Prof. dr hab. inż. Aleksander Nawrat
Wydział Automatyki Elektroniki i Informatyki
Katedra Automatyki i Robotyki
Dyrektor Centrum Cyberbezpieczeństwa
Politechnika Śląska w Gliwicach

Gliwice, 03.06.2024 r.

Rada dyscypliny
informatyka techniczna i telekomunikacja
Zachodniopomorski Uniwersytet Technologiczny

Recenzja rozprawy doktorskiej

Tytuł: *„Zastosowanie zaawansowanych systemów blockchain do wzmacniania odporności systemów informatycznych”*

Doktorant: mgr inż. Kamil Kaczyński

Recenzowana rozprawa mgra inż. Kamila Kaczyńskiego została napisana pod kierunkiem **prof. dra hab. n. mat. inż. Jerzego Gawineckiego**. Praca składa się ze 153 stron, w tym spisu treści, bibliografii, wykazu skrótów, streszczeń oraz spisu tabel i rysunków. Autor podzielił pracę na dziesięć rozdziałów, których zdecydowana większość została podzielona na od trzech do pięciu podrozdziałów.

Rozdział pierwszy stanowi wstęp wskazujący na motywacje doktoranta w zakresie wyboru tematyki rozprawy doktorskiej oraz przedstawia streszczenie kolejnych rozdziałów. W rozdziale drugim zdefiniowany został cel i główna teza pracy a także określono problemy badawcze. Rozdział trzeci został podzielony na trzy podrozdziały, które przedstawiają odpowiednio rys historyczny technologii rejestru rozproszonego, specyfikację techniczną sieci Bitcoin oraz specyfikację wybranych

algorytmów konsensusu stosowanych w protokołach blockchain. Doktorant skupił się na przedstawieniu pierwszej generacji technologii blockchain, która była dedykowana w szczególności aplikacjom finansowym. Następnie opisane zostały podstawowe metody osiągania konsensusu, takiej jak Proof of Work czy BFT, a także ich znaczenie w zapewnianiu integralności rejestru. Rozdział czwarty ma charakter teoretyczny i przedstawia rozwój technologii opartych o rejestr rozproszony. Doktorant wykorzystał pięć podrozdziałów do przybliżenia kluczowych ewolucji i zastosowań technologii blockchain w generacjach 2.0 i 3.0 a także przedstawienia technologii zdecentralizowanego przechowywania danych. W kolejnych podrozdziałach omówione zostały sieci Ethereum, IOTA oraz Hyperledger Fabric. Następnie przedstawione zostały technologie zdecentralizowanego przechowywania danych - IPFS oraz Arweave. Ostatni podrozdział przedstawia praktyczne zastosowania opisanych wcześniej generacji blockchain, w szczególności:

- Zdecentralizowane finanse (DeFi);
- Zdecentralizowane autonomiczne organizacje (DAO);
- Tokeny niezamienne (NFT).

Rozdział piąty rozpoczyna część praktyczną pracy. Przedstawione zostały w nim autorskie propozycje wykorzystania technologii DLT w celu decentralizacji infrastruktury. Doktorant w trzech kolejnych podrozdziałach opisał możliwości wykorzystania DLT w kontekście zapewniania integralności i dostępności danych oraz prowadzenia obliczeń rozproszonych. Pierwszy podrozdział skupiał się na analizie autorskich propozycji dotyczących zapewniania integralności danych. Poprzez zaprezentowany autorski przypadek użycia DLT do monitorowania łańcucha dostaw produktów medycznych, autor wskazał przewagi tego podejścia nad systemami scentralizowanymi. Drugi podrozdział wprowadza czytelnika w rozważania dotyczące autorskich koncepcji zwiększania dostępności danych poprzez wykorzystanie technologii rejestru rozproszonego. Autor przeprowadził w nim analizę decentralizacji infrastruktury, wskazując na możliwość jej decentralizacji z wykorzystaniem technologii IPFS prowadzącej do poprawy niezawodności i dostępności danych, a także eliminacji możliwości cenzurowania opublikowanych treści. Wskazany przez autora schemat pozwala na realizację dostępu do danych w sytuacjach kryzysowych, czy też ograniczonej łączności. W ostatnim, trzecim podrozdziale wprowadzone zostały autorskie rozważania dotyczące zastosowania technologii rejestru rozproszonego do

realizacji obliczeń rozproszonych. Autor skupił się na przedstawieniu możliwości wykorzystania technologii DLT do realizacji autonomicznego roju dronów, co zgodnie z zapewnieniami przekłada się na większą odporność na zakłócenia i ataki radioelektroniczne. Zaproponowane podejście zakłada wysoki poziom autonomiczności roju, co pozwala na zwiększenie elastyczności i dynamiki prowadzonych operacji.

Rozdział szósty recenzowanej rozprawy jest skupiony wokół autorskiego rozwiązania schematu uwierzytelnionego dostępu do danych w środowisku rozproszonym. Do realizacji schematu autor wykorzystał szereg technologii, takich jak Ethereum, IPFS, Secret Network, Web Cryptography API czy JS. Rozdział został podzielony na trzy podrozdziały. W pierwszym z nich autor przedstawił specyfikę przechowywania sekretów w publicznej sieci blockchain. W kolejnym podrozdziale przedstawione zostały implementacje smart kontraktów i aplikacji webowych realizujących zamierzone funkcjonalności. Trzeci i ostatni podrozdział stanowi ewaluacja zaproponowanego w pracy schematu, skupiona na weryfikacji spełnienia założonych wymagań funkcjonalnych i niefunkcjonalnych.

Rozdział siódmy stanowi podsumowanie wyników przeprowadzonych badań oraz wnioski autora w zakresie możliwości ich wykorzystania. Rozdziały ósmy, dziewiąty i dziesiąty stanowią odpowiednio bibliografię, spis tabel i spis rysunków.

Recenzując rozprawę doktorską, należy odwołać się do wymagań przedstawionych przez ustawodawcę w ustawie z dnia 20 lipca 2018 r. - Prawo o szkolnictwie wyższym i nauce. Artykuł 187 tej ustawy definiuje wymagania odnośnie rozpraw doktorskich:

1. *Rozprawa doktorska prezentuje ogólną wiedzę teoretyczną kandydata w dyscyplinie albo dyscyplinach oraz umiejętność samodzielnego prowadzenia pracy naukowej lub artystycznej.*
2. *Przedmiotem rozprawy doktorskiej jest oryginalne rozwiązanie problemu naukowego, oryginalne rozwiązanie w zakresie zastosowania wyników własnych badań naukowych w sferze gospodarczej lub społecznej albo oryginalne dokonanie artystyczne.*
3. *Rozprawę doktorską może stanowić praca pisemna, w tym monografia naukowa, zbiór opublikowanych i powiązanych tematycznie artykułów*

naukowych, praca projektowa, konstrukcyjna, technologiczna, wdrożeniowa lub artystyczna, a także samodzielna i wyodrębniona część pracy zbiorowej.

Przedstawiona mi rozprawa stanowi pracę pisemną, będącą spójną całością zrealizowaną w sposób, jakiego oczekuje się od prac naukowych. W związku z powyższym należy uznać, iż wymóg art. 187 pkt 3 został spełniony.

Rozprawa mgra inż. Kamila Kaczyńskiego ma charakter teoretyczno-praktyczny. Bibliografia zawiera 192 pozycje, które w większości stanowią recenzowane artykuły naukowe w języku angielskim. Dla każdej z pozycji literaturowych istnieje stosowne odniesienie w tekście rozprawy. W kontekście zgodności treści z dyscypliną informatyka techniczna i telekomunikacja, należy zauważyć, iż jednym z głównych obszarów informatyki technicznej jest zapewnienie bezpieczeństwa systemów informatycznych. Technologia rejestru rozproszonego bez wątpienia oferuje nowe możliwości w zakresie zabezpieczania danych i systemów przed nieautoryzowanym dostępem, manipulacją czy różnego rodzaju cyberatakami. Poziom szczegółowości zamieszczonych przez doktoranta opisów wybranych technologii blockchain, jak i ich wykorzystania w konkretnych przypadkach użycia bez wątpienia pokazuje jego dogłębną wiedzę w tejże dyscyplinie. Struktura pracy jest przemyślana, a kolejne rozdziały przygotowują czytelnika do interpretacji wyników przeprowadzonych badań. Uważam zatem, iż rozprawa prezentuje ogólną wiedzę kandydata w dyscyplinie informatyka techniczna i telekomunikacja oraz potwierdza jego umiejętność do samodzielnego prowadzenia pracy naukowej, tym samym spełniając wymogi art. 187 pkt 1 ustawy.

Tematem recenzowanej rozprawy jest „Zastosowanie zaawansowanych systemów blockchain do wzmacniania odporności systemów informatycznych". W kontekście rozwiązania problemu naukowego, mgr inż. Kamil Kaczyński postawił następujące hipotezy badawcze:

Główna hipoteza badawcza:

Zastosowanie technologii blockchain pozwala na realizację uwierzytelnionego dostępu do danych zdecentralizowanych.

Szczegółowe hipotezy badawcze:

1. *Zastosowanie połączenia różnych technologii blockchain pozwala na stworzenie rozproszonej usługi szyfrowania danych.*

2. *Technologia blockchain pozwala na prowadzenie komunikacji w niezaufanym środowisku.*
3. *Możliwe jest utworzenie schematu składowania danych w sieci publicznej, gwarantującego integralność i poufność treści.*

Przedstawione hipotezy zostały zweryfikowane w rozdziałach 5 i 6, w części praktycznej pracy. Opracowany przez doktoranta schemat uwierzytelnionego dostępu do danych zdecentralizowanych został zbudowany w oparciu o sieci blockchain Ethereum i Secret Network, usługę zdecentralizowanego przechowywania danych IPFS oraz aplikację przeglądarkową, która może być uruchamiana lokalnie na urządzeniu końcowym. W wyniku połączenia tych technologii autor opracował system zapewniający poufność, integralność i dostępność przechowywanych danych. Należy zauważyć, że technologia blockchain stanowiła kluczowy element tego rozwiązania. Pozwoliła na wykonywanie operacji kryptograficznych w środowisku rozproszonym, przy jednoczesnym zachowaniu poufności przechowywanych i przetwarzanych danych. Przedstawione w pracy schematy oraz załączone fragmenty kodów źródłowych wskazują na oryginalność rozwiązania postawionego problemu. Wykorzystane technologie wskazują na szeroką wiedzę mgra inż. Kamila Kaczyńskiego w zakresie praktycznego zastosowania posiadanej wiedzy teoretycznej w dyscyplinie informatyka techniczna i telekomunikacja. Oceniam, iż przedstawiona rozprawa prezentuje oryginalne rozwiązanie problemu naukowego, tym samym spełniając pkt 1 art. 187 ustawy Prawo o szkolnictwie wyższym i nauce.

Praca została napisana językiem poprawnym, właściwym dla tego typu opracowań. W dokumencie można odnaleźć nieliczne literówki, błędy interpunkcyjne i gramatyczne, które nie mają większego wpływu na pozytywny odbiór pracy, np. „*serwerów usługodawcy, przechowujących treść objętych cenzurą*" zamiast „*serwerów usługodawcy, przechowujących treść objętą cenzurą*". Autor zamieścił w pracy obszerną listę skrótów, jednak mimo wszystko nie jest ona kompletna. Przykładowo, w pracy możemy znaleźć odwołanie do *HLS*, który to skrót nie został objaśniony w przedstawionym wykazie.

W części praktycznej pracy doktorant zdecydował o wykorzystaniu schematu ECIES wykorzystującego krzywą secp256k1. Krzywa ta posiada znane wady konstrukcyjne, które w szczególności mogą ułatwiać dokonywanie ataków typu side-channel na wykorzystujące ją implementację. Z mojego punktu widzenia dobrze byłoby

w pracy poruszyć ten problem i zasugerować możliwe rozwiązania, lub też w bardziej dosadny sposób wyartykułować potrzebę wykorzystania tejże krzywej w projektowanym systemie. Podobnie, dobrze byłoby w pracy wykorzystać oznaczenia funkcji szyfrującej i deszyfrującej szeroko wykorzystywane w literaturze przedmiotu, tj. odpowiedni *E* i *D* zamiast *Enc* i *Dec*. Uwagi te mają jednakże charakter polemiczny i nie wpływają na moją pozytywną ocenę rozprawy.

Podsumowując niniejszą recenzję uważam, że rozprawa mgr inż. Kamila Kaczyńskiego **spełnia wszystkie wymagania formalne stawiane rozprawom doktorskim** określone przez ustawę z dnia 20 lipca 2018 r. – Prawo o szkolnictwie wyższym i nauce. Doktorant udowodnił swoją szeroką wiedzę teoretyczną z zakresu dyscypliny informatyka techniczna i telekomunikacja, a także postawił problem badawczy, który został przez niego rozwiązany w sposób oryginalny. W związku z powyższym wnioskuję o dopuszczenie mgra inż. Kamila Kaczyńskiego do dalszych etapów przewodu doktorskiego.