SPIS TREŚCI

WSTĘP 7

Rozdział 1. TEORIA 13
1.1. Kryptowaluty 14
1.2. Zasada działania 17
1.3. Elementy kryptografii 18
1.3.1. Kryptograficzne funkcje skrótu 19
1.3.2. Podpisy cyfrowe 27
1.4. Klucze 36
1.5. Adresy 37
1.6. Łańcuch bloków 46
1.7. Wydobywanie kryptowalut 60
1.8. Modele transakcji 66
1.8.1. Model zastosowany w sieci Bitcoin 66
1.8.1.1. Transakcja 1 → 1 67
1.8.1.2. Transakcja 1 → 2 68
1.8.1.3. Transakcja 1 → m 70
1.8.1.4. Transakcja n → 1 71
1.8.1.5. Transakcja n → 2 72
1.8.1.6. Transakcja n → m 74
1.8.1.7. Transakcja 0 → 1 75
1.8.1.8. Porównanie częstości występowania transakcji 77
1.8.2. Model zastosowany w sieci Ethereum 78

Rozdział 2. PRAKTYKA 79
2.1. Rodzaje przestępstw 79
2.1.1. Przestępstwa popełniane przy użyciu kryptowalut 79
2.1.1.1. Zakazany handel – darknet 79
2.1.1.2. Pranie pieniędzy 84
2.1.1.3. Scam 87
2.1.1.4. Wspieranie działalności terrorystycznej 92
2.1.2. Przestępstwa popełniane w celu uzyskania kryptowalut 93
2.1.2.1. Złośliwe oprogramowanie 93
2.1.2.2. Włamania do podmiotów zajmujących się obrotem kryptowalutami 101
2.1.2.3. Przestępstwa związane z technologią 104
2.1.2.4. Fizyczne ataki 108
2.2. Pozyskiwanie kryptowalut 113
2.2.1. Cinkciarz 113
2.2.2. Giełdy kryptowalut 114

2.2.3. Kantory kryptowalut ... 118
2.2.4. Bitomaty ... 120
2.2.5. Wydobywanie kryptowalut ... 123
2.2.6. Otrzymywanie kryptowalut w prezencie ... 128
2.3. Portfele ... 130
2.3.1. Typologia portfeli ... 131
2.3.1.1. Fizyczne monety ... 131
2.3.1.2. Portfele papierowe i nieśmiertelniki ... 134
2.3.1.3. Portfele sprzętowe ... 137
2.3.1.4. Portfele aplikacyjne ... 144
2.3.1.5. Portfele przeglądarkowe ... 146
2.3.2. Podział portfeli ... 146
2.4. Heurystyki ... 149
2.4.1. Heurystyka 1 ... 150
2.4.2. Heurystyka 2 ... 151
2.5. Narzędzia deanonimizacyjne ... 153
2.5.1. Darmowe narzędzia wspomagające deanonimizację ... 153
2.5.2. Komercyjne narzędzia wspomagające deanonimizację ... 157
2.5.3. Autorski system deanonimizacji użytkowników ... 161

Rozdział 3. PRZEWODNIK ... 165
3.1. Zabezpieczanie materiału dowodowego ... 165
3.2. Poszukiwanie cyfrowych śladów ... 167
3.3. Zabezpieczanie działających komputerów ... 202
3.4. Analiza adresów kryptowalut ... 203
3.5. Identyfikacja właściciela ... 205
3.6. Monitorowanie adresów kryptowalut ... 206
3.7. Zabezpieczanie kryptowalut ... 208
3.8. Śledzenie transakcji ... 211
3.9. Studium przypadków ... 213
3.10. Wyzwania ... 215

ZAKOŃCZENIE ... 219

BIBLIOGRAFIA ... 223

SPIS TABEL ... 231

SPIS RYSUNKÓW ... 233

SPIS WYKRESÓW ... 239