ČESKÁ TECHNICKÁ NORMA

ICS 35.030; 35.240.40; 35.240.99 **Listopad 2023**

Blockchain a technologie distribuovaného registru – Referenční architektura

ČSN
ISO 23257

36 9013

Blockchain and distributed ledger technologies – Reference architecture

Technologies des chaînes de blocs et technologies de register distribué – Architecture de référence

Tato norma je českou verzí mezinárodní normy ISO 23257:2022. Překlad byl zajištěn Českou agenturou pro standardizaci. Má stejný status jako oficiální verze.

This standard is the Czech version of the International Standard ISO 23257:2022. It was translated by the Czech Standardization Agency. It has the same status as the official version.

Národní předmluva

Informace o citovaných dokumentech

ISO 22739 zavedena v ČSN EN ISO 22739 (36 9009) Blockchain a technologie distribuovaného registru – Slovník

ISO/IEC 24760-1 zavedena v ČSN EN ISO/IEC 24760-1 (36 9716) Bezpečnost IT a soukromí – Rámec pro řízení identit – Část 1: Terminologie a pojmy

Souvisící ČSN

ČSN ISO 7498-2:1993 (36 9615) Systémy na spracovanie informácií. Prepojenie otvorených systémov (OSI). Základný referenčný model. Část 2: Bezpečnostná architektúra

ČSN EN ISO 16484-2:2005 (73 8521) Automatizační a řídicí systémy budov – Část 2: Hardware

ČSN ISO/TR 18307 (98 1018) Zdravotnická informatika – Interoperabilita a slučitelnost v normách pro předávání zpráv a komunikací – Klíčové charakteristiky

ČSN ISO/IEC 17788:2017 (36 9865) Informační technologie – Cloud computing – Přehled a slovník

ČSN ISO/IEC 17789:2017 (36 9866) Informační technologie – Cloud computing – Referenční architektura

ČSN ISO/IEC 21823-1:2020 (36 9022) Internet věcí (IoT) – Interoperabilita systémů IoT – Část 1:

Struktura

ČSN EN ISO 22300 (01 2301) Bezpečnost a odolnost – Slovník

ČSN EN ISO/IEC 24760-1 (36 9716) Bezpečnost IT a soukromí – Rámec pro řízení identit – Část 1: Terminologie a pojmy

ČSN EN ISO/IEC 27000 (36 9790) Informační technologie – Bezpečnostní techniky – Systémy řízení bezpečnosti informací – Přehled a slovník

ČSN EN ISO/IEC 27001 (36 9797) Informační bezpečnost, kybernetická bezpečnost a ochrana soukromí – Systémy managementu informační bezpečnosti – Požadavky

ČSN EN ISO/IEC 27018 (36 9709) Informační technologie – Bezpečnostní techniky – Soubor postupů na ochranu osobně identifikovatelných informací (PII) ve veřejných cloudech vystupujících jako zpracovatelé PII

ČSN ISO/IEC 27031:2016 (36 9801) Informační technologie – Bezpečnostní techniky – Směrnice pro připravenost informačních a komunikačních technologií pro kontinuitu činnosti organizace

ČSN EN ISO/IEC 29100 (36 9705) Informační technologie – Bezpečnostní techniky – Rámec soukromí

ČSN EN ISO/IEC 29134 (36 9712) Informační technologie – Bezpečnostní techniky – Směrnice pro posuzování dopadu na soukromí

ČSN EN ISO/IEC 29151 (36 9711) Informační technologie – Bezpečnostní techniky – Soubor postupů na ochranu osobně identifikovatelných informací

ČSN ISO/IEC 30141 (36 9021) Internet věcí (IoT) – Referenční architektura

ČSN ISO/IEC 38500:2020 (36 9045) Informační technologie – Správa a řízení IT technologií v organizaci

ČSN EN ISO/IEC 29100:2015/Amd. 1:2020 (36 9705) Informační technologie – Bezpečnostní techniky – Rámec soukromí

ČSN EN ISO 37101:2022 (73 0931) Udržitelný rozvoj ve společenstvích – Systém managementu udržitelného rozvoje – Požadavky s pokyny k použití

Vysvětlivky k textu této normy

V případě nedatovaných odkazů na evropské/mezinárodní normy jsou ČSN uvedené v článcích „Informace
o citovaných dokumentech“ a „Souvisící ČSN“ nejnovějšími vydáními, platnými v době schválení této normy. Při používání této normy je třeba vždy použít taková vydání ČSN, která přejímají nejnovější vydání nedatovaných evropských/mezinárodních norem (včetně všech změn).

Vysvětlivky k textu převzaté normy

Pro účely této normy byly použity následující anglické termíny v původní podobě, vzhledem k rozšíření těchto termínů v odborné komunitě a/nebo absenci českého ekvivalentu:

middleware, peer-to-peer, Proof of Stake, Proof of Work, Round Robin, uncle block

Upozornění na národní poznámky

Do normy byla k heslu 3.14 doplněna upřesňující národní poznámka. K heslu 3.18 byla doplněna národní poznámka převzatá z ČSN EN ISO 37101:2022.

Vypracování normy

Zpracovatel: ELA Blockchain Services a. s., IČO 08176868, Ing. Věra Šmídová

Technická normalizační komise: TNK 42 Výměna dat

Pracovník České agentury pro standardizaci: Ing. Miroslav Škop

Česká agentura pro standardizaci je státní příspěvková organizace zřízená Úřadem pro technickou normalizaci, metrologii a státní zkušebnictví na základě ustanovení § 5 odst. 2 zákona č. 22/1997 Sb., o technických požadavcích na výrobky a o změně a doplnění některých zákonů, ve znění pozdějších předpisů.

MEZINÁRODNÍ NORMA

Blockchain a technologie distribuovaného registru – Referenční architektura

ISO 23257
První vydání
2022-02

ICS 35.030; 35.240.40; 35.240.99

Obsah

Strana

Strana

Předmluva

ISO (Mezinárodní organizace pro normalizaci) je celosvětová federace národních normalizačních orgánů (členů ISO). Mezinárodní normy obvykle vypracovávají technické komise ISO. Každý člen ISO, který se zajímá o předmět, pro který byla vytvořena technická komise, má právo být v této technické komisi zastoupen. Práce se zúčastňují také vládní i nevládní mezinárodní organizace, s nimiž ISO navázala pracovní styk. ISO úzce spolupracuje s Mezinárodní elektrotechnickou komisí (IEC) ve všech záležitostech normalizace v elektrotechnice.

Postupy použité při tvorbě tohoto dokumentu a postupy určené pro jeho další udržování jsou popsány ve směrnicích ISO/IEC, část 1. Zejména se má věnovat pozornost rozdílným schvalovacím kritériím potřebným pro různé druhy dokumentů ISO. Tento dokument byl vypracován v souladu s redakčními pravidly uvedenými ve směrnicích ISO/IEC, část 2 (viz www.iso.org/directives).

Upozorňuje se na možnost, že některé prvky tohoto dokumentu mohou být předmětem patentových práv. ISO nelze činit odpovědnou za identifikaci jakéhokoliv nebo všech patentových práv. Podrobnosti o jakýchkoliv patentových právech identifikovaných během přípravy tohoto dokumentu budou uvedeny v úvodu a/nebo v seznamu patentových prohlášení obdržených ISO (viz www.iso.org/patents).

Jakýkoliv obchodní název použitý v tomto dokumentu se uvádí jako informace pro usnadnění práce uživatelů a neznamená schválení.

Vysvětlení nezávazného charakteru technických norem, významu specifických termínů a výrazů ISO, které se vztahují k posuzování shody, jakož i informace o tom, jak ISO dodržuje principy Světové obchodní organizace (WTO) týkající se technických překážek obchodu (TBT), viz www.iso.org/iso/foreword.html.

Tento dokument vypracovala technická komise ISO/TC 307 *Blockchain a technologie distribuovaného registru*.

Jakákoli zpětná vazba nebo otázky týkající se tohoto dokumentu mají být adresovány národnímu normalizačnímu orgánu uživatele. Úplný seznam těchto orgánů lze nalézt na adrese www.iso.org/members.html.

Úvod

Záznamy transakcí, založené na určitých dohodnutých podmínkách, tvoří základ pro výměnu aktiv mezi stranami. Podniky a vlády na tomto základu fungují po staletí. I když se kdysi používaly fyzické registry, byly z velké části nahrazeny moderní technologií. V tradičních přístupech však musí být registr centrálně řízen jednou nebo malým počtem stran a ostatní zúčastněné strany se na ně musí spoléhat jako na prostředníky, kteří tyto registry mění.

Důležitou vlastností registru je ověřitelnost. To znamená, že strany mohou ověřit, zda je soubor transakcí v registru úplný a přesný. V důsledku toho mohou tyto strany identifikovat nesrovnalosti v transakcích, například ověřit, zda jsou digitální aktiva účastníků správně zaúčtována ve finančním registru. V současné době je možné dosáhnout ověřitelného registru centralizovaným způsobem na základě určitých předpokladů důvěryhodnosti. Ověřitelnosti však lze dosáhnout také distribucí úložiště a decentralizací řízení registru s minimální důvěrou v kteroukoliv stranu.

Systémy technologie distribuovaného registru (DLT) včetně blockchainových systémů umožňují udržováním registru v distribuované síti sdílet pohled na registr mnohem širšímu okruhu stran a provádět v něm jejich vlastní změny.

Je možné široké spektrum obchodních řešení založených na DLT. Tento dokument představuje referenční architekturu pro taková řešení založená na DLT. Začíná definicemi a pojmy blockchainu a DLT, jako je organizace systému, povaha přístupu, typ konsenzu a role a odpovědnosti účastníků. Vzhledem k tomu, že referenční architektura musí pojmout širokou škálu možných případů použití, dotýká se na vysoké úrovni různých obchodních domén a jejich příslušných případů použití. Historicky registry usnadňovaly výměnu aktiv, ale řešení DLT lze využít i šířeji, a to pro výkaznictví, audity a koordinaci. Dokument nakonec čtenáři předkládá různé vrstvy referenční architektury pro systémy DLT a funkční komponenty v těchto vrstvách.

Tento dokument je určen mimo jiné pro akademiky, architekty řešení, zákazníky, uživatele, vývojáře, regulační orgány, auditory a organizace zabývající se tvorbou norem.

1 Předmět normy

Tento dokument stanovuje referenční architekturu pro systémy technologie distribuovaného registru (DLT) včetně blockchainových systémů. Referenční architektura se zabývá koncepty, průřezovými aspekty, architektonickými úvahami a pohledy na architekturu, včetně funkčních komponent, rolí, činností a jejich vztahů pro blockchain a DLT.