Blockchain jako ekosystem zaufania w wizji Amit Kumara Tyagiego: od technologii finansowej do infrastruktury wiarygodności danych.

AUTOR

Fundacja Dobre Państwo

STRESZCZENIE / ABSTRACT

Artykuł redefiniuje blockchain, przesuwając punkt ciężkości z kryptowalut na architekturę instytucjonalnego zaufania. Autor argumentuje, że technologia ta służy przede wszystkim jako niezmienny rejestr pamięci, który rozwiązuje konflikty interesów i zapewnia audyt owalność w obszarach takich jak medycyna, administracja czy Przemysł 5.0. Kluczowym elementem jest relacja blockchaina z AI: podczas gdy sztuczna inteligencja dostarcza mocy analitycznej, blockchain gwarantuje integralność danych wejściowych i transparentność procesów decyzyjnych, eliminując problem „czarnej skrzynki”. Zaufanie nie zostaje usunięte, lecz przeniesione z centralnych instytucji na protokoły kryptograficzne i mechanizmy konsensusu, tworząc nową warstwę wiarygodności w cyfrowym społeczeństwie.

The article redefines blockchain, shifting the focus from cryptocurrencies to the architecture of institutional trust. The author argues that this technology serves primarily as an immutable memory register that resolves conflicts of interest and ensures auditability in areas such as medicine, administration, or Industry 5.0. A key element is the relationship between blockchain and AI: while artificial intelligence provides analytical power, blockchain guarantees the integrity of input data and the transparency of decision-making processes, eliminating the 'black box' problem. Trust is not removed but transferred from central institutions to cryptographic protocols and consensus mechanisms, creating a new layer of credibility in digital society.

Artykuł stawia tezę, że blockchain nowej generacji ewoluuje z niszowego narzędzia finansowego w fundamentalną infrastrukturę zaufania i instytucjonalną pamięć cywilizacji. Autor argumentuje, że prawdziwy potencjał technologii nie tkwi w spekulacyjnych kryptowalutach, lecz w stworzeniu niezmiennej warstwy wiarygodności dla danych, decyzji i tożsamości w kluczowych obszarach: inteligentnych miastach, e-administracji oraz ochronie zdrowia. Kluczem do masowej adopcji jest rozwiązanie trilematu blockchaina (bezpieczeństwo, decentralizacja, skalowalność) poprzez architektury wielowarstwowe i nowe mechanizmy konsensusu, co pozwoli przejść od teoretycznych obietnic do realnej infrastruktury. W synergii z AI i IoT, blockchain ma pełnić rolę 'notariusza przyszłości', zabezpieczając integralność danych wejściowych dla algorytmów i chroniąc prywatność obywateli. Całość zostaje osadzona w paradygmacie Przemysłu 5.0, gdzie technologia musi być podporządkowana wartościom humanistycznym, by uniknąć ryzyka stworzenia 'cyfrowego panoptikonu' lub zautomatyzowanej biurokracji pozbawionej empatii.

SŁOWA KLUCZOWE

ekosystem zaufania | infrastruktura wiarygodności danych | instytucjonalna warstwa zaufania | protokół pamięci i audytu AI | trilemat blockchaina | skalowalność sieci rozproszonych | cyfrowe waluty banków centralnych CBDC | uczenie federacyjne | szyfrowanie homomorficzne | Poufność różnicowa | Przemysł 5.0 | interoperacyjność danych medycznych | smart kontrakty w zdrowiu | niezmienny rejestr kryptograficzny | warstwa koordynacji i audytu

Blockchain jako instytucjonalna warstwa zaufania

Koniec mitu "łańcucha bloków" jako zabawki spekulantów. Największym błędem w myśleniu o blockchainie jest zamknięcie go w getcie kryptowalut. To tak, jakby o elektryczności mówić wyłącznie przez pryzmat pierwszej żarówki, a o druku jedynie przez rachunek z drukarni. Bitcoin był historycznie ważny, Ethereum poszerzyło horyzonty dzięki smart kontraktom, a zdecentralizowane finanse rozbudziły ambicje budowy nowej infrastruktury finansowej. Jednak prawdziwy ciężar tej technologii ujawnia się dopiero wtedy, gdy przestajemy pytać o cenę tokena, a zaczynamy o architekturę zaufania: Kto potwierdza fakt? Kto przechowuje zapis? Kto może go

zmienić? Kto widzi historię działań? Kto ponosi odpowiedzialność za błąd? Kto ma władzę nad regułami dostępu?

Blockchain jest zatem mniej "technologią pieniądza", a bardziej technologią instytucjonalnej pamięci. Jego podstawowa obietnica polega na tym, że zdarzenie zapisane w rozproszonej księdze przestaje być prywatną deklaracją jednego centrum, stając się elementem wspólnego rejestru, którego zmiana wymagałaby naruszenia całego porządku walidacji. To dlatego Tyagi przesuwa punkt ciężkości z kryptowalut na ekosystemy: zdrowie, inteligentne miasta, rolnictwo, administrację, łańcuchy dostaw, ochronę dziedzictwa kulturowego, bezpieczeństwo AI i Przemysł 5.0.

Nie chodzi tu o fetysz decentralizacji samej w sobie, gdyż nie jest ona cnotą absolutną. Źle zaprojektowany system rozproszony może być wolniejszy, droższy, mniej przejrzysty dla użytkownika i bardziej podatny na ukrytą dominację aktorów technicznych niż system scentralizowany. Nie każda baza danych potrzebuje blockchaina. Sens tej technologii pojawia się tam, gdzie istnieje konflikt interesów, potrzeba audytowalności, ryzyko manipulacji, brak zaufania do centralnego operatora albo konieczność koordynacji wielu podmiotów bez jednego suwerena technicznego. W przeciwnym razie "wrzućmy to na blockchain" jest tylko nową odmianą starego biurokratycznego zaklęcia: "powołajmy zespół roboczy". To przesunięcie od technologii do instytucji jest kluczowe.

Blockchain nowej generacji nie ma być wyłącznie narzędziem transferu wartości, lecz warstwą wiarygodności dla danych, decyzji, tożsamości, pochodzenia rzeczy, procesów administracyjnych i automatycznych transakcji. W łańcuchach dostaw pozwala ustalić pochodzenie produktu; w zdrowiu może zapisywać ścieżkę dostępu do dokumentacji medycznej; w administracji zabezpieczać rejestry; w rolnictwie chronić dane z czujników i dronów; w ochronie dziedzictwa potwierdzać autentyczność zdigitalizowanych manuskryptów; a w AI służyć jako warstwa audytu decyzji algorytmicznych. Notatka używa celnego sformułowania: blockchain przechodzi "od narzędzia finansowego do ekosystemu zaufania".

Ta formuła wymaga jednak dopowiedzenia. Zaufanie nie znika, lecz zmienia lokalizację. W tradycyjnych instytucjach ufamy urzędowi, bankowi, notariuszowi, szpitalowi, archiwum, księdze wieczystej, centralnemu operatorowi infrastruktury albo wielkiej platformie cyfrowej. W systemach blockchainowych zaufanie zostaje przesunięte na protokół, kryptografię, mechanizm konsensusu, reguły dostępu, jakość kodu, odporność infrastruktury oraz społeczność walidującą system. To nie jest koniec zaufania, lecz jego techniczna rekonstrukcja. Kto twierdzi, że blockchain usuwa zaufanie, sprzedaje metafizykę w opakowaniu po informatyce. Kto zaś twierdzi, że może on zmienić

geometrię zaufania, mówi już poważniej. Pytanie brzmi zatem: czy społeczeństwo cyfrowe potrzebuje nowej warstwy wiarygodności? Odpowiedź jest twierdząca, choć nie naiwna.

Potrzebuje jej, ponieważ skala automatyzacji przekracza możliwości tradycyjnej kontroli, a stopień centralizacji danych tworzy nowe punkty awarii i dominacji. Przez dekady cyfryzację rozumiano głównie jako przeniesienie dokumentu z papieru na serwer lub usługi z okienka do aplikacji. Dzisiaj problem jest głębszy: dane stają się tworzywem decyzji automatycznych, które z kolei wpływają na zarządzanie ludźmi – często w systemach nieprzejrzystych dla obywatela, pacjenta czy pracownika. W tym punkcie blockchain spotyka się ze sztuczną inteligencją. AI generuje potęgę obliczeniową i analityczną, ale nie gwarantuje prawdziwości danych wejściowych. Może rozpoznawać wzorce i automatyzować decyzje, lecz jeśli dane są skażone lub sfałszowane, inteligencja systemu staje się tylko elegancką formą przyspieszonego błędu. Blockchain może tu pełnić funkcję księgi pochodzenia danych, ścieżki audytu i mechanizmu kontroli integralności. Tyagi wskazuje ten dwukierunkowy układ: AI może wzmacniać cyberbezpieczeństwo, a blockchain wiarygodność danych i transparentność procesów decyzyjnych AI.

Blockchain jako protokół pamięci i audytu dla systemów AI

Jest to szczególnie istotne w obliczu problemu „czarnej skrzynki”. Współczesne modele głębokiego uczenia często działają skutecznie, lecz ich proces decyzyjny pozostaje nieprzejrzysty. W medycynie, finansach, administracji publicznej czy zarządzaniu infrastrukturą krytyczną odpowiedź w stylu „algorytm tak uznał” jest niewystarczająca. Tam, gdzie decyzja dotyka praw człowieka, zdrowia, majątku, dostępu do świadczeń, bezpieczeństwa lub wolności obywatelskich, niezbędna jest jasna ścieżka odpowiedzialności.

Blockchain nie sprawi, że AI stanie się automatycznie wyjaśnialna, ale może rejestrować dane wejściowe, wersje modelu, uprawnienia, przebieg zatwierdzania i historię decyzji. W ten sposób może stać się protokołem pamięci dla systemów, które z natury rzeczy mają skłonność do mgły. Nieprzypadkowo w najnowszych debatach technologicznych obok blockchaina pojawiają się pojęcia uczenia federacyjnego, poufności różnicowej, szyfrowania homomorficznego i bezpiecznych obliczeń wielostronnych (MPC). Są to techniki ochrony prywatności, których wspólny cel – choć technicznie złożony – jest prosty: cyfrowa przyszłość nie może polegać na tym, że wszystkie dane świata zostaną wrzucone do jednego kotła, zamieszane przez algorytm i podane obywatelowi jako zupa postępu. Dane wrażliwe muszą być przetwarzane tak, by chronić jednostkę, a nie tylko efektywność systemu. Uczenie federacyjne pozwala szkolić modele bez przenoszenia surowych

danych z lokalnych środowisk; poufność różnicowa minimalizuje ryzyko identyfikacji osób, zaś szyfrowanie homomorficzne i MPC umożliwiają obliczenia na danych zaszyfrowanych. W takim układzie blockchain pełni rolę warstwy koordynacji, audytu i potwierdzania integralności.

Wymagana jest jednak sceptyczna korekta: blockchain nie jest tożsamy z prywatnością. Publiczny, niezmienny rejestr bywa błogosławieństwem dla audytu, ale może stać się przekleństwem dla danych osobowych, jeśli zostanie źle zaprojektowany. Niezmienność, będąca zaletą w łańcuchu dostaw, w obszarze danych osobowych koliduje z prawem do sprostowania, ograniczenia przetwarzania czy usunięcia informacji. Dlatego dojrzałe systemy nie powinny zapisywać w blockchainie wszystkiego, lecz raczej kryptograficzne skróty (hashe), metadane, potwierdzenia i odniesienia do danych przechowywanych poza łańcuchem (off-chain). Model ten widać w systemach zdrowotnych typu CareBlock, gdzie ciężkie pliki medyczne zostają na zewnątrz, a do blockchaina trafia jedynie niezmienny odcisk kryptograficzny dokumentu.

To rozróżnienie ma znaczenie ustrojowe. W świecie analogowym kontrola nad dokumentem często oznaczała kontrolę nad procesem. W rzeczywistości cyfrowej trzeba oddzielić dane od metadanych, uprawnień, ścieżki audytu, logiki automatyzacji oraz warstwy przechowywania i wykonawczej. Blockchain staje się interesujący właśnie dlatego, że pozwala te warstwy uporządkować.

Dzieje się to jednak tylko pod warunkiem, że projektant systemu rozumie nie tylko informatykę, lecz także prawo, ekonomię instytucjonalną, socjologię zaufania i antropologię władzy. Technologia pozbawiona teorii instytucji szybko staje się albo gadżetem, albo narzędziem dominacji. Najbardziej trzeźwe podejście do blockchaina zaczyna się więc od analizy problemu, a nie od zachwytu nad samym narzędziem.

Skalowalność jako warunek przejścia od obietnic do infrastruktury

Jeśli problemem jest brak interoperacyjności między szpitalami, blockchain może pomóc, lecz nie zastąpi standardów medycznych, zgód pacjenta ani odpowiedzialności zawodowej. Jeśli kwestią sporną jest fałszowanie pochodzenia leków, technologia ta wzmocni identyfikowalność, ale nie wyeliminuje potrzeby inspekcji, sankcji i kontroli jakości. W przypadku braku zaufania do procesu głosowania blockchain zabezpieczy integralność zapisu, jednak sam w sobie nie rozwiąże problemów tajności, przymusu, kupowania głosów czy wykluczenia cyfrowego i społecznego zaufania do procedury. Z kolei przy skalowaniu globalnych płatności nowe modele muszą zmierzyć

się z przepustowością, kosztami, finalnością transakcji, cyberbezpieczeństwem oraz regulacjami. Właśnie dlatego kluczowym technicznym węzłem niniejszej analizy musi być skalowalność.

Bez niej blockchain pozostanie obietnicą o rozmachu cywilizacyjnym i wydajności kancelarii z jednym segregatorem. Bariera ta jest fundamentalna: tradycyjne sieci mają ograniczoną liczbę transakcji na sekundę, walidacja wymaga udziału wielu węzłów, a konsensus Proof of Work pochłania nadmierną energię i czas, co przy przeciążeniach prowadzi do opóźnień oraz wzrostu opłat. To nie jest drobiazg techniczny, lecz warunek polityczno-ekonomiczny. System, który ma obsługiwać miasto, służbę zdrowia, administrację, łańcuch dostaw czy pieniądz cyfrowy, nie może działać jak klub kolekcjonerów rzadkich znaczków, w którym każdy zapis jest celebrowany przez pół sieci.

Proponowane rozwiązania dzielą się na trzy grupy. Pierwszą stanowią rozwiązania warstwy drugiej i transakcje off-chain, przenoszące część aktywności poza główny łańcuch w celu odciążenia sieci bazowej. Druga to sharding, czyli podział sieci na mniejsze fragmenty przetwarzające transakcje równolegle. Trzecia to zmiana mechanizmów konsensusu – przede wszystkim odejście od energochłonnego Proof of Work na rzecz Proof of Stake, Delegated Proof of Stake lub modeli hybrydowych. W tle pojawia się również kierunek sprzętowy: wykorzystanie tranzystorów CNTFET i pamięci SRAM, które mają zmniejszać opóźnienia, zwiększać szybkość walidacji i poprawiać efektywność energetyczną.

Nie należy jednak mylić skalowalności z samą szybkością. W systemach społeczno-technicznych skalowalność oznacza zdolność do wzrostu bez utraty bezpieczeństwa, przejrzystości, decentralizacji, dostępności i odporności. Łatwo przyspieszyć system, oddając kontrolę jednemu operatorowi. Łatwo uprościć walidację, rezygnując z rozproszonej kontroli. Łatwo obniżyć koszt, przerzucając ryzyko na użytkownika.

Prawdziwy problem blockchaina polega na próbie jednoczesnego zachowania rozproszonego zaufania, bezpieczeństwa kryptograficznego, odporności na manipulacje i wysokiej wydajności. To słynny, choć często upraszczany konflikt między decentralizacją, bezpieczeństwem a skalowalnością. Kto obiecuje pełne zwycięstwo we wszystkich trzech wymiarach bez ponoszenia kosztów, ten prawdopodobnie sprzedaje nie architekturę, lecz powerpoint.

Regulacje i CBDC jako przejście blockchaina w fazę infrastruktury nadzorowanej

Aktualny kontekst regulacyjny zmienia stawkę gry. Unijne rozporządzenie MiCA zaczęło w pełnym zakresie obejmować rynek kryptoaktywów od końca 2024 roku, przy czym ESMA przewidziała okresy przejściowe dla części podmiotów działających wcześniej na rynku. Nie jest to jedynie techniczna regulacja branżowa, lecz sygnał, że blockchain wychodzi z fazy dzikiego pogranicza i wchodzi w fazę infrastruktury nadzorowanej. Dla jednych to zdrada pierwotnego ducha decentralizacji; dla innych warunek masowej adopcji. W istocie jest to moment dojrzewania. Każda technologia dotykająca pieniędzy, danych, własności, zdrowia czy administracji prędzej czy później spotyka się z państwem. Pytanie nie brzmi zatem, czy regulować, lecz jak robić to w sposób, który nie zdusi innowacji i nie pozostawi obywatela samotnego wobec protokołu, którego nie rozumie nawet jego własny bank.

Sytuację głębiej zmienia wejście cyfrowych walut banków centralnych (CBDC). Bank Rozrachunków Międzynarodowych od kilku lat rozwija wizję tokenizacji i tzw. unified ledger – wspólnej infrastruktury, w której cyfrowy pieniądz banku centralnego, depozyty bankowe i tokenizowane aktywa mogłyby funkcjonować na programowalnej platformie rozliczeniowej. Oznacza to, że blockchainowa wyobraźnia może zostać częściowo przejęta przez sektor publiczny i bankowość centralną. CBDC nie musi być klasycznym publicznym blockchainem; może korzystać z wybranych idei tokenizacji, rozproszonej infrastruktury, programowalności i audytowalności, bez przyjęcia pełnej anarchicznej mitologii kryptowalutowej. Państwo patrzy na blockchain i konkluduje: piękne narzędzia, szkoda byłoby zostawić je wyłącznie libertarianom i giełdom. Wejście CBDC może wywołać trzy skutki.

Po pierwsze, zwiększy presję na standardy bezpieczeństwa, prywatności, interoperacyjności i odporności. Jeśli pieniądz banku centralnego zostanie udostępniony w formie cyfrowej, użytkownicy będą oczekiwać wygody płatności prywatnych przy jednoczesnym zachowaniu bezpieczeństwa właściwego pieniądzowi publicznemu. Po drugie, CBDC może zmienić układ sił między bankami centralnymi i komercyjnymi, operatorami płatności, stablecoinami a zdecentralizowanymi finansami. Po trzecie, może zaostrzyć spór o prywatność. Cyfrowy pieniądz publiczny może być narzędziem inkluzji, suwerenności monetarnej i odporności systemu płatniczego, lecz źle zaprojektowany stanie się architekturą nadzoru. Tu nie ma miejsca na dziecięcą naiwność.

Pieniądz zawsze był technologią władzy; cyfrowy pieniądz jest technologią władzy z interfejsem użytkownika. Europejska debata o cyfrowym euro pokazuje, że instytucje zdają sobie sprawę z tej

dwuznaczności. EBC podkreśla, że decyzja o emisji cyfrowego euro wymaga podstawy legislacyjnej i musi być zgodna z procesem prawnym. Jednocześnie kładzie się nacisk na funkcjonalność offline, odporność oraz prywatność zbliżoną do gotówki w określonych sytuacjach. Według doniesień z grudnia 2025 roku Rada UE poparła model cyfrowego euro działającego zarówno online, jak i offline, z limitami sald i bezpłatnymi usługami podstawowymi. Jest to kluczowe, gdyż bez funkcji offline CBDC może wykluczać osoby słabiej zinformatyzowane i tracić odporność w sytuacjach awaryjnych. Bez limitów rodzi ryzyko odpływu depozytów z banków komercyjnych, bez prywatności może stać się koszmarem nadzorczym, a bez wygody przegra z kartą, BLIK-iem, portfelem mobilnym czy stablecoinem.

CBDC będzie zatem testem dojrzałości całej filozofii blockchainowej. Jeżeli blockchain miał być buntem przeciwko centralizacji pieniądza, to CBDC jest odpowiedzią centrum: „my też potrafimy tokenizować". Jeśli miał być narzędziem zaufania bez pośredników, to CBDC pokazuje, że pośrednik najwyższego rzędu – państwo i bank centralny – nie znika, lecz modernizuje swój aparat. Jeżeli blockchain miał zdemokratyzować dostęp do finansów, to CBDC może ten cel wesprzeć albo odwrócić, zależnie od konstrukcji prawnej i technicznej. Pytanie o przyszłość nie brzmi więc: kryptowaluty czy banki centralne? Pytanie brzmi: jaki model pieniądza cyfrowego zachowa wolność obywatela, stabilność systemu i możliwość innowacji?

Blockchain jako konstytucja kodu i wyzwanie skalowalności

W tym miejscu powracamy do aksjologii Przemysłu 5.0, która dominuje w niniejszej notatce. Model ten zakłada odejście od czystej automatyzacji na rzecz human-centricity, sustainability i resilience – technologii zorientowanej na człowieka, zrównoważonej i odpornej. Jest to niezbędna korekta wobec technokratycznego entuzjazmu. Jeśli blockchain, AI, IoT i cyfrowe bliźniaki mają tworzyć infrastrukturę przyszłości, pytanie nie może brzmieć wyłącznie: czy system działa szybciej? Musi brzmieć: komu służy, kto go kontroluje, kto rozumie jego logikę, kto może zakwestionować decyzję, kto zostaje wykluczony, kto ponosi koszt transformacji i kto czerpie rentę z nowej infrastruktury.

Blockchain nowej generacji jest zatem polem walki o kształt cyfrowej cywilizacji. Z jednej strony może wspierać przejrzyste łańcuchy dostaw, uczciwsze rejestry, odporniejszą administrację, bezpieczniejszą dokumentację medyczną, ochronę dziedzictwa, rolnictwo precyzyjne i audytowalną AI. Z drugiej – może zostać sprowadzony do modnego opakowania dla nowych monopoli, cyfrowej biurokracji i automatyzacji nierówności. Technologia, która zapisuje wszystko, niekoniecznie rozumie cokolwiek. Rozumienie pozostaje domeną człowieka, prawa, nauki, instytucji i debaty

publicznej. Dlatego dojrzała opowieść o blockchainie musi być jednocześnie techniczna i humanistyczna. Techniczna, gdyż bez znajomości skalowalności, kryptografii, konsensusu, architektur off-chain, interoperacyjności i odporności kwantowej łatwo popaść w slogan. Humanistyczna, ponieważ bez zrozumienia zaufania, władzy, prawa, pamięci społecznej, prywatności i odpowiedzialności blockchain staje się tylko maszyną do produkowania nieusuwalnych błędów. Najbardziej niebezpieczna nie jest sama technologia, lecz przekonanie jej użytkowników o jej neutralności.

Neutralny bywa młotek. Protokół zarządzający pieniędzmi, zdrowiem, tożsamością i rejestrem własności nie jest młotkiem. Jest konstytucją w języku kodu. Skalowalność to próg, na którym kończy się metafora, a zaczyna infrastruktura. Blockchain najłatwiej podziwiać w języku idei: decentralizacja, zaufanie, niezmienność, przejrzystość, odporność na manipulację. Trudniej zachować entuzjazm, gdy schodzimy do poziomu przepustowości, opóźnień, kosztów transakcyjnych, mechanizmów konsensusu, limitów pamięci, rozmiaru bloku, finalności zapisu i energetycznej ceny bezpieczeństwa. A jednak to właśnie tutaj rozstrzyga się przyszłość tej technologii. Cywilizacja cyfrowa nie żyje z manifestów, lecz z infrastruktury.

Jeżeli infrastruktura nie działa szybko, tanio, przewidywalnie i bezpiecznie, to nawet najpiękniejsza filozofia decentralizacji pozostaje poezją dla informatyków po północy.

Źródło trafnie wskazuje skalowalność jako jedno z najbardziej krytycznych ograniczeń masowej adopcji blockchaina. Tradycyjne sieci rozproszone przetwarzają ograniczoną liczbę transakcji na sekundę, ponieważ każda operacja wymaga walidacji przez wiele węzłów, a mechanizmy konsensusu – zwłaszcza Proof of Work – generują dodatkowy koszt obliczeniowy, energetyczny i czasowy. W efekcie systemy te łatwo wpadają w zatory i opóźnienia, co prowadzi do wzrostu opłat wraz ze wzrostem liczby użytkowników. To paradoks technologii mającej służyć masowej koordynacji: im większy jest popyt na jej użycie, tym szybciej ujawnia się jej kruchość. Problem skalowalności nie jest więc techniczną ciekawostką, lecz sprawdzianem instytucjonalnym.

Jeśli blockchain ma obsługiwać inteligentne miasto, musi przetwarzać strumienie danych z transportu, energetyki, gospodarki odpadami, parkingów, czujników środowiskowych i infrastruktury krytycznej. W sektorze zdrowia musi zapewniać dostęp do dokumentacji, zarządzać zgodami pacjenta, ścieżkami audytu oraz danymi z urządzeń ubieralnych i zdalnego monitoringu. Wsparcie dla łańcuchów dostaw wymaga nadążenia za ruchem towarów, dokumentów, płatności, kontroli jakości i certyfikatów. W ekosystemie CBDC musi natomiast sprostać oczekiwaniu natychmiastowości właściwej nowoczesnym płatnościom. Nikt nie będzie czekał na ideologicznie czystą transakcję, jeśli terminal płatniczy, aplikacja bankowa czy BLIK zrobią to szybciej. W gospodarce cyfrowej cierpliwość użytkownika jest zasobem rzadszym niż bitcoin. Skalowalność

należy więc rozumieć szerzej niż tylko jako liczbę transakcji na sekundę; choć jest to widoczny wskaźnik, nie wyczerpuje on istoty problemu.

Wielowarstwowa architektura jako odpowiedź na trilemat blockchaina

Równie istotna jest finalność – moment, w którym zapis uznaje się za nieodwracalny i bezpieczny. Do kluczowych parametrów należą także: koszt jednostkowej operacji, przewidywalność opłat, odporność na przeciążenia, zdolność aktualizacji protokołu, dostępność dla mniejszych uczestników, wymogi sprzętowe wobec węzłów, efektywność energetyczna oraz zgodność z regulacjami. System może być szybki, lecz scentralizowany; bezpieczny, ale powolny; zdecentralizowany, lecz niewydajny; tani, ale podatny na nadużycia. Blockchain nie ucieka od ekonomii wyboru. On tylko ubiera ją w kryptografię.

W tle tych rozważań leży klasyczne napięcie między decentralizacją, bezpieczeństwem a skalowalnością. Nie jest to matematyczny wyrok śmierci dla blockchaina, lecz ostrzeżenie przed reklamową przesadą. Jeśli dążymy do tego, by każdy węzeł niezależnie weryfikował znaczną część historii systemu, zyskujemy wysoką odporność na manipulacje, ale płacimy spadkiem wydajności. Zwiększenie przepustowości poprzez ograniczenie liczby walidatorów lub podniesienie wymogów sprzętowych przyspieszy system, lecz stworzy ryzyko koncentracji władzy. Przenosząc transakcje poza główny łańcuch redukujemy obciążenie, jednak musimy zapewnić wiarygodne powiązanie warstwy drugiej z bazową. Każde "rozwiązanie" jest więc także przesunięciem ryzyka.

Pierwszą odpowiedzią na te wyzwania są rozwiązania Layer-2. Ich logika jest intuicyjna: nie wszystkie operacje muszą być wykonywane bezpośrednio na głównym łańcuchu. Część aktywności można przenieść poza warstwę bazową, a do blockchaina zapisywać jedynie wynik, skrót, dowód lub rozliczenie końcowe. W praktyce oznacza to odciążenie sieci, redukcję kosztów i skrócenie czasu transakcji – przykładem jest Lightning Network w sieci Bitcoin, umożliwiający szybkie operacje poza głównym łańcuchem przy minimalnych kosztach.

Znaczenie Layer-2 wykracza poza techniczną optymalizację. To dowód na to, że blockchain dojrzewa poprzez architekturę wielowarstwową. Podobnie jak współczesne państwo nie funkcjonuje wyłącznie przez jeden urząd centralny, lecz poprzez system instytucji, procedur, rejestrów i organów wykonawczych, tak społecznie użyteczny blockchain nie będzie monolitem. Stanie się raczej ekosystemem warstw: bazowej, odpowiedzialnej za bezpieczeństwo, oraz warstw wykonawczych, danych, identyfikacji, prywatności i aplikacyjnych.

Sharding i nowe konsensusy jako drogi do skalowalności

Marzenie o jednym łańcuchu do wszystkiego przypomina wizję jednego ministerstwa zarządzającego każdym aspektem życia. Brzmi to sprawnie tylko do momentu, gdy trzeba załatwić pierwszą sprawę. Alternatywą jest sharding, czyli fragmentacja sieci. Zamiast wymagać, aby cała sieć przetwarzała każdą transakcję, dzieli się ją na mniejsze części pracujące równolegle. Podejście to przypomina podział wielkiej instytucji na wyspecjalizowane departamenty: organizm zachowuje wspólną tożsamość, ale nie każdy urzędnik musi czytać każdy dokument. Technicznie sharding zwiększa przepustowość dzięki równoległemu przetwarzaniu danych w shardach, co czyni go jedną z głównych dróg skokowego wzrostu wydajności blockchaina.

Sharding nie jest jednak darmowym obiadem. Im bardziej dzielimy system, tym trudniej zapewnić bezpieczeństwo całej sieci, synchronizację stanu, komunikację między fragmentami oraz ochronę przed atakami ukierunkowanymi na konkretny shard. W administracji znamy analogiczny problem: decentralizacja kompetencji może zwiększyć sprawność lokalną, ale rodzi ryzyko niespójności i luk koordynacyjnych.

W blockchainie jest podobnie. Podział zwiększa wydajność, lecz wymaga precyzyjnej architektury bezpieczeństwa. Zła fragmentacja nie tworzy sieci; tworzy cyfrowy archipelag, w którym każdy shard mówi własnym dialektem i modli się, aby mosty nie runęły. Kolejną odpowiedzią jest zmiana mechanizmów konsensusu. Proof of Work odegrał historyczną rolę, dowodząc, że rozproszony system można zabezpieczyć bez centralnego administratora za pomocą kosztu obliczeniowego. Jednak cena energetyczna, ograniczona przepustowość i długi czas finalizacji sprawiają, że w zastosowaniach cywilnych, administracyjnych czy zdrowotnych jest on nieadekwatny.

Dlatego kluczowym kierunkiem rozwoju jest przejście ku Proof of Stake, Delegated Proof of Stake i modelom hybrydowym. Zmiana konsensusu to nie tylko zmiana algorytmu, lecz przede wszystkim zmiana ekonomii władzy w systemie. Proof of Work zakłada, że bezpieczeństwo wynika z energii i mocy obliczeniowej. Proof of Stake opiera je na ekonomicznym udziale i ryzyku utraty stawki. Delegated Proof of Stake wprowadza delegowanie uprawnień walidacyjnych wybranym reprezentantom. Każde z tych rozwiązań niesie własną filozofię polityczną. PoW jest brutalnym liberalizmem mocy: kto dysponuje energią i sprzętem, ten konkuruje. PoS jest arystokracją udziału: kto posiada stawkę, ten zabezpiecza system i zarabia, ale także ryzykuje. DPoS to demokracja przedstawicielska w wersji protokolarnej: użytkownicy wybierają walidatorów, ryzykując jednak oligarchizację reprezentacji. Jak zwykle w historii instytucji: kiedy pojawia się reprezentacja, pojawiają się i reprezentanci, a wraz z nimi ich własne interesy.

Materialne i prawne fundamenty skalowalności blockchaina

Czwartym, bardziej futurystycznym, lecz istotnym kierunkiem wskazanym w książce są rozwiązania sprzętowe: CNTFET, czyli tranzystory z nanorurek węglowych, oraz integracja z pamięcią SRAM. W przedstawionej wizji mają one zapewnić szybsze przełączanie, niższe opóźnienia, efektywniejszy dostęp do danych i wyższą energooszczędność węzłów blockchainowych. To szczególnie interesujący motyw, gdyż przypomina, że blockchain nie jest wyłącznie abstrakcyjnym protokołem. Każda chmura stoi na ziemi.

Każdy łańcuch bloków wymaga fizycznych maszyn, energii, pamięci, chłodzenia, układów scalonych oraz dostępu do sieci i centrów danych. Cyfrowość nie unieważnia materialności; ona ją jedynie maskuje. W praktyce oznacza to, że przyszłość blockchaina zależeć będzie nie tylko od programistów i ekonomistów tokenów, ale także od inżynierii materiałowej, półprzewodników, energetyki i infrastruktury telekomunikacyjnej. W dobie geopolitycznych napięć wokół chipów, łańcuchów dostaw i suwerenności technologicznej aspekt ten przestaje być detalem. Jeśli infrastruktura zaufania społeczeństwa cyfrowego opiera się na sprzęcie, którego produkcja jest skoncentrowana w kilku regionach świata, decentralizacja protokołu może współistnieć z centralizacją materialnych warunków jego działania. Można mieć rozproszony ledger i bardzo nierozproszony dostęp do układów scalonych.

To nie paradoks, lecz lekcja realizmu. Energooszczędność stanowi osobną oś sporu. Wczesne narracje blockchainowe często traktowały zużycie energii jako cenę wolności od centrum. Jednak społeczeństwo deklarujące transformację klimatyczną, odporność energetyczną i zrównoważony rozwój nie może ignorować kosztów energetycznych systemów cyfrowych. Tyagi wskazuje na przejście od Proof of Work ku Proof of Stake, modelom hybrydowym i warstwom drugim jako element zrównoważonego rozwoju. Zauważa również, że sam blockchain może służyć do monitorowania emisji, śledzenia śladu węglowego i wspierania etycznych łańcuchów dostaw. Tu pojawia się istotne napięcie: technologia może zarówno konsumować energię, jak i pomagać ją racjonalizować. Blockchain energochłonny, służący spekulacji bez społecznej wartości dodanej, jest łatwym celem krytyki. Natomiast blockchain energooszczędny, wykorzystywany do weryfikacji pochodzenia surowców, rozliczania energii odnawialnej czy automatyzacji rynku prosumenckiego, ma zupełnie inny bilans aksjologiczny.

Nie wystarczy pytać o ilość zużytej energii. Należy pytać, jaką funkcję pełni system, co zastępuje, jakie koszty redukuje i czy istnieje prostsza alternatywa. Ekologia bez rachunku funkcji staje się

moralizowaniem, a technologia bez rachunku ekologicznego pychą w silikonowym garniturze. Skalowalność wiąże się również z interoperacyjnością.

W świecie przyszłych zastosowań nie będzie jednego blockchaina. Powstaną różne sieci: publiczne, prywatne, konsorcjalne, administracyjne, branżowe czy medyczne. Problemem nie będzie sama sprawność poszczególnych systemów, lecz ich zdolność do wymiany danych, potwierdzeń, tokenów i tożsamości bez utraty bezpieczeństwa. Tyagi podkreśla, że ustanowienie uniwersalnych standardów będzie kluczowe dla płynnej współpracy między niezależnymi sieciami. Interoperacyjność jest technicznym imieniem pokoju między systemami. Bez niej cyfrowa cywilizacja rozpadnie się na silosy, w których każdy rejestr jest niezmienny, lecz nieczytelny dla innych; każdy token wiarygodny, ale zamknięty; a obywatel, mimo istnienia platform administracyjnych, nadal będzie musiał nosić cyfrowe odpowiedniki papierowych zaświadczeń. Byłaby to ironia: technologia stworzona by ograniczać tarcia zaufania, wytworzyłaby nowe tarcia między protokołami. Przyszłość blockchaina zależy więc od standardów tak samo jak od kryptografii. Bez nich nawet najlepsza innowacja przypomina genialnego samotnika: imponuje, ale nie buduje instytucji.

Skalowalność ma również wymiar prawny. Im głębiej blockchain wchodzi w obszary regulowane – finanse, zdrowie czy administrację – tym bardziej musi spełniać wymogi prawa. Prawo wymaga nie tylko bezpieczeństwa, lecz także odpowiedzialności, możliwości audytu i zgodności z zasadami ochrony danych. Tymczasem niezmienność blockchaina, będąca jego największą zaletą, staje się problematyczna tam, gdzie dane są błędne lub powinny zostać usunięte. Prawdziwa infrastruktura nie może odpowiedzieć obywatelowi: "przepraszamy, protokół nie przewidział pańskiego prawa".

Dlatego dojrzałe projekty będą musiały wykorzystywać rozwiązania hybrydowe: zapisywanie na blockchainie dowodów i metadanych zamiast pełnych danych osobowych, stosowanie architektur off-chain, projektowanie mechanizmów cofania uprawnień oraz tworzenie procedur odpowiedzialności za błędy smart kontraktów.

Blockchain jako warstwa wiarygodności w ekosystemie technologicznym

Nie wystarczy głosić, że „kod jest prawem”. To slogan efektowny, lecz niebezpieczny. Kod potrafi wykonać regułę, ale nie rozumie sprawiedliwości. Prawo bowiem nie jest jedynie automatem wykonawczym; to język ważenia wartości, wyjątków, winy, dobrej wiary, proporcjonalności i odpowiedzialności.

Smart kontrakty stanowią tu szczególnie pouczający przykład. W projekcie Q-BALAK mają one służyć automatyzacji w rolnictwie, łańcuchach dostaw, ochronie zdrowia czy administracji. Mogą na przykład uruchamiać systemy nawadniania, gdy wilgotność gleby spadnie poniżej określonego poziomu, lub automatyzować płatności po potwierdzeniu jakości i dostawy plonów. W logistyce mogą samodzielnie składać zamówienia przy niskim stanie surowców, a następnie realizować przelewy po otrzymaniu towaru.

Obietnica efektywności jest ogromna, jednak automatyzacja staje się cnotą tylko wtedy, gdy warunki są precyzyjnie zdefiniowane, dane wejściowe wiarygodne, a wyjątki przewidziane. Smart kontrakt nie posiada zdrowego rozsądku. Jeśli czujnik poda błędny odczyt, kontrakt może wykonać błędną decyzję z perfekcyjną konsekwencją. Gdy warunki umowy są zbyt sztywne, automatyzacja może utrwalić niesprawiedliwość. Z kolei jeśli dane dostarczy podmiot zainteresowany manipulacją, blockchain zachowa niezmienny zapis nieprawdy.

Kluczowe jest zrozumienie, że blockchain zabezpiecza integralność zapisu po jego wprowadzeniu, ale nie gwarantuje prawdziwości stanu faktycznego przed tym zapisem. Problem „oracle” – czyli wiarygodnego połączenia świata zewnętrznego z łańcuchem bloków – pozostaje jednym z centralnych wyzwań. Nie wystarczy mieć świętą księgę, jeśli kapłan wpisuje do niej fałszywe proroctwa.

Właśnie dlatego przyszłość blockchaina zależy od jakości ekosystemów danych. IoT, czujniki, drony, urządzenia ubieralne czy dokumentacja zdrowotna muszą być nie tylko podłączone do sieci, ale przede wszystkim wiarygodne, kalibrowane i odporne na manipulacje. Synergia blockchaina z AI, IoT, 5G i cyfrowymi bliźniakami tworzy kompleksową infrastrukturę wielotechnologiczną. Blockchain sam w sobie nie widzi świata – robią to czujniki. Nie interpretuje wzorców – od tego jest AI. Nie przesyła danych z minimalnym opóźnieniem – tę rolę pełnią sieci komunikacyjne. Nie symuluje procesów przemysłowych ani miejskich – zajmują się tym cyfrowe bliźniaki.

Blockchain nie zapewnia również prywatności obliczeń; wspierają go w tym techniki kryptograficzne i architektury privacy-preserving. Siła tej technologii nie tkwi zatem w samowystarczalności, lecz w roli warstwy wiarygodności. Jest mniej samotnym bohaterem, bardziej notariuszem przyszłości – choć takim, którego kancelaria mieści się jednocześnie w tysiącach węzłów.

W tym miejscu warto przywołać koncepcję Przemysłu 5.0. O ile Przemysł 4.0 kojarzono z robotyzacją i pełną automatyzacją systemów produkcyjnych, o tyle wersja 5.0 wprowadza korektę humanistyczną: człowiek nie jest tu zbędnym elementem po automatyzacji, lecz współtwórcą

wartości. Model ten opiera się na trzech filarach: human-centricity, sustainability i resilience – czyli orientacji na człowieka, zrównoważeniu i odporności.

Skalowalność jako narzędzie władzy i warunek akceptacji społecznej

Skalowalność blockchaina musi zostać oceniona właśnie w tym świetle. Nie chodzi o to, aby przetwarzać więcej transakcji dla samego przetwarzania. Chodzi o to, aby systemy społeczne były bardziej odporne, mniej podatne na fałszerstwo, bardziej przejrzyste i lepiej dostosowane do potrzeb ludzi. Skalowalność bez human-centricity może oznaczać tylko większą skalę kontroli. Skalowalność bez sustainability może oznaczać większą skalę zużycia energii. Skalowalność bez resilience może oznaczać szybsze rozprzestrzenianie awarii. Skalowalność bez prawa może oznaczać automatyzację bez odpowiedzialności. Skalowalność bez etyki może oznaczać, że niesprawiedliwość dostaje lepszy procesor. Dlatego każdy projekt blockchainowy należy pytać nie tylko o TPS, ale także o społeczny cel, model dostępu, ochronę słabszych uczestników, możliwość audytu, procedury naprawy i koszty uboczne.

Technologia naprawdę nowej generacji nie polega na tym, że stary problem biegnie szybciej. Z tego punktu widzenia szczególnie istotna jest kwestia CBDC. Cyfrowe waluty banków centralnych mogą wymusić standardy skali, których dotychczasowe systemy blockchainowe często nie musiały spełniać. Płatności detaliczne są bezlitosne: muszą działać szybko, masowo, tanio, intuicyjnie i niezawodnie. Jeśli CBDC ma funkcjonować obok gotówki, kart, przelewów, portfeli mobilnych i stablecoinów, musi oferować nie tylko bezpieczeństwo państwowego pieniądza, ale także wygodę użytkownika. A to oznacza, że wszystkie problemy omawiane wyżej - finalność, przepustowość, odporność, prywatność, offline, interoperacyjność, integracja z bankami komercyjnymi - przestają być akademickimi przypisami. Stają się warunkiem politycznej akceptowalności.

CBDC może także zmienić rolę blockchaina w gospodarce. Dotąd blockchain był często przedstawiany jako alternatywa wobec tradycyjnego pieniądza i instytucji finansowych. Wraz z CBDC część jego logiki może zostać wchłonięta przez instytucje publiczne. Tokenizacja, programowalność, automatyczne rozliczenia, audytowalność przepływów, cyfrowa tożsamość płatnicza - wszystko to może zostać wykorzystane w systemie, który nie jest antypaństwowy, lecz państwowo-bankowy. To może przynieść korzyści: szybsze rozliczenia, tańsze płatności transgraniczne, większą odporność systemu, inkluzję finansową. Może też przynieść ryzyka: koncentrację informacji, programowalność pieniądza w sposób ograniczający wolność, nowe formy wykluczenia i zależność obywatela od infrastruktury cyfrowej. Najważniejsza lekcja brzmi więc

następująco: skalowalność nie jest neutralna. Skaluje się nie tylko technologia, ale także model władzy wpisany w technologię. Jeśli system jest przejrzysty, odpowiedzialny i zorientowany na człowieka, skalowanie może zwiększyć dobro społeczne. Jeśli jest nieprzejrzysty, opresyjny albo podporządkowany wąskiej grupie interesów, skalowanie uczyni go tylko bardziej skutecznym narzędziem dominacji. Kiedyś mówiono, że papier wszystko przyjmie. Dzisiaj trzeba powiedzieć: blockchain wszystko zapamięta. I właśnie dlatego trzeba uważać, co, kto i na jakich zasadach do niego wpisuje.

Smart Cities i e-administracja: miasto jako organizm danych, państwo jako infrastruktura zaufania

skalowalność jest technicznym progiem wejścia blockchaina do świata realnych zastosowań, inteligentne miasta i e-administracja są jego pierwszym wielkim egzaminem cywilizacyjnym. W finansach blockchain mógł długo udawać prywatny eksperyment wizjonerów, spekulantów, kryptografów i antybankowych romantyków. W mieście już nie może. Miasto nie jest giełdą tokenów.

Blockchain jako warstwa wiarygodności w Smart Cities

Miasto to ruch drogowy, energia, woda i odpady; to bezpieczeństwo, usługi publiczne, zdrowie mieszkańców, decyzje administracyjne, budżet i nieruchomości. To suma konfliktów interesów i codziennych doświadczeń obywatela. Tu technologia przestaje być obietnicą i zaczyna pachnieć asfaltem, śmieciarką, korkiem, awarią wodociągu i kolejką do urzędu.

Źródło słusznie wskazuje na Smart Cities jako jeden z kluczowych obszarów zastosowania blockchaina. Inteligentne miasto oparte na rozproszonej księdze ma integrować dane z urządzeń brzegowych, sieci komunikacyjnych i czujników IoT za pomocą inteligentnych kontraktów, by optymalizować transport, energetykę czy infrastrukturę. Blockchain pełni tu rolę zdecentralizowanej, odpornej na manipulacje bazy danych, przechowującej ogromne ilości informacji generowanych przez miejską tkankę. To ujęcie jest trafne, lecz wymaga doprecyzowania: inteligentne miasto to nie takie, które jest „naszpikowane technologią”. To miasto, które potrafi rozumnie koordynować zasoby, ograniczać marnotrawstwo, reagować na zakłócenia, chronić mieszkańców i redukować tarcia administracyjne.

Sam czujnik nie jest inteligencją. Kamera nie jest polityką publiczną. Aplikacja nie jest partycypacją, a dashboard nie jest demokracją. Miasto zasługuje na miano inteligentnego dopiero wtedy, gdy dane nie służą ozdobieniu prezentacji burmistrza, lecz realnej poprawie bytu obywateli. W tradycyjnym modelu dane są rozproszone w złym sensie: tkwią w odrębnych systemach i

wydziałach, są nieaktualne, niekompatybilne i trudne do audytu, często zależne od kaprysów dostawców oprogramowania. Transport ma swoje rejestry, energetyka własne systemy, wodociągi osobne czujniki, a administracja zamknięte bazy. Obywatel ma wrażenie, że mieszka nie w jednej wspólnocie samorządowej, lecz w labiryncie cyfrowych księstewek. Każde z nich posiada własny herb w postaci logotypu aplikacji i osobną procedurę resetowania hasła.

Blockchain nie rozwiąże tego chaosu automatycznie, ale może dostarczyć wspólną warstwę wiarygodności. Nie musi przechowywać wszystkich danych miejskich – byłoby to nieefektywne i ryzykowne dla prywatności. Może jednak archiwizować skróty, rejestry zdarzeń, potwierdzenia, uprawnienia oraz historię zmian. W takim modelu miasto nie buduje jednego totalnego magazynu danych, lecz wspólną księgę odniesień. Pozwala ona ustalić, co się wydarzyło, kto wprowadził zmianę, kiedy została zatwierdzona i na jakiej podstawie. To mniej efektowne niż hasło „miasto przyszłości", ale o wiele ważniejsze. Cywilizacja upada nie od braku hologramów, lecz od braku wiarygodnych procedur.

Pierwszym oczywistym obszarem zastosowania jest transport. Inteligentne systemy mogą wykorzystywać IoT do zbierania danych o ruchu i pogodzie, a blockchain wraz ze smart kontraktami może automatyzować optymalizację sygnalizacji czy wyznaczanie tras dla pojazdów uprzywilejowanych. Celem jest ograniczenie korków i poprawa bezpieczeństwa. W tym scenariuszu blockchain nie jest jednak „mózgiem" transportu – tę rolę przejmuje analityka AI i modele predykcyjne.

Blockchain jest raczej pamięcią i gwarantem integralności procesu. Jeśli system zmienia priorytet świateł dla karetki, musi być jasne, że decyzja była autentyczna i wynikała z realnego zdarzenia. Jeśli miasto wprowadza dynamiczne opłaty parkingowe, obywatel powinien móc sprawdzić reguły, według których cena uległa zmianie. Jeśli dane o ruchu służą planowaniu inwestycji, muszą być audytowalne. W przeciwnym razie inteligentny transport łatwo stanie się jedynie inteligentną wymówką dla nieprzejrzystych decyzji.

Blockchain w służbie miast i administracji: od optymalizacji zasobów po cyfrową tożsamość

Drugim obszarem jest energetyka. Tradycyjna sieć była projektowana dla modelu, w którym energia płynie od dużych producentów do odbiorców. Transformacja energetyczna wprowadza jednak logikę rozproszoną: panele fotowoltaiczne, magazyny energii, lokalne wspólnoty, prosumenci, mikrosieci, dynamiczne taryfy czy ładowarki samochodów elektrycznych, a do tego

rosnące znaczenie danych pogodowych. Blockchain może tu umożliwić bezpośredni handel energią peer-to-peer, wspierać równoważenie obciążenia sieci i wprowadzać zautomatyzowane mechanizmy cenowe. To jeden z najbardziej obiecujących, ale i najtrudniejszych regulacyjnie kierunków. Handel energią nie jest przecież prostą wymianą jabłek na targu.

Dotyczy on infrastruktury krytycznej, bezpieczeństwa dostaw, taryf, koncesji, odpowiedzialności operatorów oraz ochrony odbiorców wrażliwych. Blockchain może zarejestrować transakcję między prosumentami, zautomatyzować rozliczenia i potwierdzić pochodzenie energii, ale nie zastąpi polityki energetycznej. Jeśli źle zaprojektujemy rynek lokalny, technologia jedynie pogłębi nierówności: ci, których stać na panele, magazyny i inteligentne liczniki, będą optymalizować koszty, podczas gdy reszta zostanie z rachunkami i kazaniami o innowacji.

Trzeci obszar to gospodarka odpadami i ekologia miejska. Pojawiają się tu interesujące rozwiązania, w których obywatele otrzymują wirtualne waluty, takie jak LitterCoin czy Green Coin, za tagowanie zanieczyszczeń lub oddawanie odpadów do autoryzowanych punktów recyklingu. Przykład ten wydaje się lekki, niemal gadżetowy, lecz kryje głębszą intuicję: blockchain może służyć do budowania mikrosystemów odpowiedzialności i motywacji. Obywatel przestaje być tylko petentem czy podatnikiem; staje się uczestnikiem miejskiej sieci danych, dostawcą informacji i współtwórcą porządku ekologicznego. Należy jednak unikać infantylizacji. Nie każde dobro publiczne warto grywalizować, nie każda postawa obywatelska wymaga tokena, a nie każdy problem rozwiąże aplikacja z monetką. W przeciwnym razie stworzymy groteskowe miasto, w którym segregujemy odpady nie z poczucia wspólnego interesu, lecz by zbierać punkty niczym w programie lojalnościowym stacji benzynowej. Tokenizacja motywacji może być użyteczna, ale nie zastąpi edukacji, infrastruktury, prawa czy odpowiedzialności producentów za odpady. Blockchain nie powinien być cyfrowym listkiem figowym dla braku realnej polityki środowiskowej.

Smart Cities obnażają podwójną naturę technologii. Z jednej strony blockchain zwiększa przejrzystość i odporność systemów miejskich, z drugiej – generuje nowe ryzyka: wykluczenie cyfrowe, nadmierną inwigilację lokalizacyjną, uzależnienie od dostawców technologii czy automatyzację decyzji bez realnej ścieżki odwoławczej. Pojawia się też iluzja, że problem polityczny można rozwiązać zakupem platformy. Bariery wdrożeniowe są przy tym konkretne: przestarzała infrastruktura, brak przepustowości, problemy z interoperacyjnością oraz konieczność ochrony wrażliwych danych zdrowotnych i lokalizacyjnych. To ostatnie jest kluczowe, gdyż inteligentne miasto bywa potencjalnie bardzo ciekawskie.

Wie, gdzie jedziemy, kiedy wyrzucamy odpady, ile zużywamy energii i jakie wzorce mobilności wykazują różne grupy społeczne. Te dane mogą służyć lepszej polityce publicznej, ale mogą też stać się narzędziem profilowania, kontroli, dyskryminacji cenowej lub komercjalizacji życia miejskiego.

Smart city bez praw obywatelskich jest tylko ładnie oświetlonym panoptikonem. Dlatego w centrum systemu musi stać nie technologia, lecz człowiek. Human-centricity, jeden z filarów Przemysłu 5.0, powinien być tu nadrzędną zasadą projektowania. Systemy miejskie muszą być zrozumiałe, dostępne i audytowalne. Obywatel powinien mieć pełną wiedzę o tym, jakie dane są zbierane, w jakim celu, przez kogo i na jak długo.

Niezbędny jest tryb analogowy dla osób wykluczonych cyfrowo oraz realna możliwość zakwestionowania decyzji algorytmicznej. Miasto nie może odpowiedzieć mieszkańcowi: „algorytm zdecydował, proszę się rozejść". Od tego zaczyna się nie innowacja, lecz cyfrowy feudalizm.

Wymiar e-administracji jest jeszcze bardziej delikatny, gdyż dotyka rdzenia relacji obywatel-państwo. Administracja zawsze była technologią zaufania: rejestrowała urodzenia, własność, dyplomy czy podatki. Problem w tym, że dotychczasowa cyfryzacja często była jedynie zmianą nośnika, a nie logiki działania. Papierowy formularz stał się PDF-em, kolejka do okienka – kolejką w systemie, a pieczątka – podpisem kwalifikowanym. Petent pozostał petentem, tyle że z profilem zaufanym.

Blockchain proponuje zmianę radykalną: administrację jako sieć rejestrów odpornych na manipulacje, współdzielonych między instytucjami i zdolnych do automatyzacji procesów. Znajduje to zastosowanie w zarządzaniu cyfrową tożsamością, aktami własności, księgami wieczystymi czy e-usługami. W praktyce oznacza to mniej pośredników, krótsze procedury, mniejsze ryzyko fałszerstw i większą przejrzystość decyzji publicznych.

Blockchain w administracji między emancypacją a nadzorem

Najbardziej klasycznym przykładem są rejestry własności. Księgi wieczyste, akty własności, rejestry gruntów i dokumenty notarialne stanowią fundament bezpieczeństwa obrotu prawnego. Tam, gdzie rejestry są niewiarygodne, gospodarka choruje. Niepewność prawa własności blokuje inwestycje, ułatwia korupcję, wzmacnia silniejszych i uderza w obywatela, który nie dysponuje armią prawników. Blockchain mógłby teoretycznie stworzyć rejestr odporny na manipulacje i nieuprawnione zmiany. Należy jednak pamiętać, że sam rejestr nie tworzy prawa własności – on je jedynie zapisuje. Jeżeli w świecie analogowym doszło do oszustwa, przymusu, błędu, wadliwej decyzji albo historycznej niesprawiedliwości, blockchain może jedynie zamrozić problem w bardziej eleganckiej formie. Niezmienność nie jest tym samym co sprawiedliwość.

Podobnie sprawa wygląda z dyplomami, licencjami zawodowymi i certyfikatami. Blockchain może ułatwić weryfikację autentyczności dokumentów, ograniczyć fałszerstwa i przyspieszyć uznawanie kwalifikacji. W dobie mobilności zawodowej, pracy transgranicznej, migracji i edukacji zdalnej takie rozwiązania mają ogromny potencjał. System musi być jednak zaprojektowany tak, aby nie tworzyć nowych barier. Jeśli dostęp do cyfrowej tożsamości lub portfela certyfikatów wymagałby wysokiej sprawności technologicznej, posiadania stabilnego urządzenia, stałego dostępu do internetu i biegłości w procedurach, osoby najsłabsze mogą zostać wypchnięte z systemu, który miał je obsłużyć. Administracja cyfrowa nie może być klubem dla tych, którzy pamiętają hasło.

Cyfrowa tożsamość jest jednym z najbardziej obiecujących i jednocześnie najbardziej niebezpiecznych zastosowań. Można ją postrzegać jako sposób na przekazanie kontroli nad danymi użytkownikom, eliminację konieczności wielokrotnego udowadniania tożsamości w różnych urzędach oraz ograniczenie oszustw. W modelu idealnym obywatel dysponuje portfelem tożsamości, w którym przechowuje potwierdzone atrybuty: wiek, obywatelstwo, uprawnienia, status zawodowy, certyfikaty, prawo jazdy czy wybrane dane zdrowotne.

Dzięki temu nie musi ujawniać wszystkiego wszystkim. Może potwierdzić spełnienie konkretnego warunku bez udostępniania pełnego zestawu danych, co stanowiłoby rewolucję w kierunku minimalizacji danych. Obywatel nie musiałby za każdym razem oddawać całej teczki swojej tożsamości, aby załatwić jedną sprawę – wystarczyłby kryptograficzny dowód spełnienia warunku. Tu pojawia się potencjał technik takich jak dowody z wiedzą zerową, które pozwalają potwierdzić prawdziwość twierdzenia bez ujawniania pełnej informacji. W duchu tej logiki administracja przyszłości mogłaby pytać mniej i wiedzieć mniej, a mimo to działać sprawniej. Byłaby to cyfrowa dojrzałość: nie „zbierzmy wszystko, bo może się przyda", lecz „zbierzmy tylko to, co konieczne, i pozwólmy obywatelowi zachować kontrolę".

Z drugiej strony cyfrowa tożsamość może stać się narzędziem totalizującym. Połączona z płatnościami, usługami publicznymi, zdrowiem, ruchem miejskim i historią administracyjną, tworzy infrastrukturę o ogromnej sile nadzorczej. W tym miejscu zderzają się dwie wizje: emancypacyjna i kontrolna. W pierwszej obywatel odzyskuje kontrolę nad swoimi danymi; w drugiej państwo i platformy otrzymują idealny klucz do życia obywatela. Technologia pozostaje ta sama – różni się konstytucja systemu.

Dlatego o blockchainie w administracji nie można mówić bez uwzględnienia prawa, kontroli sądowej, zasady proporcjonalności, ochrony danych i procedur odwoławczych. Szczególnie drażliwym tematem jest głosowanie elektroniczne oparte na blockchainie. Technologia ta może rejestrować głosy jako niezmienne transakcje, zabezpieczać integralność procesu, a jednocześnie zachowywać poufność wyborców dzięki narzędziom kryptograficznym. Może również ułatwić

głosowanie zdalne przez smartfony lub komputery, znosząc bariery logistyczne. Brzmi to kusząco w obliczu spadku frekwencji i oczekiwania wygody usług cyfrowych, jednak właśnie tutaj należy zachować największy sceptycyzm.

Wybory nie są zwykłą transakcją. Wymagają jednoczesnej identyfikacji uprawnionego wyborcy, tajności głosu, odporności na przymus i kupowanie głosów, przejrzystości procedury, możliwości niezależnej kontroli oraz powszechnego zaufania społecznego. Blockchain może pomóc w integralności zapisu, ale nie rozwiązuje problemu środowiska głosowania. W lokalu wyborczym państwo tworzy przestrzeń kontrolowaną: kabina, komisja, urna i obserwatorzy. W głosowaniu zdalnym obywatel może znajdować się pod presją pracodawcy, rodziny, lokalnego układu lub „życzliwego pomocnika", który akurat trzyma telefon. Nie wszystko, co wygodne, jest demokratycznie bezpieczne.

Nie oznacza to konieczności odrzucenia wszelkich eksperymentów, lecz wskazuje, że blockchainowe głosowanie powinno być traktowane jak technologia wysokiego ryzyka ustrojowego. Można ją badać i testować w ograniczonych zastosowaniach – w organizacjach, konsultacjach czy budżetach partycypacyjnych – ale wdrożenie w wyborach powszechnych wymagałoby wyjątkowo silnych gwarancji. Demokracja nie jest aplikacją, którą aktualizuje się po wykryciu błędu. Gdy błąd dotyczy wyborów, nie da się powiedzieć: „przepraszamy, poprawimy w następnej wersji". System wyborczy musi być nie tylko bezpieczny, ale i zrozumiały społecznie. Jeśli obywatel nie rozumie, dlaczego ma ufać wynikowi, sama kryptografia nie wystarczy.

DAO i blockchain w administracji: między partycypacją a cyfrowym wykluczeniem

W tym miejscu pojawia się koncepcja DAO, czyli zdecentralizowanych organizacji autonomicznych. Sugeruje ona, że przyszłość zarządzania miejskiego może ewoluować w stronę systemów demokratyzujących rządy, dając obywatelom bezpośredni wpływ na alokację budżetu i kształtowanie lokalnych polityk. To jedna z najbardziej pociągających wizji, gdyż łączy blockchain z realną partycypacją. Zamiast sprowadzać obywatela do roli wyborcy pojawiającego się przy urnie raz na kilka lat, czyni go współuczestnikiem mikrodecyzji – osobą współzarządzającą wspólnym budżetem, głosującą nad priorytetami i kontrolującą wykonanie zadań.

Implementacja DAO w przestrzeni miejskiej wymaga jednak większej ostrożności niż w świecie kryptowalut. Miasto nie jest klubem inwestorów w tokeny. Decyzje lokalne dotyczą ludzi, którzy mogą nie posiadać kompetencji cyfrowych, czasu lub zasobów niezbędnych do ciągłego głosowania.

Uczestnictwo nie może premiować wyłącznie najaktywniejszych i najlepiej zinformatyzowanych; demokracja bezpośrednia wsparta technologią, choć zdolna ożywić wspólnotę, może łatwo przeobrazić się w tyranię zaangażowanej mniejszości. Jeśli głosowanie nad budżetem dzielnicy wymaga portfela cyfrowego i biegłości w procedurach, emerytka bez smartfona przestaje być obywatelką pełnej kategorii. A przecież miasto należy także do niej.

Efektywna e-administracja oparta na blockchainie nie powinna zatem polegać na zastąpieniu polityki kodem. Jej celem powinno być uczynienie wybranych procesów bardziej przejrzystymi i odpornymi, przy jednoczesnym zachowaniu przestrzeni na deliberację, odpowiedzialność urzędniczą, kontrolę sądową oraz polityczne rozstrzyganie wartości. Państwo nie może abdykować na rzecz smart kontraktu; powinno go wykorzystywać tam, gdzie reguły są jasne, dane wiarygodne, a automatyzacja usprawnia proces bez odbierania obywatelowi prawa do sprzeciwu. Automatyzujmy kolejkę, nie sumienie. Automatyzujmy potwierdzenie, nie sprawiedliwość.

E-administracja blockchainowa może skutecznie ograniczać korupcję i arbitralność tam, gdzie problemem jest manipulacja rejestrem, niejawne zmiany czy brak ścieżki audytu. Gdy każda modyfikacja w rejestrze publicznym pozostawia trwały ślad, trudniej udawać, że „system nie pamięta". Logowanie dostępu do dokumentów utrudnia ukrycie nieuprawnionego wglądu, a powiązanie decyzji administracyjnej z konkretnymi danymi wejściowymi i podpisem osoby odpowiedzialnej ułatwia rekonstrukcję procesu. Administracja często broni się przed przejrzystością argumentem o złożoności procedur. Blockchain odpowiada na to krótko: złożoność nie zwalnia z pamięci.

Należy jednak ostrzec przed pułapką pozornej przejrzystości. Można publikować hashe dokumentów, których nikt nie widzi, tworzyć niezmienne, lecz niezrozumiałe rejestry lub mówić o audycie przy zamkniętym kodzie. Można decentralizować zapis, jednocześnie centralizując dostęp i rozpraszać dane, koncentrując władzę interpretacji. Przejrzystość techniczna nie jest tożsama z przejrzystością społeczną. Obywatel nie kontroluje administracji samym faktem istnienia zapisu w łańcuchu bloków. Kontroluje ją wtedy, gdy posiada prawo, kompetencje i narzędzia oraz instytucjonalne wsparcie pozwalające ten zapis odczytać i wykorzystać. W tym miejscu kluczową rolę zaczynają odgrywać standardy publiczne.

Ryzyko cyfrowego uzależnienia w e-administracji

Jeśli miasta i państwa będą wdrażać blockchain poprzez przypadkowe zamówienia, zamknięte platformy i obietnice „rewolucji w 90 dni", skończą na cyfrowym uzależnieniu. Administracja stanie się zakładnikiem vendor lock-in – sytuacji, w której podmiot publiczny nie może łatwo zmienić

dostawcy, ponieważ dane, procedury i integracje zostają zamknięte w prywatnym ekosystemie. Byłby to ponury żart historii: technologia stworzona do decentralizacji, wdrożona w sposób wzmacniający monopol korporacyjny. Decentralizacja na folderze, centralizacja na fakturze.

Aby tego uniknąć, e-administracja potrzebuje otwartych standardów, interoperacyjności, audytu kodu i przejrzystych zamówień publicznych, a także minimalizacji danych, ochrony prywatności oraz mechanizmów kontroli obywatelskiej. Przede wszystkim jednak potrzebuje kompetentnego państwa. Suwerenności cyfrowej nie da się kupić w przetargu, jeśli administracja nie rozumie technologii, którą zamawia. Instytucje publiczne muszą dysponować własną wiedzą ekspercką: prawną, informatyczną, ekonomiczną i etyczną, a także w obszarze cyberbezpieczeństwa. W przeciwnym razie będą jedynie ceremonialnie zatwierdzać rozwiązania zaprojektowane przez tych, którym zależy na ich nieprzejrzystości. Smart Cities i e-administracja stawiają więc kluczowe pytanie polityczne: czy technologia zwiększy władzę obywatela nad instytucją, czy władzę instytucji nad obywatelem?

Odpowiedź nie tkwi w samym protokole. Wynika ona z projektu prawnego, architektury danych, modelu dostępu, kultury administracyjnej i jakości demokracji. Blockchain może być narzędziem obywatelskiej kontroli, ale może stać się również instrumentem administracyjnej perfekcji bez empatii. A perfekcyjna biurokracja pozbawiona empatii to nie nowoczesność – to Kafka z chmurą obliczeniową.

Miasto przyszłości nie powinno wiedzieć o mieszkańcu wszystkiego; powinno wiedzieć wystarczająco dużo, by działać sprawnie, i wystarczająco mało, by nie naruszać jego wolności. Państwo przyszłości nie powinno automatyzować każdej decyzji, lecz jedynie rutynę, pozostawiając człowieka tam, gdzie niezbędna jest odpowiedzialność, interpretacja i sprawiedliwość. Blockchain może pomóc zbudować taką administrację, o ile zostanie potraktowany nie jako magiczny skrót, lecz jako element dojrzałej filozofii instytucjonalnej.

Blockchain jako strażnik intymności i przepływu danych medycznych

W zdrowiu chodzi o ciało, chorobę i ryzyko śmierci; o intymność, lęk, zaufanie do lekarza oraz prawo do prywatności i skutecznego leczenia. Tutaj nie wystarczy stwierdzenie, że dane są zasobem. Dane medyczne to szczególny rodzaj zapisu: mówią o słabości człowieka, jego historii biologicznej, obciążeniach rodzinnych, diagnozach, lekach i terapiach. Dokumentują nałogi, zabiegi, badania genetyczne, choroby psychiczne, reprodukcję, starzenie się i śmierć. Kto

kontroluje te dane, nie włada jedynie informacją. Kontroluje fragment ludzkiej bezbronności. Blockchain może stać się fundamentem nowej organizacji opieki zdrowotnej. Tradycyjne systemy elektronicznej dokumentacji medycznej są często scentralizowane i rozproszone instytucjonalnie, co czyni je podatnymi na awarie, ataki hakerskie czy nieautoryzowany dostęp, a także generuje brak interoperacyjności między szpitalami. Problem nie sprowadza się tylko do faktu, że dane istnieją w wielu miejscach. Chodzi o to, że pacjent często nie ma realnej kontroli nad własnym śladem medycznym, a instytucje nie potrafią wymieniać informacji w sposób szybki, bezpieczny i zgodny z prawem. W medycynie opóźnienie informacyjne może mieć konsekwencje kliniczne. Brak dostępu do historii leczenia, alergii, wyników badań czy danych obrazowych nie jest zwykłą niedogodnością administracyjną. Może prowadzić do błędów, powtórnych badań, zbędnych kosztów i złych decyzji terapeutycznych w czasie, którego pacjentowi często brakuje. Zarazem zbyt swobodny przepływ danych medycznych może naruszać prywatność, zwiększać ryzyko dyskryminacji ubezpieczeniowej, zawodowej lub społecznej oraz tworzyć pokusę komercyjnej eksploatacji informacji o zdrowiu. Medycyna cyfrowa żyje więc w napięciu między dostępnością danych a ich ochroną. Potrzebuje jednocześnie przepływu i granicy. Blockchain jest interesujący właśnie dlatego, że pozwala projektować ten przepływ bez całkowitego rozbrojenia granicy. Wizja systemów takich jak CareBlock opiera się na rozwiązaniu hybrydowym. Ciężkie pliki medyczne – obrazy rezonansu magnetycznego, tomografii czy obszerna dokumentacja pacjenta – nie powinny być przechowywane bezpośrednio w blockchainie. Byłoby to kosztowne, niewydajne i sprzeczne z zasadą minimalizacji danych. Zamiast tego dane mogą być przechowywane poza łańcuchem (off-chain), na przykład w zdecentralizowanych sieciach plików takich jak IPFS, podczas gdy na blockchainie zapisuje się jedynie kryptograficzny skrót – hash – stanowiący niezmienne odniesienie do dokumentu. Ten model jest istotny, gdyż stanowi dojrzałą odpowiedź na jeden z najczęstszych błędów w myśleniu o tej technologii. Nie chodzi o to, aby "wrzucić medycynę na łańcuch bloków". To brzmiałoby efektownie, ale byłoby fatalne.

Blockchain jako strażnik danych medycznych i autentyczności leków

Blockchain powinien stać się warstwą integralności, zgody, audytu i odniesienia, podczas gdy same dane medyczne pozostaną w bezpiecznych, kontrolowanych środowiskach. Hash pozwoli sprawdzić, czy dokument nie został zmieniony, smart kontrakt przejmie kontrolę nad dostępem, a logi utrwalą, kto, kiedy i w jakim celu próbował uzyskać wgląd. Pacjent zyska możliwość udzielenia zgody granularnej – precyzyjnie określonej: konkretnemu lekarzowi, konkretnej placówce, na konkretny zakres danych i w określonym czasie.

To punkt zwrotny. W tradycyjnym modelu pacjent bywa obiektem dokumentacji; w modelu nowej generacji powinien stać się podmiotem zarządzania dostępem do własnych danych. Nie chodzi o to, by pacjent samodzielnie administrował całą medycyną jak domowym folderem na pulpicie, lecz by system uznał jego prawo do kontroli, wiedzy i zgody. Pacjent powinien widzieć, kto zaglądał do jego dokumentacji i móc ograniczać dostęp tam, gdzie nie jest on konieczny. Musi mieć możliwość udostępnienia danych lekarzowi w sytuacji nagłej, ale i prawo do ochrony przed ciekawością osób nieuprawnionych. W medycynie prywatność nie jest kaprysem – jest warunkiem godności. Blockchain może tu pełnić rolę cyfrowego strażnika progu. Nie lekarza, nie sędziega, nie etyka, lecz strażnika reguł dostępu. Smart kontrakt wykona wcześniej zdefiniowaną zgodę, dopuszczając wgląd tylko przy spełnieniu określonych warunków i automatycznie wygaszając uprawnienia po zakończeniu terapii, konsultacji czy badania klinicznego. Może również zapisać każdą próbę dostępu, w tym nieudaną.

To ostatnie ma kluczowe znaczenie. Nieautoryzowany wgląd w dane medyczne jest często trudny do wykrycia i jeszcze trudniejszy do udowodnienia. Blockchainowa ścieżka audytu mogłaby zmienić kulturę odpowiedzialności: „system nie pamięta” przestałoby być wygodnym alibi. Tu jednak konieczna jest sceptyczna korekta. Pacjent nie może zostać obciążony pełną odpowiedzialnością za zarządzanie skomplikowanymi zgodami w systemie, którego nie rozumie. Hasło „pacjent kontroluje dane” brzmi pięknie, ale może stać się przerzuceniem ciężaru na osobę chorą, starszą, przerażoną diagnozą, wykluczoną cyfrowo lub po prostu niemającą kompetencji technicznych. Prawdziwe upełnomocnienie wymaga projektowania przyjaznego, opiekuńczego i wielokanałowego. System musi oferować domyślne ustawienia chroniące prywatność, zrozumiałe komunikaty, wsparcie analogowe, reprezentację ustawową oraz procedury nagłe i możliwość odwołania. Samo przekazanie panelu zgód nie jest jeszcze wolnością. Czasem jest tylko cyfrowym formularzem winy.

Kolejnym obszarem jest farmaceutyczny łańcuch dostaw. Blockchain może służyć do śledzenia leków od producenta, przez dystrybutora, aż po aptekę, eliminując z rynku produkty podrobione, skażone lub transportowane w niewłaściwych warunkach. Smart kontrakty mogą współpracować z czujnikami IoT – na przykład mierzącymi temperaturę w chłodniach – aby potwierdzać zachowanie wymogów transportowych. To zastosowanie jest szczególnie istotne, gdyż dotyczy problemu, w którym zaufanie do opakowania nie wystarcza. Lek jest towarem szczególnym: jego jakość, pochodzenie, temperatura przechowywania, autentyczność i integralność opakowania mogą decydować o życiu. Blockchain może stworzyć paszport leku, w którym każdy etap drogi pozostawia zapis: producent potwierdza serię, dystrybutor przyjęcie, hurtownia warunki magazynowania, transport czujniki temperatury, a apteka odbiór. System może wówczas błyskawicznie wykrywać rozbieżności. W idealnym scenariuszu pacjent lub farmaceuta weryfikuje autentyczność produktu, a organy nadzoru szybciej identyfikują źródło problemu.

Nie należy jednak ulegać magii zapisu. Blockchain potwierdza jedynie to, co zostało wprowadzone do systemu. Jeśli na wejściu pojawi się fałszywa informacja, źle skalibrowany czujnik, skorumpowany operator lub nieuczciwy podmiot, łańcuch może utrwalić nieprawdę. Dlatego blockchain w farmacji musi być powiązany z certyfikacją, inspekcją, odpowiedzialnością producentów, audytem urządzeń IoT, kontrolą jakości i sankcjami.

W przeciwnym razie stworzymy technologię, która bardzo elegancko zapisuje kłamstwo. A kłamstwo z hashem nadal jest kłamstwem – tylko trudniej je potem udawać za przypadek.

Blockchain w medycynie: między precyzyjną opieką a ryzykiem nadzoru

Trzecim wymiarem są medyczne systemy cyber-fizyczne i Internet Rzeczy. Integracja blockchaina z inteligentnymi sensorami oraz urządzeniami ubieralnymi pozwala na zbieranie w czasie rzeczywistym parametrów życiowych: tętna, ciśnienia, saturacji, rytmu serca, poziomu aktywności czy jakości snu, a w zaawansowanych systemach także danych kluczowych dla chorób przewlekłych. Informacje te mogą być analizowane przez modele uczenia maszynowego i głębokiego uczenia, w tym sieci LSTM, które interpretując sekwencje czasowe, potrafią przewidywać anomalie, takie jak drgawki czy incydenty kardiologiczne. Blockchain ma tu za zadanie zabezpieczyć integralność wrażliwych strumieni danych biomedycznych przed nieuprawnioną modyfikacją. To jeden z najbardziej obiecujących, ale i najbardziej niepokojących scenariuszy.

Zdalne monitorowanie może fundamentalnie zmienić opiekę nad osobami starszymi oraz pacjentami kardiologicznymi, diabetologicznymi, neurologicznymi czy pooperacyjnymi. Pozwala skracać hospitalizacje, umożliwia wcześniejszą interwencję, ogranicza koszty i wspiera medycynę domową. Zamiast czekać, aż pacjent trafi do szpitala w stanie ostrym, system może wykryć odchylenia znacznie wcześniej. Medycyna staje się mniej epizodyczna, bardziej ciągła. Lekarz widzi nie tylko wynik z gabinetu, ale rytm życia organizmu. Jednak ta ciągłość monitorowania może łatwo przeobrazić się w ciągłość nadzoru. Jeśli dane z urządzeń ubieralnych trafią do ubezpieczycieli, pracodawców, platform usługowych lub nieprzejrzystych brokerów danych, pacjent stanie się jedynie ocenianym obiektem ryzyka. „Nie chodzi pan wystarczająco dużo, składka rośnie”. „Śpi pani za krótko, profil ryzyka niekorzystny”. „Historia pulsu wskazuje stres, zdolność kredytowa spada”. Brzmi to jak satyra? Historia technologii uczy jednak, że dzisiejsza satyra bywa jutrzejszą funkcją premium. Dlatego blockchainowa ochrona integralności danych musi iść w parze z prawną ochroną przed ich wtórnym, dyskryminacyjnym wykorzystaniem.

W tym miejscu powraca kwestia AI. Algorytmy mogą wykrywać anomalie szybciej niż człowiek, ale mogą również się mylić. Fałszywy alarm wywołuje niepotrzebny stres i koszty; brak alarmu może mieć skutki tragiczne. Gdy system przewiduje ryzyko zawału, napadu padaczkowego czy pogorszenia stanu zdrowia, musi być jasne, kto ponosi odpowiedzialność: producent urządzenia, dostawca modelu, placówka medyczna, lekarz, operator danych, a może pacjent, który nie zareagował na powiadomienie? Blockchain pomoże ustalić historię zdarzeń, wersję modelu, dane wejściowe i czas powiadomienia. Odpowiedzialność pozostaje jednak kategorią prawną i etyczną, a nie tylko techniczną.

Czwartym obszarem jest medycyna spersonalizowana i badania kliniczne. Blockchain może wspierać organizację badań, udostępnianie wielkich zbiorów danych przy zachowaniu prywatności oraz rozwój terapii dostosowanych do indywidualnych uwarunkowań genetycznych, alergicznych i klinicznych pacjenta. Może również przyspieszać reakcję na epidemie poprzez bezpieczną wymianę informacji między instytutami, rządem a szpitalami. Jest to szczególnie istotne w epoce, w której medycyna przestaje być nauką o „średnim pacjencie". Terapie celowane, onkologia precyzyjna, farmakogenomika i sekwencjonowanie genomowe tworzą model oparty na coraz bardziej indywidualnym profilu. Taka personalizacja wymaga jednak ogromnych ilości danych z różnych ośrodków, populacji i krajów.

Tu pojawia się klasyczny konflikt: nauka potrzebuje szerokiego dostępu do informacji, pacjent ochrony prywatności, a system wiarygodności i kontroli zgód. Blockchain może w tym układzie pełnić rolę rejestru zgód badawczych, ścieżki dostępu oraz mechanizmu rozliczalności. Pacjent mógłby udzielać zgody na konkretny typ badań, wycofywać ją lub monitorować, jakie instytucje korzystały z jego danych; badacz zaś zyskałby pewność co do wiarygodności źródła. W połączeniu z uczeniem federacyjnym możliwe jest trenowanie modeli na danych pozostających lokalnie w szpitalach, bez konieczności przesyłania surowych informacji. Blockchain potwierdzałby wówczas udział węzłów i zgodność procesu z regułami. Nie oznacza to jednak końca problemów.

Zgoda pacjenta w badaniach medycznych jest kwestią złożoną. Czy pacjent naprawdę rozumie, na co się zgadza? Czy zgoda na jedno badanie obejmuje przyszłe wykorzystanie danych? Czy dane genomowe nie dotyczą również krewnych, którzy zgody nie wyrazili? Czy można realnie zanonimizować bogate i rzadkie dane medyczne połączone z innymi zbiorami? I wreszcie: czy pacjent powinien otrzymywać wynagrodzenie za udostępnienie danych? Pytanie brzmi, czy dane zdrowotne są dobrem osobistym, zasobem naukowym, własnością, dobrem wspólnym, czy wszystkim tym naraz.

Automatyzacja rozliczeń wymaga nadzoru humanistycznego

Blockchain nie odpowie na te pytania; może jedynie sprawić, że odpowiedzi będą lepiej zapisane, egzekwowalne i kontrolowalne. Kolejnym wymiarem są ubezpieczenia zdrowotne i rozliczenia. Blockchain może wspierać zarządzanie tym obszarem, ograniczając koszty oraz liczbę oszustw dzięki automatyzacji roszczeń. To tutaj smart kontrakty kuszą szczególnie mocno: jeśli procedura została wykonana, dokumentacja potwierdzona, a warunki polisy spełnione, płatność mogłaby zostać uruchomiona automatycznie. Mniej papieru, sporów, opóźnień i pośredników – brzmi to rozsądnie. Jednak w medycynie roszczenie rzadko jest prostą operacją logiczną. Leczenie bywa niestandardowe, przypadki bywają graniczne, dokumentacja niepełna, a człowiek nie mieści się w warunku "jeżeli-to".

Automatyzacja rozliczeń może zatem ograniczyć biurokrację, ale jednocześnie usztywnić system. Jeśli smart kontrakt odmówi pokrycia świadczenia z powodu jednego niespełnionego parametru, pacjent stanie twarzą w twarz z automatem – szybkim i logicznym, lecz bezdusznym. Dlatego w ubezpieczeniach zdrowotnych smart kontrakty powinny obsługiwać rutynę, a nie zastępować tryby wyjątkowe, odwołania, ocenę medyczną czy zasadę proporcjonalności. Automatyzacja bez humanizmu jest administracją o twarzy kalkulatora. A kalkulator, choć niezwykle pożyteczny, nigdy nie powinien być rzecznikiem pacjenta. Ta kwestia prowadzi nas do kolejnego obszaru: cyberbezpieczeństwa. Dane medyczne są jednym z najcenniejszych celów ataków, gdyż łączą w sobie wartość finansową, szantażową i identyfikacyjną. Numer karty można zmienić, ale historii choroby, genomu czy diagnozy psychiatrycznej – już nie.

Blockchain jako kręgosłup zaufania w służbie człowieka

Tyagi przedstawia blockchain jako warstwę ochrony przed manipulacją danymi oraz element szerszej architektury bezpieczeństwa, opartej na AI, wykrywaniu anomalii, logice rozmytej, modelach LSTM i analizie wzorców. To kluczowe, gdyż współczesne cyberbezpieczeństwo nie może być wyłącznie murem. Musi być układem odpornościowym.

AI wykrywa nietypowe zachowania, podejrzane dostępy, anomalie w ruchu sieciowym, próby phishingu czy odchylenia od normalnych wzorców. Blockchain z kolei zabezpiecza integralność logów i utrudnia ich późniejszą modyfikację. Gdy napastnik włamie się do systemu, zazwyczaj stara się zatrzeć ślady – niezmienna ścieżka audytu skutecznie ogranicza ten manewr. W medycynie,

gdzie błąd lub atak mogą mieć skutki fizyczne, taka pamięć systemu nie jest jedynie technicznym dodatkiem, lecz elementem bezpieczeństwa pacjenta.

Cyberbezpieczeństwo oparte na blockchainie nie jest jednak absolutne. Smart kontrakty mogą zawierać błędy, klucze prywatne mogą zostać utracone lub skradzione, a interfejsy użytkownika pozostają podatne na phishing. Słabymi punktami bywają mosty między systemami, źle skonfigurowane węzły czy dane off-chain. Ponadto człowiek, będący najbardziej pomysłowym i jednocześnie najkruchszym ogniwem każdej architektury, wciąż może kliknąć w złośliwy link. Technologia nie zwalnia więc z higieny bezpieczeństwa; przeciwnie – im bardziej krytyczna infrastruktura, tym silniejszej potrzeby procedur, szkoleń, audytów i kultury zgłaszania incydentów wymaga.

Istotny jest tu również wymiar międzynarodowy. Zdrowie nie zna granic: ludzie migrują, podróżują, chorują za granicą czy korzystają z telemedycyny, a pandemie nie zatrzymują się na szlabanach. Blockchain może wspierać interoperacyjność dokumentacji i certyfikatów zdrowotnych, lecz tylko pod warunkiem istnienia wspólnych standardów danych, tożsamości, zgód oraz odpowiedzialności.

W przeciwnym razie powstaną narodowe lub korporacyjne wyspy zdrowotne. Każda będzie bezpieczna we własnej narracji, a pacjent nadal będzie woził historię choroby w pliku PDF albo, bardziej klasycznie, w reklamówce. Medycyna blockchainowa wymaga zatem nie tylko technologii, ale nowego kontraktu instytucjonalnego. Pacjent powinien sprawować kontrolę, lecz nie być samotnym administratorem. Lekarz musi mieć szybki dostęp do danych, ale bez nieograniczonej ciekawości systemowej. Szpital powinien wymieniać informacje, a nie handlować prywatnością. Badacz ma korzystać z danych z poszanowaniem zgody i minimalizacją ryzyka. Państwo powinno tworzyć standardy i nadzór, ale nie budować medycznego panoptikonu. Firmy technologiczne zaś dostarczać narzędzia, nie przejmując władzy nad infrastrukturą zdrowia.

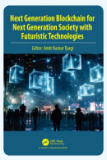
Każdy z tych warunków jest trudny do spełnienia, lecz razem stanowią miarę dojrzałości systemu. W tej perspektywie opieka zdrowotna 5.0 nie jest kolejnym etapem cyfryzacji, lecz próbą przejścia od medycyny instytucji do medycyny relacyjnej – spersonalizowanej, odpornej i skoncentrowanej na człowieku. Blockchain może stać się jej kręgosłupem zaufania, ale nie sercem. Serce pozostaje w relacji lekarza z pacjentem, w etyce zawodowej, prawie do informacji oraz ochronie godności. Technologia może uporządkować zapis i ograniczyć nadużycia, lecz nie może zapomnieć, że po drugiej stronie rekordu jest człowiek, a nie rekord.

Blockchain w zdrowiu ma sens wtedy, gdy pacjent zyskuje kontrolę, lekarz lepszą informację, system odporność, a nauka bezpieczny dostęp do danych. Traci go, gdy staje się kolejną warstwą

technicznej dominacji i cyfrowych barier. Dane medyczne nie są ropą XXI wieku. To popularne, lecz moralnie podejrzane porównanie; ropa służy do wydobywania wartości, dane medyczne zaś przede wszystkim do ochrony osoby. Kto o tym zapomina, może zbudować bardzo nowoczesny system, by stworzyć w nim bardzo stare nadużycie.

> Blockchain może stać się najdoskonalszym strażnikiem prawdy i transparentności, ale tylko pod warunkiem, że nie zapomnimy o różnicy między niezmiennością zapisu a sprawiedliwością rozstrzygnięcia. W świecie, gdzie kod staje się konstytucją, największym zagrożeniem nie jest błąd w protokole, lecz przekonanie o neutralności narzędzia, które zarządza naszym zdrowiem i wolnością. Ostatecznie to nie szybkość transakcji, lecz odwaga w projektowaniu systemów zorientowanych na człowieka zdecyduje, czy budujemy infrastrukturę wyzwolenia, czy jedynie bardziej elegancką formę cyfrowego feudalizmu.

Inspiracje

[1] 

"Next Generation Blockchain for Next" Amit Kumar Tyagi

2026 | CRC Press | ISBN: 9781041026075

Amit Kumar Tyagi jest badaczem akademickim i adiunktem, obecnie związanym z Narodowym Uniwersytetem Nauk Kryminalistycznych w Gandhinagarze w stanie Gudżarat w Indiach. W 2018 roku uzyskał stopień doktora na Uniwersytecie Centralnym w Pondicherry. Jego bogata kariera naukowa obejmuje stanowiska w różnych instytucjach, w tym w Instytucie Technologii Vellore (VIT) i Narodowym Instytucie Technologii Mody (NIFT). Dr Tyagi jest starszym członkiem IEEE i wniósł znaczący wkład w rozwój technologii blockchain, uczenia maszynowego, nauki o danych, systemów cyberfizycznych i inteligentnych komputerów. Jest autorem i redaktorem wielu książek oraz opublikował ponad 350 artykułów naukowych. Jego praca koncentruje się na rozwiązywaniu problemów związanych z prywatnością i bezpieczeństwem w nowych technologiach, w tym w aplikacjach samochodowych i medycznych systemach cyberfizycznych. Otrzymał wiele nagród Faculty Research Awards za wkład w badania naukowe i działalność naukową.

Amit Kumar Tyagi *is an academic researcher and Assistant Professor currently affiliated with the National Forensic Sciences University in Gandhinagar, Gujarat, India. He earned his Ph.D. in 2018 from Pondicherry Central University. His extensive academic career includes positions at various institutions, including the Vellore Institute of Technology (VIT) and the National Institute of Fashion Technology (NIFT). Dr. Tyagi is a senior member of the IEEE and has contributed significantly to the fields of blockchain technology, machine learning, data science, cyber-physical systems, and smart computing. He has authored and edited numerous books and published over 350 research articles. His work focuses on addressing privacy and security challenges in emerging technologies, including vehicular applications and medical cyber-physical systems. He has received multiple Faculty Research Awards for his contributions to research and academia.*

National Forensic Sciences University

Literatura uzupełniająca

Książki

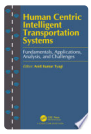
Książki autora i dzieła przywołane w tekście:



[1] "Advanced Machine Learning"

Dr. Amit Kumar Tyagi, Dr. Khushboo Tripathi, Dr. Avinash Kumar Sharma

2024 | BPB Publications | ISBN: 9789355516343



[2] "Human Centric Intelligent Transportation Systems"

Amit Kumar Tyagi

2026 | CRC Press | ISBN: 9781040625033



[3] "Internet of Things Theory and Practice"

Amit Kumar Tyagi

2022 | BPB Publications | ISBN: 9789355512437



[4] "6G-Enabled Technologies for Next Generation"

Amit Kumar Tyagi, Shrikant Tiwari, Shivani Gupta, Anand Kumar Mishra

2024 | John Wiley & Sons | ISBN: 9781394258345



[5] "Intelligent Transportation Systems: Theory and Practice"

Amit Kumar Tyagi, Niladhuri Sreenath

2022 | Springer Nature | ISBN: 9789811976223

[6] "Artificial Intelligence for Cyber Security: Methods, Issues and Possible Horizons Or Opportunities"

Sanjay Misra, Amit Kumar Tyagi

2021 | ISBN: 9783030722371

Książki autorów przywoływanych i literatura pokrewna:

[7] "Zero Knowledge Infinite Trust"

Eli Ben-Sasson

Artykuły naukowe

Prace autorów przywoływanych w tekście:

[1] "How Can One Take Delight in the World Unless One Flees to It for Refuge ? ” : The Fear of Freedom in"

E. Fromm., Franz Kafka

2019

Źródło

Artykuły naukowe autora:

[2] "The Role of Machine Learning Techniques in Internet of Things-Based Cloud Applications"

Shashvi Mishra, Amit Kumar Tyagi

2022 | Internet of things | DOI: 10.1007/978-3-030-87059-1_4

Źródło

[3] "Blockchain—Internet of Things Applications: Opportunities and Challenges for Industry 4.0 and Society 5.0"

Amit Kumar Tyagi, Sathian Dananjayan, Deepshikha Agarwal, Hasmath Farhana Thariq Ahmed

2023 | Sensors | DOI: 10.3390/s23020947

Źródło

[4] "The Future with Industry 4.0 at the Core of Society 5.0: Open Issues, Future Opportunities and Challenges"

Meghna Mannoj Nair, Amit Kumar Tyagi, N. Sreenath

2021 | DOI: 10.1109/iccci50826.2021.9402498

Źródło

[5] "Intelligent Automation Systems at the Core of Industry 4.0"

Amit Kumar Tyagi, Terrance Frederick Fernandez, Shashvi Mishra, Shabnam Kumari

2021 | Advances in intelligent systems and computing | DOI: 10.1007/978-3-030-71187-0_1

Źródło

[6] "Industry 5.0 for Healthcare 5.0: Opportunities, Challenges and Future Research Possibilities"

L. Gomathi, Anand Kumar Mishra, Amit Kumar Tyagi

2023 | DOI: 10.1109/icoei56765.2023.10125660

Źródło

[7] **"Cyber Physical Systems: Analyses, challenges and possible solutions"**

Amit Kumar Tyagi, N. Sreenath

2021 | Internet of Things and Cyber-Physical Systems | DOI: 10.1016/j.iotcps.2021.12.002

Źródło

[8] **"Machine Learning and Deep Learning: Open Issues and Future Research Directions for the Next 10 Years"**

Akshara Pramod, Harsh Sankar Naicker, Amit Kumar Tyagi

2021 | DOI: 10.1002/9781119785750.ch18

Źródło

[9] **"AI, IoT, blockchain, and cloud computing: The necessity of the future"**

Meghna Manoj Nair, Amit Kumar Tyagi

2023 | Elsevier eBooks | DOI: 10.1016/b978-0-323-96146-2.00001-2

Źródło

[10] **"RETRACTED: Autonomous Intelligent Vehicles (AIV): Research statements, open issues, challenges and road for future"**

Amit Kumar Tyagi, S Aswathy

2021 | International Journal of Intelligent Networks | DOI: 10.1016/j.ijin.2021.07.002

Źródło

Treść tworzy Fundacja Dobre Państwo.
Redaguje i publikuje APA ONE, autorski system redakcyjny Fundacji oparty na AI.
APA ONE Publishing System
Fundacja Dobre Państwo © 2026
Article ID: 7ebfc8cc-84e5-46bb-8f9b-c47844109bcb