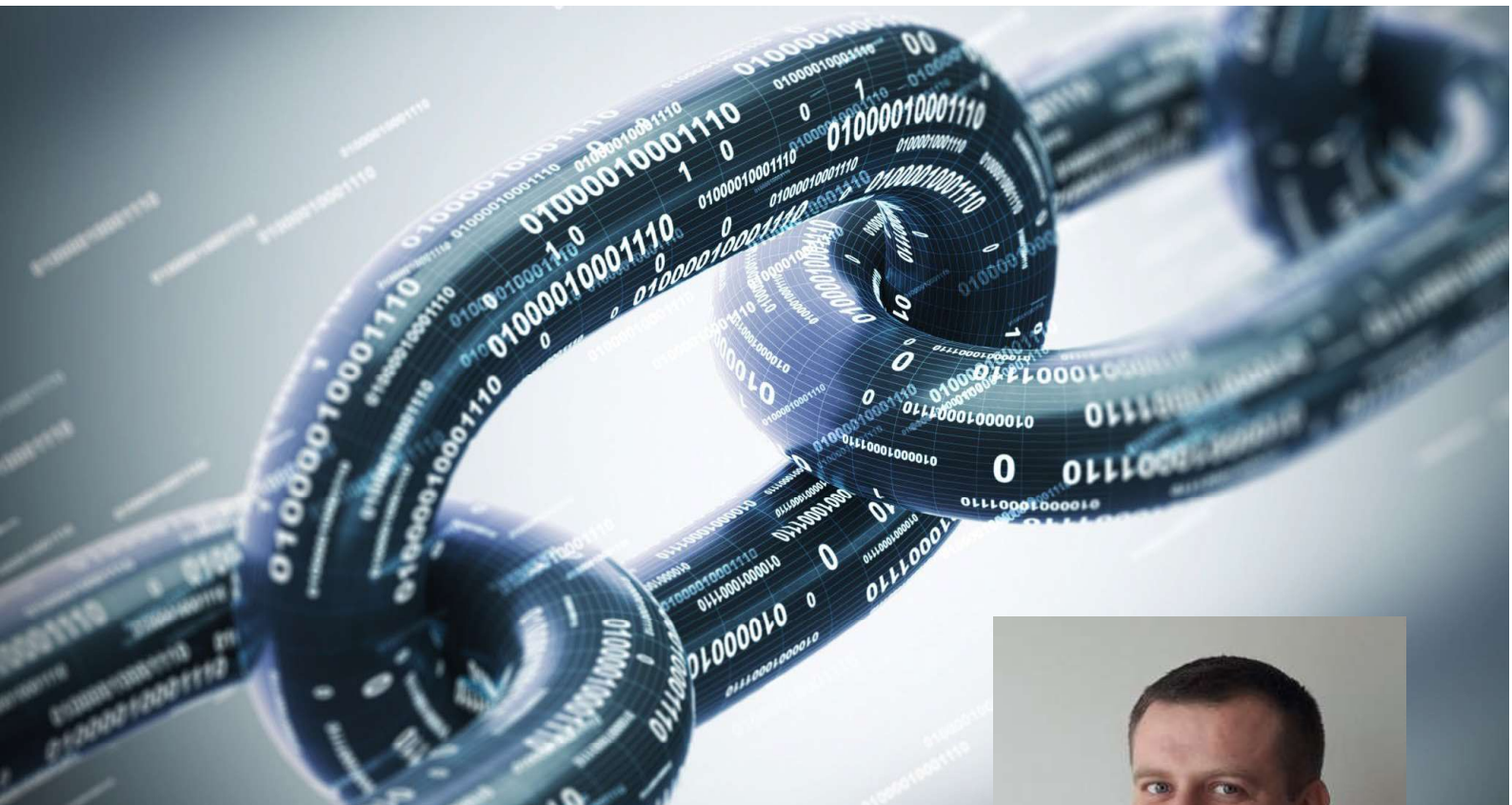


TECHNOLOGIA BLOCKCHAIN I ROZPROSZONYCH REJESTRÓW DLT

RAPORT O STANIE NORMALIZACJI



Organizacje normalizacyjne ISO/CEN-CLC/PKN

Normy międzynarodowe zawierają zasady oraz wytyczne lub opisują cechy charakterystyczne działań i ich wyników, a ich celem jest osiągnięcie optymalnego stopnia uporządkowania w danym kontekście. Takim kontekstem jest niewątpliwie technologia BLOCKCHAIN, technologia o globalnym oddziaływaniu. To właśnie zakres tego oddziaływania, liczba zaangażowanych podmiotów wymagają ujednoczenia podejścia do zagadnienia, sformułowania wytycznych bezpieczeństwa i eliminacji barier technicznych pomiędzy interesariuszami.

Międzynarodowy Komitet Techniczny ISO/TC 307 Blockchain and Distributed Ledger Technologies (ISO – International Organization for Standardization; TC – Technical Committee) powstał w 2016 r. Celem Komitetu jest zaspokojenie powyższych potrzeb poprzez opracowywanie i publikację norm, raportów i specyfikacji technicznych dotyczących blockchain i technologii rozproszonych rejestrów DLT (Distributed Ledger Technology). Sekretariat komitetu prowadzony jest przez australijską organizację normalizacyjną SA (Standards Australia). Komitet tworzy 46 członków czynnych (P – participating member) z prawem do głosowania oraz 14 członków obserwujących (O – observing member) bez takiego prawa. Polska jest członkiem czynnym.

W komitecie technicznym ISO/TC 307 toczą się najbardziej zaawansowane prace dotyczące opracowywania od podstaw nowych standardów w zakresie technologii blockchain. Cztery dokumenty zostały opublikowane przez TC 307, co przedstawia tabela nr 1, a jedenaście jest w trakcie opracowywania bądź prac rozwojowych, co zostało przedstawione w tabeli nr 2.



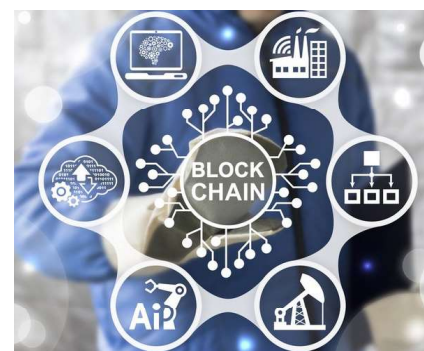
MICHAŁ ŁONIEWSKI

Kierownik Wydziału Rozwoju Usług Technicznych i Metod Badawczych Departament Innowacji i Rozwoju Urząd Dozoru Technicznego

Przewodniczący Komitetu Technicznego PKN nr 333 ds. Blockchain i Technologii Rozproszonych Rejestrów oraz członek grupy roboczej ISO/TC 307/WG 6 ds. praktycznego zastosowania technologii. Certyfikowany specjalista bezpieczeństwa funkcjonalnego (CFSS) oraz audytor w obszarze certyfikacji systemów zarządzania bezpieczeństwem funkcjonalnym – FSM oraz cyberbezpieczeństwa.

Tabela 1. Standardy opublikowane przez komitet techniczny ISO/TC 307

Numer normy/raportu technicznego	Tytuł normy/raportu technicznego
ISO 22739:2020	Blockchain and distributed ledger technologies – Vocabulary
ISO/TR 23244:2020	Blockchain and distributed ledger technologies – Privacy and personally identifiable information protection considerations
ISO/TR 23455:2019	Blockchain and distributed ledger technologies – Overview of and interactions between smart contracts in blockchain and distributed ledger technology systems
ISO/TR 23576:2020	Blockchain and distributed ledger technologies – Security management of digital asset custodians



Komitetem europejskim ściśle współpracującym z ISO/TC 307 jest Komitet Techniczny **CEN-CENELEC/JTC 19 Blockchain and Distributed Ledger Technologies** (Joint Technical Committee), prowadzony przez włoską organizację normalizacyjną UNI (Ente Italiano di Normazione). Komitet zawiązał się w 2019 r., jego głównymi działaniami są: identyfikacja i wdrażanie norm międzynarodowych, które zostały już opublikowane bądź są w trakcie opracowywania. Przykładem takiego dokumentu jest norma dotycząca terminologii występującej w technologii blockchain i rozproszonych rejestrów DLT: **ISO 22739:2020 Blockchain and distributed ledger technologies – Vocabulary**, nad którą trwają prace w CEN/CLC dotyczące przyjęcia jej jako standardu europejskiego.

Krajowym komitetem, którego zakresem działania jest normalizacja w dziedzinie blockchain i technologii rozproszonych rejestrów, jest komitet techniczny **PKN/KT 333 ds. Blockchain i Technologii Rozproszonych Rejestrów**. To najmłodszy komitet spośród trzech wymienionych, powstał w grudniu 2019 r. Jest to organ wiodący w zakresie współpracy z CEN/CLC JTC 19 oraz ISO/TC 307. Urząd Dozoru Technicznego jest członkiem Komitetu Technicznego nr 333. Na co dzień w jego pracach uczestniczy dwóch reprezentantów UDT.

Wybrane aspekty normalizacji blockchain/DLT

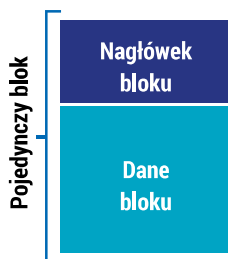
ISO 22739:2020 Blockchain and distributed ledger technologies – Vocabulary

Norma zawiera 84 definicje wspólne dla wszystkich standardów opracowywanych w ISO/TC 307 i dotyczących technologii blockchain oraz DLT. Obecnie trwają prace nad drugą edycją dokumentu. Przykładowe definicje umieszczone w standardzie wyglądają następująco (definicje w oryginale występują w języku angielskim; tłumaczenie na język polski wykonano na potrzeby niniejszego artykułu).

Tabela 2. Standardy w trakcie prac rozwojowych komitetu technicznego ISO/TC 307

Numer normy/specyfikacji/raportu technicznego	Tytuł normy/specyfikacji/raportu technicznego
ISO/DTR 3242	Blockchain and distributed ledger technologies – Use cases
ISO/WD TR 6039	Blockchain and distributed ledger technologies – Identifiers of subjects and objects for the design of blockchain systems
ISO/WD TR 6277	Blockchain and distributed ledger technologies – Data flow model for blockchain and DLT use cases
ISO/WD 22739	Blockchain and distributed ledger technologies – Vocabulary (2 edycja)
ISO/DTR 23249	Blockchain and distributed ledger technologies – Overview of existing DLT systems for identity management
ISO/DIS 23257	Blockchain and distributed ledger technologies – Reference architecture
ISO/DTS 23258	Blockchain and distributed ledger technologies – Taxonomy and Ontology
ISO/WD TS 23259	Blockchain and distributed ledger technologies – Legally binding smart contracts
ISO/DTS 23635.2	Blockchain and distributed ledger technologies – Guidelines for governance
ISO/AWI TR 23642	Blockchain and distributed ledger technologies – Overview of smart contract security good practice and issues
ISO/WD TR 23644	Blockchain and distributed ledger technologies – Overview of trust anchors for DLT-based identity management (TADIM)

Block – structured data comprising a block header and block data;
 → Blok – dane strukturalne zawierające nagłówek i dane bloku. Blok schematycznie przedstawiono na rysunku nr 1.



Rys. 1. Pojedynczy blok w łańcuchu bloków

Block data – Structured data comprising zero or more transaction records or references to transaction records;

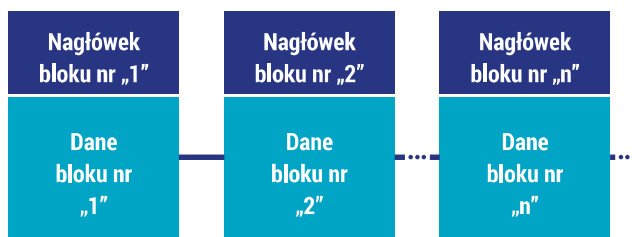
→ Dane bloku – ustrukturyzowane dane zawierające zero lub więcej rekordów transakcji lub odniesienia do rekordów transakcji.

Block header – structured data that includes a cryptographic link to the previous block unless there is no previous block;

→ Nagłówek bloku – dane strukturalne, które zawierają klucze kryptograficzne do poprzedniego bloku, chyba że nie ma poprzedniego bloku (blok pierwszy).

Blockchain – distributed ledger with confirmed blocks organized in an append-only, sequential chain using cryptographic links;

→ Łańcuch bloków – rozproszona księga/rejestr z potwierdzonymi blokami zorganizowanymi w sekwencyjny łańcuch, z możliwością tylko dopisywania, przy użyciu łączy kryptograficznych. Ideę łańcucha bloków przedstawia rysunek nr 2.



Rys. 2. Łańcuch bloków – pojedyncza kopia rozproszonego rejestru

Smart contract – computer program stored in a DLT system wherein the outcome of any execution of the program is recorded on the distributed ledger

→ Inteligentny kontrakt – program komputerowy przechowywany w systemie DLT, w którym wynik dowolnego wykonania programu zapisywany jest w rozproszonym rejestrze.

Pod definicją znajduje się informacja, że inteligentny kontrakt może reprezentować warunki umowy w prawie i tworzyć prawnie wykonalne zobowiązanie na mocy przepisów obowiązującej jurysdykcji. Oznacza to, że standard dopuszcza prawne skutki systemów blockchain/DLT wykorzystujących inteligentne kontrakty, o ile jest to zgodne z obowiązującym prawem krajowym lub lokalnym.

Kwestie prawne dotyczące stosowania inteligentnych kontraktów w systemach blockchain będzie omawiać projektowana specyfikacja techniczna **ISO/WD TS 23259 Blockchain and distributed ledger technologies – Legally binding smart contracts**. Kwestie techniczne natomiast zostały poruszone w raporcie technicznym **ISO/TR 23455:2019 Blockchain and distributed ledger technologies – Overview of and interactions between smart contracts in blockchain and distributed ledger technology systems**.

ISO/DTR 3242 Blockchain and distributed ledger technologies – Use Cases Summary Report

Raport techniczny dotyczący przykładów wykorzystania technologii blockchain/DLT jest w trakcie opracowywania. Celem dokumentu jest prezentacja procesów i struktur praktycznych przykładów zastosowania technologii blockchain/DLT, które mogą być wykorzystane przez odbiorców dokumentu.

Raport zawiera 21 przypadków rzeczywistego zastosowania technologii. Każdy z przypadków to 20–30 stron szczegółowego opisu w 45 pozycjach, m.in.:

- Jaki problem (biznesowy) jest rozwiązywany przez system BC/DLT?
- Stan bieżący: w produkcji / w testach / w implementacji
- Prognozowane wyniki z implementacji
- Dlaczego użyto DLT?
- Wymagania funkcjonalne / niefunkcjonalne
- Jak będzie zapewnione bezpieczeństwo, prywatność, identyfikowalność?
- Informacje o użytych smart kontraktach – np.: cel użycia, rola
- Informacje o zastosowanym Open Source Software
- Zidentyfikowane ryzyka
- Normy / specyfikacje / raporty referencyjne
- Analizy przepływu danych
- Architektura systemu
- Diagram sekwencji działania systemu / inteligentnego kontraktu

Przypadki zastosowania podzielone zostały na cztery kategorie:

- Pochodzenie danych (*data provenance*)
- Łańcuch dostaw (*supply chain*)
- Finanse (*fintech*)
- Inteligentna energia (*smart energy*)

Wśród nich możemy znaleźć systemy: weryfikacji autentyczności dyplomów uczelni wyższych, autentyczności czerwonych sycylijskich pomarańczy, oryginalności pochodzenia leków, systemy zarządzania odpadami komunalnymi czy też służące do rozliczania prosumentów energii elektrycznej przetwarzanej ze źródeł odnawialnych w mikrosieciach i oddawanej do sieci krajowej.

Innowacyjne zastosowania technologii

Technologia blockchain w zastosowaniach fintech, jak np. sieć ethereum/bitcoin, przestaje być uznawana za innowacyjną. Innowacyjne natomiast wciąż pozostają jej inne, nietypowe zastosowania. Ciekawym przykładem takiego zastosowania jest wykorzystanie technologii wraz z przemysłowym internetem rzeczy (IIoT – Industrial Internet of Things) oraz technologią dużych stosów danych (big data) i siecią 5G.

Technologia IIoT dostarcza bezprzewodowo bieżące wartości istotnych parametrów procesowych (ciśnienie, temperatura) zbieranych za pomocą czujników fizycznie rozmieszczonych na instalacji. Technologia blockchain/DLT pozwala na kolekcjonowanie danych z czujników IIoT w sposób niezaprzeczalny, co minimalizuje ryzyko kompromitacji wartości danych procesowych (element cyberbezpieczeństwa). Analiza dużych stosów danych pochodzących z czujników IIoT za pomocą rozwiązań big data umożliwia predykcję w zakresie potencjalnych, zbliżających się zagrożeń dla instalacji. Sieć 5G natomiast umożliwia bezproblemową komunikację czujników IIoT z odpowiednimi systemami IT/OT. Rysunek nr 3 przedstawia przykładowe opomiarowanie instalacji przemysłu procesowego.

Przykłady łączenia szeroko pojętej technologii IoT (Internet of Things) wraz z technologią blockchain będzie można znaleźć w projektowanym raporcie technicznym połączonego komitetu technicznego dwóch międzynarodowych organizacji normalizacyjnych ISO oraz IEC (IEC – International Electrotechnical Commission) – ISO/IEC JTC 1/SC 41 Internet of things and digital twin (cyfrowy bliźniak), w grupie roboczej WG5:

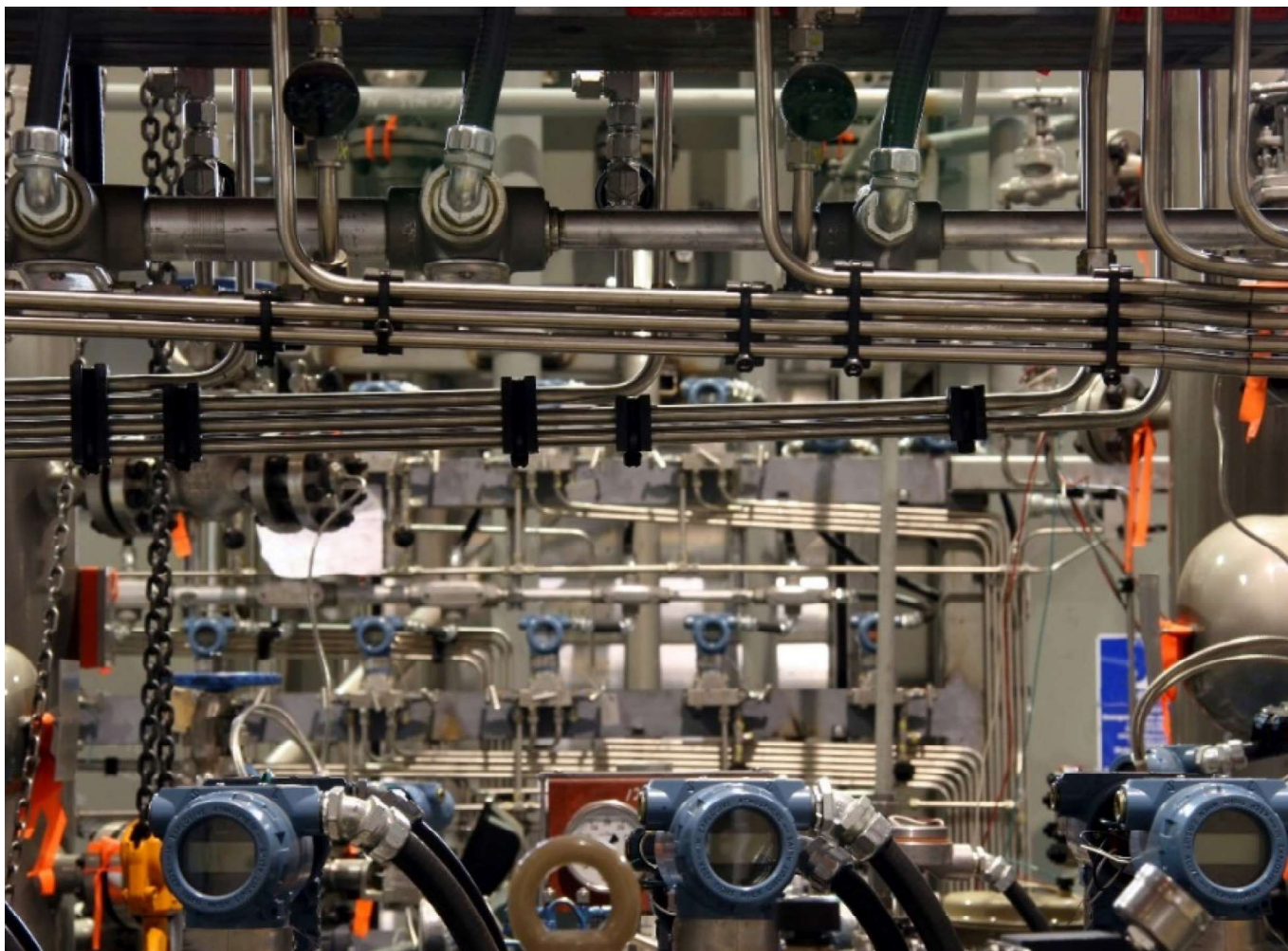
IoT Application (wdrożenia/aplikacje technologii internetu rzeczy): **ISO/IEC DTR 30176: Internet of Things (IoT) – Integration of IoT and DLT/Blockchain: Use Cases.**

Podsumowanie

Podstawowym celem normalizacji jest zapewnienie, uzgodnionych na arenie międzynarodowej, najlepszych praktyk i ram poprawiających bezpieczeństwo i interoperacyjność technologii. Systemy blockchain zbudowane są na różnych mechanizmach konsensusu, z różnymi poziomami uprawnień węzłów sieci (węzły trzymające kopie rejestru, węzły walidujące nowe transakcje, uczestniczące w mechanizmie konsensusu). Brak standaryzacji znacząco ograniczyłoby stosowanie systemów o globalnym zasięgu i oddziaływaniu. Wspólne wytyczne i praktyka inżynierska ujęte w standardach to eliminacja barier technicznych dla wszystkich interesariuszy systemów blockchain/DLT – integratorów systemów, beneficjentów technologii, audytorów czy też zamawiających.

Osoby zainteresowane, które chciałyby czynnie uczestniczyć w pracach normalizacyjnych komitetu PKN KT 333, w każdej chwili mogą dołączyć do prac jego członków poprzez kontakt z sekretariatem oraz wysłanie zgłoszenia na adres: Polski Komitet Normalizacyjny, 00-050 Warszawa, ul. Świętokrzyska 14 B lub michal.loniewski@udt.gov.pl.

Zgłoszenie do PKN/KT 333 daje możliwość bezpośredniego udziału w pracach ISO/TC 307 oraz CEN/CLC/JTC 19 poprzez członkostwo czynne P-member w wyżej wymienionych komitetach. ■



Rys. 3. Przykład opomiarowania instalacji procesowej z wykorzystaniem czujników, przetworników i rurek impulsowych