prof. dr hab. inż. Radosław Pytlak

Politechnika Warszawska,

Wydział Matematyki i Nauk Informacyjnych

data 10.06.2024

KWESTIONARIUSZ- RECENZJA ROZPRAWY DOKTORSKIEJ DLA RADY WYDZIAŁU INFORMATYKI ZACHODNIOPOMORSKIEGO UNIWERSYTETU TECHNOLOGICZNEGO W SZCZECINIE

Tytuł rozprawy: Zastosowanie zaawansowanych systemów blockchain do wzmacniania odporności systemów informatycznych

Autor rozprawy: mgr inż. Kamil Kaczyński

1. **Jakie zagadnienie naukowe jest rozpatrzone w pracy /teza rozprawy/ i czy zostało ono dostatecznie jasno sformułowane przez autora? Jaki charakter ma rozprawa (teoretyczny, doświadczalny, inny)?**

   Autor postawił w rozprawie doktorskiej następujący hipotezę badawczą:

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

   Ten cel ogólny został następnie doprecyzowany poprzez postawienie kilku hipotez szczegółowych:

   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.

   Autor rozprawy rozwiązuje problem badawczy związany z postawioną główną hipotezą badawczą oraz hipotezami szczegółowymi poprzez przedstawienie koncepcji budowy systemu pozwalającego na uwierzytelniony dostęp do danych zdecentralizowanych, opartego na różnych technologiach blockchain – w tym przypadku Etehereum i Secret Network. Autor rozprawy zakłada, że dane składowane są w sieciach publicznych (czyli w środowisku niezaufanym) – Ethereum, Secret Network oraz IPFS. Autor pokazuje, że wykorzystanie tych technologii pozwala na zachowanie integralności i poufności danych. Ponadto autor ocenia

zaproponowany schemat uwierzytelnionego dostępu do danych.

Teza rozprawy została jasno sformułowana, praca ma charakter projektowy. Należy jednak zaznaczyć, że o ile koncepcja rozwiązania projektowego została przedstawiona to nie wszystkie elementy związane z realizacją projektu zostały w pracy zaprezentowane.

2. **Czy w rozprawie przeprowadzono w sposób właściwy analizę źródeł / w tym literatury światowej, stanu wiedzy i zastosowań w przemyśle /świadczący o dostatecznej wiedzy autora. Czy wnioski z przeglądu źródeł sformułowano w sposób jasny i przekonywujący?**

Przegląd literatury dotyczący tematyki rozprawy jest mocną stroną omawianej rozprawy doktorskiej. Autor rozprawy dokonał wnikliwej analizy stanu wiedzy dotyczącej zaawansowanych systemów blockachin pod kątem ich wykorzystania do postawionego zadania badawczego.

Opis stanu wiedzy związanej z tematyką rozprawy znajduje się w pierwszych czterech rozdziałach rozprawy. Pierwsze dwa rozdziały rozprawy stanowią wprowadzenie do tematyki technologii blockchain pod kątem uzasadnienia podjęcia badań omawianych w rozprawie z uwzględnieniem celów, które muszą być zrealizowane w ich trakcie. W rozdziale pierwszym autor nawiązuje do pierwszych zastosowań technologii blockchain związanych z realizacją płatności z wykorzystaniem tzw. kryptowalut, oraz do wprowadzonych następnie obliczeń wewnątrz sieci blockchain. Autor rozprawy twierdzi, że pełna transparentność transakcji i zawartości technologii blockchain spowodowała brak możliwości realizacji bardziej wymagających przypadków użycia związanych, np. z przepływem danych, które nie powinny zostać upublicznione. Następnie autor rozprawy przekonuje, że wymiana informacji z wykorzystaniem klasycznych technologii informacyjnych wymaga istnienia zaufanych pośredników potwierdzających tożsamość serwerów biorących udział w procesie transmisji danych. Zastosowanie centralnej infrastruktury potwierdzającej tożsamość może prowadzić do ustanowienia cenzury. Autor rozprawy przechodzi następnie do konkluzji, że zastosowanie technologii rejestru rozproszonego pozwoli na decentralizację procesu podejmowania decyzji co bezpośrednio przełoży się na zwiększenie bezpieczeństwa usług oraz uniemożliwi zaistnienia takich zdarzeń jak tych związanych z aferą DigNotar z 2011 roku, kiedy to grupa przestępcza przechwyciła przepływ danych w scentralizowanym systemie przepływu informacji. Na podstawie analizy działania systemów scentralizowanych i zdecentralizowanych autor rozprawy, w rozdziale drugim, formułuje swoją hipotezę badawczą przedstawiając jednocześnie powiązane z nią hipotezy szczegółowe.

W rozdziale trzecim Autor przedstawił pierwszą generację technologii blockchain. W pierwszym podrozdziale przedstawiony został rys historyczny, wskazujący na główne kamienie milowe w rozwoju koncepcji rejestru rozproszonego. W podrozdziale drugim dokładny opis techniczny działania sieci Bitcoin jest przedstawiony. Szczegółowo omówiona jest struktura transakcji, proces tworzenia (kopania) nowych środków oraz dokonana jest analiza metod zabezpieczania transakcji stosowanych w sieci. Opis procesów realizowanych z wykorzystaniem sieci Bitcoin charakteryzuje się dużą szczegółowością, Autor odwołuje się do niskopoziomowych struktur danych oraz omawia mechanizmy kryptograficzne. Istotny wpływ na prawidłowe funkcjonowanie procesów w sieciach Bitcoin mają wykorzystywane algorytmy konsensusu - Autor rozprawy skoncentrował się na opisie następujących metod: Proof of Work, Proof of Stake, Problem Bizantyjskich Generałów, PBFT, IOTA.
W rozdziale czwartym kolejne generacje technologii rejestru rozproszonego, oznaczone jako 2.0 i 3.0, zostały zaprezentowane. W odrębnych podrozdziałach sieci Ethereum, IOTA, Hyperledger Fabric zostały przedstawione, kolejne podrozdziały zostały poświęcone zastosowaniom blockchain nowej generacji oraz technologiom zdecentralizowanego przechowywania danych. W przypadku sieci Ethereum Autor rozprawy koncentruje się na opisie mechanizmów przejścia stanów oraz na typach stosowanych kont. Ponadto Autor rozprawy opisuje specyfikę 'smart' kontraktów, ich wykorzystanie w sieci oraz sposoby obsługi transakcji i wiadomości. W przypadku protokołu IOTA, przeznaczonego do stosowania w Internecie Rzeczy, uwaga Autora została skierowana na strukturę rejestru rozproszonego mającego postać skierowanego grafu acyklicznego oraz na podstawowe algorytmy związane z IOTA takie jak TSA (Tip Selection Algorithm) oraz MAM (Masked Authenticated Messaging). W przypadku rozwiązania Hyperledger Fabric przedstawiona została architektura sieci oraz omówione zostały możliwości wykonywania kodu. W kolejnym podrozdziale różne aspekty technologii zdecentralizowanego przechowywania danych zostały omówione. Autor rozprawy dokonał analizy mechanizmów, w szczególności sposobów adresowania danych, oraz przedstawił protokoły komunikacyjne stosowane do wyszukiwania i dystrybucji danych w systemach Interplanetary File System i Arweave. Podrozdział piąty omawia zastosowanie technologii blockchain 2.0 i 3.0 w realizacji zdecentralizowanych usług. W szczególności Autor skupia się na zdecentralizowanych finansach i autonomicznych organizacjach.

Przedstawiona powyżej zawartość rozdziałów trzeciego i czwartego sprawia wrażenie, że przegląd stanu wiedzy związanej z tematyką rozprawy jest zbyt szczegółowy dla prezentacji wyników wykonanej pracy badawczej, jednak zawartość rozdziału szóstego, w którym przedstawiona jest koncepcja realizacji zdecentralizowanego systemu wymiany danych, temu

przeczy. Dla wykazania zasadności zastosowanych technologii wykorzystywanych w proponowanym rozwiązaniu szczegółowa prezentacja technologii w rozdziałach trzecim i czwartym jest konieczna. Należy ponadto zaznaczyć, że omówienie poszczególnych technologii w tych rozdziałach jest bardzo klarowne.

Przegląd literatury jest bardzo obszerny i obejmuje 192 pozycji, w tym źródeł literaturowych opublikowanych w 2024. Moje główne zastrzeżenie odnoszące się do przeglądu literatury dotyczy skromnego powołania się autora rozprawy na własne prace – w spisie literatury jest tylko jedna pozycja autora rozprawy.

3. **Czy autor rozwiązał postawione zagadnienia, czy użył właściwej do tego metody i czy przyjęte założenia są uzasadnione?**

Szósty rozdział prezentuje autorskie rozwiązanie schematu uwierzytelnionego dostępu do danych w środowisku rozproszonym. Autor wykorzystuje w tym celu połączenie technologii IPFS, Ethereum, Secret Network oraz Web Cryptography API. Rozdział ten składa się z trzech podrozdziałów. W pierwszym podrozdziale Autor opisuje technologię przechowywania sekretów w publicznej sieci blockchain, koncentrując się na przedstawieniu zastosowania technologii Trusted Execution Environment, stosowanego algorytmu konsensusu, a także wykonywanych przez sieć operacji bazodanowych. Drugi podrozdział zawiera opis autorskiej implementacji mechanizmów autoryzacji wykorzystujący 'smart' kontrakty sieci Ethereum i Secret Network. Autor przedstawia fragmenty kodów źródłowych odpowiedzialne za realizację krytycznych funkcjonalności - listingi kodów w językach Solidity, Rust i JavaScript są zamieszczone. Weryfikacja założonych wymagań niefunkcjonalnych, składająca się na ocenę zaproponowanego schematu, przedstawiona jest w podrozdziale trzecim. Uwaga Autora skupiona jest na wykorzystywanych prymitywach kryptograficznych w kontekście zapewniania integralności, poufności oraz dostępności przechowywanych danych. Możliwe hipotetyczne podatności tak skonstruowanego schematu są omawiane.

Tytuł rozprawy doktorskiej sugeruje, że praca nie dotyczy tylko sytemu informatycznego realizującego uwierzytelniony dostęp do danych w środowisku rozproszonym. Zakładam, że uzasadnieniem takiego sformułowania tytułu rozprawy jest zawartość rozdziału piątego rozprawy, w którym przedstawiono opis autorskich propozycji zastosowania technologii rejestru rozproszonego do zapewniania integralności i dostępności danych, a także realizacji obliczeń rozproszonych. Rozdział podzielony został na trzy podrozdziały poruszające odpowiednio każdy z wcześniej wymienionych tematów. Pierwszy podrozdział przedstawia autorskie propozycje wykorzystania rejestru rozproszonego do realizacji systemu

monitorowania łańcucha dostaw produktów medycznych. Kolejny podrozdział przedstawia autorską koncepcję zwiększenia dostępności do informacji w przypadku wystąpienia sytuacji kryzysowych lub ograniczeń łączności. Autor wykorzystuje technologie IPFS w kontekście udostępniania zasobów w sieciach publicznych i prywatnych. Ostatni podrozdział przedstawia autorską koncepcję wykorzystania blockchain do implementacji zdecentralizowanej autonomicznej organizacji mającej za zadanie zarządzanie rojem dronów. Autor dokonuje porównania dwóch możliwych do wykorzystania technologii – Hyperledger Fabric oraz IOTA oraz ich integracji ze składowaniem danych w IPFS.

Autor rozprawy rozwiązał postawione przez siebie zadanie badawcze prezentując koncepcje systemów informatycznych wykorzystujących technologie blockchain w celu zwiększenia odporności systemów informatycznych. Przedstawione koncepcje rozwiązań omówione są w różnym stopniu ogólności, przy czym koncepcje rozwiązań zaprezentowane w rozdziale piątym stanowią, w mojej opinii, zarys koncepcji. Propozycja systemu omówiona w rozdziale szóstym jest najbardziej kompletna i towarzysząca jej analiza dotycząca zapewnienia poufności poprzez wykorzystanie mechanizmów kryptograficznych oraz analiza zapewnienia dostępności danych dają gwarancje spełnienia wymagań funkcjonalnych i niefunkcjonalnych dla systemu. Ponadto koncepcja systemu opisana w rozdziale szóstym uzupełniona jest o pewne szczegóły implementacyjne poprzez zaprezentowanie szczegółowych rozwiązań na poziomie skryptów języków programowania.
Niemniej rozprawa doktorska zyskałaby wyższą ocenę, gdyby autor rozprawy skoncentrowałby się na realizacji koncepcji przedstawionej w rozdziale szóstym i przedstawiłby wyniki testów zrealizowanego systemu informatycznego uwzględniające wydajność systemu, jego skalowalność oraz koszty użytkowania.

4. **Czy autor wykazał umiejętność poprawnego i przekonywującego przedstawienia uzyskanych przez siebie wyników /zwięzłość, jasność, poprawność redakcyjna rozprawy/?**

Autor przyjął właściwy układ rozprawy. W rozdziale pierwszym autor przekonuje o zasadności podjęcia badań nad tematyką rozprawy W rozdziale drugim przedstawiono problemy badawcze występujące przy podjęciu zaproponowanej tematyki i wynikające z nich hipotezy badawcze. W kolejnych dwóch rozdziałach omówione są obszernie technologie, które będą wykorzystywane przy realizacji celów badawczych z krytyczną ich analizą i w takim zakresie, aby możliwe było zaprezentowanie koncepcji realizacji celów badawczych. Oryginalne rozwiązania autora przedstawione są w rozdziałach piątym i szóstym. Rozdział siódmy zawiera podsumowanie wyników badań, weryfikację spełnienia postawionych hipotez badawczych i wnioski dotyczące możliwości wykorzystania uzyskanych wyników. Pozostała

część pracy to spis literatury, rysunków i tabel.

Praca przedstawia w sposób zwięzły i jasny uzyskane przez autora rozprawy wyniki. Ponadto praca jest napisana bardzo starannie. Uwagi dotyczące strony redakcyjnej odnoszą się przede wszystkim do dwóch kwestii: 1) nieuzasadnionego wprowadzenia definicji w opisach, np. Definicji 3.3 grafu skierowanego; 2) wykorzystywanie pewnych funkcji do definicji innych funkcji, przy jednoczesnej prezentacji tych funkcji kilka stron dalej, np. funkcja 'R' na str. 116 jest określona poprzez funkcje 'Enc' oraz 'Dec', które przedstawione są na stronach 123 oraz 124 odpowiednio.

5. Jakie są słabe strony rozprawy i jej główne wady?

Autor rozprawy prezentuje koncepcje rozwiązań systemów informatycznych. Ponieważ koncepcje te nie zostały zrealizowane w postaci systemów informatycznych pełna ich ocena nie jest możliwa ze względu na brak, np. testów wydajnościowych implementacji.

Mimo powyższej uwagi moja ocena wykonanej przez Autora pracy jest wysoka.

6. Podsumowanie

Podsumowując recenzję, biorąc pod uwagę powyższe opinie i wymagania zawarte w art. 187 Ustawy z dnia 20 lipca 2018 r. – Prawo o szkolnictwie wyższym i nauce (Dz. U. 2023 poz. 742)., stwierdzam, że rozprawa mgra inż. Kamila Kaczyńskiego pt. „Zastosowanie zaawansowanych systemów blockchain do wzmacniania odporności systemów informatycznych" spełnia wymagania stawiane pracom doktorskim w dyscyplinie informatyka techniczna i telekomunikacja, w szczególności:

- rozprawa zawiera oryginalne rozwiązanie problemu naukowego w dyscyplinie informatyka techniczna i telekomunikacja
- kandydat posiada ugruntowaną, głęboką wiedzę w dyscyplinie informatyka techniczna i telekomunikacja
- kandydat posiada umiejętność samodzielnego prowadzenia pracy naukowej.

Wnoszę o jej przyjęcie i dopuszczenie do dalszych etapów postepowania doktorskiego.

Radosław Pytlak

podpis