TCVN | **TIÊU CHUẨN QUỐC GIA**

DỰ THẢO

TCVN XXXXX:2026
ISO 22739:2024

Xuất bản lần 1

CÔNG NGHỆ BLOCKCHAIN VÀ SỔ CÁI PHÂN TÁN – TỪ VỰNG

Blockchain and distributed ledger technologies – Vocabulary

HÀ NỘI – 2026

MỤC LỤC

Lời nói đầu

TCVN XXXXX:2026 hoàn toàn tương đương với ISO 22739:2024.

TCVN XXXXX:2026 do Ban Cơ yếu Chính phủ biên soạn, Bộ trưởng Bộ Quốc phòng đề nghị, Ủy ban Tiêu chuẩn Đo lường Chất lượng Quốc gia thẩm định, Bộ Khoa học và Công nghệ công bố.

Lời giới thiệu

Tiêu chuẩn này định nghĩa các thuật ngữ liên quan đến các công nghệ chuỗi khối và sổ cái phân tán (DLT) để làm rõ ý nghĩa của các thuật ngữ và khái niệm được sử dụng trong các tài liệu khác thuộc lĩnh vực của ISO/TC 307.

Các tiêu chuẩn rõ ràng, nhất quán và mạch lạc đòi hỏi các thuật ngữ cũng rõ ràng, nhất quán và mạch lạc. Tài liệu này tuân theo Các quy tắc và nguyên tắc được đặt ra bởi ISO/TC 37, *Ngôn ngữ và thuật ngữ*, cho các tiêu chuẩn về thuật ngữ.

Tiêu chuẩn này áp dụng cho tất cả các dạng tổ chức (ví dụ: các doanh nghiệp thương mại, các cơ quan chính phủ và các tổ chức phi lợi nhuận). Đối tượng mục tiêu bao gồm nhưng không giới hạn ở các nhà nghiên cứu, kiến trúc sư giải pháp, khách hàng, người dùng, nhà phát triển công cụ, nhà quản lý, kiểm toán viên và các tổ chức phát triển tiêu chuẩn.

TIÊU CHUẨN QUỐC GIA **TCVN XXXXX:2026**

CÔNG NGHỆ BLOCKCHAIN VÀ SỔ CÁI PHÂN TÁN – TỪ VỰNG

Blockchain and distributed ledger technologies – Vocabulary

1 Phạm vi áp dụng

Tiêu chuẩn này quy định các thuật ngữ cơ bản cho các công nghệ chuỗi khối và sổ cái phân tán.

2 Tài liệu viện dẫn

Trong tiêu chuẩn này không có tài liệu nào được viện dẫn.

3 Thuật ngữ và định nghĩa

Tiêu chuẩn này sử dụng các định nghĩa và thuật ngữ sau đây:

3.1

tài sản (asset)

bất kỳ thứ gì có giá trị đối với một bên liên quan

[NGUỒN: ISO 19299:2020, 3.1, đã sửa đổi — CHÚ THÍCH đối với mục đã bị loại bỏ.]

3.2

khối (block)

dữ liệu có cấu trúc bao gồm *tiêu đề khối* (3.4) và *dữ liệu khối* (3.3)

3.3

dữ liệu khối (block data)

dữ liệu có cấu trúc bao gồm không hoặc nhiều *bản ghi giao dịch* (3.95) hoặc các tham chiếu đến các bản ghi giao dịch

3.4

tiêu đề khối (block header)

dữ liệu có cấu trúc bao gồm một *liên kết băm* (3.47) đến *khối* (3.2) trước đó, nếu có

CHÚ THÍCH 1: Tiêu đề khối cũng có thể chứa *dấu thời gian* (3.91), *nonce* (3.62), và dữ liệu đặc trưng của *nền tảng công nghệ sổ cái phân tán (DLT)* (3.33) khác, bao gồm *giá trị băm* (3.48) của *các bản ghi giao dịch* (3.95) tương ứng.

3.5

phần thưởng khối (block reward)

phần thưởng được cấp cho *thợ đào* (3.59) hoặc *người xác thực* (3.99) sau khi một *khối* (3.2) *được xác nhận (*3.9) trong *hệ thống chuỗi khối* (3.7)

CHÚ THÍCH 1: Phần thưởng có thể ở dạng *tài sản mã hóa* (3.14).

3.6

chuỗi khối (blockchain)

sổ cái phân tán (3.23) với các *khối* đã *được xác nhận* (3.10) được tổ chức thành một chuỗi tuần tự, chỉ cho phép ghi tiếp vào bằng cách sử dụng các *liên kết băm* (3.47)

3.7

hệ thống chuỗi khối (blockchain system)

hệ thống triển khai một *chuỗi khối* (3.6)

CHÚ THÍCH 1: Hệ thống chuỗi khối là một loại *hệ thống công nghệ sổ cái phân tán (DLT)* (3.35).

3.8

công nghệ chuỗi khối (blockchain technology)

công nghệ cho phép vận hành và sử dụng các *chuỗi khối* (3.6)

3.9

được xác nhận (confirmed)

được chấp nhận bởi *sự đồng thuận* (3.12) để ghi vào *sổ cái phân tán* (3.23)

3.10

khối đã được xác nhận (confirmed block)

khối (3.2) đã *được xác nhận* (3.9)

3.11

giao dịch đã được xác nhận (confirmed transaction)

giao dịch (3.93) đã *được xác nhận* (3.9)

3.12

sự đồng thuận (consensus)

thỏa thuận giữa *các nút công nghệ sổ cái phân tán* (DLT) (3.31) rằng:

- một *giao dịch* (3.93) được *xác thực* (3.97);

- *sổ cái phân tán* (3.23) chứa một tập hợp nhất quán và có thứ tự xác định của các bản ghi giao dịch đã được xác thực

CHÚ THÍCH 1: Sự đồng thuận không nhất thiết có nghĩa là tất cả các nút DLT đều đồng ý.

CHÚ THÍCH 2: Các chi tiết liên quan đến đồng thuận thì khác nhau giữa các *hệ thống DLT* (3.35) và đây có thể là một đặc trưng phân biệt giữa hệ thống DLT này và hệ thống DLT khác.

3.13

cơ chế đồng thuận (consensus mechanism)

tập hợp các quy tắc và thủ tục để đạt được *sự đồng thuận* (3.12)

CHÚ THÍCH 1: Các quy tắc và thủ tục này có liên quan với nhau.

3.14

tài sản mã hóa (cryptoasset)

tài sản số (3.21) được triển khai bằng cách sử dụng các kỹ thuật mật mã

CHÚ THÍCH 1: Các *hệ thống công nghệ sổ cái phân tán* (DLT) (3.35) có thể được sử dụng để quản lý hoặc chuyển giao các tài sản mã hóa.

3.15

tiền mã hóa (cryptocurrency)

tài sản mã hóa (3.14) được thiết kế để hoạt động như một phương tiện thanh toán hoặc trao đổi giá trị

CHÚ THÍCH 1: Tiền mã hóa liên quan đến việc sử dụng kiểm soát phi tập trung và *mật mã học* (3.16) để bảo mật *các giao dịch* (3.93), kiểm soát việc tạo ra các *tài sản* (3.1) bổ sung và xác minh việc chuyển giao tài sản trong *hệ thống công nghệ sổ cái phân tán (DLT)* (3.35).

3.16

mật mã học (cryptography)

ngành khoa học bao gồm các nguyên tắc, phương thức và các phương pháp biến đổi dữ liệu để che giấu nội dung ngữ nghĩa, ngăn chặn việc sử dụng trái phép hoặc ngăn chặn các sửa đổi không bị phát hiện

[NGUỒN: ISO 7498-2:1989, 3.3.20, đã sửa đổi — CHÚ THÍCH đối với mục đã bị loại bỏ.]

3.17

ứng dụng phi tập trung (decentralized application)

Dapp

ứng dụng chạy trên một *hệ thống phi tập trung* (3.20)

3.18

định danh phi tập trung (decentralized identifier – DID)

định danh (3.49) được cấp hoặc quản lý trong một *hệ thống phi tập trung* (3.20) và được thiết kế là duy nhất trong bối cảnh cụ thể

CHÚ THÍCH 1: Các định danh phi tập trung được sử dụng trong các hệ thống không phụ thuộc vào các bên có thẩm quyền đăng ký trung tâm.

3.19

danh tính phi tập trung (decentralized identity)

danh tính (3.50) được quản lý trong một *hệ thống phi tập trung* (3.20)

3.20

hệ thống phi tập trung (decentralized system)

hệ thống phân tán (3.24) trong đó quyền kiểm soát được phân bổ cho các cá nhân hoặc các tổ chức tham gia vào vận hành của hệ thống

CHÚ THÍCH 1: Trong một hệ thống phi tập trung, sự phân phối quyền kiểm soát giữa các cá nhân hoặc các tổ chức tham gia vào hệ thống được xác định bởi thiết kế của chính hệ thống đó.

3.21

tài sản số (digital asset)

tài sản (3.1) chỉ tồn tại dưới dạng số hoặc là biểu diễn số của một tài sản khác

3.22

chữ ký số (digital signature)

dữ liệu mà khi được gắn vào dữ liệu cần được ký, cho phép người dùng dữ liệu xác thực nguồn gốc và tính toàn vẹn của dữ liệu đó

[NGUỒN: ISO 14641:2018, 3.17, đã sửa đổi — “tài liệu kỹ thuật số” đã được thay thế bằng “dữ liệu cần được ký”.]

3.23

sổ cái phân tán (distributed ledger)

sổ cái (3.54) được chia sẻ trên một tập hợp các *nút công nghệ sổ cái phân tán (DLT)* (3.31) và được đồng bộ hóa giữa các nút DLT thông qua *cơ chế đồng thuận* (3.13)

CHÚ THÍCH 1: Sổ cái phân tán được thiết kế là *bất biến* (3.51), kháng can thiệp trái phép, phát lộ can thiệp trái phép và chỉ ghi thêm, chứa các *bản ghi sổ cái* (3.55) cuối cùng và xác quyết về *các giao dịch* (3.93) đã *được xác nhận* (3.9) và *xác thực* (3.97)

3.24

hệ thống phân tán (distributed system)

hệ thống trong đó các thành phần nằm trên các máy tính kết nối mạng giao tiếp và phối hợp hành động thông qua tương tác với nhau.

3.25

công nghệ sổ cái phân tán (distributed ledger technology – DLT)

công nghệ cho phép vận hành và sử dụng các *sổ cái phân tán* (3.23)

3.26

tài khoản công nghệ sổ cái phân tán (distributed ledger technology account - DLT account)

đại diện cho một *thực thể* (3.38) tham gia vào một *giao dịch* (3.93) trong một *hệ thống DLT* (3.35)

3.27

địa chỉ công nghệ sổ cái phân tán (distributed ledger technology - DLT address)

phần tử dữ liệu chỉ định nguồn khởi tạo hoặc đích đến của một *giao dịch* (3.93)

3.28

cầu nối công nghệ sổ cái phân tán (distributed ledger technology bridge - DLT bridge)

một *oracle DLT* (3.32) cho phép *tính liên tác* (3.52) giữa một *hệ thống DLT* (3.35) và các hệ thống khác triển khai các *sổ cái* (3.54)

CHÚ THÍCH 1: Các hệ thống khác cũng có thể là hệ thống DLT.

3.29

quản trị công nghệ sổ cái phân tán (distributed ledger technology governance - DLT governance)

hệ thống dùng để điều hành và kiểm soát một *hệ thống DLT* (3.35), bao gồm việc phân bổ các quyền ra quyết định trên *sổ cái* (3.68) và *ngoài sổ cái* (3.66), các khuyến khích, trách nhiệm và trách nhiệm giải trình

3.30

mạng công nghệ sổ cái phân tán (distributed ledger technology network - DLT network)

mạng lưới *các nút DLT* (3.31) tạo nên một *hệ thống DLT* (3.35)

3.31

nút công nghệ sổ cái phân tán (distributed ledger technology node - DLT node)

thiết bị hoặc quy trình tham gia vào một mạng và lưu trữ một bản sao hoàn chỉnh hoặc một phần của các *bản ghi sổ cái* (3.55)

3.32

oracle công nghệ sổ cái phân tán (distributed ledger technology oracle - DLT oracle)

dịch vụ cập nhật *sổ cái phân tán* (3.23) bằng cách sử dụng dữ liệu từ bên ngoài *hệ thống DLT* (3.35)

CHÚ THÍCH 1: Oracle DLT có thể được sử dụng bởi các hợp đồng thông minh (3.88) để truy cập dữ liệu từ các nguồn bên ngoài hệ thống DLT.

3.33

nền tảng công nghệ sổ cái phân tán (distributed ledger technology platform - DLT platform)

tập hợp các *thực thể* (3.38) xử lý, lưu trữ và truyền thông mà cùng nhau cung cấp các khả năng của *hệ thống DLT* (3.35) trên mỗi *nút DLT* (3.31)

3.34

giải pháp công nghệ sổ cái phân tán (distributed ledger technology solution - DLT solution)

giải pháp được xây dựng bằng cách sử dụng một *hệ thống DLT* (3.35) để hoàn thành các mục tiêu kinh doanh chung cho một nhóm *người dùng DLT* (3.36)

CHÚ THÍCH 1: Một giải pháp DLT bao gồm hệ thống DLT với các *nút DLT* (3.31) và mạng truyền thông của nó cộng với tất cả các *ứng dụng phi tập trung* (3.17) được kết nối với mỗi nút DLT, cùng với bất kỳ hệ thống phi DLT có liên quan nào được kết nối với hệ thống DLT.

3.35

hệ thống công nghệ sổ cái phân tán (distributed ledger technology system - DLT system)

hệ thống triển khai một *sổ cái phân tán* (3.23)

3.36

người dùng DLT (DLT user)

thực thể (3.38) sử dụng các dịch vụ do *hệ thống DLT* (3.35) cung cấp

3.37

chi tiêu kép (double spending)

sự cố (3.39) của *nền tảng công nghệ sổ cái phân tán (DLT)* (3.33) trong đó quyền kiểm soát một *tài sản mã hóa* (3.14) bị chuyển giao không chính xác nhiều hơn một lần

CHÚ THÍCH 1: Chi tiêu kép thường liên quan đến *tiền mã hóa* (3.15).

3.38

thực thể (entity)

người, tổ chức hoặc vật thể có thể được phân biệt trong bối cảnh cụ thể

CHÚ THÍCH 1: Một thực thể có thể là một người, một tổ chức, một thiết bị, một hệ thống con, một quy trình hoặc một nhóm các mục đó.

3.39

sự cố

failure

mất khả năng thực hiện theo yêu cầu

[NGUỒN: IEC 60050-192:2015, 192-03-01, đã sửa đổi — Các CHÚ THÍCH đối với mục đã được loại bỏ.]

3.40
khả năng chịu lỗi (fault tolerance)

khả năng của một đơn vị chức năng tiếp tục thực hiện một chức năng được yêu cầu khi có sự xuất hiện của các lỗi hoặc sai sót

[NGUỒN: ISO/IEC 2382:2015, 2123055, đã sửa đổi - Thuật ngữ được chấp nhận "khả năng phục hồi" đã được loại bỏ; các CHÚ THÍCH đối với mục đã được loại bỏ.]

3.41

tính hoàn kết (finality)

trạng thái của một *bản ghi sổ cái* (3.55) mà trong đó bản ghi đó đã trở nên không thể đảo ngược và không thể sửa đổi hoặc xóa

CHÚ THÍCH 1: Tính hoàn kết có thể mang tính xác suất.

3.42

khả hoán (fungible)

có khả năng thay thế lẫn nhau giữa các đơn vị riêng lẻ

CHÚ THÍCH 1: Các đơn vị riêng lẻ có thể là *tài sản số* (3.21), ví dụ: *token* (3.92).

3.43

token khả hoán (fungible token)

token (3.92) mà là *khả hoán* (3.42)

3.44

khối khởi tạo (genesis block)

khối đầu tiên (3.2) trong một *chuỗi khối* (3.6)

CHÚ THÍCH 1: Khối khởi tạo không có khối trước đó và dùng để khởi tạo chuỗi khối.

3.45

phân nhánh cứng (hard fork)

nền tảng công nghệ sổ cái phân tán (DLT) (3.33) trong đó các *bản ghi sổ cái* (3.55) hoặc các *khối* (3.2) mới được tạo ra bởi các *nút DLT* (3.31) sử dụng phiên bản mới của nền tảng DLT không được chấp nhận là hợp lệ bởi các nút DLT sử dụng phiên bản cũ của nền tảng DLT

CHÚ THÍCH 1: Nếu không được tất cả các nút DLT chấp nhận, một phân nhánh cứng có thể dẫn đến *phân tách sổ cái* (3.56).

3.46

hàm băm (hash function)

hàm băm mật mã (cryptographic hash function)

hàm ánh xạ các chuỗi bit có độ dài thay đổi (nhưng thường có giới hạn trên) vào các chuỗi bit có độ dài cố định, thỏa mãn các thuộc tính sau:

- đối với một đầu ra cho trước, không khả thi về mặt tính toán để tìm một đầu vào ánh xạ đến đầu ra này;
- đối với một đầu vào cho trước, không thể tính toán được để tìm một đầu vào thứ hai ánh xạ đến cùng một đầu ra;
- không thể tính toán được để tìm bất kỳ hai đầu vào khác nhau nào ánh xạ đến cùng một đầu ra.

CHÚ THÍCH 1: Khả năng tính toán phụ thuộc vào các yêu cầu bảo mật và môi trường cụ thể. Tham khảo ISO/IEC 10118-1:2016, Phụ lục C.

[NGUỒN: ISO/IEC 10118-1:2016, 3.4, đã sửa đổi — Thuật ngữ ưu tiên “hàm băm mật mã” đã được thêm vào; một mục thứ ba trong danh sách đã được thêm vào.]

3.47

liên kết băm (hash link)

liên kết mật mã (cryptographic link)

Tham chiếu đến dữ liệu, được tạo ra bằng cách áp dụng một *hàm băm* (3.46) lên dữ liệu đó.

CHÚ THÍCH 1: Một liên kết mật mã được sử dụng trong *tiêu đề khối* (3.4) để tham chiếu đến *khối* (3.2) trước đó nhằm tạo ra một chuỗi tuần tự, chỉ ghi thêm để hình thành nên một *chuỗi khối* (3.6).

CHÚ THÍCH 2: Một liên kết mật mã cho phép phát hiện những thay đổi trong dữ liệu mà nó tham chiếu đến.

3.48

giá trị băm (hash value)

chuỗi bit là đầu ra của một *hàm băm* (3.46)

[NGUỒN: ISO/IEC 27037:2012, 3.11]

3.49

định danh (identifier)

biểu diễn của một *danh tính* (3.50)

3.50

danh tính (identity)

tập hợp của các thuộc tính mà để phân biệt một *thực thể* (3.38) trong một ngữ cảnh

3.51

tính bất biến (immutability)

tính chất của một *sổ cái phân tán* (3.23) trong đó các *bản ghi sổ cái* (3.55) không thể bị sửa đổi hoặc xóa bỏ sau khi được thêm vào sổ cái phân tán đó

CHÚ THÍCH 1: Khi thích hợp, tính bất biến cũng giả định việc giữ nguyên thứ tự của các bản ghi sổ cái và các liên kết giữa các bản ghi sổ cái.

CHÚ THÍCH 2: Tính bất biến có thể xuất hiện từ sự tương tác giữa các nút riêng lẻ trong một *hệ thống phi tập trung* (3.20), ngay cả khi các bản ghi sổ cái trong bất kỳ *nút DLT* (3.31) nhất định nào thay đổi

3.52

tính liên tác (interoperability)

khả năng của hai hoặc nhiều hệ thống hoặc ứng dụng trao đổi thông tin và sử dụng lẫn nhau thông tin đã được trao đổi

CHÚ THÍCH 1: Tính liên tác có thể khả thi giữa các ứng dụng trên một *hệ thống công nghệ sổ cái phân tán (DLT)* (3.35) duy nhất, giữa các hệ thống DLT, hoặc giữa một hệ thống DLT và các hệ thống bên ngoài.

[NGUỒN: ISO/IEC 17788:2014, 3.1.5, đã sửa đổi — CHÚ THÍCH 1 đã được bổ sung.]

3.53

nút lá (leaf node)

nút (3.61) không có nút con

3.54

sổ cái (ledger)

kho lưu trữ thông tin mà lưu giữ các *bản ghi* (3.81) về các *giao dịch* (3.93), được dự định là cuối cùng, xác quyết và *bất biến* (3.51).

3.55

bản ghi sổ cái (ledger record)

bản ghi (3.81) chứa các *bản ghi giao dịch* (3.95), các *giá trị băm* (3.48) của các bản ghi giao dịch, hoặc các tham chiếu đến các bản ghi giao dịch được ghi *trên sổ cái* (3.68)

CHÚ THÍCH 1: Một tham chiếu có thể được triển khai dưới dạng một *liên kết mật mã* (3.47).

3.56

phân tách sổ cái (ledger split)

phân nhánh (fork)

việc tạo ra hai hoặc nhiều phiên bản khác nhau của một *sổ cái phân tán* (3.23) bắt nguồn từ một điểm khởi đầu chung với một lịch sử duy nhất

3.57

gốc Merkle (Merkle root)

nút gốc (3.83) của *cây Merkle* (3.58)

3.58

cây Merkle (Merkle tree)

cấu trúc dữ liệu dạng cây trong đó mỗi *nút lá* (3.53) được gắn nhãn bằng *giá trị băm* (3.48) của một phần tử dữ liệu và mỗi nút không phải nút lá được gắn nhãn bằng giá trị băm của các nhãn thuộc các *nút* (3.61) con của nó

3.59

thợ đào (miner)

nút công nghệ sổ cái phân tán (DLT) (3.31) tham gia vào hoạt động *khai thác* (3.60)

3.60

khai thác (mining)

hoạt động trong một số *cơ chế đồng thuận* (3.13) nhằm tạo ra và *xác thực* (3.98) các *khối* (3.2) hoặc *xác thực các bản ghi sổ cái* (3.55)

CHÚ THÍCH 1: Việc tham gia khai thác thường được khuyến khích bằng *phần thưởng khối* (3.5) *và phí giao dịch* (3.94).

3.61

nút (node)

thành phần cơ bản từ đó một cấu trúc dữ liệu được xây dựng

3.62

nonce

một số hoặc chuỗi bit được sử dụng một lần trong một tập hợp các phép toán mật mã

CHÚ THÍCH 1: Một nonce thường là ngẫu nhiên hoặc giả ngẫu nhiên. Nó thường được sử dụng để chống lại các cuộc tấn công phát lại, trong đó một thông điệp bị kẻ xấu chặn thu và gửi lại. Trong một số *hệ thống chuỗi khối (3.7),* nó được sử dụng để điều chỉnh việc *khai thác* (3.60) trong quá trình tạo một *khối* (3.2) mới và được lưu trữ trong *tiêu đề khối* (3.4).

3.63

phi khả hoán (non-fungible)

không có khả năng thay thế lẫn nhau giữa các đơn vị riêng lẻ

CHÚ THÍCH 1: Các đơn vị riêng lẻ có thể là *tài sản số* (3.21), ví dụ: *token* (3.92).

3.64

token phi khả hoán (non-fungible token)

NFT

token (3.92) mà là *phi khả hoán* (3.63)

3.65

ngoài chuỗi (off-chain)

liên quan đến một *hệ thống chuỗi khối* (3.7) nhưng được đặt, thực hiện hoặc vận hành bên ngoài hệ thống blockchain đó.

3.66

ngoài sổ cái (off-ledger)

liên quan đến một *hệ thống công nghệ sổ cái phân tán (DLT)* (3.35) nhưng được đặt, thực hiện hoặc vận hành bên ngoài hệ thống DLT đó

3.67

trên chuỗi (on-chain)

được đặt, thực hiện hoặc vận hành bên trong một *hệ thống chuỗi khối* (3.7)

3.68

trên sổ cái (on-ledger)

được đặt, thực hiện hoặc chạy bên trong một *hệ thống công nghệ sổ cái phân tán (DLT)* (3.35)

3.69

khối orphan (orphan block)

khối (3.2) đã *được xác nhận* (3.9) trước đó nhưng hiện không còn được xác nhận nữa

CHÚ THÍCH 1: Một khối có thể trở thành khối orphan vì nhiều lý do, ví dụ, do sự cạnh tranh giữa các *thợ đào* (3.59) trong quá trình đạt được *sự đồng thuận* (3.12).

3.70

ngang hàng (peer-to-peer)

liên quan đến, sử dụng hoặc là một mạng lưới gồm các bên ngang hàng bình đẳng, chia sẻ thông tin và tài nguyên trực tiếp với nhau mà không dựa vào một *thực thể* (3.38) trung tâm

3.71

được cấp phép (permissioned)

yêu cầu sự cho phép để thực hiện một hoạt động hoặc các hoạt động cụ thể

3.72

hệ thống sổ cái phân tán được cấp phép (permissioned distributed ledger system)

hệ thống công nghệ sổ cái phân tán được cấp phép (permissioned distributed ledger technology system - permissioned DLT system)

hệ thống DLT (3.35) trong đó các cấp phép được yêu cầu

3.73

không cần cấp phép (permissionless)

không yêu cầu sự cho phép để thực hiện bất kỳ hoạt động cụ thể nào

3.74

hệ thống DLT không cần cấp phép (permissionless DLT system)

hệ thống sổ cái phân tán không cần cấp phép (permissionless distributed ledger system)

hệ thống công nghệ sổ cái phân tán không cần cấp phép (permissionless distributed ledger technology system)

hệ thống DLT (3.35) là *không cần cấp phép* (3.73)

3.75

hệ thống DLT riêng tư (private DLT system)

hệ thống sổ cái phân tán riêng tư (private distributed ledger system)

hệ thống công nghệ sổ cái phân tán riêng tư (private distributed ledger technology system)

hệ thống DLT (3.35) chỉ cho phép truy cập sử dụng bởi một nhóm *người dùng DLT* (3.36) hạn chế

CHÚ THÍCH 1: Các nhóm phân loại công khai và riêng tư áp dụng cho người dùng DLT, và các nhóm phân loại *được cấp phép* (3.71) và *không cần cấp phép* (3.73) áp dụng cho người dùng DLT và các *thực thể* (3.38) quản lý hoặc vận hành hệ thống DLT.

3.76

khóa riêng (private key)

khóa của cặp khóa bất đối xứng của một *thực thể* (3.38) được giữ bí mật và chỉ nên được sử dụng bởi thực thể đó

[NGUỒN: ISO/IEC 9798-1:2010, 3.22]

3.77

cắt tỉa (prune)

tạo ra một bản sao nhỏ hơn của *sổ cái phân tán* (3.23) bằng cách xóa tất cả thông tin đáp ứng các tiêu chí cụ thể, trong khi vẫn đảm bảo rằng thông tin có thể được khôi phục với tính toàn vẹn nếu cần

3.78

hệ thống DLT công khai (public DLT system)

hệ thống sổ cái phân tán công khai (public distributed ledger system)

hệ thống công nghệ sổ cái phân tán công khai (public distributed ledger technology system)

hệ thống DLT (3.35) mà công chúng có thể truy cập để sử dụng

3.79

khóa công khai (public key)

khóa của cặp khóa bất đối xứng của một *thực thể (*3.38) có thể được công khai

[NGUỒN: ISO/IEC 9798-1:2010, 3.25]

3.80

mật mã khóa công khai (public-key cryptography)

mật mã học (3.16) trong đó *khóa công khai* (3.79) và *khóa riêng* (3.76) tương ứng được sử dụng để mã hóa và giải mã, hoặc được sử dụng để xác minh chữ ký số và ký số, một cách tương ứng

3.81

bản ghi (record)

thông tin được tạo hoặc nhận được và được lưu giữ như một bằng chứng và như một *tài sản* (3.1) bởi một tổ chức theo nghĩa vụ pháp lý hoặc trong quá trình kinh doanh

CHÚ THÍCH 1: Thuật ngữ này áp dụng cho thông tin ở bất kỳ phương tiện, dạng hoặc định dạng nào.

[NGUỒN: ISO 30300:2020, 3.2.10 — Các CHÚ THÍCH 1 và 2 đối với mục đã được loại bỏ và một CHÚ THÍCH 1 mới đối với mục đã được thêm vào]

3.82

hệ thống phần thưởng (reward system)

cơ chế khuyến khích (incentive mechanism)

phương pháp của việc đưa ra phần thưởng cho một số hoạt động liên quan đến việc vận hành của một *hệ thống công nghệ sổ cái phân tán (DLT)* (3.35)

CHÚ THÍCH 1: Một ví dụ của một phần thưởng là một *phần thưởng khối* (3.5).

3.83

nút gốc (root node)

nút (3.61) không có nút cha

3.84

token chứng khoán (security token)

token (3.92) với các đặc tính cụ thể mà đáp ứng định nghĩa về công cụ tài chính hoặc công cụ đầu tư khác theo luật pháp hiện hành trong khu vực tài phán có liên quan

3.85

danh tính tự chủ (self-sovereign identity – SSI)

danh tính (3.50) mà được kiểm soát duy nhất bởi *thực thể* (3.38) mà danh tính phân biệt

CHÚ THÍCH 1: Một danh tính tự chủ nói chung được sử dụng để bảo vệ quyền tự trị của một thực thể và sự kiểm soát đối với các danh tính của nó.

CHÚ THÍCH 2: Sự kiểm soát đối với danh tính có toàn quyền của một thực thể có thể được ủy quyền trong một số trường hợp.

3.86

sổ cái chia sẻ (shared ledger)

sổ cái phân tán (3.23) trong đó nội dung các *bản ghi sổ cái* (3.55) có thể truy cập được bởi nhiều *thực thể* (3.38)

3.87

chuỗi bên (sidechain)

hệ thống chuỗi khối (3.7) có *tính liên tác* (3.52) với một hệ thống chuỗi khối liên kết riêng biệt để thực hiện một chức năng cụ thể liên quan đến hệ thống chuỗi khối liên kết

CHÚ THÍCH 1: Theo quy ước, chuỗi gốc thường được gọi là "chuỗi chính", trong khi bất kỳ *chuỗi khối* (3.6) bổ sung nào cho phép *người dùng công nghệ sổ cái phân tán (DLT)* (3.36) giao dịch trên chuỗi chính được gọi là các "chuỗi bên"

3.88

hợp đồng thông minh (smart contract)

chương trình máy tính được lưu trữ trong *hệ thống công nghệ sổ cái phân tán (DLT)* (3.35) trong đó kết quả của bất kỳ lần thực thi nào của chương trình đều được ghi lại trên *sổ cái phân tán* (3.23)

CHÚ THÍCH 1: Một hợp đồng thông minh có thể đại diện cho các điều khoản trong một hợp đồng pháp lý và tạo ra nghĩa vụ có hiệu lực thi hành về mặt pháp lý theo quy định pháp luật của một khu vực tài phán áp dụng.

3.89

phân nhánh mềm (soft fork)

nền tảng *công nghệ sổ cái phân tán (DLT)* (3.33) không phải là *phân nhánh cứng* (3.45) và trong đó một số *bản ghi* (3.81) hoặc *khối* (3.2) được tạo bởi các *nút DLT* (3.31) sử dụng phiên bản cũ của nền tảng DLT không được các nút DLT sử dụng phiên bản mới của nền tảng DLT chấp nhận là hợp lệ

3.90

chuỗi con (subchain)

chuỗi được phân tách logic có thể tạo thành một phần của một *hệ thống chuỗi khối* (3.7)

CHÚ THÍCH 1: Một chuỗi con cho phép cô lập dữ liệu và bảo mật thông tin

3.91

dấu thời gian (timestamp)

tham số biến thiên theo thời gian biểu thị một thời điểm so với một mốc thời gian tham chiếu chung

[NGUỒN: ISO/IEC 18014-1:2008, 3.12, đã sửa đổi - Khoảng trống giữa "time" và "stamp" đã được loại bỏ.]

3.92

token

tài sản (3.1) đại diện cho một tập hợp các quyền lợi

3.93

giao dịch (transaction)

đơn vị nhỏ nhất của một quy trình công việc bao gồm một hoặc nhiều chuỗi hành động cần thiết để tạo ra một kết quả tuân thủ các quy tắc quản lý

3.94

phí giao dịch (transaction fee)

phí được trả cho *thợ đào* (3.59) hoặc *người xác thực* (3.99) để xử lý một *giao dịch* (3.93) trong một *hệ thống công nghệ sổ cái phân tán (DLT)* (3.35)

3.95

bản ghi giao dịch (transaction record)

bản ghi (3.81) ghi lại một *giao dịch* (3.93) thuộc bất kỳ loại nào

CHÚ THÍCH 1: Các bản ghi giao dịch có thể được bao gồm trong hoặc được đề cập đến trong *bản ghi sổ cái* (3.55).

CHÚ THÍCH 2: Các bản ghi giao dịch có thể bao gồm kết quả của một *giao dịch* (3.93)

3.96

token tiện ích (utility token)

token (3.92) mà chủ sở hữu của nó có thể sử dụng để nhận quyền tiếp cập vào hàng hóa hoặc dịch vụ

CHÚ THÍCH 1: Token tiện ích thường chỉ được chấp nhận bởi nhà phát hành token đó.

3.97

được xác thực (validated)

trạng thái của một *thực thể* (3.38) khi các điều kiện bắt buộc về tính toàn vẹn của nó đã được kiểm tra và đáp ứng

CHÚ THÍCH 1: Ví dụ, trong *hệ thống công nghệ sổ cái phân tán* (DLT) (3.35), một *giao dịch* (3.93), *bản ghi sổ cái* (3.55) hoặc *khối* (3.2) có thể được xác thực.

3.98

xác thực (validation)

chức năng mà một *giao dịch* (3.93), *bản ghi sổ cái* (3.55) hoặc *khối* (3.2) *được xác thực* (3.97)

3.99

người xác thực (validator)

thực thể (3.38) trong *hệ thống công nghệ sổ cái phân tán* (DLT) (3.35) tham gia vào *xác thực* (3.98)

CHÚ THÍCH 1: Trong một số hệ thống DLT, *nút DLT* (3.31) có vai trò người xác thực có thể ký số vào một *bản ghi sổ cái* (3.55) hoặc *khối* (3.2).

3.100

ví (wallet)

ứng dụng hoặc cơ chế được sử dụng để tạo, quản lý, lưu trữ hoặc sử dụng *khóa riêng* (3.76) và *khóa công khai* (3.79) hoặc các *tài sản số* (3.21) khác

CHÚ THÍCH 1: Ví có thể được triển khai bằng phần mềm, triển khai dưới dạng một mô đun phần cứng, hoặc được ghi trên các phương tiện phi kỹ thuật số như giấy hoặc kim loại.

CHÚ THÍCH 2: Các tài sản số được lưu trữ trong các ví có thể bao gồm, ví dụ, các *token phi khả hoán* (3.64).

Thư mục tài liệu tham khảo

[1] ISO/IEC 2382:2015, Information technology — Vocabulary

[2] ISO 7498-2:1989, Information processing systems — Open Systems Interconnection — Basic Reference Model — Part 2: Security Architecture

[3] ISO/IEC 9798-1:2010, Information technology — Security techniques — Entity authentication — Part 1: General

[4] ISO 14641:2018, Electronic document management — Design and operation of an information system for the preservation of electronic documents — Specifications

[5] ISO/IEC 17788:2014, Information technology — Cloud computing — Overview and vocabulary

[6] ISO/IEC 18014-1:2008, Information technology — Security techniques — Time-stamping services — Part 1: Framework

[7] ISO 19299:2020, Electronic fee collection — Security framework

[8] ISO/IEC 27037:2012, Information technology — Security techniques — Guidelines for identification, collection, acquisition and preservation of digital evidence

[9] ISO 30300:2020, Information and documentation — Records management — Core concepts and vocabulary

[10] IEC 60050-192:2015, International Electrotechnical Vocabulary (IEV) — Part 192: Dependability

[11] ISO/IEC 10118-1:2016, Information technology — Security techniques — Hash-functions — Part 1: General