Contents

1 Introduction **1**

1.1 Problem Analysis . . . 3

1.1.1 Promises of Blockchain Technology . . . 3

1.1.2 Problems of Blockchain-based Data Management . . . 5

1.2 Research Questions . . . 8

1.3 Contributions . . . 9

1.3.1 Attribution of Contributions . . . 14

1.4 Outline . . . 16

2 Bitcoin and Blockchain Technology **17**

2.1 Bitcoin Overview . . . 18

2.2 Blockchain Structure . . . 23

2.2.1 Overview . . . 23

2.2.2 Block Structure . . . 24

2.2.3 Merkle Trees . . . 27

2.3 Transactions . . . 29

2.3.1 Overview . . . 29

2.3.2 Coin Ownership . . . 31

2.3.3 Scripting System . . . 35

2.3.4 Segregated Witnesses . . . 42

2.3.5 Managing Unspent Transaction Outputs . . . 43

2.4 Consensus . . . 44

2.4.1 Mining Process . . . 45

2.4.2 Distribution and Validation Process . . . 47

2.4.3 Forks . . . 49
2.5 Peer-to-Peer Network . . . 52
2.5.1 Network Overview . . . 52
2.5.2 Node Connections . . . 55
2.5.3 Data Dissemination . . . 56
2.5.4 Initial Synchronization Process . . . 58
2.6 Summary . . . 59

3 Systematic Analysis of Non-Financial Blockchain Content **61**
3.1 Motivation . . . 61
3.1.1 Contributions . . . 62
3.2 Problem Analysis . . . 64
3.2.1 History of Bitcoin Content Insertion . . . 64
3.2.2 Model for Blockchain Content Insertion and Distribution . . . 66
3.3 Analysis of Content Insertion Methods . . . 67
3.3.1 Low-Level Content Insertion Methods . . . 68
3.3.2 Content Insertion Services . . . 72
3.4 Benefits and Risks of Blockchain Content . . . 74
3.4.1 Benefits of Blockchain Content Insertion . . . 74
3.4.2 Negative Consequences of Blockchain Content Insertion . . . 75
3.5 Analysis of Non-Financial Content . . . 81
3.5.1 Measurement Framework and Methodology . . . 81
3.5.2 Quantitative Analysis of Content Insertion . . . 86
3.5.3 Assessment of Blockchain Files . . . 95
3.6 Related Work . . . 99
3.7 Conclusion and Future Work . . . 101

4 Mitigation of Unwanted Blockchain Content **103**
4.1 Motivation . . . 103
4.1.1 Constraints for Mitigation Schemes . . . 105
4.1.2 Contributions . . . 107
4.2 Prevention Strategies Against Unwanted Content . . . 107

4.2.1 Related Work . . . 109
4.2.2 Problem Statement . . . 110
4.2.3 Filtering Content-Holding Transactions . . . 112
4.2.4 Mandatory Minimum Transaction Fees . . . 114
4.2.5 Hardened On-Chain Addresses . . . 120
4.2.6 Summary and Future Work . . . 124
4.3 Moderation of Blockchain Content . . . 125
4.3.1 Related Work . . . 126
4.3.2 Missing Swift and Transparent Redactions . . . 129
4.3.3 Cryptographic Building Blocks . . . 131
4.3.4 RedactChain Overview . . . 135
4.3.5 Detecting Unwanted Blockchain Content . . . 137
4.3.6 Decentralized Redaction Process . . . 139
4.3.7 Coordinating Short-Lived Redaction Juries . . . 142
4.3.8 Evaluation . . . 145
4.3.9 Summary and Future Work . . . 150
4.4 Conclusion . . . 152

5 Retrofitting Blockchains with Pruning Capabilities 153
5.1 Motivation . . . 154
5.1.1 Problem Analysis . . . 155
5.1.2 Contributions . . . 158
5.2 Survey of Related Work . . . 159
5.2.1 Survey Criteria . . . 159
5.2.2 Retrospective Changes to Established Blockchain Systems . . . 159
5.2.3 Alternative Blockchain Designs with Pruning Capabilities . . . 162
5.3 Design Goals . . . 164
5.4 CoinPrune Overview . . . 165
5.5 Retrofittable Block Pruning . . . 167
5.5.1 Data Management . . . 167
5.5.2 Coordination of Established Nodes . . . 169
5.5.3 Bootstrapping of New Nodes . . . 169

5.6 Handling Application-Level Data . . . 170
5.6.1 Obfuscation of Illicit Data from the UTXO Set . . . 170
5.6.2 Preservation of Application-Level Data . . . 173
5.7 Seamless Integration into Bitcoin . . . 174
5.7.1 Additional On-Chain Data . . . 174
5.7.2 Adaptions to the Peer-to-Peer Protocol . . . 174
5.8 Security Discussion . . . 175
5.8.1 Snapshot Validity . . . 175
5.8.2 Reliability of Reaffirmations . . . 177
5.8.3 Peer-to-Peer Attacks . . . 178
5.9 Performance Evaluation . . . 179
5.9.1 Testbed Setup for Synchronization Measurements . . . 179
5.9.2 Storage Savings . . . 179
5.9.3 Evaluation of Synchronization Performance . . . 181
5.10 Conclusion and Future Work . . . 183

6 Blockchain-based Bootstrapping of Anonymity Services 185
6.1 Motivation . . . 186
6.1.1 Problem Analysis . . . 186
6.1.2 Contributions . . . 190
6.2 Design Goals . . . 191
6.3 AnonBoot Overview . . . 192
6.3.1 Design Intuition . . . 192
6.3.2 Overview of Bootstrapping Steps . . . 193
6.4 Sybil-Resistant Index of Peers and Services . . . 195
6.4.1 Message Types . . . 195
6.4.2 Pulse-based Message Release . . . 198
6.5 Bootstrapping Secure Anonymity Services . . . 199
6.5.1 Connecting Users and Privacy Peers . . . 200
6.5.2 Local Selection of Privacy Peers . . . 200
6.5.3 Service Requests for Peer Election . . . 201
6.6 Realization of Use Cases . . . 202

6.6.1 Decentralized Onion Routing via AnonBoot 202
6.6.2 Shuffling Networks and Cryptocurrency Tumblers 203
6.6.3 User-Centered Redaction Juries 204
6.7 Security Discussion 205
6.7.1 Proof of Work Against Sybil Attacks 206
6.7.2 Security of Bootstrapped Services 207
6.8 Performance Evaluation 210
6.8.1 Synchronization with Host Blockchain 210
6.8.2 Small Blockchain Footprint and Low Costs 211
6.9 Related Work 212
6.10 Conclusion and Future Work 213

7 Conclusion **215**

7.1 Contributions 216
7.1.1 Systematic Analysis of Non-Financial Blockchain Content . . 216
7.1.2 Mitigation of Unwanted Blockchain Content 216
7.1.3 Retrofitting Blockchains with Pruning Capabilities 217
7.1.4 Blockchain-based Bootstrapping of Anonymity Services 218
7.2 Future Work 219
7.3 Closing Remarks 220

Abbreviations and Acronyms **221**

Bibliography **223**