

**Blockchain i bezpieczeństwo systemów rozproszonych / Sachin S. Shetty, Charles A. Kamhoua, Laurent L. Njilla. – Wydanie I. – Warszawa, 2020**

Spis treści

|                                                                                        |             |
|----------------------------------------------------------------------------------------|-------------|
| <b>Przedmowa</b>                                                                       | <b>XI</b>   |
| <b>Wprowadzenie</b>                                                                    | <b>XIII</b> |
| <b>Lista autorów</b>                                                                   | <b>XVI</b>  |
| <b>CZĘŚĆ I WPROWADZENIE DO BLOCKCHAINA</b>                                             |             |
| <b>01 Wprowadzenie</b>                                                                 | <b>3</b>    |
| 1.1. Podstawowe informacje na temat łańcucha bloków                                    | 3           |
| 1.2. Zawartość książki                                                                 | 20          |
| Bibliografia                                                                           | 28          |
| <b>02 Protokoły i algorytmy rozproszonego konsensusu</b>                               | <b>30</b>   |
| 2.1. Wprowadzenie                                                                      | 30          |
| 2.2. Odporny na awarie konsensus w systemie rozproszonym                               | 31          |
| 2.3. Konsensus Nakamoto                                                                | 46          |
| 2.4. Nowe algorytmy konsensusu dla blockchaina                                         | 50          |
| 2.5. Ocena i porównanie                                                                | 58          |
| 2.6. Podsumowanie                                                                      | 58          |
| Podziękowania                                                                          | 60          |
| Bibliografia                                                                           | 60          |
| <b>03 Przegląd płaszczyzn ataków w sieci blockchain</b>                                | <b>62</b>   |
| 3.1. Wprowadzenie                                                                      | 62          |
| 3.2. Omówienie technologii blockchain i jej działania                                  | 64          |
| 3.3. Ataki na łańcuch bloków                                                           | 65          |
| 3.4. System peer-to-peer łańcucha bloków                                               | 68          |
| 3.5. Ataki zorientowane na zastosowania                                                | 73          |
| 3.6. Powiązane prace                                                                   | 75          |
| 3.7. Podsumowanie i dalsza praca                                                       | 76          |
| Bibliografia                                                                           | 77          |
| <b>CZĘŚĆ II ROZWIĄZANIA BLOCKCHAINOWE DLA BEZPIECZEŃSTWA SYSTEMÓW ROZPROSZONYCH</b>    |             |
| <b>04 ProvChain: oparte na blockchainie potwierdzanie pochodzenia danych w chmurze</b> | <b>83</b>   |

|                                                                                                                             |            |
|-----------------------------------------------------------------------------------------------------------------------------|------------|
| 4.1. Wprowadzenie                                                                                                           | 83         |
| 4.2. Kontekst i powiązane prace                                                                                             | 85         |
| 4.3. Architektura ProvChain                                                                                                 | 91         |
| 4.4. Implementacja ProvChain                                                                                                | 96         |
| 4.5 .Ocena                                                                                                                  | 103        |
| 4.6. Podsumowanie i dalsza praca                                                                                            | 110        |
| Podziękowania                                                                                                               | 111        |
| Bibliografia                                                                                                                | 111        |
| <b>05 Oparte na blockchainie rozwiązania problemów bezpieczeństwa i prywatności danych dla branży motoryzacyjnej</b>        | <b>114</b> |
| 5.1. Wprowadzenie                                                                                                           | 114        |
| 5.2. Wprowadzenie do łańcucha bloków                                                                                        | 118        |
| 5.3. Proponowane rozwiązanie                                                                                                | 122        |
| 5.4. Zastosowania                                                                                                           | 124        |
| 5.5. Ocena i dyskusja                                                                                                       | 131        |
| 5.6. Powiązane prace                                                                                                        | 136        |
| 5.7. Podsumowanie                                                                                                           | 138        |
| Bibliografia                                                                                                                | 138        |
| <b>06 Oparte na blockchainie dynamiczne zarządzanie kluczami w sieciach IoT do zapewniania bezpieczeństwa w transporcie</b> | <b>140</b> |
| 6.1. Wprowadzenie                                                                                                           | 140        |
| 6.2. Rozważane zastosowanie                                                                                                 | 142        |
| 6.3. Schemat dynamicznego zarządzania kluczami w oparciu o blockchain                                                       | 149        |
| 6.4. Algorytm dynamicznego gromadzenia transakcji                                                                           | 150        |
| 6.5. Skład czasu                                                                                                            | 153        |
| 6.6. Ocena wydajności                                                                                                       | 156        |
| 6.7. Podsumowanie i dalsze prace                                                                                            | 165        |
| Bibliografia                                                                                                                | 167        |
| <b>07 Blockchainowy framework wymiany informacji dla cyberbezpieczeństwa</b>                                                | <b>169</b> |
| 7.1. Wprowadzenie                                                                                                           | 169        |
| 7.2. Framework BIS                                                                                                          | 171        |
| 7.3. Transakcje w BIS                                                                                                       | 173        |
| 7.4. Wykrywanie cyberataków i udostępnianie informacji                                                                      | 175        |
| 7.5. Międzygrupowa gra ataku w blockchainowym frameworku BIS: atak jednokierunkowy                                          | 176        |
| 7.6. Międzygrupowa gra ataku w blockchainowym frameworku BIS: atak dwukierunkowy                                            | 178        |
| 7.7. Użycie gry Stackelberga do analizy cyberataku i obrony                                                                 | 180        |
| 7.8. Podsumowanie                                                                                                           | 184        |
| Bibliografia                                                                                                                | 185        |

## **CZĘŚĆ III ANALIZA BEZPIECZEŃSTWA BLOCKCHAINA**

|                                                                                                              |            |
|--------------------------------------------------------------------------------------------------------------|------------|
| <b>08 Analiza bezpieczeństwa chmur blockchainowych</b>                                                       | <b>189</b> |
| 8.1. Wprowadzenie                                                                                            | 189        |
| 8.2. Mechanizmy konsensusu blockchaina                                                                       | 192        |
| 8.3. Chmura blockchainowa i jej podatności                                                                   | 202        |
| 8.4. Model systemu                                                                                           | 212        |
| 8.5. Zwiększanie mocy obliczeniowej                                                                          | 213        |
| 8.6. Analiza strategii ataku zaburzającego                                                                   | 214        |
| 8.7. Wyniki symulacji i dyskusja                                                                             | 221        |
| 8.8. Podsumowanie i dalsze prace                                                                             | 223        |
| Podziękowania                                                                                                | 225        |
| Bibliografia                                                                                                 | 225        |
| <b>09 Blockchainy zamknięte i otwarte</b>                                                                    | <b>228</b> |
| 9.1. Wprowadzenie                                                                                            | 228        |
| 9.2. Rozsądny wybór węzłów                                                                                   | 229        |
| 9.3. Mechanizmy wyboru komisji                                                                               | 232        |
| 9.4. Prywatność w blockchainach zamkniętych i otwartych                                                      | 235        |
| 9.5. Podsumowanie                                                                                            | 238        |
| Bibliografia                                                                                                 | 239        |
| <b>10 Atak niepotwierdzonymi transakcjami na pulę pamięci blockchaina: nowe ataki DDoS i środki zaradcze</b> | <b>241</b> |
| 10.1. Wprowadzenie                                                                                           | 241        |
| 10.2. Powiązane prace                                                                                        | 243        |
| 10.3. Podstawowe informacje o blockchainie i cyklu życia transakcji                                          | 245        |
| 10.4. Model zagrożenia                                                                                       | 248        |
| 10.5. Przebieg ataku                                                                                         | 250        |
| 10.6. Zapobieganie atakom na pulę pamięci                                                                    | 253        |
| 10.7. Eksperyment i wyniki                                                                                   | 264        |
| 10.8. Podsumowanie                                                                                           | 267        |
| Bibliografia                                                                                                 | 267        |
| <b>11 Zapobieganie atakom górników na spółdzielnie wydobywcze z wykorzystaniem paradygmatu reputacji</b>     | <b>271</b> |
| 11.1. Wprowadzenie                                                                                           | 271        |
| 11.2. Informacje wstępne                                                                                     | 273        |
| 11.3. Przegląd literatury                                                                                    | 276        |
| 11.4. Model wydobywania oparty na reputacji                                                                  | 278        |
| 11.5. Wydobywanie w modelu opartym na reputacji                                                              | 280        |
| 11.6. Ocena naszego modelu za pomocą analiz według teorii gry                                                | 287        |
| 11.7. Uwagi końcowe                                                                                          | 290        |
| Podziękowania                                                                                                | 290        |
| Bibliografia                                                                                                 | 291        |

## **CZĘŚĆ IV IMPLEMENTACJE BLOCKCHAINÓW**

|                                                                                            |            |
|--------------------------------------------------------------------------------------------|------------|
| <b>12 Konfiguracje blockchainów prywatnych dla poprawy bezpieczeństwa Internetu rzeczy</b> | <b>295</b> |
| 12.1. Wprowadzenie                                                                         | 295        |
| 12.2. Strategia bramki blockchainowej                                                      | 297        |
| 12.3. Strategia blockchainowych inteligentnych urządzeń końcowych                          | 304        |
| 12.4. Powiązane prace                                                                      | 313        |
| 12.5. Podsumowanie                                                                         | 314        |
| Bibliografia                                                                               | 315        |
| <b>13 Platforma do oceny łańcuchów bloków</b>                                              | <b>317</b> |
| 13.1. Wprowadzenie                                                                         | 317        |
| 13.2. Hyperledger Fabric                                                                   | 322        |
| 13.3. Pomiary wydajności                                                                   | 335        |
| 13.4. Prosta symulacja Blockchaina                                                         | 345        |
| 13.5. Wprowadzenie do symulacji blockchainów                                               | 349        |
| 13.6. Podsumowanie i dalsza praca                                                          | 356        |
| Bibliografia                                                                               | 357        |
| <b>14 Podsumowanie i dalsze prace</b>                                                      | <b>358</b> |
| 14.1. Wprowadzenie                                                                         | 358        |
| 14.2. Blockchain i bezpieczeństwo chmury                                                   | 359        |
| 14.3. Blockchain i bezpieczeństwo Internetu rzeczy                                         | 360        |
| 14.4. Bezpieczeństwo i prywatność blockchainów                                             | 362        |
| 14.5. Eksperymentalna platforma testowa i ocena wydajności                                 | 364        |
| 14.6. Przyszłość                                                                           | 365        |
| <b>Indeks</b>                                                                              | <b>367</b> |

oprac. BPK