its structure encourages a layered, cumulative understanding of blockchain technologies.

1

Money and Cryptocurrencies

his chapter traces the intellectual and technological lineage of Bitcoin and digital money. While Nakamoto's white paper launched Bitcoin, its roots extend through decades of economic theory, cryptographic innovation, and activist movements. We examine how the Austrian and Chicago Schools of Economics provided a framework for stateless and non-inflationary money, and how Cypherpunk ideals shaped the push for privacy and decentralization. The chapter reviews early experiments with digital currencies such as DigiCash, b-money, and e-gold, highlighting the technical shortcomings, regulatory battles, and user adoption barriers that prevented their success but furnished essential building blocks for Bitcoin. We then contrast the classical financial attributes of money—medium of exchange, unit of account, and store of value—with additional digital requirements such as offline spendability, identity-less spendability, and fungibility. Finally, we show how Bitcoin resolved the long-standing double-spending problem without a central authority through proof-of-work, situating it as both a culmination of earlier efforts and the starting point for a new era of cryptocurrencies.

Although Nakamoto's paper marked the launch of Bitcoin, the system's intellectual roots lie in a wider lineage. Earlier work on blinded signatures by David Chaum, the structure and vulnerabilities of centralized digital gold projects like e-gold, and the ideological foundations laid by the Cypherpunks all contributed essential ingredients. Moreover, regulatory responses after 9/11 and ongoing battles over anonymity and control further shaped the environment in which Bitcoin emerged. It is more accurate to view Bitcoin as a culmination of technical lessons and philosophical motivations stretching across decades, rather than a sudden and solitary invention.