PODPIS ZAUFANY
GRZEGORZ
BAZYDŁO
21.09.2025 22:09:08 [GMT+2]
Dokument podpisany elektronicznie
podpisem zaufanym

UNIWERSYTET ZIELONOGÓRSKI

DZIEDZINA NAUK INŻYNIERYJNO-TECHNICZNYCH

DYSCYPLINA: INFORMATYKA TECHNICZNA I TELEKOMUNIKACJA

ROZPRAWA DOKTORSKA

Opracowanie oraz wdrożenie elektronicznej usługi w postaci nośnika trwałego umożliwiającej przetwarzanie oraz zarządzanie wrażliwymi dokumentami elektronicznymi

Development and implementation of an electronic service as a durable medium for processing and managing sensitive electronic documents

mgr inż. Kamil Kozdrój

Opieka naukowa nad przygotowaniem rozprawy doktorskiej:

Promotor:
prof. dr hab. inż. Remigiusz Wiśniewski

Promotor pomocniczy:
dr inż. Grzegorz Bazydło

Rozprawę akceptuję:

Signed by / Podpisano przez:
.....
Remigiusz Grzegorz Wiśniewski
Date / Data: 2025-09-19 20:46

Zielona Góra, wrzesień 2025

Autor pragnie bardzo serdecznie podziękować obu promotorom oraz firmie Perceptus, bez których nie udałoby się tak wiele osiągnąć w tak krótkim czasie, jakim były trzy lata trwania Szkoły Doktorskiej oraz projektu „Doktorat wdrożeniowy”

Pracę tę dedykuję mojej narzeczonej,
która wspierała mnie na każdym etapie realizacji doktoratu
i trwała przy mnie w każdej ciężkiej chwili zwątpienia

Badania zamieszczone w pracy zrealizowano w ramach projektu „Doktorat wdrożeniowy” (nr projektu DWD/4/90/2020) realizowanego w latach 2020-2023 i finansowanego ze środków Ministerstwa Edukacji i Nauki.

Streszczenie

W pracy doktorskiej zaprezentowano autorski projekt, realizację oraz wdrożenie bezpiecznej i zaufanej elektronicznej usługi (e-usługi) w postaci nośnika trwałego, która umożliwia przetwarzanie oraz zarządzanie wrażliwymi dokumentami elektronicznymi. Ze względu na charakter niniejszej rozprawy, prowadzone prace łączyły aspekty zarówno naukowe, jak i wdrożeniowe. W pierwszej kolejności dokonano przeglądu aktualnego stanu wiedzy w zakresie trwałego nośnika (zarówno rozwiązań opisanych w literaturze jak i dostępnych na rynku). Przeprowadzono także analizę aspektów prawnych oraz wykonano przegląd zastosowań technologii blockchain i zaufanej trzeciej strony. Zrealizowane prace naukowe stanowiły podstawę prac wdrożeniowych. Przeprowadzono szereg badań eksperymentalnych zrealizowanej e-usługi, zarówno w zakresie wykorzystania technologii blockchain, jak i wybranych algorytmów oraz metod kryptograficznych w projektowanej e-usłudze. Najistotniejszym etapem prac wdrożeniowych była implementacja opracowanej e-usługi w infrastrukturze serwerowej firmy Perceptus sp. z o.o. z Zielonej Góry, która stanowiła fundament docelowego wdrożenia. Przeprowadzone testy końcowe potwierdziły poprawność opracowanej e-sługi. W szczególności, potwierdzona została zgodność wymagań (funkcjonalnych oraz technicznych) określonych w ramach opracowanego modelu e-usługi z wynikami uzyskanymi po jej wdrożeniu. Zaprojektowana i wdrożona e-usługa jest bezpieczna (poprzez wykorzystanie sieci blockchain oraz algorytmów kryptograficznych) oraz zaufana (dzięki roli zaufanej trzeciej strony jaką pełni firma Perceptus sp. z o.o., dostawca e-usługi).

Słowa kluczowe: e-usługa, trwały nośnik, blockchain, zaufana trzecia strona

Abstract

The dissertation presents a novel concept of a secure and trusted electronic service (e-service) as a durable medium for processing and managing sensitive electronic documents. The developed e-service was further practically implemented in a real company. Due to the nature of this dissertation, the presented descriptions combine both: scientific and implementation aspects. Firstly, the current state of the art in the field of durable media was reviewed (regarding solutions presented in the literature, as well, as those available on the market). An analysis of legal aspects and a review of the applications of blockchain technology and a trusted third party were also analyzed.

Both scientific and developmental research were the basis for further implementation. Experimental verification of the implemented e-service was carried out, both in terms of the use of blockchain technology, as well, as selected algorithms and cryptographic methods applied in the designed e-service. The most important step of the implementation stage referred to the deployment of the developed e-service within the IT infrastructure of "Perceptus sp. z o. o." – a company located in Zielona Góra, Poland. The results confirmed the correctness of the developed e-service. In particular, the compliance of the requirements (functional and technical) specified in the developed e-service model with the results obtained after its implementation was confirmed. This means that the designed and implemented e-service is secure (through the use of the blockchain network and cryptographic algorithms) and trusted (thanks to the role of a trusted third party played by "Perceptus sp. z o. o." – the e-service provider).

Keywords: e-service, durable medium, blockchain, trusted third party

Spis treści

Spis najważniejszych skrótów

AES	Advanced Encryption Standard
BPNM	Business Process Model and Notation
HSM	Hardware Security Module
HTTP	Hypertext Transfer Protocole
IBFT	Istanbul Byzantine Fault Tolerance
IPFS	InterPlanetary File System
JVM	Java Virtual Machine
PKI	Public Key Infrastructure
PoA	Proof-of-Authority
PoW	Proof-of-Work
P2P	Peer-to-Peer
RSA	Rivest-Shamir-Adleman
SHA	Secure Hash Algorithm
SSL	Secure Sockets Layer
TLS	Transport Layer Security
TTP	Trusted Third Party

1. Wstęp

Postęp technologiczny ostatnich lat, a także pandemia koronawirusa (2019-2020) wymusiły zmianę postrzegania tradycyjnego rynku usług. Tam, gdzie to było możliwe, pojawiały się elektroniczne usługi, które wypierały tradycyjne podejście do sposobu „załatwiania" typowych spraw np. w bankach, organach administracji publicznej, uczelniach, szkołach, zakładach pracy itp. Okazało się, że dzięki e-usługom wiele kwestii administracyjnych można zrealizować szybciej, efektywniej i taniej. Coraz częściej dokumenty papierowe zastępowane są cyfrowymi, a wiele z nich od początku powstania aż do ich skasowania nigdy nie jest drukowanych, czyli nie przyjmuje fizycznej formy w postaci papierowego wydruku. Jednak posługiwanie się (np. w relacjach biznesowych) wyłącznie dokumentami elektronicznymi oprócz całej gamy zalet, niesie także ze sobą szereg niebezpieczeństw i wyzwań. Dlatego istnieje rosnące zapotrzebowanie na elektroniczne usługi, które będą spełniać stawiane przez współczesny świat niełatwe wymagania dot. bezpieczeństwa, efektywności czy zaufania. Niniejsza praca jest próbą odpowiedzi na te właśnie współczesne wyzwania dot. rynku elektronicznych usług, a zaproponowana e-usługa pozwoli rozszerzyć ofertę biznesową firmy, w której została wdrożona i tym samym umożliwi konkurować na (ciągle jeszcze kształtującym się) rynku elektronicznych usług.

1.1. Wprowadzenie

W dzisiejszym, cyfrowym świecie, w którym technologia rozwija się w zawrotnym tempie, regulacje prawne starają się dostosować do nowych wyzwań związanych m.in. z przechowywaniem i udostępnianiem informacji. Jednym z kluczowych aspektów w tym obszarze jest pojęcie tzw. *trwałego nośnika* – wymogu prawno-administracyjnego dotyczącego zachowania informacji na trwałym medium przez określony czas [1]. Spełnienie tego wymogu jest jednak sporym wyzwaniem, zwłaszcza w kontekście postępu technologicznego i zmian w otoczeniu prawnym.

Trwały nośnik[1] może być zrealizowany w formie fizycznej w postaci wydrukowanego dokumentu przekazywanego klientowi albo w formie elektronicznej. Ta druga forma może być realizowana w taki sposób, że dokument elektroniczny przechowywany jest na fizycznym nośniku danych (np. płyta CD/DVD, pendrive, karta pamięci), który jest

[1] używane jest także sformułowanie „nośnik trwały" i w pracy oba te terminy będą stosowane zamiennie

przesyłany do klienta (a przez bank przechowywany elektronicznie np. na dysku twardym) lub w formie elektronicznej usługi mającego na celu dostarczenie dokumentu elektronicznego do klienta bez użycia fizycznego nośnika (np. wysłanie dokumentu pocztą elektroniczną, przesłanie linku z dostępem do pliku na serwerze w chmurze itp.). Wszystkie ww. formy realizacji trwałego nośnika pozwalają konsumentowi i przedsiębiorcy przechowywać informacje (w tym wrażliwe dokumenty elektroniczne) w sposób umożliwiający dostęp do nich w przyszłości przez czas odpowiedni do celów w jakim zostały utworzone (np. okres obowiązywania umowy).

Tradycyjne metody przechowywania i udostępniania informacji za pomocą papierowych dokumentów wiążą się z czasochłonnymi procesami drukowania, sortowania i archiwizacji. Implementacja rozwiązań elektronicznych mających na celu spełnienie wymagań trwałego nośnika niesie ze sobą wiele korzyści (zarówno dla danego przedsiębiorstwa i jego klientów) w kontekście przechowywania i przetwarzania dokumentów elektronicznych, np. poprawę efektywności procesu przepływu dokumentów, zmniejszenie kosztów ponoszonych tradycyjnymi sposobami (np. brak konieczności wysyłania płyt CD/DVD), zwiększenie bezpieczeństwa i lepszą ochronę danych (w tym danych osobowych), zwiększenie dostępności do dokumentów, itp. Przechowywanie dokumentów w formie elektronicznej może przynieść też znaczne oszczędności finansowe, ponieważ eliminuje się koszty związane z zakupem papieru, drukowaniem, przechowywaniem fizycznych dokumentów, przesyłaniem ich tradycyjnymi metodami, itp. Istnieje też możliwość łatwego tworzenia kopii zapasowych i archiwizacji elektronicznych dokumentów, co minimalizuje ryzyko utraty informacji. Ponadto wprowadzenie rozwiązań elektronicznych jako trwałego nośnika umożliwia zastosowanie zaawansowanych środków zabezpieczających i uwierzytelniania, takich jak szyfrowanie, podpis elektroniczny czy uwierzytelnianie dwuskładnikowe. To zapewnia większe bezpieczeństwo przechowywanych informacji, ogranicza ryzyko dostępu osób nieuprawnionych i minimalizuje potencjalne zagrożenia związane z kradzieżą lub utratą dokumentów. Nośnik trwały w wersji elektronicznej umożliwia łatwiejsze udostępnianie informacji i dokumentów. Dodatkowo, elektroniczne dokumenty mogą być dostępne online w dowolnym czasie i miejscu, co zapewnia większą ich dostępność, elastyczność i mobilność. Przechowywanie dokumentów w formie elektronicznej przyczynia się także do zrównoważonego rozwoju i ochrony środowiska, poprzez redukcję zużycia papieru, zmniejszenia emisji CO_2 związanej z produkcją i transportem dokumentów papierowych oraz ogranicza powstawanie odpadów.

Warto zauważyć, że niektóre rozwiązania, które teoretycznie spełniałyby znamiona nośnika trwałego mogą budzić szereg wątpliwości dot. zaufania klientów do tych rozwiązań, jeśli są one realizowane wyłącznie przez bank (jako podmiot dominujący w relacji biznesowej z klientem) albo implementowane wyłącznie wewnątrz infrastruktury serwerowej banku. Klienci mogą wtedy podejrzewać, że bank w przyszłości może próbować dane w jakiś sposób zmanipulować, zmodyfikować bądź usunąć (np. z powodu rzekomej „awarii"). Stąd bardzo ważne jest, aby rozwiązanie trwałego nośnika było z jednej strony bezpieczne (np. przechowywane w formie zaszyfrowanej, aby w przypadku ew. wycieku cyberprzestępcy nie byli w stanie uzyskać wrażliwych danych zawartych w dokumentach), ale też i zaufane, czyli nie budzące wątpliwości co do sposobu oraz intencji ich przechowywania i przetwarzania.

Podsumowując, rozwój technologiczny i postęp cyfryzacji wpływają pozytywnie na sposób, w jaki przechowywana i udostępniana jest informacja. W przypadku nośnika trwałego, implementacja rozwiązań elektronicznych może przynieść wiele korzyści. Efektywność, oszczędność czasu i kosztów, bezpieczeństwo danych, łatwość udostępniania oraz ochrona środowiska są tylko niektórymi z wielu powodów, dla których warto implementować wymagania dot. nośnika trwałego jako rozwiązania elektroniczne.

1.2. Motywacja podjęcia tematu

Przedsiębiorcy mają obowiązek przechowywania i udostępniania informacji konsumentowi w sposób, który umożliwia dostęp do tych danych przez określony czas. Czas ten zależny jest od specyfiki tych danych. Na przykład dla umów zawartych na czas określony, wszystkie strony umowy mają mieć możliwość dostępu do tych umów przez okres co najmniej obejmujący czas trwania tej umowy. Trwały nośnik, zgodnie z wymogami polskiego prawa musi umożliwiać odtworzenie informacji w nim zawartych w niezmienionej postaci i wyłączając jakikolwiek wpływ podmiotu, który był twórcą tych informacji [2].

Urząd Ochrony Konkurencji i Konsumentów (UOKIK) w Polsce w roku 2018 dokonał inspekcji banków pod kątem sposobu przekazywania informacji o zmianach umów na trwałym nośniku [3]. Wyniki tej kontroli pokazały, że banki w latach 2015-2018 dostarczały informacje o podwyżkach wyłącznie w swoich systemach elektronicznej bankowości, które nie spełniały wymogów nośnika trwałego. Dokumenty udostępniane przez system własny banku mogły być dowolnie zmieniane, podmieniane czy wręcz trwale usuwane. Dodatkowo nie było pewności, że klienci banku w ogóle wiedzieli, że taką

informację posiadają w systemie. Jeżeli klient rzadko logował się do systemu bankowego, to czasami nie miał nawet możliwości zareagować na zmiany danego dokumentu (np. umowy) [3]. Po wspomnianych inspekcjach UOKIK nałożył rożne kary na banki, np. zobowiązania do zwrotów ewentualnych nadpłat, zwolnień z wybranych opłat dla klientów, którzy w świetle prawa zostali nieprawidłowo poinformowani o zmianach w dokumentach. W tej sytuacji banki rozpoczęły poszukiwanie innych rozwiązań, w celu spełnienia wymogów stawianych przez prawo [3].

Istnieje więc zapotrzebowanie na bezpieczne i zaufane elektroniczne usługi (e-usługi) spełniające wymagania trwałego nośnika. Bezpieczeństwo e-usługi dotyczy przede wszystkim sposobu przechowywania danych poprzez szyfrowanie dokumentów, kontrolę dostępu do wrażliwych danych, stosowanie algorytmów kryptograficznych itp. Zaufanie w kontekście e-usługi oznacza natomiast jej realizację w sposób, który nie budzi wątpliwości co intencji strony przechowującej i przetwarzającej dane np. poprzez zastosowanie sieci blockchain, w której zapisane dane są z definicji niemodyfikowalne, czy implementacja e-usługi w infrastrukturze niezależnej od każdej ze stron. Dlatego idealnym wyborem wydaje się być tutaj wykorzystanie zaufanej trzeciej strony (ang. *Trusted Third Party* – TTP), która z racji niezależności wobec podmiotów będących w biznesowej relacji, budzi zaufanie jako strony pełniącej rolę niezależnego, zewnętrznego arbitra.

1.3. Teza, cel i zakres pracy

Głównym celem określonym w pracy jest projekt oraz realizacja bezpiecznej i zaufanej elektronicznej usługi (e-usługi) trwałego nośnika umożliwiającej przetwarzanie oraz zarządzanie wrażliwymi dokumentami elektronicznymi. Wrażliwe dokumenty rozumiane są tutaj jako dokumenty zawierające ważne dla danej strony (przedsiębiorstwa, klienta, osoby fizycznej itp.) informacje. Mogą być to np. poufne dane przedsiębiorstwa, dane osobowe itp. Warto podkreślić, że to dany podmiot decyduje, co dla niego konkretnie oznaczają „wrażliwe dane" przechowywane w elektronicznych dokumentach. Kierując się motywacjami z poprzedniego rozdziału przeprowadzono gruntowną analizę obecnego stanu wiedzy, a następnie przeprowadzono badania eksperymentalne, na podstawie których sformułowano następującą tezę pracy:

Możliwe jest opracowanie oraz wdrożenie elektronicznej usługi trwałego nośnika, która jest zarówno bezpieczna, jak i zaufana.

Przez termin *bezpieczna* usługa autor rozumie usługę, w której dane przechowywane i przetwarzane są z wykorzystaniem algorytmów kryptograficznych. Chodzi o takie wykorzystanie metod kryptograficznych, aby kluczowe dane przechowywać w bazie danych w formie zaszyfrowanej (w przypadku wycieku danych nie powinno dojść do ujawnienia ważnych informacji) oraz aby klucze kryptograficzne generować i przechowywać w sprzętowym module bezpieczeństwa, w którym także będą wykonywane krytyczne operacje kryptograficzne (np. szyfrowanie).

Drugim krytycznym aspektem proponowanej usługi jest termin *zaufana*, który w tym przypadku oznacza wykorzystanie podmiotu pełniącego rolę zaufanej trzeciej strony, niezależnego od każdej strony transakcji. Ponadto, usługa *zaufana* dotyczy także sposobu przechowywania danych (np. z wykorzystaniem sieci blockchain) tak, aby niemożliwe było ich usunięcie lub modyfikacja.

W celu udowodnienia tezy wyznaczone zostały zadania zarówno o charakterze naukowym, jak i wdrożeniowym. Zakres zadań naukowych obejmował:

- analizę aspektów prawnych (głównie polskich regulacji) dotyczących trwałego nośnika,
- przegląd i analizę istniejących rozwiązań teoretycznych (przegląd literatury) oraz praktycznych (w tym usług i produktów dostępnych na rynku) dot. trwałego nośnika,
- sprecyzowanie wymagań funkcjonalnych i technicznych dot. projektowanej e-usługi trwałego nośnika,
- przegląd i analizę dostępnych technologii cyberbezpieczeństwa (w tym technologii algorytmów kryptograficznych, technologii blockchain, sprzętowych modułów bezpieczeństwa itp.) pod kątem projektowanej e-usługi,
- analizę możliwości wykorzystania zaufanej trzeciej strony (TTP) pod kątem projektowanej e-usługi,
- opracowanie schematu (modelu procesu) realizacji e-usługi,
- opracowanie struktury sieci blockchain pod kątem projektowanej e-usługi.

Z kolei zadania wdrożeniowe dotyczyły następujących aspektów:

- przeprowadzenie badań eksperymentalnych w zakresie wykorzystania technologii blockchain oraz wybranych algorytmów i metod kryptograficznych w projektowanej e-usłudze,
- programową implementację opracowanych metod,

- wdrożenie (implementację) opracowanego modelu (schematu) e-usługi w infrastrukturze serwerowej,
- wdrożenie opracowanego rozwiązania w firmie (wymóg projektu „Doktorat wdrożeniowy", w ramach którego zrealizowano niniejszą rozprawę doktorską, który zakładał realizację wdrożenia opracowanego rozwiązania w firmie Perceptus sp. z o.o. [4] z Zielonej Góry),
- przeprowadzenie badań eksperymentalnych (testów końcowych) opracowanego i wdrożonego rozwiązania.

Przyjęto, że wymiernym potwierdzeniem tezy będzie poprawność opracowanej e-sługi, potwierdzona na podstawie **zgodności wymagań określonych w ramach prac naukowych** (opracowany model e-usługi) **z wynikami uzyskanymi w ramach prac wdrożeniowych** (wyniki eksperymentalne wdrożonej e-usługi).

1.4. Struktura pracy

W kolejnych rozdziałach pracy zostały szczegółowo scharakteryzowane zagadnienia związane z rozwiązaniami elektronicznymi dot. nośnika trwałego, analiza istniejących regulacji prawnych, technologii i wyzwań, a także charakterystyka wybranych rozwiązań, dobrych praktyk i perspektyw na przyszłość dot. implementacji nośnika trwałego. W pracy została także przedstawiona autorska koncepcja bezpiecznej i zaufanej e-usługi oraz wyniki badań dot. wdrożenia rozwiązania spełniającego założenia nośnika trwałego zgodnie z polskimi regulacjami prawnymi.

Praca została podzielona na pięć rozdziałów. Pierwszy rozdział stanowi wprowadzenie do tematyki badań, przedstawia motywację podjęcia tematu, definiuje cel i tezę pracy, a także omawia wynikające z niej zadania. W rozdziale drugim dokonano przeglądu i analizy aktualnego stanu wiedzy dot. zagadnień obejmujących temat rozprawy, w szczególności trwały nośnik, zaufaną trzecią stronę i technologię blockchain. W rozdziale trzecim została zaproponowana bezpieczna i zaufana e-usługa trwałego nośnika, w tym jej wymagania funkcjonalne oraz algorytm działania projektowanej e-usługi. Określona została także struktura sieci blockchain oraz rola zaufanej trzeciej strony. W rozdziale czwartym zostały przedstawione zagadnienia dot. implementacji oraz wdrożenia zaproponowanej e-usługi, w tym przedstawienie wymagań technicznych uzupełniających wymagania funkcjonalne z poprzedniego rozdziału, przybliżenie projektu e-usługi oraz przedstawienie etapów jej realizacji. W tym rozdziale zostały także przedstawione wyniki testów (badań eksperymentalnych) oraz opisano aspekty

wdrożeniowe, jak i ograniczenia proponowanej e-usługi. W rozdziale piątym ustosunkowano się do tezy pracy, wymieniono elementy nowatorskie oraz określono dalsze obszary badań.

2. Przegląd i analiza aktualnego stanu wiedzy

Przed przystąpieniem do realizacji e-usługi trwałego nośnika dokonano przeglądu i analizy dostępnych rozwiązań teoretycznych, technicznych oraz rynkowych dot. trwałego nośnika. Ponadto przeprowadzono analizę technologii dot. cyberbezpieczeństwa (w tym algorytmów kryptograficznych i sieci blockchain) oraz zaufanej trzeciej strony pod kątem możliwości wykorzystania ich w proponowanej e-usłudze. Uzyskana w ten sposób wiedza pozwoliła z jednej strony zdefiniować wymagania projektowanego rozwiązania, a z drugiej wybrać odpowiednie technologie, niezbędne do realizacji bezpiecznej i zaufanej e-usługi trwałego nośnika.

2.1. Trwały nośnik

Pojęcie *trwałego nośnika* (ang. *durable medium*) jest kluczowe w kontekście niniejszej pracy, dlatego warto na początku zdefiniować to pojęcie, nakreślić jego ramy prawne, a także scharakteryzować trwały nośnik jako usługę i e-usługę.

2.1.1. Definicja trwałego nośnika

Po raz pierwszy pojęcie *trwałego nośnika* pojawiło się w dyrektywie 97/7/WE Parlamentu Europejskiego i Rady z 20 maja 1997 r. w kwestii dotyczącej ochrony konsumentów w przypadku zawierania przez nich umów na odległość [1]. We wskazanym powyżej akcie prawnym wskazano, iż konsument musi otrzymać informacje w formie pisemnej lub na innym trwałym, dostępnym dla niego nośniku. Także w tym akcie prawnym po raz pierwszy posłużono się przymiotnikiem *trwały* w zestawieniu go z terminem *nośnik*. Następnie pojęcie trwałego nośnika zostało użyte w kolejnej dyrektywie Parlamentu Europejskiego i Rady [5] wskazując, iż „trwałe nośniki umożliwiają konsumentowi przechowywanie informacji tak długo, jak jest to dla niego konieczne w celu ochrony swoich interesów wynikających ze stosunków łączących go z przedsiębiorcą. Takie nośniki powinny obejmować w szczególności papier, pamięć USB, płyty CD-ROM, DVD, karty pamięci lub dyski twarde komputerów, a także pocztę elektroniczną" [5]. Następna dyrektywa [6] także zdefiniowała pojęcie trwałego nośnika, wskazując, iż trwałym nośnikiem może być strona internetowa, jeżeli umożliwia dostęp do informacji w przyszłości przez wystarczający okres do celów dostępu do tych informacji i pod warunkiem, że strony te umożliwiają odtworzenie przechowywanych informacji w niezmienionej postaci [6].

W polskim prawie pojęcie trwałego nośnika pojawia się w Ustawie z dnia 30 marca 2014 r. o prawach konsumentów, tj. ustawie implementującej wcześniej wspomnianą dyrektywę [5]. Ustawodawstwo polskie pod pojęciem trwałego nośnika rozumie materiał lub narzędzie umożliwiające konsumentowi lub przedsiębiorcy przechowywanie informacji kierowanych osobiście do niego, w sposób umożliwiający dostęp do informacji w przyszłości przez czas odpowiedni do celów, jakim te informacje służą i które pozwalają na odtworzenie przechowywanych informacji w niezmienionej postaci [7]. Wskazać należy, iż ustawodawstwo polskie nie zdefiniowało katalogu materiałów lub narzędzi, które mają stanowić trwałe nośniki informacji [8]. Reasumując, należy wskazać, iż brak jest jednej, kompleksowej i legalnej definicji pojęcia „trwały nośnik" lub „trwały nośnik informacji". Dzisiaj, głównie dzięki ustawodawstwu prawa unijnego można opracować definicję pojęcia „trwałego nośnika", dzięki wyszczególnieniu cech, które muszą towarzyszyć tej koncepcji bądź usłudze. Wobec powyższego, trwały nośnik, jest to każde urządzenie, produkt lub usługa, które ma za zadanie spełnić jednocześnie dwa podstawowe warunki. Pierwszy, to pozwolić na przechowywanie informacji kierowanych osobiście do osób trzecich (tj. konsumenta, przedsiębiorcy) w sposób umożliwiający dostęp do nich w przyszłości przez określony czas właściwy do celów tych informacji. Drugi warunek polega na możliwości odtworzenia przechowywanych informacji w niezmienionej postaci. Warto podkreślić, że pojęcie trwałego nośnika jest spełnione, jeżeli powyższe warunki są spełnione jednocześnie.

2.1.2. Trwały nośnik jako usługa i e-usługa

Koncepcja trwałego nośnika jako usługi polega na archiwizacji lub przechowywaniu danych w sposób trwały i niezmienny, gwarantując przy tym zapewnienie im bezpieczeństwa. Usługa taka może polegać na gromadzeniu danych na papierze (w formie wydrukowanej), bądź w formie cyfrowej, np. na dysku twardym komputera, taśmie magnetycznej, płycie CD/DVD, pamięci masowej, pendrive, dysku optycznym itp. Należy jednak pamiętać, iż usługa trwałego nośnika będzie spełniona wyłącznie w sytuacji realizacji przez daną instytucję bądź przedsiębiorcę dwóch warunków opisanych w poprzednim rozdziale. W praktyce często oznacza to konieczność przesyłania do użytkownika (klienta) wersji papierowej lub fizycznego nośnika danych (np. płyty CD) z umieszczoną na nim wersją cyfrową dokumentu. Przesyłanie danych np. nagranych na płytę CD może też nieść za sobą korzyści wynikające z takiej formy przesyłania informacji. Pozwala to w pewnym sensie na rozproszenie danych i w przypadku awarii systemu banku klienci mają dostęp do danych dostępnych na nośnikach fizycznych

w formie płyt CD, które posiadają w domu. Mimo korzyści jakie oferują nośniki fizyczne, taki sposób przesyłania informacji ma również wady, takie jak koszt płyt CD, koszty nagrania danych na płytę, dystrybucji i wysyłki do klientów, co również wpływa negatywnie na środowisko.

Trwały nośnik jako elektroniczna usługa (e-usługa) odnosi się do dostarczenia dokumentu lub informacji w formie elektronicznej, która ma charakter trwały i możliwy do przechowywania przez odbiorcę. Tradycyjnie nośnikiem trwałym były fizyczne nośniki danych, takie jak np. płyty CD/DVD, które zapewniały wysłanie ich do odbiorcy i długotrwałe przechowywanie informacji. Jednak w erze cyfrowej pojawiły się tzw. *e-usługi trwałego nośnika*, które umożliwiają dostarczenie dokumentów i informacji w formie elektronicznej, zapewniając jednocześnie ich trwałość, ale nie wymagają wysyłania fizycznych nośników do klientów, a jedynie przekazania im dostępu do wybranych funkcjonalności tej e-usługi.

E-usługa trwałego nośnika może obejmować przechowywanie i przetwarzanie różnych rodzajów dokumentów, takich jak umowy, faktury, deklaracje podatkowe, sprawozdania finansowe, zaświadczenia i inne. Istotą e-usługi trwałego nośnika jest zapewnienie odbiorcy dostępu do elektronicznej wersji dokumentu, która ma taką samą wartość prawno-dowodową jak tradycyjny (fizyczny) trwały nośnik. Aby spełnić wymogi trwałości, e-usługi nośnika trwałego zwykle wykorzystują technologie i narzędzia, takie jak szyfrowanie, podpis elektroniczny, znaczniki czasowe, zabezpieczenia przed modyfikacją danych, systemy archiwizacyjne i inne. Dzięki temu dokumenty dostarczane w formie elektronicznej są chronione przed utratą, uszkodzeniem i manipulacją.

E-usługi nośnika trwałego mogą być oferowane przez różne podmioty, w tym przez instytucje finansowe, dostawców usług telekomunikacyjnych, dostawców usług pocztowych czy specjalizowane platformy elektroniczne. Ważne jest, aby e-usługi trwałego nośnika spełniały określone standardy bezpieczeństwa, zgodności prawnej i regulacyjnej oraz były dostosowane do konkretnych wymagań dotyczących przechowywania dokumentów zgodnie z obowiązującymi przepisami.

Warto zauważyć jeszcze jeden problem, który może wystąpić podczas implementacji założeń e-sługi trwałego nośnika. Jeśli dostawcą takiej e-usługi jest np. bank, który tę e-usługę wdrożył samodzielnie i we własnej infrastrukturze serwerowej, to zaufanie klientów do tej e-usługi może być niewielkie. Mogą oni bowiem mieć uzasadnione obawy dot. możliwości ingerencji banku w przechowywane w niej dokumenty i ich modyfikację lub usunięcie.

2.2. Zaufana trzecia strona

W dzisiejszym dynamicznym świecie cyfrowym, zaufanie jest kluczowym czynnikiem w budowaniu długoterminowych relacji i osiąganiu sukcesu. Wiele organizacji polega na usługach i produktach oferowanych przez inne podmioty (strony), aby rozszerzyć swoje możliwości i zwiększyć efektywność. Jednak zaufanie do tych stron trzecich jest niezbędne, aby zapewnić bezpieczeństwo danych, ochronę prywatności i utrzymanie reputacji przedsiębiorstwa czy organizacji.

Właśnie dlatego zaufana trzecia strona (ang. *Trusted Third Party* – TTP) pojawia się często w kontekście cyberbezpieczeństwa, np. opartym o infrastrukturę klucza publicznego (ang. *Public Key Infrastructure*) i urzędy certyfikacji (ang. *Certificate Authority*) weryfikujące tożsamość podmiotów i wydające im certyfikaty cyfrowe. Najczęściej zaufana trzecia strona jest niezależną instytucją, która może zagwarantować, że klucze należą do określonych podmiotów (np. osób fizycznych, organizacji, a także komputerów, urządzeń sieciowych itp.). TTP odpowiada za wydawanie certyfikatów oraz poprawną weryfikację podmiotów oraz ich tożsamości i w tym kontekście często nazywana jest urzędem certyfikacji bądź centrum certyfikacji.

2.2.1. Definicja zaufanej trzeciej strony

Pojęcie zaufanej trzeciej strony nie posiada jednej obowiązującej i prawnej definicji. Zazwyczaj koncepcja ta jest używana w zestawieniu z szeroko pojętym bezpieczeństwem informatycznym, a przez zaufaną trzecią stronę najczęściej rozumie się stronę internetową bądź elektroniczną usługę, która jako zweryfikowana, służy bezpiecznemu przechowywaniu danych, w tym danych wrażliwych. Przykładowo może to być witryna internetowa, na której zalogowani użytkownicy mogą dokonywać zakupów online, bądź może być to dostawca usług chmurowych, który gwarantuje bezpieczeństwo i poufność przechowywanych danych. Zaufana trzecia strona charakteryzuje się posiadaniem odpowiednich certyfikatów bezpieczeństwa np. certyfikatu SSL/TLS, certyfikatu ISO 27001 itp., odpowiednią polityką prywatności oraz zabezpieczeń. Należy przy tym pamiętać, iż najważniejszą cechą zaufanej trzeciej strony jest jej wiarygodność, która przejawia się w pozytywnej reputacji wśród użytkowników. Zaufana trzecia strona to również podmiot przyjmujący dla określonej transakcji rolę obserwatora lub arbitra, czyli strony nie będącej częścią transakcji między dwoma podmiotami, ale monitorujący w jej trakcie obie strony, a w trakcie sporu między nimi podejmujący wiążące, rozstrzygające decyzje. Dlatego ważne jest przestrzeganie przez TTP zasad bezstronności

w podejmowaniu wszelkich decyzji, bazując jedynie na wiarygodnych informacjach otrzymanych w określonym procesie.

2.2.2. Wiarygodność zaufanej trzeciej strony

Wiarygodność TTP odnosi się do postrzegania jej na zewnątrz w kontekście określonej dziedziny i gromadzonych informacji, takich jak np. dane osobowe, medyczne, naukowe, prawne. Strona trzecia jest uważana za wiarygodną, gdy zostaną spełnione łącznie następujące warunki:

a) niezależność – brak konfliktów i wpływu zewnętrznego,
b) kompetencje i autorytet – zapewnienie posiadania specjalnych kompetencji, wiedzy oraz odpowiedniego doświadczenia w danej dziedzinie,
c) dowody i źródła – na nich TTP opiera swoje informacje i opinie,
d) transparentność – funkcjonowanie TTP oparte jest na jawnych zasadach, a tym samym TTP jest transparentne w swoich działaniach, podejmowanych decyzjach i prezentowanych informacjach.

2.3. Technologia blockchain

Technologia blockchain od ostatnich kilku lat zdobywa ogromną popularność, a nawet uznawana jest za rewolucję w sposobie przetwarzania danych. Uważa się, że blockchain jest innowacyjnym rozwiązaniem, które może przyczynić się do rewolucji w wielu dziedzinach, takich jak finanse, logistyka, ochrona danych, zarządzanie łańcuchem dostaw itp. Nowe sposoby wykorzystania tej technologii mogą prowadzić do efektywniejszych, bezpieczniejszych i bardziej przejrzystych systemów. Sposób przechowywania danych, zasady tworzenia i łączenia bloków, zabezpieczenia kryptograficznie i zdecentralizowany charakter sieci sprawiają, że blockchain jest trudniejszy do atakowania i bardziej odporny na manipulacje. W tym rozdziale zostaną przedstawione podstawy technologii blockchain, jej działanie i zastosowania w różnych dziedzinach. Zostaną omówione również potencjalne korzyści i wyzwania związane z jej wdrożeniem.

2.3.1. Definicja i zasada działania blockchain

Technologia blockchain to rozwiązanie, które umożliwia tworzenie rozproszonych i niezmiennych rejestrów transakcji lub danych. Głównym celem blockchain jest zapewnienie bezpieczeństwa, transparentności i niezawodności procesów transakcyjnych bez konieczności posiadania zaufania do jednej centralnej instytucji.

Struktura blockchain składa się z sekwencji bloków, które są ze sobą powiązane w logiczną łańcuchową strukturę. Każdy blok zawiera zestaw transakcji lub danych oraz unikalny identyfikator, znany jako skrót kryptograficzny, który odnosi się do poprzedniego bloku w łańcuchu. Ta struktura umożliwia tworzenie chronologicznego rejestru, który trwale przechowuje historię wszystkich transakcji.

Transakcje stanowią podstawową jednostkę danych w blockchain. Każda transakcja zawiera informacje o przekazaniu wartości, danych lub aktywów między uczestnikami sieci. Kiedy wiele transakcji jest zebranych, są one grupowane w bloki. Bloki zawierają również dodatkowe dane, takie jak znaczniki czasowe, wersje oprogramowania itp. Transakcje w bloku mają formę struktury drzewa Merkle'a (ang. *Merkle Tree*) [9]. W drzewie Merkle'a dane są organizowane w postaci binarnego drzewa, w którym każdy liść (najniższy węzeł) reprezentuje pojedynczy fragment danych, a każdy węzeł (w tym liście) ma swój unikalny hash (sumę kontrolną) obliczany na podstawie tych danych. Dzięki temu drzewo Merkle'a pozwala na efektywne skompresowanie dużych ilości danych w pojedynczy hash nazywany *Merkle Root*. Wszystkie transakcje w bloku są uporządkowane jako liście drzewa Merkle'a, a następnie scala się je hierarchicznie, aż do uzyskania jednego Merkle Root, który reprezentuje całe dane transakcji w bloku. Dzięki temu, aby zweryfikować, czy dana transakcja jest częścią bloku, wystarczy porównać jej hash z Merkle Root, co jest znacznie bardziej efektywne niż weryfikacja każdej transakcji osobno.

Innym kluczowym elementem działania blockchain jest *konsensus*. Oznacza on, że wszyscy uczestnicy sieci muszą zgodzić się co do poprawności bloków i transakcji, które są dodawane do łańcucha. Istnieje wiele różnych algorytmów konsensusu, z których najważniejsze to [10]:

- Proof-of-Work (PoW),
- Proof-of-Stake (PoS),
- Proof-of-Authority (PoA),
- Delegated-Proof-of-Stake (DPoS),
- Proof-of-Capacity (PoC),
- Proof-of-Importance (PoI),
- Proof-of-Burn (PoB),
- Proof-of-Storage (PoStorage),
- Istanbul Byzantine Fault Tolerance (IBFT),
- Crash Fault Tolerant (CFT).

Algorytmy te opierają się na różnych zasadach potwierdzania poprawności transakcji, takich jak np. dowód wykonanej pracy, posiadanie aktywów kryptograficznych, delegowanie uprawnień itp. Przed dodaniem bloku do łańcucha, węzły sieci weryfikują poprawność transakcji wewnątrz bloku. W zależności od algorytmu konsensusu, węzły mogą być nagradzane za udział w procesie weryfikacji (jak np. ma to miejsce w kryptowalutach). Ponadto, blockchain wykorzystuje zaawansowane mechanizmy kryptograficzne, takie jak kryptograficzne funkcje skrótu (np. SHA-256 [11]) i podpisy cyfrowe, aby zapewnić integralność danych i bezpieczeństwo sieci. Kiedy blok jest dodany do łańcucha, staje się praktycznie niemożliwy do zmiany. Powodem tego jest fakt, że każdy kolejny blok zawiera odwołanie do poprzedniego bloku w formie jego skrótu. Wprowadzenie zmiany w bloku wymagałoby zmiany wszystkich kolejnych bloków, co jest bardzo trudne i wymaga ogromnej mocy obliczeniowej. Ta cecha blockchain czyni go odpornym na manipulacje i zapewnia niezmienność danych.

2.3.2. Zastosowania technologii blockchain

Zastosowania technologii blockchain obejmują kryptowaluty i finanse, łańcuchy dostaw, zarządzanie prawami autorskimi, głosowania elektroniczne itp. W przypadku kryptowalut i finansów, blockchain jest wykorzystywany do funkcjonowania cyfrowych walut, takich jak Bitcoin [12] czy Ethereum [13], [14], a także do usprawniania rozliczeń transakcji i zwiększania przejrzystości w systemach płatności. W sektorze finansowym blockchain ma duży potencjał do zrewolucjonizowania tradycyjnych systemów płatności i rozliczeń. Dzięki technologii blockchain możliwe staje się natychmiastowe przesyłanie środków, eliminacja pośredników i zmniejszenie kosztów transakcji. Ponadto, blockchain zapewnia większą przejrzystość, bezpieczeństwo i niezmienność danych transakcyjnych, co przyczynia się do budowania zaufania w sektorze finansowym. Przykładem jest projekt Ripple [15], który wykorzystuje blockchain do natychmiastowych rozliczeń międzybankowych na całym świecie.

W obszarze łańcuchów dostaw, blockchain może poprawić zarządzanie, umożliwiając śledzenie etapów produkcji, transportu i dystrybucji towarów. Dzięki temu można zapewnić autentyczność produktów oraz zwiększyć efektywność procesów logistycznych. Dzięki blockchain możliwe jest ścisłe monitorowanie i rejestrowanie każdego etapu dostawy, od producenta do ostatecznego odbiorcy. To pozwala na lepszą kontrolę jakości, zapewnienie autentyczności produktów oraz wykrywanie ewentualnych nieprawidłowości w procesie logistycznym. Przykładem jest projekt IBM Food Trust [16], który wykorzystuje blockchain do śledzenia łańcucha dostaw żywności, zapewniając

transparentność i bezpieczeństwo informacji o pochodzeniu i jakości produktów spożywczych.

Technologia blockchain jest również wykorzystywana do zarządzania prawami autorskimi, umożliwiając artystom i twórcom ochronę ich własności intelektualnej, śledzenie transakcji dotyczących ich dzieł oraz sprzedaż i licencjonowanie ich twórczości [17].

W dziedzinie głosowania elektronicznego, blockchain jest stosowany do prowadzenia bezpiecznych i przejrzystych systemów do głosowania, eliminujących możliwość fałszowania głosów [18]. Dzięki zdecentralizowanej naturze i niezmienności danych, można zapewnić integralność procesu wyborczego.

W sektorze zdrowia publicznego blockchain może przyczynić się do poprawy zarządzania danymi medycznymi, dostępu do informacji pacjentów i wymiany danych między różnymi podmiotami. Dane medyczne przechowywane w blockchain są bezpieczne i niezmienne, co przyczynia się do ochrony prywatności pacjentów oraz unikania fałszerstw czy manipulacji. Przykładem jest projekt Medicalchain [19], który wykorzystuje blockchain do umożliwienia pacjentom kontrolowania swoich danych medycznych i udostępniania ich wybranym lekarzom i instytucjom medycznym.

W sektorze nieruchomości blockchain może znacząco ułatwić procesy związane z transakcjami i przekazywaniem praw własności. Dzięki zastosowaniu blockchain możliwe jest tworzenie niezmiennych, publicznych rejestrów transakcji nieruchomości, które są łatwo dostępne i wiarygodne. To zapewnia większą przejrzystość, skraca czas transakcji i minimalizuje ryzyko oszustw. Przykładem jest projekt Propy [20], który wykorzystuje blockchain do przeprowadzania międzynarodowych transakcji w tym sektorze.

Oprócz wymienionych obszarów, technologia blockchain znajduje również zastosowanie w takich branżach jak cyberbezpieczeństwo, zarządzanie łańcuchem dostaw farmaceutycznych, audyty i wiele innych. Jej transparentność, niezmienność i bezpieczeństwo danych otwierają nowe możliwości innowacyjnych rozwiązań i zastosowań sieci blockchain także w innych dziedzinach gospodarki.

2.3.3. Korzyści wynikające z zastosowania technologii blockchain

Ogólnie rzecz ujmując, główne korzyści wynikające z zastosowania technologii blockchain obejmują bezpieczeństwo, transparentność, efektywność i innowacyjność. Blockchain zapewnia wysoki poziom bezpieczeństwa danych dzięki zastosowaniu zaawansowanych mechanizmów kryptograficznych. Dane są zabezpieczone przed

nieautoryzowanym dostępem i modyfikacją, co przyczynia się do budowy zaufania w systemach, gdzie ważna jest integralność informacji. W sieci blockchain wszystkie transakcje są dostępne publicznie dzięki czemu sieć jest transparentna. To oznacza, że uczestnicy sieci mogą śledzić i weryfikować każdą transakcję, co prowadzi do większej przejrzystości procesów biznesowych i zmniejsza ryzyko oszustw. Dzięki temu blockchain może przyspieszyć procesy biznesowe poprzez automatyzację i eliminację niepotrzebnych etapów weryfikacji. To z kolei prowadzi do zwiększenia efektywności operacyjnej i oszczędności czasu.

Technologia blockchain oferuje elastyczność i skalowalność w zależności od rodzaju sieci i algorytmu konsensusu, umożliwiając obsługę dużej liczby transakcji w sposób równoległy. Prywatne sieci blockchain mają większe możliwości skalowania niż sieci publiczne, ponieważ mogą mieć mniej uczestników i wymagają mniej złożonych mechanizmów konsensusu. W sieciach publicznych, gdzie udział jest otwarty i liczba uczestników może być duża, skalowalność jest bardziej skomplikowana. Wybór algorytmu konsensusu ma także duży wpływ na skalowalność. Niektóre algorytmy, takie jak Proof-of-Work, mogą być mniej efektywne w skalowaniu z powodu intensywnego zużycia energii i ograniczeń wydajnościowych, w przeciwieństwie np. do algorytmów typu Proof-of-Stake czy Proof-of-Authority, choć zależy to także od sposobu ich implementacji. Sama technologia blockchain jest technologią otwartą, która zachęca do tworzenia innowacyjnych rozwiązań. Deweloperzy mogą budować aplikacje i inteligentne kontrakty oparte na sieci blockchain, co prowadzi do powstawania nowych modeli biznesowych i możliwości wykorzystania tej technologii w różnych dziedzinach.

Te korzyści sprawiają, że technologia blockchain znajduje zastosowanie w wielu obszarach, w tym w finansach, logistyce, łańcuchach dostaw, ochronie danych, usługach zdrowotnych i wielu innych, przyczyniając się do zmiany sposobu funkcjonowania różnych sektorów gospodarki.

2.3.4. Wyzwania i perspektywy rozwoju technologii blockchain

Jednym z głównych wyzwań stojących przed technologią blockchain jest skalowalność, czyli zdolność do obsługi dużej liczby transakcji w krótkim czasie. Obecnie istniejące rozwiązania blockchain mają ograniczenia wydajnościowe, co może stanowić problem w przypadku systemów o dużej skali operacji. Pomimo rosnącego zainteresowania blockchain i jego popularnością, nadal istnieje wyzwanie związane z powszechnym przyjęciem tej technologii. Konieczne jest edukowanie i zachęcanie przedsiębiorstw oraz instytucji do wdrażania technologii blockchain w swoich działalnościach. Dodatkowo

oszustwa związane z kryptowalutami oparte w głównej mierze na nieznajomości samej technologii i wynikających z tego błędach ludzkich nie wpływają korzystnie na jej odbiór, a ponieważ giełdy kryptowalut są ściśle kojarzone z technologią blockchain, cierpi na tym „reputacja" samej technologii. Chociaż blockchain jest ogólnie uważany za bezpieczny, istnieją wyzwania związane z cyberatakami i nieuczciwymi działaniami. Ataki hakerskie, kradzieże kluczy prywatnych czy próby manipulacji transakcjami stanowią ryzyko dla systemów opartych na łańcuchach bloków.

Technologia blockchain jest względnie nową i ciągle rozwijającą się technologią, przez co brakuje konkretnych unormowań prawnych w tym zakresie. Z drugiej strony opracowanie oraz wdrożenie odpowiednich przepisów i uregulowań prawnych, które uwzględniałyby specyfikę tej technologii, stanowi duże wyzwanie. Ponadto konieczne jest również zapewnienie zgodności z istniejącymi przepisami dotyczącymi prywatności, ochrony danych i zwalczania procederu „prania pieniędzy".

Sama technologia musi sprostać jeszcze wielu wyzwaniom, jak na przykład temu, że większość projektów blockchain działa w izolacji, co utrudnia interoperacyjność między różnymi sieciami. Rozwój standardów i protokołów, które umożliwią komunikację i współpracę między różnymi sieciami blockchain jest wyzwaniem dla dalszego rozwoju tej technologii. Aczkolwiek pojawiają się już projekty próbujące rozwiązać ten problem z coraz większą skutecznością [21], [22] .

Niektóre typy sieci blockchain oparte są o algorytmy konsensusu, takie jak np. Proof-of-Work, które wymagają znacznej mocy obliczeniowej i zużywają dużo energii. To generuje kolejne wyzwania dla zrównoważonego rozwoju technologii blockchain i konieczności poszukiwania bardziej efektywnych rozwiązań energetycznych bądź nowych, wydajniejszych algorytmów.

Mimo wszystko perspektywy rozwoju technologii blockchain są bardzo obiecujące i obejmują wiele obszarów. Wdrażanie sieci blockchain w różnych sektorach, takich jak finanse, logistyka, zdrowie, łańcuchy dostaw, nieruchomości i energetyka, rozwija się bardzo dynamicznie. W przyszłości można oczekiwać dalszego dostosowywania technologii blockchain do specyficznych potrzeb tych sektorów, co przyczyni się do usprawnienia procesów i wprowadzenia większej ich przejrzystości.

Kolejnym obszarem rozwoju jest skalowalność technologii. Istniejące publiczne sieci blockchain mają ograniczenia wydajnościowe, więc perspektywy rozwoju obejmują opracowanie nowych rozwiązań, takich jak technologie warstw bocznych i nowe, bądź zmodyfikowane mechanizmy konsensusu, które umożliwią obsługę większej liczby

transakcji. Zmiany te mogą również prowadzić do poprawy efektywności energetycznej, która też jest kolejną perspektywą rozwoju technologii blockchain. Rozwój bardziej efektywnych algorytmów konsensusu może wpłynąć na zmniejszenie zapotrzebowania energii energetycznej, co jest ważnym aspektem dla zmniejszenia negatywnego wpływu technologii blockchain na środowisko.

Integracja z innymi technologiami, takimi jak sztuczna inteligencja albo Internet Rzeczy (ang. *Internet of Things*), może również przyczynić się do rozwoju technologii blockchain. Połączenie tych technologii otwiera nowe zastosowania i możliwości rozwoju. Perspektywy te obejmują również rosnącą rolę sektora publicznego. Rządy i instytucje publiczne mogą wykorzystać blockchain do poprawy efektywności usług publicznych, zapewnienia bezpieczeństwa danych, walki z korupcją i rozwijania innowacyjnych rozwiązań dla obywateli.

Jak widać, mimo potencjału technologii blockchain, istnieje jeszcze wiele wyzwań, które muszą być rozwiązane, aby umożliwić pełne jej wdrożenie i wykorzystanie w różnych sektorach gospodarki. Poszukiwanie rozwiązywań dla tych wyzwań jest kluczowe dla dalszego rozwoju technologii blockchain.

2.4. Przegląd i analiza dostępnych rozwiązań trwałego nośnika

W niniejszym rozdziale przedstawiono wyniki przeglądu i analizy dostępnych rozwiązań trwałego nośnika. Wskazano na wady i zalety każdego z analizowanych podejść. Analizując występujące w literaturze oraz dostępne na rynku proponowane rozwiązania i produkty, zwracano uwagę szczególnie na te cechy, którymi, zdaniem autora, powinno charakteryzować się optymalne rozwiązanie dot. trwałego nośnika, a mianowicie: bezpieczeństwo, zaufanie, trwałość, niska cena oraz spełnienie norm prawnych.

Analizę podzielono na trzy obszary. Pierwszym był przegląd komercyjnych usług i produktów dot. nośnika trwałego dostępnych na rynku. Drugi obszar stanowił analizę rozwiązań dot. przetwarzania dokumentów wykorzystujących technologię blockchain. Trzecim obszarem analizy był przegląd podejść wykorzystujących zaufaną trzecią stronę.

2.4.1. Analiza dostępnych na rynku rozwiązań trwałego nośnika

W ramach pracy dokonano przeglądu i analizy rynku w celu określenia aktualnego stanu istniejących rozwiązań implementujących wymagania trwałego nośnika (zarówno na rynku polskim jak i światowym). W wyniku przeprowadzonej analizy zidentyfikowano m.in. banki, które wykorzystują rozwiązanie trwałego nośnika na polskim rynku. Na

przykład BNP Paribas i PKO BP korzystają z rozwiązania dostarczonego przez Krajową Izbę Rozliczeniową (KIR), które wykorzystuje prywatną sieć blockchain i archiwum zaufanej strony trzeciej jaką jest KIR [23], [24]. Rozwiązanie to wykorzystuje nie tylko blockchain oparty na Hyperledger Fabric (HLF), ale też macierz obiektową WORM (ang. *Write Once, Read Many*) firmy Hitachi, która pozwala na jednokrotny zapis danych na nośniku, bez późniejszej możliwości ich modyfikowania [25]. Całość rozwiązania została zaimplementowana w chmurze oraz zintegrowana z siecią blockchain HLF, w której przechowywana jest suma kontrolna opublikowanych dokumentów [26].

Rozwiązanie [27] oferuje możliwość trwałego nośnika na bazie blockchain jak i możliwość podpisywania dokumentów podpisem elektronicznym. By zapobiec przesyłaniu dokumentów poufnych do zaufanej strony trzeciej, oferowany jest dedykowany węzeł zwany S3DOC Witness. Usługa wspomnianego wcześniej węzła polega na weryfikacji łańcuchów bloków, przekazywane do niego są wyłącznie dane, które umożliwiają walidację łańcucha bloków wyłączając dane osobiste i finansowe. W związku z powyższym ten komponent może zostać uruchomiony u zaufanej trzeciej strony bez potrzeby podpisywania specjalnych umów o przekazaniu przetwarzania danych osobowych [27].

Technika przedstawiona w [28] przechowuje w blockchain całe kompletne dokumenty, których treść w momencie publikacji ulega dekompozycji i rozproszeniu po węzłach sieci blockchain. Rozwiązanie to stosują między innymi firmy Tauron, Syneriz, Polska Sekcja IEEE oraz Politechnika Świętokrzyska [29].

Dedykowana usługa elektroniczna do podpisywania elektronicznie dokumentów z wykorzystaniem nośnika trwałego została także opisana w pracy [30]. Pomysł opiera się na własnej implementacji technologii blockchain, która jest zgodna z rozporządzeniem wydanym przez Unię Europejską eIDAS [31].

Autorzy w [32] wykorzystali technologie WORM oraz blockchain, w której po stronie banku i zaufanej trzeciej strony przechowywane są skróty dokumentów, zaś oryginały dokumentów umieszczone są w macierzy WORM na bezpiecznych zasobach dyskowych. Omawiana usługa pozwala również na przechowywanie danych na określony okres retencji, po zakończeniu którego klient ma możliwość zarządzać dokumentem, czyli np. usunąć go w celu bycia zapomnianym w myśl rozporządzenia RODO.

Podsumowanie przeglądu i analizy rozwiązań stosowanych przez wybrane, największe przedsiębiorstwa w Polsce zaprezentowano w Tabeli 1. Przedstawia ona uproszczone zestawienie technologii jakie wykorzystywane są w celu spełnienia wymagań

nośnika trwałego. Znak „+" w tabeli oznacza, że dana firma wykorzystuje daną metodę, „–" oznacza, że nie wykorzystuje tego rozwiązania, a w jednym przypadku brakuje danych by jednoznacznie wykluczyć tę możliwość.

Tabela 1. Zestawienie rozwiązań stosowanych przez największe przedsiębiorstwa w Polsce

	S3DOC [27]	**Atende ChainDoc** [32]	**KIR, PKO** [23]	**Autenti** [30]	**DoxyChain** [33]	**Billon** [28]
Macierz WORM	+	+	+	–	–	-
Podpis elektroniczny	+	*brak danych*	–	+	+	+
Blockchain	+	+	+	–	+	+

Jak wynika z przeprowadzonej analizy, obecnie najbardziej rozwijającą się technologią w realizacji zaufanych e-usług jest blockchain. Niemniej, warto również zwrócić uwagę na macierz WORM, która jest także chętnie wybieranym rozwiązaniem. Jednak niektórzy obserwatorzy (np. w [34]) sugerują, że wybór tego podejścia przez banki był raczej spowodowany obawą przed karami i krótkim czasem na wdrożenie „gotowego produktu", niż wynikiem poszukiwania najlepszego (najbardziej bezpiecznego, efektywnego i zaufanego) rozwiązania. Wadą macierzy WORM są między innymi koszty, ponieważ są specjalistycznym, dedykowanym rozwiązaniem, co oznacza, że może być ono droższe w zakupie i utrzymaniu w porównaniu do innych, alternatywnych podejść. Innym zagrożeniem może być potencjalna utrata danych, jeśli macierz WORM ulegnie uszkodzeniu lub awarii (specyfika tego sprzętowego rozwiązania powoduje, że odzyskiwanie danych z macierzy WORM może być dużo trudniejsze i bardziej kosztowne niż w przypadku tradycyjnych nośników danych).

Technologia blockchain w ostatnich latach została mocno rozbudowana i jest coraz aktywniej wykorzystywana w różnych dziedzinach gospodarki oraz przedmiotem badań naukowych. Wobec powyższego, zdecydowano się na dokładniejszą analizę możliwości zastosowania technologii blockchain w proponowanym rozwiązaniu, zarówno od strony naukowej, jak i wdrożeniowej oraz prawnej.

2.4.2. Analiza rozwiązań wykorzystujących technologię blockchain

Idea łańcucha połączonych bloków nie jest nowa, opisana po raz pierwszy w 1991 roku [35] i zastosowana do oznaczania dokumentów znacznikami czasu. Prawdziwy postęp technologii blockchain nastąpił wraz z pojawieniem się kryptowaluty Bitcoin w 2009 roku [12]. Przez ostatnie 12 lat technologia ta została mocno rozwinięta i obecnie istnieje wiele różnych wersji i typów blockchain.

Zastosowanie techniki peer-to-peer (P2P) opartej na kryptografii symetrycznej zaproponowano w pracy [36]. Metoda wykorzystuje blockchain Ethereum, w którym tworzone są tzw. „inteligentne kontrakty" w celu zabezpieczenia komunikacji pomiędzy dostawcą danych a konsumentem tych danych. W szczególności dostawca danych rejestruje uprawnionych użytkowników za pomocą listy kontroli dostępu. Dane te są następnie weryfikowane przez konsumentów, co skutkuje uzyskaniem dostępu do inteligentnej umowy. Komunikacja odbywa się w ramach metodologii blockchain Ethereum. Główną zaletą proponowanej metody jest ograniczony i zabezpieczony dostęp do wrażliwych danych, które są chronione przed nieuprawnionym dostępem. Jednak ze względu na utrzymanie zaplecza technicznego takie rozwiązanie w dłuższej perspektywie może być bardzo kosztowne.

Artykuł przeglądowy [37] koncentruje się na analizie metod konsensusu w technikach opartych na łańcuchu bloków. Generalnie można wyróżnić dwa cele takiego konsensusu. Pierwszy związany jest z kolejnością transakcji zapisanych w tzw. księdze (ang. *ledger*), drugi natomiast nastawiony jest na zapobieganie dubletom (czyli dwukrotnemu zapisaniu identycznej transakcji). Autorzy opisali 69 różnych rozwiązań, które podzielono na cztery kategorie, w tym konsensus oparty o dowód pracy (ang. *Proof-of-Work*), dowód koncepcji (ang. *Proof-of-concept*), dowód zasobów (ang. *Proof-of-resources*) i konsensus „bez uprawnień" (ang. *permissionless consensus*). Przeprowadzona analiza wykazała, że większość istniejących (recenzowanych) metod nie spełnia wymaganych (zakładanych przez Autorów) warunków. Artykuł kończy się ponadto stwierdzeniem, że nie ma jasnych, przyszłych kierunków analizowanych technik konsensusu.

Zdecentralizowany schemat podpisu grupowego (ang. *Decentralized Group Signature Scheme* – DGSS) jest rozważany w [38]. Pomysł opiera się na technologii blockchain, natomiast prywatność tożsamości użytkownika jest zabezpieczona przez koncepcję logarytmu dyskretnego. Jak stwierdzają Autorzy, istniejące schematy podpisu grupowego nie są dostatecznie zabezpieczone przed wyciekiem prywatności. Zaproponowana koncepcja składa się z czterech algorytmów (inicjacja, podpisywanie, weryfikacja i implementacja). Główną zaletą proponowanych algorytmów jest wielomianowa złożoność obliczeniowa. Choć pomysł wydaje się ciekawy i użyteczny, w artykule skupiono się głównie na aspektach matematycznych, bez odniesienia do implementacji rozwiązania.

W przypadku systemów opartych na sieci blockchain, PKI zwiększa bezpieczeństwo zarządzania danymi. Ponadto warto wspomnieć, że ataki typu Man-in-the-Middle

(MITM) są mniej prawdopodobne po zastosowaniu technologii blockchain, ponieważ jest ona odporna na manipulacje i żaden złośliwy podmiot nie może zmienić zapisanych danych ani w nie ingerować. Wynika to z faktu, że dane są przechowywane w wielu lokalizacjach, a nie w jednej [39], [40], [41], [42]. Co więcej, pojedynczy wątek komunikacyjny, który mógłby zostać przechwycony, nie stwarza potencjalnego zagrożenia [43].

Kolejny artykuł przeglądowy [44] analizuje obecne wykorzystanie usług elektronicznych i aplikacji w e-administracji. W szczególności praca skupia się na technologii blockchain i bada jej efektywność w e-usługach. Zdaniem autorów w kilku krajach wzrosła rola usług elektronicznych. Ponadto omawiane są możliwe obszary blockchain, w tym kryptowaluty, struktury przechowywania danych, przetwarzanie w chmurze i inne. Warto podkreślić, że zastosowania aplikacji w e-administracji nie są ograniczone do konkretnych metod czy technik. Na koniec dokonano analizy studium przypadku e-usługi opartej na blockchain. W szczególności badane i porównywane są usługi elektroniczne wykorzystywane w Arabii Saudyjskiej z krajami z regionu Zjednoczone Emiraty Arabskie, Bahrajn, Kuwejt, Oman, Katar, Iran, Egipt, Jordania, Irak. Tak szeroka analiza doprowadziła autorów do wniosku o konieczności zamiany tradycyjnych metod i usług na elektroniczne oparte o technologię blockchain.

Artykuł [45] skupia się na wykorzystaniu technologii blockchain w sektorze opieki zdrowotnej. W artykule rozważono kilka możliwych zastosowań medycznych, wskazując główne zalety metod opartych o blockchain. W szczególności omawiane są między innymi neurologia, farmacja, biomedycyna, genomika i medycyna kliniczna. Na przykład taką technologię z powodzeniem wdraża się w zdalnym leczeniu i diagnostyce komórek nowotworowych, gdzie wykorzystuje się inteligentne kontrakty. Kolejna metoda opisana w artykule nawiązuje do teledermatologii, gdzie blockchain wykorzystywany jest podczas konsultacji on-line. Zaprezentowano także koncepcję przechowywania danych DNA w bazie blockchain. W pracy szczegółowo omówiono możliwe zastosowania i wyzwania związane z tą technologią. Jest to jednak typowy artykuł przeglądowy, dlatego nie przedstawiono żadnych nowych pomysłów ani nie zaproponowano nowych technik.

Jak wynika z przeprowadzonej analizy, obecnie najbardziej rozwijającą się technologią w realizacji zaufanych e-usług jest blockchain. Technologia ta w ostatnich latach została mocno rozbudowana i jest coraz aktywniej wykorzystywana w różnych dziedzinach gospodarki oraz badaniach naukowych. Wobec powyższego, zdecydowano się na dokładniejszą analizę możliwości zastosowania technologii blockchain

w planowanym rozwiązaniu, zarówno od strony naukowej, jak i wdrożeniowej oraz prawnej. Dokonano także przeglądu rynkowych rozwiązań oraz artykułów naukowych (w tym artykułów o tematyce prawnej) związanych z zagadnieniem nośnika trwałego, technologii blockchain oraz podpisu elektronicznego. Przeprowadzono również analizę porównawczą wad i zalet stosowanych algorytmów kryptograficznych, jak i rozwiązań wpływających na bezpieczeństwo e-usług. W tabeli 2 zaprezentowano porównanie trzech stosowanych i najbardziej popularnych typów technologii blockchain.

Tabela 2. Porównanie trzech najbardziej popularnych typów technologii blockchain

Cecha	Publiczny blockchain	Prywatny blockchain	Hybrydowy blockchain
Prywatność	prywatny	częściowo prywatny	prywatny
Anonimowość	pseudoanonimowy	brak anonimowości	brak anonimowości
Transparentność	transparentny	brak pełnej transparentności	brak pełnej transparentności
Skalowalność	słaba skalowalność	skalowalny	skalowalny
Bezpieczeństwo	bezpieczny	bezpieczny	bezpieczny

Występujące w tabeli pojęcie *pseudoanonimowy* oznacza, że mimo iż w sieci blockchain przechowywane transakcje są zaszyfrowane kluczem publicznym użytkownika, to na podstawie tego klucza można prześledzić każdą transakcję zapisaną w blokach i w ten sposób odnaleźć wszystkie transakcje danego użytkownika. Jeśli w jakikolwiek sposób możliwe będzie powiązanie klucza publicznego użytkownika z fizyczną osobą, to w ten sposób można ujawnić wszystkie transakcje tej osoby zapisane w blockchain.

Podsumowując, technologia blockchain ma ogromny potencjał do zrewolucjonizowania sposobów, w jaki przetwarzane są dane i realizowane są transakcje. Jej właściwości, takie jak decentralizacja czy niezmienność i bezpieczeństwo, czynią ją atrakcyjną w projektowanych zastosowaniach. Dodatkowo każdy z typów blockchain ma swoje wady i zalety, a wybór odpowiedniego zależy od konkretnych wymagań organizacji lub projektu. Niemniej jednak każdy typ blockchain posiada także główne zalety tej technologii i może zaoferować bezpieczną i przejrzystą architekturę do przechowywania wrażliwych danych w formie rozproszonej i niemodyfikowalnej.

2.4.3. Analiza rozwiązań wykorzystujących zaufaną trzecią stronę

Istnieje wiele rozwiązań wykorzystujących zaufaną trzecią stronę (TTP), które różnią się między sobą pod względem skali działania, sposobu implementacji i kompetencji. Do najważniejszych rozwiązań w zakresie TTP należą:

- instytucje finansowe, takie jak banki czy firmy ubezpieczeniowe, które pełnią rolę zaufanych pośredników w procesie wymiany danych i informacji związanych z transakcjami finansowymi,
- systemy certyfikacji, takie jak np. infrastruktura klucza publicznego (ang. *Public Key Infrastructure* – PKI), które umożliwiają weryfikację tożsamości użytkowników i zapewnienie bezpieczeństwa przesyłanych danych,
- platformy do zarządzania dokumentami elektronicznymi, które pozwalają na bezpieczne przechowywanie, przetwarzanie i wymianę dokumentów elektronicznych.

Warto zauważyć, że gdy usługa jest świadczona z udziałem skonfliktowanych ze sobą stron, konsensus można osiągnąć poprzez włączenie do transakcji cyfrowych zaufanej trzeciej strony (TTP). Z drugiej strony, jeśli problemem może być konieczność zaufania jednej, wybranej stronie (tu TTP), sieć blockchain może decentralizować zaufanie (zaufanie rozłożone jest wtedy na wiele węzłów). Natomiast problemem wynikającym z zastosowania technologii blockchain jest to, że nie istnieje żaden natywny mechanizm do bezpiecznego zarządzania tożsamością zaangażowanych aktorów [46].

Rozwiązania wykorzystujące TTP są szeroko znane i stosowane na przestrzeni ostatnich kilkudziesięciu lat. Już w latach 90-tych XX wieku zaczęto prowadzić badania wokół koncepcji TTP i szukano rozwiązania problemu dostarczania usług zaufanej trzeciej strony [47], takich jak np. zarządzanie kluczami kryptograficznymi dla szyfrowania end-to-end w sposób spełniający wymogi prawne. Autorzy w pracy [47] przedstawiają również inne możliwości i problemy w zastosowaniu trzeciej strony, np. konieczność hierarchizowania certyfikacji w celu określenia wspólnego punktu zaufania dla różnych TTP, udostępnianie kluczy pomiędzy TTP, propozycja dwukierunkowego schematu komunikacji, w którym wykorzystuje się dwa klucze – po jednym do każdego kierunku (można także oba te klucze połączyć w jeden klucz lub używać tylko jednego z nich) [47].

Dostępne są też rozwiązania, w których opracowano modele zabezpieczenia danych w chmurze przy wykorzystaniu TTP, która odpowiada tu za uwierzytelnianie danych, poufność i integralność danych. W tym celu wykorzystywane są jednorazowe hasła (ang. *One-Time Password* – OTP) do zapewnienia uwierzytelnienia. Ponadto, poufność danych zapewniają algorytmy wykorzystane do szyfrowania i deszyfrowania danych, a integralność danych zapewniona jest poprzez wykorzystanie skrótów (hasz) danych [48].

Inne interesujące zastosowanie „półzaufanej" strony trzeciej (ang. *Semi-Trusted Third Party*) przedstawiono w pracy [49], gdzie autorzy wprowadzają protokół znaku wodnego

dla kupującego i sprzedającego, który może być przydatny w zapobieganiu kopiowaniu i ochronie prywatności w środowisku chmury obliczeniowej. Proponowane rozwiązanie łączy w sobie usługi infrastruktury chmurowej jako usługi (ang. *Infrastructure as a Service* – IaaS), dostawcę usług w chmurze (ang. *Cloud Service Provider* – CSP) traktowanego tu jako „półzaufaną" trzecią stronę, kryptosystem homomorfizmu prywatności z algorytmem wymiany kluczy Diffiego-Hellmana oraz sprawdzone i wiarygodne techniki znakowania wodnego. Proponowane podejście próbuje rozwiązać problemy śledzenia piractwa, anonimowości lub problemy dot. praw klienta. Chmura odgrywa tutaj kluczową rolę, ponieważ zmniejsza obciążenie komunikacyjne i wspiera proces znakowania wodnego.

W pracy [50] autorzy proponują schemat TTP oparty na tzw. *signcryption* wykorzystujący protokół wymiany kluczy sesji jako symetrycznych. Dzięki temu protokół wymiany kluczy sesji zapobiega podsłuchiwaniu podczas ataków takich jak Denial of Service (DoS) [51] i Man-in-the-Middle (MITM) [52]. Ponieważ proces szyfrowania realizowany jest przez użytkownika usług chmurowych (ang. *Cloud Service User* – CSU), a proces deszyfrowania przez dostawcę usług w chmurze (CSP), dodatkowe obciążenie związane z szyfrowaniem i odszyfrowywaniem TTP zostało tu zredukowane. Ponadto główną rolą TTP w prezentowanym rozwiązaniu jest rozstrzyganie ewentualnych sporów pomiędzy CSU a CSP. Proponowany system zapewnia siedem funkcji bezpieczeństwa, takich jak integralność danych, poufność danych, autentyczność, niezaprzeczalność, tajemnica przekazywania, niefałszowalność i nieidentyfikowalność.

W artykule [53] autorzy prezentują schemat wymiany kluczy i szyfrowanie danych poprzez zaufaną trzecią stronę pomiędzy użytkownikami. Celem jest tu zapewnienie dobrego bezpieczeństwa między wymienianymi danymi, a także przeniesienie większości obciążenia obliczeniowego na TTP. Za przechowywanie i okresowe odnawianie certyfikatów klucza publicznego może także odpowiadać zaufana trzecia strona. Proponowane rozwiązanie łączy TTP z kryptografią symetryczną i asymetryczną, zapewniając wysoki poziom bezpieczeństwa danych.

Kolejnym ciekawym rozwiązaniem jest opracowany w pracy [54] protokół, który łączy zalety bezpieczeństwa, skalowalności, prostoty implementacji i możliwości realnego wdrożenia. Protokół wykorzystuje tzw. *lekką zaufaną trzecią stronę* działającą on-line. Dzięki temu od odbiorcy końcowego wymagany jest tylko standardowy czytnik poczty elektronicznej oraz przeglądarka internetowa. Proponowane rozwiązanie nie potrzebuje także infrastruktury klucza publicznego.

W artykule [55] autorzy wykorzystali TTP do opracowania bezpiecznego protokołu sumy [56] do poprawy prywatności i bezpieczeństwa danych, gdy są one zbierane z różnych źródeł do wykonania bezpiecznych obliczeń wielostronnych (ang. *Multi-Party Computations*). Proces obliczeniowy, który jest wykonywany przez TTP, zapewnia większe bezpieczeństwo i osiąga niższą złożoność obliczeniową niż istniejące bezpieczne protokoły sum.

Badania w kierunku wykorzystania TTP pojawiają się także w informatyce kwantowej. W [57] autorzy proponują zaufany protokół TPEP (ang. *Third Party E-Payment*) bazujący na kwantowym podpisywaniu bez splątania, podczas którego wszyscy uczestnicy w ciągu całej transakcji operują jednocząsteczkową bramką kwantową *H*. Zdaniem autorów, prezentowany protokół zużywa mniej zasobów i jest łatwiejszy do realizacji od innych protokołów wykorzystujących stany splątane. Natomiast w pracy [58] opracowany został nowatorski schemat DMMQSS (ang. *Dynamic Multiparty To Multiparty Quantum Secret Sharing Scheme*), który przygotowuje wszystkie zasoby kwantowe, dzięki czemu żaden z uczestników schematu nie musi przygotowywać żadnych kwantowych zasobów splątanych, co skutecznie zmniejsza liczbę generatorów qubitów [58].

Analiza pokazała, że także w modelowaniu systemów inteligentnego domu można wykorzystać TTP, które działa tu jako framework pośredniczący w komunikacji i transmisji danych [59]. Skutkuje to, zdaniem autorów, zwiększoną wydajnością energetyczną, dłuższym czasem życia systemu i szybszym dostarczaniem danych. Z pomocą TTP i timera zdarzeń, PRR (ang. *Packet Reception Ratio*) jest na wysokim poziomie ok. 91%. Ponadto narzut sieci jest zmniejszony, średnia latencja pakietów jest znacznie zredukowana, a przepustowość jest zwiększona.

Koncepcja TTP jest także dobrze znana i stosowana w celu zapewnienia bezpieczeństwa w aplikacjach medycznych [60]. Polega ona na wykorzystaniu zaufanej trzeciej strony do potwierdzania prawdziwości przesyłanych wiadomości, zarządzania kluczami kryptograficznymi dla szyfrowania end-to-end oraz zabezpieczania przed atakami typu DoS lub MITM. Jest to alternatywny system dla dobrze znanej infrastruktury klucza publicznego (PKI).

Również w steganografii audio można efektywnie wykorzystywać zaufaną trzecią stronę. W pracy [61] autorzy wykorzystują klucz indeksowania z TTP, który zwiększa poufność tajnej wiadomości i dodaje kolejną warstwę ochrony dla modułu dekodera. Prezentowana metodologia wykorzystywana jest przy plikach audio i najlepiej nadaje się dla 32-bitowych plików, ponieważ w ich strukturze jest więcej dostępnych tzw. *Least*

Significant Bits (LSBs), które można wykorzystać do przesłania tajnej wiadomości. Warto zauważyć, że zgodnie z definicją steganografii, nie tylko jest tu szyfrowana wiadomość, ale utajniony jest sam fakt jej przesyłania.

Autorzy w pracy [62] prezentują ciekawe i efektywne podejście poprawiające bezpieczeństwo danych w chmurze obliczeniowej (dla tzw. cloud client'a – CC) z wykorzystaniem półzaufanego audytora strony trzeciej (ang. *Third Party Auditor* – TPA). Proponowana koncepcja przyjmuje zaawansowany standard szyfrowania, aby wspierać prywatność właściciela danych oraz kryptograficzną funkcję skrótu, aby utrzymać integralność danych właściciela. Ponadto wykorzystuje kryptografię krzywej eliptycznej, aby zapewnić poufność danych, poprawność i bezpieczeństwo podczas przesyłania danych przez niezabezpieczone kanały. Użyta tu została także funkcja szyfrowania AES do zabezpieczenia danych podczas audytu. Oznacza to, że częściowo zaufany TPA nie może ujawnić ani wyodrębnić zawartości pliku danych i jest on odpowiedzialny za audyt integralności danych w chmurze w imieniu CC (ponieważ TPA posiada wiedzę i możliwości, których nie posiada CC). Zdaniem autorów, zaletą proponowanego podejścia jest właśnie to, że TPA nie jest w stanie wydobyć zawartości danych przechowywanych na serwerze w chmurze podczas procesu audytu, co eliminuje koszty związane z audytem i łagodzi obawy CC przed wyciekiem danych.

Zaufana strona trzecia jest też obecna w wielu innych dziedzinach. Np. połączenie TTP oraz systemów agentowych może pomóc w kontroli jakości umów o świadczenie usług oraz zagwarantowania przejrzystości i symetrii w odniesieniu do umów o gwarantowanym poziomie świadczenia usług (ang. *Service Level Agreement* – SLA) pomiędzy potencjalnymi sygnatariuszami [63].

Ciekawe są także badania dotyczące wykorzystania TTP w zarządzaniu usługami w chmurach samochodowych [64]. Autorzy porównują dwa algorytmy: *Service Latency Sensitive Mode* (SLSM) i *Neutral mode* do łączenia się pojazdów z chmurą obliczeniową z wykorzystaniem TTP w celu dostarczania usług. W efekcie, opóźnienia w połączeniu pojazdów z TTP są mniejsze (w zależności od ilości dostawców, liczby pojazdów jak i liczby dostępnych usługodawców).

W obszarze kryptowalut i technologii blockchain, badacze zwracają uwagę na problem braku zaufania, który jest związany z transakcjami w sieci Bitcoin. Ponieważ transakcje te są nieodwracalne, konsumenci mogą obawiać się ich zawierania [65]. W pracy [66] autorzy wskazują, że mimo wielu zalet jakie niesie technologia blockchain z jej zdecentralizowanym rejestrem (ang. *ledger*) przechowującym bloki, w wielu

zastosowaniach nie da się zastąpić zaufania reprezentowanego przez fizyczny podmiot lub osobę. W niektórych przypadkach konieczne będzie zaangażowanie drugiej strony w celu weryfikacji pewnych predykatów. Ogólnie rzecz biorąc, predykaty zależne np. od pomiarów czujnika pozostaną zewnętrzne, ponieważ czujnik jest obiektem fizycznym, którego nie można w całości przedstawić w systemie cyfrowym. W rezultacie, chociaż technologia blockchain ma potencjał dla nowych zastosowań, wiele przypadków nadal będzie wymagać zaufanej trzeciej strony.

2.5. Podsumowanie

Jak wynika z przeprowadzonych analiz, zagadnienie nośnika trwałego dalej stanowi problem natury prawnej, ponieważ brak jest jednoznacznych wymagań dot. stosowanej technologii, co daje pewną dowolność w wyborze technologii mogących spełniać określone normy prawne i wymagania. Fakt ten daje możliwość wykorzystania zarówno zaufanej trzeciej strony, która zapewnia wiarygodność wymiany danych poufnych pomiędzy stronami (np. przedsiębiorstwem a konsumentami), a także zastosowania technologii blockchain zapewniającej bezpieczeństwo, trwałość i niezmienność danych. Jak widać również ostatnie lata przyniosły ogromny postęp w upowszechnieniu technologii blockchain. Perspektywy rozwoju technologii blockchain są także bardzo obiecujące. Jej zastosowanie ma potencjał wspierający transformacje różnych dziedzin gospodarki, wprowadzając w nich większą przejrzystość, bezpieczeństwo i efektywność operacyjną.

Zarówno koncepcja zaufanej trzeciej strony jak i technologia blockchain są znane i szeroko stosowane od wielu lat, to jednak ich połączenie jest dość innowacyjne, zwłaszcza w kontekście spełnienia założeń trwałego nośnika. I choć samo pojęcie trwałego nośnika nie jest w pełni i jednoznacznie zdefiniowane prawnie, to stawia wysokie wymagania przedsiębiorcom i instytucjom finansowym w zakresie przechowywania i przetwarzania wrażliwych dokumentów elektronicznych. Dlatego istnieje potrzeba poszukiwania bezpiecznych i zaufanych rozwiązań realizowanych w formie usług elektronicznych spełniających wymagania trwałego nośnika. Jednym z takich rozwiązań jest właśnie proponowana w pracy e-usługa, która te wymagania w pełni realizuje, łącząc zalety technologii blockchain i algorytmów kryptograficznych z korzyściami płynącymi z wykorzystania TTP jako niezależnego arbitra i dostawcy e-usługi nośnika trwałego umożliwiającej przetwarzanie oraz zarządzanie wrażliwymi dokumentami elektronicznymi.

3. Proponowana bezpieczna i zaufana e-usługa trwałego nośnika

Wykonany przegląd i analiza rozwiązań dot. trwałego nośnika istniejących zarówno w literaturze jak i dostępnych na rynku w postaci usług i produktów komercyjnych zaowocowała zidentyfikowaniem wymagań funkcjonalnych, jakie powinna spełniać projektowana e-usługa, aby nie tylko odpowiadać na współczesne potrzeby rynku, realizować wymagania nośnika trwałego, ale też być konkurencyjną do innych, obecnych na rynku produktów i usług. Analiza ta wykazała także, że obecnie najbardziej rozwijającym się trendem w realizacji e-usług jest technologia blockchain, której stosowanie staje się powoli synonimem bezpieczeństwa. W połączeniu z wybranymi algorytmami kryptograficznymi (np. funkcje skrótu, kryptografia asymetryczna, podpis cyfrowy) daje to spore możliwości w realizacji ciekawych zastosowań sieci blockchain (także w nowych obszarach takich jak np. zdrowie publiczne i służba zdrowia [67]). Ponadto zauważono coraz większy udział zaufanej trzeciej strony w realizowanych e-usługach, która często pełni rolę niezależnego arbitra realizowanych transakcji, a w niektórych przypadkach jest także dostawcą infrastruktury do implementacji usługi trwałego nośnika lub sama tę usługę oferuje. Dlatego w pracy zdecydowano się na połączenie zalet technologii blockchain (bezpieczeństwo) oraz zaufanej trzeciej strony (zaufanie) do opracowania autorskiej e-usługi trwałego nośnika.

3.1. Wymagania funkcjonalne

Projektowana e-usługa powinna spełniać pod względem funkcjonalnym następujące wymagania:

- dane jednego podmiotu (np. banku) powinny być przechowywane w niepublicznej bazie danych ograniczonej tylko do danych danego podmiotu,
- dane powinny być przechowywane w sposób uniemożliwiający ich modyfikację (po zapisaniu w bazie danych nie powinna istnieć możliwość ich usunięcia lub modyfikacji),
- dane (w tym wrażliwe dokumenty elektroniczne) powinny być przechowywane w formie zaszyfrowanej, aby w przypadku ew. wycieku były one (oraz dane osobowe w nich zawarte) bezużyteczne dla osób trzecich,
- dostęp do danych powinien być z jednej strony wygodny (zwłaszcza dla użytkowników/klientów) a z drugiej bezpieczny i kontrolowany,

- do szyfrowania dokumentów powinien zostać użyty szybki algorytm szyfrowania symetrycznego,
- usługa powinna być opracowana pod kątem podmiotów (np. finansowych) z dużą liczbą klientów (podmiot pełni tu rolę dominującą), którzy mają potrzebę przechowywania i przetwarzania dokumentów zgodnie z wymaganiami trwałego nośnika (zgodnie z polskimi regulacjami prawnymi), ale z drugiej strony na tyle uniwersalna, aby możliwe było zastosowanie jej do wielu równorzędnych podmiotów (np. kilka przedsiębiorstw połączonych relacjami biznesowymi),
- dane powinny być zapisane w zdecentralizowanej bazie danych pozwalającej na rozproszenie danych między węzłami,
- usługa powinna oferować możliwość generowania klucza symetrycznego AES i szyfrowania/deszyfrowania go za pomocą pary kluczy asymetrycznych RSA.

Dokładna analiza powyższych wymagań pozwoliła nakreślić koncepcję rozwiązania oraz technologie niezbędne do realizacji ww. wymagań. Do przechowywania danych przetwarzanych w ramach projektowanej e-usługi zdecydowano się na wybór prywatnej sieci blockchain (po jednej dla każdego podmiotu „dominującego"). Określono także rolę zaufanej trzeciej strony w proponowanym rozwiązaniu. Ponadto do rozwiązania włączono także wybrane metody kryptografii symetrycznej (AES-256), asymetrycznej (RSA-2048), podpisu cyfrowego i funkcji skrótu (SHA-256). Całość została spięta opisem algorytmu, który szczegółowo przedstawia zadania TTP oraz prezentuje wykorzystanie każdej z tych technologii oraz metod. To właśnie algorytm e-usługi zostanie zaprezentowany jako pierwszy w dalszej części niniejszego rozdziału.

3.2. Algorytm projektowanej e-usługi

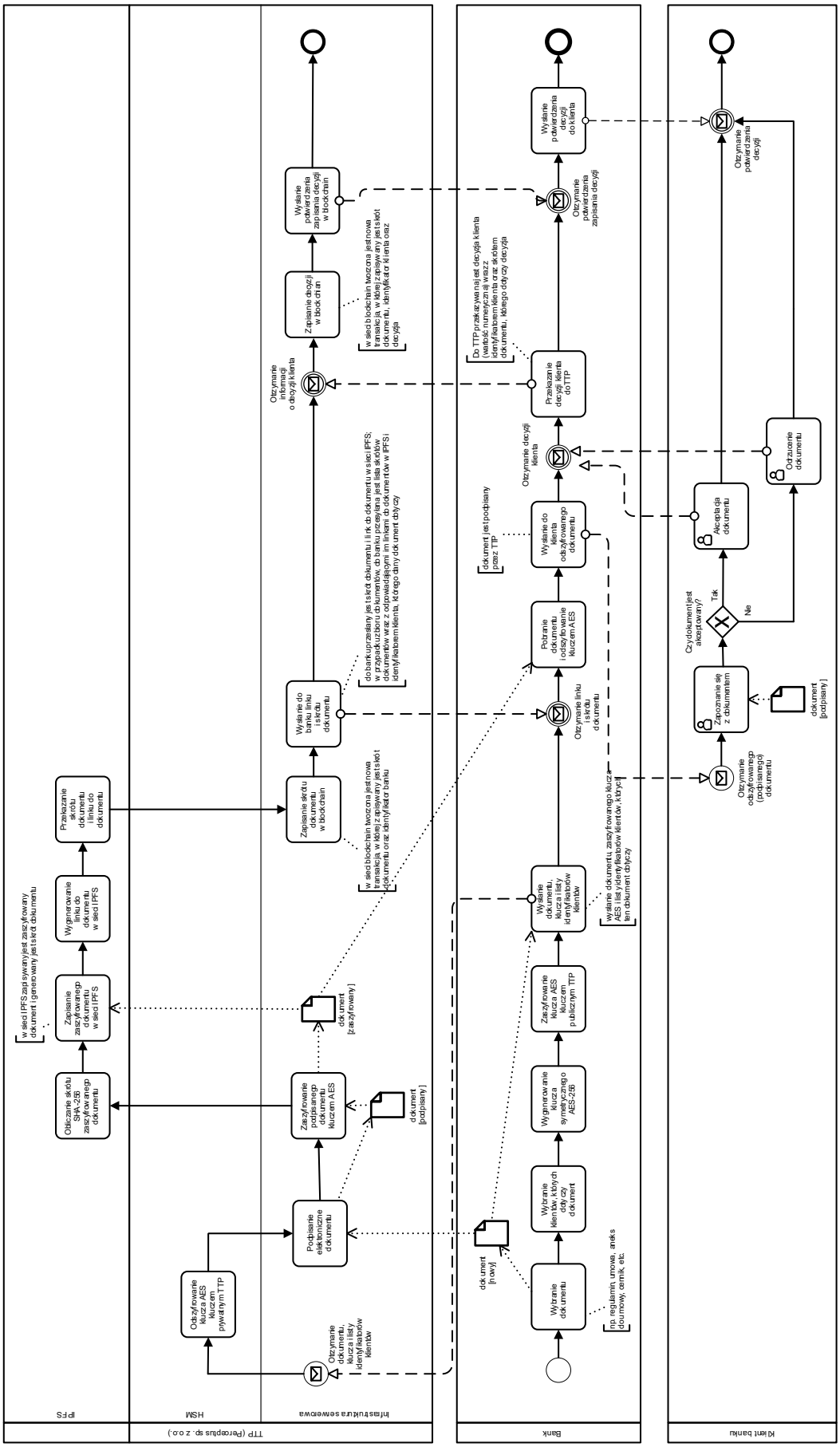
W trakcie prowadzonych badań nad opracowaniem bezpiecznej i zaufanej usługi trwałego nośnika opartej o technologię blockchain, rozważano szereg możliwych podejść do problemu oraz analizowano możliwości zastosowania sieci blockchain, zaufanej trzeciej strony oraz wybranych algorytmów kryptograficznych. W efekcie tych prac powstało kilka koncepcji proponowanej e-usługi. Niektóre z nich zostały opublikowane w artykułach konferencyjnych [68] oraz w czasopismach naukowych [69]. W niniejszej pracy zaprezentowano finalną, najbardziej dojrzałą koncepcję e-usługi trwałego nośnika.

Proponowana e-usługa została opracowana pod kątem dużych podmiotów i instytucji finansowych (np. banków), posiadających dużą liczbę klientów (liczoną często w dziesiątkach lub setkach tysięcy), które mają potrzebę bezpiecznego przechowywania

i przetwarzania dokumentów dot. swoich klientów, takich jak np. umowy, aneksy do umów, cenniki, regulaminy itp., zgodnie z wymaganiami trwałego nośnika, zapewniającymi m.in. trwałe przechowywanie dokumentów i ich niezmienność przy jednoczesnym dostępie do nich każdej ze stron (np. banku i klienta). W przyjętych założeniach bank (lub inny duży podmiot) jest stroną dominującą, która inicjuje każdą transakcję dot. przetwarzania dokumentów (np. zmiana regulaminu, warunków umowy, cennika, wprowadzenie aneksu do umowy itp.). Klienci mają tylko możliwość akceptacji bądź odrzucenia proponowanego im dokumentu, bez możliwości inicjowania procesu przetwarzania nowego dokumentu. Rolą zaufanej trzeciej strony jest dostarczenie niezbędnych usług (w tym usług kryptograficznych z wykorzystaniem sprzętowych modułów bezpieczeństwa) i infrastruktury serwerowej, w której zrealizowana jest sieć blockchain oraz IPFS (ang. *Interplanetary File System* – IPFS).

Na rysunku 3.1 zaprezentowano algorytm e-usługi opracowany w notacji BPMN [70] (ang. *Business Process Model and Notation*). Notacja ta z powodzeniem stosowana jest do modelowaniu procesów biznesowych i zdaniem autora dobrze nadaje się także do prezentacji proponowanego rozwiązania, gdyż przyjęty poziom abstrakcji e-usługi jest bliższy koncepcjom biznesowym niż systemowym. Na prezentowanym diagramie BPMN występują trzej aktorzy (reprezentowani jako tzw. pule i tory, ang. *pools and lanes*): bank, klient banku (dla zwiększenia czytelności diagramu pokazano działanie e-usługi tylko dla jednego, przykładowego klienta) oraz zaufana trzecia strona (tu rolę TTP pełni firma Perceptus sp. z o.o. oferująca e-usługę trwałego nośnika, w tej puli wyszczególniono trzy wewnętrzne tory dot. infrastruktury serwerowej firmy, sprzętowego modułu bezpieczeństwa, ang. *Hardware Security Module* – HSM oraz sieci IPFS).

Cały proces rozpoczyna się od aktora jakim jest bank, który chce uzgodnić z klientem nowy dokument (np. regulamin, umowa, aneks, cennik itp.) lub nową wersję istniejącego dokumentu (z punktu widzenia algorytmu traktowane jest to jak przetwarzanie nowego dokumentu). W pierwszym kroku bank wybiera dokument, który chce przetwarzać oraz określa listę klientów, których ten dokument dotyczy (przygotowywana jest lista identyfikatorów tych klientów). W kolejnym kroku bank generuje dla danego dokumentu 256-bitowy klucz symetryczny korzystając z algorytmu AES-256, a następnie szyfruje ten klucz symetryczny AES kluczem publicznym RSA należącym do TTP. Klucz publiczny TTP to jeden z pary 2048-bitowych kluczy RSA wygenerowanych w HSM dla TTP. Klucz publiczny TTP jest udostępniany zewnętrznym podmiotom (np. bankowi), natomiast klucz prywatny TTP nie jest upubliczniany i przechowywany jest wyłącznie w HSM.



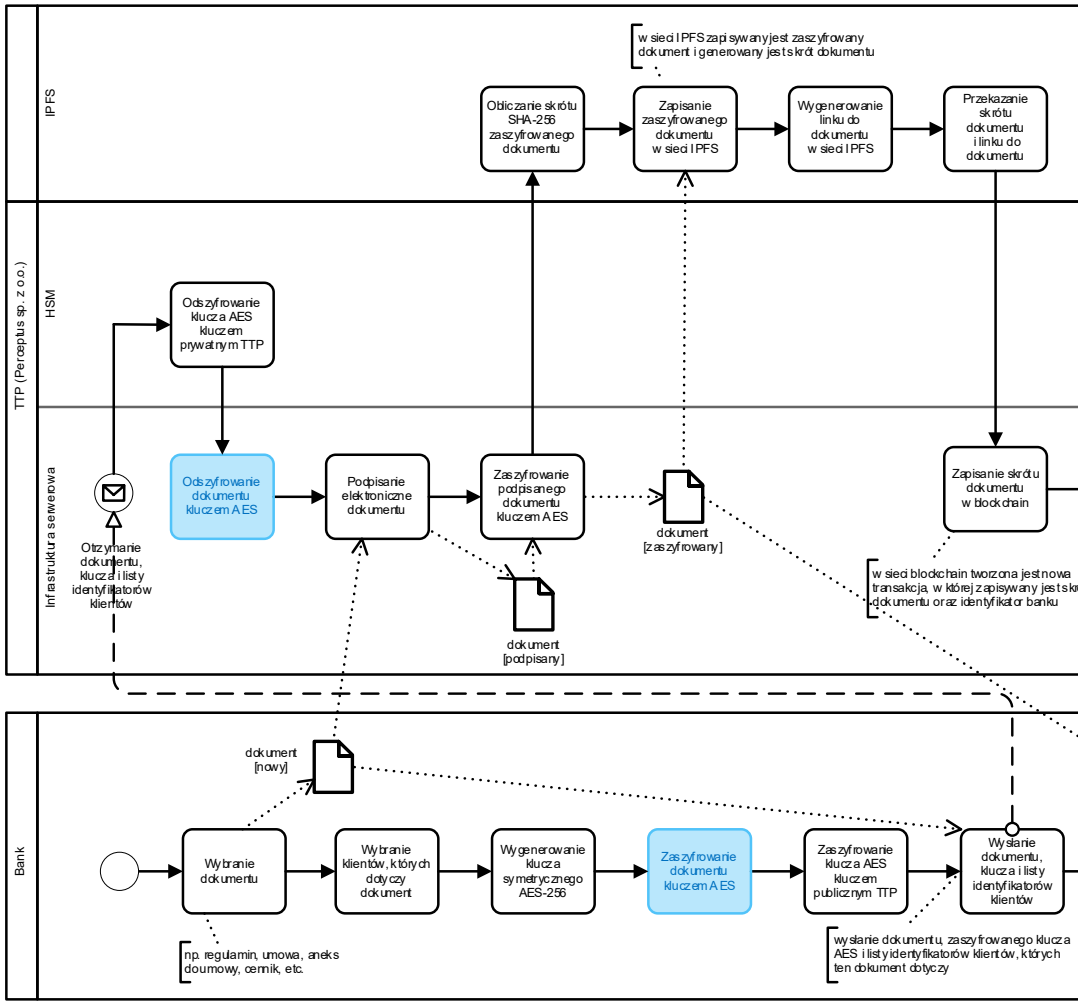
Rys. 3.1. Diagram BPMN dla proponowanej e-usługi trwałego nośnika

Kolejny etap to przesłanie do TTP wybranego dokumentu (np. nowego regulaminu), listy identyfikatorów klientów, którzy mają podjąć decyzję dot. akceptacji lub odrzucenia tego dokumentu oraz zaszyfrowanego klucza symetrycznego AES. Warto zauważyć, że w opisywanym podejściu, dokument przetwarzany przez wszystkich klientów jest dokładnie ten sam (oczywiście można sobie wyobrazić inny scenariusz, kiedy bank będzie przetwarzać dokumenty, które będą spersonalizowane pod kątem każdego z klientów; wtedy do TTP zamiast jednego dokumentu przesłany zostanie cały zbiór dokumentów z odpowiadającymi im identyfikatorami klientów oraz zaszyfrowanymi kluczami AES – po jednym dla każdego dokumentu).

W kolejnym kroku TTP, korzystając z HSM odszyfrowuje kluczem prywatnym RSA będącym w posiadaniu TTP otrzymany zaszyfrowany klucz AES. Następnie TTP podpisuje dokument elektronicznie i szyfruje go za pomocą odszyfrowanego klucza AES. W dalszych etapach przetwarzany jest już wyłącznie zaszyfrowany dokument.

Warto zwrócić uwagę na cel użycia w proponowanym rozwiązaniu kryptografii asymetrycznej. Dzięki wykorzystaniu 2048-bitowego klucza publicznego TTP, klucz symetryczny AES wygenerowany przez bank jest bezpiecznie przesyłany do TTP. Nawet atak typu Man-In-the-Middle lub inny powodujący przejęcie tego zaszyfrowanego klucza AES okaże się nieskuteczny, gdyż bez prywatnego klucza RSA, przechowywanego wyłącznie w HSM po stronie TTP, nie da się go odszyfrować. Prywatny klucz RSA jest generowany w HSM, nigdy nie opuszcza HSM i nie jest ujawniany, ponieważ operacja deszyfrowania za pomocą tego klucza odbywa się także wyłącznie w HSM.

Godnym uwagi jest również fakt, że w prezentowanym algorytmie dokument przesyłany przez bank do TTP jest w formie jawnej, choć za pomocą bezpiecznego, ustalonego wcześniej przez obie strony kanału komunikacyjnego. Mimo to, ew. przejęcie jawnego dokumentu przez nieuprawnioną osobę, może mieć negatywne skutki, ponieważ przesyłany dokument może zawierać dane osobowe klientów, czy inne wrażliwe informacje. Dlatego można prezentowany algorytm nieco zmodyfikować, wprowadzając dodatkowy krok po stronie banku dot. szyfrowania wybranego dokumentu za pomocą wygenerowanego symetrycznego klucza AES i dopiero ten zaszyfrowany dokument (wraz z zaszyfrowanym kluczem AES) przesłać do TTP. Fragment zmodyfikowanego algorytmu (dodane czynności oznaczono kolorem niebieskim) przedstawiono na rys. 3.2, a cały diagram umieszczono w dodatku A (rys. A.1).

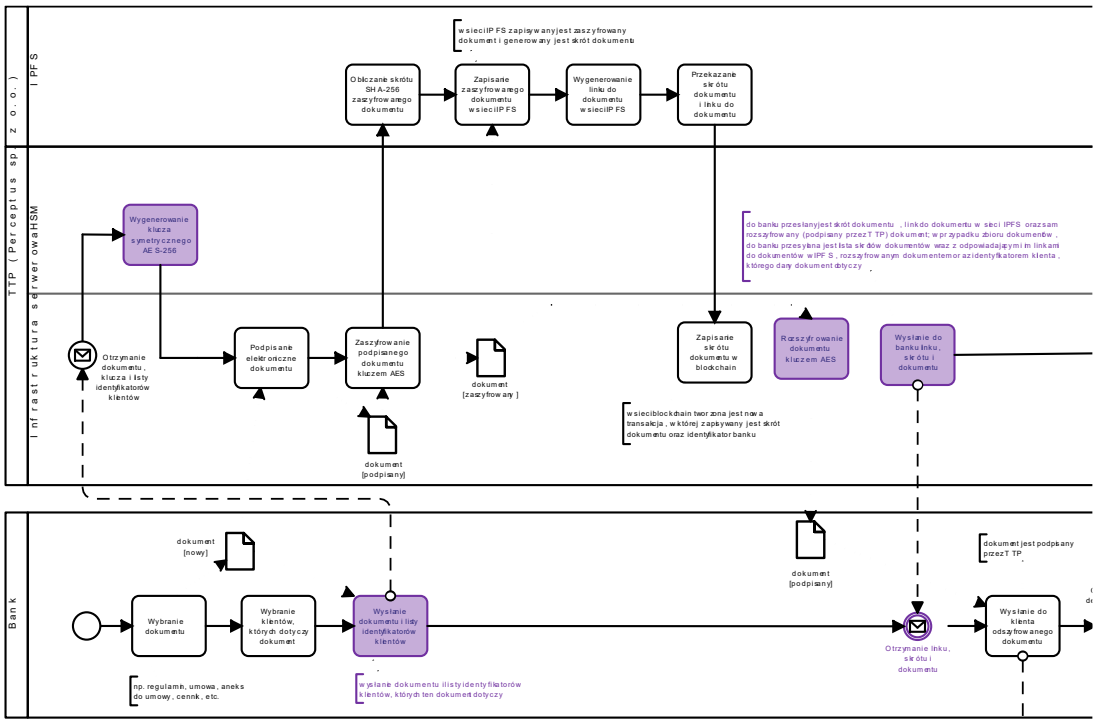


Rys. 3.2. Fragment zmodyfikowanego diagramu BPMN dla proponowanej e-usługi (szyfrowanie dokumentu przez bank)

W takim przypadku, przejęcie zaszyfrowanego dokumentu będzie dla cyberprzestępcy bezużyteczne. Takie rozwiązanie z jednej strony czyni kanał komunikacyjny pomiędzy bankiem a TTP bezpiecznym, ale z drugiej narzuca na bank konieczność wykonania dodatkowej operacji jakiej jest szyfrowanie dokumentu, co przy dużym zbiorze dokumentów (np. w liczbie kilkudziesięciu lub kilkuset tysięcy) może znacznie obciążyć infrastrukturę obliczeniową banku, dlatego to podejście traktowane jest w pracy jako alternatywne.

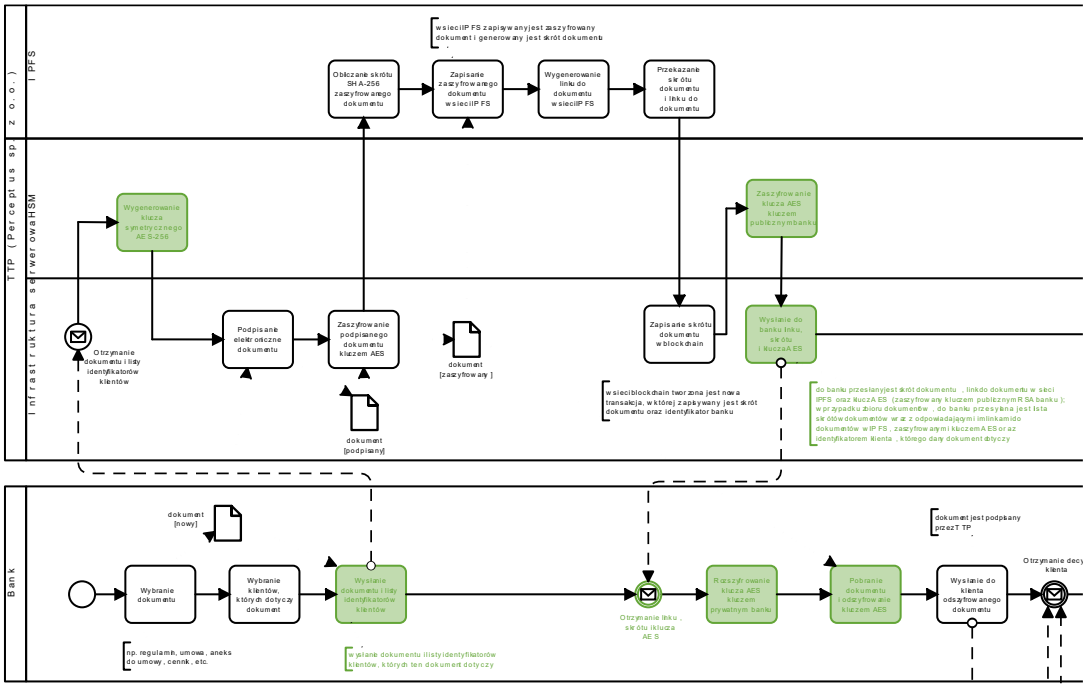
Innym, alternatywnym podejściem może być sytuacja, w której bank zrezygnuje z generowania kluczy symetrycznych AES i zadanie to (podobnie jak szyfrowanie i deszyfrowanie dokumentów) będzie leżeć wyłącznie po stronie TTP. W tym podejściu można rozważyć dwa rozwiązania dot. przekazania do banku informacji dot. umieszczonego w sieci IPFS zaszyfrowanego dokumentu. W pierwszym z nich przed przekazaniem do banku skrótu do dokumentu i linka do dokumentu w sieci IPFS, dokonane będzie rozszyfrowanie dokumentu i przesłanie go do banku w formie

niezaszyfrowanej (ale podpisanej przez TTP). Warto zauważyć, że także w formie niezaszyfrowanej był on przekazany do banku (oczywiście przesyłanie dokumentów do i z banku może być zrealizowane za pomocą ustalonego wcześniej, bezpiecznego kanału komunikacji pomiędzy bankiem a TTP). Fragment takiego algorytmu zaprezentowano na rys. 3.3 (zmodyfikowane czynności w stosunku do wersji algorytmu z rys. 3.1 oznaczono kolorem fioletowym), a kompletny diagram przedstawiono w dodatku A (rys. A.2).



Rys. 3.3. Fragment zmodyfikowanego diagramu BPMN dla proponowanej e-usługi (generowanie klucza AES oraz odszyfrowanie dokumentu przez TTP)

Drugie rozwiązanie zakłada przekazanie wraz ze skrótem dokumentu i linkiem także wygenerowanego przez TTP klucza symetrycznego AES, którym został zaszyfrowany dokument umieszczony w sieci IPFS. Klucz ten jednak musi zostać przekazany w formie zaszyfrowanej. Można tu wykorzystać kryptografię asymetryczną, zakładając, że bank posiada parę kluczy RSA (publiczny i prywatny). Klucz symetryczny AES byłby zaszyfrowany kluczem publicznym RSA należącym do banku i bezpiecznie przesłany (nawet niezabezpieczonym kanałem). Korzystając ze swojego klucza prywatnego RSA, bank odszyfrowałby klucz symetryczny AES, którym mógłby następnie odszyfrować dokument pobrany z serwera IPFS przed wyświetleniem go klientowi. Fragment algorytmu z drugim rozwiązaniem pokazano na rys. 3.4 (zmodyfikowane czynności w stosunku do pierwotnej wersji algorytmu z rys. 3.1 oznaczono kolorem zielonym), a kompletny diagram przedstawiono w dodatku A (rys. A.3).



Rys. 3.4. Fragment zmodyfikowanego diagramu BPMN dla proponowanej e-usługi (generowanie klucza AES oraz szyfrowanie go przez TTP)

Wracając do głównego algorytmu, w następnym kroku prezentowanego algorytmu zaszyfrowany dokument umieszczany jest przez TTP na serwerze IPFS. Serwer IPFS oblicza skrót dokumentu oraz generuje link, który razem z wygenerowanym skrótem przesyła zwrotnie do TTP. Następnie TTP skrót ten umieszcza w strukturze blockchain. W rzeczywistości do sieci blockchain dodawany jest nowy blok z transakcją zawierającą m.in. skrót dokumentu oraz identyfikator podmiotu, który przesłał dokument (tu: bank). Warto zauważyć, że sam dokument, ze względu na ograniczenia technologii blockchain (limit danych możliwych do zapisania w jednej transakcji) nie jest zapisywany w sieci blockchain. Właściwy, zaszyfrowany dokument wraz z jego skrótem przechowywany jest na zewnętrznym serwerze IPFS. Ponieważ ten sam skrót dokumentu umieszczony jest także w sieci blockchain, połączenie logiczne transakcji w blockchain z fizycznym właściwym dokumentem nie jest trudne (serwer IPFS może być efektywnie przeszukiwany na podstawie skrótu dokumentu). Warto także wspomnieć, że w sieci blockchain celowo nie jest zapisywany link do dokumentu w IPFS, ponieważ byłoby to ograniczeniem proponowanego rozwiązania. Zmiana linku, np. z powodu zmiany infrastruktury IPFS spowodowałaby, że link umieszczony w blockchain byłby nieprawidłowy, a z założenia zmiana danych w sieci blockchain jest niedopuszczalna. Przechowywanie tylko skrótu zaszyfrowanego dokumentu zarówno w strukturze blockchain oraz na serwerze IPFS pozwala na większą elastyczność rozwiązania (w tym np. przeniesienie dokumentów na inny serwer IPFS).

W kolejnym etapie skrót dokumentu oraz link do dokumentu w IPFS przesyłane są zwrotnie do banku. W przypadku zbioru dokumentów, zwrotnie przesłana byłaby lista skrótów dokumentów wraz z odpowiadającymi im linkiem do dokumentu w IPFS i identyfikatorem klienta, którego dany dokument dotyczy (w przypadku jednego dokumentu, który dotyczy wszystkich klientów przesyłanie identyfikatorów klientów wydaje się zbędne).

Następnie bank za pomocą otrzymanego linku pobiera dokument z sieci IPFS i rozszyfrowuje go posiadanym symetrycznym kluczem AES. W kolejnym kroku bank (ustalonym wcześniej z klientem bezpiecznym kanałem komunikacyjnym) przesyła rozszyfrowany dokument klientowi. Warto zaznaczyć, że dokument prezentowany klientowi jest dokumentem podpisanym przez TTP, dzięki temu klient ma pewność, że przetwarzany dokument jest tym właściwym (którego skrót umieszczony jest w sieci blockchain, a sam dokument w sieci IPFS), co znacznie ogranicza możliwość manipulacji przez bank i podnosi zaufanie klientów do całej usługi.

Na prezentowanym schemacie funkcjonalność wyświetlenia rozszyfrowanego dokumentu klientowi dostarcza bank, ale równie dobrze może to być usługa typu „bezpieczny pokój" oferowana przez TTP. Innym rozwiązaniem może być także przekazanie klientowi linku do zaszyfrowanego dokumentu w IPFS wraz z kluczem AES (np. innym kanałem komunikacyjnym). W tej sytuacji po stronie klienta będzie leżeć konieczność pobrania i rozszyfrowania dokumentu.

Innym ważnym aspektem jest także fakt, że w prezentowanym algorytmie to bank jest odpowiedzialny za przesłanie rozszyfrowanego dokumentu (lub linku do dokumentu wraz z kluczem AES) do wszystkich klientów, co zmniejsza ilość przesyłanych do TTP danych i powoduje, że dane osobowe klientów oraz ich dane adresowe (np. adresy e-mail, numery telefonów) nie są przekazywane do TTP. Natomiast trzeba też zwrócić uwagę, że przesyłane przez bank do TTP dokumenty mogą takie dane zawierać i należy to uwzględnić w kontekście wymagań rozporządzenia RODO [71]. Oczywiście można rozważyć przesyłanie do TTP już wcześniej zaszyfrowanych przez bank dokumentów. W tej sytuacji nie przesyłany byłby klucz AES, co wykluczyłoby możliwość ich odczytu przez TTP, a tym samym przetwarzaniu ew. zawartych tam danych osobowych klientów. Nie byłoby także konieczności stosowania kryptografii asymetrycznej RSA, co uprościłoby nieco cały algorytm, ale z drugiej strony TTP nie mógłby podpisać rozszyfrowanego dokumentu (a w takiej wersji prezentowany jest on klientów), co zmniejszyłoby wiarygodność i zaufanie klientów do tej usługi. Rola TTP ograniczona

zostałaby wyłącznie do podmiotu odpowiedzialnego za bezpieczne przechowywanie danych, z mocno ograniczoną możliwością kontroli procesu przetwarzania dokumentów (np. klienci nie mieliby pewności, czy prezentowany im dokument jest tym, który został umieszczony w sieci blockchain/IPFS, ponieważ nie będzie posiadać podpisu TTP).

W kolejnym kroku klient zapoznaje się z dokumentem i podejmuje decyzję o jego akceptacji lub odrzuceniu. Decyzja ta (w zakodowanej formie) jest przekazywana przez bank do TTP i wraz z identyfikatorem klienta oraz skrótem dokumentu umieszczana w sieci blockchain w postaci nowej transakcji w bloku.

Opisany etap jest powtarzany dla każdego z klientów (na diagramie dla zwiększenia czytelności pokazano czynności tyko dla jednego klienta). Ostatecznie po podjęciu decyzji przez każdego z *n* klientów w sieci blockchain pojawi się *n+1* transakcji (pierwsza transakcja z dokumentem dostarczonym od banku i *n* transakcji z decyzjami *n* klientów dot. tego dokumentu).

Oczywiście można też rozważyć inny scenariusz, w którym bank chce np. zmienić umowę z każdym klientem procesując aneks do umowy. W tym wypadku każdy aneks musi zostać przygotowany indywidualnie dla każdego klienta, co oznacza, że w sieci blockchain po zakończonym procesie akceptacji bądź odrzucenia przez wszystkich klientów, pojawi się *2n* nowych transakcji (*n* transakcji z aneksami dla każdego klienta oraz *n* decyzji klientów).

Warto zauważyć, że prezentowane podejście może znaleźć zastosowanie nie tylko w banku czy instytucji finansowej, ale także w każdej firmie czy przedsiębiorstwie, gdzie istnieje potrzeba uzgadniania dokumentów pomiędzy firmą a klientem w sposób bezpieczny i zaufany. Ponadto nic nie stoi na przeszkodzie, aby dostęp do dokumentu (przekazywanego przez bank poprzez link) wzmocnić dodatkowo uwierzytelnianiem dwuskładnikowym (ang. *two-factor authentication* – 2FA) lub wieloskładnikowym (ang. *multi-factor authentication* – MFA), ale to już leży po stronie odpowiedzialności banku.

Dzięki temu, że cały proces jest nadzorowany przez TTP oraz sieć blockchain przechowywana jest w infrastrukturze TTP, klient w przypadku wątpliwości co do prawidłowości przebiegu procesu przetwarzania dokumentu lub podejrzeniu manipulacji przez bank może na żądanie uzyskać dostęp do sieci blockchain (oczywiście bank także może taki dostęp uzyskać) i zweryfikować jaki dokument (przesłany przez bank) został faktycznie umieszczony w sieci blockchain oraz IPFS i jaka decyzja jego jako klienta została zwrotnie umieszczona w łańcuchu bloków. Takie podejście mocno ogranicza możliwości manipulacji procesem przetwarzania dokumentów przez każdą ze stron,

czyniąc proponowaną e-usługę bezpieczną i zaufaną. Ponadto, prezentowana e-usługa spełnia wymogi polskiego prawa dot. nośnika trwałego, a więc między innymi konieczność trwałego przechowywania elektronicznych dokumentów w niezależnej od każdej ze stron infrastrukturze, a także konieczność monitorowania procesu ich składowania, przetwarzania i udostępniania.

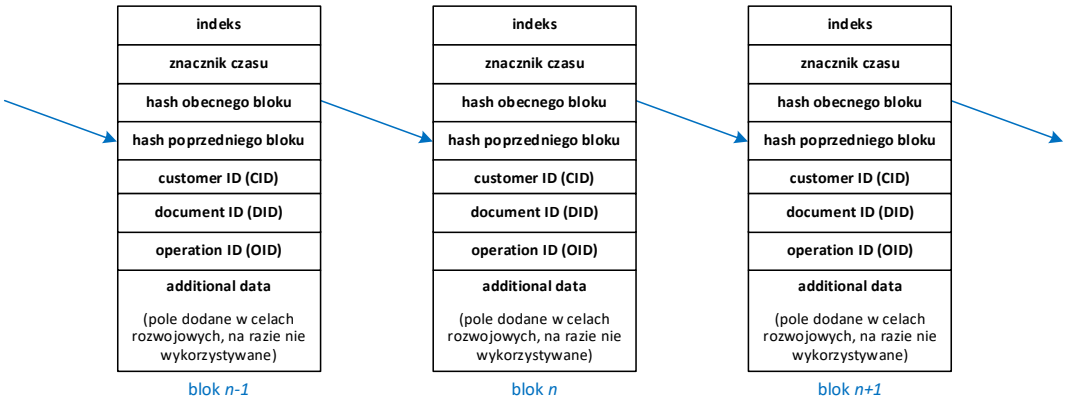
3.3. Struktura sieci blockchain

Wybór technologii blockchain nie był przypadkowy. Obecnie blockchain jest jednym z najlepszych powszechnie stosowanych rozwiązań do przechowywania kluczowych danych w strukturach trudnych do manipulacji. Dlatego z powodzeniem stosowany jest w kryptowalutach i innych aplikacjach biznesowych [72]. W proponowanej e-usłudze wykorzystywana jest prywatna wersja sieci blockchain. Oznacza to, że dostęp do określonych danych (zapisanych w blokach) możliwy jest jedynie posiadając odpowiednie uprawnienia. W prezentowanym rozwiązaniu TTP tworzy oddzielną sieć blockchain dla każdego dużego podmiotu (np. banku). Dzięki temu w jednej sieci nie są przechowywane dane pochodzące z różnych podmiotów (banków) i od klientów różnych banków.

Należy pamiętać, że bezpieczeństwo sieci blockchain jest tym większe, im większa jest ilość węzłów tej sieci. Jak wynika z zaprezentowanego algorytmu ilość tworzonych węzłów zależy od rodzaju dokumentu oraz liczby klientów. Ponieważ projektowana e-usługa dedykowana jest dużym podmiotom (głównie finansowym), duża liczba klientów przekłada się na dużą liczbę transakcji, co pozytywnie wpływa na bezpieczeństwo sieci blockchain i znacząco zmniejsza możliwość manipulacji (zwłaszcza, że blockchain jest przechowywany i zarządzany przez TTP, a nie bank). Warto także zauważyć, że generowanie dokumentów dla klientów (oraz przechowywanie ich skrótów w blockchain) może mieć charakter iteracyjny, a co za tym idzie przewidywalny, w przeciwieństwie do decyzji klientów (poszczególni klienci uzyskują dostęp do dokumentu i podejmują decyzję w losowym czasie).

Aby efektywnie przechowywać niezbędne dane w sieci blockchain konieczne było opracowanie struktury tej sieci, w tym pojedynczego bloku (rys. 3.5). Dla większej przejrzystości rysunku przyjęto, że każdy blok zawiera dokładnie jedną transakcję, choć w praktyce bardzo często bloki zawierają po kilka, kilkanaście czy nawet kilkadziesiąt transakcji. Część pól w prezentowanej strukturze blockchain jest typowymi polami sieci blockchain (np. indeks, znacznik czasu „timestamp", hash bloku, hash poprzedniego bloku itp.), pozostałe pola zostały zaproponowane przez autora. Są to:

- *customer ID* (CID) – numeryczny identyfikator klienta. Pole to służy do identyfikacji strony transakcji, która wykonała jakąś operację na dokumencie (dodanie, odrzucenie, akceptacja). W przypadku dodania dokumentu przez bank do procedowania, pole to przyjmuje ustaloną wartość identyfikującą dany bank. W pozostałych przypadkach są to numeryczne identyfikatory klientów banku;
- *document ID* (DID) – to wygenerowany skrót podpisanego dokumentu;
- *operation ID* (OID) – pole numeryczne, gdzie dla każdej operacji na dokumencie (np. dodanie, akceptacja, odrzucenie) przypisano określoną wartość numeryczną;
- *additional data* – pole dodane w celach rozwojowych, na razie nie wykorzystywane.



Rys. 3.5. Proponowana struktura sieci blockchain

Warto zauważyć, że zaproponowana struktura jest dość elastyczna i w łatwy sposób pozwala definiować np. nowe rodzaje operacji na dokumencie (np. podpisanie, zgłoszenie poprawek, wycofanie itp.) – wystarczy rozszerzyć słownik pola OID. Ponadto, powyższa struktura może być także z powodzeniem wykorzystywana w e-usłudze, w której liczba stron nie jest ograniczona tylko do 3 (np. może być kilku równorzędnych przedsiębiorców, z których każdy może inicjować proces przetwarzania danego dokumentu przez wskazane, wybrane strony transakcji).

Ważną kwestią dot. sieci blockchain jest także wybór mechanizmu konsensusu, czyli techniki osiągania porozumienia w kwestii dodawania nowych bloków pomiędzy węzłami sieci utrzymującej blockchain [73]. Ponieważ blockchain zarządzany jest przez TTP, to zamiast korzystać z mechanizmu Proof-of-Work (PoW), wymagającego dużych zasobów obliczeniowych (a przez to także ilości energii elektrycznej, co wpływa negatywnie na środowisko), do wydobycia bloków używany jest skuteczniejszy w tym przypadku mechanizm Proof-of-Authority (PoA). Dzięki temu rozwiązaniu sieć blockchain nie potrzebuje mocy obliczeniowej do tworzenia nowych węzłów. Jednym z rodzajów algorytmów PoA jest algorytm Istanbul Byzantine Fault Tolerance (IBFT) i właśnie ten

rodzaj PoA został zaimplementowany w proponowanym rozwiązaniu. W sieciach prywatnych, gdzie uczestnicy są znani i zaufani, PoA pozwala na znacznie szybsze przetwarzanie transakcji w porównaniu do bardziej zdecentralizowanych algorytmów konsensusu, takich jak PoW czy Proof-of-Stake (PoS). Brak konkurencji o wydobycie bloków, jak w przypadku PoW, eliminuje potrzebę rozwiązywania skomplikowanych problemów matematycznych, co przyspiesza proces weryfikacji transakcji. PoA jest bardziej skalowalny niż PoW, ponieważ nie ma potrzeby angażowania dużej mocy obliczeniowej w proces wydobycia bloków. To oznacza, że sieci PoA mogą obsługiwać większą liczbę transakcji na sekundę. Ponadto w sieciach prywatnych często istnieje potrzeba przestrzegania regulacji i zgodności z prawem, a PoA umożliwia bardziej kontrolowane zarządzanie siecią, co ułatwia dostosowywanie się do przepisów i wymagań prawnych. Konsensus typu PoS może prowadzić do centralizacji, ponieważ osoby z większym udziałem w kryptowalucie mają większą kontrolę nad siecią. Podobnie jest w przypadku konsensusu Delegated-Proof-of-Stake (DPoS), który także może prowadzić do centralizacji, ponieważ tylko wybrani delegaci biorą udział w walidacji transakcji w sieci, a decyzje przez nich podejmowane mogą wpłynąć na całą sieć i jej użytkowników.

3.4. Zaufana trzecia strona

W proponowanym podejściu bardzo ważnym elementem jest zaufana trzecia strona, bo to właśnie ona ma największy wpływ na zaufanie przyszłych klientów do tego rozwiązania. Z jednej strony kwestie bezpieczeństwa (m.in. zastosowane algorytmy kryptograficzne, szyfrowanie, elektroniczne podpisywanie danych, sieć blockchain typu prywatnego) budują zaufanie użytkowników do usługi, ale zdecydowanie największe ich obawy skupiają się wokół możliwości manipulacji danymi przez podmiot dominujący. Stąd m.in. jedno z wymagań dot. trwałego nośnika dotyczy tego, aby infrastruktura, w której implementowana jest e-usługa była niezależna od każdego z podmiotów (głównie mowa tu o podmiocie dominującym, np. banku), tak aby żadna ze stron nie miała prawnych lub technicznych możliwości ingerencji w przechowywane dane. Dlatego w proponowanym rozwiązaniu sieć blockchain jest przechowywana w infrastrukturze serwerowej należącej do TTP i zarządzana wyłącznie przez TTP. Oczywiście możliwe są też inne rozwiązania, w której rola TTP może być ograniczona wyłącznie do funkcji arbitra, który tylko nadzoruje procesy dot. przechowywania i przetwarzania dokumentów przez obie strony, a w przypadku sporu podejmuje wiążące decyzje. Wydaje się jednak, że przyjęte w pracy podejście, aby TTP było nie tylko zaufaną trzecią stroną, ale i dostawcą

e-usługi jest rozwiązaniem najbardziej efektywnym, a także korzystnym z punktu widzenia kosztów implementacji rozwiązania. Dlatego w zrealizowanej e-usłudze rolę TTP pełni firma Perceptus sp. z o.o., w której wdrożone zostało prezentowane rozwiązanie i której infrastruktura jest tu wykorzystywana.

3.5. Podsumowanie

Na podstawie przeprowadzonej analizy rozwiązań dot. trwałego nośnika istniejących zarówno w literaturze jak i dostępnych na rynku w postaci usług i produktów komercyjnych, można było skutecznie określić wymagania funkcjonalne jakie powinna spełniać projektowana e-usługa. Wymieniono także listę funkcjonalności jakie musi posiadać taka usługa oraz wybrano typ sieci blockchain, który zostanie zaimplementowany w proponowanym rozwiązaniu. Najlepszym typem sieci okazał się prywatny blockchain. Opracowywany algorytm ewoluował na przestrzeni ostatnich lat prowadzonych badań, ale ostateczna i najbardziej „dojrzała" wersja algorytmu została zaprezentowana w tym rozdziale. Koncepcja ta określa schemat przepływu danych pomiędzy podmiotem dominującym (np. bankiem), klientami oraz zaufaną trzecią stroną. Ponadto wskazuje ona sposób zarządzania kluczami, szyfrowania dokumentów i operacji na sieci blockchain oraz sieci IPFS, w której przechowywane są właściwe, zaszyfrowane wrażliwe dokumenty elektroniczne.

Należy też zwrócić uwagę, że opracowana koncepcja e-usługi jest na tyle uniwersalna, że z powodzeniem może być zastosowana do bezpiecznego przetwarzania wrażliwych dokumentów elektronicznych procesowanych przez kilka równorzędnych stron. Można sobie wyobrazić sytuację, w której np. kilku przedsiębiorców chciałoby w sposób bezpieczny i zaufany przeprocesować ważną kilkustronną umowę, w której żadna ze stron nie jest dominującą. Zarówno struktura sieci blockchain jak i sama idea e-usługi umożliwia łatwe wdrożenie proponowanego rozwiązania dostosowanego do ww. potrzeb klientów.

Warto podkreślić, że proponowana koncepcja powstała w wyniku prac naukowych, a także szeregu spotkań i dyskusji zarówno z naukowcami jak i specjalistami z firmy Perceptus. Prezentowany w pracy algorytm był wielokrotnie modyfikowany i rozwijany tak, aby spełniał wymagania w dynamicznie zmieniającym się rynku usług z zakresu cyberbezpieczeństwa. Wydaje się jednak, że wpłynęło to bardzo pozytywnie na ostateczny kształt e-usługi (bezpieczeństwo, elastyczność, wydajność), która wdrożona może konkurować z innymi, dostępnymi na rynku rozwiązaniami.

4. Implementacja i wdrożenie proponowanej e-usługi

W ramach pracy zostały przeprowadzone przegląd i analiza rynku pod kątem istniejących biznesowych koncepcji, a także rozwiązań konkurencji. Na podstawie uzyskanej w ten sposób wiedzy, a także technicznych uwarunkowań i dostępnych zasobów firmy Perceptus sp. z o.o. powstał zbiór wymagań technicznych, stanowiący swoiste uzupełnienie wymagań funkcjonalnych przedstawionych w rozdziale 3.1, niezbędnych do wdrożenia opracowanej koncepcji e-usługi. Ponadto dokonano przeglądu dostępnych narzędzi i technologii dot. implementacji projektowanej e-usługi. Między innymi określono parametry konfiguracyjne sieci blockchain, a także wybrano platformę implementacyjną blockchain (tzw. *hyperledger*) oraz narzędzia monitorujące procesy zachodzące w tej sieci. Powstałe w ten sposób koncepcje realizacji e-usługi były weryfikowane podczas prezentacji w firmie i udoskonalane. Przygotowana lista dostępnych w firmie zasobów okazała się także bardzo pomocna, ponieważ pozwoliła wykorzystać już istniejące usługi i zoptymalizować koszty realizowanego rozwiązania.

4.1. Wymagania techniczne

Zidentyfikowane w ramach pracy wymagania techniczne dot. projektowanej e-usługi są następujące:

- do bezpiecznego generowania i przechowywania krytycznego materiału kryptograficznego (klucze symetryczne i asymetryczne) oraz do wykonywania krytycznych operacji (szyfrowanie, deszyfrowanie) zostanie użyty zewnętrzny sprzętowy moduł bezpieczeństwa (HSM), który będzie dysponować następującymi funkcjonalnościami:
  - generowanie 256-cio bitowego klucza symetrycznego za pomocą algorytmu AES -256,
  - generowanie pary 2048-bitowych kluczy RSA,
  - szyfrowanie klucza symetrycznego AES-256 za pomocą klucza prywatnego RSA,
- generowanie skrótu (hash) zaszyfrowanego dokumentu (SHA-256),
- szyfrowanie dokumentu za pomocą klucza symetrycznego AES-256,
- nawiązywanie bezpiecznego połączenia z HSM,
- nawiązywanie bezpiecznego połączenia z prywatną siecią blockchain,

- umieszczenie w sieci blockchain smart kontraktów odpowiadających za przechowywanie danych dotyczących publikowanych dokumentów oraz decyzji klientów dot. tych dokumentów,
- integracja e-usługi z serwerem (siecią) IPFS do zapisywania zaszyfrowanego pliku dokumentu,
- przesyłanie skrótu zaszyfrowanego dokumentu do sieci blockchain,
- generowanie linku dostępowego do zaszyfrowanego pliku umieszczonego w sieci IPFS,
- uzyskiwanie dostępu do danych w sieci blockchain (w tym do danych dokumentu umieszczonych w bloku),
- generowanie listy przetwarzanych dokumentów zawierającej skrót dokumentu wraz z odpowiadającym mu linkiem do właściwego dokumentu w sieci IPFS, zaszyfrowanym symetrycznym kluczem AES-256, kluczem publicznym i identyfikatorem klienta, którego dany dokument dotyczy,
- udostępnianie za pomocą tzw. external API (ang. *Application Programming Interface*) wybranych funkcjonalności (np. dodawanie danych do sieci blockchain, generowanie linku dostępowego do dokumentu, dodawanie dokumentów do sieci IPFS),
- pobieranie zaszyfrowanego dokumentu z sieci IPFS,
- odszyfrowywanie dokumentu z sieci IPFS.

4.2. Projekt i realizacja e-usługi

Projektowana e-usługa skierowana jest głównie do banków i dużych instytucji finansowych w celu bezpiecznego (z wykorzystaniem trwałego nośnika) przechowywania i przetwarzania dokumentów dot. ich klientów, spełniając wymóg informacyjny stawiany przez Urząd Ochrony Konkurencji i Konsumentów [2] oraz Dyrektywy Parlamentu Europejskiego i Rady Europy [5]. W e-usłudze można wyodrębnić trzy typy użytkowników (bank, klient oraz TTP), którzy będą wykonywali różne czynności w systemie. Bank musi mieć możliwość: przesyłania dokumentu (lub zbioru dokumentów), wskazywania odbiorców dokumentu (klientów banku, których dany dokument dotyczy), przekazywania dostępu (linka) do dokumentów klientom, potwierdzenia autentyczności i integralności dokumentu, generowania potwierdzenia wykonanej akcji przez odbiorcę. Jednocześnie bank nie może mieć możliwości zmiany lub usuwania wcześniej dodanych dokumentów. TTP jako podmiot zarządzający siecią

blockchain jak i całym procesem przetwarzania dokumentu ma mieć możliwość: elektronicznego podpisywania dokumentu, generowania skrótu dokumentu, generowania pary kluczy RSA-2048, generowania klucza symetrycznego AES-256, szyfrowania i deszyfrowania dokumentu za pomocą klucza symetrycznego AES-256, szyfrowania i deszyfrowania klucza symetrycznego AES-256 za pomocą klucza asymetrycznego RSA, umieszczenie dokumentu w sieci IPFS, generowanie linku dostępowego do dokumentu w sieci IPFS, przeglądanie danych sieci blockchain, dodawanie nowych transakcji do sieci blockchain. Klient banku ma mieć z kolei możliwość wyświetlania dokumentu (za pomocą otrzymanego z banku linku), pobrania dokumentu, dokonania akcji potwierdzenia bądź odrzucenia dokumentu (lub proponowanych w nim zmian).

Ponadto projektowana e-usługa powinna mieć możliwość integracji z innymi istniejącymi w firmie Perceptus sp. z o.o. systemami (np. sieć IPFS, oprogramowanie do wykonywania zdalnych podpisów elektronicznych, system zarządzania certyfikatami) oraz urządzeniami (np. HSM, serwer plików, przełączniki sieciowe itp.).

W związku z dynamicznie rozwijającym się postępem technologicznym i zapotrzebowaniem rynku zdecydowano, że największą elastyczność zapewni wdrożenie e-usługi w infrastrukturze firmy w formie API, która pozwoli na szeroką możliwość integracji z systemami klientów poprzez udostępnione tzw. zewnętrzne API. Jest to zestaw reguł i protokołów, które umożliwiają jednej aplikacji komunikowanie się i współpracę z inną aplikacją lub usługą, która działa niezależnie poza pierwszą aplikacją. Może być łatwo używane przez programistów wewnątrz organizacji i każdego innego programistę z zewnątrz, który chce skorzystać z interfejsu. W ramach zewnętrznego API e-usługa powinna udostępniać wybrane funkcjonalności (np. dodawanie danych do sieci blockchain, generowanie linku dostępowego do dokumentu w IPFS, pobranie dokumentu z IPFS, odszyfrowanie dokumentu, przesłanie decyzji do blockchain, itp.). Dzięki takiemu rozwiązaniu klienci mogą integrować swoje obecne systemy z proponowaną e-usługą bez konieczności wykorzystywania dodatkowej aplikacji/systemu, co dla instytucji bankowych ma często kluczowe znaczenie. Firma Perceptus sp. z o.o. widzi wielki potencjał w technologii blockchain i wdrażania jej w innych swoich rozwiązaniach stąd pomysły, aby w przyszłości wykorzystywać kolejne węzły sieci blockchain i rozszerzać możliwości usługi API o kolejne funkcjonalności.

4.2.1. Język Java

Proponowana w pracy e-usługa została zrealizowana w języku Java [74]. Język ten jest jednym z najpopularniejszych języków programowania na świecie i jest szeroko stosowany

w aplikacjach biznesowych, dzięki swoim cechom i zaletom. Język Java został zaprojektowany z myślą o przenośności. Aplikacje napisane w Javie mogą być uruchamiane na różnych platformach sprzętowych i systemach operacyjnych bez konieczności modyfikacji kodu. Jest to możliwe dzięki tzw. maszynie wirtualnej Javy (ang. *Java Virtual Machine* – JVM), która tłumaczy kod Javy na kod zrozumiały dla danej platformy. Java posiada wbudowane mechanizmy bezpieczeństwa, które pomagają chronić aplikacje przed atakami i zagrożeniami. Język ten ma także zintegrowane mechanizmy obsługi wyjątków, co pozwala na bardziej kontrolowane reagowanie na błędy i nieprawidłowe sytuacje w aplikacji. To przyczynia się do większej stabilności i niezawodności aplikacji biznesowych tworzonych w tym języku. Java jest skalowalnym językiem programowania, który może być używany do budowania programów o dowolnej wielkości, od małych aplikacji na komputery stacjonarne po duże systemy na poziomie przedsiębiorstwa. Java dostarcza obszerną bibliotekę standardową, która zawiera gotowe komponenty do obsługi różnych zadań, takich jak manipulacja danymi, komunikacja sieciowa, obsługa plików, obsługa wątków i wiele innych, co znacząco przyspiesza rozwój aplikacji. Technologia ta jest darmowa w użyciu i ma ogromną społeczność, bardzo aktywną w tworzeniu nowych narzędzi i frameworków. Wbudowane klasy i narzędzia do obsługi komunikacji sieciowej (np. TCP/IP) oraz protokołów takich jak HTTP ułatwiają budowę aplikacji typu klient-serwer oraz integrację z systemami zewnętrznymi.

Java jest językiem obiektowym, co umożliwia tworzenie modularnych i skalowalnych aplikacji. Dzięki mechanizmom takim jak dziedziczenie, polimorfizm i interfejsy, można tworzyć hierarchie klas, które odzwierciedlają struktury biznesowe. Czytelność kodu Javy, zasada „write once, run anywhere" oraz narzędzia do zarządzania projektem przyczyniają się do łatwości utrzymania aplikacji, szczególnie w większych i długoterminowych projektach. W ekosystemie Javy istnieje wiele popularnych frameworków biznesowych, takich jak Spring [75] czy Java EE (obecnie znane jako Jakarta EE [76]), które dostarczają gotowych rozwiązań i narzędzi do budowy zaawansowanych aplikacji biznesowych. Ponadto dzięki wielowątkowości, obsłudze sieci, modułowości i narzędziom do zarządzania pamięcią, Java umożliwia budowę skalowalnych systemów biznesowych, które mogą obsługiwać dużą liczbę użytkowników i ogromne ilości danych.

4.2.2. Implementacja technologii blockchain

Technologia blockchain to innowacyjne rozwiązanie, które oferuje wiele interesujących cech i możliwości. Jest to rozproszona i zdecentralizowana baza danych, która przechowuje transakcje i informacje w blokach powiązanych ze sobą za pomocą

algorytmów kryptograficznych. W sieci blockchain dane są przechowywane w formie łańcucha bloków, w którym każdy blok zawiera zestaw transakcji. Ponadto każdy blok jest powiązany z poprzednim za pomocą unikalnego identyfikatora, co tworzy niezmienną historię transakcji. Blockchain działa w oparciu o konsensus, co oznacza, że wszyscy uczestnicy sieci muszą zgodzić się na poprawność i spójność danych. To zapewnia bezpieczeństwo i niezmienność transakcji.

Blockchain może być publiczny, dostępny dla wszystkich lub prywatny, ograniczony do wybranych uczestników. Blockchain publiczny jest transparentny, ponieważ wszystkie transakcje są widoczne dla wszystkich uczestników sieci. Prywatne sieci blockchain często oferują większą prywatność i kontrolę nad dostępem do danych. Jednak tożsamość uczestników może być anonimowa lub pseudoanonimowa, co zależy od konkretnych implementacji sieci blockchain. Technologia blockchain oferuje niezmienność danych, ponieważ po dodaniu bloku do łańcucha, jego zmiana jest bardzo trudna lub wręcz niemożliwa. Jest to osiągane dzięki zastosowaniu algorytmów kryptograficznych i powiązaniu bloków za pomocą skrótów (hash).

Istnieje wiele platform implementacyjnych dedykowanych technologii blockchain. Jednym z przykładów jest MultiChain [77]. Jest to rozszerzone rozwiązanie Bitcoin o otwartym kodzie źródłowym. Oferuje dobrze dobrany zestaw funkcji dla użytkowników biznesowych i może być używany do budowania sieci blockchain zarówno z uprawnieniami dostępu prywatnego, jak i publicznego. MultiChain obsługuje duże ilości danych i jest znany ze swojej szybkości działania i łatwości wdrożenia.

Kolejnym ciekawym i bardzo popularnym rozwiązaniem opartym na blockchain jest Hyperledger Fabric (HLF) [26] firmy IBM. Umożliwia tworzenie aplikacji o architekturze modułowej. HLF pozwala na jednoczesne uruchamianie wielu komponentów i wspiera usługi członkowskie. Hyperledger Fabric jest platformą typu open source dla przedsiębiorstw, która zapewnia kilka kluczowych cech różniących ją od innych popularnych platform blockchain, takich jak modularność, elastyczność, prywatność oraz wsparcie dla aplikacji biznesowych.

Jednym z protokołów blockchain typu open source jest Quorum [78]. Wywodzi się on z Ethereum [13]. Quorum obsługuje prywatne sieci blockchain z jednym właścicielem wszystkich węzłów, a także sieć blockchain w modelu konsorcjum, w której wielu członków sieci jest właścicielem części sieci.

Ciekawym wieloplatformowym rozwiązaniem open-source jest także Hyperledger Besu [79]. Jest to klient Ethereum [13] napisany w języku Java (na licencji Apache 2.0)

i implementujący specyfikację Enterprise Ethereum Alliance (EEA). Można go uruchomić zarówno w publicznych, jak i prywatnych sieciach Ethereum. Hyperledger Besu został zaprojektowany z myślą o przedsiębiorstwach dla publicznych i prywatnych przypadków użycia sieci uprawnionych, z implementacją środowiska wirtualnej maszyny EVM (ang. *Ethereum Virtual Machine*). Hyperledger Besu oferuje kilka algorytmów konsensusu, w tym Proof-of-Stake (PoS), Proof-of-Work (PoW) i Proof-of-Authority (PoA), co daje elastyczność w wyborze algorytmu konsensusu w zależności od potrzeb sieci blockchain [79]. Posiada też silne zabezpieczenia, w tym możliwość integracji z różnymi mechanizmami uwierzytelniania i kontroli dostępu, takimi jak LDAP (ang. *Lightweight Directory Access Protocol*) czy OAuth.

Hyperledger Besu obsługuje wiele języków programowania, co ułatwia programistom tworzenie inteligentnych kontraktów i aplikacji na platformie Ethereum oraz oferuje skalowalność poprzez możliwość tworzenia sieci prywatnych, publicznych lub hybrydowych. W zależności od potrzeb można także dostosować parametry sieci blockchain, takie jak rozmiar bloku czy czas blokowania. Ponadto umożliwia on konfigurowanie uprawnień dostępu i kontroli na poziomie konta, inteligentnych kontraktów i transakcji, co zapewnia większą elastyczność i prywatność.

Hyperledger Besu zapewnia wsparcie dla standardów interfejsów programistycznych (API), takich jak Ethereum JSON-RPC (ang. *JavaScript Object Notation – Remote Procedure Call*), co ułatwia integrację z istniejącymi aplikacjami, oferuje narzędzia i biblioteki, które umożliwiają rozwój, testowanie i wdrażanie inteligentnych kontraktów oraz aplikacji blockchain. Zapewnia także wysoką wydajność dzięki zoptymalizowanym mechanizmom transakcyjnym i przetwarzaniu danych.

Każda z przedstawionych platform implementacyjnych blockchain ma swoje wady i zalety. Analizowane w niniejszym rozdziale rozwiązania podsumowano w tabeli 3.

Tabela 3. Porównanie analizowanych platform implementacyjnych sieci blockchain

Rozwiązanie	Rodzaj łańcucha bloków	Rodzaj konsensusu
Multichain	Private, Permissioned	PBFT
Quorum	Private, Permissioned	Raft, QuorumChain, IBFT
Hyperledger Fabric	Private, Permissioned	Raft
Hyperledger Besu	Public, Private, Permissioned	PoW (Ethash), PoS, PoA (IBFT, QBFT, Clique)

W proponowanym podejściu wykorzystywana jest prywatna wersja blockchain, co oznacza, że dostęp do danych przechowywanych w sieci blockchain możliwy jest wyłącznie po posiadaniu odpowiednich uprawnień dostępu. Co więcej, generowana jest tylko jedna sieć dla każdego podmiotu np. banku (przechowywanie w jednej sieci

blockchain danych dot. wszystkich klientów banku jest bezpieczniejsze niż generowanie osobnych sieci blockchain dla każdego klienta osobno).

Podsumowując, Hyperledger Besu jest kompleksowym i elastycznym rozwiązaniem blockchain, które dostarcza zaawansowanych funkcji i narzędzi dla przedsiębiorstw. Jego wszechstronność, skalowalność i wysoka wydajność czynią go atrakcyjnym wyborem dla różnych przypadków użycia jako rozwiązania biznesowego technologii blockchain. Hyperledger Besu jest, zdaniem autora, bardziej elastyczny niż Hyperledger Fabric i pozwala na łatwiejsze dostosowanie go do różnych przypadków użycia. Ponadto Hyperledger Fabric jest, w ocenie autora, bardziej skomplikowany niż Hyperledger Besu [26], [79]. Dlatego do implementacji technologii blockchain w projektowanej e-usłudze zdecydowano się na wybór Hyperledger Besu. Wymagania implementacyjne stawiane przez Hyperledger Besu dla VM (ang. *Virtual Machine*) to min. 6 GB pamięci RAM (ang. *Random-Access Memory*) oraz pojemność dysku twardego z co najmniej 10 GB przestrzeni dyskowej (rekomendowane 20 GB) [79].

Konfiguracja Hyperledger Besu wymagała instalacji na VM z systemem Linux wchodzących w skład usługi TTP zawierającej węzły sieci blockchain oraz konfiguracji bloku genezy (ang. *genesis block*). Sieć została oparta o algorytm konsensusu Proof-of-Authority (PoA) IBFT 2.0 w celu uniknięcia rozgałęzień (ang. *fork*) łańcuchów bloków co jest kluczowe dla założeń projektu. W sieciach IBFT 2.0 zatwierdzone konta, zwane walidatorami, zatwierdzają transakcje i bloki. Walidatorzy na zmianę tworzą kolejny blok, a przed umieszczeniem bloku w łańcuchu, większość walidatorów (większa lub równa 2/3) musi najpierw podpisać blok. Atrybuty specyficzne dla IBFT 2.0 są to:

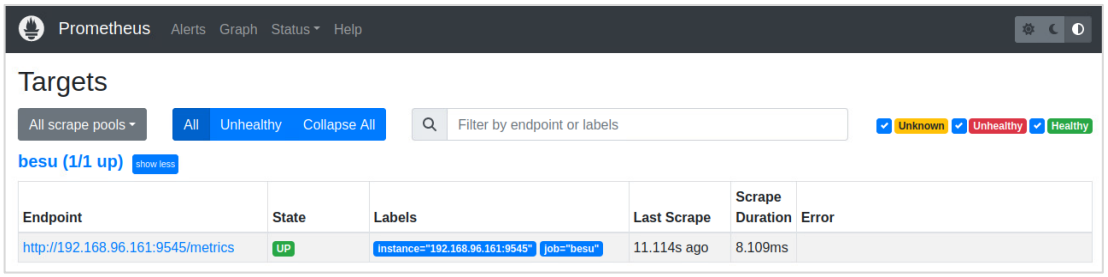
- blockperiodseconds – minimalny czas bloku w sekundach,
- requesttimeoutseconds – limit czasu (w sekundach) dla każdej rundy konsensusu przed zmianą rundy,
- blockreward – opcjonalna kwota nagrody w *Wei* (to najmniejszy nominał *Ether*, czyli monety kryptowaluty używanej w sieci Ethereum), którą ma zostać nagrodzony beneficjent (wszystkie węzły w sieci muszą używać tej samej wartości),
- extraData – dodatkowe dane zakodowane w protokole RLP (ang. *Resource Location Protocol*).

Prywatna sieć blockchain wymagała ponadto skonfigurowania sieci w taki sposób, aby nie wymagała tzw. *gazu* (ang. *free gas network*). Transakcje wykorzystują zasoby obliczeniowe, więc wiążą się z nimi koszty. Kosztem transakcji jest zużyty *gaz * cena gazu*

(tu: *gaz* to jednostka kosztu, a *cena gazu* to cena za jednostkę gazu). W wielu sieciach prywatnych uczestnicy sieci prowadzą walidatory i nie wymagają gazu jako zachęty. Sieci, które nie wymagają gazu jako zachęty, zwykle konfigurują cenę gazu na zero (czyli gaz jest bezpłatny). W bezpłatnej sieci transakcje nadal wykorzystują gaz, ale cena gazu wynosi zero, co oznacza, że także koszt transakcji wynosi zero. W bezpłatnych sieciach gazowych należy zwiększyć limit wielkości bloku i limit wielkości kontraktu na wartość maksymalną, co także zostało wykonane w implementowanej sieci blockchain.

4.2.3. Narzędzia monitorujące

W celu monitorowania usługi blockchain zostały zainstalowane w firmie i odpowiednio skonfigurowane na VM z systemem Linux odpowiednie narzędzia monitorujące. Jednym z nich jest *Prometheus* [80] (rys. 4.1).



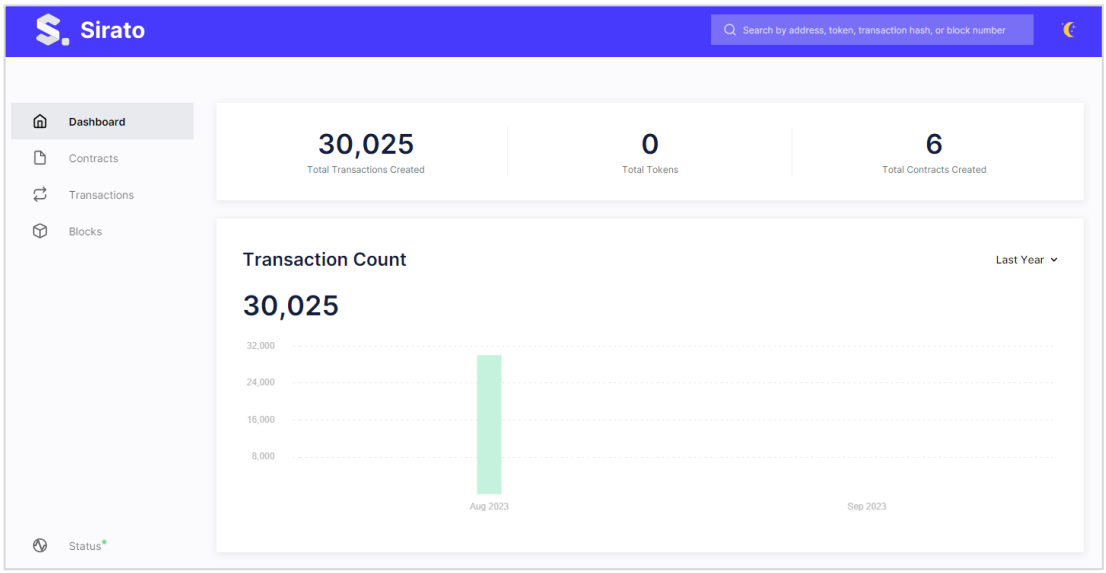
Rys. 4.1. Narzędzie Prometheus wdrożone w firmie do monitorowania sieci Blockchain

Prometheus to otwarte narzędzie do monitorowania i alarmowania, które jest szeroko stosowane w dziedzinie monitorowania systemów i aplikacji. Jest to także bardzo popularne narzędzie w świecie DevOps i inżynierii oprogramowania, ponieważ umożliwia skuteczne monitorowanie aplikacji i infrastruktury oraz szybkie reagowanie na potencjalne problemy. Dzięki swojej elastyczności i bogatej społeczności użytkowników oraz deweloperów, jest często wybierany jako narzędzie do monitorowania w różnych projektach.

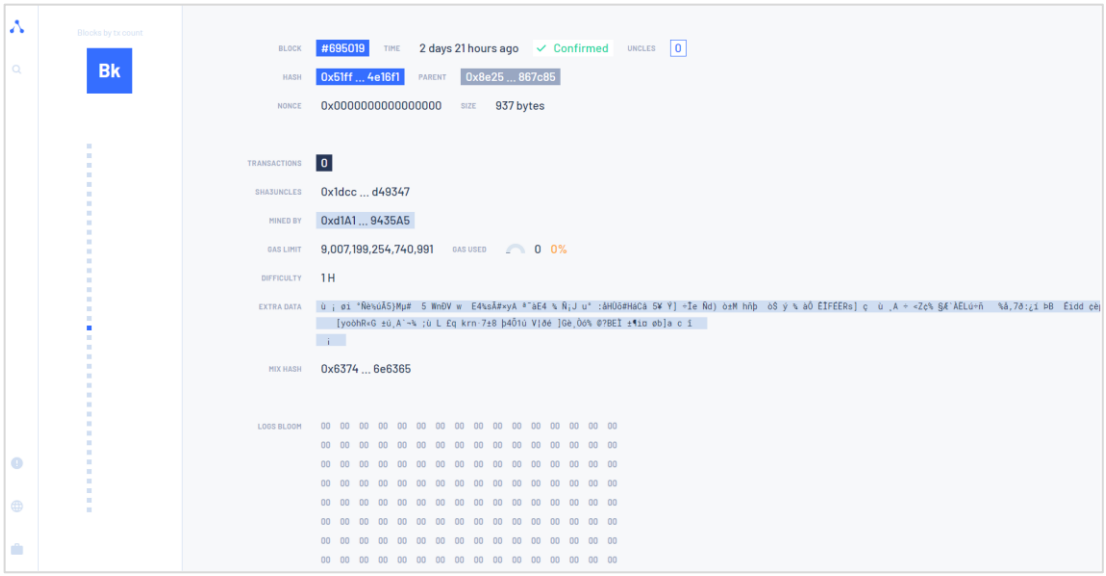
Prometheus zbiera dane metryczne (tzw. metryki) z różnych źródeł, takich jak aplikacje, serwery, urządzenia sieciowe i wiele innych (metryki to liczby, które reprezentują stan i wydajność systemu lub aplikacji, takie jak liczba żądań HTTP na sekundę, zużycie CPU, dostępność usług itp.). Posiada własny język zapytań nazywany *PromQL*, który pozwala na zaawansowane przetwarzanie danych metrycznych, w tym na tworzenie złożonych zapytań, agregowanie danych i generowanie wykresów. Przechowuje zebrane dane metryczne w bazie danych czasowej, która jest zoptymalizowana pod kątem efektywnego przechowywania i przetwarzania danych historycznych. Dzięki temu można analizować dane z przeszłości i generować wykresy trendów. System jest projektowany

z myślą o skalowalności, co pozwala na zbieranie i przetwarzanie dużych ilości danych metrycznych z rozproszonych systemów.

Kolejnymi narzędziami monitorującymi sieć blockchain (w tym dane transakcji, bloków i inteligentnych kontraktów) były *Sirato Explorer* [81] (rys. 4.2) oraz *Alethio Lite Explorer* [82] (rys. 4.3). Są to narzędzia służące do eksploracji i analizy danych związanych z siecią Ethereum. Pozwalają na przeglądanie pojedynczych bloków, transakcji i adresów, a także umożliwiają dostęp do różnych informacji i statystyk dotyczących sieci Ethereum w sposób przejrzysty i interaktywny. Wyświetlają dane takie, jak liczba potwierdzeń, wartość przesłanych środków, koszty gazowe itp. Oferują różnego rodzaju wykresy i statystyki dotyczące działania sieci Ethereum i pozwalają na monitorowanie zmian w rozmiarze bloków, przepływie ETH, aktywności smart kontraktów itp.

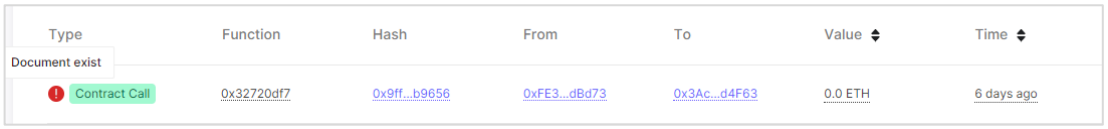


Rys. 4.2. Narzędzie Sirato Explorer wdrożone w firmie do monitorowania sieci blockchain



Rys. 4.3. Narzędzie Alethio Lite Explorer wdrożone w firmie do monitorowania sieci blockchain

Oba narzędzia dają m.in. możliwość śledzenia historii transakcji związanych z danym kontraktem. Dzięki przejrzystemu interfejsowi i zaawansowanym funkcjom analizy danych możliwe jest lepsze zrozumienie działania sieci Ethereum oraz skomplikowanych relacji między transakcjami i kontraktami. Na rys. 4.4 zaprezentowano przykładowy podgląd transakcji odrzuconej ze statusem „dokument istnieje" (ang. *document exist*) w narzędziu Sirato Explorer. Oba narzędzia zostały zaimplementowane i odpowiednio skonfigurowane pod kątem monitorowania usługi Hyperledger Besu wdrożonej w firmie.



Rys. 4.4. Podgląd transakcji odrzuconej ze statusem „dokument istnieje" (ang. *document exist*) w narzędziu Sirato Explorer

4.2.4. Algorytm szyfrowania AES

AES (ang. *Advanced Encryption Standard*) to symetryczny algorytm szyfrowania, który został uznany za standard szyfrowania przez National Institute of Standards and Technology (NIST) [83]. Jest powszechnie stosowany w różnych aplikacjach i protokołach komunikacyjnych w celu ochrony poufności danych.

AES wykorzystuje symetryczne szyfrowanie, co oznacza, że ten sam klucz jest używany zarówno do szyfrowania, jak i deszyfrowania danych (nadawca i odbiorca muszą posiadać ten sam klucz i otrzymać go poufnie). Algorytm obsługuje różne długości klucza, takie jak 128, 192 i 256 bitów. Klucz o długości 128 bitów jest najczęściej stosowany i uważany za wystarczająco bezpieczny. AES jest blokowym algorytmem szyfrowania, co oznacza, że dane są szyfrowane w blokach o stałej wielkości. Standardowy blok AES ma 128 bitów. Algorytm działa na pojedynczym bloku danych i może być stosowany wielokrotnie dla dłuższych danych. Szyfrowanie algorytmem AES składa się z serii rund, w których stosowane są różne transformacje danych. Liczba rund zależy od długości klucza: 10 rund dla klucza 128-bitowego, 12 rund dla klucza 192-bitowego i 14 rund dla klucza 256-bitowego. W każdej rundzie wykonywane są operacje takie jak podstawienia bajtów, mieszanie kolumn i dodawanie kolejnych kluczy rundy.

AES jest uznawany za bezpieczny algorytm szyfrowania, który jest odporny na szeroki zakres ataków kryptograficznych. Przeszedł liczne badania i audyty, co przyczyniło się do jego akceptacji jako standardu szyfrowania. Oczywiście, bezpieczeństwo algorytmu AES zależy od prawidłowego zarządzania kluczami i jego implementacji. Szyfrowanie algorytmem AES znajduje zastosowanie w wielu obszarach, takich jak ochrona danych w transmisjach sieciowych, kryptografia dyskowa, protokoły bezpieczeństwa, aplikacje

mobilne i wiele innych. Jego popularność wynika z kombinacji wydajności, bezpieczeństwa i powszechności implementacji. Z racji na wydajność tego algorytmu w opracowanym rozwiązaniu dokumenty są szyfrowane właśnie za pomocą algorytmu AES z kluczem 256-cio bitowym i trybem pracy CBC.

4.2.5. Algorytm szyfrowania RSA

Algorytm RSA (ang. *Rivest-Shamir-Adleman*) to asymetryczny algorytm kryptograficzny, który został zaproponowany przez Ronalda Rivesta, Adi Shamira i Leonarda Adlemana [84]. Jest szeroko stosowany do szyfrowania danych, podpisywania cyfrowego i wymiany kluczy. Opiera się na problemie faktoryzacji liczb całkowitych. Zakłada się, że faktoryzacja dużych liczb na czynniki pierwsze jest trudna do wykonania w rozsądnym czasie, co stanowi podstawę bezpieczeństwa tego algorytmu. Algorytm do swojego działania wykorzystuje parę kluczy: klucz publiczny do szyfrowania danych i klucz prywatny do deszyfrowania danych. Klucz publiczny jest udostępniany publicznie, podczas gdy klucz prywatny pozostaje tajny i dostępny tylko dla właściciela.

Proces szyfrowania polega na podniesieniu danej wiadomości do potęgi modulo wartości z klucza publicznego. Szyfrowanie może być z łatwością wykonane przy użyciu klucza publicznego i jest trudne do odwrócenia bez posiadania odpowiadającego klucza prywatnego. Z kolei proces deszyfrowania polega na podniesieniu zaszyfrowanej wiadomości do potęgi modulo wartości z klucza prywatnego. Deszyfrowanie odbywa się za pomocą klucza prywatnego i tylko właściciel klucza prywatnego może odzyskać oryginalną wiadomość. Dodatkowo algorytm ten jest również wykorzystywany do generowania podpisów cyfrowych, które potwierdzają autentyczność i integralność wiadomości. Podpisy cyfrowe są generowane przy użyciu klucza prywatnego, a weryfikowane przy użyciu klucza publicznego.

RSA jest algorytmem kryptograficznym uważanym za bezpieczny, ale bezpieczeństwo zależy od długości kluczy. Im większa długość klucza, tym trudniejsze jest złamanie jego szyfrowania poprzez atak typu siłowego (ang. *brute force*). NIST zaleca stosowanie kluczy o minimalnej sile 112 bitów w celu ochrony danych do 2030 r. 2048-bitowy klucz RSA zapewnia 112-bitowe bezpieczeństwo. Narodowy Instytut Standardów i Technologii (NIST) okresowo publikuje zalecenia dotyczące stosowania algorytmów kryptograficznych [85]. Algorytm RSA jest szeroko stosowany w różnych aplikacjach, takich jak bezpieczna komunikacja, uwierzytelnianie, wymiana kluczy i podpisy cyfrowe. Jego popularność wynika z bezpieczeństwa oraz szerokiego wsparcia w różnych narzędziach kryptograficznych i bibliotekach programistycznych.

Zastosowanie algorytmu RSA do szyfrowania dużej ilości danych (np. dokumentów) nie jest efektywnym rozwiązaniem, dlatego najczęściej do szyfrowania wykorzystywany jest szybki algorytm AES, a tylko symetryczny klucz AES szyfrowany jest za pomocą algorytmu RSA. Takie właśnie podejście zastosowano także w proponowanym rozwiązaniu. Dokumenty nie są szyfrowane za pomocą algorytmu RSA, ponieważ jest on mało wydajny dla plików o dużych rozmiarach, a dodatkowo wymagałoby to dodatkowego dzielenia plików na mniejsze fragmenty. W celu zapewnienia największego bezpieczeństwa klucza symetrycznego AES, tylko sam klucz AES jest szyfrowany za pomocą przechowywanego w HSM klucza RSA o długości 2048 bitów.

4.2.6. Funkcja skrótu SHA-256

SHA-256 (ang. *Secure Hash Algorithm* 256-bit), jest jednym z najpopularniejszych algorytmów kryptograficznych służących do generowania skrótów (hashów) danych [69]. Algorytm ten został stworzony przez amerykańską Agencję Bezpieczeństwa Narodowego (ang. *National Security Agency* – NSA) i jest szeroko wykorzystywany w świecie kryptografii oraz technologii blockchain. Jego nazwa wskazuje na to, że generuje on skróty o długości 256 bitów. Działa na zasadzie przekształcania dowolnie długiego ciągu danych wejściowych w unikalny, stałej długości skrót, który jest praktycznie niemożliwy do odwrócenia. Jest on wykorzystywany w różnych aplikacjach, takich jak weryfikacja integralności plików, uwierzytelnianie haseł oraz w protokołach kryptograficznych [87].

Algorytm SHA-256 jest często stosowany w kontekście kryptowalut, szczególnie w przypadku kryptowaluty Bitcoin i innych opartych na technologii blockchain. Każdy blok transakcji w blockchain dla Bitcoin jest zabezpieczony przy użyciu SHA-256, co oznacza, że skrót wygenerowany dla danego bloku musi spełniać ściśle określone kryteria, aby blok ten został uznany za prawidłowy. Proces generowania skrótu SHA-256 jest bardzo wymagający obliczeniowo, co dodatkowo zwiększa bezpieczeństwo sieci blockchain. W rezultacie, SHA-256 jest nie tylko ważnym narzędziem w dziedzinie kryptografii, ale także odgrywa kluczową rolę w utrzymaniu integralności i bezpieczeństwa wielu systemów informatycznych, w tym kryptowalut i sieci blockchain.

4.2.7. Sprzętowy moduł bezpieczeństwa (HSM)

Sprzętowy moduł bezpieczeństwa (ang. *Hardware Security Module* – HSM) to fizyczne urządzenie lub moduł, który został zaprojektowany w celu zapewnienia wysokiego poziomu zabezpieczeń dla operacji kryptograficznych (np. szyfrowania, deszyfrowania, podpisywania, silnego uwierzytelniania), przechowywania kluczy, certyfikatów cyfrowych

(służących np. do uwierzytelniania i nawiązywania bezpiecznych połączeń) i innych wrażliwych danych. Moduły te tradycyjnie występują w formie karty lub zewnętrznego urządzenia, które bezpośrednio dołącza się do komputera lub serwera sieciowego. HSM zawiera jeden lub więcej bezpiecznych układów kryptoprocesorów. Wiele algorytmów kryptograficznych i protokołów bezpieczeństwa wymaga losowych liczb. HSM dostarcza źródła entropii do generowania liczb losowych, co jest fundamentem dla bezpieczeństwa tych mechanizmów.

Ze względu na kluczową rolę, jaką odgrywają HSM w zabezpieczaniu aplikacji i infrastruktury, są one zwykle certyfikowane według międzynarodowych standardów, takich jak Common Criteria [88], [89] (np. przy użyciu profilu ochrony EN 49 221-5 „Moduł kryptograficzny dla usług zaufania") lub FIPS 140 [90]. Chociaż najwyższym poziomem certyfikacji bezpieczeństwa FIPS 140 jest poziom bezpieczeństwa 4, większość HSM posiada certyfikat poziomu 3. HSM powinien z definicji być odporny na naruszenie zabezpieczeń i posiadać funkcje pozwalające na reakcję w przypadku wykryciu naruszenia zabezpieczeń (np. automatyczne usuwanie materiału kryptograficznego) lub funkcje zapewniające dowody na naruszenie zabezpieczeń (np. widoczne oznaki naruszenia zabezpieczeń, rejestrowanie i alarmowanie). Ponadto HSM jest zaprojektowany w taki sposób, aby był on odporny na różnego rodzaju ataki, takie jak typu *side-channel* (ataki wykorzystujące np. analizę zużycia energii czy czasu operacji), próby złamania kluczy czy próby fizycznego dostępu do urządzenia.

HSM są powszechnie stosowane w sektorze finansowym do zabezpieczania operacji finansowych, takich jak płatności elektroniczne i przesyłanie środków. HSM są też używane do generowania i przechowywania kluczy prywatnych niezbędnych do elektronicznego podpisywania dokumentów. Dzięki zastosowaniu HSM firmy i organizacje mogą skutecznie chronić swoje poufne dane i procesy. Dokumenty takie jak umowy i transakcje elektroniczne mogą być ponadto weryfikowane pod kątem integralności i autentyczności. HSM znajdują zastosowanie w różnych dziedzinach, takich jak bankowość, finanse, opieka zdrowotna, sektor publiczny, chmura obliczeniowa i wiele innych, gdzie bezpieczeństwo kluczy i danych jest priorytetowe.

4.2.8. Sieć IPFS

InterPlanetary File System (IPFS) to protokół i system rozproszonego przechowywania i udostępniania danych w Internecie. IPFS jest oparty na idei zamiany tradycyjnego modelu opartego na lokalizacji (hosting plików na konkretnych serwerach) na model oparty na zawartości (przechowywanie plików w sieci rozproszonej). IPFS i technologia

blockchain są często rozważane razem, ponieważ obie mają podobne cele związane ze zdecentralizowanym przechowywaniem danych i zapewnieniem bezpieczeństwa oraz niezmienności tych danych. Każdy plik przechowywany w IPFS jest identyfikowany za pomocą unikalnego skrótu jego zawartości, znanej jako „Content Identifier". Ten identyfikator jest związany z zawartością pliku, co oznacza, że nawet małe zmiany w pliku generują zupełnie inny skrót. IPFS działa na zasadzie protokołu P2P (ang. *peer-to-peer*) co oznacza, że węzły sieci są równorzędne i mogą komunikować się bezpośrednio między sobą. Dzięki temu eliminuje się punkty awarii i jednocześnie zwiększa wydajność i odporność systemu. Zamiast odnoszenia się do lokalizacji pliku na konkretnej maszynie, w IPFS pliki są odnoszone do ich skrótów, co pozwala na przechowywanie tych plików w wielu węzłach sieci. To umożliwia także odnalezienie plików niezależnie od ich fizycznej lokalizacji. IPFS wykorzystuje mechanizm pamięci podręcznej (ang. *cache*), dzięki któremu często używane dane są przechowywane lokalnie na węzłach, co poprawia szybkość dostępu do tych danych. Dane w IPFS są podpisane cyfrowo, co pomaga w zweryfikowaniu ich integralności i autentyczności. Ponadto IPFS wspiera szyfrowanie treści w celu ochrony prywatności. Dzięki temu, że wiele węzłów przechowuje kopie tych samych danych, IPFS automatycznie zapewnia pewną redundancję, co przyczynia się do trwałości danych nawet w obliczu awarii węzłów. IPFS ma wiele zastosowań, takich jak udostępnianie zawartości internetowej, dystrybucja plików, przechowywanie danych, tworzenie aplikacji opartych na blockchain i wiele innych. Dzięki swojej rozproszonej naturze i możliwości przechowywania danych w sposób odporny na cenzurę, IPFS jest także jednym z narzędzi wspierających ideę otwartego i zdecentralizowanego Internetu.

4.3. Testowanie e-usługi

Pierwsze testy zrealizowanego rozwiązania były przeprowadzane już podczas opracowywania usługi i implementacji kolejnych jej funkcjonalności. Testy te obejmowały weryfikację działania kodu oraz testy związane z konfiguracją usługi jak i wykorzystaniem różnych platform i narzędzi. Kolejna część testów została przeprowadzona po wdrożeniu finalnej wersji e-usługi. Były to testy funkcjonalne i wydajnościowe w środowisku produkcyjnym, w celu upewnienia się, że wszystko działa zgodnie z oczekiwaniami. W pracy zaprezentowano dwa zrealizowane scenariusze testowe. W każdym z nich założono, że e-usługa nośnika trwałego została wdrożona dla banku, który pełni w niej rolę dominującą (tylko bank może inicjować przetwarzanie dokumentu), a rola klienta banku ogranicza się tylko do akceptacji lub odrzucenia dokumentu. Zaufana trzecia strona

pełni tu rolę dostawcy e-usługi oraz nadzorcy monitorującego cały proces przechowywania i przetwarzania dokumentów (w tym zarządzanie siecią blockchain i siecią IPFS).

Zaimplementowana na platformie Hyperledger Besu sieć blockchain posiadała odpowiednie parametry konfiguracyjne – wybrane z nich zostały zestawione w tabeli 4.

Tabela 4. Parametry konfiguracyjne zrealizowanej sieci blockchain

Parametr	Wartość
algorytm konsensusu	IBFT
liczba węzłów uprawnionych do zatwierdzania	4
blockperiodseconds (w sekundach)	2
requesttimeoutseconds (w sekundach)	4
gasLimit	0x1FFFFFFFFFFFF
contractSizeLimit	2147483647
min-gas-price	0

4.3.1. Scenariusz 1

W pierwszym scenariuszu testowym założono, że bank chce wprowadzić nowy dokument dla każdego z 10 tys. klientów (np. aneks do umowy). Każdy z tych dokumentów jest spersonalizowany oraz dedykowany jednemu z klientów banku i musi zostać przez niego zaakceptowany lub odrzucony. W konsekwencji e-usługa musi przetworzyć 10 tys. różnych dokumentów, które trzeba uzgodnić z 10 tys. klientami banku.

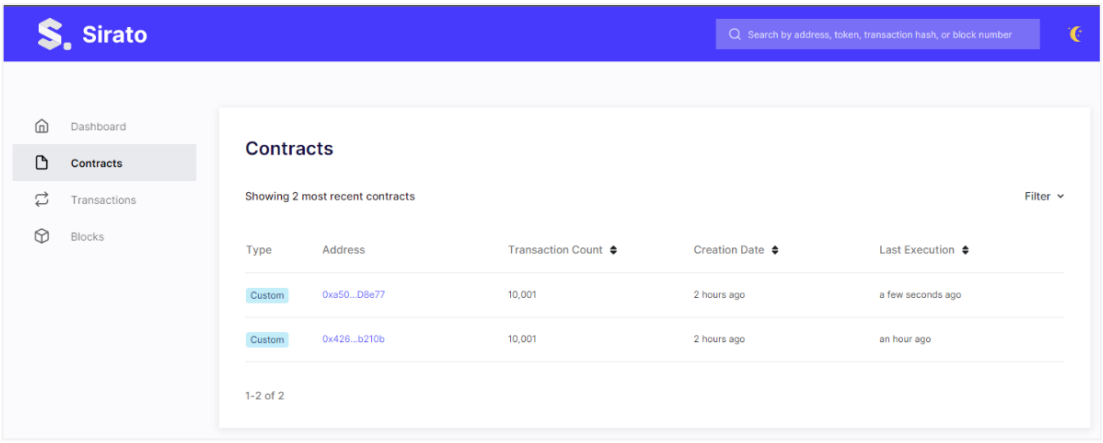
W pierwszym kroku bank generuje dla każdego dokumentu 256-bitowy symetryczny klucz AES i korzystając z asymetrycznego algorytmu kryptograficznego RSA każdy z tych kluczy szyfruje za pomocą 2048-bitowego klucza publicznego TTP. Następnie bank przesyła do TTP zestaw składający się z 10 tys. (jawnych) dokumentów, 10 tys. identyfikatorów klientów banku, których te dokumenty dotyczą oraz 10 tys. zaszyfrowanych symetrycznych kluczy AES (przypisanych po jednym do każdego dokumentu).

W kolejnym kroku TTP odszyfrowuje wszystkie 10 tys. otrzymanych kluczy AES za pomocą klucza prywatnego RSA należącego do TTP (ta operacja wykonywana jest z wykorzystaniem bezpiecznego modułu sprzętowego HSM należącego do TTP) i podpisuje elektronicznie wszystkie otrzymane dokumenty swoim podpisem. Następnie za pomocą rozszyfrowanych kluczy AES szyfruje symetrycznie każdy z 10 tys. dokumentów (każdy dokument innym, odpowiadającym mu kluczem AES).

Następnie TTP przesyła zaszyfrowane (podpisane) dokumenty na serwer IPFS, który generuje skróty dokumentów za pomocą algorytmu SHA-256 i razem z zaszyfrowanymi

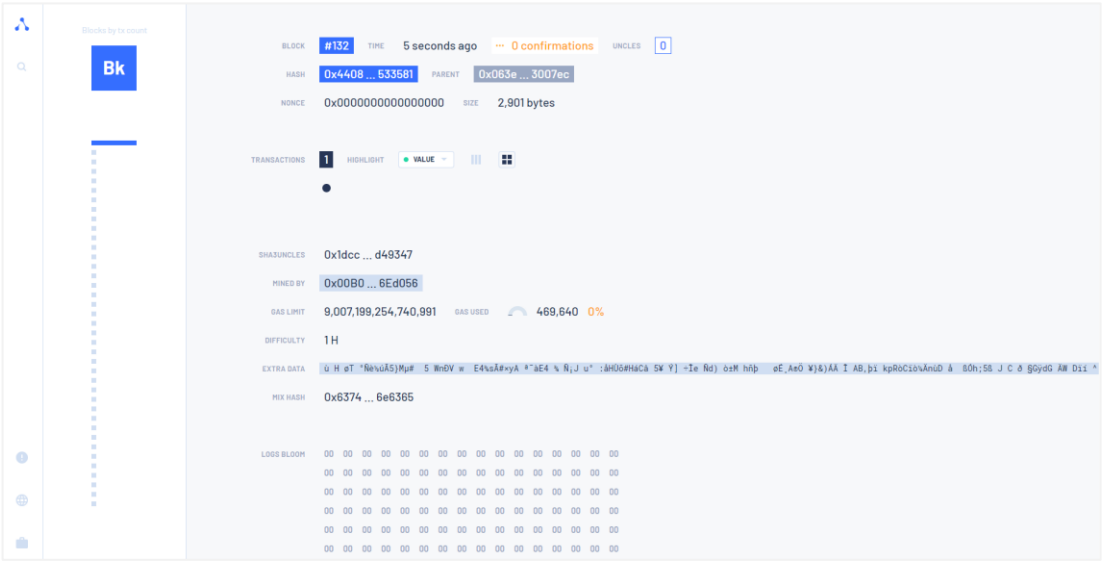
dokumentami umieszcza w sieci IPFS. Do każdego umieszczonego dokumentu IPFS generuje link, który razem ze skrótami przesyła zwrotnie do TTP. W kolejnym kroku TTP do sieci blockchain dodaje 10 tys. transakcji (dla każdego dokumentu oddzielnie). Każda transakcja zawiera skrót dokumentu SHA-256 (pole DID w strukturze bloku blockchain), identyfikator podmiotu, który przesłał dokument (jest to numeryczna wartość identyfikująca bank – pole CID) oraz identyfikator operacji dodania dokumentu (pole OID). Sam dokument, ze względu na ograniczenia limitu danych możliwych do zapisania w sieci blockchain, nie jest zapisywany w bloku. Właściwe, zaszyfrowane dokumenty wraz z ich skrótami przechowywane są w sieci IPFS.

W kolejnym kroku lista zawierająca 10 tys. pozycji przesyłana jest zwrotnie do banku. Każda pozycja w liście posiada następujące informacje: skrót dokumentu, link do dokumentu w sieci IPFS oraz identyfikator klienta, którego dotyczy dokument. Następnie bank korzystając z linków do dokumentów pobiera dokumenty z sieci IPFS i rozszyfrowuje je za pomocą posiadanych kluczy AES. W kolejnym etapie bank udostępnia te dokumenty klientom (w formie rozszyfrowanej, aby klienci mogli się z nimi zapoznać, a także pobrać na swoje urządzenie). Każdy z klientów po zapoznaniu się z dokumentem podejmuje decyzję o akceptacji bądź jego odrzuceniu. Decyzja klienta jest przekazywana do banku, który zwrotnie przekazuje ją do TTP (wraz z identyfikatorem klienta oraz skrótem dokumentu). Następnie TTP każdą decyzję (traktowaną jako operację na dokumencie i przechowywaną w bloku w polu OID) wraz z identyfikatorem klienta (CID) oraz skrótem dokumentu (DID) umieszcza w sieci blockchain w postaci nowej transakcji w bloku. Ostatecznie po podjęciu decyzji przez każdego z 10 000 klientów w sieci blockchain pojawi się 20 000 transakcji (10 tys. transakcji z dokumentami dostarczonymi od banku i 10 000 transakcji z decyzjami 10 000 klientów dot. tych dokumentów), co zostało przedstawione na rys. 4.5. Na rysunku widocznych jest o 2 transakcje więcej (po jednej dla każdego smart kontraktu dot. dodania dokumentu i dodania decyzji). Wynika to z faktu, że samo dodanie smart kontraktu jest już rejestrowane jako pierwsza transakcja tego smart kontraktu.



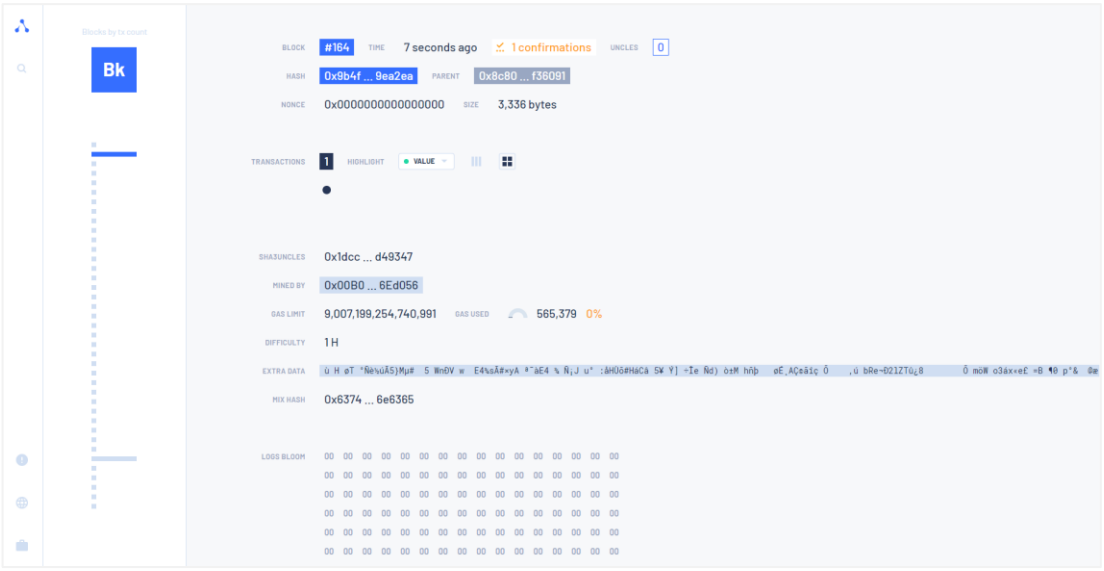
Rys. 4.5. Podsumowanie liczby transakcji po realizacji scenariusza 1 w narzędziu Sirato Explorer

Pierwszy dodany smart kontrakt w sieci blockchain (widoczny na rys. 4.6) jest kontraktem odpowiadającym za zapisywanie danych o przesłanych dokumentach w sieci blockchain. Na rysunku można zauważyć „0 confirmation" (na górze rysunku), co oznacza, że transakcja została już dodana do sieci, ale nie została jeszcze potwierdzona przez węzły blockchain odpowiadające za konsensus, czyli potwierdzanie transakcji.



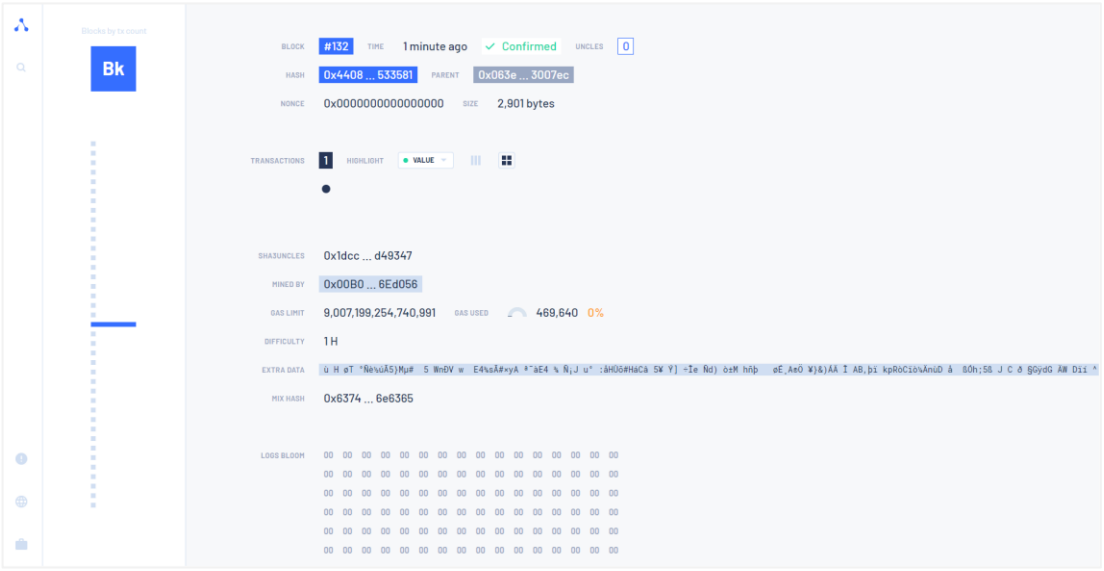
Rys. 4.6. Pierwszy wysłany smart kontrakt do sieci blockchain

Później został przesłany drugi smart kontrakt (rys. 4.7) odpowiadający za przesyłane decyzje klientów.



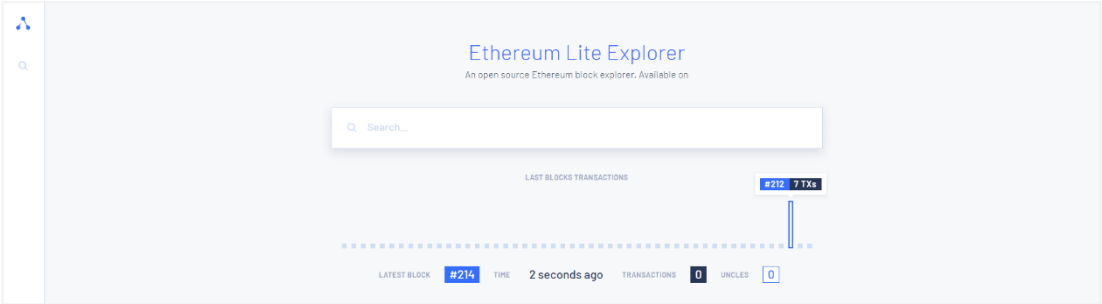
Rys. 4.7. Drugi wysłany smart kontrakt do sieci blockchain

Przykładową, w pełni zaakceptowaną transakcję dodaną do sieci blockchain prezentuje rysunek 4.8 (potwierdza to w górnej części rysunku zielony napis „Confirmed").



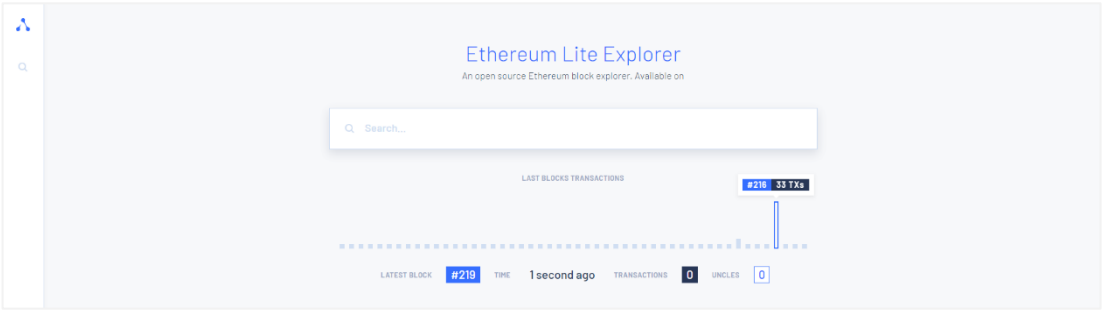
Rys. 4.8. Pierwsza w pełni zaakceptowana transakcja zapisana w sieci blockchain

Na diagramie z rysunku 4.9 widać pierwszy „pik", czyli pierwszy blok zawierający siedem pierwszych transakcji przesłanych do sieci blockchain.



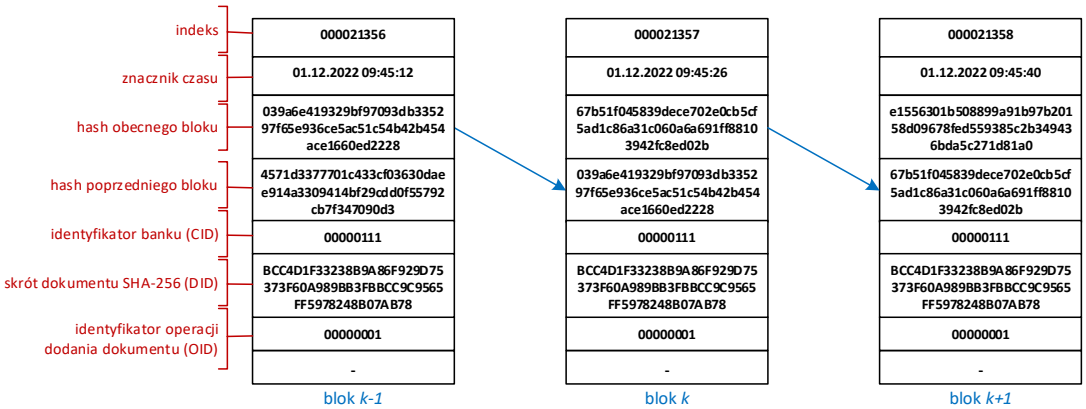
Rys. 4.9. Pierwszy blok (zawierający 7 transakcji) przesłany do sieci blockchain

Na kolejnym diagramie (rys. 4.10) widoczny jest drugi, większy „pik" oznaczający drugi blok przesłany do sieci blockchain zawierający 33 transakcje.



Rys. 4.10. Drugi blok (zawierający 33 transakcje) przesłany do sieci blockchain

Przykładowy fragment łańcucha bloków w scenariuszu 1 mógłby wyglądać jak na rys. 4.11 (dla zwiększenia czytelności rysunku przyjęto, że każdy blok sieci zawiera dokładnie jedną transakcję – choć taka sytuacja hipotetycznie może się zdarzyć, to jednak jest bardzo rzadka, ponieważ w praktyce blok zawiera informacje o wielu transakcjach).



Rys. 4.11. Fragment przykładowej struktury blockchain w scenariuszu 1

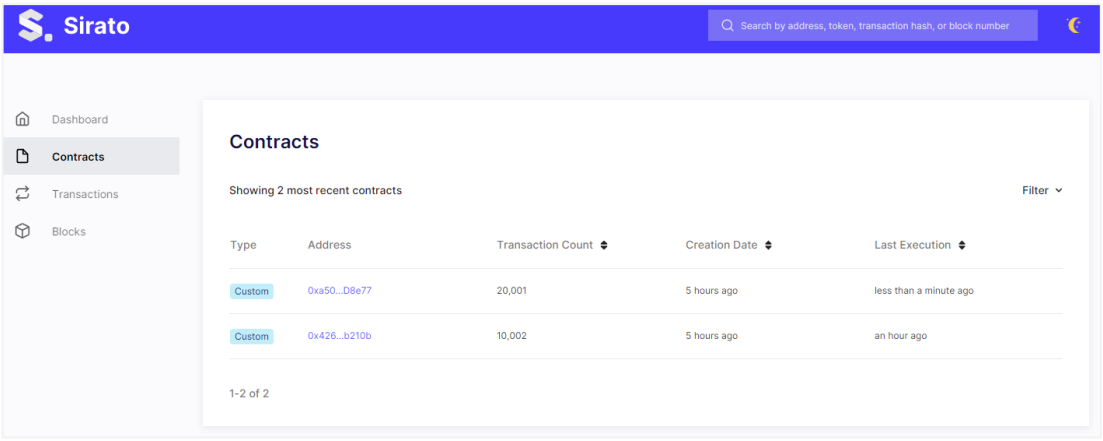
4.3.2. Scenariusz 2

Drugi zrealizowany scenariusz testowy zakładał, że bank wprowadza nowy dokument (np. regulamin) wspólny dla wszystkich klientów, który trzeba uzgodnić z każdym z 10 000 klientów banku. W pierwszym kroku bank przesyła do TTP nowy dokument oraz listę 10 tys. identyfikatorów klientów banku, których ten dokument dotyczy.

W kolejnym kroku TTP podpisuje dokument elektronicznie swoim podpisem i generuje dwa 2048-bitowe klucze RSA (prywatny i publiczny), a także symetryczny 256-bitowy klucz za pomocą algorytmu AES-256. Za pomocą tego klucza symetrycznego AES szyfrowany jest dokument, a sam klucz symetryczny AES szyfrowany jest za pomocą klucza prywatnego RSA. Warto zauważyć, że generowanie kluczy AES i RSA przeprowadzane jest w bezpiecznym module sprzętowym HSM.

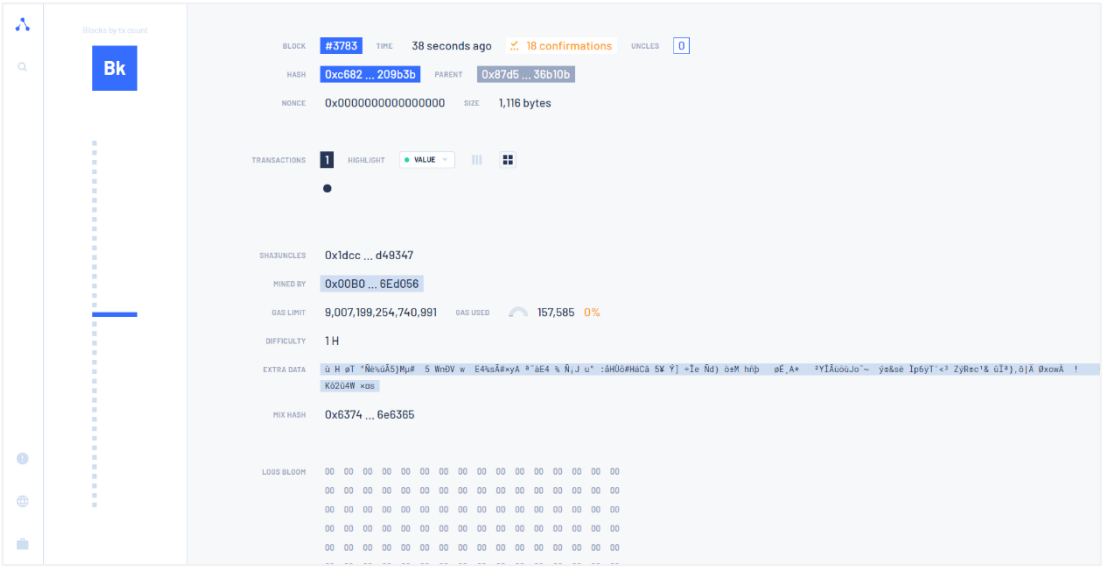
Następnie TTP umieszcza w sieci IPFS zaszyfrowany dokument. IPFS zwrotnie przesyła skrót dokumentu (SHA-256) oraz link do dokumentu w sieci IPFS, dzięki któremu możliwy będzie później dostęp do tego dokumentu. W kolejnym kroku TTP dodaje do sieci blockchain nowy blok z transakcją zawierającą skrót dokumentu SHA-256 (pole DID w strukturze bloku blockchain), identyfikator podmiotu, który przesłał dokument (jest to numeryczna wartość identyfikująca bank – pole CID) oraz identyfikator operacji dodania dokumentu (pole OID). Sam dokument, ze względu na ograniczenia limitu danych możliwych do zapisania w sieci blockchain, nie jest zapisywany w bloku, ale umieszczany w sieci IPFS.

W kolejnym kroku skrót dokumentu, link do dokumentu w IPFS, zaszyfrowany symetryczny klucz AES oraz klucz publiczny RSA przesyłane są zwrotnie do banku. Następnie bank korzystając z linku do dokumentu oraz posiadanych kluczy udostępnia dokument klientowi (np. w formie rozszyfrowanej, aby klient mógł się z nim zapoznać, a także pobrać na swoje urządzenie). Klient po zapoznaniu się z dokumentem podejmuje decyzję o akceptacji bądź jego odrzuceniu. Decyzja klienta jest przekazywana do banku, który zwrotnie przekazuje ją do TTP. Następnie decyzję tę wraz z identyfikatorem klienta (CID) oraz skrótem dokumentu (DID) TTP umieszcza w sieci blockchain w postaci nowej transakcji w bloku. Proces akceptacji bądź odrzucenia dokumentu przez pozostałych klientów jest analogiczny i iteracyjnie powtarzany przez bank. Ostatecznie po podjęciu decyzji przez każdego z 10 000 klientów w sieci blockchain pojawi się 10 001 transakcji (pierwsza transakcja z dokumentem dostarczonym od banku i 10 000 transakcji z decyzjami 10 000 klientów dot. tego dokumentu), co zostało przedstawione na rys. 4.12 (rysunek przedstawia sumaryczną ilość transakcji po realizacji scenariusza 1 i następnie scenariusza 2 w ramach tej samej sieci blockchain, dlatego ilość zrealizowanych transakcji w scenariuszu 2 wynosi 20 001 – 10 001 + 10 002 – 10 001 = 10 001).



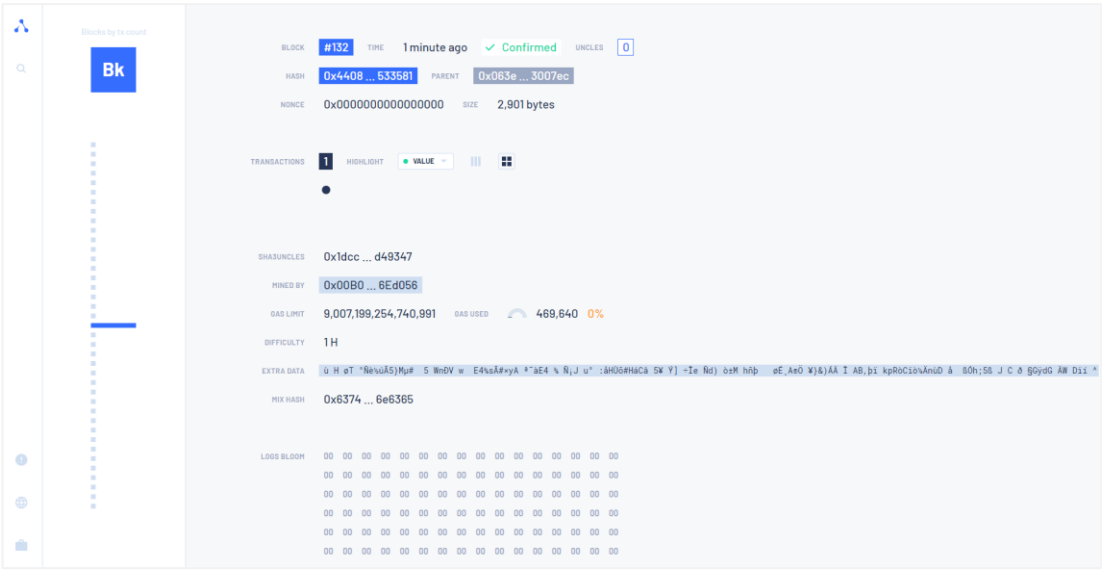
Rys. 4.12. Podsumowanie liczby transakcji po realizacji scenariusza 1 i scenariusza 2

Rysunek 4.13 przedstawia pierwsze uruchomienie smart kontraktu w scenariuszu 2. Kontrakt ten odpowiada za przesłany dokument i jak widać na rysunku transakcja w momencie zrzutu ekranu była w trakcie zatwierdzania (nie była jeszcze zatwierdzona, ale posiadała już 18 potwierdzeń).



Rys. 4.13. Pierwsza wysłana transakcja odpowiadająca za uruchomienie smart kontraktu dodania dokumentu do sieci blockchain (scenariusz 2)

Z kolei rys. 4.14 prezentuje pierwszą zaakceptowaną transakcję (zielona adnotacja „Confirmed") w pełni dodaną do sieci blockchain odpowiadającą za uruchomienie smart kontraktu z dodaniem decyzji klienta do sieci blockchain.



Rys. 4.14. Pierwsza zaakceptowana transakcja z decyzją klienta

Ponadto w scenariuszu 1 przyjęto, że ok. 80% klientów zaakceptuje dokument, a pozostałe 20% go odrzuci, a w scenariuszu 2 przyjęty poziom akceptacji wynosił 90%. Dlatego w implementacji obu scenariuszy dodano specjalne funkcje losujące, aby zrealizować powyższe założenia. W praktyce okazało się, że poziom akceptacji delikatnie różnił się od założonego (81,63% w scenariuszu 1 i 91,08% w scenariuszu 2). Pozostałe wyniki wydajnościowe uzyskane podczas realizacji obu scenariuszy zestawiono w tabeli 5.

Tabela 5. Zestawienie uzyskanych wyników eksperymentalnych dla scenariuszy 1 oraz 2

Parametr	Wynik uzyskany w scenariuszu 1	Wynik uzyskany w scenariuszu 2
Poziom akceptacji dokumentu przez klientów	81,63%	91,08%
Średni czas dodania do sieci blockchain transakcji dodania dokumentu (przez bank) [ms]	23,073	202,164
Średni czas dodania do sieci blockchain transakcji dodania decyzji klienta [ms]	0,0358544	0,0486139

Jak wynika z przeprowadzonych badań eksperymentalnych, wdrożona e-usługa działała prawidłowo. Zrealizowane dwa scenariusze testowe, w których w sumie do sieci blockchain dodano ponad 30 tys. transakcji, potwierdziły spełnienie zarówno wymagań funkcjonalnych jak i technicznych.

Otrzymane wyniki wydajnościowe także są akceptowalne. Średni czas dodania do sieci blockchain transakcji odpowiadającej za dodanie (przez bank) dokumentu do sieci blockchain wynosił ok. 23 ms, co dla 10 tys. dokumentów daje czas poniżej 4 minut. Dodanie jednego dokumentu w scenariuszu 2 wyniosło ok. 200 ms, co jest również czasem w pełni akceptowalnym (w tym scenariuszu przetwarzany był tylko jeden dokument). Średnie czasy dodawania transakcji z decyzjami klientów są podobne

i wynoszą zaledwie 0,036 ms (scenariusz 1) oraz 0,048 ms (scenariusz 2), co jest także w pełni akceptowalne.

4.4. Wdrożenie e-usługi

Wdrożenie e-usługi polegało na wprowadzeniu w infrastrukturze firmy wszystkich elementów wymaganych do działania usługi, w tym programów i narzędzi, a także zdefiniowanie wymagań serwerowych i dot. konfiguracji serwerów. Został dokonany wybór serwerów dostosowanych do wymagań usługi, biorąc pod uwagę obciążenie oraz dostępność technologii w firmie. Przygotowano zaplecze technologiczne, zapewniające niezbędne zasoby, takie jak moc obliczeniowa i przestrzeń dyskowa. Skonfigurowano parametry sieciowe, takie jak adresy IP, porty dla usług i narzędzi. Zostały ustawione prawa dostępu do plików i katalogów, aby ograniczyć dostęp tylko dla uprawnionych użytkowników. Zainstalowano oprogramowanie oraz komponenty odpowiedzialne za działanie usługi. Dokonano konfiguracji serwerów, baz danych, systemów monitoringu oraz innych narzędzi wspierających wdrażaną e-usługę.

Następnie dokonano wyboru odpowiedniego systemu operacyjnego, zgodnego z technologią używaną w innych usługach w firmie. Wybrano system operacyjny Linux Ubuntu, który został zainstalowany i skonfigurowany na każdym serwerze wchodzącym w skład e-usługi. Uruchomiono też jedną maszynę z systemem Windows Server 2019 odpowiadającą za jeden z węzłów IPFS. Maszyny odpowiedzialne za węzły blockchain posiadały przydzielone 4 wątki CPU, 8 GB pamięci RAM i 400 GB pojemności dyskowej zgodne z wymaganiami konfiguracyjnymi Hyperledger Besu. Wykorzystano także dodatkowo jedną maszynę z systemem Windows Server 2019 odpowiedzialną za wystawienie samej usługi napisanej w Javie, której celem było odbieranie zewnętrznych zapytań jak i umożliwianie komunikacji z zewnątrz z węzłami blockchain poprzez external API. Następnie zostało skonfigurowane całe środowisko obsługujące tę e-usługę. Wdrożona e-usługa znajduje się w ofercie firmy Perceptus sp. z o.o. jako niezależne rozwiązanie, które może być dostarczane klientom, dostosowując je uprzednio pod konkretne ich wymagania. Planowane jest również, aby opracowana e-usługa była w przyszłości wdrożona także w innych projektach realizowanych przez firmę. Formalne potwierdzenie realizacji wdrożenia w firmie Perceptus sp. z o.o. zostało umieszczone w niniejszej pracy w Dodatku B.

W kolejnym etapie zostały przeprowadzone szkolenia dla pracowników odpowiedzialnych za obsługę e-usługi obejmujące zapoznanie się z podstawami

technologii blockchain, a także poznanie specyfiki obsługi i działania tej usługi (w tym zapoznanie się z dokumentacją techniczną oraz ćwiczenia praktyczne związane z obsługą i utrzymaniem usługi). Szczegółowy zakres szkolenia obejmował zapoznanie się z definicją i podstawowymi pojęciami technologii blockchain, poznanie historii i rozwoju technologii, możliwości zastosowania technologii w różnych dziedzinach, porównanie różnych rodzajów sieci, wybór odpowiedniego rodzaju dla konkretnych zastosowań, przybliżenie budowy typowego bloku, przedstawienie procesu tworzenia i weryfikacji transakcji, przybliżenie mechanizmów konsensusu i ich działania oraz ich ważności, zasady działania kryptografii w technologii blockchain, bezpieczeństwo i prywatność sieci, zastosowanie kluczy kryptograficznych. Omawiano także możliwe działania związane z obsługą wdrożonej sieci blockchain w tym jej konfigurację i uruchamianie kolejnych i nowych węzłów sieci, zarządzanie dostępem i autoryzacją, testowanie i rozwijanie opracowanej sieci. Przedstawiono także działania narzędzi odpowiadających za monitoring sieci, które śledzą działanie usługi w czasie rzeczywistym. Omówiono także samą usługę zrealizowaną w języku Java oraz inteligentne kontrakty, ich definicję i zastosowanie (programowanie inteligentnych kontraktów, przykładowe kody oraz testowanie i wdrażanie nowych kontraktów). Na koniec przybliżono wybrane zagadnienia bezpieczeństwa w sieci blockchain obejmujące najczęstsze zagrożenia i ataki oraz najlepsze praktyki ich zabezpieczeń.

4.5. Ograniczenia opracowanej e-usługi

Pomimo wielu zalet wymienionych powyżej, zaproponowane rozwiązanie posiada również pewne ograniczenia. Jednym z nich jest fakt, że zrealizowana usługa wymaga ciągłego funkcjonowania (choć z punktu widzenia dostępności e-usługi może to być także jej zaleta). Oznacza to, że serwery, na których została umieszczona usługa wymagają ciągłej dostępności energii elektrycznej i zabezpieczeń zasilania awaryjnego, a w skrajnych przypadkach agregatora prądotwórczego. Przez to utrzymanie ciągłego działania usługi może generować znaczne koszty. Wymaga to ponadto zapewnienia dostępnego personelu, infrastruktury, energii elektrycznej oraz regularnych aktualizacji i konserwacji systemów. Usługi działające bez przerwy wymagają także ciągłego monitorowania i zarządzania, a to oznacza, że personel musi być dostępny 24 h na dobę przez 7 dni w tygodniu. W miarę jak technologia ewoluuje, konieczne jest też regularne aktualizowanie usługi, aby pozostała ona konkurencyjna i zgodna z aktualnymi standardami.

Kolejnym ograniczeniem jest konieczność zapewnienia dostępności węzłów w różnych lokalizacjach geograficznych w celu zapewnienia decentralizacji usługi i ograniczenia jej niedostępności. Wprowadzenie i utrzymanie infrastruktury serwerowej w różnych lokalizacjach może być kosztownym rozwiązaniem (wiąże się to z wydatkami na zakup i konfigurację sprzętu, utrzymanie, opłaty za prąd, łącza internetowe itp.).

Minusem opracowanego rozwiązania jest również duża liczba generowanych kluczy. W proponowanej e-usłudze dla każdego przetwarzanego dokumentu generowany jest symetryczny klucz AES, co przy dużej ilości dokumentów (liczonych w milionach) oznacza konieczność przechowywania i zarządzania bardzo dużą ilością krytycznego materiału kryptograficznego, przechowywanego w zewnętrznym HSM, którego pojemność jest ograniczona. Z drugiej strony warto podkreślić, że tak duża liczba kluczy pozytywnie wpływa na aspekt bezpieczeństwa proponowanego rozwiązania (przejęcie lub wyciek jednego klucza AES spowoduje dostęp tylko do jednego dokumentu).

4.6. Podsumowanie

W niniejszym rozdziale opisano aspekty implementacyjne i wdrożeniowe opracowanej e-usługi. Zdobyta wcześniej wiedza pozwoliła na sprawne określenie wymagań technicznych, które wynikały zarówno z zadań dot. nośnika trwałego, ale też z wymogów stawianych przez firmę, w kontekście posiadanych zasobów sprzętowych i istniejących już produktów i usług. Wymagania techniczne stanowiły świetne uzupełnienie wymagań funkcjonalnych określonych w rozdziale 3.1.

W dalszej części rozdziału dokonano przeglądu technik i narzędzi oraz dokonano wyboru tych najodpowiedniejszych spełniających zarówno wymogi techniczne jak i funkcjonalne wynikające ze specyfiki rozwiązania. Wybrano język programowania dla implementowanej e-usługi jak oraz rodzaj i typ sieci blockchain. Następnie zostały przedstawione wybrane narzędzia monitorujące sieć blockchain, które zostały odpowiednio skonfigurowane i wdrożone w firmie. Przybliżone zostały także wybrane algorytmy szyfrujące wykorzystane w e-usłudze, takie jak np. funkcja skrótu, algorytmy szyfrowania symetrycznego i asymetrycznego, a także scharakteryzowano sieć IPFS oraz wykorzystywany moduł HSM.

Na koniec zaprezentowano wyniki badań eksperymentalnych zrealizowanych w formie dwóch scenariuszy testowych oraz zagadnienia dot. wdrożenia zrealizowanej e-usługi w firmie Perceptus sp. z o.o., w której to rozwiązanie jest dostępne. Podsumowując, udało się zaimplementować e-usługę w oparciu o przedstawione

wymagania funkcjonalne jak i techniczne, w tym dot. nośnika trwałego pod kątem przetwarzania oraz zarządzania wrażliwymi dokumentami elektronicznymi.

5. Podsumowanie, wnioski i kierunki dalszych prac

Prace związane z realizacją niniejszej rozprawy ściśle łączyły część naukową z częścią wdrożeniową. Można nawet powiedzieć, że z części naukowej w dużym stopniu wynikała część wdrożeniowa i oba te obszary często wzajemnie się przenikały. Po opracowaniu założeń, koncepcji i schematu e-usługi zostały przeprowadzone testy i badania eksperymentalne, które potwierdziły poprawność opracowanej e-usługi oraz w pełni potwierdziły realizację celu i tezy pracy. Określone wymagania względem tezy pracy jak i wdrożenia oraz implementacji e-usługi zostały spełnione. Kierunki dalszych prac obejmują m.in. prace naukowe związane z technologią blockchain, jej rozwojem i wprowadzaniem kolejnych pomysłów w życie, a także w miarę możliwości rozwój opracowanej e-usługi w firmie oraz implementację technologii blockchain w ramach kolejnych realizowanych przez firmę projektów.

5.1. Potwierdzenie tezy pracy

Głównym celem pracy był projekt oraz realizacja bezpiecznej i zaufanej elektronicznej usługi (e-usługi) trwałego nośnika umożliwiającej przetwarzanie oraz zarządzanie wrażliwymi dokumentami elektronicznymi. Teza pracy została sformułowana następująco:

Możliwe jest opracowanie oraz wdrożenie elektronicznej usługi trwałego nośnika, która jest zarówno bezpieczna, jak i zaufana.

Ze względu na charakter niniejszej rozprawy, prowadzone prace **łączyły aspekty naukowo-wdrożeniowe**. W ramach prac naukowych w pierwszej kolejności dokonano przeglądu aktualnego stanu wiedzy w zakresie trwałego nośnika. W szczególności przeprowadzono gruntowną analizę aspektów prawnych (ze szczególnym uwzględnieniem regulacji funkcjonujących w Polsce), wykonano również przegląd teoretyczny (przegląd literatury) oraz praktyczny (w tym usług i produktów dostępnych na rynku). Na tej podstawie określono wymagania funkcjonalne oraz techniczne dotyczące projektowanej e-usługi trwałego nośnika. Kolejnym krokiem był przegląd oraz analiza dostępnych algorytmów kryptograficznych, technologii blockchain oraz sprzętowych modułów bezpieczeństwa pod kątem projektowanej e-usługi. Przeprowadzono również analizę możliwości wykorzystania zaufanej trzeciej strony (TTP) pod kątem opracowywanego rozwiązania. **Wymiernym efektem** przeprowadzonych prac naukowych było **opracowanie schematu (w szczególności**

modelu procesu) realizacji e-usługi, a także **opracowanie struktury sieci blockchain** pod kątem projektowanej usługi.

Zrealizowane prace naukowe stanowiły podstawę **prac wdrożeniowych**, w ramach których przede wszystkim **zrealizowano (implementacja programowa) opracowaną metodę e-usługi**. Następnie, **przeprowadzono szereg badań eksperymentalnych** zrealizowanego rozwiązania, zarówno w zakresie wykorzystania technologii blockchain, jak i wybranych algorytmów oraz metod kryptograficznych w projektowanej e-usłudze. Bardzo istotnym etapem prac wdrożeniowych była implementacja opracowanej e-usługi w infrastrukturze serwerowej, która stanowiła fundament docelowego wdrożenia. **Zgodnie z założeniami, opracowaną e-usługę trwałego nośnika wdrożono w firmie Perceptus sp. z o.o.** (formalne potwierdzenie znajduje się w Dodatku B). Ostatnim etapem były badania eksperymentalne – testy końcowe opracowanego i wdrożonego rozwiązania.

Przeprowadzone testy końcowe potwierdziły poprawność opracowanej e-usługi. W szczególności, potwierdzona została **zgodność wymagań określonych w ramach opracowanego modelu usługi** (element prac naukowych) **z wynikami uzyskanymi po jej wdrożeniu** (wyniki prac wdrożeniowych). **Oznacza to, że teza pracy została potwierdzona zarówno od strony naukowej** (opracowano elektroniczną usługę trwałego nośnika, która jest zarówno bezpieczna, jak i zaufana), **jak i wdrożeniowej** (opracowaną usługę fizycznie wdrożono w firmie Perceptus sp. z o.o.).

5.2. Oryginalne wyniki pracy

Nowatorskie, oryginalne wyniki niniejszej pracy mogą zostać podzielone na dwie zasadnicze grupy:

1. W zakresie prac naukowych, tzn. **opracowania elektronicznej usługi trwałego nośnika, która jest zarówno bezpieczna, jak i zaufana:**
    - przeprowadzenie gruntownej analizy aktualnego stanu wiedzy w zakresie trwałego nośnika, z uwzględnieniem aspektów prawnych, teoretycznych oraz praktycznych;
    - przeprowadzenie przeglądu oraz analizy dostępnych algorytmów kryptograficznych, technologii blockchain oraz sprzętowych modułów bezpieczeństwa pod kątem projektowanej e-usługi trwałego nośnika;
    - przeprowadzenie analizy możliwości wykorzystania zaufanej trzeciej strony pod kątem opracowywanej e-usługi;

- opracowanie wymagań funkcjonalnych oraz technicznych projektowanej e-usługi;
- opracowanie modelu procesu realizacji e-usługi (wraz z jego wariantami);
- opracowanie struktury sieci blockchain pod kątem projektowanej e-usługi;
- **opracowanie elektronicznej usługi trwałego nośnika, która jest zarówno bezpieczna, jak i zaufana.**

2. W zakresie prac wdrożeniowych, tzn. **wdrożenia elektronicznej usługi trwałego nośnika, która jest zarówno bezpieczna, jak i zaufana:**
   - przeprowadzenie gruntownej analizy w zakresie trwałego nośnika pod kątem aspektów implementacyjnych oraz wdrożeniowych;
   - implementacja programowa opracowanej e-usługi trwałego nośnika;
   - przeprowadzenie wstępnych badań eksperymentalnych zrealizowanej e-usługi pod kątem wykorzystanej technologii blockchain oraz wybranych algorytmów i metod kryptograficznych;
   - implementacja sprzętowa opracowanej e-usługi w infrastrukturze serwerowej;
   - **wdrożenie opracowanej usługi trwałego nośnika w firmie Perceptus sp. z o.o.,**
   - przeprowadzenie badań eksperymentalnych, które stanowiły testy końcowe opracowanego i wdrożonego rozwiązania.

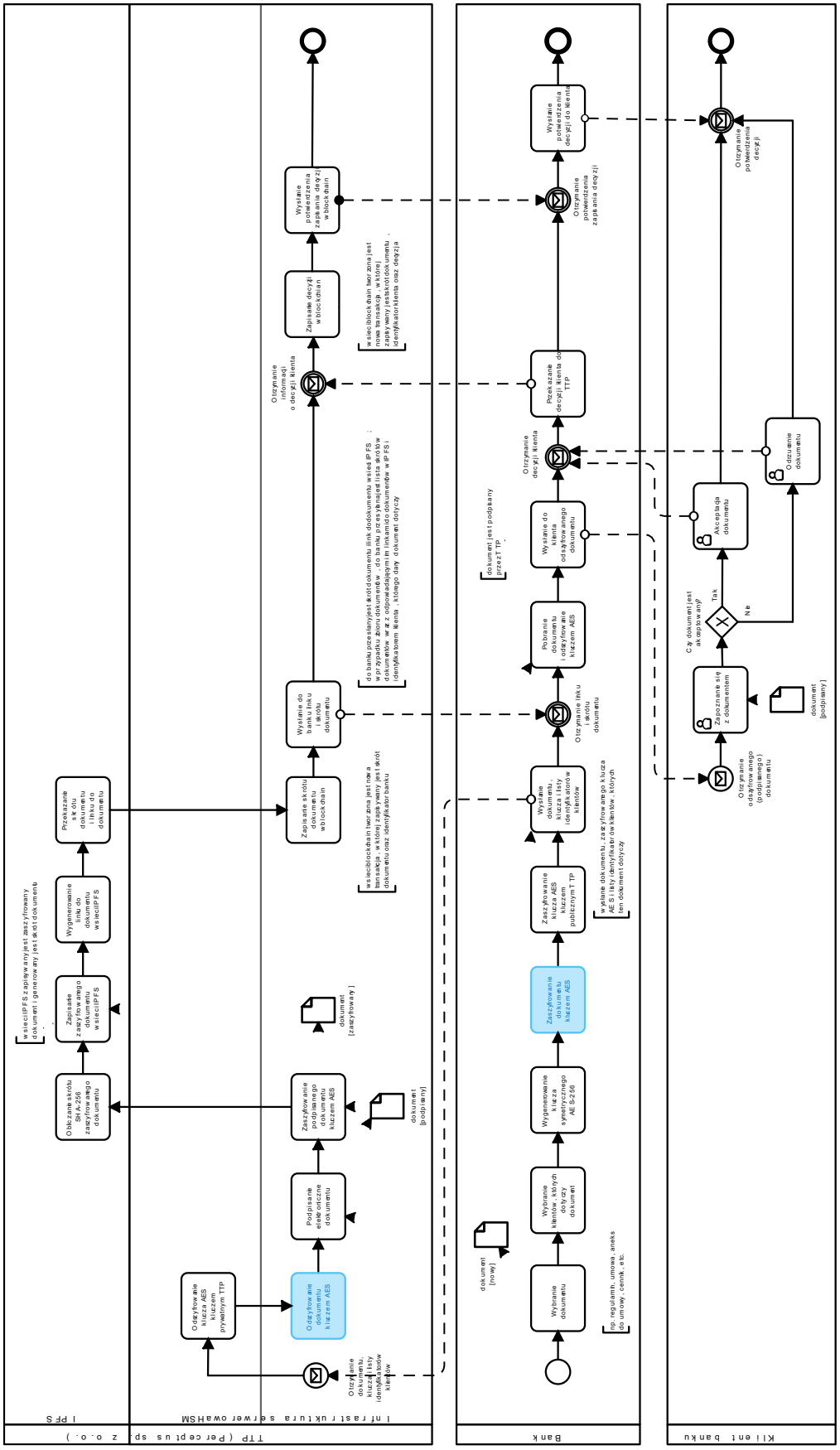
5.3. Kierunki dalszych prac

Dalsze prace będą koncentrowały się wokół zagadnień skalowalności opracowanego rozwiązania, zwiększaniu przepustowości sieci blockchain, poprawie wydajności i redukcji kosztów transakcyjnych. Autor planuje także opracować nowy protokół konsensusu, który byłby bardziej efektywny i zużywający mniej zasobów. Dodatkowo planowane są prace dot. popularyzacji opracowanej technologii wśród społeczeństwa.

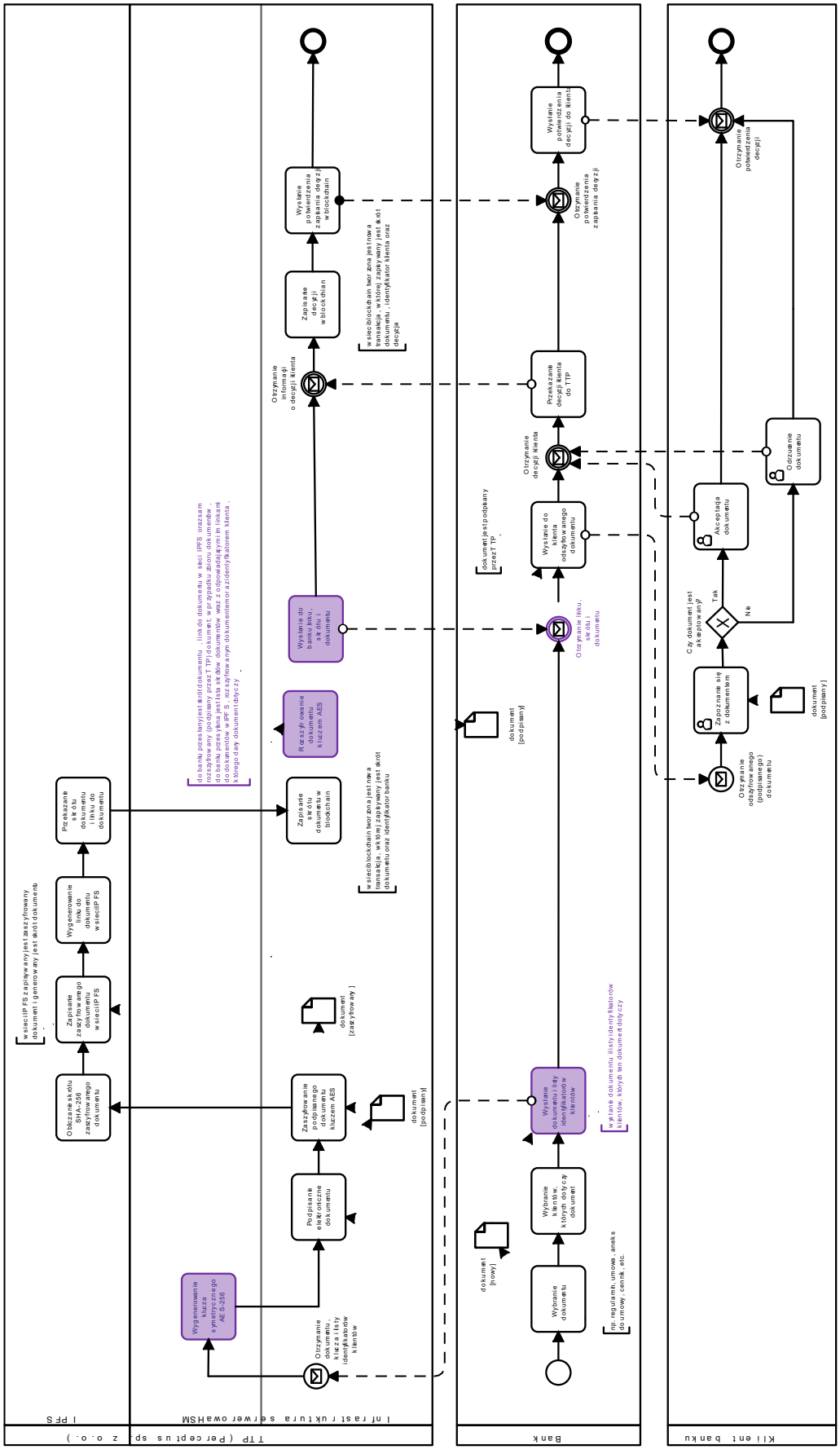
Ponadto autor planuje dalsze badania związane z technologią blockchain, ze względu na jej duży potencjał i możliwości zastosowania także w innych obszarach gospodarki. Jednym z nich jest implementacja sieci blockchain w architekturze Internetu Medycznych Rzeczy (ang. *Internet of Medical Things* – IoMT). Uzyskane wyniki tych badań zostały opublikowane w artykule naukowym w czasopiśmie *Electronics* [69]. Warto podkreślić, że wspomniany artykuł był efektem współpracy międzynarodowej autora z prof. Aniruddha Bhattacharjya z Indii – specjalistą z zakresu technologii blockchain i jej zastosowań.

Dodatek A. Warianty algorytmu e-usługi

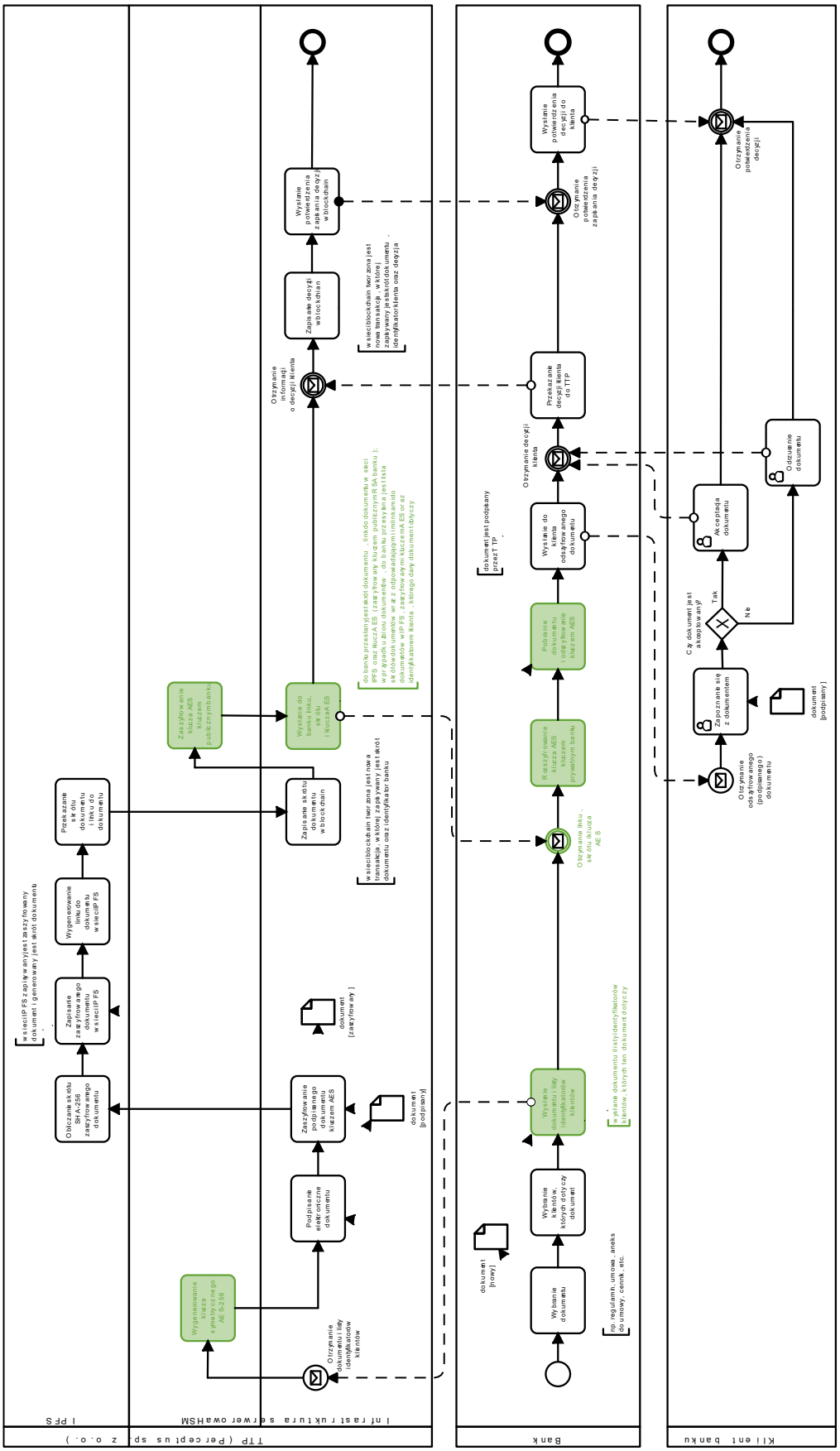
W niniejszym dodatku zaprezentowano kompletne wersje wariantów algorytmu proponowanej e-usługi szczegółowo omówione w rozdziale 3.2. Na rysunku A.1 przestawiono wersję algorytmu, w którym szyfrowanie dokumentu kluczem symetrycznym AES (wygenerowanym przez bank) odbywa się po stronie banku. Rysunek A.2 przedstawia wariant algorytmu, w którym cały proces szyfrowania i deszyfrowania dokumentów wraz z generowaniem niezbędnych kluczy symetrycznych AES odbywa się po stronie TTP. Ostatni rysunek A.3 prezentuje podobny do poprzedniego wariant algorytmu, z tą różnicą, że wygenerowany przez TTP klucz symetryczny AES jest w formie zaszyfrowanej przekazywany do banku (wykorzystano tu algorytm szyfrowania asymetrycznego, w którym klucz AES szyfrowany jest za pomocą klucza publicznego banku, a następnie odszyfrowywany przez bank z wykorzystaniem jego prywatnego klucza RSA).



Rys. A.1. Diagram BPMN dla wariantu algorytmu proponowanej e-usługi (szyfrowanie dokumentu przez bank)



Rys. A.2. Diagram BPMN dla wariantu algorytmu proponowanej e-usługi (generowanie klucza AES oraz odszyfrowanie dokumentu przez TTP)



Rys. A.3. Diagram BPMN dla wariantu algorytmu proponowanej e-usługi (generowanie klucza AES oraz szyfrowanie go przez TTP)

Dodatek B. Potwierdzenie zrealizowania wdrożenia

W niniejszym dodatku zamieszczono skan dokumentu potwierdzającego zrealizowanie wdrożenia w firmie Perceptus sp. z o.o. z Zielonej Góry.

perceptus

Zielona Góra, dn. 27.10.2023 r.

Perceptus sp. z o. o.
ul. Nowy Kisielin - A. Wysockiego 10
66-002 Zielona Góra

INFORMACJA

o zrealizowaniu wdrożenia w ramach doktoratu

Niniejszym informujemy, iż opracowana przez doktoranta, Pan Kamila Kozdrója, e-usługa nośnika trwałego w ramach doktoratu wdrożeniowego pt.: *„Opracowanie oraz wdrożenie elektronicznej usługi w postaci nośnika trwałego umożliwiającej przetwarzanie oraz zarządzanie wrażliwymi dokumentami elektronicznymi"* została wdrożona w infrastrukturze firmy i włączona do oferty firmy Perceptus sp. z o. o.

PREZES ZARZĄDU
Jacek Starościc

PERCEPTUS Sp z o.o.
ul Nowy Kisielin - A Wysockiego 10
66-002 Zielona Góra
NIP 929-180-85-78, REGON 080307093

Perceptus sp. z o. o.
ul. Nowy Kisielin – A. Wysockiego 10
66-002 Zielona Góra
+48 68 470 07 70
perceptus@perceptus.pl

NIP: 929 180 85 78
REGON: 080307093
KRS: 0000320099
Kapitał zakładowy 50 000,00 zł wpłacony w całości

Bank: Alior Bank S.A. (SWIFT: ALBPPLPW)
PLN: 46 2490 0005 0000 4530 7544 5466
EUR: 48 2490 0005 0000 4600 5832 7990

Bibliografia

[1] M. Ryszczyk, „Bankowość elektroniczna jako trwały nośnik informacji", nr 3, s. 48–58, 2018.

[2] „UOKiK - Prawa konsumenta - Słownik", UOKiK - Prawa konsumenta. Dostęp: 14 wrzesień 2023. [Online]. Dostępne na: https://prawakonsumenta.uokik.gov.pl/slownik/

[3] UOKIK, „UOKiK Trwały nośnik - decyzje wobec ING, Getin Noble i PKO BP". Dostęp: 14 wrzesień 2023. [Online]. Dostępne na: https://uokik.gov.pl/aktualnosci.php?news_id=14909&news_page=4

[4] „Systemy bezpieczeństwa IT - niezawodne rozwiązania", Perceptus. Dostęp: 24 wrzesień 2023. [Online]. Dostępne na: https://perceptus.pl/

[5] „Dyrektywa Parlamentu Europejskiego i Rady 2011/83/UE z dnia 25 października 2011 r. w sprawie praw konsumentów, zmieniająca dyrektywę Rady 93/13/EWG i dyrektywę 1999/44/WE Parlamentu Europejskiego i Rady oraz uchylająca dyrektywę Rady 85/577/EWG i dyrektywę 97/7/WE Parlamentu Europejskiego i RadyTekst mający znaczenie dla EOG".

[6] „Dyrektywa Parlamentu Europejskiego i Rady (UE) 2015/ z dnia 25 listopada 2015 r. w sprawie usług płatniczych w ramach rynku wewnętrznego, zmieniająca dyrektywy 2002/65/WE, 2009/110/WE, 2013/36/UE i rozporządzenie (UE) nr 1093/2010 oraz uchylająca dyrektywę 2007/64/WE".

[7] „Art. 2. - Ustawa o prawach konsumenta". Dostęp: 23 wrzesień 2023. [Online]. Dostępne na: https://lexlege.pl/ustawa-o-prawach-konsumenta/art-2/

[8] S. Piątek, *Prawo telekomunikacyjne. Komentarz*, 4. wyd. C.H. Beck.

[9] H. Liu, X. Luo, H. Liu, i X. Xia, „Merkle Tree: A Fundamental Component of Blockchains", w *2021 International Conference on Electronic Information Engineering and Computer Science (EIECS)*, Changchun, China: IEEE, wrz. 2021, s. 556–561. doi: 10.1109/EIECS53707.2021.9588047.

[10] H. Xiong, M. Chen, C. Wu, Y. Zhao, i W. Yi, „Research on Progress of Blockchain Consensus Algorithm: A Review on Recent Progress of Blockchain Consensus Algorithms", *Future Internet*, t. 14, nr 2, Art. nr 2, luty 2022, doi: 10.3390/fi14020047.

[11] M. Di Pierro, „What Is the Blockchain?", *Comput. Sci. Eng.*, t. 19, nr 5, s. 92–95, 2017, doi: 10.1109/MCSE.2017.3421554.

[12] S. Nakamoto, „Bitcoin: A Peer-to-Peer Electronic Cash System".

[13] „Ethereum", ethereum.org. Dostęp: 15 wrzesień 2023. [Online]. Dostępne na: https://ethereum.org

[14] „Ethereum Whitepaper", ethereum.org. Dostęp: 23 wrzesień 2023. [Online]. Dostępne na: https://ethereum.org

[15] „Cryptocurrency for the Financial Services Space - XRP | Ripple". Dostęp: 23 wrzesień 2023. [Online]. Dostępne na: https://ripple.com/xrp/

[16] „IBM Supply Chain Intelligence Suite - Food Trust". Dostęp: 23 wrzesień 2023. [Online]. Dostępne na: https://www.ibm.com/products/supply-chain-intelligence-suite/food-trust

[17] M. Finck i V. Moscon, „Copyright Law on Blockchains: Between New Forms of Rights Administration and Digital Rights Management 2.0", *IIC - Int. Rev. Intellect. Prop. Compet. Law*, t. 50, nr 1, s. 77–108, sty. 2019, doi: 10.1007/s40319-018-00776-8.

[18] „iVoting Everything!", iVoting everything! Dostęp: 24 wrzesień 2023. [Online]. Dostępne na: https://ivoting.pl/

[19] „Home", Medicalchain. Dostęp: 23 wrzesień 2023. [Online]. Dostępne na: https://medicalchain.com/en/

[20] „Propy | Real Estate Transaction Automated". Dostęp: 23 wrzesień 2023. [Online]. Dostępne na: https://propy.com/browse/
[21] „Polkadot: Web3 Interoperability | Decentralized Blockchain", Polkadot Network. Dostęp: 24 wrzesień 2023. [Online]. Dostępne na: https://www.polkadot.network/
[22] „ETH ↔ NEAR Rainbow Bridge", NEAR Protocol. Dostęp: 24 wrzesień 2023. [Online]. Dostępne na: https://pages.near.org/bridge/
[23] „KIR Trwały nośnik", KIR. Dostęp: 14 wrzesień 2023. [Online]. Dostępne na: https://www.kir.pl/nasza-oferta/banki/identyfikacja-i-e-podpis/trwaly-nosnik
[24] „PKO Bank Polski wdrożył trwały nośnik 2.0". Dostęp: 14 wrzesień 2023. [Online]. Dostępne na: https://bank.pl/pko-bank-polski-jako-pierwszy-bank-w-europie-wdrozyl-trwaly-nosnik-2-0/
[25] „WORM. Write Once Read Many", Macierze Hitachi Vantara. Dostęp: 23 wrzesień 2023. [Online]. Dostępne na: https://macierzehitachi.pl/compliance/worm-write-once-read-many/
[26] „Hyperledger Fabric". Dostęp: 15 wrzesień 2023. [Online]. Dostępne na: https://www.hyperledger.org/projects/fabric
[27] „S3DOC Witness bezpieczny trwały nośnik", trwały nośnik WORM. Dostęp: 15 wrzesień 2023. [Online]. Dostępne na: https://s3doc.com/s3doc-witness-bezpieczny-trwaly-nosnik/
[28] „The Unified Enterprise DLT System". Dostęp: 15 wrzesień 2023. [Online]. Dostępne na: https://billongroup.com/
[29] „Benchamarki, kopiowanie od innych, robienie na czuja. Jak Startupy robią UX?", MamStartup. Dostęp: 23 wrzesień 2023. [Online]. Dostępne na: https://mamstartup.pl/benchamarki-kopiowanie-od-innych-robienie-na-czuja-jak-startupy-robia-ux/
[30] „Autenti Blockchain". Dostęp: 23 wrzesień 2023. [Online]. Dostępne na: https://autenti.com/pl/blog/autenti-blockchain
[31] *Rozporządzenie Parlamentu Europejskiego i Rady (UE) nr 910/2014 z dnia 23 lipca 2014 r. w sprawie identyfikacji elektronicznej i usług zaufania w odniesieniu do transakcji elektronicznych na rynku wewnętrznym oraz uchylające dyrektywę 1999/93/WE*, t. 257. 2014. Dostęp: 23 wrzesień 2023. [Online]. Dostępne na: http://data.europa.eu/eli/reg/2014/910/oj/pol
[32] „Atende ChainDoc". Dostęp: 15 wrzesień 2023. [Online]. Dostępne na: https://atende.pl/pl/atende-chaindoc
[33] „Paperless po polsku. DoxyChain chce być jak amerykańsko-białoruski PandaDoc", pb.pl. Dostęp: 22 marzec 2021. [Online]. Dostępne na: //pb.pl/paperless-po-polsku-doxychain-chce-byc-jak-amerykansko-bialoruski-pandadoc-1109905
[34] T. Jangas, „Trwały nośnik. Dlaczego banki wybrały «macierz WORM»?", Tomasz Jangas. Dostęp: 24 wrzesień 2023. [Online]. Dostępne na: https://www.tomaszjangas.com/trwaly-nosnik/
[35] S. Haber i W. S. Stornetta, „How to time-stamp a digital document", *J. Cryptol.*, t. 3, nr 2, s. 99–111, sty. 1991, doi: 10.1007/BF00196791.
[36] R. A. Ziar, S. Irfanullah, W. U. Khan, i A. Salam, „Privacy Preservation for On-Chain Data in the Permission less Blockchain using Symmetric Key Encryption and Smart Contract", *Mehran Univ. Res. J. Eng. Technol.*, t. 40, nr 2, s. 305–313, kwi. 2021, doi: 10.22581/muet1982.2102.05.
[37] J. Nijsse i A. Litchfield, „A Taxonomy of Blockchain Consensus Methods", *Cryptography*, t. 4, nr 4, s. 32, lis. 2020, doi: 10.3390/cryptography4040032.
[38] S. Devidas, S. Rao Y.V., i N. R. Rekha, „A decentralized group signature scheme for privacy protection in a blockchain", 2021, doi: 10.34768/AMCS-2021-0024.

[39] A. Bhattacharjya, X. Zhong, J. Wang, i X. Li, „CoAP—Application Layer Connection-Less Lightweight Protocol for the Internet of Things (IoT) and CoAP-IPSEC Security with DTLS Supporting CoAP", w *Digital Twin Technologies and Smart Cities*, M. Farsi, A. Daneshkhah, A. Hosseinian-Far, i H. Jahankhani, Red., w Internet of Things. , Cham: Springer International Publishing, 2020, s. 151–175. doi: 10.1007/978-3-030-18732-3_9.

[40] A. Bhattacharjya, X. Zhong, J. Wang, i X. Li, „Security Challenges and Concerns of Internet of Things (IoT)", w *Cyber-Physical Systems: Architecture, Security and Application*, S. Guo i D. Zeng, Red., w EAI/Springer Innovations in Communication and Computing. , Cham: Springer International Publishing, 2019, s. 153–185. doi: 10.1007/978-3-319-92564-6_7.

[41] A. Bhattacharjya, X. Zhong, J. Wang, i X. Li, „Secure IoT Structural Design for Smart Homes", w *Smart Cities Cybersecurity and Privacy*, Elsevier, 2019, s. 187–201. doi: 10.1016/B978-0-12-815032-0.00013-5.

[42] A. Bhattacharjya, X. Zhong, J. Wang, i X. Li, „Present Scenarios of IoT Projects with Security Aspects Focused", w *Digital Twin Technologies and Smart Cities*, M. Farsi, A. Daneshkhah, A. Hosseinian-Far, i H. Jahankhani, Red., w Internet of Things. , Cham: Springer International Publishing, 2020, s. 95–122. doi: 10.1007/978-3-030-18732-3_7.

[43] P. Ekparinya, V. Gramoli, i G. Jourjon, „Impact of Man-In-The-Middle Attacks on Ethereum", w *2018 IEEE 37th Symposium on Reliable Distributed Systems (SRDS)*, Salvador, Brazil: IEEE, paź. 2018, s. 11–20. doi: 10.1109/SRDS.2018.00012.

[44] O. M. AlMendah, „A Survey of Blockchain and E-governance applications: Security and Privacy issues". Dostęp: 24 wrzesień 2023. [Online]. Dostępne na: https://www.semanticscholar.org/paper/A-Survey-of-Blockchain-and-E-governance-Security-AlMendah/d9482ceaecd1eb0c8d69e467c25f7f27af3612e6

[45] A. A. Siyal, A. Z. Junejo, M. Zawish, K. Ahmed, A. Khalil, i G. Soursou, „Applications of Blockchain Technology in Medicine and Healthcare: Challenges and Future Perspectives", *Cryptography*, t. 3, nr 1, s. 3, sty. 2019, doi: 10.3390/cryptography3010003.

[46] L. Argento *i in.*, „ID-Service: A Blockchain-Based Platform to Support Digital-Identity-Aware Service Accountability", *Appl. Sci.*, t. 11, nr 1, s. 165, grudz. 2020, doi: 10.3390/app11010165.

[47] N. Jefferies, C. Mitchell, i M. Walker, „A proposed architecture for trusted third party services", w *Cryptography: Policy and Algorithms*, t. 1029, E. Dawson i J. Golić, Red., w Lecture Notes in Computer Science, vol. 1029. , Berlin, Heidelberg: Springer Berlin Heidelberg, 1996, s. 98–104. doi: 10.1007/BFb0032349.

[48] M. Thamizhselvan, R. Raghuraman, S. Gershon Manoj, i P. Victer Paul, „A novel security model for cloud using trusted third party encryption", w *2015 International Conference on Innovations in Information, Embedded and Communication Systems (ICIIECS)*, Coimbatore, India: IEEE, mar. 2015, s. 1–5. doi: 10.1109/ICIIECS.2015.7193199.

[49] A. Kumar, „A cloud-based buyer-seller watermarking protocol (CB-BSWP) using semi-trusted third party for copy deterrence and privacy preserving", *Multimed. Tools Appl.*, t. 81, nr 15, s. 21417–21448, cze. 2022, doi: 10.1007/s11042-022-12550-7.

[50] S. Ullah, X.-Y. Li, i Z. Lan, „A novel trusted third party based signcryption scheme", *Multimed. Tools Appl.*, t. 79, nr 31–32, s. 22749–22769, sie. 2020, doi: 10.1007/s11042-020-09027-w.

[51] R. M. Needham, „Denial of service", w *Proceedings of the 1st ACM conference on Computer and communications security*, w CCS '93. New York, NY, USA: Association for Computing Machinery, Grudzie 1993, s. 151–153. doi: 10.1145/168588.168607.

[52] M. Conti, N. Dragoni, i V. Lesyk, „A Survey of Man In The Middle Attacks", *IEEE Commun. Surv. Tutor.*, t. 18, nr 3, s. 2027–2051, 2016, doi: 10.1109/COMST.2016.2548426.

[53] S. Rizvi, K. Cover, i C. Gates, „A Trusted Third-party (TTP) based Encryption Scheme for Ensuring Data Confidentiality in Cloud Environment", *Procedia Comput. Sci.*, t. 36, s. 381–386, 2014, doi: 10.1016/j.procs.2014.09.009.

[54] M. Abadi i N. Glew, „Certified email with a light on-line trusted third party: design and implementation", w *Proceedings of the 11th international conference on World Wide Web*, Honolulu Hawaii USA: ACM, maj 2002, s. 387–395. doi: 10.1145/511446.511497.

[55] I. Jahan, N. N. Sharmy, S. Jahan, F. A. Ebha, i N. J. Lisa, „Design of a secure sum protocol using trusted third party system for Secure Multi-Party Computations", w *2015 6th International Conference on Information and Communication Systems (ICICS)*, Amman, Jordan: IEEE, kwi. 2015, s. 136–141. doi: 10.1109/IACS.2015.7103216.

[56] „Efficient Collusion-Resisting Secure Sum Protocol". Dostęp: 24 wrzesień 2023. [Online]. Dostępne na: https://ieeexplore.ieee.org/abstract/document/10189911/

[57] D.-H. Jiang, Q.-Z. Hu, X.-Q. Liang, i G.-B. Xu, „A Trusted Third-Party E-Payment Protocol Based on Locally Indistinguishable Orthogonal Product States", *Int. J. Theor. Phys.*, t. 59, nr 5, s. 1442–1450, maj 2020, doi: 10.1007/s10773-020-04413-4.

[58] R.-G. Zhou, M. Huo, W. Hu, i Y. Zhao, „Dynamic Multiparty Quantum Secret Sharing With a Trusted Party Based on Generalized GHZ State", *IEEE Access*, t. 9, s. 22986–22995, 2021, doi: 10.1109/ACCESS.2021.3055943.

[59] N. Panda i M. Supriya, „Efficient data transmission using trusted third party in smart home environments", *EURASIP J. Wirel. Commun. Netw.*, t. 2022, nr 1, s. 118, grudz. 2022, doi: 10.1186/s13638-022-02200-9.

[60] A. Varvitsiotis, D. Polemi, i A. Marsh, „EUROMED-JAVA: Trusted Third Party Services for securing medical Java applets", w *Computer Security — ESORICS 98*, t. 1485, J.-J. Quisquater, Y. Deswarte, C. Meadows, i D. Gollmann, Red., w Lecture Notes in Computer Science, vol. 1485. , Berlin, Heidelberg: Springer Berlin Heidelberg, 1998, s. 209–220. doi: 10.1007/BFb0055865.

[61] V. Sharma i R. Thakur, „LSB modification based Audio Steganography using Trusted Third Party Key Indexing method", w *2015 Third International Conference on Image Information Processing (ICIIP)*, Waknaghat: IEEE, grudz. 2015, s. 403–406. doi: 10.1109/ICIIP.2015.7414805.

[62] Z. A. Hussien, H. Jin, Z. A. Abduljabbar, M. A. Hussain, S. H. Abbdal, i D. Zou, „Scheme for ensuring data security on cloud data storage in a semi-trusted third party auditor", w *2015 4th International Conference on Computer Science and Network Technology (ICCSNT)*, Harbin, China: IEEE, grudz. 2015, s. 1200–1203. doi: 10.1109/ICCSNT.2015.7490948.

[63] A. Maarouf, A. Marzouk, i A. Haqiq, „Towards a Trusted third party based on Multi-agent systems for automatic control of the quality of service contract in the Cloud Computing", w *2015 International Conference on Electrical and Information Technologies (ICEIT)*, Marrakech, Morocco: IEEE, mar. 2015, s. 311–315. doi: 10.1109/EITech.2015.7162972.

[64] M. Aloqaily, B. Kantarci, i H. T. Mouftah, „Trusted Third Party for service management in vehicular clouds", w *2017 13th International Wireless Communications and Mobile Computing Conference (IWCMC)*, Valencia, Spain: IEEE, cze. 2017, s. 928–933. doi: 10.1109/IWCMC.2017.7986410.

[65] D. Jayasinghe, K. Markantonakis, i K. Mayes, „Optimistic Fair-Exchange with Anonymity for Bitcoin Users", w *2014 IEEE 11th International Conference on e-Business Engineering*, Guangzhou, China: IEEE, lis. 2014, s. 44–51. doi: 10.1109/ICEBE.2014.20.

[66] T. Locher, S. Obermeier, i Y. A. Pignolet, „When Can a Distributed Ledger Replace a Trusted Third Party?", w *2018 IEEE International Conference on Internet of Things (iThings) and IEEE Green Computing and Communications (GreenCom) and IEEE Cyber, Physical and Social Computing (CPSCom) and IEEE Smart Data (SmartData)*, Halifax, NS, Canada: IEEE, lip. 2018, s. 1069–1077. doi: 10.1109/Cybermatics_2018.2018.00197.

[67] A. Bhattacharjya, K. Kozdrój, G. Bazydło, i R. Wisniewski, „Trusted and Secure Blockchain-Based Architecture for Internet-of-Medical-Things", *Electronics*, t. 11, nr 16, s. 2560, sie. 2022, doi: 10.3390/electronics11162560.

[68] K. Kozdrój, G. Bazydło, R. Wiśniewski, i J. Starościc, „Trusted and secure e-service based on the durable medium and blockchain technology", *AIP Conf. Proc.*, t. 2611, nr 1, s. 070005, lis. 2022, doi: 10.1063/5.0120190.

[69] G. Bazydło, R. Wiśniewski, i K. Kozdrój, „Trusted and Secure Blockchain-Based Durable Medium Electronic Service", *Cryptography*, t. 6, nr 1, s. 10, luty 2022, doi: 10.3390/cryptography6010010.

[70] „BPMN Specification - Business Process Model and Notation". Dostęp: 24 wrzesień 2023. [Online]. Dostępne na: https://www.bpmn.org/

[71] *Rozporządzenie Parlamentu Europejskiego i Rady (UE) 2016/679 z dnia 27 kwietnia 2016 r. w sprawie ochrony osób fizycznych w związku z przetwarzaniem danych osobowych i w sprawie swobodnego przepływu takich danych oraz uchylenia dyrektywy 95/46/WE (ogólne rozporządzenie o ochronie danych) (Tekst mający znaczenie dla EOG)*, t. 119. 2016. Dostęp: 24 wrzesień 2023. [Online]. Dostępne na: http://data.europa.eu/eli/reg/2016/679/oj/pol

[72] W. Viriyasitavat, L. D. Xu, D. Niyato, Z. Bi, i D. Hoonsopon, „Applications of Blockchain in Business Processes: A Comprehensive Review", *IEEE Access*, t. 10, s. 118900–118925, 2022, doi: 10.1109/ACCESS.2022.3217794.

[73] K. Piech, „LEKSYKON POJĘĆ NA TEMAT TECHNOLOGII BLOCKCHAIN I KRYPTOWALUT".

[74] „Java | Oracle". Dostęp: 24 wrzesień 2023. [Online]. Dostępne na: https://www.java.com/pl/

[75] „Spring Boot", Spring Boot. Dostęp: 24 wrzesień 2023. [Online]. Dostępne na: https://spring.io/projects/spring-boot

[76] C. Guindon, „Jakarta® EE | Cloud Native Enterprise Java | Java EE | the Eclipse Foundation | The Eclipse Foundation", Jakarta® EE: The New Home of Cloud Native Java. Dostęp: 24 wrzesień 2023. [Online]. Dostępne na: https://jakarta.ee/

[77] „Multichain – Content Blockchain". Dostęp: 15 wrzesień 2023. [Online]. Dostępne na: https://content-blockchain.org/research/multichain/

[78] „Consensys Quorum", Consensys. Dostęp: 15 wrzesień 2023. [Online]. Dostępne na: https://consensys.net/quorum/

[79] „Hyperledger Besu documentation". Dostęp: 15 wrzesień 2023. [Online]. Dostępne na: https://besu.hyperledger.org/

[80] Prometheus, „Overview | Prometheus". Dostęp: 24 wrzesień 2023. [Online]. Dostępne na: https://prometheus.io/docs/introduction/overview/

[81] „Chainlens". Web3 Labs, 21 wrzesień 2023. Dostęp: 24 wrzesień 2023. [Online]. Dostępne na: https://github.com/web3labs/chainlens-free

[82] „Ethereum Lite Explorer by Alethio". alethio, 21 sierpień 2023. Dostęp: 24 wrzesień 2023. [Online]. Dostępne na: https://github.com/Alethio/ethereum-lite-explorer

[83] S. Heron, „Advanced Encryption Standard (AES)", *Netw. Secur.*, t. 2009, nr 12, s. 8–12, grudz. 2009, doi: 10.1016/S1353-4858(10)70006-4.

[84] Xin Zhou i Xiaofei Tang, „Research and implementation of RSA algorithm for encryption and decryption", w *Proceedings of 2011 6th International Forum on Strategic*

Technology, Harbin, Heilongjiang, China: IEEE, sie. 2011, s. 1118–1121. doi: 10.1109/IFOST.2011.6021216.

[85] E. Barker, „Recommendation for Key Management Part 1: General", National Institute of Standards and Technology, NIST SP 800-57pt1r4, sty. 2016. doi: 10.6028/NIST.SP.800-57pt1r4.

[86] S. Gueron, S. Johnson, i J. Walker, „SHA-512/256", w *2011 Eighth International Conference on Information Technology: New Generations*, Las Vegas, NV, USA: IEEE, kwi. 2011, s. 354–358. doi: 10.1109/ITNG.2011.69.

[87] S. Debnath, A. Chattopadhyay, i S. Dutta, „Brief review on journey of secured hash algorithms", w *2017 4th International Conference on Opto-Electronics and Applied Optics (Optronix)*, Kolkata: IEEE, lis. 2017, s. 1–5. doi: 10.1109/OPTRONIX.2017.8349971.

[88] T. Gustavsson, „Common Criteria and Open Source: Experiences from the certification of an open source product", *Datenschutz Datensicherheit - DuD*, t. 38, nr 4, s. 226–231, kwi. 2014, doi: 10.1007/s11623-014-0096-7.

[89] N. Sun *i in.*, „Defining Security Requirements With the Common Criteria: Applications, Adoptions, and Challenges", *IEEE Access*, t. 10, s. 44756–44777, 2022, doi: 10.1109/ACCESS.2022.3168716.

[90] D. Hurley-Smith, C. Patsakis, i J. Hernandez-Castro, „On the Unbearable Lightness of FIPS 140–2 Randomness Tests", *IEEE Trans. Inf. Forensics Secur.*, t. 17, s. 3946–3958, 2022, doi: 10.1109/TIFS.2020.2988505.

Spis rysunków

Spis tabel