Streszczenie dysertacji: Bezpieczeństwo transakcji biznesowych przy wykorzystaniu rejestrów rozproszonych

Autor: mgr inż. Bartosz Lewandowski

Celem dysertacji jest zbadanie, w jaki sposób technologia rejestrów rozproszonych, oparta na protokole blockchain, może być wykorzystana do zwiększenia bezpieczeństwa transakcji cyfrowych. Praca koncentruje się na analizie bezpieczeństwa zarówno w kontekście ochrony danych, jak i w zakresie tworzenia odpornych mechanizmów wspierających konsumentów i przedsiębiorców w obszarze cyberbezpieczeństwa. Praca łączy podejście teoretyczne i praktyczne, proponując rozwiązania prawno-technologiczne, które mogą być zaimplementowane w różnych sektorach gospodarki.

Czytelnik prowadzony jest poprzez obszary związane z prawnym aspektem prowadzonego badania. Stąd w rozdziale analizującym prawne zagadnienia, zostało wykazane, że blockchain może funkcjonować jako technologia zgodna z krajowymi i unijnymi regulacjami dotyczącymi cyfrowego trwałego nośnika. W świetle prawa krajowego trwały nośnik definiowany jest jako medium, które umożliwia przechowywanie informacji w sposób umożliwiający ich dostęp przez odpowiedni czas oraz uniemożliwiający zmianę zapisanych treści. Praca wskazuje, że cechy blockchain, takie jak decentralizacja, niezmienność i integralność danych, spełniają te wymogi.

Autor wskazuje na znaczenie Dyrektywy PSD2 (Payment Services Directive 2) w kontekście bezpieczeństwa transakcji cyfrowych oraz ochrony konsumentów. PSD2, wprowadzone w Unii Europejskiej, ma na celu uregulowanie sektora płatności elektronicznych oraz zwiększenie poziomu bezpieczeństwa w tym obszarze. Z punktu widzenia konsumenta, praca w praktyczny sposób implementuje wymogi rozporządzenia PSD2, wskazując na ciąg zdarzeń w sektorze bankowym, który rozpoczął się od sprawy austriackiego banku BAWAG PSK. Sąd wykazał niezgodność używanego przez bank systemu komunikacji z konsumentami (bankowy portal internetowy) z wymogami trwałego nośnika. Sprawa ta miała kluczowe znaczenia również dla działań polskiego UOKIK, który poprzez prowadzenie swoich działań zobowiązał banki do prawidłowego komunikowania się z konsumentami.

Powyższe przykłady wskazały na potrzebę projektowania systemów informatycznych, które mają pełnić funkcję trwałego nośnika. W pracy szczegółowo omówiono, jak blockchain może być wdrożony, by nie występowały wady prawne.

Ważnym elementem analizy było uwzględnienie przepisów dotyczących ochrony danych osobowych, w tym RODO (GDPR). Prawo do zapomnienia, będące jednym z fundamentów unijnego rozporządzenia, stanowi wyzwanie w kontekście niezmienności danych zapisanych w sieci blockchain. Autor sugeruje wykorzystanie funkcji skrótu (np. SHA) do przechowywania danych w blockchain oraz bezpiecznych nośników (macierze WORM) do zapisu treści dokumentów. Podział ten umożliwia zachowanie zgodności: z jednej strony zapewnia spełnienie wymogów trwałego nośnika, z drugiej strony pozwala na realizację prawa do zapomnienia bez konieczności naruszania struktury blockchain.

Analizowane regulacje obejmują również obowiązki wynikające z ustawy o krajowym systemie cyberbezpieczeństwa, która implementuje dyrektywę NIS w polskim porządku prawnym. Blockchain, dzięki swojej odporności na manipulacje, może wspierać podmioty w spełnianiu wymogów dotyczących zapewnienia bezpieczeństwa przetwarzanych informacji oraz realizacji audytowalności procesów.

Technologia blockchain, została przedstawiona jako narzędzie mające zastosowanie w obszarze bezpieczeństwa osobistego, szczególnie w kontekście ochrony danych oraz zapewnienia transparentności procesów. Głównym założeniem wykorzystania blockchain w tym zakresie jest stworzenie środowiska, w którym prywatność użytkowników jest chroniona, a dostęp do danych pozostaje kontrolowany i zgodny z obowiązującymi regulacjami prawnymi. Blockchain, dzięki swojej zdecentralizowanej strukturze, oferuje narzędzia eliminujące ryzyko manipulacji informacjami i nieautoryzowanego dostępu.

Jednym z przykładów wykorzystania blockchain jest stworzenie mechanizmu cyfrowego trwałego nośnika. Technologia ta pozwala na bezpieczne przechowywanie danych osobowych w sposób gwarantujący ich integralność oraz dostępność w wymaganym prawnie okresie. Zaproponowana implementacja minimalizuje ryzyko wycieku danych wrażliwych.

W ramach dysertacji przygotowane zostało w sposób praktyczny rozwiązanie implementujące mechanizm cyfrowego trwałego nośnika. Przygotowane zostało w oparciu o rozproszone geograficznie serwery oparte o systemu Linux na których zaimplementowane zostało rozwiązanie o oparciu o protokół Multichain. Wraz z rozwiązaniem praktycznym została dokonana analiza wydajności rozwiązania, tak by możliwe było zapisanie milionów wpisów w łańcuchu blockchain w ciągu krótkiego czasu. Równolegle z analizą wydajności, przeprowadzona została analiza kosztów cyfrowego trwałego nośnika vs klasyczna (analogowa) forma komunikacji. Analiza Celem dysertacji jest zbadanie, w jaki sposób technologia rejestrów rozproszonych, oparta na blockchainie, może być wykorzystana do zwiększenia bezpieczeństwa transakcji cyfrowych. Praca koncentruje się na analizie bezpieczeństwa zarówno w kontekście ochrony danych, jak i w zakresie tworzenia bezpiecznych mechanizmów

wspierających konsumentów i przedsiębiorców w obszarze cyberbezpieczeństwa. jednoznacznie wskazuje na wysokie oszczędności wynikające z digitalizacji procesu.

Technologia blockchain została również zaproponowana jako narzędzie wspierające bezpieczeństwo cyfrowego głosowania. Mechanizm oparty na blockchain pozwala na rejestrowanie głosów w sposób anonimowy, a jednocześnie audytowalny, co zwiększa zaufanie do procesu wyborczego. Wdrożenie takiego systemu eliminuje ryzyko manipulacji wynikami głosowania, a dzięki decentralizacji niemożliwe jest fałszowanie zapisów przez pojedynczy podmiot. Przeprowadzone w pracy symulacje wykazały, że mechanizm ten może obsługiwać dużą liczbę operacji w krótkim czasie, co czyni go efektywnym narzędziem w masowych procesach wyborczych.

W obszarze ochrony zdrowia technologia blockchain została wskazana jako sposób na zarządzanie elektroniczną dokumentacją medyczną. Dokumenty pacjentów, takie jak wyniki badań czy historie leczenia, mogą być przechowywane w sieci blockchain, co gwarantuje ich niezmienność oraz dostępność dla uprawnionych podmiotów. Dzięki zastosowaniu kryptografii asymetrycznej, jedynie osoby z odpowiednimi kluczami mogą uzyskać dostęp do tych informacji, co zabezpiecza pacjentów przed nieautoryzowanym wykorzystaniem ich danych.

Kolejnym praktycznym zastosowaniem opisanym w pracy jest wykorzystanie blockchain do zarządzania własnością intelektualną. Technologia ta umożliwia rejestrowanie dzieł cyfrowych, takich jak muzyka, grafiki czy filmy, w sposób niezmienny i audytowalny. Dzięki temu możliwe jest śledzenie autorstwa i zapewnienie praw twórców, eliminując problem fałszerstw i nieautoryzowanego kopiowania. Każda transakcja związana z dziełem jest rejestrowana w łańcuchu bloków, co pozwala na dokładne określenie, kto i kiedy nabył prawa do danego utworu.

W kontekście bezpieczeństwa produktów blockchain wspiera również monitorowanie łańcuchów dostaw. Przykładem jest identyfikacja pochodzenia żywności, która dzięki zapisom w blockchain może być śledzona od producenta do konsumenta. Rozwiązanie to zapobiega wprowadzaniu na rynek sfałszowanych produktów i zapewnia konsumentom dostęp do informacji o źródle pochodzenia towarów. W pracy podkreślono, że takie zastosowanie może również znaleźć zastosowanie w walce z podróbkami leków czy sprzętu medycznego.

Przeprowadzona analiza wykazała także potencjał blockchain w przeciwdziałaniu dezinformacji. Dzięki niezmiennym zapisom blockchain może służyć jako narzędzie weryfikacji autentyczności publikowanych treści, takich jak artykuły, zdjęcia (wizerunek) oraz inne media. Autor pracy wskazuje, że technologia ta mogłaby znaleźć zastosowanie w śledzeniu źródeł informacji i ograniczaniu rozprzestrzeniania się fałszywych wiadomości, co ma istotne znaczenie w budowaniu zaufania społecznego do mediów cyfrowych.

Zastosowanie blockchain zostało również zaproponowane w sektorze finansowym, gdzie technologia ta może wspierać przejrzystość transakcji oraz ich audytowalność. Dzięki niezmiennym zapisom w blockchain możliwe jest eliminowanie ryzyka manipulacji w procesach księgowych oraz skuteczniejsze zapobieganie nadużyciom finansowym.

Podsumowując, praktyczne zastosowania blockchain przedstawione w pracy obejmują szerokie spektrum działań na rzecz bezpieczeństwa osobistego i społecznego. Decentralizacja, kryptografia i transparentność czynią tę technologię istotnym narzędziem w ochronie danych, budowaniu zaufania do procesów cyfrowych i wspieraniu zgodności z regulacjami prawnymi. Dzięki tym cechom blockchain ma potencjał, by zrewolucjonizować zarządzanie bezpieczeństwem osobistym w erze cyfrowej.