Blockchain jako infrastruktura odpowiedzialnego zaufania w świetle koncepcji Next Generation Blockchain for Next Amita Kumara Tyagiego

AUTOR

Fundacja Dobre Państwo

STRESZCZENIE / ABSTRACT

Artykuł analizuje przejście technologii blockchain z etapu obietnic i rozczarowań do fazy testu infrastrukturalnego. Autor wskazuje, że przyszłość blockchaina leży w staniu się niewidocznym, ale wydajnym kręgosłupem cyfrowej cywilizacji. Kluczowymi filarami tej transformacji są: rzeczywista skalowalność bez utraty decentralizacji, architektura wielowarstwowa oraz interoperacyjność semantyczna, umożliwiająca swobodny przepływ danych między różnymi sektorami, takimi jak medycyna czy administracja. Celem jest stworzenie systemu odpowiedzialnego zaufania, który zintegruje AI, iot i kryptografię postkwantową, przekształcając niszowe narzędzie w fundament Przemysłu 5.0. Blockchain musi przestać być manifestem, a stać się użytecznym standardem technicznym.

The article analyzes the transition of blockchain technology from a stage of promises and disappointments to an infrastructural testing phase. The author indicates that the future of blockchain lies in becoming an invisible but efficient backbone of digital civilization. Key pillars of this transformation include: real scalability without loss of decentralization, multi-layer architecture, and semantic interoperability, enabling the free flow of data between different sectors such as medicine or administration. The goal is to create a system of responsible trust that integrates AI, IoT, and post-quantum cryptography, transforming a niche tool into the foundation of Industry 5.0. Blockchain must stop being a manifesto and become a useful technical standard.

Artykuł analizuje ewolucję technologii blockchain, która przechodzi z fazy mesjanistycznych obietnic i spekulacyjnego chaosu do krytycznego testu infrastrukturalnego. Autor stawia tezę, że blockchain nowej generacji może stać się trwałym kręgosłupem cyfrowej cywilizacji jedynie pod warunkiem odrzucenia dogmatycznej wizji całkowitej decentralizacji na rzecz pragmatycznego modelu odpowiedzialnej infrastruktury zaufania. Tekst szczegółowo omawia techniczne i społeczne filary tej transformacji – od skalowalności, interoperacyjności i odporności kwantowej, przez synergię z AI i IoT, aż po kontrowersyjną implementację cyfrowych walut banków centralnych (CBDC). Kluczowym przesłaniem jest konieczność stworzenia systemów, w których technologia nie zastępuje ludzkiego sumienia czy prawa, lecz stanowi transparentną warstwę weryfikacji. Blockchain ma przestać być „religią" dla entuzjastów, a stać się niewidocznym, bezpiecznym narzędziem chroniącym jednostkę przed arbitralnością władzy i manipulacją danymi w świecie coraz głębszej automatyzacji.

SŁOWA KLUCZOWE

odpowiedzialne zaufanie | test infrastrukturalny | skalowalność blockchain | interoperacyjność semantyczna | kryptografia postkwantowa | synergia AI i IoT | cyfrowe bliźniaki | tokenizacja aktywów | CBDC | tożsamość cyfrowa | systemy permissioned | architektura wielowarstwowa | audytowalna AI | standardyzacja odpowiedzialności | Przemysł 5.0

Blockchain przechodzi od mesjanistycznych obietnic do testu infrastrukturalnego

Kierunki przyszłego rozwoju: blockchain po epoce obietnicy. Każda przełomowa technologia przechodzi przez trzy fazy. Najpierw jest objawieniem, potem rozczarowaniem, a dopiero później – jeśli przetrwa zderzenie z rzeczywistością – staje się infrastrukturą. Blockchain ma już za sobą etap objawienia. Przedstawiano go jako koniec banków, pośredników i państwowych monopoli; kres papieru i nieufności, a zarazem początek powszechnego bogactwa dla każdego, kto kupi właściwy token przed śniadaniem. Przeszedł również fazę rozczarowania: bańki spekulacyjne, upadki giełd,

oszustwa, koszty energetyczne, powolność sieci, fatalne interfejsy, kradzieże kluczy, błędy w smart kontraktach oraz projekty, które decentralizowały głównie odpowiedzialność za cudze straty. Teraz nadchodzi faza najważniejsza: test infrastrukturalny.

Fundacja Dobre Państwo definiuje przyszłość blockchaina jako przejście od kryptowalut do zrównoważonego, skalowalnego i wydajnego kręgosłupa cyfrowej cywilizacji. Kluczowe kierunki rozwoju obejmują skalowalność, integrację z AI, IoT, 5G i cyfrowymi bliźniakami, kryptografię odporną na komputery kwantowe, energooszczędność oraz zastosowania sektorowe, przy jednoczesnej potrzebie regulacji, standardów i interoperacyjności. To nie jest zwykły katalog technicznych ulepszeń, lecz mapa dojrzałości. Blockchain albo stanie się częścią większej architektury społeczno-technicznej, albo pozostanie niszowym narzędziem dla wspólnot, które bardziej kochają manifest niż użyteczność.

Pierwszym priorytetem pozostaje skalowalność. Bez niej wizja inteligentnych miast, e-administracji, cyfrowego zdrowia, rolnictwa, walut cyfrowych, łańcuchów dostaw i audytowalnej AI będzie jedynie konstrukcją z pięknych pojęć i zbyt małej przepustowości. Notatka wskazuje sharding, protokoły warstwy drugiej oraz sidechains jako techniki zwiększania wydajności, redukcji opóźnień i odciążania głównego łańcucha. Jest to zasadniczy warunek przejścia od eksperymentu do infrastruktury masowej. System miejski, medyczny, logistyczny czy płatniczy nie może działać w rytmie luksusowej ciekawostki; musi być szybki, tani, stabilny i odporny na przeciążenia.

Jednak przyszła skalowalność nie powinna polegać wyłącznie na biciu rekordów liczby transakcji na sekundę – taka rywalizacja bywa intelektualnie płaska. Można bowiem zwiększyć liczbę operacji poprzez centralizację walidacji, ograniczenie liczby uczestników, podniesienie wymagań sprzętowych lub rezygnację z części bezpieczeństwa. Prawdziwym wyzwaniem będzie skalowanie bez utraty istoty blockchaina: odporności na manipulacje, audytowalności, otwartości, rozproszonego zaufania i możliwości niezależnej weryfikacji. W przeciwnym razie otrzymamy system szybki jak platforma płatnicza, ale z blockchainem wyłącznie na plakacie. A plakat nie waliduje transakcji.

Pięć filarów technicznej dojrzałości blockchaina

Drugim kierunkiem będzie architektura wielowarstwowa. Przyszłość blockchaina nie należy do jednego łańcucha, który obsługuje wszystko, lecz do rozbudowanych ekosystemów: warstw bazowych, rozwiązań Layer-2, łańcuchów bocznych, mostów, warstw danych i prywatności, systemów tożsamości, protokołów interoperacyjności oraz aplikacji sektorowych. Przypomina to dojrzewanie internetu – przejście od prostych sieci do wielopoziomowej infrastruktury, w której

użytkownik nie dostrzega protokołów, a jedynie korzysta z ich efektów. Blockchain stanie się naprawdę powszechny dopiero wtedy, gdy większość osób przestanie wiedzieć, że go używa. To nie ironia, lecz dowód dojrzałości technologii; najważniejsza infrastruktura jest zwykle niewidoczna, dopóki nie przestaje działać.

Trzecim kierunkiem jest interoperacyjność. Uniwersalne standardy i protokoły są niezbędne, aby niezależne sieci mogły ze sobą współpracować, choć zagadnienie to może okazać się bardziej polityczne niż techniczne. Każda platforma preferuje własny standard, gdyż tworzy on władzę. Dostawcy wolą własne formaty danych, by zatrzymać klienta, a administracje własne systemy, które dają złudzenie kontroli. Tymczasem społeczeństwo cyfrowe potrzebuje swobodnych przepływów: między szpitalami, miastami, urzędami, bankami, platformami przemysłowymi, systemami identyfikacji, rejestrami własności i łańcuchami dostaw. Bez interoperacyjności decentralizacja zamieni się w federację samotnych twierdz.

Interoperacyjność musi obejmować nie tylko techniczny przesył danych, ale przede wszystkim zgodność znaczeń. Jeśli systemy różnie definiują zdarzenie, jakość, tożsamość, zgodę, certyfikat, prawo dostępu lub finalność transakcji, sama możliwość komunikacji niewiele daje. Cywilizacja cyfrowa potrzebuje semantycznych mostów, nie tylko kabli. Jest to kluczowe w zdrowiu, administracji, rolnictwie i logistyce – dane muszą być nie tylko dostępne, ale porównywalne, wiarygodne i osadzone w kontekście. W przeciwnym razie blockchain będzie jak biblioteka, w której każda książka jest zabezpieczona przed fałszerstwem, lecz napisana własnym alfabetem.

Czwartym kierunkiem jest zrównoważony rozwój. Oznacza to odejście od energochłonnego Proof of Work na rzecz Proof of Stake, modeli hybrydowych i rozwiązań warstwy drugiej, a jednocześnie wykorzystanie blockchaina do monitorowania emisji, śladu węglowego i zrównoważonych łańcuchów dostaw. To przesunięcie jest nieuniknione; technologia aspirująca do roli kręgosłupa przyszłej cywilizacji nie może opierać swojej legitymacji na marnotrawstwie energii, zwłaszcza w obliczu kryzysu klimatycznego i kosztów transformacji przemysłu.

Nie chodzi jednak o prostą opozycję: blockchain zły, bo zużywa energię; blockchain dobry, bo śledzi emisje. Należy oceniać konkretne architektury, zastosowania i bilanse. Energooszczędny system użyty do audytu surowców, rozliczania energii prosumenckiej czy certyfikacji obiegu zamkniętego niesie dodatnią wartość społeczną. Z kolei energochłonny blockchain służący głównie spekulacji i produkcji sztucznego niedoboru może być cywilizacyjnie jałowy. Technologia nie staje się ekologiczna przez deklarację, lecz przez rachunek skutków.

Piątym kierunkiem jest odporność kwantowa. Wraz z rozwojem komputerów kwantowych obecne standardy bezpieczeństwa mogą stać się podatne na ataki, co wymusza wdrażanie nowych

mechanizmów szyfrowania. Dla wielu brzmi to jak odległa fantastyka, tymczasem infrastruktury projektowane dziś będą działać przez dekady, a zapisane teraz dane zachowają znaczenie w przyszłości. Klucze, podpisy, certyfikaty, rejestry własności, dokumentacja zdrowotna czy aktywa tokenizowane muszą być odporne nie tylko na dzisiejsze ataki, lecz także na jutrzejsze możliwości obliczeniowe.

Odporność kwantowa jest więc nie tyle technologiczną ekstrawagancją, ile formą odpowiedzialności międzyczasowej. Budując systemy dla zdrowia, administracji czy dziedzictwa kulturowego, nie możemy zakładać, że horyzont bezpieczeństwa kończy się na najbliższej aktualizacji. Państwo, szpital i archiwum potrzebują myślenia długiego. W świecie cyfrowym często cierpimy na chorobę krótkiego cyklu: wersja, sprint, wdrożenie, patch, migracja. Tymczasem dokument własności, genom czy rejestr publiczny mają czas życia dłuższy niż moda technologiczna. Kryptografia postkwantowa jest jednym z języków tej odpowiedzialności.

Synergia AI i IoT jako fundament inteligentnej infrastruktury

Szóstym kierunkiem jest integracja z AI, rozumiana jako dwukierunkowa synergia: sztuczna inteligencja ma optymalizować procesy, wykrywać zagrożenia, udoskonalać smart kontrakty i analizować dane, podczas gdy blockchain zagwarantuje integralność, autentyczność oraz audytowalność tych danych i decyzji. To kluczowy obszar, gdyż przyszłe systemy nie będą jedynie „blockchainowe” lub „sztuczno-inteligentne”. Staną się złożonymi układami, w których AI podejmuje decyzje lub rekomenduje działania na podstawie danych zabezpieczonych, wersjonowanych i uwierzytelnianych przez blockchain. W idealnym scenariuszu AI wnosi zdolność rozpoznawania wzorców, a blockchain zapewnia pamięć i odpowiedzialność.

Taka integracja może fundamentalnie zmienić smart kontrakty. Dzisiejsze rozwiązanie to zazwyczaj zbiór sztywnych reguł warunkowych: jeśli zdarzy się X, wykonaj Y. Kontrakty przyszłości mogą być wspierane przez AI, która oceni złożone warunki, wykryje anomalie, przewidzi ryzyko lub zasugeruje wykonanie operacji. Zwiększy to elastyczność automatyzacji, ale zrodzi nowe pytania. Jeśli smart kontrakt wykona regułę na podstawie oceny AI, kto odpowie za błąd? Czy model został audytowany? Czy dane wejściowe były wiarygodne i czy człowiek miał możliwość zatrzymania procesu? Czy strona słabsza w ogóle rozumiała ten automatyczny mechanizm? Automatyzacja z AI może być mniej sztywna, lecz bardziej nieprzejrzysta. Nie każde "inteligentniejsze" jest bardziej sprawiedliwe.

Siódmym kierunkiem jest integracja z IoT i 5G. Miliardy czujników będą generować dane, których integralność zapewni blockchain, a sieci 5G umożliwią ich błyskawiczny przesył między urządzeniami. Oznacza to narodziny świata, w którym przedmioty nie tylko są połączone, ale aktywnie uczestniczą w rejestrowanych zdarzeniach. Czujnik temperatury w transporcie leków, licznik energii u prosumenta, sensor wilgotności gleby, urządzenie medyczne czy maszyna w fabryce – wszystkie te obiekty mogą dostarczać dane do systemów decyzyjnych i transakcyjnych.

Problem polega jednak na tym, że IoT drastycznie powiększa powierzchnię ataku. Każdy czujnik może stać się słabym punktem; każde urządzenie może zostać przejęte, źle skalibrowane lub podmienione. Blockchain zabezpiecza zapis, ale nie gwarantuje, że sensor mówi prawdę. Przyszłość tej integracji zależy więc od całego łańcucha zaufania: bezpieczeństwa sprzętu, certyfikacji, podpisów kryptograficznych, odpornych protokołów komunikacji oraz wykrywania anomalii przez AI. Najkrótsza definicja problemu brzmi: blockchain pamięta, ale sensor zeznaje. A świadek musi być wiarygodny.

Ósmym kierunkiem są cyfrowe bliźniaki. Ich rola w łańcuchach dostaw, przemyśle i inteligentnych miastach polega na tworzeniu wirtualnych modeli produktów, procesów logistycznych czy systemów, co umożliwia symulacje, optymalizację i przewidywanie awarii. Blockchain zabezpiecza dane generowane przez te modele, zapewniając ich integralność i bezpieczne współdzielenie. W przyszłości połączenie to może stać się fundamentem zarządzania infrastrukturą krytyczną. Cyfrowy bliźniak bez wiarygodnych danych jest symulacją życzeniową. Blockchain bez modelu świata pozostaje księgą zapisów pozbawioną predykcji. Razem mogą tworzyć system, który nie tylko rejestruje przeszłość, ale modeluje przyszłe zdarzenia – na przykład symulując skutki zmiany organizacji ruchu w mieście.

Konieczność przejścia od kultury eksperymentu do odpowiedzialnej infrastruktury prawnej

W fabryce – awarie maszyn, w rolnictwie – deficyt wody, w energetyce – przeciążenia sieci. W zdrowiu ryzyko pogorszenia stanu pacjenta, a w logistyce opóźnienia dostaw. Jednak im silniejsza staje się zdolność systemu do przewidywania, tym głośniej musimy pytać o odpowiedzialność za predykcję. Prognoza może bowiem stać się samospełniającą się decyzją: jeśli model uzna dany region za ryzykowny, kapitał może z niego odpłynąć, co w efekcie realnie zwiększy to ryzyko.

Cyfrowy bliźniak nie jest niewinnym lusterkiem. Może kształtować rzeczywistość, którą opisuje. Dziewiątym kierunkiem są zatem regulacje i zgodność prawna. Istnieje pilna potrzeba stworzenia

jasnych, globalnych ram regulacyjnych – szczególnie w obszarze kryptowalut i ochrony danych osobowych – oraz pogodzenia przejrzystości blockchaina z wymogami takimi jak RODO/GDPR. Będzie to jeden z najtrudniejszych etapów. Blockchain jest z natury transgraniczny, podczas gdy prawo pozostaje w dużej mierze terytorialne. Dane są rozproszone, walidatorzy działają w różnych jurysdykcjach, użytkownicy są globalni, a skutki lokalne. Kto w takim układzie jest administratorem danych? Gdzie dokładnie dochodzi do ich przetwarzania? Kto odpowiada za błąd smart kontraktu?

Jak zrealizować prawo do usunięcia danych w systemie niezmiennym? Jak uregulować DAO, opodatkować transakcje czy nadzorować mosty między łańcuchami? Dojrzała regulacja nie powinna być ani panicznym zakazem, ani naiwnym zachwytem. Zakaz może wypchnąć innowacje do mniej bezpiecznych jurysdykcji, natomiast zachwyt może oddać obywateli w ręce ryzykownych eksperymentów finansowo-technicznych. Potrzebna jest regulacja funkcjonalna: odrębna dla płatności, zdrowia, rejestrów publicznych, tokenów inwestycyjnych, danych IoT, systemów głosowania czy archiwów kultury. Blockchain nie jest monolitem. Regulowanie go jedną pałką po głowie albo jednym bukietem zachęt byłoby dowodem lenistwa państwa. A państwo leniwe w epoce technologicznej staje się zaproszeniem dla silniejszych aktorów.

Dziesiątym kierunkiem jest standardyzacja odpowiedzialności. Dotąd wiele projektów blockchainowych funkcjonowało w kulturze eksperymentu: użytkownik sam pilnował klucza, kod był publiczny, ryzyko spoczywało na jednostce, a decentralizacja oznaczała brak adresu reklamacyjnego. Taki model może działać w wąskiej wspólnocie entuzjastów, ale nie sprawdzi się w zdrowiu, administracji, energetyce, rolnictwie, finansach masowych czy e-usługach publicznych. Jeśli blockchain ma stać się infrastrukturą społeczną, musi posiadać procedury odpowiedzialności. Kto naprawia błąd? Kto odpowiada za lukę? Kto kompensuje szkodę?

Kto audytuje kod, zatwierdza aktualizację i reprezentuje użytkowników? Kto chroni słabszych uczestników? To jest moment, w którym trzeba odczarować mit "trustless". Systemy społeczne nigdy nie są całkowicie pozbawione zaufania. Zaufanie jedynie przesuwa się z osób na procedury, z instytucji na protokoły, z deklaracji na kryptografię, z biura na kod – ale nie znika. Jeśli użytkownik nie rozumie kodu, ufa audytorowi. Jeśli nie rozumie audytu, ufa instytucji certyfikującej. Jeśli nie rozumie instytucji, ufa prawu. A jeśli nie ufa prawu, wraca do chaosu. Blockchain może zmniejszać potrzebę ślepego zaufania, ale nie tworzy społeczeństwa bez zaufania. Społeczeństwo bez zaufania nie jest zdecentralizowane – jest rozbite.

Jedenastym kierunkiem jest zmiana relacji między blockchainem prywatnym, publicznym i konsorcjalnym. W zastosowaniach sektorowych – w zdrowiu, łańcuchach dostaw, administracji czy

rolnictwie – często bardziej realistyczne będą systemy permissioned, czyli takie, w których uczestnicy są znani i mają określone role.

Hybrydowa infrastruktura i wyzwania tokenizacji oraz CBDC

Przykładem przywoływanym w notatce przy Q-BALAK jest Hyperledger Fabric. To rozwiązania mniej romantyczne niż publiczne blockchainy, ale często bardziej praktyczne. Nie każdy system wymaga anonimowego, globalnego konsensusu; szpital, urząd, spółdzielnia rolnicza, konsorcjum logistyczne czy rejestr publiczny potrzebują raczej kontrolowanego dostępu, zgodności prawnej, wydajności i jasnej odpowiedzialności. Nie należy jednak uznawać prywatnych blockchainów za automatycznie lepsze. Jeśli system permissioned zostanie przejęty przez wąską grupę silnych podmiotów, może stworzyć kartel danych.

Z drugiej strony, publiczny blockchain, gdy staje się skrajnie kosztowny i nieefektywny, okazuje się niepraktyczny. Przyszłość będzie zatem hybrydowa: publiczne warstwy zaufania połączone z prywatnymi i konsorcjalnymi warstwami wykonawczymi, off-chain storage, standardy tożsamości, kryptograficzne dowody i integracje z regulacjami. To podejście mniej czyste ideowo, ale bardziej zgodne z rzeczywistością, która – jak zwykle – nie zapisała się do żadnej sekty technologicznej.

Kolejnym kierunkiem jest tokenizacja aktywów i usług. Blockchain pozwala reprezentować w formie cyfrowych tokenów prawa, certyfikaty, udziały, należności, energię, dane, dokumenty, pochodzenie, głosy, punkty czy roszczenia. Tokenizacja może zwiększać płynność, skracać czas rozliczeń, ułatwiać podział własności, automatyzować zgodność i otwierać nowe modele finansowania. Ma ona jednak ciemną stronę: ryzyko zamiany wszystkiego w obiekt spekulacji. Nie każda wartość społeczna powinna zostać pokrojona na tokeny i wystawiona na rynek. Tokenizując nieruchomości, energię, dane, dzieła sztuki, pracę czy relacje społeczne, musimy pytać, czy faktycznie zwiększamy dostęp, czy jedynie tworzymy nowe instrumenty ekstrakcji.

Istotna będzie również relacja blockchaina z CBDC, która stanie się osobnym polem starcia i współpracy. Cyfrowe waluty banków centralnych mogą przejąć część języka blockchaina: tokenizację, programowalność, natychmiastowe rozliczenia, audytowalność, portfele cyfrowe i infrastrukturę płatności. CBDC nie musi jednak realizować ideału decentralizacji; może być systemem scentralizowanym, hybrydowym albo opartym na kontrolowanej architekturze rozproszonej.

W każdym przypadku wejście CBDC zmieni rynek, pokazując, że państwo nie zamierza biernie patrzeć, jak prywatne stablecoiny, platformy płatnicze i kryptowaluty przejmują wyobraźnię pieniądza cyfrowego. Dla blockchaina oznacza to etap konkurencyjnego dojrzewania. Prywatne i publiczne projekty będą musiały odpowiedzieć na pytanie: jaka jest ich wartość w świecie, w którym pieniądz banku centralnego również może być cyfrowy? DeFi będzie musiało udowodnić, że oferuje coś więcej niż ryzyko opakowane w protokół. Stablecoiny będą konkurować z publiczną wiarygodnością banku centralnego, choć mogą zachować przewagę szybkości, globalności i integracji z rynkami krypto. Banki komercyjne będą bronić swojej roli w kreacji kredytu i relacjach z klientem, państwo zaś szukać równowagi między innowacją, stabilnością a kontrolą. Obywatel powinien w tym wszystkim pytać przede wszystkim o prywatność, dostępność i wolność użycia pieniądza.

CBDC może również przyspieszyć wdrażanie standardów interoperacyjności między finansami a realną gospodarką. Programowalne płatności mogą łączyć się ze smart kontraktami w łańcuchach dostaw, rolnictwie, administracji, ubezpieczeniach, zamówieniach publicznych czy energetyce. Można sobie wyobrazić płatność publiczną uruchamianą po potwierdzeniu wykonania usługi, rekompensatę rolniczą uzależnioną od parametrów pogodowych, rozliczenie energii prosumenckiej w czasie zbliżonym do rzeczywistego, fakturę regulowaną automatycznie po dostawie towaru lub wypłatę świadczenia powiązaną z cyfrową tożsamością.

Tożsamość cyfrowa i zaufanie społeczne jako warunki inkluzywności

Rozwiązania te mogą ograniczyć opóźnienia i nadużycia, ale jednocześnie zwiększyć kontrolę. Programowalność jest nożem: można nim kroić chleb, można też przeciąć wolność. Czternastym kierunkiem będzie rozwój tożsamości cyfrowej i portfeli użytkownika. Bez tożsamości masowe wdrożenie wielu zastosowań — od zdrowia i administracji, przez głosowania i licencje, aż po edukację, płatności czy uprawnienia zawodowe — pozostanie niemożliwe. Przyszłość prawdopodobnie przyniesie portfele cyfrowe, w których użytkownik będzie przechowywał potwierdzone atrybuty i przedstawiał je selektywnie. Blockchain może tu wspierać weryfikowalne poświadczenia oraz historię wydania certyfikatów. Kluczowa okaże się jednak minimalizacja danych. Dobry system tożsamości nie pyta: „jak zebrać wszystko?”, lecz: „jak potwierdzić dokładnie tyle, ile trzeba, i ani grama więcej?”.

Jest to szczególnie istotne w obliczu ryzyka połączenia tożsamości, CBDC, usług publicznych, danych zdrowotnych i systemów miejskich. Jeśli te warstwy zostaną zintegrowane bez gwarancji

prywatności, powstanie infrastruktura nadzoru o skali trudnej do porównania z czymkolwiek z epoki papierowej. Jeśli jednak połączenie to nastąpi mądrze, może ono ograniczyć biurokrację, oszustwa i wykluczenie, eliminując konieczność powtarzalnego udowadniania tych samych faktów. Różnica między emancypacją a kontrolą tkwi w architekturze prawnej i technicznej. Cyfrowa tożsamość może być kluczem do wolności usług albo kajdankami z wygodnym panelem użytkownika.

Piętnastym kierunkiem będzie społeczna legitymizacja. Blockchain może być technicznie genialny, ale jeśli użytkownicy nie będą mu ufać, nigdy nie stanie się prawdziwą infrastrukturą. Zaufanie społeczne nie buduje się za pomocą białej księgi, brandingu czy wykresów z rosnącymi strzałkami. Powstaje ono poprzez niezawodność, prostotę obsługi, ochronę przed błędami, jasne procedury reklamacyjne, edukację i niezależny audyt oraz doświadczenie, że system działa nawet wtedy, gdy coś pójdzie źle. Prawdziwa infrastruktura nie jest testowana w dniu prezentacji. Jest testowana w dniu awarii. Wtedy widać, czy projektanci przewidzieli człowieka, czy jedynie idealnego użytkownika z instrukcji.

Szesnastym kierunkiem będzie walka z wykluczeniem cyfrowym. Im głębiej blockchain wejdzie w usługi publiczne, zdrowie, rolnictwo, energetykę i administrację, tym głośniej wybrzmi pytanie o osoby bez kompetencji cyfrowych, stabilnego łącza czy nowoczesnych urządzeń — o seniorów, osoby ubogie, niepełnosprawne, mieszkańców małych ośrodków lub tych, którzy po prostu nie chcą żyć w aplikacji. Cyfrowa cywilizacja nie może twierdzić, że kto nie nadąża, ten sam sobie winien. To nie jest innowacja.

Pragmatyzm i odpowiedzialność zamiast mesjanizmu technologicznego

To społeczny darwinizm w wersji UX. Każda infrastruktura blockchainowa o znaczeniu publicznym musi zapewniać ścieżki wsparcia, zastępstwa, edukacji i dostępności. Kluczowym kierunkiem staje się zatem edukacja instytucjonalna. Państwo, samorządy, szpitale, sądy czy organizacje obywatelskie muszą rozumieć, co właściwie wdrażają. Nie każdy musi pisać smart kontrakty, tak jak nie każdy pasażer kolei musi projektować lokomotywę. Decydenci powinni jednak znać podstawowe ryzyka: niezmienność błędów, problem wyroczni (oracles), zarządzanie kluczami, prywatność, odpowiedzialność, interoperacyjność, koszty energetyczne, vendor lock-in, cyberbezpieczeństwo oraz realny model władzy w sieci.

Bez tej wiedzy będą kupować jedynie obietnice. A rynek technologiczny bardzo chętnie sprzedaje słowa z abonamentem. Ostatecznie przyszłość blockchaina nie rozstrzygnie się w haśle „wszystko zdecentralizowane", choć notatka przywołuje je jako wyraz ambicji. Nie wszystko powinno być zdecentralizowane. Niektóre procesy wymagają centralnej odpowiedzialności, szybkiej decyzji, ochrony tajemnicy, jasnej jurysdykcji lub po prostu prostoty. Prawdziwe pytanie brzmi: które elementy systemu powinny być zdecentralizowane, a które federacyjne, publiczne, prywatne, audytowalne, niezmienne lub możliwe do skorygowania? Dojrzałość polega na rozróżnianiu; fanatyzm technologiczny rozpoznaje się po tym, że ma jedną odpowiedź na wszystkie pytania. Najlepsza przyszłość blockchaina to przyszłość pragmatyczna, nie mesjanistyczna.

Blockchain może stać się warstwą integralności danych, ścieżką audytu AI, paszportem produktu czy rejestrem zgód pacjenta. Może wspierać cyfrową tożsamość, mechanizmy rozliczeń w energetyce prosumenckiej, ochronę metadanych dziedzictwa kulturowego, rolnictwo precyzyjne lub stanowić element CBDC i infrastruktury tokenizacji.

Nie wszędzie. Nie zawsze. Nie sam. Ale tam, gdzie brak zaufania, ryzyko manipulacji, wielopodmiotowość i potrzeba audytu są realne – tam może stać się technologią bardzo poważną. Najgorsza przyszłość blockchaina to przyszłość dekoracyjna: kilka tokenów, modne hasła o „web3", zielone ikony, konferencje, nieczytelne whitepapery, granty, dużo obietnic i mało odpowiedzialności. To już widzieliśmy. Cywilizacja nie potrzebuje kolejnej technologii, która obiecuje zmianę świata, zanim nauczy się obsługiwać reklamację. Jeśli blockchain ma przejść do fazy infrastruktury, musi zejść z mównicy i wejść do warsztatu: prawa, standardów, audytu, ergonomii, cyberbezpieczeństwa, interoperacyjności i kosztów utrzymania. Blockchain przyszłości nie wygra dlatego, że będzie bardziej rewolucyjny, lecz dlatego, że będzie bardziej odpowiedzialny.

CBDC jako narzędzie suwerenności w cyfrowym pieniądzu

Rewolucja jest łatwa w manifeście. Odpowiedzialność jest trudna w systemie. Jeśli technologia ta ma rzeczywiście stać się kręgosłupem cyfrowej cywilizacji, musi udowodnić, że potrafi nie tylko zapisywać transakcje, ale także chronić człowieka, dane, pamięć, środowisko, pracę, własność i wolność przed arbitralnością silniejszych. Dopiero wtedy „ekosystem zaufania" przestanie być sloganem, a stanie się instytucją.

CBDC: gdy państwo wchodzi do gry o cyfrowy pieniądz. Cyfrowa waluta banku centralnego to moment, w którym spór o blockchain, tokenizację i programowalność finansów przestaje być

domeną wyłącznie kryptografów, fintechów, inwestorów, libertarian czy spekulantów. Do gry wchodzi państwo – nie jako zewnętrzny regulator, który z opóźnieniem próbuje pojąć wizje technologów, lecz jako emitent pieniądza, strażnik stabilności systemu finansowego i projektant nowej infrastruktury płatniczej. To zmienia wszystko. Gdy bank centralny zaczyna myśleć o pieniądzu cyfrowym, blockchainowa wyobraźnia spotyka się z instytucją, która od stuleci posiada najważniejszy przywilej monetarny: zdolność definiowania publicznego pieniądza.

CBDC nie jest po prostu „kryptowalutą państwową". To określenie chwytliwe, lecz mylące. Kryptowaluty w klasycznym sensie powstawały jako odpowiedź na brak zaufania do banków, państw i scentralizowanej emisji pieniądza. CBDC wyrasta z przeciwnej logiki: ma być cyfrową formą pieniądza publicznego, dostępną w środowisku elektronicznym. Europejski Bank Centralny opisuje cyfrowe euro jako central bank money in digital form, przeznaczone do płatności w sklepach, online oraz między osobami; sam projekt po zakończeniu fazy przygotowawczej w październiku 2025 roku przeszedł do kolejnego etapu prac.

Bitcoin pytał: czy można stworzyć pieniądz bez banku centralnego? CBDC pyta: jak bank centralny ma przetrwać w świecie, w którym pieniądz staje się cyfrowy, tokenizowany, platformowy, natychmiastowy i globalnie konkurencyjny? Stablecoiny, prywatne portfele, systemy płatnicze wielkich platform oraz kryptorynki pokazały państwom, że infrastruktura pieniądza może wymknąć się z tradycyjnej mapy instytucji. CBDC jest odpowiedzią centrum na bunt peryferii: „skoro pieniądz przyszłości ma być cyfrowy, to publiczny pieniądz również musi mieć cyfrowe ciało".

Nie oznacza to jednak, że CBDC musi opierać się na publicznym blockchainie. Wiele projektów może wykorzystywać architektury scentralizowane, hybrydowe, permissioned ledger czy tokenizację bez pełnej decentralizacji. Tu kończy się prosta legenda blockchaina. Państwo nie musi przyjąć całej ideologii decentralizacji, aby przejąć wybrane narzędzia: cyfrowy token, natychmiastowe rozliczenie, programowalność, audytowalność, portfel cyfrowy czy integrację z tożsamością cyfrową. Innymi słowy: CBDC może użyć języka technologii, ale zachować gramatykę suwerenności.

Bank Rozrachunków Międzynarodowych w raporcie z 2023 roku zaproponował wizję tzw. unified ledger – wspólnej infrastruktury łączącej pieniądz banku centralnego, tokenizowane depozyty i aktywa na programowalnej platformie. Koncepcja ta jest kluczowa, gdyż pokazuje, że przyszłość CBDC nie ogranicza się do pytania o sposób płatności obywatela. Chodzi o głębszą przebudowę rynku finansowego: rozliczeń, papierów wartościowych, depozytów i transakcji transgranicznych. Pieniądz cyfrowy banku centralnego może stać się warstwą bazową nowego systemu, w którym własność i płatność zostaną połączone w jednej logice wykonawczej.

CBDC jako narzędzie efektywności i ryzyko kontroli

Wprowadzenie tych rozwiązań może przynieść realne korzyści. Rozliczenia staną się szybsze, tańsze i mniej zależne od pośredników. Spadną koszty płatności transgranicznych, a rozrachunki papierów wartościowych zyskają na natychmiastowości. Administracja będzie mogła sprawniej wypłacać świadczenia, łańcuchy dostaw automatycznie uruchamiać płatności po potwierdzeniu odbioru, a rolnicy otrzymywać środki zaraz po spełnieniu parametrów programów wsparcia.

Energetyka prosumencka zyska możliwość rozliczania mikrotransakcji niemal w czasie rzeczywistym. W takim świecie pieniądz przestaje być jedynie środkiem płatniczym – staje się elementem infrastruktury wykonawczej, która płaci, potwierdza, rozlicza, warunkuje i śledzi zgodność. To właśnie sprawia, że CBDC jest kwestią tak politycznie wrażliwą. Im bardziej pieniądz staje się programowalny, tym głośniej musimy pytać: kto pisze ten program? Jeśli programowalność oznacza jedynie automatyzację dobrowolnych kontraktów i większą efektywność, będzie ogromnym atutem. Jeśli jednak umożliwi ograniczanie tego, gdzie, kiedy, przez kogo i na co można wydać środki, pojawi się ryzyko nowej formy kontroli.

Pieniądz gotówkowy jest anonimowy, przenośny, działa offline, nie wymaga zgody aplikacji ani zapytania do serwera i nie pozostawia pełnej ścieżki transakcyjnej. CBDC może te cechy częściowo odtworzyć, a może je zniszczyć. W tym „częściowo" kryje się fundamentalny spór o wolność. Europejska debata o cyfrowym euro dobrze obrazuje tę ambiwalencję. EBC deklaruje, że projekt ma chronić wolność płacenia w coraz bardziej cyfrowym świecie; prace po październiku 2025 roku mają budować gotowość techniczną przed ewentualną decyzją o emisji, w pełnej zgodzie z procesem legislacyjnym. Jednocześnie w Europie szczególnie mocno akcentuje się prywatność, funkcję offline oraz relację cyfrowego euro do gotówki. To nie przypadek. Pamięć historyczna uczy nas, że państwo dysponujące doskonałym rejestrem zachowań obywateli nie zawsze jest przyjacielem wolności. Technologia płatności musi więc być oceniana nie tylko przez pryzmat wygody, lecz odporności na nadużycia.

Funkcja offline jest tu kluczowa. Francuski organ ochrony danych CNIL wskazywał w 2026 roku, że tryb offline cyfrowego euro jest silnie wspierany, gdyż może zapewniać wysoki poziom poufności transakcji i zbliżać się do ochrony prywatności właściwej gotówce; podkreślano przy tym znaczenie rozwiązań tokenowych oraz privacy by design. To nie jest techniczny drobiazg. Płatność offline oznacza odporność na awarie sieci, katastrofy, cyberataki czy wykluczenie infrastrukturalne. Oznacza też zachowanie przestrzeni prywatności. Cyfrowy pieniądz bez tej funkcji byłby wygodny w czasie normalności, lecz kruchy w kryzysie. Infrastruktura publiczna musi być projektowana nie na dzień pokazowy, ale na dzień awarii.

Badania nad offline CBDC pokazują jednak, że jednoczesne osiągnięcie prywatności, odporności na podwójne wydanie, limitów posiadania i zgodności regulacyjnej jest niezwykle trudne. Prace nad projektami digital euro i PayOff wskazują zarówno potencjał dowodów kryptograficznych, jak i poważne ograniczenia w zakresie bezpieczeństwa, przechowywania danych czy realnych wycieków prywatności. To ważna lekcja: hasło „gotówka cyfrowa" brzmi prosto, ale technicznie jest polem minowym. Gotówka papierowa jest genialna w swojej prostocie; jej cyfrowe odtworzenie wymaga złożonej kryptografii i pełnego zaufania do implementacji.

Warto zauważyć, że CBDC nie jest projektem jednolitym globalnie. Atlantic Council CBDC Tracker wskazuje na dziesiątki pilotaży, podczas gdy pełne uruchomienia przeprowadziły m.in. Bahamy, Jamajka i Nigeria; wiele innych państw testuje lub zawiesza prace zależnie od lokalnych priorytetów. To pokazuje, że nie ma jednej ścieżki. W małym państwie wyspiarskim CBDC może służyć inkluzji finansowej i odporności po huraganach. W Indiach może być narzędziem transferów socjalnych. W strefie euro dotyczy suwerenności monetarnej, konkurencji z prywatnymi systemami i relacji z bankami komercyjnymi. Ta sama nazwa, różne polityki.

Przykład Indii pokazuje najbardziej praktyczny wymiar programowalności. Reuters opisywał w kwietniu 2026 roku pilotaż e-rupii w systemie świadczeń, gdzie waluta miała ograniczać korupcję poprzez kierowanie środków na konkretne cele i zatwierdzonych dostawców. Z jednej strony to obietnica skuteczniejszego państwa: mniej nadużyć, szybsza pomoc i większa transparentność. Z drugiej – to dokładnie ten punkt, w którym pieniądz zaczyna tracić neutralność. Jeśli świadczenie można wydać tylko w określonym miejscu i celu, państwo zwiększa kontrolę nad beneficjentem. Czasem jest to uzasadnione, czasem paternalistyczne, a czasem niebezpieczne.

Nie należy więc mówić o programowalności wyłącznie z zachwytem – jest ona mieczem obosiecznym. Może ograniczać korupcję i poprawiać efektywność pomocy publicznej, ale może też tworzyć społeczeństwo warunkowego pieniądza, w którym obywatel nie otrzymuje wartości, lecz pozwolenie na jej użycie zgodnie z parametrem. Pieniądz tradycyjny był abstrakcyjną siłą nabywczą. Pieniądz programowalny może stać się instrukcją zachowania. A instrukcja zachowania wydana przez państwo to już nie tylko finanse. To polityka społeczna w trybie wykonawczym.

CBDC jako konflikt interesów między efektywnością a inwigilacją

Relacja CBDC z blockchainem nabierze szczególnego znaczenia w obszarze DeFi i stablecoinów. Jeśli bank centralny wprowadzi cyfrowy pieniądz publiczny, emitenci stablecoinów będą musieli

jasno uzasadnić swoją przewagę – czy będzie nią globalna dostępność, głęboka integracja z ekosystemami blockchain, szybkość, programowalność, czy może użyteczność w niszach, do których CBDC nie dotrze. Stablecoiny niosą jednak ze sobą ryzyka związane z rezerwami, płynnością, możliwością runów oraz wpływem na politykę monetarną. Z perspektywy państwa prywatny stablecoin o dużej skali może zacząć pełnić funkcję quasi-monetarną, nie ponosząc przy tym demokratycznej ani bankowo-centralnej odpowiedzialności. W tym sensie CBDC jest odpowiedzią na fundamentalne pytanie: czy pieniądz cyfrowy ma być publiczną infrastrukturą, czy prywatnym standardem platform? Jednocześnie CBDC może uderzyć w banki komercyjne. Możliwość trzymania środków bezpośrednio w banku centralnym rodzi ryzyko odpływu depozytów z sektora prywatnego, szczególnie w okresach kryzysowych. Dlatego wiele projektów zakłada wprowadzenie limitów posiadania CBDC, brak oprocentowania lub inne mechanizmy ograniczające konkurencję wobec tradycyjnych depozytów.

Reuters informował w lutym 2026 roku, że według szacunków EBC koszty wdrożenia cyfrowego euro dla banków UE mogłyby wynieść od 4 do 6 mld euro w ciągu czterech lat. Sam EBC oszacował własne wydatki na uruchomienie systemu na około 1,3 mld euro, przy rocznych kosztach operacyjnych rzędu 300 mln euro. To przypomina, że CBDC nie jest darmową modernizacją. Ktoś zapłaci za infrastrukturę, integracje, bezpieczeństwo, zgodność z przepisami i przebudowę systemów bankowych. Pojawia się zatem pytanie: komu CBDC ma realnie służyć? Konsumentom, którzy dysponują już szybkimi płatnościami? Kupcom dążącym do niższych opłat? Państwu pragnącemu suwerenności płatniczej? Bankom centralnym chcącym utrzymać rolę pieniądza publicznego? Fintechom budującym nowe usługi, czy może osobom wykluczonym finansowo i administracji dążącej do efektywniejszego wypłacania świadczeń?

Odpowiedź brzmi pewnie: wszystkim po trochu. Jednak każda z tych grup ma odmienne interesy. Konsument ceni prywatność i wygodę, kupiec niskie koszty, państwo kontrolę i odporność, bank stabilność depozytów, fintech dostęp do API i rynku, a obywatel – wolność. Projekt CBDC będzie zatem kompromisem między tymi sprzecznościami, dlatego nie wolno udawać, że mamy do czynienia z neutralną technologią. CBDC może radykalnie zmienić e-administrację: świadczenia wypłacane natychmiast po spełnieniu warunku, automatyczne rozliczanie podatków, zamówienia publiczne opłacone po kryptograficznym potwierdzeniu dostawy, dotacje środowiskowe powiązane z audytowanym systemem czy mandaty i zwroty działające w czasie rzeczywistym.

Taka sprawność może zmniejszyć biurokrację, ale jednocześnie zwiększa pokusę automatyzacji sankcji. Jeśli państwo potrafi wypłacać natychmiast, może też natychmiast potrącać, blokować, limitować i profilować. Cyfrowa efektywność administracji jest wartością wtedy, gdy służy obywatelowi. Gdy służy wyłącznie władzy, staje się perfekcyjnym fiskalnym automatem.

Najważniejszym zabezpieczeniem musi być zatem zasada proporcjonalności i minimalizacji danych. CBDC nie powinno tworzyć pełnej historii życia płatniczego obywatela, dostępnej w jednym centrum. Płatności niskokwotowe powinny zachować wysoki poziom prywatności, zwłaszcza w trybie offline. Transakcje wysokiego ryzyka mogą podlegać rygorom przeciwdziałania praniu pieniędzy i finansowaniu terroryzmu, lecz nie wolno używać tych wymogów jako pretekstu do całkowitego zniesienia prywatności finansowej. Społeczeństwo, w którym każda kawa, książka, darowizna czy lekarstwo tworzą centralny profil obywatela, nie jest nowoczesne.

Jest nagie. CBDC w połączeniu z cyfrową tożsamością tworzy dodatkową warstwę ryzyka. Europejskie prace nad portfelami tożsamości cyfrowej pokazują, że nawet systemy projektowane z myślą o prywatności mogą prowadzić do nadmiernego ujawniania atrybutów przez użytkowników. Badania nad EUDI Wallet wskazują, że skłonność ta istnieje, a narzędzia wspierające decyzje jedynie zmniejszają to ryzyko, nie eliminując go całkowicie. Jeśli połączymy portfel tożsamości z płatniczym, stawką przestaje być tylko wygoda logowania. Stawką jest ryzyko sklejenia tożsamości, zachowań finansowych i uprawnień w jeden profil. Tu naprawdę nie ma miejsca na projektowanie metodą "jakoś to będzie". "Jakoś to będzie" w systemach tożsamości i pieniądza jest krótką drogą do sytuacji, w której wszyscy będą widzieć za dużo. Z punktu widzenia blockchaina wejście CBDC może mieć skutek dyscyplinujący.

CBDC jako infrastruktura cywilna obok gotówki

Prywatne projekty będą musiały dojrzeć. Nie wystarczy mówić o wolności, gdy użytkownik traci środki przez błąd smart kontraktu i nie ma żadnej drogi odwoławczej. Nie wystarczy deklarować decentralizacji, jeśli walidację kontroluje zaledwie kilka podmiotów. Nie wystarczy głosić przejrzystości, skoro ryzyka rozumieją jedynie nieliczni eksperci. CBDC, nawet niedoskonałe, podniesie poprzeczkę w kwestiach bezpieczeństwa, zgodności prawnej, dostępności, odporności i kosztów, a także ochrony konsumenta, prywatności i integracji z obecnym systemem. Rynek krypto będzie musiał odpowiedzieć nie memem, lecz instytucją.

Możliwy jest podział funkcji w nowym ładzie finansowym. CBDC mogłoby pełnić rolę publicznej, bezpiecznej warstwy płatniczej, podczas gdy stablecoiny dominowałyby w obszarach globalnych, transgranicznych i DeFi. Tokenizowane depozyty bankowe obsługiwałyby relacje komercyjne, publiczne blockchainy zapewniały otwarte środowiska innowacji, a systemy ledgerowe (prywatne i konsorcjalne) obsługiwałyby branże regulowane. Mosty, standardy i portfele będą łączyć te światy. Nie będzie jednego zwycięzcy i jednego przegranego; bardziej prawdopodobny jest złożony

ekosystem pieniądza cyfrowego, w którym spór nie dotyczyć będzie samego istnienia tokenów, lecz kontroli nad warstwą bazową, danymi i regułami dostępu.

Kluczowe pytanie dotyczy jednak gotówki. Cyfrowe euro i inne CBDC często przedstawia się jako uzupełnienie, a nie zastępstwo pieniądza fizycznego. Komisja Europejska już w 2023 roku przedstawiła pakiet obejmujący zarówno ramy dla cyfrowego euro, jak i propozycję ochrony statusu gotówki jako prawnego środka płatniczego oraz gwarancję jej dostępności. Jest to kwestia fundamentalna. Gotówka pełni funkcję wolnościową, awaryjną, inkluzywną i kulturową. Nie każdy obywatel chce lub może płacić cyfrowo. Nie każda sytuacja powinna być rejestrowana, a nie każda awaria może czekać na przywrócenie systemu. Gotówka jest analogowym bezpiecznikiem społeczeństwa cyfrowego. Usunięcie go w imię wygody byłoby jak wymontowanie hamulca ręcznego tylko dlatego, że samochód posiada komputer. CBDC powinno więc być projektowane jako rozszerzenie publicznego pieniądza, a nie cichy pogrzeb gotówki.

Jeśli cyfrowa waluta banku centralnego stanie się pretekstem do ograniczania gotówki, zaufanie społeczne osłabnie. Jeśli natomiast CBDC będzie funkcjonować obok niej, oferując cyfrową wygodę, płatności offline, prywatność przy niskich kwotach i powszechną dostępność, może wzmocnić odporność całego systemu. Dobry projekt CBDC powinien być zatem mniej aplikacją bankową, a bardziej publiczną infrastrukturą cywilną. Ma działać w sklepie i w czasie kryzysu; służyć osobie starszej, wykluczonej z bankowości komercyjnej, małemu przedsiębiorcy, obywatelowi sceptycznemu oraz państwu, które nie chce oddać sfery płatności wyłącznie prywatnym platformom.

CBDC jako narzędzie efektywności i ryzyko algorytmicznej kontroli

CBDC wpłynie również na łańcuchy dostaw i Przemysł 5.0. Gdy pieniądz publiczny stanie się cyfrowy i programowalny, smart kontrakty w logistyce zyskają nową warstwę rozliczeń: dostawa potwierdzona przez IoT i blockchain może automatycznie uruchamiać płatność, certyfikat środowiskowy – otwierać drogę do preferencyjnego finansowania, a ubezpieczenie parametryczne – wypłacać środki natychmiast po wystąpieniu zdarzenia pogodowego. Podobnie zamówienia publiczne mogłyby być rozliczane w oparciu o mierzalne etapy realizacji, co obniżyłoby koszty transakcyjne i ograniczyło spory.

Wymaga to jednak precyzyjnego oddzielenia automatyzacji od decyzji wymagających ludzkiej oceny. Nie wszystko, co mierzalne, powinno przesądzać o płatności; gospodarka zna przecież

wyjątki, siłę wyższą i nadużycia w danych wejściowych. Smart kontrakt z CBDC nie może być sądem kapturowym w eleganckim kodzie.

W rolnictwie CBDC mogłoby usprawnić dopłaty, subsydia czy płatności za praktyki środowiskowe. Pojawia się jednak pytanie: czy rolnik zyska sprawniejszy dostęp do środków, czy zostanie poddany mikrokontroli? Jeśli płatność za retencję wody czy praktyki regeneratywne będzie powiązana z audytowanymi danymi z pola, system może stać się sprawiedliwszy i mniej podatny na fikcyjne deklaracje. Jeżeli jednak każdy aspekt gospodarstwa zostanie przekształcony w warunek cyfrowej wypłaty, rolnik stanie się wykonawcą algorytmicznej polityki rolnej. Państwo nie powinno mylić dowodu z podejrzliwością. Kontrola jest niezbędna, ale permanentna podejrzliwość to choroba administracji.

CBDC w sektorze zdrowia może usprawnić rozliczenia świadczeń, refundacje i automatyczne płatności za procedury. W tej sferze programowalny pieniądz wymaga jednak szczególnej ostrożności. Jeśli płatność zostanie zbyt mocno powiązana z algorytmiczną oceną kwalifikowalności, pacjent może utknąć w martwym punkcie między systemem medycznym, ubezpieczeniowym a płatniczym. Odmowa finansowania stałaby się natychmiastowa, podczas gdy procedura odwoławcza pozostałaby powolna. Taki układ byłby cywilizacyjnie niedopuszczalny. Automatyzacja w zdrowiu powinna przyspieszać świadczenie usługi, a nie odmowę jej udzielenia. Jeśli technologia ma mieć sumienie, tutaj musi je wykazać w pierwszej kolejności.

W administracji lokalnej CBDC może wspierać budżety partycypacyjne, granty czy mikropłatności miejskie. Wyobraźmy sobie miasto, w którym obywatel przez jeden publiczny portfel otrzymuje zwrot za recykling, opłaca transport i rozlicza energię prosumencką. To rozwiązanie wygodne, lecz gdy ten sam portfel łączy transport, energię, świadczenia, tożsamość i zachowania obywatelskie, pojawia się ryzyko nadmiernej integracji. W cyfryzacji integracja jest jak sól: bez niej mdło, z nadmiarem niejadalna.

Dlatego kluczowym kryterium CBDC powinna być odwracalność władzy technologicznej. Obywatel musi zachować możliwość wyboru metody płatności, prywatność w drobnych transakcjach, dostęp do funkcji offline oraz prawo do reklamacji i ochrony przed profilowaniem. Przedsiębiorca potrzebuje jasnych kosztów i gwarancji braku arbitralnego blokowania środków, a banki – stabilnych warunków działania. Państwo musi dysponować narzędziami walki z przestępczością, ale nie może mieć nieograniczonego wglądu w codzienność obywateli. Ten kompromis będzie trudny, lecz jeśli nie zostanie wynegocjowany jawnie, zostanie wpisany po cichu w architekturę systemu. A reguła wpisana w kod bez debaty jest polityką udającą technikę.

CBDC jako narzędzie suwerenności lub nadzoru

Cyfrowe waluty banków centralnych są elementem rywalizacji o suwerenność monetarną, niezależność płatniczą i standardy technologiczne. Europa dąży do zmniejszenia zależności od pozaeuropejskich operatorów płatności, Chiny od lat eksperymentują z cyfrowym juanem, a Indie rozwijają e-rupię. Małe państwa testują CBDC z powodów inkluzywnych i infrastrukturalnych, natomiast w Stanach Zjednoczonych trwa debata często silnie naładowana politycznie.

Kto ustanowi standard cyfrowego pieniądza, ten narzuci standardy danych, zgodności, interoperacyjności i rozliczeń. W świecie, w którym płatność jest informacją, infrastruktura płatnicza staje się infrastrukturą wpływu. CBDC może zatem stać się narzędziem suwerenności lub nową formą zależności. Jeśli państwo projektuje system samodzielnie, opierając się na otwartych standardach, silnej ochronie prywatności i interoperacyjności, wzmacnia własną odporność. Jeśli natomiast kupuje zamkniętą technologię od zewnętrznych dostawców, jedynie zmienia rodzaj podległości. Suwerenność cyfrowa nie polega na tym, że flaga państwowa pojawia się na ekranie aplikacji; polega ona na realnej kontroli nad kodem, danymi, standardami, bezpieczeństwem i audytem oraz na możliwości zmiany dostawcy. Państwo, które nie rozumie własnej infrastruktury pieniądza cyfrowego, nie jest suwerenne. Jest klientem z hymnem.

Najsilniejszy argument za CBDC głosi: publiczny pieniądz musi pozostać dostępny w epoce cyfrowej. Jeżeli codzienne płatności przejdą całkowicie do prywatnych platform, państwo utraci bezpośrednią relację obywatela z pieniądzem banku centralnego. Gotówka będzie tracić na znaczeniu, a pieniądz publiczny stanie się czymś odświętnym, niemal muzealnym. CBDC może temu zapobiec. Z drugiej strony, najsilniejszy argument przeciw brzmi: cyfrowy pieniądz publiczny może stworzyć infrastrukturę nadzoru i kontroli, której gotówka nigdy nie umożliwiała. Oba te stanowiska są poważne. Kto widzi tylko pierwsze, jest technokratą; kto dostrzega jedynie drugie, jest lękowym katastrofistą. Rozum zaczyna się tam, gdzie umiemy utrzymać oba naraz. Najuczciwsza odpowiedź brzmi więc: CBDC może być dobre albo złe w zależności od projektu. Nie ma zbawienia w samym skrócie.

Dobre CBDC powinno być dostępne, odporne, prywatne w małych transakcjach, zgodne z naturą gotówki, interoperacyjne, ograniczone prawnie, audytowalne, niedyskryminacyjne i społecznie zrozumiałe. Złe CBDC będzie centralnym rejestrem płatności, narzędziem nadmiernej kontroli, pretekstem do eliminacji gotówki, koszmarem dla prywatności, obciążeniem dla banków i kolejną aplikacją, której nikt nie potrzebuje poza jej autorami.

Blockchain jako architektura zaufania zamiast mesjanistycznej iluzji

Różnica między nimi nie jest techniczna, lecz konstytucyjna. W kontekście niniejszego artykułu CBDC stanowi moment syntezy. Łączy w sobie blockchain, regulacje, pieniądz i tożsamość, a także smart kontrakty, interoperacyjność, prywatność, administrację, łańcuchy dostaw, rolnictwo, zdrowie oraz geopolitykę. Pokazuje to, że przyszłość blockchaina nie będzie już romantycznym snem o ucieczce od instytucji, lecz negocjacją z nimi. Państwo, bank centralny i prawo nie znikną. Pytanie brzmi jedynie, czy technologia uczyni je bardziej rozliczalnymi, czy bardziej wszechobecnymi. Blockchain obiecywał zaufanie bez pośrednika; CBDC odpowiada: zaufanie do publicznego pośrednika w formie cyfrowej. Społeczeństwo musi zdecydować, w jakim stopniu chce zaufać tej odpowiedzi. Można to ująć w maksymie: pieniądz cyfrowy nie jest tylko pieniądzem; jest konstytucją codziennych transakcji. Jeśli zostanie zaprojektowany z poszanowaniem wolności, prywatności i dostępności, może stać się jednym z filarów nowoczesnego państwa usługowego. Jeśli jednak powstanie jako infrastruktura całkowitego nadzoru centrum, będzie jedynie eleganckim narzędziem kontroli.

Gotówka była anonimowym szeptem gospodarki. CBDC może być publicznym językiem cyfrowej wymiany. Nie pozwólmy tylko, aby każdy szept obywatela automatycznie trafiał do archiwum władzy.

Blockchain jako infrastruktura zaufania albo kolejna maszyna iluzji. Blockchain nowej generacji nie jest już pytaniem o kryptowaluty. Jest pytaniem o to, jak społeczeństwo cyfrowe będzie pamiętać, potwierdzać, rozliczać, automatyzować, chronić i kwestionować własne działania. Jego znaczenie wykracza zatem daleko poza rynek finansowy.

Analiza prowadzi nas przez skalowalność, Smart Cities, e-administrację, zdrowie, Przemysł 5.0, łańcuchy dostaw, bezpieczeństwo danych AI, ochronę dziedzictwa kulturowego, rolnictwo Q-BALAK, kryptografię postkwantową i przyszłość CBDC. Wszystkie te obszary łączy jedna intuicja: w epoce cyfrowej zaufanie nie może opierać się wyłącznie na deklaracjach instytucji, marketingu platformy czy dobrej woli operatora systemu. Musi posiadać architekturę. Największą siłą blockchaina jest właśnie to, że proponuje nową architekturę zaufania. Nie znosi on zaufania, jak naiwnie powtarzają entuzjaści – on je przemieszcza. Zaufanie przechodzi z pojedynczego centrum na protokół, kryptografię, mechanizm konsensusu, audytowalność, historię zmian, reguły dostępu i rozproszoną walidację. To przesunięcie może mieć znaczenie cywilizacyjne, ponieważ nasze systemy społeczne stają się zbyt złożone, szybkie i wielopodmiotowe, by opierać się wyłącznie na papierowej procedurze i hierarchicznym nadzorze. Administracja, zdrowie, łańcuchy dostaw,

rolnictwo, finanse i sztuczna inteligencja potrzebują pamięci maszynowej, ale takiej, która pozostaje kontrolowalna przez człowieka.

Nie wolno jednak mylić blockchaina z prawdą. Technologia ta może zabezpieczać zapis, lecz nie gwarantuje automatycznie prawdziwości danych wejściowych. Jeśli czujnik kłamie, człowiek wprowadza fałszywą informację, certyfikat jest fikcyjny, źródło źle opisane lub model AI pracuje na skażonych danych – blockchain jedynie utrwali błąd w bardziej elegancki sposób. To jedna z najważniejszych lekcji: niezmienność nie jest sprawiedliwością, hash nie jest mądrością, a smart kontrakt nie jest sumieniem. Technologia może utrudnić manipulację po fakcie, ale nie zwalnia z odpowiedzialności za jakość faktu przed zapisem. Dlatego przyszłość blockchaina zależy od tego, czy zostanie wpisany w szerszy porządek instytucjonalny. Potrzebuje prawa, standardów, audytu, interoperacyjności, ochrony danych, procedur sprostowania, cyberbezpieczeństwa, edukacji użytkowników i realnych mechanizmów odpowiedzialności. Bez tego stanie się kolejną maszyną iluzji: będzie obiecywał przejrzystość, której nikt nie potrafi odczytać; decentralizację kontrolowaną przez kilku operatorów; automatyzację nieznającą wyjątków oraz prywatność kończącą się tam, gdzie zaczyna się regulamin platformy. Cyfrowa cywilizacja nie potrzebuje więcej zaklęć. Potrzebuje systemów, które działają, gdy przestaje działać propaganda.

Technologia musi służyć człowiekowi, a nie nadzorowi

W ramach Smart Cities blockchain może wspierać transport, energetykę, gospodarkę odpadami, usługi publiczne oraz miejską koordynację danych. Inteligentne miasto nie może jednak stać się miastem totalnie ciekawskim. Technologia powinna służyć mieszkańcowi, a nie przekształcać go w chodzący strumień danych. Miasto przyszłości powinno wiedzieć wystarczająco dużo, by działać sprawniej, i wystarczająco mało, by nie naruszać wolności jednostki.

W e-administracji blockchain może zwiększyć wiarygodność rejestrów, ograniczyć korupcję, usprawnić zarządzanie cyfrową tożsamością oraz poprawić ścieżkę audytu. Administracja nie może jednak ukrywać arbitralności decyzji za kodem. Obywatel ma prawo rozumieć każdą decyzję, kwestionować ją i oczekiwać ludzkiej odpowiedzialności tam, gdzie zawodzi automatyzm.

W sektorze zdrowia blockchain może oddać pacjentowi kontrolę nad dokumentacją medyczną, umożliwić precyzyjne zarządzanie zgodami, zabezpieczyć ścieżkę dostępu, wspierać badania kliniczne oraz śledzić leki w łańcuchu dostaw. To jedno z najbardziej obiecujących zastosowań, gdyż dotyczy danych szczególnie wrażliwych, co wymaga najwyższej ostrożności. Dane medyczne nie są surowcem do eksploatacji; są zapisem ludzkiej kruchości. Pacjent nie może zostać sprowadzony do roli dostawcy danych dla modeli AI, ubezpieczycieli czy platform.

W Przemyśle 5.0 i łańcuchach dostaw blockchain może przywrócić przejrzystość w obszarach, które globalna gospodarka chętnie ukrywała: pochodzenie surowców, warunki produkcji, fałszowanie certyfikatów, ślad środowiskowy czy drogę produktu od źródła do konsumenta. Kluczowe jest tutaj to, że nie wystarczy śledzić produktu – trzeba śledzić odpowiedzialność. Blockchain może stać się cyfrowym paszportem towaru, ale bez rzetelnej kontroli pozostanie jedynie pustą formą. Jeśli dane środowiskowe i społeczne będą fikcyjne, technologia ta stworzy greenwashing w wersji niezmiennej. Niezmienny fałsz jest bowiem bardziej niebezpieczny niż kłamstwo zwykłe.

W kontekście bezpieczeństwa danych AI blockchain może pełnić funkcję pamięci procesu: rejestrować pochodzenie danych, wersje modeli, aktualizacje oraz ścieżki audytu. Może to pomóc ograniczyć problem „czarnej skrzynki", choć samo w sobie go nie rozwiąże. Rejestrowalność nie jest bowiem tożsama z wyjaśnialnością. Księga może pamiętać, ale nie musi rozumieć.

Blockchain jako interdyscyplinarna tarcza przed automatyzacją i nadzorem

Dlatego blockchain powinien wspierać XAI, audyty, ocenę biasu, dokumentację danych oraz odpowiedzialność instytucji. W świecie, w którym AI coraz częściej klasyfikuje, rekomenduje, diagnozuje, profiluje i decyduje, pytanie nie brzmi już tylko o to, czy model działa, lecz czy można odtworzyć, zakwestionować i naprawić jego działanie.

W obszarze ochrony dziedzictwa kulturowego blockchain i AI ukazują najbardziej humanistyczną twarz technologii. Podczas gdy AI może rekonstruować zniszczone znaki oraz wspierać OCR, transliterację i tłumaczenie manuskryptów, blockchain pozwala zabezpieczyć wersje, metadane, autentyczność i ścieżkę interpretacji. Jest to kluczowe w epoce treści generatywnych, która będzie coraz bardziej potrzebowała wiarygodnych źródeł. Im więcej syntetycznej mgły w obiegu informacyjnym, tym większa wartość autentycznego archiwum. Wymaga to jednak rygoru: oryginał, rekonstrukcja, hipoteza, tłumaczenie i komentarz muszą pozostać od siebie wyraźnie odróżnione. AI nie może produkować przeszłości pod pozorem jej ratowania.

Z kolei projekt Q-BALAK pokazuje, że blockchain przenika nawet do najstarszej infrastruktury cywilizacji: rolnictwa. Dane z czujników, dronów i systemów IoT mogą optymalizować gospodarowanie wodą, nawożenie, jakość plonów, a także usprawnić płatności, ubezpieczenia i bezpieczeństwo żywności. Lekka kryptografia oraz odporność kwantowa stanowią tu odpowiedź na realne ograniczenia urządzeń pracujących w terenie. Cyfrowe rolnictwo musi jednak chronić producenta przed nową formą zależności – kto kontroluje dane o polu, może kontrolować

przyszłość gospodarstwa. Dlatego dane rolnicze muszą podlegać zasadom własności, przenoszalności, dostępu, audytu i sprawiedliwego podziału korzyści. Ziemia nie powinna stać się tylko interfejsem dla platformy.

CBDC domyka tę układankę, przenosząc blockchainową wyobraźnię do samego centrum władzy monetarnej. Cyfrowa waluta banku centralnego może zwiększyć odporność płatności, ograniczyć koszty, wesprzeć inkluzję finansową, przyspieszyć transfery publiczne i umożliwić nowe formy rozliczeń w gospodarce tokenizowanej. Może jednak stać się również infrastrukturą nadzoru i ograniczania prywatności finansowej.

Pieniądz cyfrowy nie jest bowiem tylko pieniądzem. Jest konstytucją codziennych transakcji. Jeśli zostanie zaprojektowany z poszanowaniem gotówki, prywatności offline, limitami władzy i dostępnością dla wykluczonych, może wzmocnić państwo usługowe. Jeśli zaś stanie się centralnym rejestrem życia płatniczego, będzie cyfrowym snem biurokraty o doskonałej widoczności obywatela.

Wszystkie te obszary prowadzą do wspólnego wniosku: blockchain nowej generacji jest technologią graniczną. Stoi na styku finansów i prawa, danych i zaufania, automatyzacji i odpowiedzialności, prywatności i audytu, rynku i państwa, człowieka i maszyny oraz pamięci i predykcji. Dlatego nie wolno oddać go wyłącznie w ręce techników, inwestorów, regulatorów czy ideologów decentralizacji. Wymaga on interdyscyplinarnego nadzoru: prawników, ekonomistów, informatyków, socjologów, etyków, urbanistów, lekarzy, rolników, archiwistów, ekspertów cyberbezpieczeństwa i samych obywateli.

Blockchain jako odpowiedzialna infrastruktura zaufania

W przeciwnym razie stanie się technologią zbyt potężną, by pozostawić ją samej sobie. Najbardziej niebezpieczna jest pokusa automatyzacji pozbawionej odpowiedzialności. Smart kontrakt może wykonać warunek, ale nie rozpozna sprawiedliwości. AI może wykryć wzorzec, lecz nie zawsze zrozumie człowieka. Blockchain potrafi utrwalić zapis, ale nie oceni jego sensu. CBDC przyspieszy płatność, lecz nie rozstrzygnie, czy dany warunek był moralnie dopuszczalny. Sensor zmierzy wilgotność, ale nie zastąpi doświadczenia rolnika, a cyfrowy bliźniak może symulować miasto, lecz nigdy nie przeżyje życia jego mieszkańca.

Dlatego technologia przyszłości musi być projektowana w duchu Przemysłu 5.0: z człowiekiem w centrum, zrównoważeniem jako warunkiem i odpornością jako celem. Nie chodzi tu o sentymentalne hamowanie innowacji, lecz o poważne potraktowanie jej skutków. Entuzjazm bez kontroli jest dziecinny. Lęk bez analizy jest jałowy. Dojrzałość polega na budowaniu systemów

jednocześnie wydajnych i ograniczonych prawem, szybkich i audytowalnych, zautomatyzowanych i odwoływalnych, rozproszonych i interoperacyjnych, cyfrowych, a jednak dostępnych dla osób niecyfrowych – prywatnych, lecz zgodnych z uzasadnionym nadzorem. To nie są sprzeczności, lecz warunki cywilizowanej technologii.

Blockchain przyszłości może potoczyć się w trzech kierunkach. Pierwszy to los spekulacyjnej niszy: pozostanie narzędziem finansowych eksperymentów, tokenowych mód i społeczności żyjących na granicy regulacji. Drugi to los dekoracji: zostanie dodany do projektów publicznych i korporacyjnych jako modne hasło, bez realnej zmiany w strukturze odpowiedzialności. Trzeci zaś to los infrastruktury: stanie się warstwą wiarygodności dla danych, decyzji, tożsamości, aktywów, dokumentów, płatności i procesów społecznych. Tylko ta trzecia droga jest warta wysiłku.

Warunkiem sukcesu jest jednak pokonanie konkretnych barier. Skalowalność musi zostać rozwiązana bez uciekania się do pustej centralizacji. Interoperacyjność powinna przełamać silosy i vendor lock-in. Prywatność musi być projektowana od początku, a nie doklejana po kolejnym skandalu. Energooszczędność musi stać się normą, a kryptografia postkwantowa – wyrazem odpowiedzialności długofalowej.

AI musi być audytowalna, smart kontrakty wymagać procedur wyjątków, a CBDC chronić wolność płatniczą. Dane sektorowe – medyczne, rolnicze, miejskie czy administracyjne – muszą mieć jasny reżim własności i prawa do sprostowania. Bez tego blockchain będzie szybciej obiecywał, niż cywilizacja zdoła naprawiać jego błędy. Najtrafniejszy bon mot dla tej epoki brzmi: nie wszystko, co da się zapisać niezmiennie, zasługuje na niezmienność. Niektóre dane powinny zostać zapomniane, błędy sprostowane, decyzje podważone, a automatyzmy zatrzymane. Niektóre transakcje wymagają wyjaśnienia, rejestry otwartości, a prywatność ochrony przed ciekawością systemu. Technologia zaufania nie może stać się technologią wiecznego uwięzienia w zapisie; prawo do pamięci musi być równoważone prawem do korekty i ludzkiego kontekstu.

Ostatecznie blockchain nie jest zbawieniem cyfrowej cywilizacji, lecz narzędziem, które może pomóc jej nie utonąć w nieufności, fałszerstwach, czarnych skrzynkach czy dominacji scentralizowanych platform. Wymaga on jednak mądrego użytkownika i dojrzałych instytucji. Jeśli oddamy mu zbyt wiele, otrzymamy automatyczny porządek pozbawiony rozumu. Jeśli odrzucimy go z lęku, stracimy szansę na przejrzystą infrastrukturę. Stawka nie dotyczy tego, czy blockchain „wygra", lecz tego, czy społeczeństwo nauczy się go używać bez klękania przed nim.

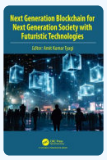
Cywilizacja cyfrowa potrzebuje kręgosłupa zaufania, ale kręgosłup nie może zastąpić mózgu, serca i sumienia. Blockchain może być tym kręgosłupem: utrzymywać zapis, porządkować przepływy i przenosić ciężar dowodu. Mózgiem muszą pozostać instytucje zdolne do krytyki. Sercem –

człowiek, którego dane, praca, zdrowie i wolność są stawką całego procesu. Sumieniem zaś prawo i etyka, które przypominają, że efektywność bez granic jest tylko elegancką formą przemocy.

Teza brzmi stanowczo: blockchain nowej generacji ma sens tylko jako technologia odpowiedzialnego zaufania. Nie jako religia decentralizacji, cudowny lek na korupcję czy ozdobnik administracyjny. Nie jako zabawka finansowa ani pretekst do nadzoru. Ma być infrastrukturą, która pomaga społeczeństwu pamiętać uczciwie, rozliczać przejrzyście i chronić człowieka przed arbitralnością tych, którzy dotąd mogli mówić: „proszę nam zaufać". W epoce cyfrowej to zdanie już nie wystarczy. Potrzebujemy systemów, które potrafią odpowiedzieć: „nie musicie wierzyć na słowo – możecie sprawdzić".

> Blockchain może dostarczyć cywilizacji cyfrowej niezbędnego kręgosłupa zaufania, lecz sam w sobie nie zastąpi mózgu, serca ani sumienia. Jeśli pozwolimy, by efektywność algorytmiczna wyparła ludzki kontekst i etykę, stworzymy jedynie elegancki system wiecznego uwięzienia w niezmiennym zapisie. Prawdziwym triumfem tej technologii nie będzie zatem moment jej powszechnego wdrożenia, lecz chwila, w której przestaniemy klękać przed kodem, a zaczniemy go używać do ochrony tego, co w nas najbardziej ludzkie.

Inspiracje

[1] 

"Next Generation Blockchain for Next" Amit Kumar Tyagi

2026 | CRC Press | ISBN: 9781041026075

Dr **Amit Kumar Tyagi** jest adiunktem na Narodowym Uniwersytecie Nauk Kryminalistycznych w Gandhinagarze w Indiach. Uzyskał tytuł doktora na Uniwersytecie Centralnym w Pondicherry w 2018 roku. W trakcie swojej kariery akademickiej zajmował stanowiska w wielu instytucjach, w tym w Narodowym Instytucie Technologii Mody i Instytucie Technologii w Vellore. Dr Tyagi jest starszym członkiem IEEE i posiada bogate portfolio badawcze, koncentrujące się na uczeniu maszynowym, technologii blockchain, systemach cyberfizycznych i prywatności danych. Brał udział w ważnych projektach badawczych, takich jak „AARIN" i „P3-Block", które dotyczą kwestii prywatności w zastosowaniach motoryzacyjnych i medycznych. Jest płodnym autorem i redaktorem, opublikował ponad 350 artykułów naukowych i brał udział w powstaniu ponad 60 książek. Jest również laureatem Nagrody Badawczej Wydziału od Instytutu Technologii w Vellore przez trzy kolejne lata (2020–2022).

*Dr. **Amit Kumar Tyagi** is an Assistant Professor at the National Forensic Sciences University in Gandhinagar, India. He earned his Ph.D. from Pondicherry Central University in 2018. Throughout his academic career, he has held positions at several institutions, including the National Institute of Fashion Technology and the Vellore Institute of Technology. Dr. Tyagi is a Senior Member of the IEEE and has an extensive research portfolio focusing on machine learning, blockchain technology, cyber-physical systems, and data privacy. He has contributed to significant research projects such as "AARIN" and "P3-Block," which address privacy issues in vehicular and medical applications. A prolific author and editor, he has published over 350 research articles and has been involved in the creation of more than 60 books. He is also a recipient of the Faculty Research Award from the Vellore Institute of Technology for three consecutive years (2020–2022).*

National Forensic Sciences University

Literatura uzupełniająca

Książki

Literatura pokrewna (Google Scholar):

[1] **"Proof of Stake Vitalik Buterin"**

[2] **"Mastering Blockchain Second Edition Imran Bashir"**

[3] **"Mastering Blockchain 4th Edition Imran Bashir"**

[4] **"Blockchain Basics David Drescher"**

[5] **"Cryptoassets Chris Burniske"**

Artykuły naukowe

Artykuły pokrewne (Google Scholar):

[1] **"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

Google Scholar

[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

Google Scholar

[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

Google Scholar

[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

Google Scholar

[5] "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

Google Scholar

[6] "Generalized Voronoi Tessellation as a Model of Two-dimensional Cell Tissue Dynamics"

Martin Böck, Amit Kumar Tyagi, Jan-Ulrich Kreft, Wolfgang Alt

2010 | Bulletin of Mathematical Biology | DOI: 10.1007/s11538-009-9498-3

Google Scholar

[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

Google Scholar

[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

Google Scholar

[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

Google Scholar

[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

Google Scholar

APA ONE Publishing System

Article ID: ef562e2c-4be9-4295-b290-102d453e20ab