Zachodniopomorski Uniwersytet Technologiczny w Szczecinie
Wydział Informatyki

Streszczenie pracy doktorskiej pt.:

WYKORZYSTANIE ŁAŃCUCHÓW BLOKÓW ZINTEGROWANYCH Z FORMULARZAMI ELEKTRONICZNYMI W REALIZACJI BEZPIECZNYCH TRANSAKCJI

autor: mgr inż. Gerard Wawrzyniak
promotor: dr hab. inż. Imed El Fray, prof. ZUT

Historia transakcji sięga tysięcy lat. Ich realizacji, rozumianej jako uzgodniona wymiana dóbr, zawsze towarzyszy wymiana informacji. Od początku zauważono, że istotnym elementem bezpieczeństwa transakcji jest konieczność dokumentowania jej przebiegu. Rozwój cywilizacji, sposobów prowadzenia transakcji i technik informacyjnych sprawił, że techniki informacyjne stały się narzędziem wspomagającym realizację transakcji w sferze gospodarowania zasobami i zarządzania wykonywaniem transakcji, w szczególności dotyczy to elektronicznej wymiany danych, informacji i dokumentów.

Formularz elektroniczny jest dokumentem elektronicznym, który posiada wszystkie cechy tradycyjnego formularza papierowego. Ponadto, co wynika z jego elektronicznej formy, posiada trójwarstwową naturę zawierającą warstwy: danych, prezentacji i logiki. Pozwalają one nie tylko na gromadzenie, przechowywanie, trarsfer i prezentację danych, ale również na dynamiczną graficzną prezentację formularza stosownie do stanu realizowanej transakcji, zapisanie reguł poprawności dokumentu oraz wymianę danych z rozmaitymi usługami i systemami sieciowymi. Formularz elektroniczny, dzięki warstwie logiki, umożliwia sterowanie realizacją transakcji z udziałem ludzi i maszyn. Transakcja wspomagana przez formularz elektroniczny może przebiegać z udziałem usług serwerowych implementowanych w różnych technologiach lub bez nich w skrajnie rozproszonym, bezserwerowym środowisku, gdy stronami transakcji są tylko ludzie.

„Akcje – działania" wbudowane w warstwę logiki dają możliwość zintegrowania formularza z różnymi usługami, protokołami i łańcuchami bloków, a także z innymi rozwijającymi się technologiami takimi jak: Internet rzeczy, systemy multimedialne.

Formularz elektroniczny gwarantuje bezpieczeństwo przechowywanych danych poprzez zastosowany system podpisów elektronicznych, obejmujących między innymi strukturę formularza wraz warstwą logiki i prezentacji oraz dane związane z realizacją poszczególnych etapów transakcji. Cechy formularza pozwoliły na osiągnięcie celu pracy jakim jest *opracowanie modelu transakcji rozproszonych sterowanych formularzami elektronicznymi* oraz pozytywną weryfikację hipotezy, zgodnie z którą *zastosowanie formularza elektronicznego z własną logiką umożliwi realizację transakcji rozproszonych w heterogenicznym środowisku bez używania infrastruktury serwerowej i udziału scentralizowanej infrastruktury PKI.*

Słowa kluczowe

formularz elektroniczny, transakcja, łańcuchy bloków, podpis elektroniczy, interoperacyjność

13.06.2023 G.Wawrzyniak

West Pomeranian University of Technology in Szczecin
Faculty of Computer Science and Information Technology

Abstract of the dissertation entitled:

THE USE OF BLOCKCHAINS INTEGRATED WITH ELECTRONIC FORMS IN THE EXECUTION OF SECURE TRANSACTIONS

by Gerard Wawrzyniak, M.Sc.Eng.
promotor: Supervisor: Dr. Imed El Fray, Prof. ZUT

The history of transactions dates back thousands of years. Their implementation, understood as an agreed exchange of goods, is always accompanied by the exchange of information. From the beginning, it was noted that an important element of transaction security is the need to document the course of the transaction. The development of civilization, ways of conducting transactions and information techniques has made information techniques a tool to support the implementation of transactions in the sphere of resource management and management of the execution of transactions, in particular, this applies to the electronic exchange of data, information and documents.

An electronic form is an electronic document that has all the features of a traditional paper form. In addition, as is evident from its electronic form, it has a three-layered nature containing layers: data, presentation and logic. They allow not only the collection, storage, trarsfer and presentation of data, but also the dynamic graphical presentation of the form according to the state of the transaction in progress, the recording of the document's rules of validity and the exchange of data with various network services and systems. The electronic form, thanks to the logic layer, makes it possible to control the execution of transactions involving humans and machines. The transaction supported by the electronic form can be carried out with or without server services implemented in various technologies in an extremely distributed, serverless environment, when only humans are parties to the transaction.

The „Actions" embedded in the logic layer provide the possibility to integrate the form with various services, protocols and blockchains, as well as with other developing technologies such as the Internet of things, multimedia systems.

The electronic form guarantees the security of the stored data through the system of electronic signatures used, covering, among other things, the structure of the form together with the logic and presentation layer, as well as the data related to the execution of the various stages of the transaction. The features of the form made it possible to achieve the goal of the work, which is *development of a model of distributed transactions controlled by electronic forms* and positive verification of the hypothesis according to which *application of an electronic form with its own logic will make it possible to implement distributed transactions in a heterogeneous environment without using server infrastructure and participation of a centralized PKI infrastructure.*

Key words

electronic form, transaction, blockchain, electronic signature, interoperability

13.06.2023

G. Wawrzyniak

Warszawa, 20 września 2023r.

dr hab. Mirosław Kurkowski, prof. UKSW, prof. APwSz

- **Instytut Informatyki**
  Uniwersytet kard. St. Wyszyńskiego w Warszawie
- **Instytut Służby Kryminalnej**
  Akademia Policji w Szczytnie

Recenzja rozprawy doktorskiej mgr inż. Gerarda Wawrzyniaka
Wykorzystanie łańcuchów bloków zintegrowanych z formularzami elektronicznymi w realizacji bezpiecznych transakcji
Promotor: dr hab. inż. Imed El Fray, prof. ZUT

Niniejsza recenzja została sporządzona na prośbę Rady Dyscypliny Naukowej Informatyka Techniczna i Telekomunikacja Zachodniopomorskiego Uniwersytetu Technologicznego wyrażonej w odpowiednim piśmie. Opiniowana rozprawa dotyczy wykorzystania technologii XML i blockchain do tworzenia bezpiecznych formularzy elektronicznych. Praca ma charakter projektowo/implementacyjny.

Zawartość rozprawy

Recenzowana rozprawa razem ze Spisem Treści, Bibliografią oraz Załącznikami liczy 222 strony. Układ rozprawy budzi zastrzeżenia. Na przykład traktowanie jako rozdział (Rozdział 8) samego sformułowania Celu rozprawy i hipotezy badawczej (mimo wprowadzenia ich już we Wstępie) jest moim zdaniem niewłaściwe. Zebrana na cele pisania rozprawy i zacytowana bogata literatura przedmiotu liczy 226 pozycji. Z dużym szacunkiem należy podkreślić jej rozmiar i zawartość.

We Wstępie autor określił Cel i hipotezę badawczą:

Celem pracy jest ***opracowanie modelu transakcji rozproszonych sterowanych formularzami elektronicznymi****, a sformułowana hipoteza badawcza to:* ***zastosowanie formularza elektronicznego z własną logiką umożliwi realizację transakcji rozproszonych w heterogenicznym środowisku bez używania infrastruktury serwerowej i udziału scentralizowanej architektury PKI****.*

Poza Wstępem (numerowanym jako Rozdział pierwszy) recenzowana rozprawa zawiera dwanaście rozdziałów właściwych, Słownik pojęć, Spis rysunków, tabel i wydruków, Spisu literatury oraz Załączników. Te ostatnie są bardzo rozbudowane. Zawierają one szczegółowo opisaną syntaktykę formularza elektronicznego zaproponowanego przez autora.

Kolejne rozdziały rozprawy od drugiego do siódmego przedstawiają szeroko wprowadzenie oraz przegląd stanu wiedzy w zakresie technik i metod transakcji elektronicznych oraz rozwiązań zapewniających bezpieczeństwo ich realizacji.

I tak w rozdziale drugim opisano historię (od starożytności) transakcji oraz metod zapewniania własności związanych z ich bezpieczeństwem, w tym wiarygodności. Rozdział trzeci przedstawia formalne specyfikacje transakcji i dotyczących ich wymagań. Zawarto tutaj także opis technik potrzebnych do przetwarzania informacji podczas zawierania transakcji. Dodatkowo przedstawiono tutaj próbę definicji formularzy elektronicznych jako pewnej określonej klasy dokumentów elektronicznych. W rozdziale czwartym opisano problemy związane z interoperacyjnością, w tym interoperacyjność procesów czy reguł.

W rozdziale piątym autor zaprezentował techniki stosowania podpisów elektronicznych w formacie XML wraz z analizą ich generowania i podatności na różnego rodzaju ataki. Rozdział szósty traktuje o technologii blockchain. Mgr Wawrzyniak prezentuje tutaj historię, zastosowania oraz zalety i wady tych rozwiązań. Jako przykład podano możliwość zastosowania blockchain do autoryzacji danych medycznych. W rozdziale siódmym autor dokonał podsumowania najistotniejszych elementów opisanych dotąd w rozprawie.

Proponowany przez autora rozdział ósmy składa się tylko z przedstawienia Celu i hipotezy badawczej zaprezentowanych wcześniej we Wstępie.

Podsumowując tę część rozprawy stwierdzam, że mgr Wawrzyniak przedstawił tutaj w sposób co najmniej wystarczający ogólną wiedzę teoretyczną dotyczącą badanego obszaru.

W następnych rozdziałach autor zamieszcza propozycje własnych rozwiązań.

I tak kolejno, w rozdziale dziewiątym zaproponowano formalną syntaktykę do zastosowania w opracowanym przez siebie formularzu elektronicznym w środowisku XML. Mgr Wawrzyniak uwzględnił tutaj interakcję formularza z człowiekiem oraz automatyczne przetwarzanie danych. Dodatkowo autor zawarł tutaj wiele przykładów z formularzy występujących w praktyce.

Rozdział dziesiąty prezentuje autorskie rozwiązania w zakresie metod zastosowania technologii blockchain w formularzach elektronicznych. W rozdziale jedenastym mgr Wawrzyniak omawia opracowane rozwiązania w zakresie realizacji transakcji przy użyciu

formularzy elektronicznych. Zaprezentowano także listę firm/instytucji, które zaadaptowały opisane metody do realizacji.

Ostatnie dwa rozdziały zawierają podsumowanie rozprawy. Najpierw mgr Wawrzyniak prezentuje zestawienie cech spełnianych przez opracowane rozwiązanie w stosunku do wymogów stawianych transakcjom elektronicznym. Kolejno przedstawiono perspektywy dalszych prac badawczych.

Podsumowując wyniki przedstawione w rozprawie należy stwierdzić, że moim zdaniem mgr Wawrzyniak w odpowiedni sposób zrealizował stawiany sobie Cel badawczy, a tym samym wykazał hipotezę badawczą.

Zaznaczyć jednak należy, że odczuwam pewien niedosyt w związku z brakiem próby bardziej formalnego uzasadnienia własności badanych przez autora rozprawy.

Uwagi polemiczne i krytyczne oraz elementy dyskusyjne

1. W moim odczuciu w wielu miejscach pracy autor zastosował skróty myślowe, czy niezbyt precyzyjne sformułowania. Uważam, że praca mogłaby być pod tym względem lepiej opracowana. Przykładem może być często wymieniana tzw. *logika* systemu. Tymczasem w nauce *logika*, to albo nauka o poprawnym rozumowaniu lub po prostu dany, określony precyzyjnie system wnioskowania.
2. Pierwsza część pracy, składająca się z sześciu rozdziałów (2 – 6), stanowi wprowadzenie do dalszych rozważań. Składają się na nią: prezentacja pierwszych historycznie transakcji, omówienie pojęcia transakcji z punku widzenia definicji, omówienie interoperacyjności jako istotnej właściwości transakcji, a także bezpieczeństwo współczesnych dokumentów z perspektywy podpisów elektronicznych oraz łańcuchów bloków jako potencjalnego źródła inspiracji do wspomagania realizacji transakcji. Całość zakończona jest podsumowaniem (Rozdział 7), które zawiera wnioski z wcześniejszych rozważań mające stanowić uzasadnienie przyjętego celu pracy oraz hipotez badawczych. Wydaje się, że ta część pracy mogłaby być krótsza i ograniczyć się do bardziej zwięzłego i bardziej precyzyjnego omówienia prezentowanej problematyki.
3. Ważnym przedmiotem rozważań rozprawy są formularze elektroniczne. Co prawda w rozdziale dziewiątym autor zaprezentował koncepcję oraz podstawy implementacji autorskiego rozwiązania formularzy elektronicznych, ale można byłoby wspomnieć o innych, o ile takie istnieją, rozwiązaniach formularzy elektronicznych, ze wskazaniem najważniejszych różnic pomiędzy nimi i rozwiązaniem zaprezentowanym przez autora.
4. Tytuł pracy *Wykorzystanie łańcuchów bloków zintegrowanych z formularzami elektronicznymi w realizacji bezpiecznych transakcji* nie do końca oddaje intencje wyrażone w celu badawczym sformułowanym jako „opracowanie modelu transakcji

rozproszonych sterowanych formularzami elektronicznymi” oraz hipotezie badawczej mówiącej, że „zastosowanie formularza elektronicznego z własną logiką umożliwi realizację transakcji rozproszonych w heterogenicznym środowisku bez użycia infrastruktury serwerowej i udziału scentralizowanej infrastruktury PKI”. Cel i hipoteza pracy nie zawierają informacji dotyczących wykorzystania łańcuchów bloków.

5. Konsekwencję powyższej uwagi można zauważyć w rozdziałach dziewiątym i jedenastym, w których zaprezentowano oraz omówiono koncepcję cech formularza umożliwiających realizację transakcji sterowanych logiką formularza, bez korzystania z aplikacji serwerowych, ale z zapewnieniem bezpieczeństwa, a także zaprezentowano przykład realizacji takiej transakcji. Natomiast w rozdziale dziesiątym autor ograniczył się do zaprezentowania i wykazania możliwości i mechanizmów jakie daje prezentowany formularz elektroniczny w zakresie integracji z łańcuchami bloków. Nie pokazano jednak przykładów transakcji, w których funkcje formularza są zintegrowane z funkcjami łańcuchów bloków.
6. Podobną uwagę można sformułować w zakresie braku konieczności korzystania ze scentralizowanej infrastruktury PKI w transakcjach realizowanych z użyciem formularzy elektronicznych będących przedmiotem pracy. Autor, w podrozdziale 6.5.3 zaprezentował, na podstawie studiów literaturowych, liczne rozwiązania implementujące funkcje i usługi systemów infrastruktury klucza publicznego opartych na łańcuchach bloków. Jednak w dalszej części pracy nie odniósł się do tej problematyki zakładając prawdopodobnie, że problem weryfikacji ważności certyfikatów klucza publicznego nie jest bezpośrednio związany z procesami realizacji transakcji i weryfikacji wiarygodności dokumentów wspomagających te transakcje, a przedstawienie w rozdziale dziesiątym skutecznych mechanizmów współpracy formularza z łańcuchem bloków jest w tej mierze wystarczające.

Uwagi redakcyjne

W pracy znalazłem kilkanaście błędów literowych lub stylistycznych, ale nie mają one znaczenia przy ocenie rozprawy jako całości.

Wniosek końcowy

Przedstawione w recenzowanej rozprawie doktorskiej rozważania i zaproponowane rozwiązania projektowo implementacyjne związane z wykorzystaniem technologii XML i blockchain do tworzenia bezpiecznych formularzy elektronicznych dotyczą ważnych i bieżących problemów informatyki. Rozprawa doktorska mgr inż. Gerarda Wawrzyniaka zawiera oryginalny wkład autora w teorię i praktykę komunikacji prowadzonej drogą elektroniczną.

Biorąc pod uwagę wyniki przedstawione w recenzowanej rozprawie doktorskiej mgr inż. Gerarda Wawrzyniaka stwierdzam, że moim zdaniem, praca ta spełnia wymagania stawiane rozprawom doktorskim przez obowiązującą aktualnie w Polsce Ustawę o Stopniach i Tytule Naukowym. Stawiam zatem wniosek o dopuszczenie mgr inż. Gerarda Wawrzyniaka do dalszych etapów przewodu doktorskiego prowadzonego w dziedzinie nauk inżynieryjno-technicznych w dyscyplinie Informatyka techniczna i telekomunikacja przez odpowiednią Radę Dyscypliny Naukowej Zachodniopomorskiego Uniwersytetu Technologicznego.

prof. dr hab. inż. Andrzej Śluzek
Instytut Informatyki Technicznej
Szkoły Głównej Gospodarstwa Wiejskiego
ul. Nowoursynowska 159, bud.34
02-776 Warszawa
email: andrzej_sluzek@sggw.edu.pl
tel. 22 59 37 281

Warszawa, 30 sierpnia 2023

RECENZJA ROZPRAWY DOKTORSKIEJ

Przedmiotem niniejszej recenzji jest rozprawa doktorska zatytułowana **„Wykorzystanie łańcuchów bloków zintegrowanych z formularzami elektronicznymi w realizacji bezpiecznych transakcji"** złożona przez Pana **mgr inż. Gerarda Wawrzyniaka** na Wydziale Informatyki Zachodniopomorskiego Uniwersytetu Technologicznego w Szczecinie.

Recenzja została przygotowana z uwzględnieniem zasad i wymogów sprecyzowanych w następujących publikacjach:

- „Recenzje w postępowaniach o awans naukowy: Poradnik" (Rada Doskonałości Naukowej, 2022).
- „Dobre praktyki w procedurach recenzyjnych w nauce" (wyd. MNiSzW, 2011).
- „Kodeks etyki pracownika naukowego" (załącznik do uchwały Nr 2/2020 Zgromadzenia Ogólnego PAN z dnia 25 czerwca 2020 r.).

umieszczonych na stronie Rady Doskonałości Naukowej: https://www.rdn.gov.pl/dobre-praktyki.poradnik-recenzje-w-postepowaniach-o-awans-naukowy.html

Recenzja składa się z sześciu części, w których omówione są kolejno:

- ✓ Ogólna charakterystyka tematu pracy oraz jej celów badawczych.
- ✓ Krótki opis struktury pracy oraz treści poszczególnych rozdziałów i innych części pracy.
- ✓ Ogólne uwagi o pracy.
- ✓ Uwagi szczegółowe.
- ✓ Ocena dorobku doktoranta.
- ✓ Podsumowanie.

1. Temat pracy oraz jej cele badawcze

Praca dotyczy szeroko pojętego tematu transakcji elektronicznych i metod zapewniających ich bezpieczną realizację niezależnie od istnienia odpowiedniej scentralizowanej infrastruktury obsługującej te transakcje (serwery, systemy uwierzytelnienia, homogeniczność środowiska implementacyjnego, itp.).

Głównym założeniem pracy jest zatem zaprojektowanie mechanizmów umożliwiających realizowanie transakcji elektronicznych w zdecentralizowanych systemach, różniących się pod wieloma względami (strukturalnie, organizacyjnie, technologicznie, a nawet kulturowo).

Autor proponuje użycie formularza elektronicznego jako podstawowego obiektu wykorzystywanego w przedstawionym w pracy modelu realizacji transakcji.

Precyzyjnie zaprojektowana syntaktyka formularza elektronicznego ma z jednej strony zapewnić formę przyjazną użytkownikowi (zrozumiała wizualizacja, weryfikacja formalnej poprawności, itp.), a z drugiej umożliwić uwzględnienie wszystkich wymogów bezpiecznych transakcji, np. niezaprzeczalność, czy wbudowanie mechanizmów kryptograficznych lub komunikacyjnych.

Wprawdzie tak zdefiniowana funkcjonalność formularzy elektronicznych nie wydaje się nadmiernie nowatorska, ale Autor uzupełnił ją o dodatkowe elementy, które decydują o możliwości rezygnacji z centralizacji systemów obsługi transakcji elektronicznych. Tymi elementami są: wprowadzenie własnej logiki formularza oraz (jako pochodna tej możliwości) użycie łańcuchów bloków (ang. *blockchains*), które mogą służyć do akceptacji transakcji (lub jej parametrów) bez konieczności wykorzystania innych narzędzi kryptograficznych, a tym samym umożliwić transparentny i zdecentralizowany system transakcji, w którym weryfikacja autentyczności transakcji polega na potwierdzeniu zgodności danych formularza transakcji z danymi, którymi dysponują wszystkie strony (lub ich większość) zaangażowane w dany system transakcyjny (a tak naprawdę w system łańcuchów bloków).

2. Struktura pracy

W sensie ogólnym, praca składa się z trzynastu rozdziałów oraz typowych elementów uzupełniających, tzn. słownika pojęć, spisów rysunków tabel i wydruków, spisu literatury oraz bardzo rozbudowanego załącznika zawierającego proponowaną syntaktykę formularza elektronicznego.

Praca ma jednak bardzo nietypową (jak na rozprawy doktorskie) strukturę. Najlepiej ilustruje to fakt, że cel i hipoteza badawcza pracy są zdefiniowane dopiero w Rozdziale 8, zaś Rozdziały 1 do 7 są tak naprawdę bardzo rozbudowanym historycznym wstępem i przeglądem stanu wiedzy w rozważanej dziedzinie.

Rozdział 1 jest wstępem omawiającym cele i strukturę pracy, a Rozdział 2 to „historia w pigułce" transakcji oraz związanych z nimi metod zapewniania wiarygodności. W Rozdziale 3 wprowadzone są formalne specyfikacje transakcji i dotyczących ich wymagań, a także związanego z nimi przetwarzania informacji. W tym samym rozdziale przedstawiono przegląd zagadnień dotyczących dokumentów elektronicznych (i związanych z nimi wymagań), a także zdefiniowano pojęcie formularza elektronicznego jako specyficznej klasy dokumentów elektronicznych.

Krótki Rozdział 4 poświęcony jest różnym aspektom i obszarom pojęcia interoperacyjności, przy czym niektóre z zamieszczonych tam definicji wydają się zbyt ogólne i niejasne (np. interoperacyjność procesów lub interoperacyjność reguł).

Rozdział 5 nosi wprawdzie tytuł *Bezpieczeństwo*, ale tak naprawdę opisuje przede wszystkim technikę podpisów elektronicznych w formacie XML, analizuje ich generację, rolę w formularzach elektronicznych i podatność na ataki hakerskie.

Rozdział 6 to dość obszerny opis technologii łańcuchów bloków, ich historii, typowych zastosowań, zalet i wad. Na tle różnych koncepcji (de)centralizacji, Autor omawia typowe topologie łańcuchów bloków, sposoby zapewniania konsensusu, itp. Szczególną uwagę zwraca na możliwości łańcuchów bloków we wspomaganiu realizacji transakcji, np. do uwierzytelniania zapisów medycznych, czy jako alternatywę lub uzupełnienie infrastruktury klucza publicznego.

Rozdział 7 podsumowuje najważniejsze (z punktu widzenia tematu pracy) punkty z poprzednich rozdziałów, a następnie (w Rozdziale 8) zdefiniowany jest cel i hipoteza badawcza przedstawionej rozprawy:

Cel badawczy: *Opracowanie modelu transakcji rozproszonych sterowanych formularzami elektronicznymi.*

Hipoteza badawcza: *Zastosowanie formularza elektronicznego z własną logiką umożliwi realizację transakcji rozproszonych w heterogenicznym środowisku bez użycia infrastruktury serwerowej i udziału scentralizowanej infrastruktury PKI.*

Kolejne rozdziały zawierają wyniki prac Autora (lub rozszerzenia istniejących rozwiązań zaproponowane przez Autora). Rozdział 9 jest propozycją formalnej syntaktyki formularza elektronicznego, ze wszystkimi elementami dotyczącymi zarówno interakcji z człowiekiem, jak i automatycznego przetwarzania/autoryzacji/weryfikacji formularza i jego treści, tzn. (używając terminologii Autora) warstwy danych, prezentacji i logiki. Można domniemywać środowisko XML (i schematy XMD) ale żeby się upewnić trzeba zajrzeć do załącznika. Omawiane struktury i działania ilustrowane są licznymi przykładami z rzeczywistych formularzy.

Rozdział 10 omawia integrację formularzy elektronicznych z technologią łańcuchów bloków. Są to przede wszystkim propozycje rozwiązań. Wprawdzie Autor przedstawia przykłady i zaimplementowane fragmenty kodu, ale rozdział zawiera raczej różnorodne koncepcje integracji, a nie konkretne rozwiązania.

Z kolei Rozdział 11 koncentruje się na przykładowych rozwiązaniach ilustrujących możliwości realizacji transakcji wspomaganych formularzem elektronicznym. Zwracając uwagę na kluczową rolę warstwy logiki, Autor pokazuje działanie metody na wybranych formularzach urzędowych, pokazuje jak realizowane jest bezpieczeństwo transakcji (w tym np. bezpieczna poczta), czy w jaki sposób realizowane są transakcje złożone wymagające wielokrotnego zwrotnego uzupełniania formularza. Jednak, podobnie jak w Rozdziale 10, integracja z łańcuchami bloków jest jedynie zasygnalizowana.

Autor podaje również listę instytucji, w których opisana metoda realizacji transakcji wspomaganych formularzem została zaimplementowana.

Rozdziały 12 i 13 są podsumowaniem pracy. W Rozdziale 12 Autor przedstawia w postaci tabelarycznej, jak zaproponowana struktura formularza odzwierciedla (i spełnia) wymogi stawiane transakcjom realizowanym elektronicznie. Dodatkowo pokazuje, choć raczej tylko w sferze koncepcyjnej, możliwości zaproponowanej struktury formularza do realizacji transakcji rozproszonych poprzez odpowiednie wykorzystanie warstwy logiki formularza.

Rozdział 13 opisuje proponowane kierunki dalszych badań. Na przykład postulowane jest podejście traktujące cały formularz jako blok łańcucha (w różnych wariantach, np. pełne dane

lub tylko funkcje skrótu) oraz analizowany problem potencjalnej integracji formularzy elektronicznych z inteligentnymi kontraktami.

3. Ogólne uwagi o pracy

Dużą zaletą pracy jest przekrojowy charakter pierwszych rozdziałów. Autor stara się w nich opisać całokształt zagadnień związanych z pojęciem transakcji i ich dokumentowaniem. Dzięki temu historyczne i przeglądowe części pierwszych rozdziałów pracy czyta się jak publikację popularno-naukową, z zaciekawieniem i bez żadnego wysiłku.

Niestety, próba podobnie dokładnego opisu bardziej złożonych tematów (np. Rozdz.5.4, czy 6.5.3) wymusza na Autorze konieczne skróty myślowe i syntetyczne odwoływanie się do pozycji literaturowych, przez co te fragmenty pierwszych rozdziałów tracą na przejrzystości. A i tak ta pierwsza część pracy wydaje się zbyt długa w stosunku do całości, a więc zaleta okazuje się również i pewną wadą.

Druga część pracy (w której Autor opisuje własne wyniki) jest już napisana bardziej jednorodnie i wszystkie zagadnienia są wystarczająco wyjaśnione (lub przynajmniej zasygnalizowane).

Nawiasem mówiąc, spis literatury jest bardzo mocną stroną pracy. Lista pozycji jest bardzo długa, ale Autor odwołuje się do (chyba?) każdej z nich, wykazując ty samym, że są one właściwie dobrane i obejmują cały zakres zagadnień omawianych w pracy. Niemniej Autor pominął kilka ważnych prac, zwłaszcza z wcześniejszych okresów rozwoju tematu, np.

- ✓ Hillman, Robert A., and Jeffrey J. Rachlinski. "Standard-form contracting in the electronic age." *NYUL Rev.* 77 (2002): 429.
- ✓ Schubert, Petra, and Mark Ginsburg. "Virtual communities of transaction: The role of personalization in electronic commerce." *Electronic Markets* 10, no. 1 (2000): 45-55.
- ✓ Chaum, David. "Security without identification: Transaction systems to make big brother obsolete." *Communications of the ACM* 28, no. 10 (1985): 1030-1044.
- ✓ Guttman, Robert H., Alexandros G. Moukas, and Pattie Maes. "Agent-mediated electronic commerce: A survey." *The Knowledge Engineering Review* 13, no. 2 (1998): 147-159.
- ✓ Tsiakis, Theodosios, and George Sthephanides. "The concept of security and trust in electronic payments." *Computers & Security* 24, no. 1 (2005): 10-15.

Kolejna uwaga dotyczy tytułu pracy. Moim zdaniem nie jest on najlepiej dobrany. Autor wprawdzie opisuje możliwości wykorzystania łańcuchów bloków w proponowanych formularzach elektronicznych, ale w porównaniu z innymi w pełni zaimplementowanymi wynikami nie są to najbardziej wyeksponowane fragmenty pracy. Tak naprawdę możliwe byłoby pominięcie w tytule łańcuchów bloków i wówczas tytuł bardziej precyzyjnie odpowiadałby treści pracy. Zwłaszcza, że ani w celu badawczym, ani w hipotezie badawczej łańcuchy bloków nie są w ogóle wymienione, a wszystkie opisy zintegrowania łańcuchów bloków z formularzami (Rozdział 10 i Rozdział 11.5) mają raczej charakter wstępnych propozycji, a nie w pełni zaimplementowanych rozwiązań.

Najważniejszym wynikiem pracy jest niewątpliwie zaproponowany model formularza elektronicznego, opisany w Rozdziale 9 i w pełni udokumentowany w Załączniku. Użyteczność

tego modelu jest potwierdzona licznymi implementacjami komercyjnymi wymienionymi w pracy (zakładam, że Autor wykorzystywał w nich zaproponowany przez siebie model).

Wprawdzie nie jest to formalne potwierdzenie poprawności modelu, ale nie udało mi się znaleźć żadnej niespójności, sprzeczności, czy redundancji w zamieszczonych w załączniku schematach XMD.

W moim odczuciu ten element pracy, niezależnie od innych zalet i niedoskonałości pracy (wspomnianych powyżej oraz wymienionych w następnych częściach recenzji) stanowi o wartości pracy, a zarazem pozycjonuje ją na pograniczu doktoratu klasycznego i doktoratu wdrożeniowego (choć raczej rozumianego trochę *a rebours*, gdyż najwyraźniej to doświadczenie zdobyte przy wdrożeniach stanowi podstawę wyników przedstawionych w pracy).

Należy przy tym podkreślić, że trójwarstwowa struktura formularza elektronicznego nie jest oczywiście oryginalnym pomysłem Autora, ale przedstawił on spójną i (jak się wydaje) kompletną klasyfikację elementów tej warstwy. Nie udało mi się dotrzeć do innych prac, w których znalazłaby się podobna systematyka.

4. Uwagi szczegółowe

Poniższe poprawki, uwagi, wątpliwości i pytania umieszczone są w kolejności wynikającej z układy pracy i nie tworzą powiązanych ze sobą tematycznie sekwencji.

Str.16, wiersz 5: Powinno być „w epokach kamienia, miedzi, brązu i **żelaza**".

Str.22, wiersz 28-29: Niejasne określenie „środowisko heterogeniczne technologicznie". Może należałoby zamieścić krótkie wyjaśnienie lub dodać definicję do słownika pojęć.

Str.28, wiersz 26: Warstwa logiki jakby mimochodem dodana do definicji formularza. Może należałoby bardziej wyeksponować pojawienie się nowej struktury? Zwłaszcza, że poniżej (wiersz 37) jest mowa o „trójwarstwowej koncepcji formularza elektronicznego".

Str.36, wiersze 11-13 i Rys.5.3: Definicja podpisu odłączonego zakłada położenie podpisywanych danych poza dokumentem XML, a prawy dolny przykład na Rys.5.3 umieszcza podpisywane dane wewnątrz dokumentu.

Str.42, ostatni akapit: Ze względu na ważność opisanego problemu, treść tego akapitu powinna być bardziej wyeksponowana.

Rys.6.3: Mało kontrastowe kolory psują czytelność rysunku.

Rys.6.5: Mylący rysunek (sugerujący, że funkcja skrótu pozostaje bez zmian przechodząc przez poszczególne bloki). Należały raczej umieścić rysunek podobny do Rys.6.6.

Str.53, wiersze 14-16: Niejasne wyjaśnienia dlaczego małe prawdopodobieństwo wygenerowania dowodu pracy oznacza, że nie wiadomo, który komputer wygeneruje następny blok. To raczej nie zależy od wielkości prawdopodobieństwa.

Rys.6.9 i 6.10: „Ceglany mur" oznacza uprawnienia dostępu, ale nie jest to wyjaśnione.

Str.64, wiersz 10: Powinno być „koszt przechowywania jest o około 20% **mniejszy**".

Str.70 i 71: Kontynuacja tabeli na następnej stronie nie jest zalecana, jeśli tabelę można zmieścić na jednej stronie.

Str.74, drugi akapit: Znaczenie treści tego akapitu powinny być w jakiś sposób podkreślone.

Str.75, wiersze 9-10: Na razie nie wykazano, że trójwarstwowa logika formularza umożliwia integrację formularza z łańcuchami bloków. Sformułowanie „umożliwi", albo „potencjalnie umożliwia" byłoby bardziej na miejscu.

Str.81-83: Ponownie tabele są rozbite na dwie strony, choć mogłyby być umieszczona na jednej. Podział na atrybuty statyczne i dynamiczne wydaje się dość arbitralny. Dlaczego np. *wartość domyślna* jest atrybutem dynamicznym, a *tekst podpowiedzi* statycznym?

Str.93, wiersz 12: Wskazane byłoby przypomnienie „W zaprojektowanym w Rozdz.9.2 formularzu elektronicznym....".

Str.93, wiersz 22: Transformacja XSLT jest na tyle ważnym pojęciem, że należałoby wspomnieć na czym ona polega.

Str.95, wiersz 1: Należałoby podkreślić, że warstwa logiki może istnieć również w „tradycyjnych" rozwiązaniach i trochę inaczej sformułować nowatorstwo zaprezentowanego modelu.

Str.102, ostatni akapit: Może zamiast „potwierdzają" należałoby stwierdzić „dają solidne podstawy do stwierdzenia". Bo Autor formalnie nie wykazał, że wymienione tam konkluzje są zawsze prawdziwe.

Rys.10.2: Można się dodatkowo odwołać do pozycji A.12-21 w Załączniku,

Str.104, ostatni akapit: Jest to raczej negatywny wniosek i należałoby tu wspomnieć, że rozwiązania w kolejnych sekcjach pracy rozwiązują ten problem.

Rys.10.4 i 10.6: Czy nie należałoby tych schematów XMD umieścić w Załączniku jako dodatkową (opcjonalną) sekcję?

Sekcja 10.4: Czy zaprezentowany mechanizm został tylko zaprojektowany, czy podjęto również próby implementacji?

Str.115: Czy nie należałoby tu umieścić również etapu archiwizacji formularza transakcji?

Str.138: Należałoby raczej stwierdzić, że „stanowi to **potwierdzenie poprawności** koncepcji..." a nie dowód.

Str.142, górna część: Czy metoda integracji formularza z łańcuchem bloków poprzez referencje do danych w łańcuchu bloków nie mogłaby być zrealizowana z użyciem mechanizmów z Rozdziału 10.2 lub 10.3?

Str,147: Def.16 i 30 są identyczne, choć dotyczą nieco innych pojęć.

Str.148: Def.30 nie wydaje się logicznie poprawna.

Str.155: W pracy wyraźnie brakuje spisu używanych akronimów (niektóre z nich nie są oczywiste). Mógłby on być umieszczony właśnie po stronie 155.

Str.187: Powinno być „A.4 **System** podpisów"

5. Ocena dorobku doktoranta

Wprawdzie ocena dorobku naukowego doktoranta nie jest wymaganym elementem recenzji rozprawy doktorskiej, ale w moim odczuciu należy jednak wspomnieć, że mgr inż. Gerard

Wawrzyniak ma w dorobku (wg Google Scholar) co najmniej pięć opublikowanych prac, przy czym dwie z nich mają wysoką punktację ministerialną (140 i 100 punktów). Co ważniejsze, wszystkie publikacje dotyczą tematów prezentowanych w rozprawie, a więc są dodatkowym potwierdzeniem naukowego znaczenia pracy.

Dodatkowo, w pracy wspomniane jest, że zaprezentowana koncepcja formularzy elektronicznych została zintegrowana z systemami w kilkudziesięciu miejscach na terenie kraju, zaś aplikacja wykorzystująca ten model otrzymała I Nagrodę w Konkursie Złoty BIT EOIF. Fakty te dodatkowo potwierdzają nie tylko poprawność, ale również przydatność wyników przedstawionych w rozprawie.

6. Podsumowanie

Rada Doskonałości Naukowej w poradniku „Recenzje w postępowaniach o awans naukowy" stwierdza, że kwintesencja recenzji rozprawy doktorskiej powinna sprowadzać się do trzech kwestii:

1. Oceny wraz z uzasadnieniem, czy rozprawa doktorska prezentuje ogólną wiedzę teoretyczną osoby ubiegającej się o nadanie stopnia doktora.
2. Oceny wraz z uzasadnieniem, czy rozprawa doktorska wykazuje umiejętność samodzielnego prowadzenia pracy naukowej przez osobę ubiegającą się o nadanie stopnia doktora.
3. Oceny wraz z uzasadnieniem, czy rozprawa doktorska stanowi oryginalne rozwiązanie problemu naukowego albo oryginalne rozwiązanie w zakresie zastosowania wyników własnych badań naukowych w sferze gospodarczej lub społecznej.

W moim odczuciu przedstawiona powyżej analiza treści rozprawy Pana mgr inż. Gerarda Wawrzyniaka w pełni upoważnia mnie do pozytywnej odpowiedzi na wszystkie trzy pytania bez konieczności dalszego uzasadniania mojej opinii.

Dodatkowo chciałbym stwierdzić (choć RDN nie zaleca by recenzenci wyrażali w swych recenzjach opinie odnoszące się do innych kwestii niż te powyższe) że cele pracy zostały osiągnięte, a hipoteza badawcza pracy została potwierdzona. Pozostaje jednak pewien niedosyt, gdyż elementy, które uważałbym za najbardziej nowatorskie (mam na myśli przede wszystkim integrację łańcuchów bloków z warstwą logiki formularza elektronicznego) zostały zrealizowane jedynie na poziomie analizy koncepcyjnej i wstępnych przykładów.

Andrzej Ślazek

UCHWAŁA NR 26

Rady Dyscypliny Informatyka Techniczna i Telekomunikacja Zachodniopomorskiego Uniwersytetu Technologicznego w Szczecinie z dnia 14 listopada 2023 r.

w sprawie nadania mgr. inż. Gerardowi Wawrzyniakowi stopnia doktora

Na podstawie § 17b ust. 1 pkt 2 Statutu ZUT (uchwała nr 75 Senatu ZUT z dnia 28 czerwca 2019 r., z późn. zm.) w związku z art. 179 ust. 2 i 3 pkt 2b ustawy z dnia 3 lipca 2018 r. Przepisy wprowadzające ustawę – Prawo o szkolnictwie wyższym i nauce (Dz. U. z 2018 r. poz. 1669, z późn. zm.) w związku z art. 14 ust. 2 pkt 5 ustawy z dnia 14 marca 2003 r. o stopniach naukowych i tytule naukowym oraz o stopniach i tytule w zakresie sztuki (tekst jedn. Dz. U. z 2017 r. poz. 1789, z późn. zm.) oraz § 16 ust. 3 i 19 uchwały nr 130 Senatu ZUT z dnia 29 maja 2023 r. (z późn. zm.) w sprawie określenia sposobu postępowania w sprawie nadania stopnia doktora przez Rady Dyscyplin Zachodniopomorskiego Uniwersytetu Technologicznego w Szczecinie uchwala się, co następuje:

§ 1.

Rada Dyscypliny Informatyka Techniczna i Telekomunikacja Zachodniopomorskiego Uniwersytetu Technologicznego w Szczecinie nadaje mgr. inż. Gerardowi Wawrzyniakowi stopień doktora w dziedzinie nauk inżynieryjno-technicznych w dyscyplinie informatyka techniczna i telekomunikacja.

§ 2.

Uchwała wchodzi w życie z dniem podjęcia.

Przewodniczący Rady Dyscypliny

dr hab. inż. Marcin Korzeń, prof. ZUT