Pomiary Automatyka Robotyka, ISSN 1427-9126, R. 25, Nr 2/2021, 61–67, DOI: 10.14313/PAR_240/61

Implementacja cyfrowego Paszportu Szczepień COVID-19 bazującego na Blockchain chroniący prywatność

Przemysław Pukocz
AGH Akademia Górniczo-Hutnicza, Katedra Automatyki i Robotyki, al. A. Mickiewicza 30, 30-059 Kraków

Streszczenie: W pracy omówiono propozycje implementacji cyfrowego Paszportu Szczepień COVID-19, bazującego na Blockchain chroniącym prywatność. Od końca zeszłego roku, po rozpoczęciu szczepień przeciw COVID-19, toczy się intensywna dyskusja nad formą wprowadzenia takiego narzędzia oraz konsekwencjami jego wdrożenia. Ma ona miejsce w wielu krajach europejskich. Jednym z elementów tej dyskusji, były kwestie bezpieczeństwa i anonimowości weryfikowanych danych szczepionych osób w sposób masowy, w różnych obszarach funkcjonowania społeczeństwa. Zagadnienia te próbuje rozwiązać proponowany system cyfrowego Paszportu Szczepień. System ten wykorzystuje dwie główne metody: Blockchain i funkcje skrótu, które pozwalają na zachowanie bezpieczeństwa, prywatności, a zarazem anonimowości. Celem poprawienia intuicyjności oraz prostoty jego funkcjonowania, w procesie weryfikacji Paszportów zaproponowano technologię kodów QR. System został zaimplementowany i przetestowany w środowisku chmury obliczeniowej Amazon AWS. Zaproponowano architekturę referencyjną bazująca na Blockchain dla środowiska AWS, dedykowaną dużym i wymagającym rozwiązaniom aplikacyjnym Paszportu Szczepień. Dodatkowo środowisko chmury oferuje dostęp do wielu narzędzi, które wykorzystano w implementacji systemu, podnoszących w znaczny sposób bezpieczeństwo całego rozwiązania.

Słowa kluczowe: Blockchain, chmura obliczeniowa, Paszport Szczepień, COVID-19, Systemy Wspomagania Decyzji, e-health

1. Wprowadzenie

Aktywna walka z pandemią COVID-19 skutkuje wieloma równoległymi inicjatywami w różnych obszarach życia społecznego, gospodarczego, a także zdrowotnego. Zauważalnymi działaniami dla obywateli są: szybka i masowa diagnostyka, izolacja zakażonych osób zgodnie z zaleceniami WHO, wprowadzanie dystansu społecznego [1]. Jednym z najistotniejszych obecnie elementów walki z pandemią są szczepienia wykonywane na masową skalę, które umożliwiają uodpornienie społeczeństwa na COVID-19. Szczepionka może złagodzić ciężki przebieg choroby lub całkowicie zapobiec infekcji w organizmie i w efekcie ograniczyć rozprzestrzenianie się wirusa. Funkcjonowanie osób zaszczepionych w społeczeństwie pozwala na poluzowanie obostrzeń. Trzeba jednak posiadać mechanizmy pozwalające na stwierdzenie, że dana osoba została zaszczepiona i nabyła w ten sposób prawo do przywilejów. Rozwiązaniem od wielu lat stosowanym na świecie jest Międzynarodowa Książeczka Szczepień, zwana „żółtą książeczką". Jako, że jest ona sprawdzona, można ją wykorzystać w obecnej sytuacji pandemicznej w formie Paszportu Szczepień COVID-19. Bardziej uniwersalnym środkiem jest wystawienie elektronicznego Paszportu Szczepień – certyfikatu, który potwierdzałby stopień podatności osoby na chorobę COVID-19. Wdrożenie sprawnej metody weryfikacji szczepienia pozwoliłoby zmniejszyć obostrzenia (często potocznie nazywane przywilejami), a przez to zmniejszyć uciążliwość ograniczeń. Przedłużanie obostrzeń w perspektywie średnio- lub długoterminowej, niesie z sobą poważne konsekwencje społeczno-ekonomiczne.

Paszport cyfrowy musi legitymizować się następującymi cechami: wiarygodność, akceptowalność i weryfikowalność w pełnym spektrum aktywności społecznej i gospodarczej. Dodatkowo dokument ten musi być również odporny na przypadki fałszowania oraz posługiwania się nim przez osoby nieupoważnione. Obecnie w przestrzeni medialnej pojawia się wiele wiadomości o procederze fałszowania zaświadczeń na obecność wirusa COVID-19. Z podobną sytuacją można się będzie spotkać w stosunku do Paszportu Szczepień. Wprowadzenie cyfrowego mechanizmu weryfikacji szczepienia powinno zapobiegać tym działaniom. Wskazany mechanizm weryfikacji

Autor korespondujący:
Przemysław Pukocz, pukocz@agh.edu.pl

Artykuł recenzowany
nadesłany 17.03.2021 r., przyjęty do druku 31.05.2021 r.

powinien być rozpatrywany również w kategoriach Systemów Wspomagania Decyzji (ang. Decision Support System).

Zaszczepienie społeczeństwa stanowi główny cel zakończenia pandemii COVID-19. Proces ten jest realizowany zgodnie z priorytetami wytyczonymi dla identyfikowanych grup przez Ministerstwo Zdrowia. Podział na grupy przeprowadzono ze względu na: zawód, stopień zaangażowania do walki z pandemią, wiek, stan zdrowia itp. Obecnie w Polsce jest kilka milionów zaszczepionych, nie mówiąc już o osobach, które przeszły zakażenie w sposób objawowy i bezobjawowy. Każda z tych grup może być poddana certyfikacji odporności. Najprostszą metoda weryfikacji coraz większej grupy zaszczepionych jest właśnie wydanie im cyfrowego Paszportu Szczepień i wprowadzenie go w sposób systemowy, np. jako jeden z elementów Cyfryzacji Państwa.

Samo posługiwanie się Paszportem Szczepień stwarza wiele obiekcji i niedomówień. Obecnie wiele osób krytykuje tę formę prewencji przeciwko zachorowaniu na COVID-19. Z taką mocną reakcją można się było spotkać w Wielkiej Brytanii. Warto w tym względzie zmienić optykę i spojrzeć na to zagadnienie z innej strony – podróży służbowych i prywatnych. Przed niektórymi wyjazdami musimy się wyposażyć w Międzynarodową Książeczkę Szczepień, zwaną potocznie „żółtą książeczką". Jej posiadanie – wraz z udokumentowanymi szczepieniami – jest wymagane przy przekraczaniu granic niektórych krajów. Odnotowywane są w niej szczepienia zalecane oraz obowiązkowe. Do szczepień wymaganych należy żółta febra, która jest poważną chorobą wirusową występującą w kilku rejonach świata: Afryce i Ameryce Południowej. Państwa w tym regionie przed wjazdem nakazują dokonanie szczepień, by zapobiegać niekontrolowanemu rozprzestrzenianiu się wirusa, co mogłoby doprowadzić do epidemii. W tym przypadku jest jednak duża akceptowalność tego narzędzia, który funkcjonuje pod nazwą International Certificate of Vaccination or Prophylaxis [2].

Sposób szczepienia na COVID-19 jest trochę odmienny od innych. Dziś mamy mnogość szczepionek wprowadzanych na rynki globalnie, lecz ich podaż jest znikoma w stosunku do popytu. Każdy środek ma różne parametry, które wpływają na jej cechy użytkowe. Warto zwrócić uwagę, że ocenie klinicznej i przedklinicznej na koniec 2020 r. poddano odpowiednio 48 i 164 szczepionki [3]. Z kolei liczba dopuszczonych szczepionek może się szybko zmieniać, również zmienne są ich parametry ochrony przed wirusem. Wdrożenie na masową skalę skutecznych i bezpiecznych preparatów rozpoczęło się w grudniu 2020 r. Od tego momentu zaczęły się szczepienia zatwierdzonymi farmaceutykami. Obecnie czyni się starania, aby szybko szczepić jak najwięcej osób, lecz w dłuższej perspektywie będzie się liczyć skuteczność szczepionek. Wdrożenie metody nadzoru i weryfikacji szczepienia wydaje się kluczowe dla życia społecznego i gospodarczego. Działanie to pozwoli na upragnione wyjście z pandemicznego kryzysu.

Mając na uwadze głosy wielu gremiów doradczych i dyskusje publiczną należy stwierdzić, że konieczne jest pośpieszne wdrożenie tego narzędzia. Możliwe jest nawet rozszerzenie zakresu jego stosowania na obszar symbiotycznej weryfikowalności certyfikatów testów na COVID-19 oraz immunologicznych. Wskazana informacja funkcjonuje w systemie odpowiednich organów. Bez wprowadzenia jej wersji cyfrowej, staje się mało użyteczna w życiu społecznym i gospodarczym. Ostatnio zdarzają się częste sytuacje podrabiana certyfikatów badań, a nawet szczepionek mRNA na COVID-19. Wobec tego faktu konieczne jest przedsięwzięcie odpowiednich kroków zabezpieczających. Podobna dyskusja trwa od niedawna również w Europie, a jej celem powinno być zaimplementowanie wspólnego dokumentu.

W tym miejscu należałoby zdefiniować problem badawczy. Jest nim pytanie, jak stworzyć cyfrowy Paszport Szczepień odporny na nieuprawnione zmiany, bezpieczny oraz zachowujący anonimowość? Rozwiązaniem tego dylematu jest stworzenie platformy informatycznej, pozwalającej na wdrożenie cyfrowego dokumentu zwanego Paszportem Szczepień lub Paszportem Zdrowia. W tym artykule zostanie przedstawiona architektura praktyczna implementacji proponowanego rozwiązania w środowisku chmury obliczeniowej Amazon AWS, bazująca na Blockchain. Udostępnione zostaną dodatkowe metody podnoszące bezpieczeństwo i anonimowość przy weryfikacji danych. Odpowiednio zaprojektowany protokół wymiany informacji może się stać powszechnym standardem weryfikacji szczepień na COVID-19 z wykorzystaniem Paszportu Szczepień.

Struktura artykułu została podzielona na siedem sekcji. Dwie pierwsze sekcje stanowią wprowadzenie w zagadnienie problemowe oraz przegląd literatury w obszarach problemowych związanymi z Paszportem Szczepień. Kolejne trzy sekcje stanowią rozwiązanie zagadnienia problemowego dotyczące metod implementacji cyfrowego Paszportu Szczepień. W rozdziale trzecim zaprezentowano ogólną architekturę rozwiązania Paszportu Szczepień bazującą na technologii Blockchain. W sekcji czwartej wskazano reguły decyzyjne weryfikacji Paszportów Szczepień chroniących prywatność. W kolejnym rozdziale przedstawiono sposób implementacji zaprojektowanego rozwiązania z wykorzystaniem chmury obliczeniowej. W podsumowaniu zawarto wnioski wynikające z realizacji prezentowanego rozwiązania.

2. Stan wiedzy

Podstawą proponowanego cyfrowego Paszportu Szczepień jest technologia Blockchain. W niej zostaną zapisane rekordy z danymi, np. rekord wykonanego szczepienia. Blockchain nazywany potocznie łańcuchem bloków, to cyfrowy, asymetryczny łańcuch oparty na szyfrowaniu, który jest niezmienny i zdecentralizowany. Koncepcja ta została po raz pierwszy zaprezentowana w 2008 r. przez Satoshi Nakamoto do przechowywania i przesyłania informacji na temat transakcji zawartych w Internecie, w kryptowalucie zwanej bitcoinem. Technologia ta była przewidziana do konstrukcji dużych, zdecentralizowanych sieci peer-to-peer, współdzielących między użytkownikami księgę transakcji. Pierwszy poziom bezpieczeństwa gwarantują algorytmy kryptografii matematycznej oraz zasada TSS (ang. *Time-Stamping Service*). Drugi poziom bezpieczeństwa gwarantuje architektura oparta na sieciach peer-to-peer, gdzie każdy użytkownik przetrzymuje kopie publicznej księgi transakcji. Co ciekawe, w rozwiązaniu tym nie jest konieczne utrzymywanie centralnej infrastruktury, z uwagi na swoisty charakter sieci peer-to-peer. Sama koncepcja sieci jest prozaiczna. Informacje są przechowywane w następujących po sobie blokach danych. Blok może zawierać dane o określonej liczbie transakcji. Gdy zostanie już zapełniony, to tworzony jest kolejny, następujący po nim. Tak powstaje łańcuch bloków – Blockchain. Każda ingerencja w łańcuch jest łatwo wykrywana przez analizę błędów w strukturze.

Technologia Blockchain sprawdziła się z powodzeniem w wielu obszarach: krytptowaluty, łańcuchy dostaw, usługi finansowe, rynek energii itd. W tym miejscu można wspomnieć o przykładach jej użytkowania przez takie firmy, jak: Sony Music, BMW Group i wiele innych. Jednak dla tego artykułu właściwym obszarem tematycznym jest pandemia wirusa COVID-19 i do tych ram zawęźmy naszą analizę. W literaturze [4] wskazuje się, że Blockchain staje się cennym narzędziem do walki z pandemią. Można wyróżnić kilka podstawowych obszarów aktywności w tej dziedzinie: śledzenie kontaktów, administracja ubezpieczeniami na wypadek klęski żywiołowej i pandemii, współdzielenie informacji o pacjencie, procedury imigracyjne i emigracyjne, zarządzanie łańcuchem dostaw, zautomatyzowane dostawy bezdotykowe i nadzór nad nimi, edukacja online i certyfikaty dydaktyczne, zarządzanie produk-

cją, e-Government, rolnictwo, dystrybucja żywności. Oznacza to, że stosujemy to rozwiązanie wszędzie tam, gdzie chcemy mieć pewność, co do bezpieczeństwa i niezmienności danych.

Istotne z punktu widzenia obecnych potrzeb walki z COVID-19 jest wykorzystanie technologii Blockchain w następujących obszarach:

- śledzenie kontaktów: SARS-CoV-2 ma średni okres od inkubacji do wystąpienia objawów około 5 dni. Dodatkowo szacuje się, że wysoki odsetek stanowią przypadki bezobjawowe. W związku z tym ważna jest skuteczna i szybka identyfikacja wszystkich interakcji społecznych, które miały miejsce w okresie inkubacji. Takie działanie wpływa bezpośrednio na ograniczenie rozprzestrzeniania się COVID-19. Najlepszą metodą realizacji tego zadania jest śledzenie interakcji społecznych z wykorzystaniem smartfonów osób znajdujących się w bliskiej odległości od zakażonego przez określony czas (np. technologii Bluetooth Low Energy (BLE)). Blockchain i Smart Contract, w tym przypadku, są realną alternatywą dla obaw o kwestie bezpieczeństwa i prywatności danych wszystkich stron działania systemu. Można wyróżnić w tym obszarze następujące przykłady [4–6].
- pomoc finansowa państwa w pandemii, datki charytatywne. Wprowadzane kolejno lockdown'y i duże ograniczenia w sferze społecznej oraz gospodarczej, mają ogromny wpływ na funkcjonowanie różnych podmiotów na całym świecie. Rządy i instytucje finansowe są odpowiedzialne za pomoc przedsiębiorstwom w tym krytycznym czasie. Użytkowane są takie instrumenty, jak: pożyczki, tarcze finansowe i inne instrumenty pomocowe. Proceduralnie fizyczny obrót dokumentów jest spowolniony z uwagi na przepisy sanitarne oraz na pracochłonność przetwarzania. Blockchain z technologią Smart Contracts może być używany do upraszczania procedur składania wniosków o różne dotacje i granty, przy zachowaniu odpowiednich standardów bezpieczeństwa. Można tu wyróżnić następujący przykład [7].
- PHR/MHR (Personal Health Record/Medical Health Record). Dla przebiegu samego procesu leczenia choroby COVID-19, sprawne dzielenie się danymi ma ogromne znaczenie. Współdzielenie takich elementów, jak dane badań, procesu leczenia oraz w efekcie samych informacji o szczepieniu, może odgrywać podstawową rolę w walce z chorobą. Dodatkowo mechanizm wymiany danych musi być zgodny z krajowymi i międzynarodowymi przepisami dotyczącymi udostępniania personaliów pacjentów. W tej koncepcji użytkowania Blockchain, pacjenci i szpitale mogą mieć większą kontrolę nad własnymi danymi medycznymi przez eliminację scentralizowanych baz danych różnych instytucji. Wdrożenie tej technologii może umożliwić udostępnianie informacji w czasie rzeczywistym, zgodnie z intencją pacjenta oraz wyeliminować problem fałszowania danych lub ich nienadzorowanej zmiany. Można wyróżnić w tym obszarze następujące przykłady: [8–11].
- kontrola graniczna i przemieszczanie się ludności. Inspekcja ruchu granicznego i transportowego jest kluczowym elementem zapanowania nad rozprzestrzenianiem się wirusa COVID-19 tym bardziej, że pojawiają się nowe, groźniejsze mutacje wirusa w innych krajach. Migracja nowych odmian powoduje powstawanie nieznanych jeszcze form ryzyka, a kontrola ruchu międzynarodowego będzie miała teraz, jak i w przyszłości, duże znaczenie dla prewencji. Blockchain służy jako platforma integracyjna wymiany informacji transgranicznej przy obsłudze różnych procedur granicznych, w tym kluczowa jest kontrola stanu zdrowia podróżujących. Technologia ta może wspomóc tworzenie bezpiecznej, zdecentralizowanej i współdzielonej platformy transgranicznej. W tym kontekście da się wyróżnić następujące przykłady [12–15].
- zarządzanie łańcuchami dostaw – w dobie pandemii koronowirusa występują zakłócenia w tradycyjnym łańcuchu dostaw towarów. Produkcja przemysłowa powoli wraca do normy pod warunkiem, że nie wystąpią kolejne ostre lockdown'y. Takie ograniczenia mają swoje poważne konsekwencje w zachwianiu praw podaży i popytu. Byliśmy już świadkami jak panika uczestników rynków spowodowała wzrost popytu na pewną grupę artykułów przemysłowych, sprzętu medycznego i produkty farmaceutyczne itp. Klasyczne metody procesowe łańcucha dostaw w krytycznych momentach zagrożenia epidemiologicznego mają duże trudności z utrzymaniem stabilności. Technologia Blockchain może odegrać kluczową rolę w budowaniu bardziej odpornego łańcucha dostaw na te negatywne przyczyny. Może łączyć (także anonimowo) ze sobą wszystkie zainteresowane strony, tworząc zaufane środowisko wymiany handlowej bez zbędnych pośredników. W tym kontekście warto wspomnieć o technologii Smart Contract. Da się tu wyróżnić następujące przykłady [16, 17].
- e-government realizacji procedur administracyjnych lub usług publicznych na rzecz obywateli i innych podmiotów z wykorzystaniem technologii ICT. E-Government wspiera digitalizację wszystkich lub niektórych usług oraz pozwala na funkcjonowanie tych usług w formie hybrydowej. Blockchain może zapewnić bezpieczeństwo poprzez zwiększenie integralności, poufności i niezmienności danych wymienianych pomiędzy podmiotami, zmniejszenie opóźnienia przetwarzania i obniżanie kosztów tych operacji. System operujący na podstawie takiego mechanizmu będzie potrafił automatycznie wykrywać możliwe błędy i próby fałszowania operacji wymiany informacji. W tym obszarze można następujące przykłady [12, 18].

Dokonując przeglądu tych podstawowych aspektów implementacji technologii Blockchain, zauważymy jej duży potencjał w walce z COVID-19. Popularność tego rozwiązania cały czas rośnie, co jest spowodowane dynamicznym rozwojem wspomnianej technologii w obszarze implementacji biznesowej. Mowa tu o sieciach Blockchain: Ethereum (start: lipiec 2015 r. https://ethereum.org) oraz Hyperledger Fabric (start: grudzień 2015 r., https://hyperledger.org), Skulchain (2014), Neo (2014). Jednak prawdziwym akceleratorem jej użytkowania są różni operatorzy chmury obliczeniowej, którzy oferują wsparcie merytoryczne i metodyczne. Tu da się wyróżnić takie podmioty, jak: Amazon, IBM, Microsoft. Porównanie kluczowych parametrów Blockchain dla wyszczególnionych powyżej głównych obszarów implementacyjnych dla walki z COVID-19 zawarto w Tab. 1.

Problem tworzenia Paszportu Szczepień należy rozpatrywać w kategorii systemów ukierunkowanych na współdzielenie informacji o pacjencie, z wykorzystaniem elektronicznego rekordu medycznego – EHR (ang. Electronic Health Record). Pojęcie samego rekordu można zdefiniować jako usystematyzowany zbiór informacji zdrowotnych przechowywanych w formacie cyfrowym [20]. Takim rekordem informacji medycznej będzie też informacja o szczepieniu, zawarta w Paszporcie Szczepień. Tutaj sugeruje się jednak, by Paszport Szczepień miał jak najprostszą formę pozwalającą na zachowanie prywatności i bezpieczeństwa danych określonego pacjenta.

W najbliższym czasie Paszporty Szczepień staną się stałym elementem procesu przemieszczania się w kraju i za granicą [21]. Obecnie wszystkie państwa biorą udział w wyścigu z czasem w obszarze szczepień przeciwko koronawirusowi COVID-19. Szybsze zaszczepienie populacji spowoduje powrót społeczeństwa i gospodarki do „normalnego" funkcjonowania. Równolegle trwa debata na temat, czy zaszczepione osoby powinny mieć pewne przywileje? Pojawia się wiele analiz i głosów ekspertów popierających ten pomysł. Jednak by korzystać

Tab. 1. Porównanie implementacji Blockchain w różnych obszarach stosowania, opracowano na podstawie [19]
Tab. 1. Comparison of Blockchain implementations in different areas of application, developed on the basis of [19]

Dziedzina aplikacji	Typ Blockchain	Typ konsensusu	Akceptowalne opóźnienie/maksymalne	Oczekiwana liczba operacji	Koszt transakcji
śledzenie kontaktów	Public	PoW/PoS	do godziny	200–2000 transakcji na dzień	niski
	Consoritum	Majority voting/DBFT			brak kosztu
pomoc finansowa państwa w pandemii, datki charytatywne	Consortium	PoW/PoS	do kilku dni	10–150 000 transakcji na dzień	średni
	Private	BFT/RAFT			brak kosztu
PHR/MHR	Consoritum	PoW/PoS	do kilku sekund	100–100 000 transakcji na minutę	niski
	Private	Proof of Interoparability CBFT			brak kosztu
międzynarodowy ruch / kontrola graniczna	Consoritum	PoW/PoS	do kilku sekund	10000–1 mln transakcji dziennie na granicę	niski
	Private	BFT			brak kosztu
zarządzanie łańcuchem dostaw	Consoritum	PoW/PoS	do kilku minut	100–10 000 na dzień na system dostaw	niski
	Private	BFT			brak kosztu
e-Government	Consortium	PoW/PoS/PoA	do kilku dni	100–10 000 dziennie na urząd	średni
	Private	BFT			brak kosztu

z przywilejów osoby zaszczepionej, muszą udowodnić odporność na chorobę. Konieczne jest więc uwiarygodnienie, że otrzymały odpowiednie szczepienie lub przeszły już tę chorobę. Posiadają wtedy przeciwciała. Realnym rozwiązaniem tego problemu są formalne zaświadczenia o szczepieniu lub odchorowaniu, czyli wprowadzenie certyfikatów immunologicznych lub skorzystanie z cyfrowego dokumentu, jakim jest Paszportów Szczepień. Sceptycy twierdzą, że takie radykalne rozwiązanie może spowodować podziały i polaryzację społeczeństwa. Jednak pragmatyzm i bezpieczeństwo powinno wziąć górę nad wadami Paszportów Szczepień. Warto zwrócić uwagę, że taką „żółtą książeczką" posługujemy się w podróżach do kilku krajów. Używamy ten dokument, by legitymować się wiarygodnym certyfikatem szczepienia przeciw chorobom zakaźnym. Paszport ten jest również międzynarodowym standardem certyfikowania otrzymania szczepień przeciwko cholerze, żółtej febrze, tyfusowi czy ospie. Czemu nie skorzystać z tych dobrych wieloletnich doświadczeń przy szczepieniach z COVID-19? Możliwość podróżowania bez barier to konieczność legitymowania się odpowiednim oświadczeniem, certyfikatem lub innym dokumentem. Wiele krajów zaczyna wymagać tego rodzaju zaświadczeń. Pojawiają się głosy, że wypracowanie takich standardów może być konieczne również w przypadku poruszania się po ulicach miast.

Szczepionki różnych producentów mają niejednorodne parametry, np. okres ochrony danej osoby przed wirusem, skuteczność, stopień zabezpieczenia przed transmisją i przed ciężki przebiegiem choroby itd. Te elementy powinny być uwzględnione w Paszporcie Szczepień. Z drugiej jednak strony, bazując na materiałach rejestracyjnych kilku szczepionek można jasno stwierdzić, że szczepienia znacząco zmniejszały rozprzestrzenianie się koronawirusa. Potwierdzają ten fakt doniesienia płynące z całego świata, w tym z Izraela. Oznacza to, że będzie rosła presja na poluzowanie obostrzeń, gdy tylko odpowiednia część populacji się zaszczepi. Pozwólmy osobom zaszczepionym powrócić do dawnego stylu życia [22]. Bez paszportów immunologicznych i szczepień niektóre sektory gospodarki i branże mogą się znaleźć w trudnej sytuacji. Wiele krajów szybko rozpoczęło pracę nad wdrożeniem Paszportów Szczepień, jednak opracowanie konkretnych rozwiązań i ich wdrożenie zapoczątkowało jedynie kilka z nich. Przegląd działań poszczególnych krajów i proponowanych przez nich rozwiązań zawarto w Tab. 2.

Cyfrowe paszporty szczepień są stosunkowo nowym obszarem badań. Dokonując przeglądu literatury dochodzimy do wniosków, że opublikowano kilka pozycji prezentujących takie rozwiązania. W bazie Scopus, w 2020 r. można było wyszukać 26 pozycji w zakresie nauk technicznych i humanistycznych. Zawężając zakres tematyczny do technologii Blockchain, da się zidentyfikować dosłownie kilka publikacji. Zostały one zamieszczone w Tab. 3.

Kolejną kluczową technologią dla implementacji Paszportu Szczepień jest chmura obliczeniowa (ang. *cloud computing*), gdzie można posługiwać się zamiennie potocznym terminem „chmura". Chmurę obliczeniową da się określić jako globalną sieć infrastruktury informatycznej udostępnionej przez Internet, dostarczanej przez jednego dostawcę, tworzącą jeden ekosystem. Chmura dostarcza takich usług, jak: sieci, serwerów wraz z oprogramowaniem, magazyn baz danych, sieci, oprogramowania i innych usług (analitycznych i Machine Learning) z wykorzystaniem uniwersalnego medium, jakim jest Internet [28]. Na tej podstawie użytkownik może budować swoje własne rozwiązania.

Chmura stanowi istotny klucz do ewoluujących aplikacyjnie rozwiązań systemowych obecnie i w przyszłości. Technologia ta obejmuje pełen stos technologiczny pozwalający na zbudowanie spójnego rozwiązania w różnych modelach świadczenia usług: PaaS (ang. *Platform-as-a-Service*), IaaS (ang. *Infrastructure as a Service*), SaaS (ang. *Software as a service*) z pełną integracją w zakresie transformacji cyfrowej, np. automatycznego skalowania całego środowiska. W tym kontekście najprościej to ujmując, chmura może dostarczyć usług obliczeniowych,

Tab. 2. Postęp prac nad implementacja Paszportu Szczepień w różnych krajach
Tab. 2. Progress on the implementation of the Vaccination Passport in different countries

Kraj	Postęp	Obszar stosowania	Data uruchomienia	Rodzaj paszportu	Blockchain
Cypr	Planowane	turyści	brak danych	brak danych	nie
Czechy	Planowane	turyści i obywatele		papierowa	nie
Holandia	Implementowane	turyści i obywatele	28 lutego 2021 r.	cyfrowy/aplikacja smartfone	nie
Estonia	Implementowane	turyści i obywatele	brak danych	cyfrowy/karta smart yellow card	nie
Grecja	Planowane	turyści	brak danych	brak danych	brak danych
Węgry	Planowane	turyści	28 lutego 2021 r.	brak danych	brak danych
Islandia	Planowane	turyści	do maja 2021 r.	brak danych	brak danych
Włochy	Planowane	turyści	brak danych	cyfrowy	brak danych
Polska	Planowane	turyści i obywatele	brak danych	cyfrowy/kod QR, konto pacjenta	brak danych
Portugalia	Planowane	turyści	brak danych	brak danych	brak danych
Słowacja	Planowane	brak danych	brak danych	brak danych	brak danych
Hiszpania	Planowane/ implementacja testowa	turyści i obywatele	brak danych	cyfrowy/karta	tak – firma Vottun
Szwecja	Planowane	turyści i obywatele	do czerwca 2021 r.	cyfrowy	brak danych
Wielka Brytania	Nieplanowane	–	–	–	–

Tab. 3. Przegląd rozwiązań w literaturze w zakresie implementacji Paszportów Szczepień bazujący na Blockchain
Tab. 3. Overview of solutions in the literature on the implementation of vaccination passports based on Blockchain

Lp.	Pozycja	Tytuł	Rezultat	Blockchain	Metoda
1	[23]	A Blockchain Based Technique for Storing Vaccination Records	Propozycja rozwiązania	Ethereum	Rozwiązanie wykorzystuje sieć Blockchain Ethereum oraz Smarts Contracts. Do przechowywania dokumentów związanych ze szczepieniami wykorzystywany jest system (IPFS) – zcentralizowany system plikowy. System rozproszony z dostępnymi interfejsami.
2	[24]	Blockchain-Based Solution for COVID-19 Digital Medical Passports and Immunity Certificates	Propozycja rozwiązania	Ethereum	Rozwiązanie wykorzystuje sieć Blockchain Ethereum oraz Smarts Contracts. Do przechowywania dokumentów związanych ze szczepieniami wykorzystywany jest system (IPFS) – zcentralizowany system plikowy. System rozproszony z dostępnymi interfejsami.
3	[25]	COVID-19 Antibody Test/ Vaccination Certification: There's an App for That	Propozycja rozwiązania	Ethereum	Aplikacja na telefon, architektura serwerowa zdecentralizowana bazująca na PKI, możliwość zmiany zakresu przechowywania personalnych danych przez użytkownika. Infrastruktura wykorzystuje technologie W3C Verifiable Credentials, Blockchain Ethereum, wykorzystanie kodu QR.
4	[26]	Framework for a DLT Based COVID-19 Passport	Propozycja rozwiązania	brak informacji	Przechowywanie certyfikatów szczepień w sieci Blockchain z wykorzystaniem metody biometrycznej do generowania hash (biometric crypto-graphic hashing techniques), który służy do identyfikacji użytkownika.
5	[27]	Sharing pandemic vaccination certificates through Blockchain: case study and performance evaluation	Propozycja rozwiązania	Hyperledger Fabric	Rozwiązanie wykorzystuje Blockchain Hyperledger Fabric, dodatkowo wykorzystywane są technologie Self-Sovereign Identity (SSI) oraz Verifiable Credentials (VC) do kontroli nad identyfikacją użytkownika i usług.

magazynowania plików, baz danych, sieci, dodatkowego oprogramowania z wykorzystaniem Internetu. Na tej podstawie użytkownik buduje swoje rozwiązanie korzystając z elastyczności zasobów, niezawodności i ekonomii skali. Usługi w chmurze są odpłatne, lecz opłaty są generowane wyłącznie za używanie konkretnych usług w chmurze, a nie za sam dostęp do infrastruktury – model Pay As You Go. W przypadku świadomego użytkowania platformy chmurowej, istnieje możliwość znacznego obniżenia kosztów wdrożonej platformy informatycznej oraz dostęp Just-In-Time do skalowalnej infrastruktury lub usług. Budowanie rozwiązań informatycznych staje się prostsze, ma to szczególne znaczenie, gdy projektuje się duże rozwiązania.

Pierwszy raz termin „Cloud Computing" pojawił się w wewnętrznych dokumentach firmy Compaq Computer [29] w 1996 r., w odniesieniu do przyszłościowej strategii budowy rozwiązań w obszarze Internetu dla trzech klas klientów biznesowych obecnych na rynku. Zgodnie z tą strategią, oprogramowanie biznesowe zostałoby przeniesione do sieci internetowej, spopularyzowanoby współdzielone usługi i infrastrukturę teleinformatyczną. Po 2000 r. znacznym czynnikiem kosztowym dla firm technologicznych było utrzymywanie infrastruktury, którą wykorzystywano w niewielkim stopniu, np. zasoby obliczeniowe i przestrzeń dyskową. Oczywiście technologie, które pozwoliły na wdrożenie chmury, zostały opracowane wcześniej. W tym kontekście warto wspomnieć o takich elementach przełomowych, jak: projekt MAC w DARPA (1963), ARPANET (Advanced Research Projects Agency Network) (1969) czy wirtualizacja lub odpłatne oferowanie usługi "virtual" private networks w latach 1990 [30]. Formalnie pierwszym komercyjnym dostawcą usług chmury był Amazon AWS. Amazon po wprowadzeniu własnych usług sprzedażowych Amazon Web Services w Internecie w 2002 r. zauważył, że jego infrastruktura jest niewykorzystywana w odpowiednim stopniu. Chcąc poprawić tę sytuację, dokonał optymalizacji własnych zasobów w 2006 r. i zaoferował odpłatny dostęp do własnej infrastruktury w modelu Cloud Computing Infrastructure Model. Później, w podobnym modelu, zaoferowały swoje usługi komercyjnie kolejne podmioty: Google – Google Cloud, Microsoft – Microsoft Azure, IBM – IBM Cloud, Oracle – Oracle Cloud oraz wiele innych.

Wykorzystanie chmury obliczeniowej jest popularnym rozwiązaniem w wielu obszarach prywatnych i publicznych, gdzie utrzymanie odpowiedniej architektury przez dany podmiot byłby drogi czy wręcz nieopłacalny. W sektorze publicznym, dla rozwiązań medycznych, można wyróżnić wiele implementacji zakończonych sukcesem, miedzy innymi [31, 32]. Biorąc pod uwagę garść zalet modelu chmurowego, należy zdawać sobie sprawę z pewnych konsekwencji. Muszą one być świadomie projektowane, a w efekcie wdrażane, ponieważ nieumiejętne implementowanie aplikacji w tym modelu spowoduje nadmierne generowanie kosztów.

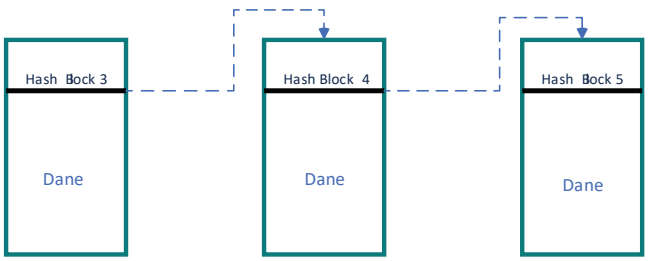
Chmurę da się podzielić na dwa główne typy: publiczne i prywatne. Publiczną definiuje się jako usługi oferowane przez dostawców zewnętrznych. Aplikacje te są dostępne dla każdego, kto chce z danej rzeczy korzystać zgodnie ze specyfikacją. Chmura prywatna zapewnia dostęp do usług obliczeniowych za pośrednictwem Internetu lub prywatnej sieci wewnętrznej wyłącznie wybranym użytkownikom. W tym modelu kładzie się nacisk na bezpieczeństwo i tworzenie systemów w kontrolowanym, bezpiecznym środowisku. Współcześnie wprowadzono dodatkowe pojęcie chmury hybrydowej, definiowanej jako typ przetwarzania w chmurze, który łączy lokalną infrastrukturę klienta lub chmurę prywatną z chmurą publiczną. Chmury hybrydowe umożliwiają przenoszenie danych i aplikacji między tymi dwoma środowiskami: prywatnym i publicznym. Naturalnym elementem ewolucji wzorca chmury jest rozwiązanie typu Multicloud. Pojęcie Multicloud odnosi się do możliwości korzystania z różnych dostawców chmury w formie jednego, heterogenicznego ekosystemu. Zasoby takie, jak oprogramowanie, aplikacje, infrastruktura są rozdzielone wg określonego klucza na kilka środowisk chmurowych, co pozwala na uniezależnienie się od jednego dostawcy rozwiązania [33].

Najważniejsze korzyści z używania chmury obliczeniowej to: optymalizacja kosztowa, szybkość, skala globalna, wydajność, skalowalność, niezawodność oraz bezpieczeństwo. Dodatkowo wielu dostawców rozwiązań chmurowych ma wsparcie dla technologii Blockchain, np. Amazon AWS, Microsoft Azure i inni. Mając powyższe na uwadze, konstrukcja aplikacji Paszportu Szczepień wymaga skalowalnych i dojrzałych rozwiązań ICT, gwarantujących niezawodność i bezpieczeństwo. Rozwiązaniem realizującym te przesłanki jest chmura obliczeniowa.

W kolejnych sekcjach zostanie zaprezentowane rozwiązania zagadnienia problemowego realizacji Paszportu Szczepień bazującego na technologii Blockchain, który został zaimplementowany z wykorzystaniem chmury obliczeniowej.

3. Koncepcja Paszportu Szczepień bazującego na technologii Blockchain

W poniższej sekcji zostanie przedstawione rozstrzygnięcie problemu implementacji Paszportu Szczepień. Rozwiązanie to wspomaga w sposób instytucjonalny pracodawców, instytucje rządowe i społeczne oraz podmioty gospodarcze w obszarze weryfikacji szczepień COVID-19. Projektowany system jest przewidziany do przechowywania certyfikatów szczepień, lecz po kilku modyfikacjach może służyć także do gromadzenia innych istotnych danych epidemiologicznych, np. testów COVID-19, statusu ozdrowieńca itd. Podstawową technologią zapisu rekordów Paszportu Szczepień powinien być Blockchain jako mechanizm bezpieczny, zapewniający niezmienność magazynowanych danych. W poprzedniej sekcji wskazano zalety i wady technologii Blockchain, dlatego nie będą tu powielane.



Rys. 1. Ogólna konstrukcja Blockchain
Fig. 1. General Blockchain structure

Blockchain jest technologią odporną na próby fałszowania i modyfikacji danych. Nie można zmieniać informacji w łańcuchu, a jeśli już pojawiła się taka potrzeba, to należy dodać nowy blok do łańcucha. Warto mieć na uwadze, że nie zostanie on już z niego wymazany. Takie działanie wynika z konstrukcji Blockchain. Ogólną budowę Blockchain wskazano na rys. 1. Odnosząc się do źródłowego problemu Paszportu, każde szczepienie pacjenta stanowi osobny rekord z danymi. Zawiera on najważniejsze informacje o szczepionce i procesie szczepienia. Notyfikacje te zapisujemy w rekordzie danych, który następnie umieszczamy w łańcuchu. Dla każdego bloku generowana jest funkcja skrótu – hash. Każdy kolejny zawiera wartość hash z poprzedniego bloku. Pojedyncza zmiana w przypadku modyfikacji rekordu danych będzie generowała inną wartość hash, zatem wartość zapisana w kolejnym bloku będzie błędna. Jeśli są one rozbieżne, wówczas oznacza to, że dokonano procederu fałszowania/zmiany danych. Koncepcja konstrukcji Blockchain pozwala na podniesienie bezpieczeństwa przechowywanych informacji.

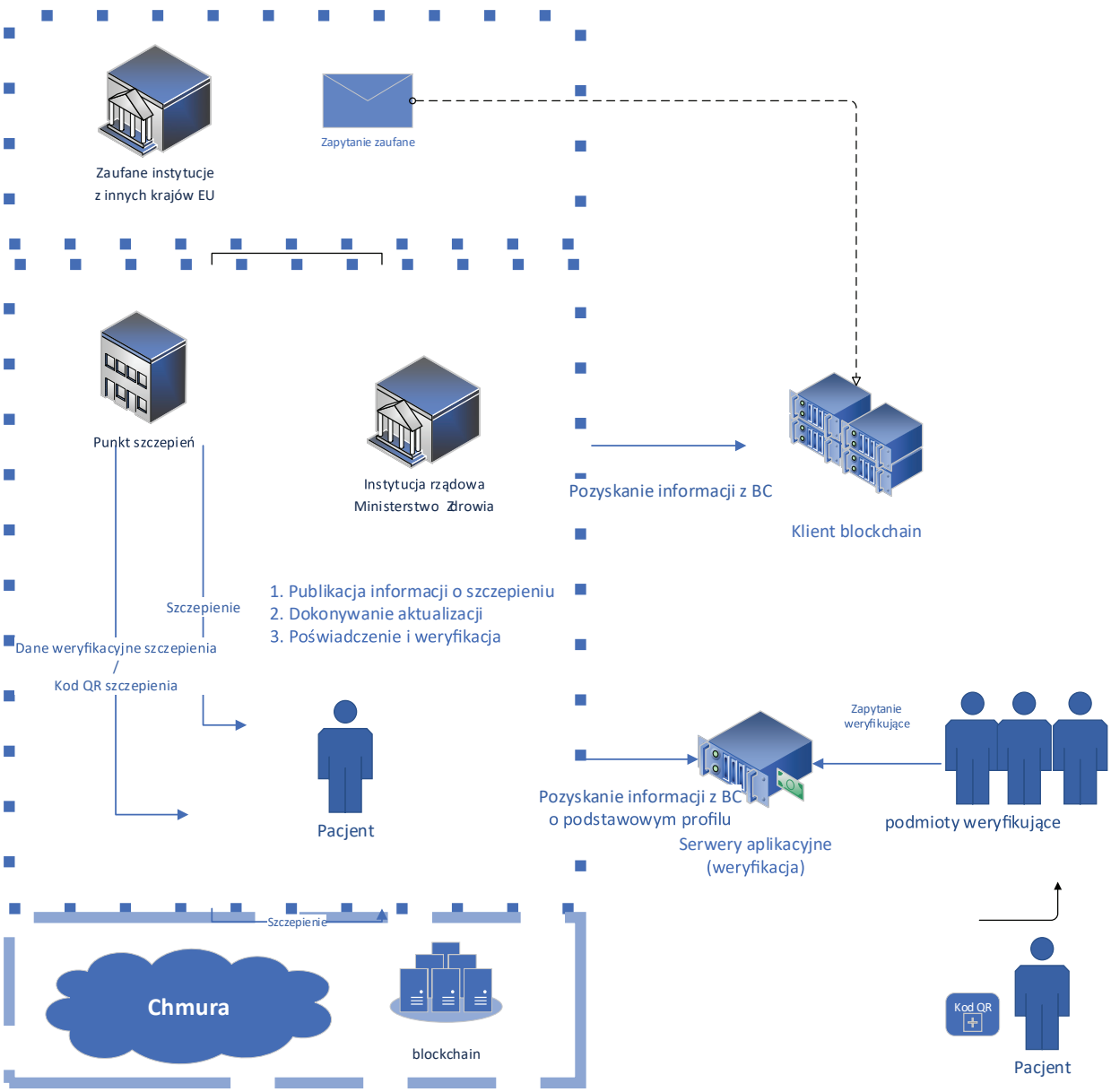
Kolejnym zabezpieczeniem Blockchain jest budowa sieci w formie peer-to-peer oraz implementacja rozproszonej księgi transakcji wraz z mechanizmem konsensusu. Sercem łańcucha bloków jest rozproszona księga, która przechowuje informacje o transakcjach, jakie miały miejsce. Termin „rozproszony" w stosunku do księgi oznacza, że bazując na sieci peer-to-peer każdy użytkownik tej sieci ma replikę księgi. Zapisanie informacji w łańcuchu może nastąpić jedynie z wykorzystaniem mechanizmów kryptograficznych. To one gwarantują, że po dodaniu transakcji do księgi nie można jej już zmodyfikować. Do obsługi całego szeregu funkcji sieci Blockchain, takich jak dostęp do księgi (transakcje i zapytania), wykorzystuje się Smart Contracts. Księga aktualizuje się tylko wtedy, gdy transakcje są zatwierdzane przez zdefiniowanych uczestników lub ich grupę. W innym przypadku aktualizacja nie jest zapisywana w księdze i blok ten nie zostanie włączony do łańcucha. Informacja z tego bloku nie będzie rozpropagowana w sieci.

Podstawowe założenia projektowe systemu powinny uwzględniać następujące parametry:

– obecne tempo szczepień ok. 1 mln szczepień każdego miesiąca, docelowa wartość ok. 5 mln transakcji/miesiąc,
– zapytanie weryfikacyjne do Paszportu Szczepień, ok. 50–200 mln zapytań/dziennie.

Prognozowane tak duże obciążenia, wymagają doboru odpowiedniej architektury systemu i wykonania jej w środowisku chmurowym. Dokonano wyboru środowiska chmurowego Amazon AWS z powodu dostępu do odpowiednich usług, np. Autoscaling. AWS, w ramach swoich usług Amazon Managed Blockchain, udostępnia dwie sieci Blockchain oparte o rozproszoną księgę transakcji: Hyperledger Fabric lub Ethereum (Preview). W proponowanym tutaj rozwiązaniu wybrano sieci Hyperledger Fabric, jako rozwiązanie stabilniejsze i dojrzałe na tej platformie chmurowej.

Podczas prac projektowych, wyróżniono dwa zasadnicze scenariusze użytkowania systemu: dodanie nowego wpisu o szczepieniu oraz proces weryfikacji szczepienia. Obecnie obywatele szczepiąc się przeciwko COVID-19 otrzymują odpowiednie dokumenty o szczepieniu w formie zaświadczenia wydawanego przez jednostkę, w której dokonano tej procedury. System zarządzający szczepieniami w Polsce jest wdrożony i nadzorowany przez Ministerstwo Zdrowia. Ta sama instytucja musi więc zadbać o utworzenie spójnego rejestru – Paszportu



Rys. 2. Proponowana platforma paszportów szczepień bazująca na Blockchain
Fig. 2. Proposed platform for vaccination passports based on the Blockchain

Szczepień. Scenariusz pierwszy powinien uwzględniać wydanie równorzędnego dokumentu potwierdzającego utworzenie Paszportu Szczepień oraz identyfikatora tego Paszportu w formie cyfrowej. Drugi scenariusz przewiduje weryfikację wykonania szczepienia przeciwko COVID-19, zachowując anonimowość i niezmienialność przechowywanych danych. Rejestr powinien pozwalać zainteresowanym stronom na łatwą (czasowo i procesowo) procedurę sprawdzenia zaistniałego zdarzenia szczepienia danego obywatela. Odpowiednią instytucją, która musi zorganizować system weryfikujący, jest ponownie Ministerstwo Zdrowia. To ona przygotowuje procedury i dostarcza infrastrukturę wraz z odpowiednimi interfejsami dostępowymi. Istnieje możliwość włączenia do powyższego systemu zewnętrznych podmiotów na podstawie umów bilateralnych lub standardów wypracowanych na poziomie Unii Europejskiej.

Propozycje architektury systemu Paszportu Szczepień zaprezentowano na rys. 2. W architekturze wyróżniono następujące kluczowe podmioty: Ministerstwo Zdrowia, punkty szczepień, zaufane instytucje EU, podmioty weryfikujące, pacjent. Ministerstwo Zdrowia, jako podmiot organizujący, wyznacza punkty, w których odbywają się szczepienia i są odpowiedzialne za wydawanie zaświadczeń. Punkt ten otrzymuje równocześnie dostęp do systemu wraz przydzieleniem mu dostępu do węzła, umożliwiającego interakcję z łańcuchem bloków. Paszporty Szczepień będą następnie weryfikowane przez dowolną organizację, publiczną lub prywatną (np. port lotniczy lub administracja publiczna, poczta itp.), które muszą sprawdzać status szczepienia danej osoby.

Obecnie w Polsce po dokonaniu szczepienia na COVID-19, każdy z pacjentów otrzymuje formalny dokument potwierdzający ten fakt. Dokument ten jest wydawany przez punkt szczepień wyznaczony przez Ministerstwo Zdrowia. Nie ma więc większego problemu organizacyjnego, by wystawiać dodatkowy dokument w formie cyfrowej, z wykorzystaniem wydruku lub zapisu cyfrowego kodu QR (Quick Response Code), zawierającego kod identyfikacyjny Paszportu Szczepień. Kod ten może być wysłany do aplikacji telefonu osoby zaszczepionej. Jeśli podmioty weryfikacyjne stanowią organy Państwa, typu Policja, Straż Graniczna, to wówczas mogą korzystać z przydzielonych im interfejsów do wymiany informacji. W przypadku masowego dopuszczenia innych podmiotów, konieczne jest wywarcie nacisku na zachowanie prywatności i bezpieczeństwa danych. Można będzie wtedy uzyskać bezpieczne, uniwersalne narzędzie, jakim jest Paszport Szczepień, respektowany nie tylko w kraju, ale także za granicą. Pozwoli to na weryfikację statusu danej osoby, np. na siłowni, basenie czy w restauracji. Taka możliwość sprzyja otwarciu gospodarki i unikaniu w przyszłości lockdown'ów.

Powyższe wytyczne, przyjęte dla proponowanego systemu obsługującego Paszporty Szczepień, są zbieżne z zapowiedziami Ministra Zdrowia Adama Niedzielskiego, jakie wygłosił 20 stycznia 2021 r. na konferencji prasowej. Mówiono wtedy, że osoby, które przyjmą obie dawki szczepionki, będą miały możliwość pobrania w punkcie szczepienia wydruku z kodem QR lub przez Internetowe Konto Pacjenta. Jednak ten dokument nie będzie uznawany w przestrzeni międzynarodowej. Cyfrowe Paszporty Zdrowotne są kluczowym sposobem weryfikacji osób, mogącym pomóc w łagodzeniu rozprzestrzeniania się chorób zakaźnych. Informacje o szczepieniu zapisane w takim dokumencie, tym bardziej wydają się być kluczowe, gdy do końca nie wiemy jaką odporność daje konkretna szczepionka oraz na jaki czas zapewnia ochronę przed wirusem (ramka czasowa). Wirus ustawicznie mutuje i pojawiają się jego nowe odmiany. Te modyfikacje jego struktury mogą decydować o takich cechach, jak: szybkość zarażania, odporność na szczepionkę, zakres odporności itp. Parametry te powinny być nadzorowane w każdej przestrzeni.

Rejestry instytucjonalne muszą być bezpieczne, zapewniając jednocześnie, że strony transakcji mają zagwarantowaną maksymalną prywatność i poufność. Taki poziom bezpieczeństwa i prywatności może zaoferować jedynie technologia Blockchain. Można wyróżnić kilka rodzajów Blockchaina: publiczny, prywatny oraz konsorcjalny. Dobór architektury technologii jest uzależniony od docelowego wdrożenia przez instytucje rządowe i europejskie.

Blockchain prywatny dopuszcza do sieci łańcucha bloków jedynie autoryzowane węzły, co zapewnia poufność. Ministerstwo Zdrowia może budować system w oparciu o ten schemat tylko w przypadku wdrożenia rozwiązania na naszym terytorium. Zakładając pewien poziom zaufania do uczestników sieci, można wówczas stosować uproszczony i efektywniejszy proces uzyskania konsensusu – zatwierdzenia wpisu w księdze transakcji. Prowadzi do skrócenia czasu akceptowania i potwierdzania transakcji.

Blockchain konsorcyjny jest podobny do Blockchaina prywatnego, pod względem projektowanej optymalizacji wydajności, skalowalności i algorytmów wypracowania konsensusu dla ograniczonej liczby węzłów. Różnica pomiędzy tymi dwoma typami polega na tym, że pierwszy typ jest wdrażany w pojedynczej organizacji, natomiast drugi może obejmować wiele organizacji, które współdziałają pomiędzy sobą. Komunikacja pomiędzy tymi podmiotami może być poufna.

Dla tego rozwiązania sugeruje się, by dobór odpowiedniego modelu Blockchain'a zależał od zasięgu akceptowalności Paszportów Szczepień, który może być krajowy – Blockchain prywatny lub na poziomie europejskim – Blockchain konsorcyjny.

4. Metoda weryfikacji informacji Paszport Szczepień

Podstawą utworzenia cyfrowego Paszportu Szczepień, obsługiwanego przez projektowany system, jest możliwość weryfikowalności faktu zaszczepienia danej osoby. Informacje w postaci elektronicznego certyfikatu mogą być bez problemu przechowywane w technologii Blockchain, w sposób zapewniający ich bezpieczeństwo i niezmienność. W celu realizacji tego postulatu, należy odpowiednio zaprojektować sieć mechanizm przechowywania. Na rysunku 1 zobrazowano ogólną postać sieci łańcucha bloków. W rekordzie danych trzeba umieścić podstawowe informacje o szczepieniu, jakie są wprowadzane podczas tej operacji medycznej: imię, nazwisko, miejsce urodzenia, rodzaj szczepionki, seria, termin wykonania szczepienia. Ten podstawowy zbiór powinien pozwolić na możliwość weryfikacji szczepienia i określenie zakresu odporności danej osoby. Istotną wiadomością jest rodzaj preparatu, jaką została zaszczepiona dana osoba oraz parametry tego środka. Obecnie występuje mnogość szczepionek. Każda ma odmienne właściwości i zakres ochrony. W tym obszarze pojawiają się też nowe aktualizacje szczepionki, co wynika z samego charakteru COVID-19, jak i szybkich jego mutacji. Proponowaną strukturę rekordu przedstawiono w tab. 4, a przykład poprawnie wypełnionego rekordu przedstawiono tab. 5. Pewne dane w tym zbiorze są dublowane, np. data urodzenia. Można ją również wyznaczyć z pola Pesel. Ta nadmiarowość nie jest przypadkowa. Ta kwestia zostanie wyjaśniona w dalszej części opisującej schemat weryfikacji uwzględniającej anonimowość.

Celem podniesienia poziomu bezpieczeństwa i zapewnienia prywatności, część pól rekordu zawierająca dane wrażliwe są „szyfrowane" algorytmem BLAKE3. Szyfrowanie oznacza, że dla tej wartości generowany jest skrót nieodwracalny, tzw. hash. Ogólna zasada weryfikacji rekordu szczepienia zmierza do potwierdzenia zgodności danych w systemie, z danymi wprowadzonymi przez osobę weryfikującą. Prywatność gwarantuje fakt, że nie porównujemy danych wrażliwych otwarcie, a jedynie wartości funkcji

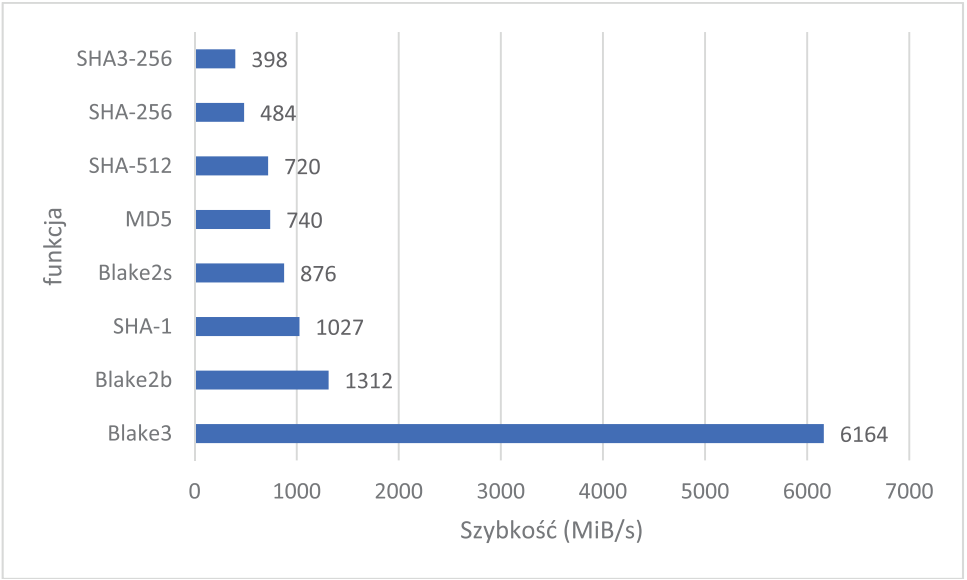
Tab. 4. Proponowana podstawowa struktura rekord danych Paszportu Szczepień
Tab. 4. Proposed basic structure of the Vaccination Passport data record

Nazwa pola danych	Pole Hash	Metoda generowania Hash
ID(Pesel)	Tak	(Pesel)Black3
Imię	Tak	(Imię⊕Data_Urodzenia⊕Miejsce_Urodzenia)Black3
Nazwisko	Tak	(Nazwisko⊕Data_Urodzenia⊕Miejsce_Urodzenia)Black3
Miejsce_Urodzenia	Tak	(Miejsce_Urodzenia⊕Data_Urodzenia⊕Miejsce_Urodzenia)Black3
Data_Urodzenia	Tak	(Data_Urodzenia⊕Data_Urodzenia⊕Miejsce_Urodzenia)Black3
Miejsce_Szczepienia-Kod	Nie	Nie dotyczy
Nazwa Szczepionki	Nie	Nie dotyczy
ATC_code	Nie	Nie dotyczy
Seria	Nie	Nie dotyczy
Data_Godzina_Szczepienia	Nie	Nie dotyczy
Pełne_Zabezpieczenie	Nie	Nie dotyczy
Ważność certyfikatu	Nie	Nie dotyczy

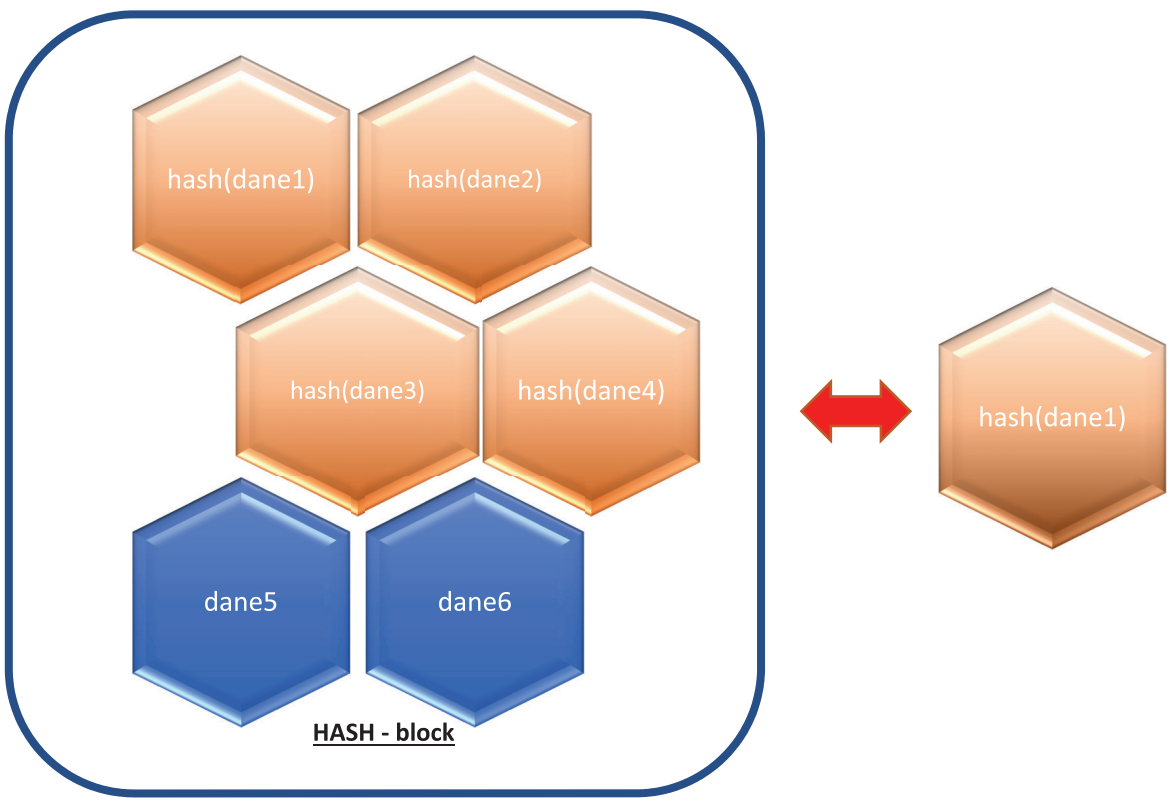
⊕ – operacja łączenia ciągów tekstowych

Tab. 5. Przykład rekordu danych zapisany w Blockchain
Tab. 5. Example of a data record saved in a Blockchain

Nazwa pola danych	Pole Hash	Dane pierwotne	Przykładowa wartość pola w rekordzie
ID(Pesel)	Tak	12345678901	d0c666ae799b9213113442ed35ff609ffddc5ca0818c04e8adcdac4dd5dadfeb
Imię	Tak	Tadeusz	3d808cd6c22c2084fe110b0a4c67307c08e783b39cc2e6574d20f6beb9feb1bd
Nazwisko	Tak	Kowalski	8683925269a149d6918393beae95b396f8de7be16e1ce9063de0c0d80f9b3d86
Miejsce_Urodzenia	Tak	Wieliczka	660bbb35d19dffd1581a6494d87a0781ae09479bcf5c69f5338adc42cc4a99de
Data_Urodzenia	Tak	11.11.1942	f538bfd30d2322ded7906e5792318e49fcf21d6e9ae976a351fe429e4ba0aeaa
Miejsce_Szczepienia	Nie	,'ZDROWIE''SP.J. A.ANTAS,M.TUNIK, M.SIEMIENAS-PALICHLEB, J.POLSZCZUK, A.WŁODARSKI	,'ZDROWIE''SP.J. A.ANTAS,M.TUNIK, M.SIEMIENAS-PALICHLEB, J.POLSZCZUK, A.WŁODARSKI
Nazwa Szczepionki	Nie	Pfizer–BioNTech COVID19	Pfizer–BioNTech COVID19
ATC_Code		J07BX	J07BX
Seria	Nie	PAA156732	PAA156732
Data_Godzina_ Szczepienia	Nie	21.01.2021	21.01.2021
Pełne_Zabezpieczenie	Nie	Nie	Nie
Ważność certyfikatu	Nie	21.01.2023	21.01.2023



Rys. 3. Porównanie wydajności różnych algorytmów Hash, platforma testowa AWS c5.metal, wejście 16 KiB, 1 wątek, źródło: https://github.com/BLAKE3-team/BLAKE3/
Fig. 3. Performance comparison of different Hash algorithms, AWS c5.metal test platform, 16 KiB input, 1 thread, source: https://github.com/BLAKE3-team/BLAKE3/



Rekord: **Block hash: 0d8b2948118ee17d2224501458bef56b69dac44eee6856f55121ef7522680640**
d0c666ae799b9213113442ed35ff609ffddc5ca0818c04e8adcdac4dd5dadfeb
3d808cd6c22c2084fe110b0a4c67307c08e783b39cc2e6574d20f6beb9feb1bd
8683925269a149d6918393beae95b396f8de7be16e1ce9063de0c0d80f9b3d86
660bbb35d19dffd1581a6494d87a0781ae09479bcf5c69f5338adc42cc4a99de
f538bfd30d2322ded7906e5792318e49fcf21d6e9ae976a351fe429e4ba0aeaa
"ZDROWIE"SP.J. A.ANTAS,M.TUNIK, M.SIEMIENAS-PALICHLEB, J.POLSZCZUK, A.WŁODARSKI
Pfizer–BioNTech COVID-19
J07BX
PAA156732
21.01.2021
Nie
21.01.2023

Nazwisko	Kowalski	8683925269a149d6918393beae95b3 96f8de7be16e1ce9063de0c0d80f9b3d86

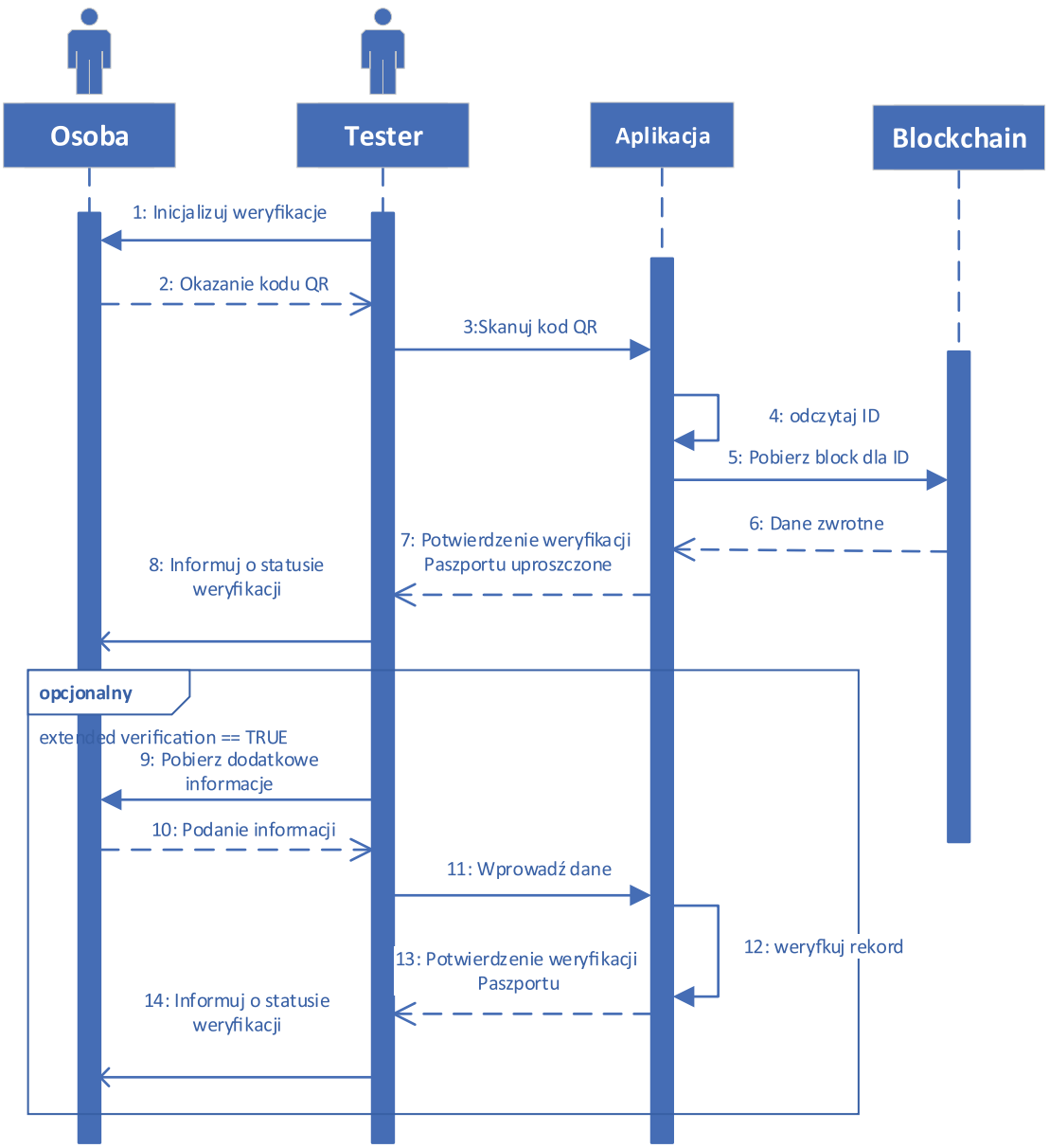
Rys. 4. Schemat weryfikacji rekordu danych zapisany w Blockchain
Fig. 4. Data record verification scheme stored in Blockchain

nieodwracalnej zapisanej w rekordzie danych. Dane szyfrowane są danymi wrażliwymi, a pozostałe dane pozostają bez szyfrowania. Zachowujemy wtedy poufność i bezpieczeństwo danych wrażliwych podczas procesu przesyłu informacji, udostępniania i weryfikacji. Politykę tę można zmieniać zależnie do poziomu bezpieczeństwa. Dodatkowy poziom prywatności i bezpieczeństwa zapewnia możliwość weryfikacji pewnych wybranych pól(losowych), zamiast wszystkich danych z rekordu.

Funkcje generujące hash są nazywane funkcjami skrótu, skrótem nieodwracalnym, funkcją mieszającą lub funkcją haszującą. Istota tej metody polega na tym, że funkcja ta dowolnie dużemu zbiorowi wejściowemu (np. liczbie, tekstowi itp.) przyporządkowuje krótką i jednoznaczną wartość o stałym rozmiarze. Jest ona niespecyficzna i quasi-losowa. Współcześnie, użytkowanie skrótu nieodwracalnego jest bardzo rozpowszechnione i w dobie wszechobecnego RODO pozwala na używanie techniki pseudonimizacji.

Technika pseudomizacji polega na przechowywaniu w określonym zbiorze jedynie identyfikatorów. Wartości te nie powiedzą innym osobom niczego na temat danych wrażliwych. Administrator danych w tym systemie ma możliwość dopasowania identyfikatora do konkretnego rekordu z danymi i powiązania go z konkretną osobą. Korzystając z funkcji skrótu, można zabezpieczyć rekord ze szczepienia w paszporcie i swobodnie używać go w systemie, zachowując przy tym anonimowość. W proponowanym rozwiązaniu sugeruje się użytkowanie funkcji BLAKE3, która została wydana w 2020 r. Autorzy funkcji, czyli Jack O'Connor, Jean-Philippe Aumasson, Samuel Neves i Zooko Wilcox-O'Hearn znacznie poprawili jej wydajność w porównaniu do pozostałych algorytmów SHA-1, SHA-2, SHA-3, MD5 i BLAKE2. Zestawienie tych wskazanych funkcji zawarto na rys. 3. Wydajność funkcji nieodwracalnej ma znaczenie w przypadku proponowanej implementacji, z uwagi na efektywność całego systemu. Zgodnie ze specyfikacją Paszportu Szczepień, obecnie wydajność szczepień wynosi ok. 100–200 tys. dziennie, a docelowo powinna się zwielokrotnić. Szacuje się, że przy obecnym stanie szczepień, liczba operacji generowania funkcji hash w ciągu dnia będzie wynosiła ok. 500 tys. razy (jest zależna od zakresu danych szyfrowanych).

Zachowanie anonimowości ma szczególne znaczenie, gdy posługujemy się danymi osobowymi – danymi wrażliwymi. Generowanie skrótu dla tych danych i wykorzystanie ich podczas weryfikacji pozwoli na nieujawnianie danych osobom postronnym, a osoby sprawdzające mają możliwość pełnej weryfikacji poprawności danych zachowując bezpieczeństwo i anonimowość. Nawet gdy ktoś uzyska dostęp do rekordu, nie będzie w stanie



Rys. 5. Diagram sekwencji procesu weryfikacji rekordu danych Paszportu Szczepień
Fig. 5. Sequence diagram of the verification process of the Vaccination Passport data record

odczytać z niego danych wrażliwych bez pomocy osoby, której te dane dotyczą. Do weryfikacji autentyczności całego paszportu wystarczy skorzystać wybiórczo z jednego pola zawierające dane wrażliwe, a nie ze wszystkich pól. Pozostałe są ukryte – zaszyfrowane. Schemat idei weryfikacji paszportu zawarto na rys. 4. W rekordzie danych zawarto dodatkowe nadmiarowe pola, np. data urodzenia. Z tych elementów można skorzystać wybiórczo przy weryfikacji dokumentu szczepienia nie odpytując bezpośrednio o wszystkie dane wrażliwe. Przykładowo, osoba weryfikowana podaje tylko nazwisko data urodzenia oraz miejscowość urodzenia. Na tej podstawie jest weryfikowana poprawność rekordu szczepienia przez obliczenie funkcji skrótu dla kombinacji tych elementów zgodnie z zastosowanym schematem, a następnie jest obliczana funkcja powtórnie dla całego rekordu po podstawieniu do tej struktury obliczonej funkcji nieodwracalnej. Jeśli weryfikacja hash rekordu pierwotnego oraz obliczonego jest prawidłowa, to wówczas dane zawarte w rekordzie są prawidłowe – zweryfikowano osobę poprawnie. Faktem jest, że data urodzenia jest częścią nr PESEL i można ją pozyskać z tego numeru. W proponowanej metodzie operuje na poziomie wartości funkcji skrótu (zaszyfrowanych), a nie bezpośrednio na danych wrażliwych. Aplikacja weryfikująca oraz osoba testująca nie mają dostępu do danych pierwotnych, a jedynie tych elementów, które poda osoba weryfikowana. Dane te muszą być proste do zapamiętania, a zarazem wystarczające do budowy odpowiedniego wzorca szyfrującego. Z drugiej jednak strony, nadmiarowość pewnych pól wrażliwych gwarantuje możliwość losowego wyboru pola poddawanego weryfikacji. Nie jest konieczne odwoływanie się do tej samej sekwencji pól: imię, nazwisko itd. Celem realizacji tej możliwości konieczny jest odpowiedni zasób danych nadmiarowych.

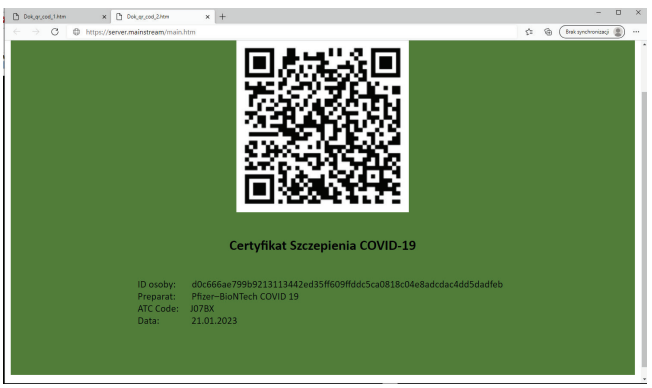
Nadrzędną zasadą jest tu minimalizm danych wrażliwych używanych w procesie weryfikacji. Aplikację weryfikacji można zatem udostępnić innym podmiotom bez obawiania się o udostepnienie danych wrażliwych obywateli w kraju i zagranicą.

Użytkowanie w życiu codziennym wartości pseudolosowej może być trudne do zapamiętania lub zapisania. Odpowiednim podejściem ułatwiającym funkcjonowanie Paszportu Szczepień powinny być kody QR. Kod ten jest na tyle uniwersalnym elementem używanym współcześnie, że mogą go odczytać i przetworzyć różne urządzenia, takie jak skanery QR, smartfony, kamery itd. Z ich wykorzystaniem można współdzielić rozmaite informacje, takie jak: adres strony internetowej, numer telefonu, sms itp. Jest to bardzo uniwersalne narzędzie. Tak samo skutecznie procesowo będzie można użytkować w życiu codziennym kodu QR do weryfikacji szczepień. Odczyt tego identyfikatora jest wystarczający do sprawdzenia np. na stacji kolejowej, podczas kontroli służby granicznej i policyjnej, w portach lotniczych, w komunikacji miejskiej, kolei itp. W proponowanym systemie, kod QR powinien być wydany przez punkt szczepień i pełnić funkcję identyfikatora Paszportu Szczepień przyporządkowanego do danego pacjenta. Proponuje się, by identyfikatorem był wynik funkcji hash numeru PESEL. W sytuacji utraty zaświadczenia lub wydruku kodu QR, pacjent może samodzielnie odtworzyć ten identyfikator.

Ważna jest prostota i intuicyjność stosowania systemu. Wprowadzanie danych do systemu udostępnionego przez Ministerstwo Zdrowia, przeznaczonego do obsługi szczepień, winno zostać rozszerzone o procedurę automatycznej obsługi Paszportów Szczepień. Ta procedura musi też skutkować wpisaniem informacji do Paszportu Szczepień i wygenerowaniem kodu QR. Przykład kodu rozdawanego pacjentom zawarto na rys. 6. Informacja otrzymana z aplikacji powinna być prosta: zaszczepiony lub niezaszczepiony, a sugeruje się w tym względzie oznaczania odpowiedzi systemu kolorami: czerwony i zielony. Przykład weryfikacji z aplikacji weryfikującej zawarto na rys. 7.

Rys. 6. Kod QR identyfikatora osoby z Tab. 5
Fig. 6. QR code of the person's identifier from Tab. 5

Podstawowy schemat procesowy użytkowania systemu, tj. „weryfikację" przedstawiono na rys. 5. Istnieją dwa podstawowe podmioty: osoba sprawdzana oraz podmiot testujący. Procedura wykonania weryfikacji szczepienia powinna być na tyle prosta i nieuciążliwa, by jak najmniej angażować strony, jednocześnie zachowując odpowiedni poziom pewności oraz ilości obsługiwanych osób przez system. Kod QR znacznie skraca czas weryfikacji, nie wymaga wprowadzania danych. W ten sposób łatwo można zautomatyzować proces weryfikacji. Taki kod może być zapisany w telefonie w formie obrazka lub na Internetowym Koncie Pacjenta. Można go wydrukować i wciąż będzie odczytywany przez urządzenia. System musi sprawnie obsługiwać weryfikację obywateli w sposób natychmiastowy, by nie powstawały zbędne zatory. Taką efektywność mogą zagwarantować rozwiązania chmurowe.



Rys. 7. Wynik zapytania weryfikującego Paszportu Szczepień
Fig. 7. Result of the inquiry verifying the Vaccination Passport

Tab. 6. Przykład pełnej weryfikacji danych wrażliwych
Tab. 6. Example of full verification of sensitive data

Lp.	Pole danych wrażliwych	Wartość pola uzyskana z zapytania	Wartość pola – zaszyfrowana	Dane podane testerowi przez osobę – wartość	Wyliczona przez testera wartość funkcji skrótu	Status weryfikacji
1.	Imię	3d808cd6c22c2084f e110b0a4c67307c08 e783b39cc2e6574d2 0f6beb9feb1bd	Tadeusz	Tadeusz	Hash(Tadeusz)=3d808cd 6c22c2084fe110b0a4c67 307c08e783b39cc2e6574 d20f6beb9feb1bd	Zgodne – Zweryfikowano poprawnie
2.	Nazwisko	8683925269a149d69 18393beae95b396f8 de7be16e1ce9063de 0c0d80f9b3d86	Kowalski	Kowalski	Hash(Kowalski)=868392 5269a149d6918393beae9 5b396f8de7be16e1ce906 3de0c0d80f9b3d86	Zgodne – Zweryfikowano poprawnie

Dla uproszczenia, działanie systemu weryfikacji można opisać dwoma podstawowymi regułami decyzyjnymi:

1. if ((Pesel)Black3) exist „jest zaszczepiony" else „nie jest zaszczepiony"
2. if dane_hash == hash(dane_weryfikacja) and hash(record_danych) == hash_record then „zgodne dane" (prawidłowa pełna weryfikacja) else „niezgodne dane"

Celem podniesienia bezpieczeństwo systemu i zapewnienia większej anonimowości możliwe jest losowy wybór danych wrażliwych w zapytaniu weryfikacji szczegółowej. Przykładowo może to być jedynie nazwisko lub imię. Weryfikacja jednej lub dwóch wartości potwierdzi prawdziwość zawartych danych bazując na konstrukcji rekordu zawartym w tab. 4.

5. Chmura obliczeniowa dedykowana realizacji Paszport Szczepień w technologii blockchain

Celem sprawdzenia koncepcji Paszportu Szczepień, wykonano rozwiązanie testowe w środowisku chmurowym z wykorzystaniem Amazon AWS (https://aws.amazon.com/). AWS (Amazon Web Services) jest chmurą obliczeniową, która dostarcza zasobów na żądanie za pośrednictwem platformy udostępnionej w sieci Internet. Chmura zapewnia zwinność implementacyjną, co gwarantuje łatwy dostęp do szerokiej gamy technologii. Dzięki temu można szybciej implementować, testować i wprowadzać własne rozwiązania oraz innowacje. Wybór platformy Amazon AWS nie był przypadkowy, lecz poparty rzeczowa analizą. Uzyskane rezultaty z prac pokrywają się z wynikami raportu [34].

Rozwiązanie informatyczne Paszportu Szczepień powinno zostać zrealizowana w chmurze obliczeniowej ze względu na możliwość budowy dynamicznie optymalizowanego rozwiązania informatycznego pod względem konstrukcji i wykorzystywanych zasobów. W klasycznym wariancie projektowania infrastruktury IT na wstępnym etapie prognozowało się spodziewane obciążenie i w zależności od tych szacunków konstruowało się infrastrukturę - optymalną. Chmura obliczeniowa pozwala na budowanie rozwiązania kompleksowo. Rozwiązanie to będzie reaktywnie zmniejszać lub zwiększać zasoby oraz dostęp do usług, w zależności od aktualnego zapotrzebowania. Chmura to również wysokie bezpieczeństwo. Można w tym względzie skorzystać z wielu dostępnych usług infrastruktury Amazon AWS do zabezpieczenia całego konstruowanego rozwiązania, np. Amazon Macie, AWS Sheld, Amazon Macie i inne.

Rozwiązania chmurowe są znacznie bardziej elastyczne niż tradycyjne instalacje on-premise. Wdrażanie zmian jest znacznie szybsze i nie wymaga dużego nakładu pracy zespołu informatyków. Co ma znaczenie w przypadku prezentowanego przedsięwzięcia, które dynamicznie będzie rozwijać się. Stwierdzenie to ma szczególne znaczenie, gdy uwzględnia się przyszłościowo fakt dostępu do zasobów w różnych regionach Europy.

Proponowaną architekturę AWS obsługującą Paszport Szczepień z implementacją technologii Blockchain zaprezentowano na rys. 8. Konstruowanie systemu w środowisku chmurowym AWS jest prostsze od rozwiązań on-premise. Rozwiązanie IT konstruowane jest z gotowych „klocków" oprogramowania oferowanych przez dostawcę usług. Elementy te można swobodnie integrować, tworząc bezpieczne i skalowalne aplikacje. Podstawowe usługi wymagane przez aplikacje to Load Balancing (https://aws.amazon.com/elasticloadbalancing/) oraz skalowalność infrastruktury i usług (https://aws.amazon.com/autoscaling/), które zostały szerzej omawiane w dokumentacji technicznej Amazon AWS.

Na diagramie architektury chmurowej można wyróżnić podstawowe usługi dla tego rozwiązania: Blockchain Services, Cognito, API Gateway, Lambda, AWS Privatelink. Przedstawiona architektura została zoptymalizowana, by w pełni obsłużyć duży ruch generowany przez użytkowników systemu Paszportu Szczepień. Obciążenie projektowe można określić jako znaczne: docelowa to dzienny przyrost rekordów, który szacuje się na 200–300 tys., a zapytania weryfikacyjne 50–80 mln każdego dnia. Docelowo wskazane parametry moja ulec zwielokrotnieniu. Taki ruch aplikacyjny jest w stanie obsłużyć jedynie wysoko wydajne środowisku chmurowe.

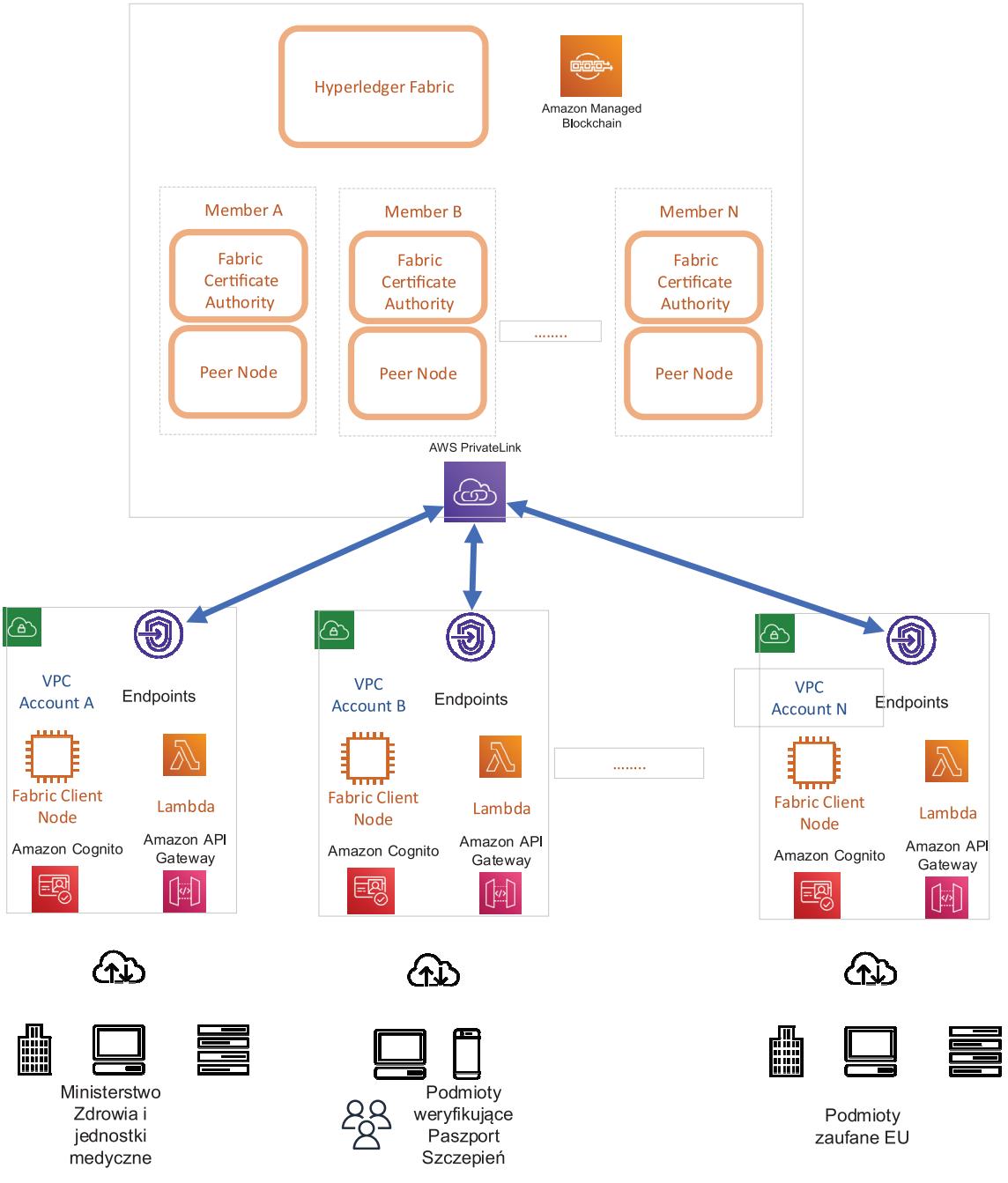
Na potrzeby aplikacji zaprojektowano i wykonano wzorcową infrastrukturę Paszportu Szczepień bazującego na technologii Blockchain. Głównym elementem infrastruktury jest Blockchain Hyperledger Fabric, który przechowuje rekordy Paszportu Szczepień pacjenta. Platforma Hyperledger Fabric to rozwiązanie oparte o framework open source nadzorowane przez Linux Foundation. Ma aktywną i rosnącą społeczność programistów, co wpływa znacznie na witalność całego projektu. Sieć ta ma mechanizm zarządzania uprawnieniami. Tożsamość każdego z uczestników sieci jest znana, jak również wykonywane przez nich operacje. Zabezpieczenia takie mają istotne znaczenie w takich dziedzinach jak finanse, e-health itp.

W projekcie skorzystano z rozwiązania Amazon Managed Blockchain. To w pełni zarządzana usługa, która pozwala skonstruować skalowalną sieć Blockchain Hyperledger Fabric i efektywnie nią zarządzać. Gdy sieć zostaje uruchomiona, Amazon Managed Blockchain ułatwia zarządzanie i utrzymanie sieci blockchain, w tym: zarządza certyfikatami i umożliwia łatwe tworzenie nowych członków (podmiotów) łączących się z siecią. Takie środowisko Blockchain tworzy bezpieczne i odporne na fałszowania miejsce do przechowywania danych pacjentów.

Jak wskazano na diagramie (rys. 8), Managed Blockchain zarządza usługami sieci Hyperledger Fabric. Wszystkie elementy składowe infrastruktury dedykowane kooperacji z Blockchain są umiejscowione w sieci szkieletowej AWS i nie są narażone na udostępnienie w publicznym Internecie. W tym kontekście można również wspomnieć o usłudze AWS PrivateLink. Usługa ta zapewnia prywatną komunikację między VPC (siecią wirtualną) oraz usługami Amazon AWS bez eksponowania tego ruchu do zewnętrznego/publicznego Internet. AWS PrivateLink ułatwia łączenie usług z różnych kont AWS oraz VPC, aby znacznie uprościć architekturę sieci. Dodatkowo ta usługa wraz z Gateway Load Balancer pozwala na równoważenia obciążenia, zapewnia identyczny poziom bezpieczeństwa i wydajności urządzeń sieci wirtualnej. Efektem jest stabilność wraz z podniesieniem efektywności komunikacji jaką można uzyskać w implementacji Paszportu Szczepień.

Amazon API Gateway wraz z Lambdą to w pełni zarządzana usługa, która ułatwia tworzenie, publikowanie, utrzymywanie, monitorowanie i zapewnienie bezpieczeństwa dla interfejsów API w dowolnej skali. Usługa ta tworzy RESTful API i WebSocket API, które pozwalają w czasie rzeczywistym na komunikacje dwukierunkowa aplikacji. Amazon API Gateway pozwala na akceptowanie i obsługę setek tysięcy równoległych zapytań API. Wymaga to zastosowania odpowiednich mechanizmów zarządzania ruchem, wsparcia cross-origin resource sharing (CORS), autentyfikacji oraz kontroli dostępu, monitorowaniem oraz zarządzaniem wersjonowaniem API.

Amazon Cognito umożliwia szybką i łatwą rejestracje użytkowników, logowania oraz kontrole dostępu do aplikacji internetowych i mobilnych. Usługa ta skaluje się do milionów użytkowników i obsługuje opcje logowania u dostawców tożsamości społecznościowych, takich jak Apple, Facebook, Google i Amazon, oraz dostawców tożsamości innych podmiotów za pośrednictwem SAML 2.0 i OpenID Connect. Usługa ta jest nieoceniona przy budowaniu złożonych środowisk aplikacyjnych. AWS Cognito może integrować się z aplikacjami: iOS Objective C, IOS Swift, Android, REACT native, Web. Temat implementacji tego systemu jest bardzo rozległy i zostanie szerzej rozwinięty w osobnym artykule.



Rys. 8. Referencyjna architektura aplikacji Paszportu Szczepień wykonano w środowisku chmurowym Amazon AWS
Fig. 8. The reference architecture of the Vaccination Passport application was made in the Amazon AWS cloud environment

Przedstawione powyżej usługi komplementarne tworzą aplikację Paszportu Szczepień, która stanowi spójną, skalowalną i bezpieczna platformę realizacji operacji weryfikacji szczepień dla wielu milionów użytkowników paszportów w życiu codziennym. Przedstawiona architektura pozwala również na unikniecie wielu wpadek obecnych systemów oferowanych przez instytucje rządowe związane z prawidłową obsługą różnego typu aplikacji oferujących usługi obywatelom.

6. Podsumowanie

W celu aktywnej walki z pandemią COVID-19 i dla szybszego poluzowania restrykcji oraz złagodzenia środków dystansowania, sugeruje się użycie Paszportów Szczepień COVID-19. Jest to dokument potwierdzający, że dana osoba zaszczepiła się przeciwko chorobie i jest odporna na koronowirusa. W związku z tym, zaszczepieni powinni liczyć na przywileje. W Polsce na dzień dzisiejszy jest to zwolnienie z kwarantanny, np. podczas przekraczania granicy. Z drugiej zaś strony, dostęp do przywilejów zachęcałby innych do fałszerstw, tak jak ma to miejsce w przypadku testów na obecność koronowirusa nabywanych w Internecie. Szybkie metody weryfikacji tego zaświadczenia, które są: efektywne czasowo, proste proceduralnie, a dodatkowo bezpieczne, zachowujące prywatność i anonimowość, są konieczne. Wiele krajów już pracuje nad rozwiązaniem tego problemu. Dzieje się to także w Europie. Jedynie rozwiązania cyfrowe mogą wspomóc walkę z pandemią COVID-19.

W artykule zaproponowano implementację Paszportu Szczepień COVID-19, bazującą na Blockchain. Dodanie certyfikatu do Paszportu Szczepień jest wykonywane przez punkty realizujące szczepienia, wyznaczone przez Ministerstwo Zdrowia. Weryfikacja Paszportów może się odbywać przez dowolny podmiot, któremu osoba zaszczepiona przedstawi swój identyfikator, bez zbędnych procedur administracyjnych. Weryfikowanie Paszportu Szczepień przebiega za pomocą kodu QR – identyfikator przyznawany osobie zaszczepionej. Takie działanie podnosi również efektywność użytkowania systemu w życiu codziennym. Kod taki można w prosty sposób wydać w postaci wydruku na kartce papieru, przez zapisanie na profilu pacjenta

lub innym nośniku cyfrowym w formacie pdf bądź w formacie graficznym. Osoba weryfikująca może odczytać kod, dzięki wbudowanej kamerze w smartfonie z zainstalowaną do tego celu aplikacją lub poprzez stacjonarny czytnik.

Mnogość podmiotów weryfikujących oraz ilość operacji może rodzić obawy o bezpieczeństwo danych i anonimowość. Rozwiązaniem tego problemu jest możliwość zastosowania technologii Blockchain oraz technik pseudomizacji, z wykorzystaniem funkcji skrótu BLACK3. Przy weryfikacji Paszportu Szczepień nie trzeba posługiwać się danymi wrażliwymi bezpośrednio, lecz można skorzystać z funkcji hash w weryfikacji poprawności danych. Dodatkowym zabezpieczeniem Paszportu Szczepień jest metoda przechowywania informacji w Blockchain, który jest odporny na modyfikacje i fałszowanie. Dzieje się tak, ponieważ raz zarejestrowane dane w bloku nie mogą być zmienione bez przekształcenia wszystkich kolejnych bloków następujących po tym modyfikowanym.

Całość rozwiązania zaimplementowano w chmurze Amazon AWS, która dodatkowo podnosi bezpieczeństwo, dzięki wykorzystaniu wielu narzędzi. Przy okazji zapewnia dynamiczną skalowalność całej aplikacji, przy prognozowanym dużym obciążeniu wykorzystania Paszportu Szczepień.

Bibliografia

1. World Health Organization: Background paper on Covid-19 disease and vaccines: prepared by the Strategic Advisory Group of Experts (SAGE) on immunization working group on COVID-19 vaccines, 22 December 2020, Geneva.
2. International certificate of vaccination or prophylaxis [www.who.int/ihr/ports_airports/icvp/en/].
3. World Health Organization: *The COVID-19 candidate vaccine landscape*. Geneva 2021.
4. Xu H., Zhang L., Onireti O., Fang Y., Buchanan W.J., Imran M.A., *BeepTrace: Blockchain-enabled Privacy-preserving Contact Tracing for COVID-19 Pandemic and Beyond*. "IEEE Internet of Things Journal", 2020, DOI: 10.1109/JIOT.2020.3025953.
5. Klaine P.V., Zhang L., Zhou B., Sun Y., Xu H., Imran M., *Privacy-Preserving Contact Tracing and Public Risk Assessment Using Blockchain for COVID-19 Pandemic*. "IEEE Internet of Things Magazine", Vol. 3, No. 3, 2020, 58–63, DOI: 10.1109/IOTM.0001.2000078.
6. Lv W., Wu S., Jiang C., Cui Y., Qiu X., Zhang Y., *Towards Large-Scale and Privacy-Preserving Contact Tracing in COVID-19 pandemic: A Blockchain Perspective*. "IEEE Transactions Network Science and Engineering", 2020, DOI: 10.1109/TNSE.2020.3030925.
7. Demir M., Turetken O., Ferworn A., *Blockchain-Based Transparent Disaster Relief Delivery Assurance*. [In:] 2020 IEEE International Systems Conference (SysCon), 1–8, DOI: 10.1109/SysCon47679.2020.9275915.
8. Kumar R., Tripathi R., *A Secure and Distributed Framework for sharing COVID-19 patient Reports using Consortium Blockchain and IPFS*. [In:] 2020 Sixth International Conference on Parallel, Distributed and Grid Computing (PDGC), 231–236, DOI: 10.1109/PDGC50313.2020.9315755.
9. Hasavari S., Song Y.T., *A Secure and Scalable Data Source for Emergency Medical Care using Blockchain Technology*. [In:] 2019 IEEE 17th International Conference on Software Engineering Research, Management and Applications (SERA), 71–75, DOI: 10.1109/SERA.2019.8886792.
10. Christodoulou K., Christodoulou P., Zinonos Z., Carayannis E.G., Chatzichristofis S.A., *Health Information Exchange with Blockchain amid Covid-19-like Pandemics*. [In:] 2020 16th International Conference on Distributed Computing in Sensor Systems (DCOSS), 412–417, DOI: 10.1109/DCOSS49796.2020.00071.
11. Delaney S., Schmidt D., Chan C., *The Logical Architecture Essential for the Creation of a Comprehensive Patient Healthcare Profile on Blockchain*. [In:] 2020 IEEE 6th World Forum on Internet of Things (WF-IoT). 1–7, DOI: 10.1109/WF-IoT48130.2020.9221024.
12. Geneiatakis D., Soupionis Y., Steri G., Kounelis I., Neisse R., Nai-Fovino I., *Blockchain Performance Analysis for Supporting Cross-Border E-Government Services*. "IEEE Transactions on Engineering Management", Vol. 67, No. 4, 2020, 1310–1322, 2020, DOI: 10.1109/TEM.2020.2979325.
13. Castaldo L., Cinque V., *Blockchain-Based Logging for the Cross-Border Exchange of eHealth Data in Europe*. [In:] Gelenbe E., Campegiani P., Czachórski T., Katsikas S.K., Komnios I., Romano L., Tzovaras D. (eds.) *Security in Computer and Information Sciences*. 46–56. Springer International Publishing, Cham 2018.
14. Shahriar Rahman M., Al Omar A., Bhuiyan M.Z.A., Basu A., Kiyomoto S., Wang G., *Accountable Cross-Border Data Sharing Using Blockchain Under Relaxed Trust Assumption*. "IEEE Transactions on Engineering Management", Vol. 67, No. 4, 2020, 1476–1486, DOI: 10.1109/TEM.2019.2960829.
15. Patel D., Balakarthikeyan Mistry V., *Border Control and Immigration on Blockchain*. [In:] Chen S., Wang H., Zhang L.-J. (eds.) Blockchain – ICBC 2018. 166–179. Springer International Publishing, Cham 2018, DOI: 10.1007/978-3-319-94478-4_12.
16. Wu H., Cao J., Yang Y., Tung C.L., Jiang S., Tang B., Liu Y., Wang X., Deng Y., *Data Management in Supply Chain Using Blockchain: Challenges and a Case Study*. [In:] 2019 28th International Conference on Computer Communication and Networks (ICCCN). 1–8, DOI: 10.1109/ICCCN.2019.8846964.
17. Malik S., Dedeoglu V., Kanhere S.S., Jurdak R., Tru*stChain: Trust Management in Blockchain and IoT Supported Supply Chains*. [In:] IEEE International Conference on Blockchain, 2019, 184–193, DOI: 10.1109/Blockchain.2019.00032.
18. Febriansyah, Antoni D., Lestari E., *The Role of Blockchain Technology in E-Govemment Capability: Literature Review*. [In:] Fifth International Conference on Informatics and Computing, 2020, 1–5, DOI: 10.1109/ICIC50835.2020.9288578.
19. Kalla A., Hewa T., Mishra R.A., Ylianttila M., Liyanage M., *The Role of Blockchain to Fight Against COVID-19*. "IEEE Engineering Management Review", Vol. 48, No. 3, 2020, 85–96, DOI: 10.1109/EMR.2020.3014052.
20. Gunter T.D., Terry N.P., *The emergence of national electronic health record architectures in the United States and Australia: models, costs, and questions*. "Journal of Medical Internet Research", Vol. 7, 2005, DOI: 10.2196/jmir.7.1.e3.
21. Bartlett J., *Chile's 'immunity passport' will allow recovered coronavirus patients to break free from lockdown, get back to work*, [www.washingtonpost.com/world/the_americas/chile-coronavirus-immunity-passport-antibody-testing-card/2020/04/20/8daef326-826d-11ea-81a3-9690c9881111_story.html].
22. Phelan A., *COVID-19 immunity passports and vaccination certificates: scientific, equitable, and legal challenges*. "The Lancet", Vol. 395, No. 10237, 2020, 1595–1598, DOI: 10.1016/S0140-6736(20)31034-5.
23. Deka S.K., Goswami S., Anand A., *A Blockchain Based Technique for Storing Vaccination Records*. [In:] 2020 IEEE Bombay Section Signature Conference, 135–139, DOI: 10.1109/IBSSC51096.2020.9332171.
24. Hasan H.R., Salah K., Jayaraman R., Arshad J., Yaqoob I., Omar M., Ellahham S., *Blockchain-Based Solution for COVID-19 Digital Medical Passports and Immunity Certificates*. "IEEE Access", Vol. 8, 2020, 222093–222108, DOI: 10.1109/ACCESS.2020.3043350.

25. Eisenstadt M., Ramachandran M., Chowdhury N., Third A., Domingue J.: *COVID-19 Antibody Test/Vaccination Certification: There's an App for That*, "IEEE Open Journal of Engineering in Medicine and Biology", Vol. 1, 2020, 148–155, DOI: 10.1109/OJEMB.2020.2999214.
26. Chaudhari S., Clear M., Tewari H., *Framework for a DLT Based COVID-19 Passport*. ArXiv Prepr. ArXiv200801120, 2020.
27. Hernández-Ramos J.L., Karopoulos G., Geneiatakis D., Martin T., Kambourakis G., Fovino I.N., *Sharing pandemic vaccination certificates through blockchain: Case study and performance evaluation*, 2021.
28. Hayes B., *Cloud computing*, "Communications of the ACM", Vol. 51, No. 7, 2008, 9–11, DOI: 10.1145/1364782.1364786.
29. Compaq Computer Corporation: Internet Solutions Division Strategy for Cloud Computing. CST presentation, 1996.
30. Sehgal N.K., Bhatt P.C.P., *Cloud Computing: Concepts and Practices*. Springer International Publishing, 2018.
31. Okediran O.O., Sijuade A.A., Wahab W.B., Oladimeji A.I., *A Framework for a Cloud-Based Electronic Health Records System for Developing Countries*. [In:] International Conference on Electrical, Communication, and Computer Engineering, 2020, 1–5, DOI: 10.1109/ICECCE49384.2020.9179276.
32. Maganti P.K., Chouragade P.M., *Secure Health Record Sharing for Mobile Healthcare in Privacy Preserving Cloud Environment*. [In:] IEEE International Conference on Electrical, Computer and Communication Technologies, 2019, 1–4, DOI: 10.1109/ICECCT.2019.8869390.
33. Varghese B., Buyya R., *Next generation cloud computing: New trends and research directions*, "Future Generation Computer Systems", Vol. 79, 2018, 849–861, DOI: 10.1016/j.future.2017.09.020.
34. *State of the Cloud Report 2021 from Flexera*. Flexera, Itasca, Illinois, United States (2021).

Implementation of the Digital COVID-19 Vaccination Passport based on Blockchain Protecting Privacy

Abstract: The paper discusses proposals for implementing the COVID-19 digital Vaccination Passport based on Blockchain that protects privacy. Since the end of the last year, after the commencement of vaccination against COVID-19, there has been an intense discussion on the form of introducing such a tool and the consequences of its implementation. This discussion is taking place in many European countries. One element of this discussion was the safety and anonymity of the massively verified data of persons on vaccinations in various areas of society functioning. These issues are being resolved by the proposed digital Vaccination Passport system. This system uses two major methods: Blockchain and hash functions, which allow you to maintain security, privacy, and anonymity at the same time. To improve the intuitiveness and simplicity of the system operation, the QR code technology was proposed in the passport verification process. The system has been implemented and tested in the Amazon AWS cloud computing environment. A reference architecture based on Blockchain for the AWS environment was proposed, dedicated to large and demanding application solutions. In addition, the cloud environment offers access to many tools that were used in the system's implementation, significantly increasing the security of the entire solution.

Keywords: Blockchain, cloud computing, Vaccination Passport, COVID-19, Decision Support Systems, e-health

dr inż. Przemysław Pukocz
pukocz@agh.edu.pl
ORCID: 0000-0002-0702-5505

Absolwent Akademii Górniczo-Hutniczej w Krakowie w dyscyplinie informatyka. Stopień naukowy doktora nauk technicznych w dyscyplinie informatyka uzyskał w 2017 r. w macierzystej uczelni na Wydziale Elektrotechniki, Automatyki, Informatyki i Inżynierii Biomedycznej. Pracuje na stanowisku asystenta w Katedrze Automatyki i Robotyki AGH. W swoich pracach badawczych zajmuje się rozwiązaniami chmur obliczeniowych, systemami wspomagania decyzji ze szczególnym uwzględnieniem metod optymalizacji wielokryterialnej.