

TECHNICAL FOUNDATIONS FOR DIGITAL INVESTIGATIONS



ROHAS NAGPAL

Table of Contents

Introduction.....	08
 1. Blockchain Technology	
BLOCKCHAIN CORE CONCEPTS	
1-1. Blockchain Technology Overview.....	11
1-2. Blocks.....	13
1-3. Transactions.....	15
1-4. Ledger & Record-Keeping Models.....	18
1-5. Hashing Functions.....	21
1-6. Merkle Trees.....	24
1-7. Consensus Mechanisms.....	27
1-8. Validators & Miners.....	32
1-9. Transaction Propagation.....	37
1-10. Immutability.....	42
1-11. Forks.....	45
BLOCKCHAIN INFRASTRUCTURE & ACCESS	
1-12. Blockchain Nodes.....	51
1-13. RPC Endpoints.....	57
1-14. Blockchain APIs.....	61
1-15. Public vs. Private Node Infrastructure.....	66
1-16. Rate Limits & API Key Management.....	69
 2. Smart Contracts	
FOUNDATION	
2-1. Smart Contract Basics.....	72
VULNERABILITIES AND ATTACKS	
2-2. Access Control Failure.....	82
2-3. Flash Loan Attacks.....	84
2-4. Front-Running (MEV).....	87
2-5. Governance Takeover.....	90
2-6. Integer Overflow/Underflow.....	93
2-7. Oracle Manipulation.....	95

2-8. Reentrancy Attack.....	97
2-9. Unchecked Return Values.....	100
2-10. Upgrade Function Abuse.....	103
2-11. Weak Randomness.....	106
INVESTIGATION CHECKLISTS	
c4 checklist for Smart Contract Analysis.....	109

3. Token Standards

FOUNDATIONS

3-1. Introduction to Blockchain Tokens.....	112
3-2. Building Tokens with Open Zeppelin.....	116

STANDARDS

3-3. Algorand Standards.....	131
3-4. Avalanche Standards.....	136
3-5. Bitcoin-Based Standards.....	141
3-6. BNB Chain Standards.....	147
3-7. Cardano Standards.....	152
3-8. Cosmos Standards.....	157
3-9. EVM Standards.....	162
3-10. Hedera Standards.....	167
3-11. Move-Based Standards.....	172
3-12. Polkadot / Substrate Standards.....	177
3-13. Solana Standards.....	182
3-14. Stellar Standards.....	188
3-15. Tezos Standards.....	194
3-16. TON Standards.....	200
3-17. Tron Standards.....	206

INVESTIGATION CHECKLISTS

c4 checklist for Token Analysis.....	212
--------------------------------------	-----

4. Internet & Web Technology

4-1. Internet Protocol.....	213
4-2 Domain Name System.....	219
4-3 Hyper Text Transfer Protocol.....	227
4-4 Simple Mail Transfer Protocol.....	234

4-5. File Transfer Protocol.....	242
4-6. SSL/TLS Certificates.....	250
4-7. Web Servers.....	257
4-8. Cloud Infrastructure.....	265
4-9. Content Delivery Networks.....	273
4-10. Web Browsers.....	281
INVESTIGATION CHECKLISTS	
c4 checklist for IP Address Investigation.....	289
c4 checklist for DNS Investigation.....	291
c4 checklist for Web Server Investigation.....	293
c4 checklist for FTP Server Investigation.....	294
c4 checklist for Email Investigation.....	295
c4 checklist for Browser Investigation.....	296
 5. On-Chain and Off-Chain Data	
5-1. On-Chain Data Types & Sources.....	297
5-2. Off-Chain Data Types & Sources.....	301
5-3. Linking On-Chain to Off-Chain Evidence.....	206
 6 Python for Investigators	
6-1. Introduction to Python.....	311
6-2. Python Libraries for Blockchain & Cryptocurrency Investigation.....	317
6-3. Python Libraries for Digital Forensics & Disk Analysis.....	324
6-4. Python Libraries for Malware Analysis & Reverse Engineering.....	331
6-5. Python Libraries for Browser Forensics & Analysis.....	335
6-6. Python Libraries for Penetration Testing.....	340

Rohas Nagpal is an author, lawyer, and investigator with over 25 years of experience. He has worked across 18 countries on complex cases involving digital forensics, cyber terrorism, financial crime, and corporate liability.

He is the co-founder of the Asian School of Cyber Laws, a pioneering institution in cyber law and digital forensics education, and has assisted the Government of India in drafting rules under the Information Technology Act.

He authored the Cryptocurrency Investigation & Forensics Manual 2026 and the Cyber Crime Investigation Manual, described by The Times of India as the "Bible for cybercrime investigators", and wrote India's first legal commentary on the Information Technology Act.

Rohas first encountered Bitcoin in 2011 during a narcotics investigation, an experience that led to a long-term focus on blockchain, cryptocurrency crime, and financial infrastructure.

He later co-founded BankChain, a blockchain consortium of 37 banks, designed a Layer-1 protocol for regulated finance, and served as a consultant to the Reserve Bank Innovation Hub on NFTs & CBDCs.

