Blockchain i sztuczna inteligencja w ochronie danych: bezpieczne przechowywanie i analiza

Wypracowanie naukowe autor Marcin Niedopytalski 2.09.2024 Katowice

Technologie takie jak blockchain i sztuczna inteligencja (SI) na stałe zagościły w dyskusjach naukowych i biznesowych, szczególnie w kontekście bezpieczeństwa danych. W dobie przyspieszonej cyfryzacji i rosnącej liczby zagrożeń w cyberprzestrzeni, pytanie o to, jak zapewnić skuteczną ochronę i anonimowość użytkowników, staje się absolutnie kluczowe. Jako Marcin Niedopytalski, badacz zafascynowany tą tematyką, staram się od lat obserwować, analizować i wdrażać rozwiązania z pogranicza obu tych światów blockchain oraz SI. W niniejszym wypracowaniu chciałbym przybliżyć zarówno teoretyczne podstawy, jak i praktyczne zastosowania technologii blockchain w połączeniu ze sztuczną inteligencją, skoncentrowane wokół ochrony danych. Postaram się także wskazać potencjalne zagrożenia oraz wyzwania, które czekają na nas w nadchodzących latach w tej dynamicznie rozwijającej się dziedzinie. Na pierwszy rzut oka blockchain i sztuczna inteligencja zdają się należeć do zupełnie różnych obszarów informatyki. Blockchain kojarzy się przede wszystkim z krypto walutami, kontraktami inteligentnymi (smart contracts) i rozproszonym rejestrem, który trudno sfałszować. Z kolei sztuczna inteligencja łączy się z algorytmami uczenia maszynowego, przetwarzania języka naturalnego czy rozpoznawania obrazów. Jednak przy bliższym przyjrzeniu się obu koncepcjom łatwo zauważyć, że mogą się one doskonale uzupełniać.
Z jednej strony blockchain zapewnia bezpieczne, rozproszone środowisko przechowywania danych. Mechanizm ten chroni przed nieuprawnionymi modyfikacjami czy wyciekiem informacji. Z drugiej strony sztuczna inteligencja wymaga ogromnych ilości danych do efektywnego uczenia się i wnioskowania. Zastosowanie tych dwóch technologii łącznie otwiera więc nowe możliwości: możemy nie tylko bezpiecznie magazynować informacje, ale także dokonywać zaawansowanych analiz w czasie rzeczywistym lub niemal w czasie rzeczywistym, w oparciu o zweryfikowane i niezmienne źródła danych. Aby zrozumieć, jak blockchain może wzmacniać bezpieczeństwo danych, warto przyjrzeć się jego fundamentalnym cechom. Blockchain to w dużym uproszczeniu rozproszona baza danych, która przechowuje informacje w blokach połączonych w łańcuch (stąd nazwa „łańcuch bloków. W

kontekście ochrony danych kluczowe jest to, że blockchain jest odporny na modyfikacje informacji: jeśli ktoś chciałby zmienić zawartość jednego bloku, musiałby w zasadzie podmienić wszystkie kolejne bloki. Ta cecha, w połączeniu z rozproszeniem rejestru wśród wielu niezależnych węzłów, chroni przed nieautoryzowanym dostępem oraz manipulacją. W efekcie blockchain oferuje nie tylko bezpieczeństwo, ale również przejrzystość i audyt owalność wszelkich operacji. Sztuczna inteligencja to dziedzina informatyki skupiająca się na tworzeniu systemów zdolnych do wykonywania zadań, które tradycyjnie wymagałyby ludzkiej inteligencji. W jej skład wchodzi uczenie maszynowe (machine learning), uczenie głębokie (deep learning), przetwarzanie języka naturalnego (NLP) czy systemy ekspertowe. W praktyce chodzi o budowanie modeli matematycznych, które potrafią rozpoznawać wzorce, dokonywać predykcji czy wyciągać wnioski z dużych zbiorów danych. Jednak aby sztuczna inteligencja mogła działać efektywnie, potrzebuje przede wszystkim obszernych i wiarygodnych zbiorów danych. Modele SI uczą się poprzez analizę przykładów im więcej i lepiej przygotowanych danych, tym większa szansa na uzyskanie trafnych rezultatów. Z tego powodu bezpieczeństwo i jakość danych mają tutaj priorytetowe znaczenie. Jeśli dane będą zafałszowane, niekompletne lub nieaktualne, to model SI też będzie generował błędne wnioski. Jednym z najbardziej oczywistych obszarów zastosowania blockchain w połączeniu ze sztuczną inteligencją jest zapewnienie wysokiego poziomu wiarygodności danych, na których trenują się modele SI. Wyobraźmy sobie, że mamy rozproszony rejestr, do którego różne instytucje, firmy czy organizacje publiczne wpisują informacje na przykład dane medyczne, dane finansowe czy informacje z sensorów IoT (Internetu Rzeczy). Dzięki mechanizmowi blockchain, każda transakcja (czyli każdy wpis) jest potwierdzana i opatrzona znacznikiem czasu. Jakakolwiek późniejsza próba modyfikacji tych danych jest ekstremalnie utrudniona. Z punktu widzenia sztucznej inteligencji takie podejście oznacza, że mamy do dyspozycji gwarantowane, niezmienne źródło informacji, na podstawie którego możemy uczyć modele. Dodatkowo, korzystając z inteligentnych kontraktów (smart contracts), można projektować systemy, w których dane są przekazywane dalej wyłącznie wtedy, gdy spełnione zostaną określone warunki bezpieczeństwa. Przekłada się to na wyeliminowanie ryzyka manipulacji wejściowymi danymi, co w efekcie wpływa na lepszą jakość analiz i predykcji. Wyobraźmy sobie szpital, w którym codziennie generowane są tysiące plików dokumentacji pacjentów. Informacje te zawierają wrażliwe dane: historię choroby, wyniki badań, szczegółowe zapisy parametrów

życiowych. Każda nieautoryzowana ingerencja może doprowadzić do poważnych skutków, nie tylko w sferze prywatności, ale także bezpieczeństwa zdrowotnego. Blockchain pozwala w takiej sytuacji na stworzenie niezamienialnej bazy danych o stanie pacjentów, do której dostęp mogą mieć jedynie uprawnione osoby. Co więcej, jeśli wdrożymy moduły SI do analizy tych danych, możemy z czasem opracować systemy wspomagające diagnozę albo sugerujące lekarzom optymalne terapie. Dzięki temu model SI nie tylko znajduje praktyczne zastosowanie w optymalizacji procesu leczenia, ale jednocześnie działa na zbiorze możliwie najbardziej wiarygodnych informacji – wolnych od potencjalnych manipulacji czy błędów powstałych podczas przepisywania danych między różnymi systemami. Kolejnym przykładem synergii blockchain i SI jest możliwość analizowania danych w czasie rzeczywistym. W tradycyjnym modelu przetwarzania informacji, zanim dane trafią do hurtowni czy narzędzia analitycznego, często mija sporo czasu, przez co wyniki stają się nieaktualne. Blockchain, dzięki temu, że rozproszony rejestr działa wielokierunkowo, pozwala na bieżące wprowadzanie nowych transakcji. Sztuczna inteligencja może „zasysać" te informacje i w niemal natychmiastowym tempie przeprowadzać analizę, na przykład wykrywać anomalie czy przewidywać trendy. Przykład z sektora finansowego: bank wykorzystuje blockchain do bezpiecznego zapisu transakcji klientów, a moduł SI bada wzorce podejrzanych zachowań, typowych dla prób wyłudzeń czy prania pieniędzy. Dzięki automatyzacji i szybkiemu dostępowi do danych w rejestrze, można szybko wyłapać transakcje niespełniające wybranych kryteriów bezpieczeństwa. W efekcie istotnie poprawia się skuteczność przeciwdziałania nadużyciom. Jednym z najczęściej dyskutowanych wyzwań w kontekście blockchain jest pogodzenie prywatności danych z transparentnością, jaka jest wpisana w strukturę łańcucha bloków. Z jednej strony blockchain jest przejrzysty i każdy węzeł w sieci może weryfikować transakcje. Z drugiej strony mamy często do czynienia z danymi poufnymi (np. finansowymi, medycznymi), które nie powinny być jawne dla osób postronnych.

Sposobem na rozwiązanie tego dylematu może być zastosowanie różnego rodzaju technologii kryptograficznych, takich jak „zerowe dowody wiedzy" (zero-knowledge proofs, ZKP) czy anonimizacja danych. Dzięki nim możliwe jest udowodnienie pewnego faktu (np. że dana transakcja jest poprawna), bez ujawniania pełnej treści zapisanych w niej informacji. Tutaj pojawia się również rola sztucznej inteligencji, która potrafi rozpoznawać wzorce czy dokonywać klasyfikacji na danych „zanonimizowanych", jeśli tylko zostaną one odpowiednio przetworzone. Daje to

szansę na łączenie bezpieczeństwa i prywatności z jednoczesną audytowalnością. Choć idea połączenia blockchain i SI brzmi niezwykle obiecująco, w praktyce wdrożenia nastręczają wielu trudności. Po pierwsze, rozmiar danych jeśli chcemy przechowywać duże pliki (np. medyczne skany) bezpośrednio w łańcuchu bloków, możemy szybko doprowadzić do przeładowania sieci i wzrostu kosztów transakcji. Dlatego często stosuje się hybrydowe podejście: dane przechowuje się w zaszyfrowanym magazynie (np. w chmurze), a w blockchain zapisuje się jedynie ich skróty (hash).
Po drugie, wydajność klasyczne blockchain, takie jak Bitcoin, mają ograniczoną przepustowość transakcji (kilka do kilkunastu na sekundę). Przy projektach biznesowych, gdzie kluczowy jest wysoki throughput, może to być niewystarczające. Z kolei sieci o większej przepustowości, takie jak niektóre nowsze łańcuchy (np. Solana), wymagają jeszcze szerokiej ewaluacji stabilności. Dopiero właściwy dobór infrastruktury i mechanizmów konsensusu pozwala na zrównoważenie bezpieczeństwa, skalowalności i decentralizacji. W dobie postępującej cyfryzacji coraz większą uwagę zwraca się na aspekty etyczne związane z technologiami cyfrowymi. W przypadku blockchain chodzi przede wszystkim o to, by nie zamieniać przejrzystości w masową inwigilację. Owszem, dane mogą być jawne, ale to nie znaczy, że każdy powinien mieć wgląd w szczegóły transakcji prywatnych osób czy firm. Jeżeli chodzi o sztuczną inteligencję, to kwestią sporną stały się możliwe nadużycia związane z profilowaniem użytkowników, automatyczną dyskryminacją w algorytmach czy manipulacją opinią publiczną (np. przez ukierunkowaną reklamę polityczną). W projekcie łączącym blockchain i SI należy więc zadbać o odpowiednie mechanizmy nadzoru, ramy prawne oraz transparentne zasady działania. Konieczne jest wprowadzanie audytów algorytmów SI i kontrola jakości danych wprowadzanych do blockchain, aby zminimalizować ryzyko systemowych błędów. Kolejnym czynnikiem spowalniającym adaptację technologii blockchain z komponentami SI są niejednoznaczne regulacje prawne. Przykładowo, w Unii Europejskiej obowiązuje RODO (Rozporządzenie o Ochronie Danych Osobowych), które nakłada określone wymagania dotyczące przetwarzania danych osobowych. Blockchain, ze swoją niezmienialnością, może wchodzić w konflikt z ideą „prawa do bycia zapomnianym”. Organizacje międzynarodowe, takie jak ISO (International Organization for Standardization), pracują nad stworzeniem standardów dla technologii rozproszonych rejestrów (DLT). Wraz z rozwojem SI pojawiają się też projekty tworzenia wytycznych dla sztucznej inteligencji (np. w zakresie etyki czy bezpieczeństwa). Dla wszystkich, którzy chcą

projektować systemy łączące te rozwiązania, pozostaje więc trzymać rękę na pulsie i reagować na bieżące zmiany w prawie oraz standardach. Sektor publiczny coraz chętniej spogląda w stronę blockchain i SI. Na przykładzie Estonii widać, jak można skutecznie wdrażać cyfrowe rozwiązania. Rejestrowanie dokumentów obywateli w technologii blockchain pozwala tam na błyskawiczną weryfikację i zmniejsza ryzyko oszustw. Dodanie warstwy SI mogłoby dać kolejne korzyści: np. przy analizie zapotrzebowania na usługi społeczne czy przewidywaniu trendów demograficznych. Jednak wdrożenie takich rozwiązań wymaga stabilnej infrastruktury i dobrze przemyślanej architektury bezpieczeństwa. Trzeba również rozwiązać potencjalne problemy natury politycznej i społecznej: np. czy społeczeństwo zaufa algorytmom podejmującym decyzje administracyjne? Jakie mechanizmy kontroli można wprowadzić, aby zapobiec nadużyciom i zachować zaufanie społeczne? Dyskusja na te tematy toczy się obecnie w wielu krajach, a jej wynik zadecyduje o przyszłości wdrożeń blockchain i SI w sektorze publicznym. Z punktu widzenia biznesu, technologie łączące blockchain i SI mogą stać się poważną przewagą konkurencyjną. Firmy, które zainwestują w zapewnienie wysokiego bezpieczeństwa danych i jednocześnie będą potrafiły szybko wyciągać trafne wnioski z dostępnych informacji, mogą usprawnić procesy, zredukować koszty i budować nowe modele biznesowe. Przewiduje się, że w ciągu najbliższych kilku lat pojawi się coraz więcej platform ułatwiających wdrażanie takich rozwiązań – zarówno na poziomie chmury obliczeniowej (cloud), jak i dedykowanych infrastruktur typu blockchain-as-a-service. Wiodące korporacje technologiczne, ale też innowacyjne startupy, będą się koncentrować na takich zagadnieniach jak skalowalność, interoperacyjność czy bezpieczeństwo. Kwestie związane z analizą big data staną się jeszcze ważniejsze, bo przepływ informacji będzie przyspieszał, a rola automatyzacji wzrośnie wraz z popularyzacją Internetu Rzeczy. Bez względu na to, jak obiecujące są technologie, w grę zawsze wchodzi czynnik ludzki i potrzeba odpowiedniego przygotowania społeczeństwa. Blockchain, ze względu na swój stopień złożoności, bywa dla przeciętnego użytkownika czymś wręcz magicznym: łańcuchy bloków, mechanizmy konsensusu, portfele kryptowalut to wszystko wymaga wyjaśnień i zrozumienia. Z kolei sztuczna inteligencja bywa postrzegana jako technologia przyszłości, która może człowieka zastąpić w wielu zawodach, budząc tym samym obawy i niepokój. Jednak, zamiast bać się tych zmian, powinniśmy patrzeć na nie przez pryzmat szans. Dlatego kluczową rolę odgrywa edukacja i to zarówno na poziomie specjalistycznym (inżynierskim, programistycznym), jak i społecznym.

Konieczne jest wprowadzenie do szkół i na uczelnie przedmiotów ukazujących praktyczne zastosowania zarówno blockchain, jak i AI, a także dbanie o zrozumiały przekaz w mediach. Tylko wtedy możemy uniknąć rosnącej polaryzacji gdy jedni będą maniakalnie zachwyceni technologicznym progresem, a inni całkowicie go odrzucą z powodu niewiedzy i lęku. Jako osoba naukowo zaangażowana w badania nad rozwiązaniami łączącymi blockchain i SI, widzę ogromną potrzebę zintensyfikowania działań na polu międzysektorowej współpracy. Uniwersytety, instytuty badawcze, firmy technologiczne oraz organy regulacyjne powinny coraz częściej pracować ramię w ramię, aby wypracowywać optymalne standardy i protokoły bezpieczeństwa. Inicjatywy typu hackathony, konkursy na najlepsze rozwiązania i platformy współpracy mogą przyspieszyć proces wymiany doświadczeń oraz promować innowacyjność.
Z perspektywy naukowca niezwykle ważne jest też publikowanie wyników badań w otwartym dostępie (open access) tak, aby społeczność miała szansę je weryfikować, rozwijać i aplikować w praktyce. Dzięki temu możemy uniknąć wyścigu rozwiązań „zamkniętych" i niekompatybilnych ze sobą. Transparentność i otwarta współpraca są szczególnie ważne w dziedzinie, w której bezpieczeństwo danych i prywatność użytkowników mogą wpływać na stabilność całych instytucji i gospodarek.
Technologie blockchain i sztuczna inteligencja niewątpliwie wpłyną na przyszłość cyfrowego świata, zwłaszcza w obszarze ochrony danych i zaawansowanej analizy. Synergia tych dwóch podejść tworzy fundament dla systemów, w których przechowywane informacje są nie tylko bezpieczne i trudne do sfałszowania, ale również natychmiast gotowe do automatycznej analizy. Jednak droga od pomysłów do masowych wdrożeń nie jest usłana różami. Czekają nas wyzwania natury regulacyjnej, technicznej i etycznej, które musimy rozwiązać, by w pełni wykorzystać potencjał tych rozwiązań. Z mojej perspektywy, kluczowym elementem wprowadzającym zmiany na lepsze będzie edukacja i szerzenie świadomości na temat możliwości i ograniczeń blockchain i SI. Ważne jest, by koncentrować się nie tylko na aspektach technologicznych, ale też humanistycznych: zadawać pytania o to, komu służą te rozwiązania, jakie wartości promują, jak wpłyną na relacje społeczne i gospodarcze. Tylko takie holistyczne spojrzenie da nam gwarancję, że nowe technologie będą wykorzystywane w sposób odpowiedzialny i przyniosą pozytywne skutki zarówno dla jednostek, jak i całej ludzkości. Mam nadzieję, że przedstawiona analiza pomogła ukazać, jak istotne i zarazem fascynujące jest połączenie technologii blockchain ze sztuczną inteligencją w celu ochrony danych, ich bezpiecznego przechowywania i

zaawansowanej analizy. W nadchodzących latach możemy się spodziewać dalszego rozwoju innowacji w tym zakresie, a także powstawania nowych inicjatyw, w których połączą się najlepsze cechy obu światów. Pozostaje tylko czekać (i aktywnie działać), abyśmy wszyscy mogli korzystać z owoców tej technologicznej rewolucji w sposób etyczny, przejrzysty i korzystny dla społeczeństwa. W miarę jak technologia blockchain dojrzewa, a narzędzia sztucznej inteligencji stają się coraz bardziej wyrafinowane, obserwujemy pojawianie się kolejnych możliwości integracji obu światów. W mojej dotychczasowej analizie skoncentrowałem się głównie na temacie bezpieczeństwa danych, niemniej warto nakreślić też szerszy obraz przyszłości. Ostatnie lata przyniosły wiele inspirujących koncepcji, które mają szansę w niedalekiej perspektywie ukształtować cały ekosystem usług cyfrowych w gospodarce, administracji publicznej i życiu codziennym. Przede wszystkim, na naszych oczach dokonuje się rewolucja w zakresie wydajności rozwiązań blockchainowych. Jeszcze niedawno kluczowym zarzutem wobec pierwszej generacji łańcuchów bloków (np. sieci Bitcoin) była stosunkowo niska przepustowość oraz wysokie zużycie energii. Obecnie rozwijane są protokoły o znacznie wyższej skalowalności, korzystające z mechanizmów konsensusu takich jak Proof of Stake (PoS), Delegated Proof of Stake (DPoS) czy inne hybrydowe metody. Każde z tych rozwiązań stara się równoważyć trzy najważniejsze elementy: decentralizację, bezpieczeństwo i skalowalność. Z perspektywy AI jest to o tyle istotne, że pozwala na szybszy dostęp do danych zapisanych na blockchain, co ułatwia ich przetwarzanie w czasie rzeczywistym. Z perspektywy postępu naukowego zwraca się też coraz większą uwagę na wykorzystanie tzw. sieci warstwy drugiej. Przykładem mogą być rozwiązania typu state channels czy sidechainy, które przenoszą znaczną część obliczeń poza główny łańcuch bloków, zachowując przy tym bezpieczeństwo i niezmienność bazowego rejestru. Dla systemów AI oznacza to możliwość nie tylko szybkiego odczytu, ale także szybkich zapisów i mniejszego obciążenia podstawowego łańcucha. To z kolei stwarza grunt pod dalszy rozwój złożonych aplikacji, w których algorytmy machine learning mogą nauczyć się sprawniej wykrywać nieprawidłowości, prognozować trendy czy nawet wykonywać złożone zadania decyzyjne w czasie zbliżonym do rzeczywistego. Choć blockchain, w połączeniu z AI, ma ogromny potencjał, wciąż nie możemy mówić o pełnej interoperacyjności pomiędzy różnymi łańcuchami czy platformami. Obecny ekosystem przypomina nieco wczesne lata rozwoju internetu mamy wiele „wysp” technologicznych, które potrafią sprawnie działać we własnych granicach, ale wymiana danych pomiędzy nimi bywa utrudniona.

W przypadku AI interoperacyjność jest szczególnie ważna, ponieważ modele uczenia maszynowego często muszą sięgać do różnych źródeł danych. W praktyce oznacza to potrzebę standaryzacji API (interfejsów programistycznych), protokołów komunikacji oraz formatów danych. Dopiero gdy różne łańcuchy bloków będą w stanie efektywnie „rozmawiać" ze sobą za pośrednictwem specjalnych mostów (tzw. bridges) albo wspólnych warstw, modele AI będą mogły wykorzystywać zasoby całego ekosystemu, a nie tylko pojedynczych projektów. Są już obiecujące inicjatywy, takie jak Cosmos czy Polkadot, które dążą do tego, by blockchain mogły współistnieć i korzystać z dobrodziejstw decentralizacji. Rozwiązania te oferują mechanizmy łączące różne łańcuchy w sieć sieci. W dalszej perspektywie, gdy te koncepcje wejdą w fazę dojrzałości, może się okazać, że powstanie globalny ekosystem, w którym sztuczna inteligencja będzie czerpać z praktycznie nieograniczonych źródeł niezmiennych, wiarygodnych danych. Rosnąca popularność blockchain, zwłaszcza w kontekście kryptowalut, wywołała dyskusję na temat zużycia energii. Krytyka pod adresem mechanizmów takich jak Proof of Work (stosowanego w Bitcoinie) jest uzasadniona, bo rzeczywiście wymaga on sporej mocy obliczeniowej. Z kolei systemy AI również nie są wolne od zarzutu o duże zapotrzebowanie na energię i zasoby sprzętowe szczególnie gdy mówimy o trenowaniu zaawansowanych modeli głębokiego uczenia (deep learning). Z tego powodu coraz częściej mówi się o potrzebie zrównoważonego podejścia do rozwiązań łączących blockchain i AI. W praktyce oznacza to poszukiwanie alternatywnych metod konsensusu, wspomnianych już mechanizmów PoS, jak również zastosowanie energooszczędnych algorytmów uczenia maszynowego. Pojawiają się też inicjatywy typu „green NFT", które promują tworzenie i handel tokenami w sieciach o niskim zużyciu energii. W kontekście AI próbuje się m.in. ograniczać rozmiar modeli, stosować optymalizacje w chmurze czy wykorzystywać hardware dedykowany (procesory GPU i TPU), który może wykonywać obliczenia w bardziej efektywny sposób. Kolejny ważny wątek to recykling danych. Sztuczna inteligencja – co do zasady – uczy się na dużych zestawach informacji. Jednak nie wszystkie muszą być wykorzystywane jednocześnie czy przechowywane wiecznie. Racjonalne podejście do retencji danych, określenie warunków ważności oraz mądre gospodarowanie miejscem w łańcuchu bloków mogą znacznie zredukować „ślad węglowy" takich projektów. Z perspektywy użytkowników i firm wprowadzenie zasad zrównoważonego rozwoju staje się też kwestią wizerunkową, bo coraz więcej osób zwraca uwagę na aspekt ekologiczny przy wyborze usług cyfrowych. Jednym z ciekawszych trendów, w którym

blockchain może odegrać istotną rolę, jest koncepcja rozproszonego uczenia maszynowego (federated learning) oraz edge computing. Zamiast gromadzić wszystkie dane w centralnym miejscu (np. w chmurze), można trenować modele AI lokalnie, na urządzeniach brzegowych (smartfony, czujniki IoT, kamery przemysłowe), a następnie łączyć wnioski bez przesyłania całości surowych danych do serwera. Blockchain może tu posłużyć jako rodzaj „rejestru zaufania" gwarantując niezmienność i transparentność procesu aktualizacji modelu. Każde urządzenie brzegowe, zanim prześle wytrenowane parametry sieci neuronowej, może opatrzyć je cyfrowym podpisem i zapisem w rozproszonym łańcuchu, dzięki czemu wszyscy uczestnicy federacji mają pewność co do pochodzenia i integralności danych. Tego typu rozwiązania są szczególnie wartościowe w branży medycznej (gdzie wrażliwe informacje o pacjentach pozostają na miejscu, a do chmury trafiają tylko wnioski statystyczne), branży automotive (samochody autonomiczne uczą się w trakcie jazdy, dzieląc się wiedzą na temat sytuacji drogowych) czy w systemach inteligentnych miast (analiza danych z kamer miejskich czy sensorów jakości powietrza). Zaletą takiego podejścia jest m.in. lepsza ochrona prywatności, ponieważ surowe dane nie opuszczają urządzenia, oraz poprawa skalowalności, bo nie tworzy się jednego gigantycznego, scentralizowanego zbioru informacji. Minusem może być potrzeba większej mocy obliczeniowej na urządzeniach brzegowych oraz potencjalnie wolniejszy czas trenowania modelu. Niemniej jednak, w połączeniu z blockchainem, federated learning i edge computing otwierają drogę do nowych, zdecentralizowanych aplikacji SI, w których bezpieczeństwo i prywatność stawia się na pierwszym miejscu. Wspominałem już o tym, że inteligentne kontrakty (smart contracts) mogą odpowiadać za automatyczne przekazywanie danych do analizy przez moduły SI. Warto jednak zwrócić uwagę na to, że ten mechanizm może mieć znacznie szersze zastosowanie w automatyzacji procesów biznesowych i społecznych. Smart contract to nic innego jak program uruchamiany w sieci blockchain, który w sposób deterministyczny wykonuje określone operacje po spełnieniu warunków zapisanych w kodzie. W połączeniu z SI, taki kontrakt mógłby samodzielnie decydować o zakupie odpowiednich danych, jeżeli uzna, że są one niezbędne do usprawnienia modelu (oczywiście w granicach budżetu i parametrów ustalonych przez człowieka). Może też wywoływać kolejne operacje, np. przesyłać wyniki analizy do innego kontraktu, który odpowiada za weryfikację jakości tych wyników, a następnie dystrybuować tokeny do uczestników, którzy dostarczyli wartościowych danych. Dzięki temu powstają samoorganizujące się ekosystemy, w których sztuczna inteligencja

współdziała z ludźmi i maszynami w modelu peer-to-peer. Taka wizja rodzi pytania natury prawnej i etycznej. Czy i w jakim zakresie automatyczne transakcje przeprowadzane przez SI powinny być regulowane? Jak zadbać o odpowiedzialność za błędne decyzje algorytmów, skoro pewien etap obsługi umowy przejęły inteligentne kontrakty działające na blockchainie? To kwestie, które prędzej czy później znajdą się na agendzie organów regulacyjnych i sądów, a także staną się przedmiotem ożywionej debaty w środowiskach naukowych. W dyskusjach o przyszłości blockchain i AI coraz częściej pojawia się temat komputerów kwantowych (quantum computing). Z punktu widzenia kryptografii stanowią one potencjalne zagrożenie, ponieważ część algorytmów, na których opiera się bezpieczeństwo blockchain, może być w przyszłości łamana przez odpowiednio silne komputery kwantowe. Za najbardziej narażone uważa się obecne standardy kryptografii asymetrycznej (RSA, ECDSA), kluczowe dla podpisów cyfrowych i zabezpieczenia transakcji. Z drugiej jednak strony, komputery kwantowe oferują też zupełnie nowy poziom mocy obliczeniowej, co może przynieść bezprecedensowe przyspieszenie w dziedzinie sztucznej inteligencji. Trening złożonych modeli głębokiego uczenia, analiza dużych zbiorów danych czy optymalizacja procesów to wszystko może zostać znacznie usprawnione przez technologie kwantowe. Jednym z wyzwań będzie zatem opracowanie „post-quantum" algorytmów kryptograficznych, aby blockchain pozostał bezpieczny, przy jednoczesnym wykorzystaniu korzyści płynących z kwantowej mocy obliczeniowej dla SI. Już teraz trwają badania i standardyzacja rozwiązań odpornych na ataki kwantowe (tzw. PQC Post-Quantum Cryptography). Kilka firm oraz instytucji akademickich pracuje nad wdrożeniem w blockchain nowych typów podpisów cyfrowych oraz protokołów konsensusu uwzględniających potencjalne ataki kwantowe. Także w obszarze AI tworzone są eksperymentalne algorytmy kwantowo-klasyczne (hybrid quantum-classical algorithms), które w przyszłości mogą działać w symbiozie z rozproszonymi bazami danych. Niezależnie od rozwoju technologii i zachęcających perspektyw, kluczowym elementem powodzenia wprowadzania innowacyjnych rozwiązań jest zaufanie społeczne. To temat, który podejmowałem wcześniej, ale warto go dodatkowo rozszerzyć. Społeczeństwo często obawia się nowych technologii AI postrzegana jest jako coś, co może prowadzić do masowych zwolnień czy wręcz przejęcia kontroli nad ludzkim życiem, zaś blockchain kojarzony bywa z nieprzejrzystym obszarem kryptowalut i ryzykiem inwestycyjnym. Właśnie dlatego tak ważna jest powszechna edukacja na temat podstawowych zasad działania obu tych dziedzin. Już w szkołach i

na wczesnych etapach kształcenia warto wprowadzać elementy informatyki i logiki, by kolejne pokolenia lepiej rozumiały, w jaki sposób działa sztuczna inteligencja, jakie są jej mocne i słabe strony, a także czym są klucze kryptograficzne, hash i czym różni się scentralizowana baza danych od blockchaina. Na poziomie akademickim z kolei należy kłaść większy nacisk na interdyscyplinarność: studenci prawa powinni mieć styczność z tematyką AI i blockchainu, inżynierowie z wiedzą socjologiczną czy psychologiczną, natomiast ekonomiści z technologicznymi podstawami rejestrów rozproszonych. Wielką rolę odgrywają też media i liderzy opinii. To, w jaki sposób przekazują informacje o zagrożeniach i korzyściach płynących z technologii, wpływa na postawy ogółu. Transparentność w komunikacji, pokazywanie konkretnych przykładów zastosowań (zwłaszcza tych, które rzeczywiście ułatwiają codzienne życie) oraz otwarta dyskusja o ryzyku pozwalają budować świadome społeczeństwo. A tylko takie jest w stanie w pełni wykorzystać potencjał blockchainu i AI, unikając pułapek nieodpowiedzialnego wdrażania lub radykalnego odrzucenia nowości. Praktyczne wdrożenia technologii blockchain i AI wymagają dobrej strategii, która uwzględnia zarówno aspekty techniczne, jak i organizacyjne, finansowe oraz kulturowe. Z moich doświadczeń i obserwacji wynika, że kluczowe jest podejście ewolucyjne zamiast wdrażać skomplikowany system od razu na szeroką skalę, lepiej zacząć od pilotażu w wybranych obszarach biznesu czy administracji. Dzięki temu można zweryfikować realne korzyści, zidentyfikować problemy i stopniowo skalować rozwiązanie. Nie zawsze blockchain i SI będą najbardziej odpowiednim narzędziem. W niektórych sytuacjach tradycyjne bazy danych czy klasyczne metody analizy mogą w pełni wystarczyć. Dlatego tak ważne jest, by najpierw precyzyjnie określić, jakie cele chcemy osiągnąć i jakie mamy problemy do rozwiązania. Na rynku istnieje wiele blockchainu (Ethereum, Hyperledger Fabric, Polkadot, Tezos, Solana, Avalanche i inne), różniących się sposobem konsensusu, szybkością, kosztami transakcji, poziomem dojrzałości ekosystemu. Decyzja o wyborze konkretnej sieci często determinuje sukces projektu. Wdrożenie blockchainu musi iść w parze ze spełnieniem wymagań prawnych (np. RODO), zwłaszcza gdy mamy do czynienia z danymi osobowymi. Konieczne może być też wdrożenie mechanizmów anonimizacji, szyfrowania i zarządzania kluczami kryptograficznymi. AI wymaga dużej ilości danych i mocy obliczeniowej. Odpowiednia architektura powinna przewidywać, gdzie fizycznie będą przechowywane dane (on-chain czy off-chain), jak będą przesyłane do narzędzi analitycznych i jak wyniki będą wprowadzane z powrotem do blockchainu (np. w postaci zapisów w inteligentnym

kontrakcie). Udana implementacja wymaga specjalistów od blockchainu, kryptografii, projektowania smart kontraktów, a także ekspertów od AI (data scientists, inżynierów uczenia maszynowego). Ponadto konieczna jest współpraca z prawnikami oraz ekspertami ds. ochrony danych. Bardzo często o sukcesie decydują czynniki miękkie, takie jak akceptacja użytkowników końcowych, odpowiednie przeszkolenie pracowników, a także komunikacja celów i korzyści. Blockchain i AI potrafią zmieniać istniejące procesy dość radykalnie, co może budzić opór w organizacji. Patrząc w perspektywie 5–10 lat, można wyobrazić sobie kilka scenariuszy rozwoju technologii łączących blockchain i AI. Dochodzi do powszechnej standaryzacji i uproszczenia technologii blockchain, powstają platformy typu „plug and play", w których nawet mniejsze podmioty bez ogromnych nakładów finansowych mogą wdrażać zaawansowane systemy rozproszone. AI staje się „commodity" w wielu sektorach, a dzięki interoperacyjności łańcuchów i jakości danych, algorytmy coraz trafniej pomagają w kluczowych decyzjach społecznych i biznesowych. Społeczeństwo zyskuje, bo pojawiają się innowacyjne usługi zdrowotne, finansowe czy edukacyjne, oparte na transparentnych i bezpiecznych mechanizmach rozliczeń. Technologia rozwija się w różnych niszach i sektorach. Część branż (np. finanse, logistyka) osiąga wysoki poziom automatyzacji i decentralizacji, ale inne (np. administracja publiczna w krajach mniej rozwiniętych) zostają w tyle ze względu na brak odpowiedniej infrastruktury i regulacji. Blockchain i AI funkcjonują, jednak ich możliwości nie są w pełni zintegrowane na globalną skalę. Wciąż dochodzi do wycieków danych i incydentów cyberbezpieczeństwa, ale w mniejszej skali niż obecnie. Rozwiązania oparte na blockchainie i AI stają się domeną wąskiej grupy gigantów technologicznych, którzy narzucają własne standardy i kontrolują kluczowe zasoby informacyjne. Dochodzi do podziału świata na sfery wpływów dużych graczy, rośnie ryzyko monopolizacji, a brak transparentności w niektórych wdrożeniach SI wywołuje społeczne konflikty i obawy. Zaufanie do technologii spada, co skutkuje zaostrzonymi regulacjami i hamuje dalszy rozwój innowacji. Naturalnie, rzeczywistość jest zwykle bardziej złożona i nie musi idealnie wpisywać się w żaden z powyższych scenariuszy. Niemniej warto je rozpatrywać jako „punkty orientacyjne", które pozwalają nam zrozumieć możliwe konsekwencje decyzji podejmowanych dziś przez rządy, korporacje i społeczność naukową. Na zakończenie moich rozważań nie mogę nie podkreślić roli humanistyki cyfrowej i szeroko rozumianej etyki technologicznej. Zaawansowane systemy AI, oparte na blockchainie, coraz głębiej ingerują w naszą codzienność, relacje społeczne i

sposób funkcjonowania gospodarki. Wymaga to nie tylko wiedzy technicznej, ale też refleksji nad wartościami, jakie promuje ta cyfrowa rewolucja. Często powtarzam, że kluczowym pytaniem jest: *komu i czemu służą nowe technologie?* Czy blockchain i AI mają w pierwszej kolejności zwiększać zyski akcjonariuszy korporacji, czy też wspierać rozwój społeczny i ograniczać nierówności? Czy wprowadzamy je z myślą o dobrostanie człowieka, czy kierując się wyłącznie żądzą optymalizacji i kontroli?

Humanistyka cyfrowa to obszar, w którym łączy się perspektywa nauk społecznych, filozofii, etyki oraz wiedza o technologiach informacyjnych. Dzięki niemu możemy lepiej rozumieć wpływ cyfryzacji na kulturę i relacje społeczne. Coraz więcej uniwersytetów tworzy interdyscyplinarne zespoły badawcze, w których inżynierowie współpracują z antropologami, socjologami czy filozofami. Takie podejście wydaje mi się nie tylko pożądane, ale wręcz niezbędne, abyśmy mogli kontrolować kierunek, w jakim zmierzają globalne innowacje technologiczne. W kontekście AI i blockchainu pojawiają się też dylematy związane z wolną wolą, autonomią decyzji, własnością intelektualną czy prawami człowieka. Przykładowo: czy w pełni zautomatyzowany system oparty na łańcuchu bloków, który decyduje o przydziale świadczeń socjalnych, nie narusza przypadkiem godności i prywatności obywateli? Albo jak pogodzić prawo do zapomnienia (kasowania danych) z niezmiennością łańcucha bloków? To pytania, na które nadal nie ma ostatecznej odpowiedzi, a ich rozwiązanie wymaga debaty wykraczającej daleko poza świat wyłącznie technologiczny. Reasumując, dynamiczny rozwój technologii blockchain i sztucznej inteligencji niesie ze sobą ogromny potencjał i liczne szanse: od poprawy bezpieczeństwa danych, przez automatyzację procesów, aż po tworzenie zupełnie nowych modeli biznesowych i społecznych. Droga do pełnego wykorzystania tych możliwości usiana jest jednak wyzwaniami: natury prawnej, organizacyjnej, etycznej i stricte technicznej. Wraz z upływem czasu będą powstawać kolejne narzędzia i ramy regulacyjne, które ułatwią wdrażanie rozwiązań opartych na blockchainie. Sztuczna inteligencja będzie coraz lepiej rozumiała otoczenie, wychodząc poza analizę statystyczną i zaczynając choć brzmi to futurystycznie „myśleć" w kategoriach semantycznych. Nie oznacza to jednak, że możemy przyglądać się temu rozwojowi z boku. Każdy z nas, jako użytkownik internetu czy konsument usług cyfrowych, jest częścią ekosystemu i ma wpływ na kierunek innowacji. W mojej ocenie, najważniejsze staje się zachowanie równowagi między zyskiem a dobrostanem społecznym, między prywatnością a transparentnością, między centralizacją a decentralizacją. Technologia – choć pociągająca i innowacyjna jest tylko narzędziem.

Kluczowe zawsze będzie to, jak ludzie zdecydują się z niej korzystać. Czy posłuży nam do wzmocnienia struktur demokratycznych, zwiększenia sprawiedliwego dostępu do dóbr i usług, a może odwrotnie stanie się instrumentem nadzoru i kontroli? Jako Marcin Niedopytalski, mam nadzieję, że niniejsza kontynuacja rozważań jeszcze wyraźniej pokazała, jak wiele wątków i perspektyw obejmuje temat „Blockchain i sztuczna inteligencja w ochronie danych: bezpieczne przechowywanie i analiza". Zachęcam wszystkich do dalszego zgłębiania tej fascynującej dziedziny i aktywnego udziału w kształtowaniu przyszłości, w której blockchain i AI odegrają niewątpliwie jedną z kluczowych ról. Technologie blockchain i sztucznej inteligencji, coraz bardziej obecne w rozmaitych sektorach gospodarki, nadal kryją w sobie wiele nieoczywistych zastosowań. Pierwotne koncepcje takie jak kryptowaluty czy modele uczenia maszynowego – były tylko wierzchołkiem góry lodowej, która wciąż rośnie dzięki nowym odkryciom i ulepszeniom. W dalszej części tego opracowania przedstawiono kolejne, bardziej szczegółowe aspekty łączenia blockchainu z AI. Poruszono także wyzwania techniczne, ekonomiczne i społeczne, które należy brać pod uwagę, aby w pełni wykorzystać potencjał wynikający z synergii obu technologii. Jednym z często omawianych wyzwań przy wdrażaniu rozwiązań opartych na blockchainie jest kwestia prywatności. O ile transparentność łańcucha bloków pozwala na łatwy audyt i weryfikację transakcji, o tyle nie zawsze jest pożądane, by wszelkie informacje – szczególnie wrażliwe były widoczne dla całej sieci. Zero-Knowledge Proofs to narzędzia kryptograficzne, które umożliwiają udowodnienie określonego faktu (np. poprawności transakcji, posiadania odpowiednich uprawnień lub wystarczających środków) bez ujawniania dodatkowych informacji. Dzięki temu możliwe jest zachowanie prywatności tożsamości lub szczegółów transakcji przy jednoczesnym zachowaniu bezpieczeństwa i zaufania w łańcuchu bloków. W kontekście AI rozwiązania oparte na ZKP mogą służyć do przechowywania modeli bądź parametrów uczenia maszynowego w sposób, który nie narusza praw własności intelektualnej lub prywatności danych. Ciekawym kierunkiem jest też homomorficzne szyfrowanie, które pozwala wykonywać operacje matematyczne na zaszyfrowanych danych tak, aby wynik po odszyfrowaniu był tożsamy z wynikiem, jaki uzyskalibyśmy, operując na danych w formie jawnej. Z punktu widzenia AI oznacza to potencjalnie możliwość trenowania modeli machine learning bez bezpośredniego dostępu do surowych informacji (np. danych medycznych). Blockchain, jako rozproszona i niezmienna warstwa rejestracji

wyników, może tu zapewniać kontrolę nad przepływem zaszyfrowanych pakietów, zwiększając transparentność i eliminując ryzyko nadużyć.

Te dwa przykłady pokazują, jak technologie kryptograficzne mogą rozwijać się równolegle z blockchainem, wspierając go w ochronie prywatności, jednocześnie nie ograniczając możliwości wykorzystania danych w analizach sztucznej inteligencji. Pierwsze blockchainy, takie jak Bitcoin, wykorzystywały konsensus typu Proof of Work (PoW). Choć cechuje się on wysokim poziomem bezpieczeństwa, jest także energochłonny i stosunkowo wolny w przetwarzaniu wielu transakcji. Współczesne projekty blockchain coraz częściej sięgają po alternatywne mechanizmy, bardziej przyjazne środowisku i szybsze. Mechanizm PoS polega na tym, że walidatorzy zabezpieczają sieć, „blokując" pewną liczbę tokenów (stake). Im większy stake, tym większa szansa na wybór węzła do dodania kolejnego bloku. PoS zużywa mniej energii i jest wydajniejszy pod względem przepustowości. Dzięki temu lepiej nadaje się do zastosowań biznesowych lub naukowych, gdzie integracja z AI wymaga obsługi licznych i częstych zapisów w łańcuchu. Odmiana PoS, w której użytkownicy mogą delegować swoje tokeny na wybranych walidatorów (delegatów) ci zaś odpowiadają za generowanie bloków i utrzymywanie sieci. Rozwiązanie to jeszcze bardziej zwiększa wydajność, a jednocześnie daje społeczności pewien wpływ na skład walidatorów. Dla systemów AI obsługujących ogromne ilości danych ten mechanizm może okazać się kluczowy, bo pozwala zachować zdecentralizowany charakter sieci przy jednoczesnej optymalizacji przepustowości. Tutaj z kolei zaufanie opiera się na ograniczonej liczbie węzłów (autorytetów), co sprawdza się w sieciach prywatnych lub konsorcjach, gdzie uczestnicy dobrze się znają i muszą przestrzegać spisanych reguł. W połączeniu z AI bywa to przydatne w przypadkach, gdy kilka firm lub instytucji naukowych prowadzi wspólny projekt, a potrzeba zachować wysoki stopień prywatności i stabilności.

Wybór konsensusu powinien być zawsze podyktowany specyfiką projektu. W systemach analitycznych, naszpikowanych algorytmami uczenia maszynowego, liczy się zwłaszcza przepustowość i szybkość potwierdzania nowych bloków. Sztuczna inteligencja może działać wyłącznie w oparciu o dane, które otrzymuje z otoczenia. W przypadku blockchainu kluczową rolę pełnią tzw. oracles, czyli usługi zewnętrzne przekazujące dane ze świata „poza łańcuchem" (off-chain) do świata „wewnątrz łańcucha" (on-chain). Blockchain z definicji nie posiada wbudowanej „bramy" do zewnętrznych źródeł, ponieważ projektowano go tak, aby był systemem samowystarczalnym i odpornym na manipulacje. Oracles umożliwiają import danych

np. o kursach walut, wynikach sportowych czy temperaturze z czujników IoT. W kontekście AI, oracles mogą również przekazywać wyniki analiz obliczanych poza łańcuchem (np. w chmurze obliczeniowej), co pozwala aktualizować stan sieci lub wywoływać kolejne inteligentne kontrakty. Jeśli zostanie przejęty przez hakerów albo okaże się nierzetelny, to blockchain będzie przechowywał nieprawdziwe informacje, a AI bazująca na tych danych może generować błędne wnioski. Odpowiedzią na to zagrożenie jest replikacja oracles – korzystanie z wielu źródeł i mechanizmów konsensusu, które pozwalają określić, które dane są najbardziej wiarygodne. W dobie rosnącej liczby urządzeń IoT, oracles mogą pełnić też rolę pośredników między inteligentnymi sensorami a inteligentnymi kontraktami. Dzięki temu możliwe jest automatyczne wywoływanie akcji, gdy np. czujnik jakości powietrza wykryje przekroczenie dopuszczalnych norm. Dla algorytmów AI staje się to kopalnią bieżących danych, doskonałych do trenowania sieci neuronowych w czasie rzeczywistym. Blockchain pozwala nie tylko przechowywać informacje o transakcjach, ale także definiować własne tokeny stanowiące środki płatnicze, udziały lub formę gratyfikacji dla uczestników sieci. W połączeniu z AI ta funkcjonalność może być wykorzystana na wiele sposobów. Jednym ze sposobów na zachęcenie użytkowników do dostarczania jakościowych informacji do systemów AI jest wprowadzenie tokenów jako formy wynagrodzenia. Dzięki temu każdy, kto udostępni swoje dane (np. dotyczące stanu zdrowia, lokalizacji czy preferencji zakupowych), może otrzymać określoną liczbę tokenów. Blockchain służy tu jako mechanizm rozliczeniowy i rejestr transakcji potwierdzający, kto i kiedy wprowadził dane. Możliwe jest też tworzenie rynków zbytu dla samych modeli uczenia maszynowego. W takiej sytuacji AI staje się produktem, który można „spieniężyć" w formie tokenów. Przykładowo, firma A może wytrenować wysokiej klasy model do rozpoznawania obiektów na zdjęciach i wystawić go na zdecentralizowanym rynku. Firma B nabywa licencję dostępu, płacąc tokenami, a transakcja zostaje zapisana w blockchainie w sposób gwarantujący niezmienność i przejrzystość. W inteligentnych miastach lub systemach IoT kluczową rolę mogą odgrywać mikropłatności, np. za dostęp do danych w ograniczonym zakresie czasowym. Sztuczna inteligencja może samodzielnie decydować, jakie dane są jej potrzebne w danym momencie, i automatycznie opłacać dostęp przy użyciu tokenów blockchainowych. To otwiera drogę do w pełni autonomicznych ekosystemów, w których maszyny i algorytmy AI współpracują ze sobą, kupując i sprzedając zasoby bez udziału człowieka. Oprócz niezmienności i przejrzystości zapisu, blockchain oferuje

również bezpieczeństwo wynikające z rozproszonej architektury. Każdy węzeł sieci przechowuje kopię łańcucha bloków, co minimalizuje ryzyko całkowitej utraty danych. Dla systemów AI, które często potrzebują stabilnego zaplecza danych, jest to kluczowe. W tradycyjnych, scentralizowanych rozwiązaniach atak DDoS (Distributed Denial of Service) może zablokować dostęp do bazy danych lub systemu analitycznego. W przypadku dobrze zaprojektowanego blockchainu ryzyko to jest znacząco niższe, ponieważ nie ma jednego punktu awarii. Duże pliki (np. obrazy medyczne czy dane wideo) mogą być przechowywane poza łańcuchem, w tzw. zdecentralizowanych systemach plików (np. IPFS – InterPlanetary File System), a w blockchainie zapisuje się jedynie skróty (hash), co potwierdza integralność plików. AI ma więc pewność, że dane, do których sięga, nie zostały zmodyfikowane. Jeśli algorytm AI otrzymuje dane z wielu węzłów sieci blockchain, może je wzajemnie porównywać, wykrywając ewentualne rozbieżności. Mechanizmy konsensusu sprawiają, że większość węzłów musi zgodzić się co do poprawności danych jeżeli jakaś niewielka część zostanie zainfekowana lub zhakowana, trudno będzie im przełamać zgodę większości. W sektorze energetycznym blockchain i AI mogą wspólnie poprawić stabilność sieci, umożliwiając elastyczną regulację podaży i popytu. Blockchain może rejestrować wolumeny dostarczanej energii ze źródeł odnawialnych (np. panele słoneczne w gospodarstwach domowych). Sztuczna inteligencja analizuje dane w czasie rzeczywistym i prognozuje zapotrzebowanie na energię w danej okolicy, wywołując automatyczne transakcje typu peer-to-peer pomiędzy uczestnikami (kupno/sprzedaż nadwyżek energii). Efektywne zarządzanie danymi obywateli (np. dowodami osobistymi, prawem jazdy, rejestrami gruntów) wymaga pełnej wiarygodności i transparentności. Dzięki blockchainowi rejestry pozostają trudne do sfałszowania, a sztuczna inteligencja może na tej bazie przeprowadzać zaawansowane analizy, np. dotyczące planowania przestrzennego, zarządzania budżetem obywatelskim czy przewidywania przyszłych potrzeb społecznych (ochrona zdrowia, edukacja).

W logistyce łańcucha dostaw blockchain może zagwarantować niezmienność informacji dotyczących pochodzenia produktu, jego transportu czy warunków przechowywania. AI może zaś analizować wzorce popytu, identyfikować potencjalne problemy (np. opóźnienia, niezgodności w dokumentach) i automatycznie przekazywać ostrzeżenia czy rekomendacje menedżerom. Dodatkowo, analiza predykcyjna pomaga firmom lepiej zarządzać zapasami, redukując koszty magazynowania. Branża finansowa już w dużej mierze bazuje na algorytmach uczenia maszynowego (wycena ryzyka,

scoring kredytowy, wykrywanie nadużyć). Dodanie do tego warstwy blockchainu wzmacnia bezpieczeństwo i automatyzuje proces rozliczania transakcji. W dziedzinie ubezpieczeń (insurtech) możliwe jest projektowanie inteligentnych polis – wypłata świadczenia odbywa się w sposób automatyczny, gdy warunki zaprogramowane w smart kontrakcie zostaną spełnione (np. w przypadku zaistnienia zdarzenia zarejestrowanego w blockchainie przez oracles). Rosnące znaczenie economy powoduje zapotrzebowanie na platformy, które uczciwie i transparentnie pośredniczą w relacji między zleceniodawcą a wykonawcą. Blockchain może rejestrować wykonanie zadań i wypłaty wynagrodzeń, a AI – oceniać jakość pracy i dopasowywać freelancerów do projektów. Tokenizacja pozwala wprowadzić system nagród i reputacji, który sprzyja rzetelnym wykonawcom, jednocześnie minimalizując ryzyko oszustw. Połączenie blockchainu z AI nie ogranicza się wyłącznie do przechowywania danych i rejestracji transakcji. Istnieją także pomysły na przyspieszenie samego procesu uczenia maszynowego w środowisku rozproszonym. Dzięki blockchainowi możliwe jest tworzenie platform, na których użytkownicy udostępniają niewykorzystaną moc obliczeniową swoich urządzeń (komputerów, serwerów, farm GPU) w zamian za wynagrodzenie w tokenach. AI może rozdzielać zadania treningowe między różne węzły, efektywnie wykorzystując dostępne zasoby szczególnie w zadaniach, które można zrównoleglić (np. trenowanie fragmentów dużej sieci neuronowej). Koncepcja federated learning (uczenia federacyjnego) zakłada, że modele maszynowe są trenowane lokalnie na urządzeniach użytkowników, a do sieci przekazywane są jedynie wyuczone parametry. Blockchain może pełnić rolę „księgi" zapisu zmian w modelu, co pozwala wszystkim węzłom śledzić postęp i weryfikować autentyczność aktualizacji. Taki model nie wymaga przesyłania surowych danych, co chroni prywatność i oszczędza łącze sieciowe. Analiza big data wymaga dostępu do dużych i różnorodnych zbiorów informacji. Dzięki blockchainowi można stworzyć mechanizm współdzielenia danych (data sharing), w którym każda ze stron wie, iż niezmienność i autentyczność informacji są gwarantowane. W zamian za to inni uczestnicy sieci mogą oferować własne zestawy danych albo zapłatę w tokenach. Sztuczna inteligencja otrzymuje tym samym bardziej zróżnicowany materiał treningowy, co zwykle przekłada się na wyższą trafność predykcji. Szybki rozwój technologii nierzadko wyprzedza zdolność ustawodawców do tworzenia spójnych regulacji. W kontekście blockchain i AI dochodzi dodatkowe wyzwanie: obie te dziedziny mają silny charakter ponadnarodowy – sieci blockchain mają uczestników rozsianych na całym świecie, a algorytmy AI

wykorzystują zasoby chmury obliczeniowej, nieraz zlokalizowanej na różnych kontynentach. W Unii Europejskiej wciąż toczy się dyskusja, jak pogodzić niezmienność łańcucha bloków z prawem do usunięcia danych. Jedną z propozycji jest przechowywanie w samym łańcuchu jedynie kryptograficznych odwołań do danych, a faktyczne pliki w systemach off-chain, które można usunąć lub zanonimizować, choć i to nie zawsze rozwiązuje problem w pełni. Coraz więcej państw i organizacji pracuje nad kodeksami etycznymi, dotyczącymi sztucznej inteligencji (np. wytyczne OECD czy inicjatywy Komisji Europejskiej). W połączeniu z blockchainem pojawia się pytanie, w jaki sposób egzekwować te zasady, jeżeli decyzje podejmują zdecentralizowane smart kontrakty i algorytmy rozproszone po wielu węzłach. Podobnie jak w początkowych fazach rozwoju internetu, konieczne jest ustalenie wspólnych standardów, dzięki którym różne blockchainy i systemy AI będą mogły się ze sobą komunikować. Międzynarodowe organizacje, takie jak ISO (International Organization for Standardization), intensywnie pracują nad określeniem norm w zakresie interoperacyjności, prywatności i bezpieczeństwa. W niektórych zastosowaniach (np. medycznych czy prawniczych) kluczowe jest, by algorytm nie tylko podawał wynik, ale też potrafił wyjaśnić tok rozumowania. Połączenie XAI z blockchainem daje szansę na pełną audyt owalność zarówno wejściowych danych, jak i decyzji podejmowanych przez model. Dzięki temu można weryfikować, czy algorytm nie działa stronniczo ani nie narusza czyichś praw. Nadejście komputerów kwantowych może podważyć część dzisiejszych mechanizmów kryptograficznych, w tym te stosowane w blockchainie. W obszarze AI z kolei komputery kwantowe mogą znacząco przyspieszyć obliczenia. Potrzebne będą więc nowe protokoły i algorytmy (np. algorytmy post-kwantowe) gwarantujące, że bezpieczeństwo danych zostanie zachowane nawet w dobie kwantowej mocy obliczeniowej. W przyszłości można spodziewać się rozwoju całych ekosystemów z udziałem wielu agentów zarówno ludzkich, jak i sztucznych (boty AI). Blockchain może pełnić wówczas rolę „warstwy zaufania", w której rejestrowane są wzajemne interakcje i transakcje. Taki system multi-agentowy będzie w stanie podejmować złożone decyzje dotyczące dystrybucji zasobów, zarządzania projektami czy nawet tworzenia nowych usług. Ponieważ smart kontrakty są kluczowym elementem łańcucha bloków, a AI jest w stanie analizować duże ilości kodu, spodziewany jest rozwój narzędzi do automatycznej weryfikacji i testowania poprawności inteligentnych kontraktów. Algorytmy uczenia maszynowego mogą wykrywać potencjalne błędy, luki bezpieczeństwa czy backdoory, ograniczając ryzyko

przeprowadzenia ataków hackerskich na sieć. Technologia, jakkolwiek zaawansowana, zawsze stoi przed barierami czysto ludzkimi: brakiem specjalistycznych kompetencji, lękiem przed nowością czy niedostatecznym zrozumieniem potencjalnych korzyści. Coraz częściej firmy muszą inwestować w szkolenia z zakresu blockchain, kryptografii oraz sztucznej inteligencji. Potrzebni są inżynierowie, analitycy danych, ale też konsultanci biznesowi, którzy potrafią wytłumaczyć działanie złożonych systemów w sposób zrozumiały dla decydentów. Rynek specjalistów w obszarze blockchain i AI jest wciąż ograniczony. Mała podaż kadr sprawia, że stawki za usługi programistyczne i doradcze rosną, co z kolei może blokować mniejsze organizacje przed wchodzeniem w tę technologię. Jednym z rozwiązań jest rozwijanie platform z gotowymi szablonami smart kontraktów i narzędziami do analizy danych, tak by obniżyć próg wejścia dla nowych projektów. Aplikacje oparte na AI i blockchainie, które ingerują w prywatność lub dokonują automatycznych decyzji (np. przy przyznawaniu kredytu), mogą spotykać się z nieufnością obywateli. Kluczowe staje się zapewnienie przejrzystości, mechanizmów odwoławczych i weryfikacji algorytmów, aby zachować równowagę między innowacyjnością a odpowiedzialnością społeczną. Duże przedsiębiorstwa, świadome wagi bezpieczeństwa danych oraz korzyści płynących z analityki AI, coraz częściej wdrażają hybrydowe rozwiązania. Proces ten odbywa się zwykle w kilku etapach: Korporacje zaczynają od zastosowań w działach wewnętrznych: np. rejestrowanie zgód marketingowych klientów w prywatnym łańcuchu bloków albo testowanie AI do analizy wydajności procesów. Dzięki temu można ocenić opłacalność i skalowalność technologii, zanim wdroży się ją na krytycznych polach działalności. Z czasem korporacja zaprasza do współpracy dostawców i kontrahentów, aby tworzyć blockchain, w którym każdy uczestnik ma określone uprawnienia i współdzieli dane. AI może wówczas analizować cały łańcuch dostaw, wykrywać anomalie, a także optymalizować koszty i terminy dostaw w czasie rzeczywistym. Największym wyzwaniem bywa połączenie nowej technologii z już funkcjonującymi w przedsiębiorstwie systemami typu ERP, CRM czy hurtowniami danych (data warehouse). Potrzebne są moduły integracyjne (tzw. middleware) oraz migracje części danych. Decyzję o wprowadzeniu blockchainu i AI trzeba często traktować jak strategiczną zmianę architektury IT, a nie tylko eksperyment technologiczny. Docelowo korporacja może wprowadzić model, w którym część transakcji (np. rozliczenia licencji oprogramowania, nagradzanie pracowników lub programy lojalnościowe dla klientów) odbywa się w sposób zautomatyzowany, przy użyciu tokenów. Sztuczna inteligencja

podejmuje decyzje o rozdziale zasobów, a blockchain zapewnia niezmienność i audytowalność operacji. Często pojawia się pytanie, czy wraz z rozwojem AI i blockchainu rola człowieka w weryfikacji prawidłowości danych oraz w podejmowaniu decyzji nie stanie się zbędna. W istocie, sztuczna inteligencja potrafi automatyzować wiele czynności, ale wciąż istnieją obszary, w których rola ekspertów ludzkich okazuje się niezastąpiona: Algorytmy uczą się głównie na podstawie wzorców występujących w danych. Jednak niektóre sytuacje wymagają kontekstowego zrozumienia, rozumowania przyczynowo skutkowego bądź znajomości przepisów i uwarunkowań kulturowych. Decyzje o znaczeniu społecznym czy moralnym często nie mogą być pozostawione wyłącznie algorytmom. Nawet najbardziej wyrafinowana sieć neuronowa nie potrafi samodzielnie podjąć decyzji w oparciu o system wartości, jeśli nie zostanie on zaprogramowany i przejrzysty dla ludzi. Niektóre procesy biznesowe i innowacje wymagają kreatywnego podejścia, łączenia pozornie odległych dziedzin wiedzy czy intuicji, która wciąż pozostaje domeną człowieka. W praktyce zatem AI i blockchain będą raczej wspomagać ludzi w weryfikacji olbrzymich zestawów danych i automatyzacji rutynowych procesów, pozostawiając człowiekowi bardziej złożone, wieloaspektowe decyzje. Rozwój blockchainu i AI w dużej mierze napędza społeczność open source programistów, naukowców i entuzjastów technologii, którzy współpracują na forach internetowych, w projektach na GitHubie czy uczestniczą w konferencjach i hackathonach. Wspólny rozwój oprogramowania ma kilka korzyści. Otwarte projekty są częściej i intensywniej sprawdzane przez specjalistów z całego świata. Błędy i luki bezpieczeństwa są szybciej wykrywane i poprawiane. Projekty open source często stają się standardami de facto, ułatwiając integrację między różnymi platformami i narzędziami. Dostępność kodu źródłowego pozwala małym firmom i niezależnym twórcom korzystać z rozwiązań, które w modelu zamkniętym mogłyby być kosztowne. Sprzyja to różnorodności i konkurencji, co przekłada się na szybszy postęp technologiczny. Wśród przykładów można wymienić platformy takie jak Hyperledger (inicjatywa wspierana przez Linux Foundation), Ethereum (open source'owy blockchain), a także liczne biblioteki sztucznej inteligencji (TensorFlow, PyTorch, scikit-learn), które są powszechnie używane i stale rozwijane. Technologie blockchain oraz sztuczna inteligencja rozwijają się w imponującym tempie, a ich synergia zwłaszcza w kontekście ochrony danych, bezpieczeństwa i zaawansowanej analizy wydaje się coraz bardziej obiecująca. Korzyści, jakie niosą, obejmują: *Wysoki poziom bezpieczeństwa i odporności na manipulacje danych*, osiągany dzięki rozproszonej

architekturze łańcucha bloków i algorytmom kryptograficznym. *Efektywniejszą analizę dużych, zweryfikowanych zbiorów danych* przez modele AI, które dzięki blockchainowi mają pewność co do niezmienności informacji i mogą bardziej ufać w ich autentyczność. *Automatyzację procesów biznesowych i społecznych* (smart kontrakty, mikropłatności, tokenizacja), co może przyczynić się do redukcji kosztów oraz eliminacji pośredników. *Możliwość tworzenia nowych modeli współpracy w świecie cyfrowym*, opartych na autonomicznych systemach wieloagentowych, rynkach danych czy decentralizacji usług. Mimo to nie można bagatelizować ograniczeń i wyzwań, które wciąż towarzyszą tym technologiom: *Skalowalność i wydajność* wiele sieci blockchain, zwłaszcza starszej generacji, boryka się z niską przepustowością transakcji i relatywnie wysokimi kosztami. *Regulacje prawne* kwestie związane z prywatnością, prawami autorskimi, odpowiedzialnością za decyzje AI i zgodnością z międzynarodowymi przepisami wciąż pozostają otwarte. *Koszty wdrożenia i brak fachowców* specjalistyczna wiedza bywa trudno dostępna, co podnosi koszty projektów i może utrudniać wejście na rynek mniejszym podmiotom. *Zaufanie społeczne i akceptacja technologii* konieczne jest prowadzenie działań edukacyjnych, by przełamać lęk przed nowością i niezrozumieniem działania łańcucha bloków oraz algorytmów uczenia maszynowego. Patrząc w perspektywie najbliższych lat, można oczekiwać dalszego rozwoju narzędzi kryptograficznych, przyjaznych środowisku mechanizmów konsensusu oraz rosnącej popularności koncepcji takich jak federated learning czy edge computing w połączeniu z blockchainem. Również pojawienie się komputerów kwantowych będzie wymuszać transformacje w zakresie zabezpieczeń kryptograficznych i może przyspieszać analizę danych przez AI. W dłuższej perspektywie, jeśli bariery zostaną przełamane, a regulacje prawne i standardy międzynarodowe będą sprzyjać adaptacji, blockchain i AI mogą razem stworzyć fundamenty przyszłej infrastruktury cyfrowej w pełni bezpiecznej, zautomatyzowanej i zdecentralizowanej. Byłby to ekosystem, w którym dane przepływają pomiędzy inteligentnymi kontraktami, algorytmy AI na bieżąco uczą się i modyfikują swoje modele, a całość jest nadzorowana i kontrolowana przez rozproszoną sieć, wykluczającą możliwość nadużyć i manipulacji. Już dziś widać, że korporacje i instytucje publiczne stopniowo sięgają po hybrydowe rozwiązania od systemów zarządzania tożsamością cyfrową, poprzez automatyczne wnioski kredytowe, aż po inteligentne sieci energetyczne. Całokształt tych trendów zwiastuje, że w ciągu kolejnej dekady liczba zastosowań blockchainu i AI w ochronie i analizie danych znacznie wzrośnie.

Ostateczny kształt tego ekosystemu będzie jednak zależał od równowagi pomiędzy innowacyjnością a odpowiedzialnością, pomiędzy dążeniem do usprawnienia procesów a poszanowaniem prywatności oraz od współpracy wielu zainteresowanych stron firm technologicznych, rządów, organizacji pozarządowych i naukowców. Wielu ekspertów postrzega nadchodzące lata jako okres konsolidacji pojawienia się stabilnych standardów, wyraźnych ram prawnych i większego zrozumienia społecznego. Jeśli te warunki zostaną spełnione, blockchain i AI mają szansę wejść w fazę dojrzałości, stając się nieodzownymi elementami zaawansowanych systemów przetwarzania danych. W ten sposób mogą przyczynić się do stworzenia świata, w którym wymiana informacji i analiza są zarówno bezpieczne, jak i zautomatyzowane na niespotykaną dotąd skalę – ze wszystkimi konsekwencjami, jakie niesie to dla gospodarki, administracji i codziennego życia ludzi. Od momentu pojawienia się pierwszych rozwiązań blockchainowych (np. Bitcoin) i postępów w dziedzinie sztucznej inteligencji (zwłaszcza uczenia głębokiego), dyskutuje się o możliwościach łączenia tych dwóch światów. Blockchain wprowadza koncepcję rozproszonego rejestru: niezmienną, odporną na manipulacje bazę danych, którą wypełniają kolejne transakcje, grupowane w bloki. Sieć osiąga konsensus – ustala, który blok jest uznawany za prawidłowy – dzięki mechanizmom takim jak Proof of Work, Proof of Stake czy ich odmiany. Sztuczna inteligencja zaś to szeroki zbiór metod obliczeniowych zdolnych do automatycznej analizy dużych zbiorów danych i generowania wniosków. Połączenie tych technologii jest atrakcyjne ze względu na kilka kluczowych cech. Przede wszystkim blockchain daje pewność integralności danych – informacja zapisana w łańcuchu bloków nie może zostać zmieniona bez śladu. Z punktu widzenia AI to ogromnie istotne, bo modele machine learning czy deep learning muszą uczyć się z wiarygodnych źródeł. Zakłócenie integralności (np. w wyniku ataku hakerskiego) mogłoby wypaczyć wyniki algorytmów. Drugim atutem jest transparentność w otwartych sieciach praktycznie każdy węzeł dysponuje kopią rejestru i może śledzić historię transakcji. To pozwala na audyt nawet bardzo rozległych baz danych. Kolejna ważna korzyść wynika z samej natury AI: automatyczne przetwarzanie i analiza wrażliwych informacji – medycznych, finansowych czy logistycznych – musi być zabezpieczone przed przejęciem i nadużyciem. Blockchain, jeśli zostanie połączony z odpowiednimi technikami kryptograficznymi (m.in. Zero-Knowledge Proofs), wspiera poufność i prywatność, nie rezygnując z weryfikowalności. Blockchain jest z założenia rozproszoną księgą rachunkową, przechowującą dane w blokach, które kryptograficznie łączą się z blokiem poprzednim.

Każda próba modyfikacji we wcześniejszych blokach wymuszałaby zmianę także we wszystkich kolejnych, co w otwartej sieci z tysiącami węzłów jest ekstremalnie trudne (czy wręcz nierealne). W praktyce blockchain stał się słynny dzięki kryptowalutom, ale jego zastosowania wykraczają daleko poza rynek finansowy. W branży medycznej służy do zabezpieczania dokumentacji pacjentów, w administracji – do przechowywania rejestrów (np. gruntów), w logistyce do śledzenia produktów w łańcuchu dostaw. Wszędzie tam, gdzie priorytetem jest niezmienność informacji, potwierdzana konsensusem, można rozważyć wdrożenie blockchainu. Obecnie wiele projektów pracuje nad zmianami w warstwie konsensusu, przechodząc od energochłonnego Proof of Work (znanego z Bitcoina) do bardziej skalowalnych rozwiązań, takich jak Proof of Stake czy Delegated Proof of Stake. Niezależnie od wybranego mechanizmu, fundamentem blockchainu pozostaje rozproszone zarządzanie danymi, trudność fałszowania i wysoki poziom audytowalności. AI to nie jedynie popularne sieci neuronowe czy algorytmy uczenia głębokiego w jej obrębie mieści się mnóstwo technik, w tym systemy ekspertowe, algorytmy uczenia maszynowego, przetwarzanie języka naturalnego czy metody wnioskowania probabilistycznego. Sednem sztucznej inteligencji jest zdolność do samouczenia się na podstawie przykładów, rozpoznawania wzorców i automatycznego podejmowania decyzji. Dane to paliwo AI. Im większy i bardziej różnorodny zbiór, tym lepiej modele uczą się rozróżniać cechy i zjawiska. Jednakże, jeśli dane są zniekształcone, niekompletne lub sfabrykowane, AI zaczyna opierać się na fałszywych przesłankach. Tutaj blockchain przychodzi z pomocą jako gwarant niezmienności i integralności, dając pewność, że model przetwarza rzetelne informacje. W ostatnich latach rośnie popularność federated learning (uczenia federacyjnego), w którym dane pozostają lokalnie na urządzeniach użytkowników, a do centralnego serwera (lub rozproszonej sieci) trafiają jedynie wyuczone parametry. Blockchain może rejestrować każdą iterację uczenia i zapewniać, że nikt nie modyfikuje parametrów w sposób nieuprawniony. Podstawową korzyścią jest wiarygodność danych: wszelkie rekordy, które zasilały będą model AI, są przechowywane w łańcuchu odpornym na manipulacje. Odpowiednio ustawione smart kontrakty mogą zadbać o to, by dopuszczać do analizy tylko te zestawy informacji, które spełniają kryteria bezpieczeństwa i jakości. AI z kolei automatyzuje przetwarzanie danych zapisanych w blockchainie, wykrywa anomalie, przewiduje trendy i informuje o potencjalnych zagrożeniach. Przykładowo, w sektorze finansowym sieć blockchain przechowuje wszystkie transakcje, a algorytm machine learning nadzoruje pojawiające się schematy

mogące wskazywać na oszustwo bądź pranie pieniędzy. Dodatkowo, techniki takie jak Zero-Knowledge Proofs (ZKP) pozwalają inteligentnym kontraktom weryfikować, czy określone warunki zostały spełnione, bez ujawniania zbędnych szczegółów transakcji. Jest to więc sposób na zachowanie prywatności danych w połączeniu z niepodważalnym dowodem ich poprawności. AI może wówczas przetwarzać dane w formie zaszyfrowanej, jeśli zastosujemy np. homomorficzne szyfrowanie. Dokumentacja medyczna pacjentów, z natury bardzo wrażliwa, może być przechowywana w sposób niezmienny i audytowalny w prywatnym (bądź konsorcyjnym) łańcuchu bloków. SI analizuje te dane w celu wspomagania diagnoz lub personalizowanych terapii. Dzięki blockchainowi pacjenci zyskują pewność, że informacje o ich zdrowiu nie zostaną zmodyfikowane czy sprzedane bez ich zgody. Blockchain wykorzystuje się do automatyzacji procesów rozliczeniowych, rejestracji operacji w bankach czy firmach inwestycyjnych. Algorytmy AI wykrywają oszustwa, nadzorują scoring kredytowy i oceniają ryzyko w czasie rzeczywistym. Zaś w branży ubezpieczeniowej inteligentne kontrakty mogą samoczynnie wypłacać świadczenia po spełnieniu zdefiniowanych warunków (zweryfikowanych przez dane na blockchainie). W globalnych łańcuchach dostaw pojawia się problem sfałszowanych dokumentów, ukrytych opóźnień i nieodpowiednich warunków transportu. Blockchain potrafi rejestrować kolejne etapy przesyłki w niezmienny sposób, podczas gdy AI analizuje te zapisy, by wykryć nieprawidłowości lub prognozować możliwe zatory. W administracji możliwe jest wykorzystanie rejestrów blockchain, np. dla rejestrów obywateli czy własności gruntów. AI może wówczas pomagać w podejmowaniu decyzji dotyczących wydatków budżetowych, planów zagospodarowania przestrzennego czy przewidywania zapotrzebowania na usługi społeczne. Dynamiczny przyrost instalacji OZE (panele słoneczne, turbiny wiatrowe) rodzi wyzwania w bilansowaniu sieci. Rozproszony rejestr transakcji energii, obsługiwany przez blockchain, pozwala decentralizować handel nadwyżkami. AI z kolei steruje podażą i popytem, przewidując zapotrzebowanie i automatycznie wprowadzając korekty (np. uruchamiając rezerwowe źródła). Mimo obiecujących możliwości, nie brakuje barier ograniczających tempo adaptacji blockchainu i AI w szerszej skali. Pierwsze sieci (Bitcoin, Ethereum w wersji przed przejściem na Proof of Stake) cierpią na niską przepustowość i wysokie koszty transakcji. Dla systemów AI, które mogą generować wiele zapisów, jest to utrudnienie. Dlatego coraz większe znaczenie mają sieci typu layer 2 (np. sidechainy, state channels), a także nowe projekty umożliwiające przeprowadzanie tysięcy transakcji na

sekundę. Mechanizm Proof of Work wymaga potężnej mocy obliczeniowej. Choć obecnie wiele sieci przechodzi na Proof of Stake, jest to wciąż punkt zapalny dyskusji. Z drugiej strony, trening zaawansowanych modeli AI też pochłania mnóstwo energii. Pojawiają się więc inicjatywy na rzecz „zielonego" blockchainu i optymalizacji obliczeń w AI (hardware dedykowany GPU, TPU). Dane, które AI potrzebuje do analizy, zwykle pochodzą z różnych, często scentralizowanych źródeł. Konieczne są tzw. oracles, czyli mechanizmy łączące „świat zewnętrzny" (off-chain) z łańcuchem bloków (on-chain). Jeśli oracles są nierzetelne lub zhakowane, blockchain może zawierać błędne informacje. W Unii Europejskiej duże znaczenie ma RODO, które chroni dane osobowe i daje jednostce prawo do ich usunięcia. Blockchain z natury jest niezmienny, co stwarza pytania o to, jak „skasować" dane na łańcuchu. Pojawiają się próby rozdzielania metadanych (hashy) od plików przechowywanych w systemach off-chain, by móc zadośćuczynić przepisom. Blockchain wciąż kojarzy się wielu osobom głównie z kryptowalutami i spekulacjami. AI zaś budzi obawy o inwigilację i utratę miejsc pracy. Konieczne jest szerokie uświadamianie korzyści oraz ograniczeń tych technologii, tak by nie było to jedynie narzędzie gigantów technologicznych. Aby pogodzić wymóg przejrzystości z potrzebą prywatności, stosuje się zaawansowane metody kryptograficzne: Umożliwiają wykazanie prawdziwości danej informacji (np. mam powyżej 18 lat, posiadam wystarczającą liczbę tokenów) bez ujawniania pozostałych szczegółów. Dzięki temu prywatne dane nie wyciekają do całej sieci. Pozwala na wykonywanie działań matematycznych na zaszyfrowanych danych bez wcześniejszego odszyfrowywania. Z punktu widzenia AI jest to obiecujące, bo model może trenować się na danych zachowujących poufność, co minimalizuje ryzyko naruszenia prywatności. Często dane w blockchainie trzeba tak przekształcić, by nie można było łatwo zidentyfikować konkretnej osoby. Techniki te jednak mają swoje ograniczenia, bo przy wystarczająco dużej ilości informacji reidentyfikacja staje się możliwa. Blockchain otwiera drogę do tokenizacji różnego rodzaju aktywów, w tym danych czy nawet modeli AI. Można nagradzać użytkowników, którzy udostępniają swoje dane do treningu modeli uczenia maszynowego. Token staje się formą zapłaty, a rejestr w łańcuchu bloków zapewnia rozliczalność. Istnieją projekty pozwalające wystawiać wytrenowane modele na sprzedaż lub wymianę. Ktoś może zapłacić za dostęp do parametrów sieci neuronowej – w pełni automatycznie, za pośrednictwem smart kontraktu. Dzięki smart kontraktom możliwe jest tworzenie mikropłatności w czasie rzeczywistym, co przydaje się w IoT. Urządzenie (np. czujnik) może płacić za

dostęp do cudzego strumienia danych lub do mocy obliczeniowej, podejmując decyzje wspierane przez algorytmy AI. Firmy i instytucje publiczne, chcąc skorzystać z synergii blockchain–AI, zazwyczaj zaczynają od projektów pilotażowych w obszarach, gdzie potencjalne ryzyko jest mniejsze. Na przykład testuje się blockchain do rejestrowania zgód marketingowych albo prototypowo wdraża się uczenie maszynowe do analizy przepływu dokumentów. W kolejnym kroku o ile wyniki są obiecujące – organizacja poszerza zasięg i zaprasza do projektu partnerów (dostawców, kontrahentów). Powstaje wtedy model konsorcyjny, w którym każda strona ma swoją kopię łańcucha i może prześledzić historię transakcji (z zachowaniem poufności przy użyciu wspomnianych narzędzi kryptograficznych). Najtrudniejsze zwykle okazuje się przełamanie oporu przed zmianą, integracja ze starymi systemami (tzw. legacy) i wypracowanie standardów współpracy. Konieczne jest też zadbanie o kompetencje zespołu – zarówno programistów, jak i kierownictwa, które musi rozumieć zasady działania i możliwości płynące z obu technologii. Rozwój blockchainu i AI w ciągu najbliższych lat prawdopodobnie ulegnie przyspieszeniu, ale jednocześnie stanie się bardziej dojrzały i uregulowany. Wiele projektów, takich jak Polkadot czy Cosmos, pracuje nad łączeniem różnych łańcuchów bloków w jeden ekosystem. Powstaną więc „mosty" między blockchainami, a AI będzie mogła sięgać do całej gamy danych zapisanych w różnych sieciach. Jeśli komputery kwantowe staną się wystarczająco potężne, mogą złamać obecną kryptografię asymetryczną. Pojawiają się więc badania nad algorytmami post-kwantowymi. W dziedzinie AI komputery kwantowe mogą znacznie przyspieszyć trening złożonych modeli. Dla kluczowych zastosowań medycyny czy sądownictwa istotne jest, aby AI tłumaczyła, w jaki sposób doszła do danego wniosku. Jeżeli wyniki i ścieżki decyzyjne zostaną zarejestrowane w blockchainie, zainteresowane strony uzyskają dostęp do kompletnego „logu" procesu decyzyjnego, co zwiększy zaufanie i ułatwi rozstrzyganie sporów. Dynamiczna ewolucja AI i blockchainu stawia pytania dotyczące prywatności, równości dostępu i wolności obywatelskich. Jeśli pewne modele decydują o przyznaniu kredytu czy ubezpieczenia, trzeba mieć pewność, że nie dyskryminują one określonych grup. Z kolei blockchain może stać się narzędziem masowej inwigilacji, jeżeli ktoś wymusi udostępnianie zbyt dużego zakresu informacji. Bez odpowiedniego przygotowania społeczeństwa zarówno na poziomie uczelni i szkół, jak i programów informacyjnych dla dorosłych rozwój tych technologii może być nierówny i budzący niepotrzebne obawy. W wielu miejscach na świecie brakuje ekspertów w dziedzinach kryptografii, projektowania smart kontraktów czy analizy big

data. Społeczności open source, takie jak deweloperzy Ethereum, Hyperledger czy liczne środowiska pracujące nad bibliotekami AI (TensorFlow, PyTorch), napędzają innowacje i starają się tworzyć standardy de facto. Otwartość kodu sprzyja przejrzystości można szybciej wychwycić błędy, a także prowadzić niezależne audyty bezpieczeństwa. Z perspektywy globalnej transformacji cyfrowej, kluczowe będą projekty integrujące blockchain i AI w sposób przyjazny użytkownikom końcowym. Zaawansowane rozwiązania powinny zachować możliwie prosty interfejs, by nie wymagać od laików głębokiej wiedzy technicznej. Blockchain staje się powszechny w rejestrach publicznych i wewnętrznych systemach dużych firm. AI analizuje dane w czasie rzeczywistym. Ustawodawstwo nadąża z regulacjami, zapewniając równowagę między innowacyjnością a ochroną prywatności. W tym scenariuszu blockchain i AI wchodzą w fazę dojrzałości, stając się niezauważalnym, ale kluczowym elementem globalnej infrastruktury cyfrowej. W niektórych sektorach (finanse, logistyka) technologie te zostaną mocno wykorzystane, w innych – z powodu braków kompetencyjnych, oporu społecznego czy ryzyka inwestycyjnego – ich zastosowanie pozostanie ograniczone. Rozwój jest nierównomierny, a globalna standaryzacja przebiega wolno. Istnieje też ryzyko, że światowi giganci opanują kluczowe patenty i zasoby, blokując dostęp mniejszym podmiotom. Blockchain, zamiast sprzyjać decentralizacji, może stać się „prywatną siecią" wykorzystywaną do kontroli. AI, w rękach garstki firm, może pogłębiać nierówności i prowadzić do braku zaufania społecznego. We wszystkich przytoczonych fragmentach i rozważaniach wyraźnie wybrzmiewa główny wniosek: blockchain i sztuczna inteligencja mają olbrzymi potencjał w obszarze bezpiecznego przechowywania oraz zaawansowanej analizy danych. Blockchain stanowi niezawodną, rozproszoną „warstwę zaufania", która utrudnia manipulacje i zapewnia niezmienność zapisów. AI zaś pozwala przekuć dane w wiedzę przewidywać trendy, wychwytywać anomalie, optymalizować procesy.

Wspólne zastosowania tych technologii wchodzą do branż tak różnorodnych, jak medycyna, energetyka, finanse czy administracja. Wszędzie tam, gdzie trzeba zabezpieczyć czułe dane i jednocześnie uzyskać z nich cenne wnioski, korzyści są ogromne. Blockchain służy jako „szkielet" przechowujący kluczowe informacje, a AI jako „mózg" przetwarzający i interpretujący te dane. Niemniej jednak należy pamiętać o szeregu wyzwań i zagrożeń. Istnieją kwestie skalowalności, koszty energii, rozbieżne regulacje prawne i wciąż niedostateczne zrozumienie ze strony społeczeństwa. Wprowadzenie mechanizmów kryptograficznych (ZKP, homomorficzne szyfrowanie),

warstw drugiego rzędu (layer 2), a także rozwinięcie ekosystemu oracles i standaryzacja protokołów to tylko niektóre z kroków, które będą stopniowo usuwane w miarę rozwoju technologii. Dużą rolę odgrywają również inicjatywy open source, pozwalające na szeroką współpracę ekspertów i pasjonatów z całego świata. Mimo że rynek potrzebuje jeszcze czasu na „dojrzenie", a ustawodawstwo wymaga mądrego dostosowania do tak dynamicznych zmian, trendy wskazują na to, iż blockchain i AI przenikną do naszych systemów gospodarczych i społecznych, podobnie jak niegdyś stało się z internetem. Czy zatem w kolejnych dekadach zobaczymy w pełni zautomatyzowane miasta, w których rozproszone algorytmy zarządzają dostawą wody, energii i usług transportowych, a wszelkie transakcje mieszkańców odnotowywane są w blockchainie i analizowane przez AI w czasie rzeczywistym? Możliwe, choć warunkiem jest równoczesne zapewnienie prywatności, bezpieczeństwa i zachowanie kontroli społecznej nad tymi systemami. Z pewnością stoimy u progu cywilizacyjnej zmiany, która jeśli zostanie poprowadzona rozważnie może przynieść szereg korzyści dla ludzi na całym świecie. Sumując wszystkie te wątki, można z całą pewnością powiedzieć, że tematyka „Blockchain i sztuczna inteligencja w ochronie danych: bezpieczne przechowywanie i analiza" zasługuje na dalsze badania i szereg nowych wdrożeń. Największe wyzwanie stanowi zachowanie odpowiedzialnego balansu między rozwojem technologicznym a poszanowaniem ludzkich wartości: prywatności, przejrzystości, wolności wyboru i równego dostępu do dóbr. Dalszy dialog pomiędzy naukowcami, inżynierami, regulatorami i społeczeństwem będzie kluczowy, by nie stracić z oczu nadrzędnego celu służenia ludziom i wspierania postępu w sposób zrównoważony i bezpieczny.