dr hab. inż. Zbigniew Tarapata, prof. WAT
Wydział Cybernetyki
Wojskowa Akademia Techniczna
ul. Gen. S. Kaliskiego 2, 00-908 Warszawa
e-mail: zbigniew.tarapata@wat.edu.pl

Warszawa, 09.12.2024 r.

RECENZJA ROZPRAWY DOKTORSKIEJ

(na zlecenie Rady Wydziału Nauk o Bezpieczeństwie Uniwersytetu Andrzeja Frycza Modrzewskiego w Krakowie, zgodnie z uchwałą nr 3/2024 z dn. 25.10.2024 r.)

Tytuł Rozprawy: *Bezpieczeństwo transakcji biznesowych przy wykorzystaniu rejestrów rozproszonych*
Autor rozprawy: mgr inż. Bartosz Lewandowski
Promotor rozprawy: ks. dr hab. Mirosław Michalski, prof. ChAT

1. Cel badań - tezy rozprawy

Rozprawa poświęcona jest praktycznemu wykorzystaniu technologii blockchain w kontekście bezpieczeństwa transakcji cyfrowych. Zadanie, którego podjął się Doktorant jest dość ambitne, bardzo istotne z punktu widzenia bezpieczeństwa cyfrowego, wymagające wiedzy z wielu dziedzin: organizacji i zarządzania, legislacji, informatyki, cyberbezpieczeństwa. Celem badań prowadzonych w rozprawie jest wskazanie na praktyczne wykorzystanie technologii blockchain w zakresie podniesienia bezpieczeństwa przechowywania oraz audytowania danych cyfrowych w aspekcie technicznym, organizacyjnym oraz prawnym. Bezpieczeństwo cyfrowe obejmuje szeroki wachlarz procedur skierowanych na ochronę systemów komputerowych, sieci oraz przetwarzanych danych przed nieautoryzowanym dostępem lub uszkodzeniem. Istotne jest wszędzie tam, gdzie mamy do czynienia m.in. z przetwarzaniem danych wrażliwych w systemach teleinformatycznych. Ma zastosowanie w bankowości, medycynie, rejestrach publicznych i innych obszarach. W rozprawie wyeksponowano obszary takie, jak bezpieczeństwo transportu oraz przechowywania żywności i leków, bezpieczeństwo zapisu i dostępu do dokumentacji medycznej, bezpieczeństwo systemów informatycznych. Wskazane obszary, dzięki technologii blockchain, radykalnie zwiększają bezpieczeństwo konsumentów w relacji do przedsiębiorstw oraz organizacji. Blockchain jako nowoczesna technologia wprowadzona z kryptowalutą Bitcoin, prezentuje filozofię zdecentralizowanego (rozproszonego) systemu przetwarzania danych w postaci tzw. łańcuchów bloków, który dzięki swoimi podstawowym cechom charakterystycznym: gwarancji niezmienności i integralności danych, pełności i trwałości danych, bezpieczeństwa tych danych i audytowalności stał się technologią przełomową. W wielu krajach trwają ciągłe prace nad usprawnianiem rozwiązań formalno-prawnych, organizacyjno-funkcjonalnych oraz technicznych poprawiających bezpieczeństwo cyfrowe sieci teleinformatycznych oraz systemów z nich korzystających. Recenzowana rozprawa wpisuje się w te prace.

Cele pracy badawczej zostały sformułowane w następujący sposób:

TA

1. Cel teoretyczny – opracowanie modelu mechanizmu trwałego nośnika przy wykorzystaniu protokołu blockchain oraz wypracowanie metod podniesienia poziomu bezpieczeństwa działania przedsiębiorstw i możliwości ograniczania ryzyka w działalności gospodarczej.
2. Cel poznawczy – wskazanie metod podniesienia bezpieczeństwa przetwarzania informacji oraz umacniania zaufania do rozwiązań cyfrowych poprzez wybór mechanizmu konsensusu w zapisach transakcji w sieci blockchain przy uwzględnieniu przetwarzania dużej liczby operacji, ze szczególnym uwzględnieniem instytucji finansowych, FMCG, medycznych.
3. Cel praktyczny – budowa rozproszonej sieci blockchain realizującej praktycznie mechanizm trwałego nośnika.
Autor definiuje również 8 celów szczegółowych.

Autor rozprawy stawia następującą hipotezę badawczą:

Przypuszcza się, że rozproszone sieci blockchain mają wpływ na bezpieczeństwo organizacji poprzez zapewnienie jej zgodności z wymaganiami regulatorów rynkowych, a wymagania prawne stawiane przez prawo UE oraz krajowe względem rozwiązania zaproponowanego jako cel badania zostaną prawidłowo zaadresowane. Zakłada się, że rozwiązanie będzie mogło implementować prawo do zapomnienia pod warunkiem zapisu w protokole blockchain skrótów dokumentów.

Autor następnie definiuje **hipotezy szczegółowe**:

1. *Cele stawiane mechanizmowi cyfrowego trwałego nośnika w kontekście ustawodawstwa krajowego i europejskiego oraz wynikające z nich potrzeby technologiczne są przypuszczalnie rozwiązane poprzez technologię blockchain.*
2. *Bezpieczeństwo prawne przedsiębiorstwa wynikające z realizacji wymogów ustaw w zakresie komunikacji z konsumentem prawdopodobnie zwiększy poziom bezpieczeństwa operacyjnego przedsiębiorstwa wdrażającego tego typu technologie do swoich procesów. Zabezpieczone zostaną m.in. takie procesy prowadzone przez nowoczesną organizację, jak transparentność działania, ochrona informacji, digitalizacja procesów.*
3. *Rozwiązanie blockchain, biorąc pod uwagę koszt, licencje, dostępność technologii, jest potencjalnie korzystniejsze od alternatywnych rozwiązań, które mogą być wykorzystane do implementacji cyfrowego trwałego nośnika.*
4. *Aktualnie dostępne technologie blockchain wraz z algorytmami optymalizującymi zapis danych prawdopodobnie pozwolą na hurtowe zapisywanie dokumentów.*
5. *Prawdopodobnie wszelkie zagrożenia związane z wdrożeniem protokołu blockchain można zidentyfikować i wykluczyć. Główne zagrożenie to wyciek danych, dlatego nie należy publikować dokumentów, lecz wyniki funkcji skrótu. Równocześnie bezpieczeństwo potencjalnie się zwiększy poprzez wprowadzenie audytowalności danych na węzłach blockchain – zawsze będzie można zweryfikować pochodzenie informacji.*
6. *Potencjalnie konsensus odpowiada za bezpieczeństwo protokołu – jego odpowiedni dobór zabezpiecza sieć przed atakiem. Wymagający konsensus, np. odporny na ataki 51%, zapewnia bezpieczeństwo danych.*
7. *Aktualny stan technologiczny pozwala przypuszczać, że implementacja rozwiązania mechanizmu trwałego nośnika w oparciu o technologię blockchain jest możliwa i zapewnia zgodność z krajowym oraz unijnym ustawodawstwem.*

Doktorant w rozprawie zdefiniował następujące szczegółowe problemy badawcze, które skojarzone są z przedstawionymi hipotezami szczegółowymi:
1. Czy i w jakim zakresie rozwiązanie blockchain pokrywa obszary zdefiniowane w prawie krajowym oraz europejskim związane z zagadnieniem cyfrowego trwałego nośnika, zapewniając bezpieczeństwo przechowywanych informacji poprzez trwały, integralny oraz audytowany zapis danych?
2. Czy wdrożenie technologii blockchain w organizacji zwiększy bezpieczeństwo prawne i operacyjne podmiotów gospodarczych, zapewniając transparentność działania, ochronę informacji, bezpieczne digitalizowanie procesów i jednocześnie uchroni organizację od potencjalnego ryzyka prawnego?
3. W jakim zakresie wdrożenie sieci blockchain jest dla przedsiębiorstwa lub organizacji ekonomicznie uzasadnione w kontekście alternatywnych rozwiązań oraz na ile zapewnia bezpieczeństwo ekonomiczne?
4. W jaki sposób wydajność protokołu blockchain umożliwi działanie na hurtowej ilości danych, co pozwoli na wykorzystanie technologii w operacjach masowych, które liczone są w milionach dziennie?
5. Na ile zwiększy się bezpieczeństwo organizacji w kontekście przechowywania danych, w szczególności pod kątem narażenia na cyberataki i ochrony niezmienności danych?
6. W jaki sposób osiągnięty konsensus zapewnia bezpieczeństwo transakcjom, tak by możliwość ich fałszowania była minimalna, a co za tym idzie, by zapis spełniał prawne formy cyfrowego trwałego nośnika w zakresie zachowania dostępu do oryginalnych danych?
7. W jaki sposób możliwa jest implementacja rozwiązania cyfrowego trwałego nośnika, zgodnego z obowiązującym prawem, w oparciu o technologię blockchain?

Tytuł rozprawy, cele badań, hipoteza badawcza, hipotezy szczegółowe i problemy badawcze zostały sformułowane w sposób dość przejrzysty, chociaż nie rozumiem za bardzo sformułowania pierwszej hipotezy szczegółowej. Z treści hipotezy wynika, że cele [...] oraz [...] „wynikające z nich potrzeby są przypuszczalnie rozwiązane przez technologię blockchain". Cele się przecież realizuje a potrzeby zaspokaja, stąd moje niezrozumienie. Ciekaw również byłem jak Doktorant poradzi sobie z odpowiedzią na pytanie badawcze nr 5: „Na ile zwiększy się bezpieczeństwo [...]". Już samo sformułowanie pytania wprowadza komplikacje przy odpowiedzi na nie.
W dalszej części recenzji odniosę się szczegółowo do poszczególnych elementów składowych rozprawy.

2. Charakter rozprawy (teoretyczny, doświadczalny, projektowy, konstrukcyjny, technologiczny)

Rozprawa ma generalnie charakter teoretyczny, choć znajdują się w niej również elementy eksperymentowania opartego na symulacji komputerowej. Autor najpierw dokonał analizy aktów prawnych obowiązujących w Polsce oraz w Unii Europejskiej. Zbadał dziedziny, których wymóg trwałego nośnika dotyka, w szczególności prawo bankowe, akty związane z ochroną konsumentów, prawo cywilne i przepisy dotyczące usług elektronicznych. Opisał obszary, w których cyfrowy trwały nośnik potencjalnie zwiększy bezpieczeństwo prowadzenia transakcji, transparentność procesów oraz zaufanie do systemów informatycznych, uniemożliwiając nieautoryzowane operacje. Następnie, w aspekcie technicznym i technologicznym, wykazał, że blockchain, poprzez swoją architekturę, zapewnia niezmienność przechowywanych danych oraz wysoki poziom bezpieczeństwa

i integralności danych, co jest kluczowe dla ochrony interesów konsumentów. Wykazywał również, że transakcje w protokole blockchain są zapisane w sposób trwały i łatwo weryfikowalny, co sprzyja transparentności procesów i ułatwia audyty, zwiększając tym samym zgodność technologii z wymogami RODO. W aspekcie praktycznym, Doktorant pokazał działanie mechanizmu trwałego nośnika na bazie technologii blockchain, poprzez własną implementację przykładowego rozwiązania. Zaproponował też architekturę sieci blockchain w podmiocie leczniczym.
Wspomniane aspekty technologiczno-techniczne są bardzo mocno akcentowane w rozprawie, co świadczy o dużej wiedzy Autora z tego obszaru i powoduje, że rozprawa ma charakter interdyscyplinarny.

3. Sposób przeprowadzenia analizy źródeł (w tym literatury światowej) i formułowania wniosków z analizy

Recenzowana rozprawa zawiera 104 pozycje źródłowe, z czego 56 to źródła internetowe. Zakres tematyczny pozycji źródłowych obejmuje szerokie spektrum problemów, którymi zajmuje się w rozprawie Autor: od aktów legislacyjnych, raportów, po monografie i artykuły naukowe. Przegląd i analizę źródeł Autor rozprawy przeprowadził w rozdziałach 1÷3. W rozdziale 1 Doktorant, według mnie zupełnie niepotrzebnie, przywołuje szereg definicji z metodologii badań dotyczących celu badań, problemów badawczych, hipotez itd. Doktorant powinien znać te pojęcia, bo sam je w pracy musiał formułować, ale powoływanie się na ich definicje w literaturze dotyczącej metodologii badań to już nadmierna przesada. Doktorant nie wykonuje przecież badań w obszarze metodologii badań. W rozdziale 2 Doktorant zapoczątkował analizę źródeł przeglądem i opisem aktów prawnych związanych z bezpieczeństwem informacji oraz bezpieczeństwem społeczeństwa cyfrowego, następnie opisywał problemy związane z zagrożeniami systemów informatycznych. W dalszej kolejności scharakteryzował technologię blockchain oraz jej zastosowania, powołując się na szereg różnych źródeł zarówno w postaci publikacji naukowych, jak i raportów, czy źródeł internetowych. Dokonuje również charakterystyki technologii/standardu NFT (ang. *Non-Fungible Token*). W rozdziale 3 Doktorant rozpoczyna przegląd literatury od trwałego nośnika danych, powołując się na akty prawne i wynikające z nich prawo do bycia zapomnianym, integralność i niezmienność informacji. W dalszej części analizuje akty prawne dotyczące formy pisemnej, formy dokumentowanej oraz formy elektronicznej dokumentu oraz przy propozycji własnego rozwiązania analizuje technologię WORM i związane z elektroniczną dokumentacją medyczną.

Wnioski z przeprowadzonych analiz są poprawne i wykorzystywane w dalszych częściach rozprawy. Uważam jednak, że analiza źródeł mogła być szersza a ich zakres precyzyjniej dobrany. W szczególności brakuje szerszego odniesienia do bogatej przecież literatury dotyczącej bezpieczeństwa systemów teleinformatycznych oraz bezpieczeństwa samych transakcji cyfrowych.

4. Rozwiązanie zdefiniowanych problemów, właściwość przyjętych metod i założeń

Przedstawiona do recenzji rozprawa doktorska liczy ogółem 225 stron. We wstępie Autor wprowadza w tematykę rozprawy. W rozdziale 1, na 13 stronach, Doktorant definiuje hipotezę badawczą, siedem hipotez szczegółowych, dziewięć celów szczegółowych badań oraz siedem pytań badawczych, na które udzielone odpowiedzi mają pomóc w realizacji celów oraz potwierdzeniu przyjętych hipotez szczegółowych. W rozdziale 2, na 55 stronach, Autor dokonuje przeglądu związanego z bezpieczeństwem informacji oraz bezpieczeństwem społeczeństwa cyfrowego, jak

również zagrożeniami systemów informatycznych. W dalszej kolejności charakteryzuje technologię blockchain oraz jej zastosowania. Dokonuje również charakterystyki technologii/standardu NFT. Rozdział 3, najobszerniejszy w pracy, bo liczący 85 stron, zawiera wyniki badań własnych Doktoranta. W nim też znajdują się odpowiedzi na wszystkie pytania badawcze. Szczegółowo o zawartości tego rozdziału, najistotniejszego z punktu widzenia rozprawy, napiszę dalej w tej części recenzji. W rozdziale 4, liczącym 34 strony, Autor przedstawia przegląd dostępnych technologii blockchain ze szczególnym uwzględnieniem wymagań związanych z implementacją trwałego nośnika danych, jak również rodzaje architektury blockchain w kontekście sieci prywatnych, publicznych oraz hybrydowych. W rozdziale tym podjęto również badania dotyczące części teoretycznej, w której analizowane są modele danych oraz wydajność systemu. Zakończenie rozprawy zawiera uzasadnienie potwierdzenia szczegółowych hipotez badawczych oraz perspektywy wykorzystania trwałego nośnika danych realizowanego z wykorzystaniem technologii blockchain.

Autor w rozprawie, do przeprowadzenia badań, wykorzystał metody teoretyczne (w szczególności analizę, syntezę, porównanie, wnioskowanie) oraz empiryczne, w szczególności obserwację oraz symulację komputerową. Zaproponowane metody są właściwe.

Przejdę teraz do szczegółowej oceny poszczególnych części rozprawy.

Dokonana w rozdziale 2 analiza aktów prawnych związanych z bezpieczeństwem informacji, bezpieczeństwem społeczeństwa cyfrowego i zagrożeniami systemów informatycznych, a następnie charakterystyka technologii blockchain oraz jej zastosowań, jak również technologii/standardu NFT przedstawiona jest bardzo rzetelnie i z niewątpliwą znajomością tematu oraz wyczuciem interdyscyplinarnym. Wnioski wynikające z tej analizy, które Autor rozprawy przedstawia na bieżąco wykorzystywane są w dalszej części rozprawy oraz stanowią uzasadnienie potrzeby badań w prezentowanym w rozprawie obszarze.

W rozdziale 3, najistotniejszym w rozprawie, Autor przedstawia wyniki badań własnych. Odpowiedzi na każde z siedmiu pytań badawczych (przedstawionych przeze mnie w części 1 recenzji), skojarzonych z siedmioma hipotezami szczegółowymi, można odnaleźć w różnych częściach tego rozdziału. Zidentyfikowałem je głównie w następujących podrozdziałach:

- dla problemu badawczego nr 1 – rozdział 3.1.1;
- dla problemu badawczego nr 2 – rozdział 3.1.2;
- dla problemu badawczego nr 3 – rozdział 3.2;
- dla problemu badawczego nr 4 – rozdział 3.8;
- dla problemu badawczego nr 5 – rozdział 3.3;
- dla problemu badawczego nr 6 – rozdział 3.4;
- dla problemu badawczego nr 7 – rozdział 3.9.

W podrozdziale 3.1.1, w którym Doktorant odpowiada na pytanie badawcze nr 1 (Czy i w jakim zakresie rozwiązanie blockchain pokrywa obszary zdefiniowane w prawie krajowym oraz europejskim związane z zagadnieniem cyfrowego trwałego nośnika, zapewniając bezpieczeństwo przechowywanych informacji poprzez trwały, integralny oraz audytowany zapis danych?), najpierw definiuje pojęcie trwałego nośnika, czyli takiego, który „umożliwia użytkownikowi przechowywanie adresowanych do niego informacji w sposób umożliwiający dostęp do nich przez okres odpowiedni do celów, którym te informacje służą, i pozwalający na odtworzenie przechowywanych informacji w niezmienionej postaci" (definicja z *Prawa bankowego*). Następnie Doktorant w przekonujący sposób uzasadnia, powołując się na analizę rozwiązań prawnych oraz wnioskowanie oparte o cechy charakterystyczne technologii blockchain, że rozwiązania technologiczne w oparciu o blockchain spełniają założenia wynikające z definicji trwałego nośnika, w tym te związane z bezpieczeństwem

przechowywanych informacji. Doktorant dokonuje też bardzo ciekawego porównania skutków prawnych czynności prawnej w formie elektronicznej, tj. opatrzonej kwalifikowanym podpisem elektronicznym, oraz czynności w formie dokumentu elektronicznego wytworzonego przez system teleinformatyczny i podpisanego przez trwały nośnik na sieci blockchain. Otóż, zgodnie z wnioskami Doktoranta, dokument elektroniczny udostępniony w technologii blockchain nie jest oświadczeniem woli w formie elektronicznej, które byłoby równoważne formie pisemnej czynności prawnej. Natomiast jeśli użytkownik posługiwał się kwalifikowanym podpisem elektronicznym, podpisał dokument w postaci elektronicznej takim podpisem, a następnie zapisał dokument na trwałym nośniku w technologii blockchain, to taki dokument ma podwójny walor: jest równoważny formie pisemnej oświadczenia woli (czynności prawnej), a także posiada cechy nośnika trwałego. Do tej części rozprawy mam w zasadzie następującą uwagę: zastrzeżenie co do lokalizacji definicji trwałego nośnika, która znajduje się przecież w rozdziale poświęconym wynikom badań własnych Doktoranta. Według mnie część teoretyczna, dotycząca definicji trwałego nośnika, powinna być w rozdziale teoretycznym, czyli drugim, a w tym rozdziale wyłącznie wyniki wnioskowania przeprowadzonego przez Doktoranta.

W podrozdziale 3.1.2, w którym Doktorant odpowiada na pytanie badawcze nr 2 (Czy wdrożenie technologii blockchain w organizacji zwiększy bezpieczeństwo prawne i operacyjne podmiotów gospodarczych, zapewniając transparentność działania, ochronę informacji, bezpieczne digitalizowanie procesów i jednocześnie uchroni organizację od potencjalnego ryzyka prawnego?), bazując na uzasadnieniu i wnioskach przedstawionych w rozdziale 3.1.1, że trwały nośnik zbudowany na sieci blockchain posiada cechy trwałego nośnika oraz spełnia wymagania prawne dostarczenia informacji na trwałym nośniku. Doktorant uzasadnia odpowiedź twierdzącą na to pytanie badawcze, z czym należy się zgodzić.

W podrozdziale 3.2, w którym Doktorant odpowiada na pytanie badawcze nr 3 (W jakim zakresie wdrożenie sieci blockchain jest dla przedsiębiorstwa lub organizacji ekonomicznie uzasadnione w kontekście alternatywnych rozwiązań oraz na ile zapewnia bezpieczeństwo ekonomiczne?), przedstawia analizę kosztów wdrożenia oraz utrzymania mechanizmu trwałego nośnika w oparciu o blockchain. Doktorant dokonuje porównania kosztów związanych z dostarczaniem powiadomień do klientów, poprzez porównanie usług pocztowych oraz z wykorzystaniem cyfrowego trwałego nośnika. Dokonuje prostych kalkulacji kosztów wysyłki powiadomień do klientów banków (zakładając, że jest około 58,6 mln kont bankowych) tradycyjną pocztą oraz po implementacji technologii blockchain. Założył, że sieć blockchain będzie składać się z trzech węzłów (jeden dla zaufanej trzeciej strony, jeden dla organizacji oraz jeden administracyjny) i wycenił koszt utrzymania sieci składającej się z trzech serwerów na 10 lat (okres prawny wymagany dla dokumentów). Porównując koszty wysyłania tradycyjnych papierowych powiadomień oraz powiadomień elektronicznych z wykorzystaniem sieci blockchain dochodzi do wniosku, że to drugie rozwiązanie jest dużo tańsze. Szczerze mówiąc nie za bardzo rozumiem sens takiego porównania. Po pierwsze, banki mają wprawdzie obowiązek informowania klientów, ale mogą to robić również elektronicznie, za zgodą klienta, np. z wykorzystaniem poczty elektronicznej. Po drugie: dlaczego Autor przyjął wyłącznie koszty dostępu do serwerów (plus ewentualnie dostępu do macierzy WORM), a nie uwzględnił kosztów wdrożenia i utrzymania systemu dostępu do sieci blockkchain (choćby takich, o których pisze w rozdziale 4 rozprawy)?

W podrozdziałach 3.9.1÷3.9.6, w których Doktorant odpowiada na pytanie badawcze nr 4 (W jaki sposób wydajność protokołu blockchain umożliwi działanie na hurtowej ilości danych, co pozwoli na wykorzystanie technologii w operacjach masowych, które liczone są w milionach dziennie?),

przedstawił opis sposobu komputerowej implementacji mechanizmów głosowania, co umożliwiło pokazanie, jak można efektywnie zarządzać masowymi operacjami i je księgować. Rozważania dotyczą zarówno technicznych aspektów problemu takich, jak wybór odpowiednich algorytmów i narzędzi, jak i kwestii organizacyjnych, w tym zarządzania danymi i zapewnienia bezpieczeństwa operacji. Doktorant założył, że głosowanie dotyczy wszystkich uprawnionych do głosowania w Polsce (ok. 30 mln osób), a czas trwania głosowania to 14 godzin (taki, jak czas otwarcia lokali wyborczych). Doktorant wykonał symulację rejestrowania 50000 głosów na modelu sieci blockchain składającej się z dwóch węzłów pracujących w zwirtualizowanym środowisku, przy założeniu braku opóźnień czasowych. Takie rozwiązanie było niesatysfakcjonujące (wydajność rejestrowania średnia 1,12 transakcji na sekundę, maksymalnie 600). Następnie Doktorant przeprowadził eksperyment symulacyjny przy założeniu rejestrowania transakcji przez bufor. Zaproponował schemat procesu głosowania po tej modyfikacji. To rozwiązanie, na podstawie wyników symulacji, jest już satysfakcjonujące (wydajność rejestrowania rzędu 250 tys. transakcji na sekundę). Do tej części rozprawy mam kilka uwag. Po pierwsze, według mnie Doktorant zastosował zbyt prosty model symulacyjny z dwoma węzłami, bez opóźnień komunikacyjnych. Po drugie, Doktorant nie pokusił się o wprowadzenie nawet prostego, ale jednak mechanizmu opóźnień losowych między węzłami czy losowych czasów rejestracji – wykonał w zasadzie symulację deterministyczną otrzymując – co oczywiste – liniową zależność czasu księgowania od liczby transakcji (rejestracji).

W podrozdziale 3.3 Doktorant odpowiada na pytanie badawcze nr 5 (Na ile zwiększy się bezpieczeństwo organizacji w kontekście przechowywania danych, w szczególności pod kątem narażenia na cyberataki i ochrony niezmienności danych?). Doktorant argumentuje, że aby zapis informacji był bezpieczny, czyli informacja nie mogła być odczytana przez osoby nieuprawnione, proponuje zastosowanie mechanizmu przechowywania skrótów dokumentów, wygenerowanych przez tzw. funkcję skrótu (jednokierunkową). Pozostałe warunki bezpieczeństwa danych (integralność, niezmienność) zapewnia sama technologia blockchain. Zastrzeżenie jakie mam do tej części rozprawy wynika ze sposobu sfomułowania samego pytania badawczego, napisałem to w pierwszej części rozprawy. De facto Doktorant nie odpowiedział na pytanie: „Na ile zwiększy się bezpieczeństwo [...]". Argumentuje jedynie, że się zwiększy, ale nie wiadomo na ile. I jak to zmierzyć? Pytania badawcze trzeba stawiać w taki sposób, aby dało się na nie odpowiedzieć.

W podrozdziale 3.4 Doktorant odpowiada na pytanie badawcze nr 6 (W jaki sposób osiągnięty konsensus zapewnia bezpieczeństwo transakcjom, tak by możliwość ich fałszowania była minimalna, a co za tym idzie, by zapis spełniał prawne formy cyfrowego trwałego nośnika w zakresie zachowania dostępu do oryginalnych danych?). Doktorant opisuje dwanaście mechanizmów ustalania konsensusu w sieci blockchain analizując ich słabe i mocne strony. W szczególności koncentruje się na mechanizmie *Proof of Authority*, który wybrał do późniejszej implementacji opisanej w podrozdziale 3.9. Doktorant przekonująco uzasadnia sposób zapewnienia bezpieczeństwa transakcji przez mechanizmy konsensusu.

W podrozdziale 3.9.9 Doktorant odpowiada na pytanie badawcze nr 7 (W jaki sposób możliwa jest implementacja rozwiązania cyfrowego trwałego nośnika, zgodnego z obowiązującym prawem, w oparciu o technologię blockchain?). Doktorant najpierw zaproponował organizację (architekturę) sieci blockchain dla trwałego nośnika w połączeniu z technologią WORM (ang. Write Once, Read Many) oraz wykorzystaniem tzw. zaufanej trzeciej strony, reprezentowanej prze węzeł zaufany. Opisał szczegóły techniczne implementacji związane z zapisem danych, wykorzystaniem bufora czasu, zmiennymi adresami portfela oraz z samym oprogramowaniem. Proponuje obliczać skróty dokumentów nie na serwerze, ale w kliencie. Najbardziej dostępnym klientem jest przeglądarka

internetowa, a naturalnym językiem implementacji język JavaScript. Zauważa, że realizacja obliczania skrótu dokumentu może być wykonana przy wykorzystaniu biblioteki CryptoJS. Tak obliczony skrót zostanie zapisany w sieci blockchain. Przykładowe implementacje sieci blockchain zostały oparte na technologii Multichain. Całe listingi kodów, zarówno po stronie serwera, jak i po stronie klienta, zamieszczone są w załączniku rozprawy zawierającym kody źródłowe. Ta część rozprawy ma bardzo praktyczny charakter, Doktorant wykazał się przy okazji interdyscyplinarną wiedzą z projektowania aplikacji internetowych, bezpieczeństwa systemów informatycznych oraz samej technologii blockchain.

W rozdziale 4 Doktorant dokonał analizy porównawczej dziewięciu dostępnych technologii blockchain. Rozdział ten stanowi swego rodzaju „spinacz" dla wszystkich pytań badawczych, gdyż analizując i porównując technologie blockchain Doktorant niejako dotyka każdego aspektu poruszanego w pytaniach badawczych. Doktorant zaproponował metodę porównania opartą o cztery grupy kryteriów: (1) koszty i licencja, (2) rozwojowość, (3) prywatność i bezpieczeństwo, (4) łatwość implementacji. Każda z grup miała zdefiniowane kryteria cząstkowe (k.cz.): (1) – 2 k.cz., (2) – 7 k.cz., (3) – 2 k.cz., (4) – 5 k.cz. Wartość każdego kryterium była liczbą z przedziału [0,100] wyliczoną na podstawie najczęściej sumy wartości kryteriów cząstkowych podzielonych przez sumę maksymalnych wartości kryteriów cząstkowych, całość przemnożona przez 100. Analiza jest interesująca, zaproponowana metoda porównań technologii zgodna ze sztuką (choć dość uproszczona), wnioski z niej wyciągnięte ciekawe, łącznie z rekomendacjami (technologia Multichain). Moje uwagi do tej części są następujące. Mało precyzyjnie zapisano formuły (str. 174-175) wyliczające wartość każdego kryterium (np. wszystkie kryteria oznaczone jako „w", wartość w każdym kryterium dzielona przez „waga" podczas, gdy ta jest inna dla trzech z czterech kryteriów (2, 11, 3, 11), bo jest sumą maksymalnych wartości kryteriów cząstkowych). Doktorant napisał, że „Suma końcowa to średnia poszczególnych punktów". Znowu mało precyzyjnie. Zajęło mi trochę czasu żeby zrozumieć w jaki sposób zostały policzone wartości końcowe ocen dla poszczególnych technologii. Ponadto brakło mi w pełni wielokryterialnego podejścia opartego np. na metodach paretowskich, czy progowych, albo jakiejś funkcji kompromisu w postaci odległości od rozwiązania najlepszego w sensie wartości przyjętych kryteriów. Podejście oparte o metakryterium, które zastosował Doktorant, aczkolwiek spotykane w praktycznych zastosowaniach, to jednak w pewnym sensie wypacza sens wielokryterialności (sprowadzając problem do problemu jednokryterialnego z funkcją metakryterium).

Mimo przedstawionych uwag stwierdzam, że rozwiązanie postawionego problemu badawczego przeprowadzone zostało z wykorzystaniem poprawnego aparatu badawczego, a przyjęte założenia należy uznać za właściwe. Odpowiedzi na siedem pytań badawczych postawionych na początku rozprawy znalazły się w rozprawie, co podkreślałem wcześniej. Niedosyt budzi jedynie odpowiedź na pytanie nr 5, ale jak zwróciłem uwagę wcześniej, przy tak postawionym pytaniu odpowiedź na nie była dość karkołomna.

5. Oryginalność rozprawy, samodzielny dorobek Autora

Za samodzielny dorobek Autora oraz oryginalność rozprawy uważam:

- dość wnikliwą analizę aktów prawnych i raportów pokontrolnych związanych z bezpieczeństwem cyfrowym oraz trwałym nośnikiem, wraz z bardzo spójną argumentacją spełniania warunków prawnych i technicznych przez cyfrowy trwały nośnik oparty na technologii blockchain (rozdziały 2 i 3);

- ciekawe porównanie skutków prawnych czynności prawnej w formie elektronicznej, tj. opatrzonej kwalifikowanym podpisem elektronicznym, oraz czynności w formie dokumentu elektronicznego wytworzonego przez system teleinformatyczny i podpisanego przez trwały nośnik na sieci blockchain (rozdział 3.1.1);
- praktyczna implementacja sieci blockchain: zaproponowanie organizacji (architektury) sieci blockchain dla trwałego nośnika w połączeniu z technologią WORM oraz tzw. zaufaną trzecią stroną, opisanie szczegółów technicznych implementacji związanych z zapisem danych, wykorzystaniem bufora czasu, zmiennymi adresami portfela oraz z samym oprogramowaniem, analiza poprawy wydajności rozwiązania, propozycja schematu organizacji (architektury) sieci blockchain w podmiocie leczniczym (rozdział 3.9);
- kompleksowe, wielokryterialne podejście do oceny architektur dziewięciu sieci blockchain; Doktorant wykorzystał łącznie 16 kryteriów cząstkowych (ilościowych, jak i jakościowych) grupując je w cztery kryteria główne (rozdział 4), zarekomendował technologie „najlepsze";
- interdyscyplinarność ujęcia problemu opisywanego w rozprawie: omawianie zarówno zagadnień prawno-formalnych, organizacyjno-funkcjonalnych, jak i technologicznych.

6. Poprawność przedstawienia uzyskanych wyników (zwięzłość, jasność, umiejętność przekonywania, poprawność redakcyjna) i inne uwagi dyskusyjne

Redakcja pracy nie budzi większych zastrzeżeń. Mam pewne zastrzeżenia co do poprawności przedstawiania uzyskanych wyników, o których wcześniej pisałem, ale w całości przedstawię je w tej części recenzji. Zacznę od zastrzeżenie jakie mam do sfomułowania pytania badawczego nr 5. Powtórzę, że Doktorant samym sformułowaniem pytania skomplikował sobie odpowiedź na nie i niejako sprowokował zwrócenie uwagi przez czytającego, w tym recenzenta. Na tak postawione pytanie trudno było odpowiedzieć. Nie przekonał mnie również Doktorant odpowiedzią na pytanie badawcze nr 3, związane z uzasadnieniem ekonomiczności wprowadzenia rozwiązania opartego o technologię blockchain (porównywał koszty tradycyjnej poczty wysyłanej przez banki do klientów z kosztami rozwiązania opartego o technologię blockchain). Nie bardzo rozumiałem sens takiego porównania, gdyż banki mają wprawdzie obowiązek informowania klientów, ale mogą to robić również elektronicznie, za zgodą klienta, np. z wykorzystaniem poczty elektronicznej. Nie bardzo rozumiałem również dlaczego Autor przyjął wyłącznie koszty dostępu do serwerów (plus ewentualnie dostępu do macierzy WORM), a nie uwzględnił kosztów wdrożenia i utrzymania systemu dostępu do sieci blockkchain. Mam również zastrzeżenia co do struktury rozdziału 3, najistotniejszego w pracy. Doktorant, niepotrzebnie według mnie, zawiera w tym rozdziale zarówno wyniki badań własnych, co było istotą tego rozdziału, wraz z opisami teoretycznymi (np. definicja trwałego nośnika). Spodziewałem się, że w rozdziale dotyczącym wyników badań własnych będą wyłącznie wyniki badań własnych, odwołujące się do rozważań teoretycznych, modeli, definicji itp., które zostały opisane w rozdziale teoretycznym (np. rozdziale 2). Mam również zastrzeżenia do braku precyzji w formułowaniu formuł matematycznych, wprawdzie nielicznych, w rozprawie. Mało precyzyjnie zapisano formuły (str. 174-175) wyliczające wartość każdego kryterium (np. wszystkie kryteria oznaczone jako „w", a dotyczą czego innego!, wartość w każdym kryterium dzielona przez „waga" podczas, gdy ta jest inna dla trzech z czterech kryteriów (2, 11, 3, 11), bo jest sumą maksymalnych wartości kryteriów cząstkowych). Podobnie wzór górny na str. 136, nie wiadomo co konkretnie oznacza parametr „czas". Schematy, rysunki i tabele dobrze wspomagają Czytelnika w lepszym zrozumieniu tekstu oraz prezentowanych rozwiązań.

Uwagi dyskusyjne

1. „Skoro jest tak dobrze, to dlaczego jest tak źle?", czyli skoro technologia rejestrów rozproszonych blockchain spełnia wszelkie wymagania prawne oraz związane z bezpieczeństwem cyfrowym, to dlaczego tak wolno wchodzi do użytku w obszarach, które wymienił Autor?
2. Dlaczego Autor przy analizie kosztów wdrożenia oraz utrzymania mechanizmu trwałego nośnika w oparciu o blockchain przyjął wyłącznie koszty dostępu do serwerów (plus ewentualnie dostępu do macierzy WORM), a nie uwzględnił kosztów wdrożenia i utrzymania systemu dostępu do sieci blockkchain?
3. Na ile zwiększy się bezpieczeństwo organizacji w kontekście przechowywania danych, w szczególności pod kątem narażenia na cyberataki i ochrony niezmienności danych po wprowadzeniu technologii blockchain? Jak to zmierzyć? (nawiązanie do pytania badawczego nr 5);
4. Dlaczego Autor nie pokusił się o przeprowadzenie np. ankiety wśród potencjalnych odbiorców technologii blockchain, dzięki której mógłby oszacować skutek wprowadzanych zmian widziany oczami tych, których zmiany miałyby dotyczyć? Jakie pytania należałoby zadać w takiej ankiecie, aby zobiektywizować ocenę skutków wprowadzanych zmian i oszacować poprawę bezpieczeństwa organizacji? (nawiązanie do pytania badawczego nr 5).

7. Przydatność rozprawy dla administracji, techniki, przemysłu, itp.

Według mnie, przedstawione w rozprawie rozwiązanie w postaci perspektywy wykorzystania cyfrowego trwałego nośnika realizowanego z wykorzystaniem technologii blockchain oraz płynące z tego rozwiązania korzyści ukazują możliwość adaptowania technologii w różnych obszarach życia codziennego. W rozprawie wyeksponowano różne obszary zastosowania: bankowość i finanse publiczne, bezpieczeństwo transportu oraz przechowywania żywności i leków, bezpieczeństwo zapisu i dostępu do dokumentacji medycznej, bezpieczeństwo systemów informatycznych. Z pewnością lista tych obszarów jest jeszcze dłuższa.

8. Podsumowanie

Podsumowując, uważam, że recenzowaną rozprawę doktorską mgr. inż. Bartosza Lewandowskiego pt.: "*Bezpieczeństwo transakcji biznesowych przy wykorzystaniu rejestrów rozproszonych* " można ulokować w dyscyplinie "Nauki o bezpieczeństwie".
Przedstawione we wcześniejszych rozdziałach mojej recenzji opinie i uzasadnienia świadczą o tym, że recenzowana rozprawa doktorska:

a) prezentuje ogólną wiedzę teoretyczną Autora rozprawy w dyscyplinie „Nauki o bezpieczeństwie" (uzasadnienie w rozdziałach 4 i 5 recenzji);
b) wykazuje umiejętność samodzielnego prowadzenia pracy naukowej przez Autora rozprawy (uzasadnienie w rozdziałach 3 i 4 recenzji);
c) stanowi oryginalne rozwiązanie problemu naukowego, oryginalne rozwiązanie w zakresie zastosowania wyników własnych badań naukowych w sferze gospodarczej lub społecznej albo oryginalne dokonanie artystyczne (uzasadnienie w rozdziałach 4, 5 i 7 recenzji).

Biorąc pod uwagę powyższe stwierdzam, że **rozprawa spełnia wymagania** stawiane rozprawom doktorskim przez Art. 187 Ustawy z dnia 20 lipca 2018 r. Prawo o szkolnictwie wyższym i nauce (Dz.U. z 30 sierpnia 2018 r., poz. 1668).

W związku z tym **wnioskuję o jej dopuszczenie do publicznej obrony**.

Zbigniew Mirosław Tarapata

Podpis cyfrowy: Zbigniew Mirosław Tarapata
DN: C=PL, L=Warszawa, O=Wojskowa Akademia Techniczna, SN=Tarapata, G=Zbigniew Mirosław, SERIALNUMBER=PNOPL-69090113238, CN=Zbigniew Mirosław Tarapata, OID.2.5.4.16=#30300C1D67656E2E2053796C7765737472261204B616C69736B6965676F20322F2D0C0F30302D39303820576172737A617761, OID.2.5.4.97=VATPL-5270206300
Powód: Jestem autorem tego dokumentu
Lokalizacja:
Data: 2024.12.09 14:58:44+01'00'
Foxit PDF Reader Wersja: 2024.3.0