

Contents

Preface — V

Acknowledgments — VII

1 Basic of cryptographic payments — 1

- 1.1 Preliminaries on cryptographic signatures — 1
 - 1.1.1 Binary and hexadecimal — 1
 - 1.1.2 Hashing function — 2
 - 1.1.3 Cryptographic signatures — 4
 - 1.1.4 Takeaway — 6
- 1.2 Blockchain protocols — 7
 - 1.2.1 Consensus — 7
 - 1.2.2 Proof of work — 9
 - 1.2.3 Block difficulty adjustment — 12
 - 1.2.4 Longest-chain/heaviest-chain rule — 12
 - 1.2.5 Halving — 13
 - 1.2.6 Blocksize — 14
 - 1.2.7 Why is it called “proof of work”? — 15
 - 1.2.8 Rise of ASICs — 15
 - 1.2.9 Layer 2 networks — 16
 - 1.2.10 Cursory analysis — 16
 - 1.2.11 Proof of stake — 17
 - 1.2.12 Nodes and miners — 18
 - 1.2.13 Soft forks and hard forks — 18
- 1.3 What is Bitcoin and why does it work? — 19
- 1.4 More on mining — 20
 - 1.4.1 UTXO — 21
 - 1.4.2 Common assumptions in mining games — 23

2 Probability spaces — 25

- 2.1 Countably and uncountably infinite — 26
- 2.2 Partitions — 27
 - 2.2.1 Conditional probability — 28
- 2.3 Random variables — 29
 - 2.3.1 Expectation — 29
 - 2.3.2 Conditional expectation — 31
- 2.4 Bernoulli processes and Bernoulli schemes — 32
 - 2.4.1 The binomial distribution formula and the De Moivre–Laplace theorem — 35
 - 2.4.2 Probability-preserving isomorphisms and comparison of expectations — 37

2.5	Win-Lose-Pay game —	39
2.6	Probability distribution functions —	41
2.6.1	Jensen's inequality —	41
2.7	Poisson processes —	42
2.7.1	Naturally occurring chain splits —	44
3	Game theory basics —	46
3.1	Single-round games —	46
3.1.1	Payoff tables —	47
3.1.2	Preferences and utility function —	47
3.1.3	Matrix games —	49
3.1.4	N-player games and more terminology —	50
3.1.5	Dominant strategies —	51
3.1.6	Examples —	52
3.1.7	Nash equilibria —	53
3.1.8	Examples —	53
3.1.9	Determining Nash equilibria by looking at a table —	54
3.2	Mixed strategies —	55
3.2.1	Mixed strategies in real life —	55
3.3	Extensive-form games —	56
3.3.1	State of a game —	56
3.3.2	Game trees —	58
3.4	Schelling points —	60
4	Monopolizing pool —	62
4.1	Rough approach: Bernoulli's law of large numbers and Hoeffding's bound —	62
4.2	Binomial distribution and the De Moivre-Laplace theorem —	66
5	Basic double-spend game —	69
5.1	Simplest strategy: Charlie elects to mine his own chain when less than k blocks behind —	71
5.1.1	Recursion formulas —	71
5.1.2	A method for computing winning probability —	72
5.1.3	Another method: difference equations —	74
5.1.4	Computing expected values —	77
5.2	Longer-duration attacks —	83
5.3	Stealth six-block double-spend —	85
5.3.1	Negative binomial distribution —	86
6	Censorship attacks —	90
6.1	Working example: two rational pools —	91

- 6.1.1 Consideration for this choice of function — **94**
- 6.1.2 There are many strategies — **94**
- 6.1.3 Case 1: Pool 1 and Pool 2 are both non-compliant — **95**
- 6.1.4 Case 2: Pool 1 is non-compliant and Pool 2 is mildly compliant — **99**
- 6.1.5 Case 3: both pools are mildly compliant — **106**
- 6.1.6 Analysis: low-fee regime — **107**
- 6.1.7 Higher-fee regime — **110**
- 6.1.8 Conclusion — **111**

7 Economics of mining — 112

- 7.1 Hashing as a market — **112**
 - 7.1.1 Cournot oligopoly model — **112**
 - 7.1.2 A model for the mining market — **114**
 - 7.1.3 Linear cost model — **114**
 - 7.1.4 Monopolist pricing and collusion — **116**
 - 7.1.5 Perfectly competitive markets — **117**
 - 7.1.6 Nash equilibrium in the mining market — **118**
- 7.2 Market for ASICs — **120**
 - 7.2.1 Nash equilibrium with Bertrand assumptions — **120**
 - 7.2.2 Four regimes — **121**

8 Selfish mining — 123

- 8.1 Exploiting the difficulty adjustment — **124**
- 8.2 Basic selfish mining — **125**
- 8.3 Market distortions — **130**
- 8.4 Markov chains — **130**
- 8.5 Selfish mining analyzed via a Markov process with cuts — **133**
- 8.6 Selfish mining with partial cooperation — **135**
- 8.7 Defense against selfish mining — **137**

9 Strategic mining — 138

- 9.1 Petty compliant strategy and fee-undercutting — **139**
 - 9.1.1 Fee-undercutting — **139**
 - 9.1.2 Fee-sniping vs. fee-undercutting — **141**
 - 9.1.3 Emergence of petty compliant miners — **141**
 - 9.1.4 Selfish mining as incentive to use petty compliant mining — **142**
 - 9.1.5 Measures against undercutting — **143**
- 9.2 Other deviant mining strategies — **143**
 - 9.2.1 Accepting bribes — **143**
 - 9.2.2 Block withholding — **150**
 - 9.2.3 Protecting one's own interests — **151**
 - 9.2.4 Mine from behind — **151**

9.2.5	Extended example —	152
9.2.6	Deferring to the alpha dog —	156
9.2.7	Responding to exogenous demand for hashrate —	159
9.2.8	Harmonic mining/switch mining —	160
9.2.9	Merge-mining, layer 2, sidechains, and strategies playing out on other blockchains —	162
9.3	Will there be a transition from default compliant to a fully strategic regime? —	163
9.3.1	Block optimization and transaction selection —	164
9.3.2	Overpaying pools —	165
9.3.3	Direct signaling and optimizer training —	165
9.3.4	Purge pooling —	166
9.3.5	Precedent: MEV in Ethereum —	167
10	What discourages strategic mining? —	169
10.1	Market fragility hypothesis —	169
10.2	Repeated games and institutional norms —	169
10.2.1	Mining that can be punished —	172
10.2.2	Problems with punishment —	172
11	Declining block subsidy —	174
11.1	Security budget —	175
11.2	The mining gap —	177
11.3	Problems with a mining gap —	179
11.4	Undercutting —	180
11.4.1	Private transaction brokering —	181
11.5	Summary —	183
12	The Flattening ASIC cost curve —	184
12.1	Hash deployment ratio —	184
12.2	Purge pools —	185
12.2.1	Protection against a purge attack when HDR is low —	186
12.3	The dynamical system determined by the difficulty adjustment —	186
12.3.1	Phase transition to Galloping Gertie —	194
12.4	Financialization of hashrate markets —	196
13	Attacks —	198
13.1	Why have there been no attacks yet? —	198
13.2	Nation-state/authoritarian attacks —	199
13.2.1	The empty-block attack —	200
13.2.2	Obvious criticism of the empty-block attack —	200
13.2.3	Layer 2s under an empty-block attack —	202

- 13.2.4 The seesaw attack — 202
- 13.2.5 Bribe-flooding attack — 202
- 13.2.6 Empty-block purge attack — 203
- 13.3 Checkpointing against a persistent 51 % attack — 203
- 13.4 Buyout attacks — 206
- 13.5 Nuclear option: new proof-of-work algorithm — 207
- 13.6 Less-than-brute-force attacks — 208
- 13.6.1 Nudging towards a strategic regime — 208
- 13.6.2 FUD and social attacks — 209
- 13.6.3 Regulations — 210
- 13.7 Goldfinger attacks — 211
- 13.7.1 Slippery-slope attacks — 212
- 13.7.2 Selfish mining as a slippery-slope attack — 213
- 13.7.3 Low-probability attacks — 214
- 13.8 Soft-forkability: can the community suspend Nakamoto consensus? — 216
- 13.8.1 Additional security layers — 218
- 13.8.2 Example: purge exploit and the buyer beware response — 220
- 13.8.3 The government to the rescue — 221
- 13.8.4 Economic majority vs. mining majority — 222
- 13.8.5 A tetralemma — 223
- 14 Direct frontal takeovers — 225**
 - 14.1 Institutional response — 226
 - 14.2 Creeping corporate takeover — 227
 - 14.3 Alliances are beneficial — 228
 - 14.4 ESG takeovers — 228
 - 14.5 Government KYC takeovers — 229
 - 14.6 Overexposed bagholder exploit — 230
 - 14.7 Fee market and long-term viability — 230
 - 14.8 How much is censorship resistance worth? — 231
 - 14.9 A 67 % fiat attack — 232
 - 14.10 Permissioned bypass — 233
- 15 Nash bargaining — 234**
 - 15.1 The bargaining problem — 235
 - 15.1.1 Motivating real-world problems — 235
 - 15.1.2 Motivating game theory games — 236
 - 15.1.3 Dividing a surplus and the Nash bargaining solution — 236
 - 15.1.4 Exogenous probability of breakdown — 238
 - 15.1.5 What if players can determine the probability of breakdown? — 240
 - 15.2 Creating commitment — 242
 - 15.2.1 Enter blockchains? — 243

15.2.2	Commitment can backfire —	244
15.3	Mixed strategies and Schelling threats —	244
15.3.1	Jane's example, again —	245
15.4	Extortion and grieving —	246
15.4.1	Schelling attacks as an inexpensive way to destroy a network —	249
15.5	Wars of attrition —	249
16	Coalitional game theory —	251
16.1	Motivating examples —	251
16.2	Characteristic form and payoff configurations —	253
16.3	Standard coalitional game theory and the Bitcoin mining game —	254
16.4	Solution concepts —	255
16.4.1	The core —	256
16.4.2	The stable set —	257
16.4.3	The bargaining set —	259
16.4.4	The kernel —	260
16.4.5	The nucleolus —	261
16.5	Analysis of solution concepts for weighted majority games and CBMGs —	261
16.6	The three-player case —	267
16.6.1	Kernel —	267
16.6.2	Nucleolus —	268
16.6.3	Beyond $n = 3$ —	270
16.6.4	Notes on $\mathcal{C}$ and $\mathcal{D}$ —	271
16.7	Discussion —	271
17	Stock, flow, and economic considerations —	273
17.1	Double-spend exploits —	275
17.1.1	Finality —	277
17.2	Sabotage (Goldfinger) attack —	280
17.3	Determining the stock value of ASICs —	281
17.3.1	Moore's law —	282
17.3.2	Flow-based miner cost model —	283
17.3.3	Stock value of latent hashrate as a threat —	284
17.4	Stable regimes —	284
17.4.1	Strong expectation of community reorg, no major adversaries —	284
17.4.2	Attacks happen, but only affect a minority of users —	285
17.5	Efficiency, security, and decentralization —	285
17.5.1	Efficiency —	286
17.6	Theoretical pushout and epsilon-attacks —	289
18	Bitcoin as it matures —	291

18.1	Hyperbitcoinization — 291
18.1.1	Decentralized hyperbitcoinization — 292
18.1.2	Centralized hyperbitcoinization — 295
18.1.3	Sovereign currency will not die — 297
18.2	Will nation-states support Bitcoin? — 299
18.2.1	Reasons why a nation would support Bitcoin use (centralized or decentralized) — 300
18.2.2	Reasons why a nation would oppose Bitcoin use (centralized or decentralized) — 300
18.2.3	Reasons for a nation to maintain Bitcoin specifically as a decentralized network — 301
18.2.4	Reasons for a nation to discourage use of decentralized Bitcoin — 301
18.2.5	Indifference to centralization and the soft-forkability hypothesis — 302
18.2.6	Bitcoin mining — 303
18.3	Non-profitable mining — 304
18.3.1	Will corporations protect their bags? — 306
18.4	Geopolitical considerations in adversarial conditions — 306
18.4.1	Nice and naughty nations — 310
18.4.2	The free-rider problem with a finite supply currency — 311
18.5	Can the supply be increased? — 312
18.6	Limits as a decentralized store of value — 313
18.6.1	Asymmetric risk premium — 314
18.6.2	Failure as a functional store of value — 315
18.7	Beasts in the jungle: centralization, capture, and collapse — 316
18.7.1	Centralization — 316
18.7.2	Capture — 318
18.7.3	Collapse — 319

Bibliography — 321

Index — 325

