

Table of Contents

Editors	v
Contributors	vii
Foreword	
<i>Sandra Ro</i>	xxix
Preface	xxxi
List of Abbreviations	xxxiii
CHAPTER 1	
Understanding Blockchain	
<i>Jake van der Laan</i>	1
§1.01	Introduction 1
§1.02	Core Concepts 2
[A]	Record-Keeping 2
[B]	How Computers Encode Data 3
[C]	How Computers Store Large Numbers 4
[D]	Computer Programming 6
[1]	Variables 6
[2]	Control Structures 7
[3]	Data Structures 8
[a]	The Array 9
[b]	The Linked List 9
[4]	Syntax 10
[5]	From Program Code to Machine Code 10
§1.03	The Mathematics of Blockchain 11
[A]	The Hash Function 11
[B]	The Cryptographic Hash Function 13
[1]	The ‘Always the Same’ Property 13

Table of Contents

	[2] The 'Digital Signature' Property	13
	[3] The 'No Reverse Engineering' Property	14
	[C] The Hash List	15
	[D] The Merkle Tree	16
	[E] Public-Private Key Encryption	17
§1.04	Database Concepts	20
	[A] Database Operations	22
	[B] A Transaction Log Distinguished from a Database	22
	[C] Database Transactions: The ACID Properties	23
§1.05	Networking Fundamentals	24
	[A] P2P Networks	24
§1.06	Core Blockchain Functionality	25
	[A] Tying Blocks Together to Prevent Tampering	26
	[B] Adding a Time Cost	27
	[1] The Nonce	28
	[2] The Probabilities of Generating a Particular Hash Value	28
	[a]. Randomness	28
	[b] Sample Space	28
	[3] Not Replacing Generated Events	29
	[4] A Cryptographic Hash Function Behaves Like a Random Variable	30
	[5] Requiring a Hash Value Below a Certain Value	31
	[C] The Proof of Work Process	31
§1.07	Transactions on the Bitcoin Blockchain	32
	[A] Bitcoin Scripting	33
	[B] Entitlement Tracking	33
	[C] The UTXO Database	34
§1.08	The Distributed Blockchain	34
	[A] The Bitcoin Network	34
	[B] The Memory Pool	36
	[C] Adding a Mined Block	36
	[D] The Double Spending Problem	37
	[E] The Mining Reward	38
	[F] Mining Pools	38
	[G] The 51% Attack	39
§1.09	Blockchain Forks	40
	[A] The Soft Fork	40
	[B] The Hard Fork	40
§1.10	Blockchain as a Platform	41
	[A] Ethereum	41
	[1] Gas: Limiting How Long a Program Can Run	42
	[2] An Ethereum Transaction	43
	[3] Ethereum Transaction Account Types	44
	[a] The EOA	44
	[b] The Contract Account	44

	[4] The Ethereum Virtual Machine	44
§1.11	Smart Contracts	45
	[A] Programming Smart Contracts	46
	[B] Oracles	46
	[C] Decentralized Applications	47
§1.12	Tokens on the Blockchain	48
	[A] The ERC-20 Token Standard	48
	[B] Crowdfunding on the Blockchain	49
	[1] Initial Coin Offerings	49
	[2] Token Generation Events	50
	[3] Initial Exchange Offerings	51
	[4] Security Token Offerings	51
	[5] A Note on Token Fungibility	51
§1.13	Bitcoin and Ethereum Governance	52
	[A] The Bitcoin Governance Process	52
	[1] Bitcoin Improvement Proposals	53
	[2] Segwit	54
	[B] Ethereum Governance	55
	[C] Off-Chain and On-Chain Governances	55
§1.14	Moving Beyond Ethereum	55
	[A] Public (Permissionless) Blockchains	56
	[B] Private (Permissioned) Blockchains	56
	[C] Distributed Ledger Technologies	56
§1.15	Distributed System Consensus Theory	57
	[A] Synchronous Versus Asynchronous Processes	57
	[B] The FLP Impossibility Result	57
	[C] Consensus Mechanism Properties	58
	[1] The CAP Theorem	58
§1.16	Other DLT and Consensus Approaches	59
	[A] Byzantine Fault Tolerance (BFT)-Based Networks	59
	[1] Ripple	60
	[2] Stellar	62
	[B] Proof of Stake-Based Networks	62
	[1] Peercoin	62
	[C] Delegated Proof of Stake-Based Networks	63
	[1] BitShares	64
	[D] Directed Acyclic Graph-Based Networks	64
	[1] Graph Basics	64
	[2] Using a DAG as a Ledger	65
	[3] IOTA	66
§1.17	Enterprise Blockchain Platforms	67
	[A] Hyperledger	67
	[1] Fabric	68
	[2] Sawtooth	68
	[3] Proof of Elapsed Time Consensus	68

Table of Contents

	[4] Transaction Families	70
§1.18	Scaling the Blockchain	70
	[A] Sharding	70
	[B] Sidechains	71
	[1] The Lightning Network	72
	[C] Multilayer Blockchains	74
§1.19	Blockchain as a Service	75
	Further Reading	75
CHAPTER 2		
Blockchain and Information Security		
	<i>Dave Hirsch</i>	77
§2.01	Risks and Vulnerabilities	78
	[A] Private Keys: A Single Point of Failure	81
	[1] Lost Private Keys Typically Means a Total Loss of Bitcoins Held at the Associated Public Key Address	81
	[a] Legal Implications of Lost Private Keys	83
	[b] Policy Considerations	84
	[2] Death: Risks Associated with Digital Asset Inheritance	85
	[a] Legal Implications of Dying Without a Plan to Transfer Private Keys	86
	[b] Policy Implications	86
	[3] Stolen Keys: Beware of Hacking, Malware, and Man-in-the-Middle Attacks	86
	[a] Legal Implications	89
	[b] Policy Considerations	90
	[4] Compromised Keys: Digital Assets Are Only as Secure as the Keys That Control Them	90
	[a] Legal Implications	92
	[b] Policy Implications	92
	[5] Kidnapping Seeking Digital Assets: The Intersection of Physical and Information Security	93
	[a] Legal Implications of Kidnapping for Ransom	96
	[b] Policy Implications	97
	[6] SIM Swapping: Exploiting Vulnerabilities in Digital Identities	98
	[a] Legal Implications of SIM Swaps	102
	[b] Policy Implications	103
	[B] Digital Asset Exchanges and Third-Party Services: Different Roles, Different Risks	103
	[1] Digital Asset Exchanges: Hacks Happen	104
	[a] Legal Implications	106
	[b] Policy Implications	107
	[2] Reliance on Third Parties: Exit Scams Happen	108
	[a] Legal Implications	110

	[b] Policy Implications	111
	[3] Third-Party Exploits: Trust Misplaced	112
	[a] Legal Implications	115
	[b] Policy Implications	116
§2.02	Tools and Methods to Address Risks	118
	[A] Individual Options for Protecting Digital Assets	118
	[1] Paper Wallets	118
	[2] Hardware Wallets	119
	[3] Multi-sig Wallets	120
	[B] Outsourcing Security: Custodians	120
	Further Reading	120
CHAPTER 3		
Blockchain Regulation		
	<i>Thomas Richter</i>	123
§3.01	Defining Blockchain for Regulation Purposes	123
	[A] Background: The ‘Legal Factor’	123
	[B] The Meaning of ‘Blockchain’ in the Context of Regulation	125
	[1] The Relevance of a Legal Definition	125
	[2] Various Organizational Forms of Blockchains	126
	[3] Legal Relevance of the Blockchain Protocol	129
	[4] Inherent Characteristics of Blockchains and Their Legal Implications	131
	[5] Summary	132
	[C] The Meaning of ‘Regulation’ in the Context of Blockchain	133
	[1] Which Kind of Regulation Can Be Relevant for Blockchains?	133
	[2] Which Legal Subjects Can Be Relevant for Blockchains?	135
	[3] ‘Code Is Law’ and ‘Code As Law’	136
	[4] Summary	138
§3.02	Regulatory Challenges	139
	[A] Decentralization as Key Challenge	139
	[B] Jurisdiction	139
	[C] Anonymity	140
§3.03	Regulatory Concepts	141
	[A] The Regulatory Principle of Technology Neutrality	142
	[B] Regulating the Use Case Versus Regulating the Technology	144
	[C] Regulatory Sandboxing	145
§3.04	Regulatory Actors	146
	[A] Governments and Law Makers	146
	[B] Regulatory Authorities and Enforcement Agencies	147
	[C] Courts	147
	[D] International and European Bodies and National Banks	148
§3.05	Addressees of Regulation	149
	[A] Addressing ‘the Blockchain’ as Subject of Regulation	149

Table of Contents

	[1] Legal Personality of the Blockchain	149
	[2] The Malta Innovative Technology Arrangements and Services Act 2018	150
	[3] Decentralized Autonomous Organizations as a New Corporate Form	150
	[4] Summary	152
[B]	Addressing Blockchain Actors as Subjects of Regulation	152
	[1] Validation Nodes ('Nodes')	152
	[2] Mining Nodes ('Miners')	154
	[3] Blockchain Users	154
	[4] Coders	155
§3.06	Examples of Specific Blockchain Regulation	155
	[A] United States	155
	[B] Outside of the US	159
	[C] Definition and Summary	160
§3.07	Outlook: Financial Services Prudential Regulation	160
§3.08	Summary	161
	Further Reading	161
CHAPTER 4		
Blockchain and Smart Contracts		
<i>Philip Trillmich, Matthias Goetz & Chris Ewing</i>		163
§4.01	Terminology and Characteristics: What Is a Smart Contract?	163
	[A] History of the Term 'Smart Contract'	163
	[B] Technical Characteristics of a 'Smart Contract'	164
	[C] Terminology	165
	[1] The Meaning of the Term 'Smart' in Smart Contract	165
	[2] What Does the Term 'Contract' Mean in Smart Contract?	165
	[3] The Attempt to Develop a Definition	166
	[D] Characteristics of 'Smart Contracts' as an Application of a Blockchain	167
§4.02	Fields of Application	169
	[A] Legal Profession	169
	[B] Insurance Industry	170
	[C] Music Industry/Media industry	171
	[D] Energy Supply Industry	173
	[E] Internet of Things	174
	[F] Sharing Economy	175
§4.03	Contract Law Issues	176
	[A] Applicable Law Versus 'Code in Law'	176
	[B] Formation of a Smart Contract	177
	[1] Contracting Parties	177
	[2] Form Requirements	178
	[3] Offer and Acceptance	181
	[C] Regulatory Issues and Smart Contracts	182

	[D] Consumer-Protection Laws and Smart Contracts	182
	[1] EU Directive 2011/83/EU	182
	[2] Unfair Standard Terms	183
	[E] Interpretation of Smart Contracts and Their Terms	184
	[F] Performance and Remedies	186
§4.04	Outlook	188
	[A] Benefits, Opportunities and Limitations of Smart Contracts	188
	[B] Use of Smart Contracts in the Future	191
	Further Reading	192
CHAPTER 5		
Blockchain and Data Privacy		
	<i>Matthias Artzt, Lothar Determann & William Long</i>	193
§5.01	Introduction and Executive Summary	193
§5.02	Personal Data in the Context of the GDPR	194
	[A] Definition of Personal Data in the Context of a Blockchain	194
	[1] Public Keys	195
	[2] Transactional Data	197
	[B] How Is Personal Data Processed on a Blockchain?	198
	[C] Application of the GDPR to the Blockchain	199
§5.03	Identifying Controllers and Processors in a Blockchain Environment under the GDPR	201
	[A] Definition of Controller and Processor	201
	[B] Legal Status of Participants of a Blockchain Network	201
	[1] Static Number of Roles and Responsibilities	201
	[2] Miners	203
	[3] Nodes	205
	[4] Wallets	206
	[5] Users of a Blockchain	206
	[6] Developer of Smart Contracts	208
	[7] Oracles	209
	[8] Governance Bodies and Joint-/Co-controllership	210
	[C] Frictions Between Controllership and Obligations under the GDPR	211
§5.04	Legal Basis and Consent under the GDPR	212
	[A] Contractual Necessity	214
	[B] Consent	214
	[C] Legitimate Interest	216
	[D] Compliance with a Legal Obligation	217
	[E] Special Categories of Personal Data	218
§5.05	Security of Data Processing on a Blockchain in the Context of the GDPR	218
	[A] Personal Data Versus Anonymous Data	218
	[B] Particular Security Techniques	218
	[1] Encryption	219

Table of Contents

	[2] Hashing	219
	[3] Multi-layered Blockchains	220
	[4] Storing Personal Data Off-Chain	220
[C]	Principles of Purpose Limitation and Data Minimization	221
	[1] Purpose Limitation	221
	[2] Data Minimization	223
	[3] Evaluation in the Light of the Principles of Purpose Limitation and Data Minimization: Multi-layered Blockchains Versus Off-Chain Storage	223
[D]	Recommendation for Security Measures in a Blockchain Environment	225
[E]	Implications in the Case of Security Breaches	225
\$5.06	Data Subject Rights under the GDPR	226
	[A] How Do Data Subject Rights Apply to the Blockchain?	226
	[B] Right to Access Personal Data	227
	[C] Right to Rectification	228
	[D] Right to Erasure	229
	[1] What Does Erasure Mean?	229
	[2] The Techniques to Erase Data	230
	[3] Public Keys/Identifiers of Blockchain Users	232
\$5.07	Accountability Principles under the GDPR	233
	[A] Lawfulness, Fairness and Transparency	234
	[B] Purpose Limitation, Data Minimization and Storage Limitation	235
	[C] Use of Data Privacy Impact Assessment	236
	[D] Data Protection by Design and Default	237
	[E] Record of Processing Activities	240
	[F] Appointment of a DPO	240
\$5.08	International Data Transfers on a Blockchain under the GDPR	241
\$5.09	Outlook	243
\$5.10	Blockchain and US Privacy Law	243
	[A] US Privacy Law Versus EU Data Protection Regulation	244
	[B] Federal and State Law	249
	[C] Diverse Terminology	249
	[D] General and Specific US Privacy Laws applied to Blockchain	250
	[1] General US Privacy Laws	250
	[2] Specific US Privacy Laws	252
	[E] Blockchain and CCPA	255
	[1] Scope of CCPA	256
	[2] Which Blockchain Participants Must Comply with CCPA?	257
	[3] CCPA Compliance Obligations	258
	[4] Data Access and Deletion Rights	261
	[5] Sanctions and Remedies	262
	Further Reading	264

CHAPTER 6

Capital Markets

<i>Michael Juenemann</i>	265
§6.01 Capital Markets and Blockchain	
<i>Michael Juenemann</i>	265
[A] What Makes a Token a Security?	265
[B] Blockchain Finality	268
[C] Special Requirements for Prospectuses	271
[D] Regulatory Specifics for Organized Trade	273
§6.02 Capital Markets and Blockchain: Country Report – Austria	
<i>Johannes Frank & Philipp Kinsky</i>	275
[A] What Makes a Token a Security?	276
[B] Blockchain Finality	277
[C] Special Requirements for Prospectuses	278
[D] Regulatory Specifics for Organized Trade	278
§6.03 Capital Markets and Blockchain: Country Report – Belarus	
<i>Klim Stashevsky & Mikhail Khodosevich</i>	280
[A] What Makes a Token a Security?	280
[B] Blockchain Finality	281
[C] Special Requirements for Prospectus	282
[D] Regulatory Specifics for Organized Trade	284
§6.04 Capital Markets and Blockchain: Country Report – Estonia	
<i>Kirsti Pent</i>	286
[A] What Makes a Token a Security?	286
[B] Blockchain Finality	290
[C] Special Requirements for Prospectus	291
[D] Regulatory Specifics for Organized Trade	292
§6.05 Capital Markets and Blockchain: Country Report – Finland	
<i>Mika Puurunen</i>	293
[A] What Makes a Token a Security?	294
[B] Blockchain Finality	296
[C] Special Requirements for Prospectus	297
[D] Regulatory Specifics for Organized Trade	299
[E] Conclusion	300
§6.06 Capital Markets and Blockchain: Country Report – France	
<i>Bertrand Levy</i>	300
[A] What Makes a Token a Security?	300
[B] Blockchain Finality	301
[C] Special Requirements for Prospectus	303
[D] Regulatory Specifics for Organized Trade	305
§6.07 Capital Markets and Blockchain: Country Report – Germany	
<i>Michael Juenemann</i>	306
[A] What Makes a Token a Security?	306
[B] Blockchain Finality	308
[C] Special Requirements for Prospectus	310

Table of Contents

	[D] Regulatory Specifics for Organized Trade	312
§6.08	Capital Markets and Blockchain: Country Report – Italy	
	<i>Stefano Febbi</i>	314
	[A] What Makes a Token a Security?	314
	[B] Blockchain Finality	316
	[C] Special Requirements for Prospectuses	316
	[D] Regulatory Specifics for Organized Trade	318
§6.09	Capital Markets and Blockchain: Country Report – Liechtenstein	
	<i>Johannes Dür</i>	321
	[A] What Makes a Token a Security?	323
	[B] Special Requirements for a Prospectus	324
	[C] Blockchain Finality	325
	[D] Regulatory Specifics for Organized Trade	328
§6.10	Capital Markets and Blockchain: Country Report – Poland	
	<i>Aleksandra Widziewicz</i>	329
	[A] What Makes a Token a Security?	329
	[B] Blockchain Finality	331
	[C] Special Requirements for Prospectus	332
	[D] Regulatory Specifics for Organized Trade	332
§6.11	Capital Markets and Blockchain: Country Report – Spain	
	<i>Jose Luis Lorente Howell</i>	334
	[A] What Makes a Token a Security?	334
	[B] Blockchain Finality	337
	[C] Special Requirements for Prospectus	337
	[D] Special Requirements for Organized Trade	338
§6.12	Capital Markets and Blockchain: Country Report – Switzerland	
	<i>Olivier Favre & Fabio Elsener</i>	340
	[A] What Makes a Token a Security?	341
	[B] Blockchain Finality	342
	[1] Payment Tokens and Utility Tokens Without Claims	342
	[2] Asset Tokens and Utility Tokens Conferring Claims	342
	[3] Developments: DLT Rights	343
	[C] Regulatory Specifics for Organized Trade	344
	[1] Payment Tokens and Utility Tokens	344
	[2] Asset Tokens	345
	[3] Developments: Introduction of DLT Trading Facility	346
§6.13	Capital Markets and Blockchain: Country Report – Singapore	
	<i>Kim Kit Ow</i>	347
	[A] What Makes a Token a Security?	347
	[B] Blockchain Finality	348
	[C] Special Requirements for Prospectus	350
	[D] Regulatory Specifics for Organized Trade	352
	[E] Conclusion	353
§6.14	Capital Markets and Blockchain: Country Report – Canada	
	<i>Daniel Fuke & Mike Stephens</i>	353

[A]	What Makes a Token a Security	354
[B]	Crypto Winter	356
[C]	Special Requirements for Prospectus	357
[D]	Regulatory Specifics for Organized Trade	358
[1]	Registration Request and Oversight	358
[2]	Regulatory Gaps	358
[3]	Enforcement	358
[E]	Conclusion	360
§6.15	Capital Markets and Blockchain: Country Report – USA	
<i>James Gatto</i>		360
[A]	What Makes a Token a Security?	360
[1]	US SEC	361
[2]	The Commodities Futures Trading Commission	362
[3]	The Financial Crimes Enforcement Network	363
[4]	FINRA	365
[5]	The IRS	365
[6]	State Laws	365
Further Reading		366
CHAPTER 7		
Blockchain and Intellectual Property		
<i>Andreas Holzwarth-Rochford</i>		369
§7.01	Introduction	369
§7.02	Trademark	371
[A]	Definition	371
[B]	Duration	371
[C]	Territory	371
[D]	Goods and Services	372
[E]	Types of Trademarks	372
[F]	Registration Process	373
[G]	Post Registration	374
[H]	Enforcement	374
[I]	Examples and Practical Hints	375
§7.03	Designs	376
[A]	Definition	376
[B]	Duration/Territory	376
[C]	Registration/Invalidity Procedures/Protection Requirements	378
[D]	Enforcement	379
[E]	Examples and Practical Hints	380
§7.04	Copyright	381
[A]	Definition	381
[B]	Rights Given by Copyright, Duration and Practical Hints	381
§7.05	Open Source	382
§7.06	Patents/Utility Models	385
[A]	Definition/Content of Patent Application	385

Table of Contents

[B]	Rights Provided by a Patent	385
[C]	Territory	386
[1]	European Patents/Planned European Unitary Patent	387
[2]	Further Regional Patents European Patents/Planned European Unitary Patent	389
[D]	Protection Requirements EPO	389
[1]	Novelty/Grace Period	389
[2]	Priority	390
[3]	International Patent Applications	391
[4]	Exclusion from Patentability	392
[5]	Assessing Patentability of CII: Examples of Blockchain-Related EP Patents	393
[6]	Opposition Procedure	396
[7]	Enablement	397
[E]	Protection Requirements USPTO: Examples of Blockchain-Related US Patents	398
[F]	Practical Hints Protection by Patents	401
[1]	Strategic Considerations	401
[2]	Observation/Surveillance of Third-Party Rights	401
[3]	Transfer of Rights	402
[a]	German Act on Employee Inventions	403
[G]	Utility Models	404
[1]	Background	404
[2]	Registration Procedure: Branching Off	405
[3]	Protection Requirements/Duration	406
[4]	Protectable Subject Matter	407
[5]	Summary of Pros and Cons of Utility Models	407
§7.07	Trade Secret	408
[A]	General Background	408
[B]	Legal Basis: Definition	409
[C]	Practical Aspects	410
	Further Reading	413
CHAPTER 8		
Blockchain and Antitrust		
	<i>Jay Modrall</i>	415
§8.01	Introduction	415
§8.02	Anticompetitive Agreements, Decisions and Concerted Practices	416
[A]	Introduction to Concepts	416
[B]	Horizontal Agreements and Blockchain	418
[1]	Information Exchange	419
[2]	Standardization	421
[C]	Vertical Agreements and Blockchain	422
[D]	Appropriate Safeguards	424
§8.03	Abuse of Dominance	424

[A]	Introduction of Concepts	424
[B]	Big Data	426
	[1] Mandating Data Access	427
	[2] Policing Data Sharing and Pooling	429
[C]	Online Platforms	430
	[1] Most Favoured Nations	431
	[2] Multi-homing	431
	[3] Interoperability	431
	[4] Transparency	432
	[5] Leveraging	432
	[6] Self-Preferencing	432
[D]	Article 102 TFEU and Blockchain	432
[E]	Appropriate Safeguards	433
§8.04	Merger Control	434
	[A] Introduction to Concepts	434
	[B] Full-Function Joint Ventures	435
	[C] Gun-Jumping	436
	[D] Merger Control and Blockchain	437
	[E] Appropriate Safeguards	442
	Further Reading	443
	Bibliography	445
	Electronic References	465
	Table of Cases	475
	Index	479