A PRACTITIONER'S FIELD GUIDE

FIRST EDITION



Crypto Money Laundering Playbook 2027

Detect ➜ Trace ➜ Recover ➜ Report.

Rohas Nagpal

ASIAN SCHOOL OF CYBER LAWS

Contents

Preface 13
How to Use This Book 14
Who This Book Is For 15
The Labs 17

PART I **The Evolution of Money**

1 **Early and Physical Money** 18

UNDERSTAND

1.1 What Money Does 18
1.2 Barter and Its Limits 18
1.3 Commodity Money 19
1.4 Coins, Notes and Cash 19
1.5 What Money Laundering Is 20
1.6 Placement, Layering and Integration 20
1.7 Why Cash Still Matters to Launderers 21

2 **Hawala & Informal Value Transfer** 23

UNDERSTAND · DETECT

2.1 How Hawala Works 23
2.2 Trust, Ledgers and Settlement 24
2.3 Other Informal Value Transfer Systems 24
2.4 Why Launderers Use Informal Channels 25
2.5 How Informal Transfers Are Regulated 25
2.6 Red Flags 25
2.7 Hawala and Crypto: The Parallels 26

3 **Electronic Money** 28

UNDERSTAND · DETECT

3.1 Digital Money and Bank Transfers 28
3.2 Prepaid Cards and E-Money 28
3.3 Mobile Money 29
3.4 Centralised Digital Currencies 29
3.5 Laundering Risks in Electronic Money 29
3.6 How Electronic Money Is Controlled 30

4 **Cryptocurrencies & CBDCs** 32

UNDERSTAND

4.1 The Idea Behind Bitcoin 32
4.2 What Makes Cryptocurrency Different 32
4.3 Pseudonymity Is Not Anonymity 33
4.4 Central Bank Digital Currencies 34
4.5 Cryptocurrencies, Stablecoins and CBDCs Compared 35
4.6 What Each New Form of Money Means for Laundering 35

PART II **The Architecture of Cryptocurrency**

5 **Blockchains** 37

UNDERSTAND · TRACE

5.1 Blocks, Hashes and the Chain 38
5.2 Consensus Mechanisms 39
5.3 Public and Private Blockchains 40
5.4 Coins and Tokens 41
5.5 The Blockchains an Analyst Meets 42
5.6 Block Explorers 42
5.7 Reading Addresses, Transactions and Event Logs 43
5.8 How the Lab Works 45
5.9 What an Explorer Cannot Tell You 46

6 **Keys, Addresses & Wallets** 48

UNDERSTAND · TRACE

6.1 Public and Private Keys 49
6.2 How Addresses Are Derived 49
6.3 Address Formats Across Blockchains 50
6.4 Custodial and Non-Custodial Wallets 51
6.5 Seed Phrases and BIP-39 52
6.6 One Phrase, Many Wallets 54
6.7 Multi-Signature Wallets 56
6.8 Vanity Addresses 56
6.9 How the Labs Work 56
6.10 Wallets as Evidence 57

7 **Transactions** 59

UNDERSTAND · TRACE

7.1 Anatomy of a Transaction 59
7.2 The UTXO Model 60
7.3 The Account Model 61
7.4 Inputs, Outputs and Change 62
7.5 Gas and Fees 62
7.6 Confirmations and Finality 63
7.7 Data Hidden in Transactions 64
7.8 How the Lab Works 64

8 **Smart Contracts, Stablecoins, Privacy Coins & NFTs** 66

UNDERSTAND · DETECT

8.1 Smart Contracts 67
8.2 Token Standards 68
8.3 Stablecoins and How They Are Backed 69
8.4 Issuer Controls: Freezing and Blacklisting 70
8.5 Privacy Coins 70
8.6 NFTs 71
8.7 What Evidence Each One Leaves Behind 71
8.8 How the Lab Works 72

PART III **The Cryptocurrency Ecosystem**

9 **On-Ramps, Off-Ramps & Crypto ATMs** 74

DETECT

9.1 Where Fiat Meets Crypto 75
9.2 On-Ramps 75
9.3 Off-Ramps and Cashing Out 76
9.4 Crypto ATMs 77
9.5 Money Mules 77
9.6 Placement and Integration Risk Points 77
9.7 Red Flags 78
9.8 How the Lab Works 78

10 **Exchanges & Trading** 80

DETECT · TRACE

10.1 Centralised Exchanges 80
10.2 What Records an Exchange Keeps 81
10.3 Decentralised Exchanges 82
10.4 P2P Platforms 83
10.5 OTC Desks 83
10.6 Nested Exchanges 83
10.7 Red Flags at Each Venue 84

11 **DeFi & Cross-Chain Infrastructure** 86

DETECT · TRACE

11.1 What DeFi Is 86
11.2 Liquidity Pools and Automated Market Makers 87
11.3 Lending and Flash Loans 87
11.4 Cross-Chain Bridges 88
11.5 Wrapped Assets 88
11.6 Bridges as Laundering Channels 89
11.7 Following Funds Across a Bridge 89

12 **High-Risk Services** 91

DETECT

12.1 Mixers and Tumblers 91
12.2 Custodial and Smart-Contract Mixers 92
12.3 CoinJoin 92
12.4 Darknet Markets 93
12.5 Gambling Platforms 94
12.6 Exposure and Risk Scoring 94
12.7 Red Flags 95

13 **Laundering Techniques** 96

DETECT · TRACE

13.1 Peel Chains 96
13.2 Chain Hopping 97
13.3 Fan-Out and Fan-In 97
13.4 Wash Trading 98
13.5 NFT-Based Layering 98
13.6 Combining Techniques Across the Three Stages 99
13.7 Recognising Typologies On-Chain 99

PART IV **The Regulatory & Legal Framework**

14 **FATF Standards & VASP Obligations** 101

COMPLY

14.1 The FATF and Its Recommendations 101
14.2 Virtual Assets and Recommendation 15 102
14.3 Who Is a VASP 102
14.4 The Risk-Based Approach 103
14.5 Mutual Evaluations and Grey Lists 103
14.6 DeFi, NFTs and Unhosted Wallets 104

15 **KYC/AML Requirements & the Travel Rule** 105

COMPLY · DETECT

15.1 Customer Due Diligence 105
15.2 Enhanced Due Diligence 105
15.3 Transaction Monitoring 106
15.4 Sanctions Screening 106
15.5 Suspicious Transaction Reporting 107
15.6 The Travel Rule 107
15.7 Unhosted Wallets 108
15.8 Record-Keeping 109

16 **MiCA in the European Union** 110

COMPLY

16.1 What MiCA Covers 110
16.2 Crypto-Asset Service Providers 111
16.3 Stablecoins Under MiCA 111
16.4 The Transfer of Funds Regulation 112
16.5 The EU AML Framework for Crypto 112

17 **India's PMLA & VDA Rules** 114

COMPLY

17.1 Virtual Digital Assets Under Indian Law 114
17.2 VDA Service Providers as Reporting Entities 114
17.3 Registration with FIU-IND 115
17.4 KYC, Record-Keeping and Reporting Obligations 115
17.5 Enforcement 115
17.6 Practical Compliance for Indian Platforms 116

18 **FIUs & Cross-Border Cooperation** 118

COMPLY · RECOVER

18.1 What a Financial Intelligence Unit Does 118
18.2 From Suspicious Transaction Report to Intelligence 118
18.3 The Egmont Group 119
18.4 Mutual Legal Assistance Treaties 119
18.5 Interpol 120
18.6 Working Across Jurisdictions at Speed 121

PART V **Investigation & Recovery**

19 **Tracing Illicit Funds** 123

TRACE · REPORT

19.1 Starting a Crypto Investigation 123
19.2 Address Lookups 126
19.3 Decoding Transactions 126
19.4 Backward Tracing 127
19.5 Forward Tracing 127
19.6 Wallet Profiling 127
19.7 Checking Addresses Against Known Labels 128
19.8 How the Lab Works 128
19.9 Documenting the Trace 129

20 **Transaction Graphs & Clustering** 131

TRACE

20.1 Building a Transaction Graph 131
20.2 Reading a Graph 132
20.3 Clustering Heuristics 132
20.4 Co-Spend Analysis 133
20.5 Change Address Detection 133
20.6 Why Clustering Is Not Proof of Identity 133

21 **Smart Contract Analysis** 135

TRACE

21.1 Reading a Verified Contract 135
21.2 Function Calls and Input Data 136
21.3 Event Logs and Token Transfers 137
21.4 Following Funds Through DeFi Contracts 137
21.5 Contracts Built to Launder 137
21.6 How the Lab Works 138

22 **Exchange Subpoenas, Freezing & Seizure** 140

RECOVER

22.1 Identifying the Exchange 141
22.2 What to Ask For 141
22.3 Exchange Subpoena Strategy 142
22.4 Stablecoin Freezes 142
22.5 Asset Freezing and Seizure 143
22.6 Custody of Seized Crypto 144
22.7 Returning Funds to Victims 145
22.8 How the Lab Works 145

23 **Off-Chain Evidence** 147

TRACE · REPORT

23.1 Connecting Addresses to People 148
23.2 OSINT 148
23.3 Web Intelligence 148
23.4 Domain and Infrastructure Investigation 149
23.5 Image Forensics 149
23.6 File Forensics 150
23.7 Cryptanalysis and Seed Phrase Recovery 150
23.8 Combining On-Chain and Off-Chain Evidence 151
23.9 How the Lab Works 152

PART VI **Case Studies**

24 **Liberty Reserve** 153

CASE STUDY

24.1 Background 153
24.2 How the System Worked 153
24.3 How It Was Used to Launder 154
24.4 The Investigation and Shutdown 154
24.5 Lessons for Analysts 155

25 **Silk Road** 156

CASE STUDY

25.1 Background 156
25.2 How the Market Worked 156
25.3 Following the Bitcoin 157
25.4 From Addresses to People 157
25.5 Lessons for Analysts 158

26 **The Bitfinex Hack & Ilya Lichtenstein** 159

CASE STUDY

26.1 The 2016 Hack 159
26.2 Years of Laundering 159
26.3 Peel Chains, Darknet Markets and Exchanges 160
26.4 Tracing to the Arrests in 2022 160
26.5 Recovery of the Funds 161
26.6 Lessons for Analysts 161

27 **The TRON-USDT Nexus** 162

CASE STUDY

27.1 Why USDT on TRON 162
27.2 Scams and Laundering Networks 163
27.3 OTC Desks and Off-Ramps 163
27.4 Stablecoin Freezes 163
27.5 Lessons for Analysts 164

28 **Lazarus Group & the Ronin Bridge** 165

CASE STUDY

28.1 The 2022 Ronin Bridge Hack 165
28.2 Attribution to the Lazarus Group 165
28.3 How the Stolen Funds Were Laundered 166
28.4 Mixers, Bridges and Chain Hopping 166
28.5 Sanctions and Recovery 166
28.6 Lessons for Analysts 167

29 **Tornado Cash** 168

CASE STUDY

29.1 How Tornado Cash Worked 168
29.2 Who Used It 168
29.3 Sanctions 169
29.4 Prosecutions 169
29.5 Privacy Tools and Liability 169
29.6 Lessons for Analysts 170

PART VII **AI Agents**

30 **Introducing the CMLA Agents** 171

UNDERSTAND

30.1 Agentic Investigation 171
30.2 Agents, Agent Skills and Workflows 172
30.3 Installing the Agents 173
30.4 Keeping a Human in Charge 173

31 **Tracing Agents** 175

TRACE

31.1 Fund Flow Investigator 175
31.2 Cross-Chain Investigator 175
31.3 Mixer & Privacy Coin Investigator 176
31.4 Stablecoin Investigator 176
31.5 DeFi Laundering Investigator 176
31.6 NFT Laundering Investigator 176
31.7 Wallet Clustering Investigator 177

32 **Attribution, Compliance & Recovery Agents** 178

TRACE · COMPLY · RECOVER

32.1 Exchange & OTC Investigator 178
32.2 OSINT Investigator 178
32.3 Sanctions Screening Investigator 179
32.4 Asset Recovery Investigator 179
32.5 Cross-Border Investigation Assistant 179

33 **Running an Investigation with the Agents** 180

TRACE · RECOVER · REPORT

33.1 Coordinated Workflows 180
33.2 How Agents Collect Evidence 181
33.3 Checking What the Agents Find 181
33.4 Findings, Assumptions and Unknowns 181
33.5 The Investigation Report Writer 182
33.6 Producing the Investigation Report 182

APPENDICES

Glossary 183