

Bitcoin, Blockchain, and Cryptoassets

A Comprehensive Introduction

Fabian Schär and Aleksander Berentsen

**The MIT Press
Cambridge, Massachusetts
London, England**

Contents

Preface vii

I Introduction

1 The Context of Monetary Theory 3

- 1.1 Origin of a Monetary Unit 5
- 1.2 Functions of a Monetary Unit 5
- 1.3 Fundamental Properties of Money 8
- 1.4 Monetary Value 9
- 1.5 Monetary Control Structures 13
- 1.6 Exercises 28

2 Bitcoin Overview 31

- 2.1 Classification of Bitcoin 31
- 2.2 Bitcoin Components: An Overview 33
- 2.3 Bitcoin's Unique Selling Proposition 34
- 2.4 Bitcoin's Technology: A Primer 36
- 2.5 Origin and Governance 46
- 2.6 Exercises 65

II Technical Analysis

3 Transactional Capacity 69

- 3.1 Bitcoin Network 69
- 3.2 Extended Network 75
- 3.3 Bitcoin Communication Protocol 78
- 3.4 Exercises 81

4	Transactional Legitimacy	83
4.1	Pseudonyms	83
4.2	Hash Functions	98
4.3	Signatures	100
4.4	Transactions	117
4.5	Script Conditions	122
4.6	Signature Hash Type	129
4.7	Segregated Witness (SegWit)	130
4.8	Exercises	138
5	Transactional Consensus	139
5.1	Blocks and the Blockchain	139
5.2	Consensus Protocol	146
5.3	Bitcoin Mining: Incentives and Examples	155
5.4	Exercises	170
III	Further Remarks	
6	Bitcoin's Challenges	175
6.1	Price Volatility	175
6.2	Scalability	194
6.3	Adoption	209
6.4	Political Challenges	218
6.5	Exercises	222
7	Further Applications	223
7.1	Decentralized Verification and Attestation	223
7.2	Tokens and Colored Coins	225
7.3	Smart Property	226
7.4	Blockchain Contracts (Smart Contracts)	228
7.5	Exercises	233
8	Practical Guidelines for Bitcoin	235
8.1	Procurement	235
8.2	Storage	240
8.3	Payments	246
8.4	Exercises	250

References	251
------------	-----

Index	269
-------	-----