TCVN | **TIÊU CHUẨN QUỐC GIA**

DỰ THẢO

TCVN XXXXX:2026
ISO/IEC 23257:2022

Xuất bản lần 1

CÔNG NGHỆ BLOCKCHAIN VÀ SỔ CÁI PHÂN TÁN - KIẾN TRÚC THAM CHIẾU

Blockchain and distributed ledger technologies - Reference architecture

Technologies des chaînes de blocs et technologies de registre distribué - Architecture de référence

HÀ NỘI – 2026

MỤC LỤC

Lời nói đầu

TCVN XXXXX-:2026 hoàn toàn tương đương với ISO/IEC 23257:2022.

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

Các bản ghi giao dịch, được lập trên cơ sở những điều kiện đã được thỏa thuận, tạo thành cơ sở cho hoạt động trao đổi tài sản giữa các bên. Các doanh nghiệp và chính phủ đã vận hành dựa trên nền tảng này trong nhiều thế kỷ. Mặc dù sổ cái vật lý từng được sử dụng, hiện nay chúng phần lớn đã được thay thế bằng công nghệ hiện đại. Tuy nhiên, trong các phương thức tiếp cận truyền thống, một sổ cái phải được kiểm soát tập trung bởi một hoặc một số ít bên, và các bên có lợi ích liên quan khác phải dựa vào họ với tư cách là tác nhân ủy quyền để thực hiện thay đổi đối với các sổ cái đó.

Một đặc tính quan trọng của sổ cái là tính có thể xác minh. Điều này có nghĩa là các bên có thể xác minh rằng tập hợp các giao dịch trong sổ cái là đầy đủ và chính xác. Nhờ đó, các bên này có thể xác định các bất thường trong giao dịch - ví dụ, xác minh rằng tài sản kỹ thuật số của các bên tham gia được hạch toán chính xác trong một sổ cái tài chính. Hiện nay, có thể đạt được một sổ cái có tính xác minh theo phương thức tập trung bằng cách thiết lập một số giả định tin cậy nhất định. Tuy nhiên, tính có thể xác minh cũng có thể được đạt được bằng cách phân tán lưu trữ và phi tập trung hóa việc kiểm soát sổ cái, với mức tin cậy tối thiểu đặt vào bất kỳ một bên nào.

Bằng cách duy trì sổ cái trong một mạng phân tán, các hệ thống Công nghệ sổ cái phân tán (DLT), bao gồm cả các hệ thống chuỗi khối (blockchain), cho phép một phạm vi rộng hơn nhiều các bên có được góc nhìn chung về sổ cái và thực hiện các thay đổi của riêng mình đối với sổ cái đó.

Một phổ rộng các giải pháp kinh doanh dựa trên DLT là khả thi. Tiêu chuẩn này trình bày một kiến trúc tham chiếu cho các giải pháp dựa trên DLT nêu trên. Tiêu chuẩn bắt đầu bằng các định nghĩa và khái niệm về chuỗi khối và DLT, bao gồm tổ chức hệ thống, bản chất truy cập, loại hình đồng thuận, và vai trò cùng trách nhiệm của các bên tham gia. Do kiến trúc tham chiếu phải đáp ứng được nhiều trường hợp sử dụng khả dĩ khác nhau, tiêu chuẩn này đề cập đến nhiều lĩnh vực kinh doanh và các trường hợp sử dụng tương ứng ở mức độ khái quát. Về mặt lịch sử, sổ cái đã tạo thuận lợi cho hoạt động trao đổi tài sản, nhưng các giải pháp DLT còn có thể được sử dụng rộng rãi hơn cho mục đích báo cáo, kiểm toán và điều phối. Cuối cùng, tiêu chuẩn này giới thiệu đến người đọc các lớp khác nhau của kiến trúc tham chiếu dành cho hệ thống DLT cùng với các thành phần chức năng trong từng lớp.

Tiêu chuẩn này có liên quan đến, trong số các đối tượng khác, các nhà nghiên cứu học thuật, kiến trúc sư hệ thống, khách hàng, người dùng, nhà phát triển, cơ quan quản lý, kiểm toán viên và các tổ chức xây dựng tiêu chuẩn.

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

CÔNG NGHỆ BLOCKCHAIN VÀ SỔ CÁI PHÂN TÁN - KIẾN TRÚC THAM CHIẾU

Blockchain and distributed ledger technologies - Reference architecture

Technologies des chaînes de blocs et technologies de registre distribué - Architecture de référence

1 Phạm vi áp dụng

Tiêu chuẩn này quy định kiến trúc tham chiếu cho các hệ thống Công nghệ sổ cái phân tán (Distributed Ledger Technology - DLT), bao gồm cả các hệ thống chuỗi khối (blockchain). Kiến trúc tham chiếu đề cập đến các khái niệm, các khía cạnh xuyên suốt, các cân nhắc kiến trúc và các góc nhìn kiến trúc, bao gồm các thành phần chức năng, các vai trò, các hoạt động và các mối quan hệ của chúng đối với chuỗi khối và DLT.

2 Tài liệu viện dẫn

Trong tiêu chuẩn này các tài liệu dưới đây được viện dẫn trong văn bản theo cách thức mà một phần hoặc toàn bộ nội dung của chúng tạo thành các yêu cầu của tiêu chuẩn. Đối với tài liệu viện dẫn có ghi năm công bố, chỉ áp dụng phiên bản được nêu. Đối với tài liệu viện dẫn không ghi năm công bố, áp dụng phiên bản mới nhất của tài liệu được viện dẫn (bao gồm mọi sửa đổi).

ISO 22739, Công nghệ chuỗi khối và Công nghệ sổ cái phân tán - Từ vựng

ISO/IEC 24760-1, Công nghệ thông tin - An toàn thông tin và quyền riêng tư - Khung quản lý định danh - Phần 1: Thuật ngữ và khái niệm

3 Thuật ngữ và định nghĩa

Tiêu chuẩn này sử dụng các thuật ngữ và định nghĩa trong ISO 22739, ISO/IEC 24760-1 và các định nghĩa sau đây của ISO và IEC.

3.1
hoạt động (activity)
sự theo đuổi được chỉ định hoặc tập hợp các nhiệm vụ
[NGUỒN: ISO/IEC 17789:2014, 3.2.1]

3.2
kiến trúc (architecture)
các khái niệm hoặc thuộc tính cơ bản của một hệ thống trong môi trường của nó, được thể hiện trong các phần tử, các quan hệ của nó và các nguyên tắc thiết kế và tiến hóa của nó.
[NGUỒN: ISO/IEC/IEEE 42010:2011, 3.2]

3.3
tính liên tác hành vi (behavioural interoperability)
tính liên tác sao cho kết quả thực tế của quá trình trao đổi đạt được kết quả mong đợi
[NGUỒN: ISO/IEC 19941:2017, 3.1.6]

3.4
lưu trữ dữ liệu (data archiving)

quá trình bảo toàn kỹ thuật số thực hiện di chuyển dữ liệu vào dạng lưu trữ được quản lý để lưu trữ dài hạn.
[NGUỒN: ISO 5127:2017, 3.1.11.19]

3.5
luồng dữ liệu (data flow)
trình tự trong đó việc truyền tải, sử dụng và biến đổi dữ liệu được thực hiện trong quá trình thực thi một chương trình máy tính.
[NGUỒN: ISO/IEC/IEEE 24765:2017, 3.1006]

3.6
gián đoạn (disruption)
sự cố, dù được dự liệu trước (ví dụ: bão cuồng phong) hay không được dự liệu trước (ví dụ: mất điện/ngừng điện, động đất hoặc tấn công vào hệ thống/hạ tầng công nghệ thông tin và truyền thông), gây gián đoạn diễn tiến bình thường của các hoạt động tại địa điểm của tổ chức
[NGUỒN: ISO/IEC 27031:2011, 3.6]

3.7
quản trị Công nghệ sổ cái phân tán (distributed ledger technology governance – DLT governance)
hệ thống điều hành và kiểm soát một hệ thống công nghệ sổ cái phân tán, bao gồm việc phân bổ các quyền quyết định trên sổ cái và ngoài sổ cái, các yếu tố khuyến khích, trách nhiệm và trách nhiệm giải trình.

3.8
tính hoàn kết (finality)
thuộc tính của sổ cái đảm bảo rằng các giao dịch trong các bản ghi sổ cái đã được xác nhận là không thể đảo ngược và không thể bị sửa đổi hoặc xóa.

3.9
thành phần chức năng (functional component)
khối xây dựng chức năng cần thiết để thực hiện một hoạt động, được hỗ trợ bởi một triển khai.
[NGUỒN: ISO/IEC 17789:2014, 3.2.3]

3.10
tính khả hoán (fungible)
có khả năng thay thế lẫn nhau giữa các đơn vị riêng lẻ.
CHÚ THÍCH: Các đơn vị riêng lẻ có thể là tài sản số, ví dụ: token.

3.11
quản trị (governance)
hệ thống điều hành và kiểm soát.
[NGUỒN: ISO/IEC 38500:2015, 2.8]

3.12
sự cố (incident)
sự kiện, tập hợp sự kiện, trạng thái hoặc tình huống bất thường hoặc không lường trước xảy ra tại bất kỳ thời điểm nào trong vòng đời của một dự án, sản phẩm, dịch vụ hoặc hệ thống.
[NGUỒN: ISO/IEC/IEEE 24748-1:2018, 3.22]

3.13

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.
[NGUỒN: ISO/IEC 17788:2014, 3.1.5]

3.14
bên (party)
thể nhân hoặc pháp nhân, dù đã hay chưa được thành lập theo pháp luật, hoặc một nhóm gồm thể nhân hoặc pháp nhân.
[NGUỒN: ISO/IEC 17789:2014, 7.2.3]

3.15
thông tin nhận dạng cá nhân (personally identifiable information – PII)
thông tin mà:
(a) có thể được dùng để xác lập liên kết giữa thông tin đó và thể nhân mà thông tin đó liên quan; hoặc
(b) đang hoặc có thể được liên kết trực tiếp hay gián tiếp với một thể nhân.
CHÚ THÍCH 1: Thể nhân trong định nghĩa này là chủ thể PII. Để xác định xem chủ thể PII có thể nhận dạng được hay không, cần tính đến tất cả các phương tiện có thể được sử dụng một cách hợp lý bởi bên liên quan về quyền riêng tư đang nắm giữ dữ liệu, hoặc bất kỳ bên nào khác, để xác lập mối liên hệ giữa tập hợp PII và thể nhân.
[NGUỒN: ISO/IEC 29100:2011/Amd 1:2018, 2.9]

3.16
tính liên tác chính sách (policy interoperability)
tính liên tác trong khi tuân thủ các khuôn khổ pháp lý, tổ chức và chính sách áp dụng cho các hệ thống tham gia.
[NGUỒN: ISO/IEC 19941:2017, 3.1.7]

3.17
nguồn gốc (provenance)
thông tin ghi lại nguồn gốc hoặc xuất xứ của một tài sản, bất kỳ thay đổi nào đã diễn ra kể từ khi tài sản đó được khởi tạo, và bên đã nắm giữ tài sản đó kể từ khi tài sản đó được khởi tạo.
[NGUỒN: ISO/IEC 27050-1:2019, 3.19, sửa đổi – thay thế "thông tin lưu trữ điện tử" bằng "tài sản".]

3.18
khả năng phục hồi (resilience)
khả năng của một hệ thống duy trì các chức năng và cấu trúc của mình trước những thay đổi bên trong và bên ngoài, và suy giảm có kiểm soát khi cần thiết.

[NGUỒN: ISO 37101:2016, 3.33, sửa đổi – Định nghĩa được thay thế bằng văn bản trong CHÚ THÍCH 3, các CHÚ THÍCH khác bị xóa.]

3.19
vai trò (role)
tập hợp các hoạt động phục vụ một mục đích chung.
[NGUỒN: ISO/IEC 17789:2014, 3.2.7]

3.20
tính liên tác ngữ nghĩa dữ liệu (semantic data interoperability)

dữ liệu ngữ nghĩa
tính liên tác sao cho ý nghĩa của mô hình dữ liệu trong bối cảnh của một lĩnh vực chủ đề được hiểu bởi các hệ thống tham gia.
[NGUỒN: ISO/IEC 19941:2017, 3.1.5]

3.21
vai trò con (sub-role)
tập hợp con các hoạt động của một vai trò đã định.
[NGUỒN: ISO/IEC 17789:2014, 3.2.9]

3.22
tính liên tác cú pháp (syntactic interoperability)
tính liên tác sao cho các định dạng của thông tin được trao đổi có thể được hiểu bởi các hệ thống tham gia.

[NGUỒN: ISO/IEC 19941:2017, 3.1.4]

3.23
tính liên tác vận chuyển (transport interoperability)
tính liên tác trong đó việc trao đổi thông tin sử dụng một hạ tầng truyền thông đã được thiết lập giữa các hệ thống tham gia.
[NGUỒN: ISO/IEC 19941:2017, 3.1.3]

3.24
hợp đồng thông minh (smart contract)
chương trình máy tính được lưu trữ trong một hệ thống DLT, trong đó kết quả của bất kỳ lần thực thi nào của chương trình được ghi lại trên sổ cái phân tán.

CHÚ THÍCH 1: Một hợp đồng thông minh có thể đại diện các điều khoản trong một hợp đồng pháp lý và tạo ra nghĩa vụ có hiệu lực thi hành theo quy định pháp luật của khu vực tài phán áp dụng.
[NGUỒN: ISO 22739:2020, 3.72]

3.25
sự đồng thuận (consensus)
sự thỏa thuận giữa các nút DLT rằng (1) một giao dịch đã được xác thực và 2) sổ cái phân tán chứa một tập hợp nhất quán và có trình tự của các 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 về sự đồng thuận khác nhau giữa các thiết kế DLT và đây là một đặc trưng phân biệt giữa các thiết kế.
[NGUỒN: ISO 22739:2020, 3.11]

4 Ký hiệu và các thuật ngữ viết tắt

AMQP	Advanced Message Queuing Protocol	Giao thức hàng đợi thông điệp nâng cao

API	Application Programming Interface	Giao diện lập trình ứng dụng
CAdES	Cryptographic Message Syntax (CMS) Advanced Electronic Signature	Chữ ký điện tử nâng cao theo cú pháp thông điệp mật mã (CMS)
DLT	Distributed Ledger Technology	Công nghệ sổ cái phân tán
DNS	Domain Name System	Hệ thống tên miền
EDI	Electronic Data Interchange	Trao đổi dữ liệu điện tử
FBA	Federated Byzantine Agreement	Thỏa thuận Byzantine liên kết
GDPR	General Data Protection Regulation	Quy định chung về bảo vệ dữ liệu (GDPR)
HTTP	Hyper Text Transfer Protocol	Giao thức truyền tải siêu văn bản
HTTPS	Hypertext Transfer Protocol Secure over Socket Layer	Giao thức truyền tải siêu văn bản bảo mật qua lớp Socket
ICT	Information and Communication Technology	Công nghệ thông tin và truyền thông
IDE	Integrated Development Environment	Môi trường phát triển tích hợp
IoT	Internet of things	Internet vạn vật
IPFS	InterPlanetary File System	Hệ thống tệp liên hành tinh
JSON	JavaScript Object Notation	Ký hiệu đối tượng JavaScript
MQTT	Message Queuing Telemetry Transport	Giao thức MQTT
P2P	Peer-to-peer	Ngang hàng

PBFT	Practical Byzantine Fault Tolerance	Khả năng chịu lỗi Byzantine thực tiễn
PKI	Public Key Infrastructure	Hạ tầng khóa công khai
RA	Reference Architecture	Kiến trúc tham chiếu
XML	eXtensible Markup Language	Ngôn ngữ đánh dấu mở rộng

5 Các khái niệm

5.1 Các hệ thống DLT và blockchain

5.1.1 Tổng quan

Để hiểu được các hệ thống chuỗi khối và hệ thống Công nghệ sổ cái phân tán cần phải đưa ra mô tả về các khái niệm thiết yếu liên quan đến các hệ thống này và các loại công nghệ sổ cái phân tán hiện có.

Sổ cái là một khái niệm được thiết lập từ lâu trong kinh doanh và công nghệ. Khi áp dụng cho các hệ thống ICT, sổ cái là một kho thông tin lưu giữ các bản ghi giao dịch mang tính "cuối cùng" và "xác quyết". Ban đầu, sổ cái chủ yếu được áp dụng cho giao dịch tài chính và thực hành kế toán. Tuy nhiên, sổ cái có thể được dùng để ghi lại hầu như mọi loại giao dịch, ví dụ như việc vận chuyển và chuyển giao các đối tượng vật lý.

Một đặc tính hết sức đáng có của sổ cái là tính kháng can thiệp trái phép, tức là các bản ghi giao dịch, một khi đã được ghi vào sổ cái, rất khó bị sửa đổi do cơ chế thiết kế; và chúng không thể bị sửa đổi mà không để lại bằng chứng rõ ràng khi kiểm tra, cho dù việc sửa đổi đó là cố ý hay vô ý, có hại hay vô hại.

Thuật ngữ "kháng can thiệp trái phép" phù hợp hơn "kháng can thiệp tuyệt đối", vì việc ngăn chặn mọi hình thức can thiệp trái phép là vô cùng khó khăn. Tương tự, mặc dù tính bất biến là một mục tiêu thiết kế của các hệ thống DLT, song đặc tính này không thể được bảo đảm một cách tuyệt đối. Thuật ngữ "phát lộ can thiệp trái phép" có thể được áp dụng cho một hệ thống có đặc tính mong muốn là làm cho mọi thay đổi trái phép được hiện lộ rõ ràng.

Sổ cái phân tán có các mục nhập của nó được lưu trữ phân tán trên một chuỗi các nút trong một mạng, thay vì được lưu trữ tại một vị trí duy nhất. Ví dụ, các nút khác nhau trong mạng có thể được sở hữu và được tương tác bởi các bên khác nhau, trong đó mỗi bên có phiên bản bản ghi riêng chỉ bao gồm các giao dịch mà bên đó tham gia. Các hệ thống DLT được thiết kế để triển khai các sổ cái phân tán - đây là một thách thức đáng kể do yêu cầu phải đạt được sự thống nhất và duy trì tính nhất quán của các bản ghi giao dịch trong sổ cái phân tán.

Với DLT, sự đồng thuận đảm bảo rằng mọi phiên bản được nhân bản của một giao dịch là đồng nhất trên tất cả các nút nơi giao dịch đó được lưu trữ, và nội dung của nó được sự nhất trí chung giữa các bên liên quan tham gia vào giao dịch. Tập hợp các bản ghi trong sổ cái phân tán phải có

khả năng được xác minh và kiểm toán. Một trong những mục tiêu chính của DLT là cung cấp các bản ghi giao dịch trực tuyến không thể chối bỏ.

Việc nhìn nhận DLT theo cách này không hàm ý rằng mọi nút trong mạng đều lưu trữ chính xác cùng một tập hợp các bản ghi giao dịch (mặc dù điều này có thể đúng với một số dạng sổ cái phân tán). Điều này cũng không hàm ý rằng mọi bên tham gia vào sổ cái phân tán đều có quyền truy cập vào tất cả các bản ghi giao dịch (có thể xảy ra trường hợp các bên không có quyền truy cập vào các bản ghi giao dịch mà họ không tham gia). Các bản ghi giao dịch được lưu trữ trên một nút trong hệ thống DLT có thể là tập hợp toàn phần hoặc một phần của sổ cái phân tán được triển khai bởi hệ thống DLT đó.

5.1.2 DLT chuỗi khối và DLT phi chuỗi khối

Các hệ thống blockchain là một tập hợp con của các Công nghệ sổ cái phân tán, trong đó trạng thái của sổ cái phân tán được duy trì thông qua việc xử lý theo lô các giao dịch trong các cấu trúc dữ liệu được bảo mật bằng phương pháp mật mã, được gọi là các khối. Một giao thức hợp lệ phải đảm bảo rằng mỗi khối được liên kết bằng mật mã với khối ngay trước đó, tạo thành một chuỗi khối duy nhất theo thời gian. Chuỗi đầy đủ liên kết bằng mật mã tạo thành một cấu trúc dữ liệu chỉ cho phép ghi nối và có thể truy cập trên mọi nơi - được gọi là chuỗi khối - cung cấp phiên bản chuẩn tắc của toàn bộ lịch sử giao dịch.

Để đảm bảo rằng quá trình cập nhật sổ cái tạo ra một trạng thái sổ cái duy nhất cho một khối nhất định, các giao thức chuỗi khối bao gồm một cơ chế đồng thuận nhằm cung cấp sự sắp xếp thứ tự toàn phần của tất cả các giao dịch trong khối đó. Hoạt động tập thể của tất cả các nút trong hệ thống blockchain đóng vai trò như một máy chủ dấu thời gian, thực hiện xác thực các giao dịch đang chờ xử lý và cập nhật trạng thái sổ cái hiện hành bằng cách tuần tự gắn thêm các khối vào chuỗi khối.

Để triển khai một sổ cái phân tán, các hệ thống blockchain yêu cầu một cơ chế phân phối các khối mới đến tất cả các nút, một cơ chế xác thực các giao dịch, và một cơ chế đảm bảo tính nhất quán của tất cả các bản sao của chuỗi khối.

Thuật ngữ “blockchain” thường được dùng để chỉ đồng thời cho cả cấu trúc dữ liệu lẫn toàn bộ triển khai của một sổ cái phân tán sử dụng cấu trúc dữ liệu chuỗi khối đó.

Cấu trúc dữ liệu blockchain có thể được sử dụng để triển khai thực thể gì đó không phải là sổ cái phân tán; tuy nhiên, các cách sử dụng blockchain như vậy không thuộc phạm vi của tiêu chuẩn này. Điều này bao gồm cả việc triển khai cơ sở dữ liệu blockchain theo mô hình tập trung.

Không phải tất cả các hệ thống DLT đều dựa trên blockchain. Một số hệ thống DLT sử dụng các cấu trúc dữ liệu sổ cái khác với các cách khác để lưu trữ bản ghi giao dịch và duy trì tính toàn vẹn, vốn thường mang lại các đặc tính khác biệt (ví dụ: khả năng hỗ trợ tốc độ giao dịch cao).

Trong một số hệ thống DLT phi blockchain, mỗi bản ghi giao dịch được lưu trữ dưới dạng một mục sổ cái riêng biệt, thay vì là một phần nội dung của một khối. Ngoài ra, cấu trúc sổ cái có thể không nhất thiết là một chuỗi. Ví dụ, có những sổ cái mà cấu trúc nền tảng được tổ chức theo dạng đồ thị có hướng không tuần hoàn (DAG), với các giao dịch được biểu diễn bằng các đỉnh. Việc sử dụng DAG cho các giao dịch có thể cải thiện thời gian và chi phí cần thiết cho quá trình xác nhận giao dịch, nhưng đồng thời làm tăng khối lượng công việc cho quá trình đồng bộ hóa.

5.2 Mạng và truyền thông

Hoạt động mạng và truyền thông là một bộ phận thiết yếu của các hệ thống DLT.
Một chương trình phân tán, hay ứng dụng phân tán, là một ứng dụng chạy trên một hệ thống phân tán.
Kiến trúc ứng dụng phân tán theo mô hình P2P phân chia các tác vụ hoặc khối lượng công việc giữa các nút ngang hàng. Các nút ngang hàng là những thành viên tham gia ứng dụng có quyền hạn và năng lực ngang bằng nhau. Chúng tạo thành một mạng P2P gồm các nút.
Mạng DLT là mạng các nút DLT tạo thành một hệ thống sổ cái phân tán. Thông thường, các nút DLT giao tiếp với nhau thông qua các mạng P2P.
Giao thức được lựa chọn để giao tiếp giữa các nút DLT phụ thuộc vào các tùy chọn triển khai và các cân nhắc sẵn có.

5.3 Nền tảng DLT

Nền tảng DLT là tập hợp các thực thể xử lý, lưu trữ và truyền thông mà cùng nhau cung cấp các khả năng của hệ thống sổ cái phân tán trên mỗi nút DLT.

Trong trường hợp này, một nút là một máy trong mạng P2P chạy các thành phần phần mềm giao tiếp nhằm hỗ trợ sổ cái phân tán và có thể lưu trữ một bản sao của sổ cái. Nút có thể là một máy vật lý hoặc một dạng môi trường thực thi ảo nào đó, chẳng hạn như một hay nhiều máy ảo hoặc container. Môi trường ảo có thể được sử dụng nếu nút được triển khai trên nền tảng điện toán đám mây, ví dụ, chẳng hạn. Tham khảo ISO/IEC TS 23167 để biết thêm thông tin về các môi trường ảo và container.

Một nút lưu trữ bản sao đầy đủ của sổ cái được gọi là nút đầy đủ. Một số hệ thống DLT có các nút mà theo thiết kế, không chứa bản sao đầy đủ của sổ cái.

Nền tảng chuỗi khối là một nền tảng DLT trong đó công nghệ triển khai là chuỗi khối. Các khả năng được hỗ trợ bởi nền tảng DLT có thể bao gồm:

- Các môi trường thực thi an toàn,
- Các hợp đồng thông minh,
- Sổ cái,
- Hệ thống giao dịch,
- Các dịch vụ thành viên,
- Quản lý trạng thái,
- Cơ chế đồng thuận,
- Phân phối sự kiện,
- Các dịch vụ mật mã, và
- Các giao tiếp liên nút an toàn.

Nền tảng DLT được mô tả chi tiết hơn tại 9.3.5.

5.4 Các giao diện hệ thống DLT

Nhìn chung, các giao diện có thể được sử dụng để giao tiếp bởi người dùng, bởi quản trị viên, giữa các nút trong mạng, đến các hợp đồng thông minh, giữa các hợp đồng thông minh với nhau, giữa các hệ thống DLT với nhau, và đến các hệ thống phi DLT bên ngoài.

Để hiểu được các giao diện phù hợp cần thiết cho tính liên tác, cần phải trước tiên hiểu hệ thống và/hoặc ứng dụng nào đang trao đổi thông tin và với mục đích gì.

Hình 2 minh họa bốn loại giao diện thông dụng được sử dụng trong các hệ thống DLT:

- Giao diện liên hệ thống (Intersystem interfaces) A - trực tiếp giữa hai (hoặc nhiều hơn) hệ thống DLT;
- Giao diện bên ngoài (External interfaces) B - giữa các hệ thống DLT và các hệ thống phi DLT bên ngoài, chẳng hạn như các DLT Oracle;
- Giao diện người dùng (User interfaces) C - giữa các ứng dụng người dùng và các hệ thống DLT;
- Giao diện quản trị (Admin interfaces) D - giữa các ứng dụng quản trị và các hệ thống DLT.

Các giao diện liên hệ thống hỗ trợ giao tiếp giữa các hệ thống DLT riêng biệt.

Giao diện bên ngoài có thể cung cấp phương thức an toàn để truy cập các khả năng nằm ngoài hệ thống DLT như các nguồn dữ liệu đáng tin cậy hoặc các hàm. Các hệ thống bên ngoài đó bao gồm mã nằm ngoài sổ cái, DLT Oracle, các ứng dụng phi DLT và dữ liệu ngoài sổ cái. Các hệ thống này được liên kết với mỗi nút DLT bằng các giao diện bên ngoài. (Xem 9.3.2 để biết giải thích về cơ chế hoạt động của DLT Oracle.)

Một hệ thống DLT bao gồm cả các ứng dụng người dùng cung cấp khả năng cho người dùng cuối, lẫn các ứng dụng quản trị cung cấp khả năng quản trị và quản lý hệ thống DLT. Các ứng dụng này truy cập hệ thống DLT thông qua giao diện người dùng và giao diện quản trị của một nút, một cách tương ứng.

Các giao diện hợp đồng thông minh có thể được yêu cầu giữa các dịch vụ DLT, để các hợp đồng thông minh trên một hệ thống DLT có thể tương tác với một hệ thống DLT khác. Ngoài ra, những người dùng và các quản trị viên có thể cần giao tiếp trực tiếp với các hợp đồng thông minh.

Các giao diện vừa tác động vừa hỗ trợ tính liên tác - xem 6.7 về tính liên tác.

5.5 Sự đồng thuận

Trong bối cảnh các hệ thống DLT, đồng thuận giải quyết vấn đề thống nhất về nội dung và thứ tự của các bản ghi trong một hệ thống phân tán rộng rãi, nơi các bản ghi mới có thể cạnh tranh nhau để được thêm vào bởi nhiều nút khác nhau trong mạng.
Các hệ thống DLT có thể vận hành trong một mạng lưới các nút có khả năng phân tán rộng về mặt địa lý. Mỗi nút có thể tạo một bản ghi mới để đưa vào sổ cái hoặc nhận thông tin về một bản ghi mới. Tuy nhiên, tại thời điểm đó, bản ghi mới đó có thể chưa được tất cả các nút khác trong hệ thống nhìn thấy. Trong một số trường hợp, một nút có thể nhận được thông tin về hai bản ghi mới khác nhau, cả hai đều cạnh tranh để trở thành bản ghi mới nhất. Các cơ chế đồng thuận xác định cách tất cả các nút độc lập trong hệ thống DLT đạt được thỏa thuận về nội dung và thứ tự của các bản ghi đó.

Đồng thuận có các khía cạnh khác nhau, thường được giải quyết theo các khung thời gian khác nhau.Thứ nhất, có câu hỏi về đồng thuận liên quan đến tính hợp lệ của các giao dịch hoặc tập hợp các giao dịch. Vấn đề này thường được giải quyết trong quá trình tạo lập hệ thống DLT, sau đó được các nút chấp thuận khi tham gia mạng, và có thể được cập nhật bởi các cơ chế quản trị trong suốt vòng đời của mạng. Việc chấp thuận ban đầu và liên tục đối với các cơ chế xác thực thường được thiết lập thông qua một dạng đồng thuận xã hội phi chính thức (đối với chuỗi khối hoặc hệ

thống DLT công khai) hoặc thông qua phương thức hợp đồng (đối với chuỗi khối hoặc hệ thống DLT riêng tư). Thứ hai, có câu hỏi về việc giao dịch hợp lệ nào nên được đưa vào bản ghi sổ cái gần đây nhất (và mở rộng ra là, toàn bộ các bản ghi tiếp theo).

Nhiều cơ chế khác nhau có thể được sử dụng để đạt được sự đồng thuận về việc đưa các giao dịch vào sổ cái và thứ tự của chúng. Việc lựa chọn một cơ chế phù hợp có thể phụ thuộc vào mô hình mối đe dọa hoặc các chế độ lỗi mà mạng các nút cần được bảo vệ chống lại. Một số cơ chế trong số đó được trình bày dưới đây:

- Luân phiên (Round Robin): Các nút trong một nhóm nhỏ lần lượt đóng vai trò có thẩm quyền trong việc tạo các bản ghi mới, theo kiểu lượt nối tiếp.
- Khả năng chịu lỗi Byzantine (Byzantine Fault Tolerance - BFT) hoặc Thỏa thuận Byzantine (Byzantine Agreement): Các phương pháp tiếp cận thông thường trong tài liệu về hệ thống phân tán thường xem xét mối đe dọa từ lỗi Byzantine, trong đó các nút riêng lẻ trong mạng không chỉ có thể bị trễ trong việc tiếp nhận thông tin mới từ các nút khác, mà còn có thể nhận phải những thông tin được tạo ra một cách ác ý từ một số lượng (có hạn) các nút độc hại khác. Trong bối cảnh này, nhiều thuật toán đồng thuận chịu lỗi Byzantine đã được đề xuất, bao gồm Byzantine Paxos và PBFT. Thông thường, các cơ chế này yêu cầu số lượng nút trong mạng phải được biết trước, số lượng nút độc hại phải ở mức nhỏ (thường là ít hơn 1/3 tổng số nút), và mỗi nút phải thu thập bằng chứng từ một túc số (thường là đa số rõ ràng trong số các nút còn lại. Các cơ chế loại này thường được sử dụng trong các hệ thống DLT riêng tư. Trong thực tế, để đạt hiệu suất tốt, các cơ chế này có thể giới hạn quy mô mạng ở mức vài chục đến vài trăm nút.
- Đồng thuận Nakamoto (Nakamoto Consensus): Đối với các hệ thống chuỗi khối công khai, các nút tham gia có thể chưa được biết trước và số lượng của chúng có thể thay đổi. Do đó, các nút cần đạt được đồng thuận cũng có thể chưa được xác định. Cơ chế đồng thuận được sử dụng trong chuỗi khối Bitcoin, cũng như trong các chuỗi khối công khai khác như Ethereum, được gọi là Đồng thuận Nakamoto và giải quyết thách thức này. Theo nguyên tắc chung, mỗi nút sẽ chấp nhận chuỗi khối dài nhất mà nó đã nhìn thấy là chuỗi có thẩm quyền. Trong trường hợp xuất hiện các khối cạnh tranh thay thế nhau, có thể xuất hiện các lịch sử thay thế tồn tại trong thời gian ngắn (phân nhánh - forks, hoặc khối chú - uncle blocks) được các nút khác nhau trong mạng tạm thời chấp thuận. Tuy nhiên, các nút thường sẽ hội tụ về việc chấp thuận một lịch sử chuỗi khối chung, ít nhất là đối với các phần cũ hơn của sổ cái. Một số phiên bản đồng thuận không chỉ sử dụng độ dài chuỗi mà còn tính đến tổng độ khó tích lũy (trong Bằng chứng công việc), do đó việc đánh giá có thể mang tính đa chiều.

Bằng chứng công việc (Proof of Work) và Bằng chứng cổ phần (Proof of Stake) là hai phương pháp đào một khối mới nhằm thực hiện đồng thuận Nakamoto:

- Bằng chứng Công việc (Proof of Work): Việc tạo các khối mới trong Bitcoin yêu cầu giải một bài toán mật mã khó hoặc bài toán khó về mặt tính toán: với một tập hợp giao dịch cho một khối mới, phải chọn một giá trị nonce sao cho giá trị băm của khối nhỏ hơn một mục tiêu cản trở hiện hành đã được chấp nhận. Mặc dù việc tìm ra lời giải là khó, nhưng việc kiểm tra lời giải lại dễ dàng. Phương pháp tổng thể này được gọi là Bằng chứng Công việc. Không có lời giải hiệu quả nào được biết đến cho loại bài toán này, do đó phải sử dụng phương pháp vét cạn. Điều này có nghĩa là thời gian cần thiết để tìm ra lời giải về cơ bản là ngẫu nhiên, nhưng tỷ lệ thuận với năng lực tính toán có sẵn để giải bài toán.

Bằng chứng Công việc yêu cầu đầu tư một lượng vốn tiền tệ đáng kể vào các tài nguyên tính toán cần thiết để giải bài toán. Các nút có thể nhận được lợi ích ngay lập tức thông qua việc được thưởng cả tiền mã hóa mới được đúc (có thể được nhận như phần thưởng khối) và các khoản phí giao dịch do các giao dịch riêng lẻ được đưa vào trong khối. Việc đầu tư và lợi ích như vậy có xu hướng làm đồng nhất động cơ của các nút với việc tạo ra giá trị và tính toàn vẹn cho toàn bộ mạng DLT. Cơ chế này có thể thích ứng với bất kỳ số lượng nút nào trong mạng, bằng cách điều chỉnh độ khó của bài toán theo thời gian, nhằm đáp lại với những thay đổi về thời gian trung bình cần thiết để mạng giải mỗi bài toán.

- Bằng chứng cổ phần (Proof of Stake): Trong cơ chế này, việc bầu chọn người dẫn đầu ngẫu nhiên được xác định thông qua một hình thức đặt cược tỷ lệ thuận với lượng tiền mã hóa được đặt cọc bởi các nút đang cạnh tranh để xác định khối tiếp theo. Lượng cổ phần nắm giữ bằng tiền mã hóa của các nút phục vụ để điều chỉnh lợi ích của các nút với sự vận hành đúng đắn của mạng.

Các phương pháp tiếp cận khác cho đồng thuận cũng có thể áp dụng trong các hệ thống DLT không cần cấp quyền. Ví dụ, tất cả các nút có thể định kỳ bầu chọn một số lượng nhỏ các nút đã biết (vài chục đến vài trăm nút) để hành động thay mặt cho toàn bộ mạng. Khi đó, các cơ chế đồng thuận thông thường vốn phù hợp với các hệ thống DLT được cấp quyền có thể được sử dụng bởi các nút được bầu chọn đó. Trong bối cảnh này, hệ thống phần thưởng hoặc cơ chế khuyến khích là một yếu tố cần cân nhắc (chẳng hạn như khoản thanh toán) được trao cho một bên để thực hiện một hoạt động nhất định trong hệ thống DLT. Một ví dụ về hoạt động đó là công việc liên quan đến việc vận hành cơ chế đồng thuận. Đào là hoạt động tìm kiếm phần thưởng trong một số cơ chế đồng thuận, và trong các hệ thống đó, thợ đào sở hữu một nút chạy các chương trình đào.

Tính hoàn kết là một thuộc tính của các giao dịch đã được xác nhận, cho biết liệu các giao dịch đó có tiếp tục là một phần của sổ cái sau khi được xác nhận hay không. Một số hệ thống DLT có thể tồn tại nhiều lịch sử chuỗi khối không đồng nhất. Khi mạng DLT hội tụ về một lịch sử chuỗi khối chung, các bản sao lịch sử chuỗi khối còn lại bị loại bỏ và do đó, một số giao dịch đã được xác nhận có thể không còn là một phần của sổ cái. Điều này đặc biệt rõ ràng trong các hệ thống DLT sử dụng Đồng thuận Nakamoto, khi các nút sẽ loại bỏ lịch sử chuỗi khối hiện tại của mình để chuyển sang một lịch sử dài hơn. Do đó, một giao dịch đã được xác nhận không nhất thiết sẽ được ghi lại trong sổ cái. Do các hệ thống bên ngoài thường phụ thuộc vào việc một giao dịch đã được xác nhận là một phần của sổ cái, một thông lệ phổ biến là chờ cho đến khi một số lượng nhất định các khối được thêm vào sổ cái trước khi kết luận rằng giao dịch đó sẽ là một phần của sổ cái. Tuy nhiên, ngay cả sau khi chờ một số lượng khối nhất định, vẫn tồn tại khả năng một lịch sử chuỗi khối dài hơn được phát hiện mà không bao gồm giao dịch đó. Loại tính hoàn kết này được gọi là tính hoàn kết xác suất và đối lập với tính hoàn kết tức thì - loại được sử dụng bởi các hệ thống DLT không thể có nhiều lịch sử chuỗi khối cho một sổ cái duy nhất. Với tính hoàn kết tức thì, các hệ thống bên ngoài biết rằng một khi giao dịch đã được xác nhận, giao dịch đó được bảo đảm sẽ là một phần của sổ cái.

5.6 Các sự kiện

Một sự kiện là một tình huống nhất định xảy ra tại một thời điểm nhất định. Trong bối cảnh các hệ thống thông tin, sự kiện có thể được hiểu là một sự thay đổi trạng thái hoặc giá trị được phát hiện để xử lý và/hoặc báo cáo (xem ISO 16484-2:2004, 3.74). Ví dụ, đó có thể là một thông điệp được gửi từ một nút đến ứng dụng bên ngoài. Các sự kiện biểu thị các kích thích bên ngoài, các thay đổi đối với giá trị của trường và sự tương tác giữa các nút (xem ISO/IEC 14772-2:2004, 3.3). Từ góc độ kiến trúc, có thể phân biệt:

a. các sự kiện nội bộ - nội bộ của một hệ thống DLT; và

b. sự kiện bên ngoài - được truyền đến và/hoặc được ghi lại trong một hệ thống DLT.

Giống như các hệ thống CNTT khác, một hệ thống DLT cần đảm bảo việc xử lý, ghi nhật ký và truy xuất nguồn gốc đúng đắn của các sự kiện nội bộ nhằm đảm bảo tính an ninh, khả năng kiểm toán và tính minh bạch. Tính năng của hệ thống cần bao gồm các chức năng quản lý sự kiện, hỗ trợ các dịch vụ sự kiện được xác định trước hoặc tùy chỉnh dành cho người dùng DLT (xem, ví dụ: ISO/IEC 17789:2014, 8.3.2.2, khoản mục thứ hai trong danh sách). Thông tin được ghi lại về các sự kiện phải có khả năng phát hiện can thiệp trái phép, cho dù sự kiện đó được ghi lại trên sổ cái hay ngoài sổ cái. Khi cần thực hiện sửa đổi, việc đó có thể được thực hiện bằng cách thêm các bản ghi mới trong khi bảo toàn các bản ghi trước đó, nhằm mục đích đảm bảo tính trách nhiệm giải trình và minh bạch. Trong bối cảnh DLT, sổ cái chỉ đảm bảo tính an ninh cho dữ liệu trên sổ cái (on-ledger data). Để đảm bảo tính an ninh cho dữ liệu ngoài sổ cái, cần phải có các biện pháp an ninh riêng biệt.

Các sự kiện bên ngoài là cực kỳ quan trọng cho tính năng hướng sự kiện của hợp đồng thông minh. Kết nối với thế giới bên ngoài được thiết lập thông qua trao đổi dữ liệu, bao gồm cả dữ liệu về các sự kiện. Điều thiết yếu là phải bảo đảm độ tin cậy của các nguồn thông tin bên ngoài (được gọi là các DLT oracle). Độ tin cậy của các nguồn bên ngoài có thể liên quan đến các cân nhắc phi kỹ thuật. Các yêu cầu về độ tin cậy có thể được thiết lập, ví dụ, bởi pháp luật hiện hành, bởi các chính sách của hệ thống DLT, hoặc bởi thỏa thuận giữa các bên tham gia hợp đồng thông minh.

Vì các sự kiện được phát bởi các nhà phát hành và được nhận bởi các bên đăng ký mà trước đó đã đăng ký để nhận chúng, hình thức giao tiếp này vốn dĩ là bất đồng bộ. Tùy thuộc vào tầm quan trọng của hệ thống trong việc tiếp nhận sự kiện một cách đáng tin cậy và/hoặc kịp thời, có thể thiết lập các cơ chế xử lý sự cố mạng hoặc sự cố nút, tức là thực hiện đệm và chuyển tiếp các sự kiện chưa được tiếp nhận hoặc xác nhận khi cần thiết. Nhiều hệ thống sự kiện khác nhau đã được kiểm chứng về độ tin cậy, được hiểu rõ và phù hợp để sử dụng trong các hệ thống DLT, do đó không được giải thích thêm trong tiêu chuẩn này.

Các ví dụ về sự kiện cần xem xét bao gồm:

- Các sự kiện hạ tầng mạng: mạng sổ cái được triển khai, được tham gia hoặc trạng thái vận hành được cập nhật
- Các sự kiện nút: nút sổ cái được triển khai, cập nhật, trạng thái vận hành được cập nhật (trực tuyến/ngoại tuyến);
- Các sự kiện người dùng: tài khoản DLT được tạo, được làm mới, người dùng đăng nhập;
- Các sự kiện hợp đồng thông minh: hợp đồng thông minh được triển khai, phiên bản hợp đồng thông minh được tạo;
- Các sự kiện giao dịch: hàm phiên bản hợp đồng thông minh được thực thi, được cập nhật, trạng thái phiên bản hợp đồng thông minh được cập nhật.

5.7 Tính toàn vẹn nội dung sổ cái

Nhìn chung, tính toàn vẹn hàm ý sự đầy đủ và không bị sửa đổi hoặc xóa bỏ một cách trái phép. Trong DLT, có nhiều đặc tính liên quan đến tính toàn vẹn, chẳng hạn như tính nhất quán, tính bất biến và tính chính xác. Đối với các hệ thống DLT, tính toàn vẹn có thể được xem xét ở nhiều tầng trừu tượng hóa kiến trúc khác nhau.

Ở tầng giao dịch riêng lẻ, tính toàn vẹn có nghĩa là tính hợp lệ, theo nghĩa là giao dịch tuân thủ các quy tắc của hệ thống DLT, đảm bảo tính nhất quán bền vững cho việc đưa giao dịch vào sổ cái.

Ở tầng sổ cái, tính toàn vẹn thường có nghĩa là sổ cái phải đầy đủ, bất biến và chỉ được tạo lập theo đúng các quy tắc của nền tảng DLT. Trong trường hợp này, tính bất biến có nghĩa là chỉ có các giao dịch mới có thể được thêm vào sổ cái sau khi đạt được sự đồng thuận, và các bản ghi hiện có không thể bị thay đổi.

Ở tầng ứng dụng sử dụng sổ cái, tính toàn vẹn sẽ được xác định theo các tiêu chí riêng biệt của ứng dụng. Các tiêu chí này thậm chí có thể bao gồm những đặc tính không có khả năng thi hành hoặc xác minh một cách máy móc, chẳng hạn như tính chính xác.

Một trong những mục tiêu chính của DLT là cung cấp các bản ghi giao dịch an toàn, đồng nhất đối với tất cả các bên tham gia trong một kịch bản đa bên liên quan cụ thể, và không thể bị phủ nhận mà không cần sử dụng cơ sở dữ liệu tập trung.

Trong một số giải pháp DLT, thông tin về nguồn gốc có thể được ghi lại trên sổ cái bằng cách sử dụng một hoặc nhiều giao dịch có liên quan. Nguồn gốc là bản ghi về quyền sở hữu, gốc gác và/hoặc vị trí của một tài sản. Các hệ thống DLT hữu ích cho các ứng dụng theo dõi nguồn gốc vì tất cả các giao dịch liên quan đến một tài sản đều được duy trì trong một sổ cái có khả năng phát lộ can thiệp trái phép.

Trong một số mô hình chuỗi cung ứng, dữ liệu gắn liền với việc tạo lập và vận chuyển tài sản, nếu được theo dõi, thì được đăng ký và duy trì riêng biệt bởi từng doanh nghiệp tham gia chuỗi cung ứng. Có khả năng thông tin trong các hệ thống này khác nhau, và ngoài ra không có bảo đảm nào rằng thông tin được duy trì là bất biến. Điều này khiến việc theo dõi một tài sản trở nên khó khăn, tốn thời gian và tiềm ẩn sự không đáng tin cậy. Việc không thể truy xuất gốc gác và theo dõi hành trình của một tài sản một cách dễ dàng và đáng tin cậy có những hệ quả lớn đối với doanh nghiệp. Trong chuỗi cung ứng thực phẩm, một lượng lớn thực phẩm không bị nhiễm bẩn có thể phải bị loại bỏ cùng với một lượng nhỏ thực phẩm bị nhiễm bẩn trong quá trình thu hồi thực phẩm. Thuốc giả có nguồn gốc không rõ ràng trong chuỗi cung ứng dược phẩm có thể dẫn đến tử vong.

Khi các tài sản được tạo lập và trao đổi trong chuỗi cung ứng, các giao dịch mô tả các sự kiện này được ghi lại một cách bất biến vào sổ cái phân tán, với mỗi bên tham gia có quyền truy cập vào một bản sao cục bộ của các bản ghi giao dịch. Các mục tiêu phân tán và có khả năng phát lộ can thiệp trái phép - vốn là nền tảng cho các hệ thống DLT (như được mô tả trong 5.1) - khiến chúng phù hợp cho các mục đích này.

5.8 Tính toàn vẹn và quản lý sổ cái

Để tính toàn vẹn được bảo toàn và hệ thống DLT được tin cậy, một khi sự đồng thuận đạt được đối với các bản ghi giao dịch hoặc nội dung được thêm vào sổ cái phân tán, tính bất biến của chúng phải được đảm bảo. Các bản ghi riêng lẻ không nên bị xóa.

Việc xóa có nghĩa là xóa vĩnh viễn và loại bỏ các bản ghi đã được xác nhận khỏi sổ cái phân tán. Các hệ thống DLT loại trừ việc xóa theo thiết kế.

Do các hệ thống DLT là các hệ thống chỉ cho phép ghi thêm và các bản ghi giao dịch không bị xóa bỏ, các sổ cái phân tán có thể trở nên quá lớn và cồng kềnh để quản lý hiệu quả. Rút gọn (pruning) và lưu trữ là các phương pháp đưa các bản ghi giao dịch cũ nhất vào một số dạng kho lưu trữ và loại bỏ chúng khỏi các bản sao đang hoạt động của sổ cái phân tán. Các bản ghi đã được lưu trữ

hoặc rút gọn vẫn có thể truy cập theo yêu cầu, mặc dù tốc độ truy cập có thể chậm hơn đáng kể so với các bản ghi sổ cái trực tiếp.

Việc rút gọn sổ cái phân tán có thể được thực hiện bằng cách tạo một bản sao nhỏ hơn của sổ cái phân tán, thông qua việc lọc ra các bản ghi giao dịch đáp ứng các tiêu chí đã xác định. Các giao dịch đã bị lọc phải có khả năng được phục hồi với tính toàn vẹn nếu cần. Tiêu chí cho việc rút gọn có thể bao gồm việc cũ hơn một khoảng thời gian được chỉ định, hoặc không còn đầu ra để chi tiêu.

Việc rút gọn có thể được thực hiện đối với một tập hợp con các nút nào đó trong hệ thống DLT. Các bản sao đầy đủ của sổ cái tại các nút khác sẽ cho phép việc truy xuất các giao dịch vốn có thể đã bị rút gọn (xem lưu trữ, sao lưu và phục hồi) và sẽ duy trì tính toàn vẹn tổng thể của hệ thống. Do bản chất phân tán của các hệ thống DLT và những tác động của các hoạt động lưu trữ và sao lưu đối với sự tin cậy và tính toàn vẹn, điều thiết yếu là phải có khả năng phục hồi và quản trị mạnh mẽ bao hàm các hoạt động này để cho phép phục hồi trong trường hợp xảy ra sự gián đoạn.

Việc lưu trữ dữ liệu có thể được thực hiện để cải thiện khả năng phục hồi và độ tin cậy của hệ thống. Rút gọn không loại trừ việc lưu trữ, sao lưu và khôi phục cũng được thiết kế tích hợp vào hệ thống. Lưu trữ dữ liệu là một quá trình gìn giữ kỹ thuật số giúp di chuyển dữ liệu vào một hình thức lưu trữ được quản lý để lưu giữ dài hạn. Kho lưu trữ là một tập hợp dữ liệu, bao gồm các mục nhập bản ghi, các giao dịch hoặc tài nguyên được lưu lại để tham chiếu hoặc sử dụng sau này, có thể ở dạng ngoại tuyến.

Một phương pháp phổ biến để bảo tồn dữ liệu, độc lập với việc cắt tỉa và lưu trữ, là sử dụng việc sao lưu và khôi phục sổ cái hoặc nút.

Trong trường hợp này, sao lưu là quá trình sao chép/xuất các bản ghi giao dịch hoặc dữ liệu khác vào kho lưu trữ dữ liệu của một hệ thống sao lưu nhằm cho phép truy xuất và khôi phục các dữ liệu này hoặc thực thi lại các giao dịch trong trường hợp xảy ra sự cố hoặc gián đoạn. Bản sao này được gọi là bản sao lưu. Việc khôi phục cần được thực hiện theo cách thức bảo tồn được tính toàn vẹn (cùng số lượng và nội dung của tất cả các bản ghi) và nội dung của sổ cái phân tán.

5.9 Các chuỗi con và các chuỗi bên

Một chuỗi con là một chuỗi tách biệt về mặt lô gic mà tạo thành một phần của hệ thống DLT. Nó cũng được biết đến như là một kênh trong các kiến trúc của một số nền tảng DLT. Mỗi chuỗi con có thể được sở hữu bởi một thực thể khác nhau và có thể được truy cập bởi một tập hợp người dùng khác nhau. Các nút có thể được thiết lập sao cho một số nút tham gia vào các chuỗi con nhất định và không vào các chuỗi con khác. Kết quả của cấu hình này là các sổ cái trên một số nút có thể chứa các giao dịch cho một chuỗi con nhất định trong khi các sổ cái trên các nút khác thì không.

Một chuỗi bên là một hệ thống chuỗi khối tách biệt chạy song song với hệ thống chuỗi khối gốc mà có thể tham gia vào các giao dịch với nó thông thường theo cả hai hướng, sử dụng một giao diện hai chiều. Giao diện hai chiều cho phép khả năng hoán đổi các tài sản tại một tỷ lệ được xác định trước giữa hệ thống chuỗi khối gốc và chuỗi bên.

5.10 Các ứng dụng DLT

Một ứng dụng DLT, cũng được gọi là ứng dụng sổ cái, là một ứng dụng cung cấp các chức năng hỗ trợ một số hoạt động của những người dùng DLT. Một ứng dụng DLT có thể là một ứng dụng người dùng dành cho những người dùng hoặc một ứng dụng quản trị dành cho các quản trị viên.

Ứng dụng DLT tương tác với một hệ thống DLT thông qua User API được tạo sẵn bởi một nút DLT, và hoạt động sử dụng hệ thống DLT cùng các tập hợp khả năng do các hệ thống phi DLT cung cấp cần thiết để thực hiện tính năng của ứng dụng DLT.

User API có thể cung cấp các thao tác mà có thể được gọi bởi ứng dụng DLT và cũng là một giao diện cho ứng dụng DLT nhận các sự kiện xảy ra trong hệ thống DLT, ví dụ như các giao dịch cụ thể đang được ghi lại vào sổ cái phân tán. Ứng dụng DLT có thể khởi tạo một giao dịch trong hệ thống DLT. Trong một số trường hợp, User API cho phép giao tiếp với một hoặc nhiều hợp đồng thông minh, trong đó việc thực thi các thao tác riêng lẻ của User API được cung cấp bởi một hợp đồng thông minh.

Các ứng dụng DLT có thể hỗ trợ người dùng thông qua các giao diện người dùng điển hình như giao diện máy tính để bàn, web, di động và bảng điều khiển. Các ứng dụng DLT cũng có thể được tự động hóa. Ví dụ về các ứng dụng DLT tự động bao gồm các ứng dụng kết nối thiết bị IoT với hệ thống DLT, ví dụ khi các thiết bị IoT phát hiện các sự kiện trong thế giới vật lý và cần ghi lại các sự kiện này vào sổ cái phân tán. Trong những trường hợp này, có thể không có những người dùng là con người của ứng dụng DLT trong các hoàn cảnh bình thường.

Đối với các ứng dụng quản trị, ứng dụng DLT được sử dụng để quản trị chính hệ thống DLT hoặc để quản trị các nút DLT riêng lẻ. Các ứng dụng DLT quản trị này thường tương tác với hệ thống DLT thông qua các administration API chuyên dụng.

5.11 Các giải pháp DLT

Giải pháp DLT là thuật ngữ dùng để chỉ một giải pháp hoàn chỉnh đầu cuối được xây dựng bằng cách dùng một hệ thống DLT nhằm đạt được một số mục tiêu liên quan đến một nhóm các tổ chức. Một ví dụ là một giải pháp hỗ trợ tạo điều kiện thuận lợi thương mại chuỗi cung ứng, giao dịch với nhiều tổ chức khác nhau tham gia vào một chuỗi cung ứng, chẳng hạn như các nhà sản xuất, khách hàng, các tổ chức vận chuyển, các cơ quan chính phủ, v.v.

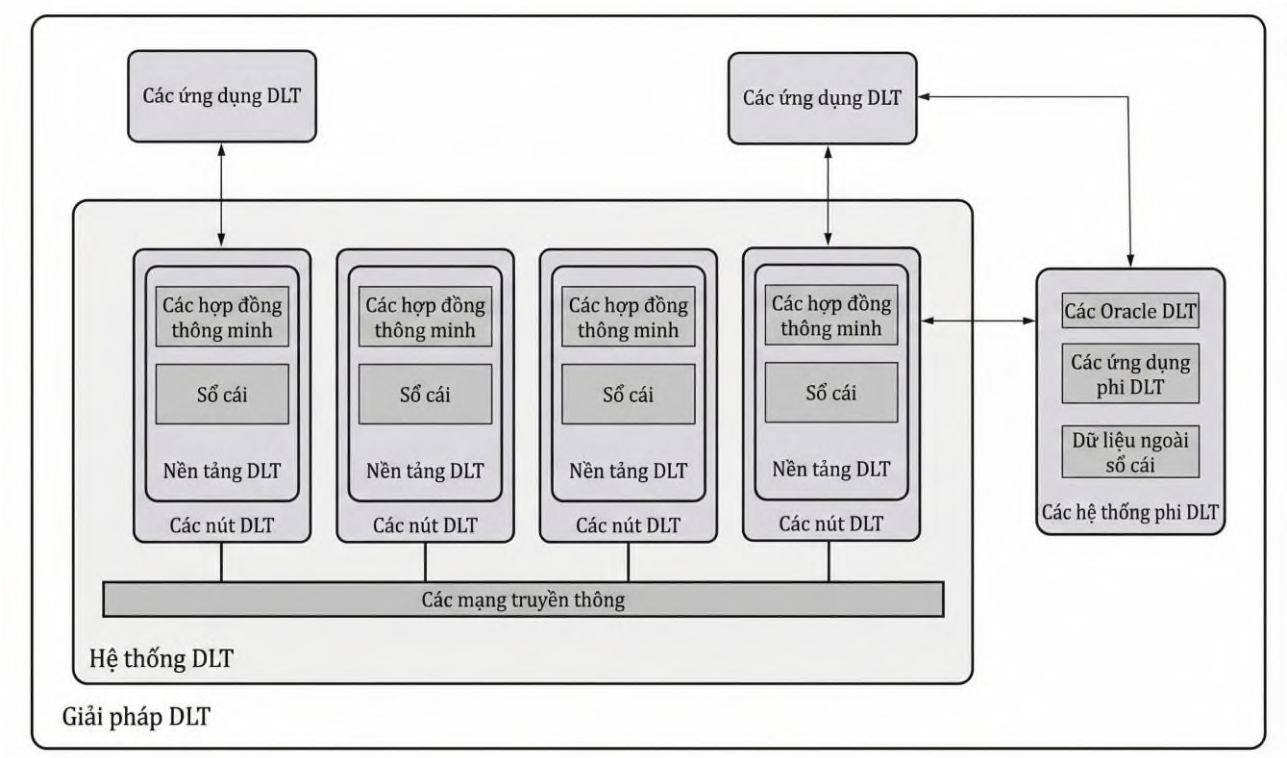
Các hệ thống DLT là phân tán theo định nghĩa, với hệ thống DLT có một số các nút DLT được nối mạng cùng nhau. Các giải pháp DLT là phân tán một cách tương tự, với vô số các thành phần được phân tán trên toàn mạng.

Thông thường các nút DLT khác nhau của một hệ thống DLT là phi tập trung, có nghĩa là chúng được kiểm soát bởi các tổ chức (hoặc các cá nhân) khác nhau, và mỗi nút DLT có thể được sử dụng bởi các ứng dụng DLT khác nhau. Mỗi ứng dụng DLT có các chức năng phản ánh các hoạt động và mối quan tâm của tổ chức liên quan và người dùng của nó. Tất nhiên cũng có khả năng là cùng một ứng dụng DLT được sử dụng bởi nhiều tổ chức và người dùng của họ, nơi tất cả họ đều đang thực hiện các hoạt động giống nhau.

Ngoài ra, các năng lực của chính hệ thống DLT có thể được định nghĩa bởi các hợp đồng thông minh tồn tại trên các nút DLT, vốn chịu trách nhiệm xử lý các yêu cầu giao dịch và thêm các bản ghi giao dịch vào sổ cái phân tán.

Một ứng dụng DLT gọi một hoặc nhiều hợp đồng thông minh thông qua API người dùng để khởi tạo một giao dịch. Một giải pháp DLT cũng có thể bao gồm một tập hợp các oracle DLT và các hệ thống phi DLT liên quan.

Do đó, giải pháp DLT bao gồm hệ thống DLT với các nút DLT và các mạng truyền thông cộng với tất cả các ứng dụng DLT được kết nối với từng nút DLT, cùng với bất kỳ hệ thống phi DLT liên kết nào được kết nối với hệ thống DLT. Các mũi tên biểu diễn các luồng dữ liệu giữa hệ thống DLT, các ứng dụng DLT và các hệ thống phi DLT, như được minh họa trong Hình 1.



Hình 1 – Giải pháp DLT và các thành phần

5.12 Các hợp đồng thông minh

5.12.1 Tổng quan

Không phải tất cả các hệ thống DLT đều sử dụng hợp đồng thông minh. Mô tả mở rộng về việc triển khai, quá trình thực thi và vòng đời của hợp đồng thông minh được trình bày trong ISO/TR 23455; do đó, tại đây chỉ các thành phần kiến trúc sẽ được mô tả.

Logic liên quan đến các hợp đồng thông minh phải thực thi một cách tất định, nếu không, sẽ không đạt được sự đồng thuận nào về kết quả của một thực thi chính xác.

Phần lớn các môi trường thực thi cho phép hợp đồng thông minh được lập trình bằng các ngôn ngữ lập trình bậc cao hoặc ngôn ngữ lập trình miền chuyên biệt. Do đó, các hợp đồng thông minh có thể có các biến để lưu trữ dữ liệu và các hàm để truy cập, xử lý và ghi dữ liệu.

Trong một số hệ thống, các hợp đồng thông minh có thể được thực thi trên mọi nút và trong các hệ thống khác chúng có thể được thực thi chỉ trên một tập hợp giới hạn các nút được chỉ định trước.

Ngoài ra, do việc thực thi mã bởi các thợ khai thác hoặc các trình xác nhận có thể ngăn cản họ thực hiện các nhiệm vụ chính của chúng - là tạo lập và xác thực các khối - số lượng và thời điểm thực thi các hợp đồng thông minh phải rất hạn chế để đảm bảo hệ thống DLT hoạt động đầy đủ chức năng. Hơn nữa, các ứng dụng thâm dụng dữ liệu cần lưu trữ và truy xuất dữ liệu của chúng ngoài sổ cái nhằm ngăn chặn tình trạng từ chối dịch vụ trong hệ thống DLT. Các kiến trúc mới hơn đang xuất hiện với khả năng xử lý đồng thời cả hai nhiệm vụ theo cách không ảnh hưởng đến hệ thống.

5.12.2 Thực thi hợp đồng thông minh trên các nút ngang hàng chuyên dụng

Các hợp đồng thông minh có thể được cài đặt và thực thi cục bộ trên các nút ngang hàng chuyên dụng. Mã được thực thi cục bộ có thể lưu trữ hoặc truy xuất tất cả các yêu cầu xử lý cho việc thực thi với kết quả tất định trên nút ngang hàng cục bộ.

Đoạn mã cục bộ này để lại một rủi ro an ninh xét về một điểm tấn công đơn lẻ do nó có thể bị sửa đổi trước hoặc thậm chí trong quá trình thực thi bởi một tác nhân độc hại. Do đó, một giai đoạn xác thực bổ sung phải được thực thi bởi một thực thể đáng tin cậy khác để xác minh tính hợp lệ của các kết quả như tính toán bởi các nút ngang hàng đã đề cập ở trên. Trong loại môi trường thực thi này, các hệ thống chuỗi khối và DLT có thể tương tác trực tiếp với môi trường của các nút ngang hàng thông qua các trình điều khiển thiết bị do điểm thực thi đã được biết.

5.12.3 Thực thi hợp đồng thông minh trên các nút ngang hàng tùy ý

Mã được thực thi tại một vị trí bất kỳ đọc trạng thái từ sổ cái do đây là vị trí duy nhất được thống nhất đồng thuận cho trạng thái xác định hiện tại. Do trạng thái này và tất cả các thay đổi đối với nó lại được sao lại trên toàn mạng P2P, các giao dịch tiêu tốn bộ nhớ cần được tránh trong các hệ thống hợp đồng thông minh chạy trên các nút ngang hàng bất kỳ.

Các hợp đồng thông minh mà thực thi trên các nút ngang hàng bất kỳ yêu cầu ba đến bốn vai trò có khả năng khác nhau:

- Hợp đồng thông minh cần được ghi vào hệ thống DLT bởi một bên được gọi là chủ sở hữu hợp đồng thông minh. Chủ sở hữu này có các quyền mở rộng đối với hoạt động của hợp đồng thông minh, chẳng hạn như vô hiệu hóa nó vĩnh viễn, còn được gọi là "hủy" hợp đồng thông minh;
- Một bên thứ hai có khả năng khác biệt có thể gọi mã bằng cách gửi một giao dịch đến địa chỉ của hợp đồng thông minh đó;
- Một bên thứ ba được biết đến như thợ khai thác hoặc trình xác nhận trong một số hệ thống DLT, khởi tạo và thực thi đoạn mã, và ghi các kết quả trên sổ cái;
- Kết quả này phải được kiểm tra bởi các thợ khai thác hoặc các trình xác nhận khác trong khi xác nhận và nối thêm một khối chứa kết quả thực thi. Vì lý do bảo mật, việc tính toán kết quả và kiểm tra nó có thể được thực hiện bởi các thợ đào hoặc các trình xác nhận khác nhau.

Bản thân mã hợp đồng thông minh có thể được triển khai thông qua một giao dịch đến mạng sổ cái phân tán, nơi nó trải qua quy trình xác thực thông thường chẳng hạn như đào và đồng thuận. Một khi đã được thêm vào sổ cái phân tán, nó thực tế là bất biến; tuy nhiên, một số hệ thống DLT cung cấp các tính năng mà cho phép sử dụng phiên bản cập nhật của hợp đồng thông minh. Do vị trí thực thi là bất kỳ, các hợp đồng thông minh có thể tương tác với các thiết bị IoT, các bộ chuyển đổi hoặc các bên thứ ba thông qua các giao diện bên ngoài, thường được gọi là Oracle DLT, có thể định địa chỉ trên các nút ngang hàng chuyên dụng của các hệ thống DLT.

5.13 Các giao dịch và cách chúng hoạt động

Vì mục đích của tiểu mục này, một giao dịch được hiểu là một sự thay đổi trạng thái nguyên tử (không thể chia nhỏ) được ghi lại trong một sổ cái phân tán. Tính toàn vẹn yêu cầu một điều kiện bất biến đối với toàn bộ hệ thống DLT phải được duy trì trong khi thực thi các giao dịch. Một giao dịch thay đổi hệ thống từ trạng thái nhất quán này sang trạng thái khác. Tính nguyên tử của một giao dịch có nghĩa là nó sẽ hoặc thành công hoặc thất bại, nhưng sẽ không bị hoàn thành chỉ một phần.

Đối với các hệ thống DLT công khai, các loại giao dịch đơn giản nhất là việc chuyển tiền mã hóa hoặc tài sản kỹ thuật số khác từ một địa chỉ này sang một địa chỉ khác. Trong các hệ thống như vậy,

trạng thái của DLT sẽ ghi lại quyền kiểm soát các tài sản bởi các địa chỉ. Các quy tắc quan trọng cho việc chuyển tài sản kỹ thuật số thường bao gồm yêu cầu địa chỉ gốc kiểm soát các tài sản đang được chuyển giao. Các quy tắc của một số hệ thống DLT chỉ cho phép chuyển giao từ một địa chỉ nguồn duy nhất đến một địa chỉ đích duy nhất, trong khi các hệ thống khác cho phép việc chuyển giao tới và từ nhiều địa chỉ trong một giao dịch đơn lẻ.

Trên một số hệ thống DLT, một số giao dịch có thể có tác động lớn hơn. Ví dụ, trên Ethereum, các giao dịch có thể ghi lại các kết quả của việc thực thi các hợp đồng thông minh. Đối với Ethereum, các quy tắc bao gồm một đặc tả về việc thực thi các lệnh của Máy ảo Ethereum (Ethereum Virtual Machine) mà cấu thành mã đối tượng (object code) cho các hợp đồng thông minh đó.

Trên một số hệ thống DLT, sự thay đổi trạng thái của một giao dịch có thể bao gồm việc ghi lại thông tin hoặc các sự kiện.

Các kết quả của việc thực thi các giao dịch có thể bị ảnh hưởng bởi các sự thay đổi trạng thái do các giao dịch khác. Do đó, thứ tự mà các giao dịch được thực thi là quan trọng. Vì lý do này, các giao dịch được thực hiện theo thứ tự tuần tự, hoặc ít nhất có thể được xem như đã được thực hiện một cách tuần tự. Tuy nhiên, các cơ chế đánh giá giao dịch tinh vi có thể cho phép việc đánh giá đồng thời các giao dịch trong khi vẫn duy trì khả năng tuần tự hóa. Điều này có thể được thực hiện nếu không có sự phụ thuộc lẫn nhau giữa các giao dịch. Tuy nhiên, việc xác định rằng hai giao dịch không có sự phụ thuộc lẫn nhau có thể là khó khăn, đặc biệt đối với các giao dịch thực thi hợp đồng thông minh.

Một số giao dịch chỉ có thể được thực thi bởi các cá nhân ở các vai trò nhất định trong phạm vi một hợp đồng hoặc đang nắm giữ một định danh trên sổ cái được ủy quyền cụ thể, ví dụ như một địa chỉ trong hệ thống DLT.

5.14 Token, tiền ảo và tiền mã hóa, coin và các khái niệm liên quan

Các hệ thống DLT đôi khi, nhưng không phải luôn luôn, tập trung vào một cơ chế theo dõi duy nhất, theo nghĩa rộng thuộc phạm trù của các token. Về mặt lịch sử, trong các hệ thống phi DLT, các token vật lý (như tiền xu, chip hoặc vé) đã được sử dụng từ lâu bên trong các hệ thống hoặc môi trường khép kín cục bộ. Tiền tệ và tiền xu có thể có giá trị nội tại (mà có thể thay đổi giá trị đáng kể - giá trị có thể biến động mạnh). Các token như các loại chip, vé, tem, vòng đeo tay, và các thiết bị khác được phát hành cho các mục đích sử dụng cục bộ, như là tại một rạp chiếu phim, cho một hệ thống tàu điện ngầm, trong một lễ hội âm nhạc, cho các trò chơi điện tử thùng, sòng bạc, hoặc để sử dụng máy giặt và máy sấy tại một tiệm giặt ủi - nhằm đơn giản hóa việc xử lý tiền mặt bên trong hệ thống. Chúng cũng có thể giảm thiểu các rủi ro của việc xử lý tiền tệ, và, cho các mục đích tâm lý, giảm bớt sự dè dặt trong việc chi tiêu, giảm rủi ro các token bị đánh cắp để được sử dụng ở nơi khác, và nâng cao rào cản việc chuyển đổi token trở lại thành tiền mặt.

Các token mật mã (cryptographic tokens), ảo và vật lý, tương tự cũng đã được sử dụng từ lâu trong nhiều môi trường hệ thống phân tán khác nhau, chủ yếu cho việc truy cập vào một hệ thống; chúng đã đảm nhận nhiều vai trò mới trong một môi trường DLT, nơi các quyền của người nắm giữ không được giám sát tập trung.

Tài sản là các mặt hàng có giá trị, mà có thể là vật lý và ảo. Tài sản kỹ thuật số là các tài sản mà chỉ tồn tại dưới dạng ảo hoặc là đại diện kỹ thuật số của các tài sản khác. Tiền mã hóa gắn liền với việc tạo dựng giá trị cho các đồng tiền hoặc token ảo.

Token là một tài sản số đại diện cho một tập hợp các quyền lợi. Thông thường, các token được bảo chứng bằng tài sản được đăng ký trong các sổ cái và sau đó được liên kết với người dùng.

Các loại token bao gồm những loại sau đây:

- Các token có giá trị nội tại: Nơi mà giá trị của token dựa hoàn toàn vào nguồn cung và cầu đối với chính token đó, nơi nó trở thành một "tiền tệ bản địa" bên trong một môi trường nào đó;
- Các token có giá trị ngoại lai: Nơi mà giá trị của token được xác định dựa trên một điểm tham chiếu bên ngoài nào đó. Giống như các token vật lý, token là đại diện thay thế cho một thứ khác: một token khác, một tài sản vật lý hoặc các tài sản ảo;
- Các token đại diện (không mang giá trị): Các token có thể được thiết kế cho nhiều mục đích khác bên trong một hệ thống, giống như chúng được sử dụng trong thế giới thực, trong đó mục tiêu chính không giới hạn ở việc trao đổi giá trị. Các token có thể được sử dụng như các thiết bị theo dõi.

Các đồng tiền điện tử được thiết kế chủ yếu cho các hệ thống thanh toán (ví dụ: Bitcoin).

Các token mật mã, ảo và vật lý, cũng đã được sử dụng từ lâu trong nhiều môi trường hệ thống phân tán khác nhau, chủ yếu để truy cập vào một hệ thống; chúng đã đảm nhận nhiều vai trò mới trong một môi trường DLT, nơi đó các quyền của người nắm giữ không được giám sát tập trung. Ví dụ, các token có thể được sử dụng để theo dõi mức độ sử dụng hoặc được dùng làm công cụ khuyến khích nhằm nâng cao chất lượng và thực thi quản trị, hoặc trong một số trường hợp chúng có thể đại diện cho các quyền khác như lợi ích thụ hưởng trong một công cụ tài chính.

"Virtual Currency Schemes" được công bố bởi Ngân hàng Trung ương Châu Âu (ECB) năm 2012 định nghĩa tiền tệ ảo là một loại tiền số không được quản lý, được phát hành và thông thường được kiểm soát bởi các nhà phát triển nó, và được sử dụng và chấp nhận trong phạm vi các thành viên của một cộng đồng ảo cụ thể. Xem Phụ lục A có toàn bộ thảo luận về token và tiền tệ.

6 Các khía cạnh xuyên suốt

6.1 Tổng quan

Các khía cạnh xuyên suốt là các hành vi hoặc năng lực được phối hợp giữa các vai trò và phải được triển khai một cách nhất quán trong một hệ thống DLT. Các khía cạnh xuyên suốt có thể được chia sẻ với và có thể tác động đến nhiều vai trò, các hoạt động và thành phần chức năng.

Các khía cạnh xuyên suốt của DLT bao gồm:

- an ninh,

- danh tính,

- quyền riêng tư,

- quản trị,

- quản lý,

- tính liên tác, và

- luồng dữ liệu.

6.2 An ninh

Do các hệ thống DLT phụ thuộc nhiều vào truyền thông phân tán, các nút phân tán, các cơ chế đồng thuận và mật mã, các yếu tố bảo mật sau đây cần được xem xét:

a) An ninh mạng;

b) sự lựa chọn và cấu hình các thuật toán và giao thức mật mã;

c) quản lý khóa mật mã;

d) bảo mật ứng dụng;

e) các quy trình quản lý an ninh;

f) triển khai an toàn và chứng nhận;

g) tính sẵn sàng.

Các xem xét an ninh đặc thù DLT đang được đề cập bao gồm:

a) an ninh đồng thuận;

b) quản lý phân nhánh cứng/mềm; và

c) quản lý dữ liệu khối.

Các dịch vụ thành viên quản lý tư cách thành viên của các hệ thống DLT căn cứ vào danh tính, bảo vệ quyền riêng tư, tính bảo mật và khả năng kiểm toán trong hệ thống DLT.

Kiểm soát truy cập dựa trên vai trò đôi khi được sử dụng để cung cấp một mô hình biểu đạt hơn cho các hệ thống chính sách kiểm soát truy cập.

Khi sổ cái mở rộng, việc quản lý khóa có thể trở thành thách thức. Ví dụ, nếu một khóa riêng bị xâm phạm, thay đổi hoặc bị thu hồi, thì sẽ khó để tin cậy và xử lý dữ liệu đã được ký trước đó bằng khóa này. Đôi khi, khi ID người dùng dựa trên khóa công khai của người dùng, điều này có thể dẫn đến những thách thức đối với việc nhận dạng người dùng. Để khắc phục điều này, các kỹ thuật thay đổi khóa chuyên biệt cần được triển khai. Đối với các hệ thống DLT riêng tư, các vấn đề nêu trên có thể được giải quyết bằng cách tích hợp PKI, CadES, v.v.

Trong một hệ thống DLT, an toàn thông tin bao gồm việc bảo vệ tính bảo mật, tính toàn vẹn và tính sẵn sàng của thông tin, và việc bảo vệ PII (Thông tin nhận dạng cá nhân), và nó bao phủ hơn sổ cái. Đây là một khía cạnh xuyên suốt và bao phủ người dùng, các hệ thống phi DLT, API, nền tảng DLT, hạ tầng và các chức năng xuyên lớp khác. Việc hiểu rõ các cân nhắc về an ninh giúp lựa chọn và tích hợp các cơ chế an ninh phù hợp để bảo vệ phần cứng, phần mềm trung gian (Middleware) và phần mềm cấu thành hệ thống DLT. Các chức năng bảo mật xuyên suốt bao gồm bảo vệ tài sản, quản lý truy cập, quản lý định danh, quản lý mật mã, quản lý đánh giá và kiểm thử, bảo vệ PII và quản lý tính sẵn sàng.

Mỗi chức năng bảo mật có thể được cấu thành từ một hoặc nhiều dịch vụ, quy trình và công cụ, có thể được triển khai để đáp ứng các yêu cầu của tổ chức xuyên suốt các lớp và các chức năng (các

hàm). Ví dụ, các dịch vụ kiểm soát truy cập có thể được triển khai ở lớp người dùng và lớp các hệ thống phi DLT, trong các chức năng phát triển, và trong các chức năng quản lý và vận hành.

Các tổ chức có thể triển khai hoặc thực thi toàn bộ, một phần hoặc không triển khai bất kỳ thành phần nào của kiến trúc. Việc lựa chọn các thành phần kiến trúc, dịch vụ, quy trình và công cụ được áp dụng có thể được định hướng bởi các yếu tố như: yêu cầu của tổ chức; năng lực của tổ chức; các hoạt động được thực hiện bởi tổ chức; các nguồn lực sẵn có; các mối đe dọa và các lỗ hổng bảo mật (điểm yếu); và mức độ chấp nhận rủi ro cùng khẩu vị rủi ro của các bên liên quan.Tuy nhiên, một số lựa chọn có thể bị giới hạn, do tổ chức tạo lập sổ cái và bản ghi ban đầu (ví dụ: khối khởi nguyên trong một hệ thống chuỗi khối) sẽ thiết lập một số tham số nhất định, chẳng hạn như thuật toán mã hóa mà tất cả các người tham gia trong một hệ thống DLT phải tuân theo.

6.3 Danh tính

Tầm quan trọng của danh tính trong Công nghệ sổ cái phân tán xuất phát từ thực tế là các giao dịch có thể bao gồm các định danh liên quan đến một thể nhân, một pháp nhân, một vật thể hoặc một quy trình. Có thể dựa vào các thực thể bên thứ ba đáng tin cậy truyền thống để cung cấp các định danh kỹ thuật số này để truyền thông và các giao dịch an toàn (Các tổ chức chứng thực X.509, các cơ quan đăng ký tên miền DNS), v.v. nhưng các định danh phi tập trung đặt sự kiểm soát trở lại vào tay chủ sở hữu danh tính, đây là một cân nhắc quan trọng đối với danh tính tự quản, phi tập trung.

6.4 Quyền riêng tư

6.4.1 Tổng quan

Một số cách sử dụng hệ thống DLT nhất thiết liên quan đến việc thu thập và lưu trữ thông tin nhận dạng cá nhân (PII - Personally Identifiable Information) bởi hệ thống. Điều này đặt ra câu hỏi về cách thức PII được lưu trữ bởi hệ thống. Một đặc điểm quan trọng của các hệ thống DLT là thông tin được lưu trữ trong sổ cái phân tán thông thường là bất biến – nó không thể thay đổi sau khi đã được ghi vào sổ cái. Đặc tính này có thể xung đột với một số nguyên tắc áp dụng cho việc bảo vệ PII; cụ thể, có thể không thể cho phép chủ thể PII xóa bất kỳ PII nào của họ sau khi đã được ghi vào sổ cái phân tán. Một chủ thể PII có thể chỉnh sửa PII bằng cách sử dụng một giao dịch khác. Tuy nhiên, thông tin trước đó vẫn còn lại trên sổ cái và có thể vẫn truy cập được.

Có nhiều kỹ thuật nhằm tăng cường bảo vệ quyền riêng tư bằng công nghệ. Cụ thể, các Công nghệ tăng cường Quyền riêng tư cung cấp một khả năng bảo vệ dữ liệu thông qua nhiều phương tiện khác nhau. Một số cách tiếp cận bao gồm như sau:

a) các kỹ thuật mật mã;

b) các kỹ thuật mạng;

c) các khuôn khổ quyền riêng tư;

d) các kỹ thuật dựa trên kênh.

Xem ISO/TR 23244 để biết thêm chi tiết về các kỹ thuật bảo vệ quyền riêng tư. Việc sử dụng các cách tiếp cận này liên quan đến với PII có chấp nhận được hay không phụ thuộc mạnh vào trường hợp sử dụng cụ thể và cơ sở pháp lý cho việc lưu trữ PII. Trong một số trường hợp, có thể được yêu cầu bởi pháp luật phải duy trì một bản ghi vĩnh viễn và không thay đổi của một số PII – một ví dụ như sổ đăng ký bất động sản. Trong các trường hợp khác, có thể được yêu cầu để cho phép

chủ thể PII xóa PII của họ. Do DLT không hỗ trợ điều này, PII do đó không nên được lưu trữ trên sổ cái. Thay vào đó, PII cần được đặt trong một cơ sở dữ liệu ngoài sổ cái (có thể thay đổi), với một loại con trỏ nào đó trỏ tới PII này được đặt vào các bản ghi của sổ cái. Cách tiếp cận này cho phép PII được cập nhật và/hoặc bị xóa trong khi vẫn bảo toàn tính bất biến của các bản ghi sổ cái.

Khi thiết kế và vận hành các hệ thống DLT, hướng dẫn và các nguyên tắc được nêu trong ISO/IEC 29100 có thể được áp dụng; có thể có thêm các xem xét đối với các vấn đề đặc thù của hệ thống DLT. Các kiến trúc DLT sẽ có tác động lớn lên quyền riêng tư và việc bảo vệ PII. Bên trong một kiến trúc, việc triển khai quản lý truy cập, các dịch vụ bảo mật và mật mã cho các ứng dụng, các API và lưu trữ xuyên suốt cả hệ thống DLT và hệ thống phi DLT có thể bảo vệ PII thông qua các biện pháp kỹ thuật và phi kỹ thuật. Nhiều biện pháp kiểm soát an toàn thông tin, nhằm bảo vệ tính bảo mật, tính toàn vẹn và/hoặc tính sẵn sàng của thông tin và dữ liệu, cũng phù hợp cho việc bảo vệ PII. Việc lựa chọn các biện pháp kiểm soát có thể được thực hiện bằng cách sử dụng các kỹ thuật quản lý rủi ro, các chính sách kinh doanh và an toàn thông tin, và các năng lực của các dịch vụ trong kiến trúc. ISO/IEC 27001, ISO/IEC 29134, ISO/IEC 29151 và ISO/IEC 29100 cung cấp các biện pháp kiểm soát và hướng dẫn cho các khía cạnh bảo mật và quyền riêng tư chung.

Cũng có thể hợp lý khi sử dụng mô hình “quyền riêng tư theo thiết kế” trong phát triển DLT để tạo ra các hệ thống DLT cung cấp việc bảo vệ PII thích hợp.

PII có thể được chứa trong hai loại kho dữ liệu:

- trên sổ cái (on-ledger);

- ngoài sổ cái (off-ledger).

6.4.2 Lưu trữ PII trên sổ cái

PII có thể được lưu trữ bên trong các bản ghi DLT (ví dụ: các khối chuỗi khối). Nếu có yêu cầu đối với PII phải được chỉnh sửa hoặc bị xóa, ví dụ để tuân thủ các yêu cầu pháp lý hoặc quy định, trong nhiều hệ thống DLT, trên thực tế có thể không thể sửa đổi hoặc xóa các bản ghi đó. Các phương án trong trường hợp xấu nhất có thể bao gồm một phân nhánh cứng. Trong trường hợp của một số hệ thống DLT riêng tư, chủ sở hữu có thể bị buộc phải đóng toàn bộ hệ thống. Ngoài ra, có một rủi ro lộ lọt liên tục, ví dụ thông qua các khóa bị rò rỉ hoặc các cuộc tấn công tiền ảnh, ngay cả khi PII được mã hóa hoặc được băm. Các tiêu chí cho các thuật toán và tham số mã hóa tốt được thảo luận trong ISO/IEC 18033-1, nhưng mã hóa tốt không nhất thiết là đủ để bảo vệ PII trong một hệ thống DLT.

Khi sổ cái tăng về kích thước và khi các giao dịch được thêm vào, sự tích lũy dữ liệu trong chính sổ cái và các liên kết đến các cơ sở dữ liệu và lưu trữ bên ngoài có thể dẫn đến các hiệu ứng tổng hợp, có khả năng cho phép nhận dạng trực tiếp hoặc gián tiếp một chủ thể PII. Những tiến bộ trong năng lực phân tích và lập hồ sơ cũng có thể dẫn đến các hiệu ứng tổng hợp hoặc các hiệu ứng khác, một lần nữa làm tăng rủi ro nhận dạng chủ thể PII.

6.4.3 Lưu trữ PII ngoài sổ cái

Trường hợp dữ liệu được lưu giữ ngoài sổ cái, việc bảo vệ quyền riêng tư và PII có thể được giải quyết bằng cách áp dụng cách tiếp cận của ISO/IEC 29100. Các hệ thống DLT thường sử dụng các giá trị băm của các tệp để cho phép dữ liệu thực tế được lưu giữ ngoài sổ cái trong khi một bản ghi đã được xác thực của tệp được lưu giữ trên sổ cái. Điều này tạo điều kiện để các tệp lớn có liên quan được lưu giữ ngoài sổ cái, trong khi tính toàn vẹn của dữ liệu được tham chiếu được duy trì

thông qua việc sử dụng hàm băm trên dữ liệu. Các định danh có thể được sử dụng để trỏ đến PII được lưu giữ ngoài sổ cái, trong đó các định danh này không bắt nguồn từ chính dữ liệu và sẽ có thể chỉ có quan hệ một chiều.

Lưu trữ thông tin "ngoài sổ cái" có thể cung cấp tính bảo mật của các chi tiết giao dịch. Hệ thống ngoài sổ cái có thể được cấu hình để hạn chế quyền truy cập vào các chi tiết giao dịch chỉ cho các bên được ủy quyền, hỗ trợ các trường hợp sử dụng mà trong đó những người tham gia muốn giữ riêng tư các chi tiết giao dịch của họ với những người tham gia DLT khác.

Tuy nhiên, lưu trữ thông tin "ngoài sổ cái" làm triệt tiêu nhiều lợi thế của việc sử dụng hệ thống DLT ngay từ đầu. Mặc dù việc sử dụng các giá trị băm cho phép đảm bảo tính toàn vẹn và phát hiện giả mạo, nhưng khi không có các chi tiết giao dịch, blockchain không còn có thể là một bản ghi đơn lẻ, được chia sẻ, có thể được xác minh bởi nhiều bên theo một tập hợp các quy tắc (nguồn sự thật). Ví dụ, việc phát hành và giao dịch các tài sản kỹ thuật số có thể chuyển nhượng, có thể thay thế được không còn khả thi nếu không tham chiếu đến hệ thống lưu giữ vị thế ngoài sổ cái (tức là một hệ thống giám sát số lượng tài sản được ghi nhận ở cấp độ hệ thống DLT và sự tuân thủ của nó với các giao dịch mà hệ thống nhận biết). Ngoài ra, lưu trữ thông tin giao dịch ngoài sổ cái thường yêu cầu cả hai đối tác duy trì bản ghi của riêng họ, hoặc ủy quyền trách nhiệm đó cho một Bên thứ ba đáng tin cậy, điều mang lại cùng với nó là các chi phí và bất lợi tương tự như việc hạn chế quyền truy cập đọc vào chuỗi khối.

Một thách thức lớn đối với các hệ thống DLT là khả năng đảm bảo rằng một tệp hoặc một khối trên một nút và bất kỳ kho lưu trữ ngoài sổ cái liên kết nào đã được xóa. DLT cũng có thể tích hợp với các hệ thống tệp phân tán, ví dụ BigChainDB và IPFS. Các hệ thống tệp này cũng có cùng thách thức trong việc đảm bảo rằng nếu một tệp bị xóa, thì xác nhận được nhận rằng trên mỗi nút tệp đó đã được xóa.

6.5 Quản trị DLT

Xem 3.7. Việc định hướng và kiểm soát ngụ ý tạo lập một khuôn khổ thiết lập chính sách, các quyền quyết định (bao gồm quyền truy cập), trách nhiệm giải trình và thực thi liên tục trong các hệ thống DLT. Quản trị các hệ thống DLT là thách thức do bản chất phân tán và phi tập trung của hầu hết các hệ thống DLT, cụ thể vì những lý do sau:

- Nhiều bên liên quan sở hữu (các cá nhân, các tổ chức) có thể cần được xem xét;

- Quản trị xuyên suốt các ranh giới tổ chức hoặc các khu vực tài phán có thể xảy ra;

- Các xem xét quản trị cho việc thiết lập các hệ thống DLT và các hoạt động liên tục có thể khác biệt;

- Một mức độ cao của các quyền quyết định tập trung có thể được cần đến ban đầu để cho phép kiểm soát phân tán và phi tập trung về sau;

- Việc đặc tả và thực thi các quyền quyết định có thể cần được tổ chức để hoạt động trong một môi trường phân tán và phi tập trung;

- Các cơ chế khuyến khích có thể cần được triển khai để mà có hiệu quả trong môi trường phân tán và phi tập trung;

- Các bản ghi được quyết định dựa trên thông qua các cơ chế đồng thuận phân tán và phi tập trung;

- Các tham số giao dịch chủ yếu được xác định sử dụng các cơ chế phân tán và phi tập trung;

- Trách nhiệm giải trình nên được đặc tả rõ ràng phản ánh bản chất phân tán và phi tập trung;

- Quản trị có thể cần mở rộng quy mô trên khắp một số lượng lớn các nút và các bên có quyền lợi liên quan;

- Một tính năng cấp quyền có thể được yêu cầu để hỗ trợ nhiều bên xuyên suốt các tổ chức và đôi khi xuyên suốt các biên giới;

- Một hệ thống quản lý danh tính phù hợp có thể cần được thiết lập.

Các quyết định cụ thể mà sẽ phải được giải quyết có thể bao gồm việc lựa chọn và định nghĩa các cơ chế đồng thuận, cách thức các cơ chế bỏ phiếu hoạt động, cách thức các xung đột được giải quyết, cách thức hoạt động đào hoạt động, và cách thức các tác nhân tổ chức và con người tham gia.

Các cơ chế và các bộ giám sát cần được định nghĩa trên các hệ thống DLT đang hoạt động sao cho chúng có thể xác minh rằng các chính sách quản trị đang được thực thi và có thể phát tín hiệu khi quản trị và các quyết định cần được điều chỉnh. ISO/TS 23635 cung cấp hướng dẫn thêm về quản trị cho các hệ thống DLT.

6.6 Quản lý

Quản lý các hệ thống DLT bao gồm việc quản lý từng nút trong hệ thống cộng với tất cả các thách thức của việc quản lý các hệ thống phân tán bao gồm nhiều nút. Nó cũng bao gồm các vấn đề liên quan đến quyền sở hữu và quyền kiểm soát khác nhau của từng nút, quy mô của các hệ thống, và việc xử lý cơ chế đồng thuận.

Quản lý bao trùm toàn bộ vòng đời của hệ thống DLT: phát triển, kiểm thử, cấu hình, triển khai, vận hành, giám sát, bảo trì và cho ngừng hoạt động.

Quản trị cần được thiết lập để hỗ trợ tất cả các loại hình quản lý, và quản lý cần báo cáo các ngoại lệ và các số liệu đo lường đến bất kỳ hệ thống quản trị nào sao cho phù hợp. Do bản chất phân tán và phi tập trung của quyền sở hữu, việc xác định ai chịu trách nhiệm cho việc thực thi các tác vụ quản trị và quản lý cần được xem xét cẩn thận và các trách nhiệm cần được phân bổ phù hợp.

Các mục tiêu cho việc quản lý trong các hệ thống DLT có thể bao gồm:

- các nút (bao gồm mã của nền tảng DLT),

- các sổ cái phân tán,

- các giao dịch,

- các môi trường thực thi an toàn,

- các hợp đồng thông minh,

- mật mã,

- các kênh,

- tư cách thành viên,

- những người dùng (các khách),

- lưu trữ dữ liệu,

- các hệ thống sự kiện,

- các ứng dụng,

- sự tuân thủ với quy định,

- các mạng, và

- bảo mật – các quyền và bảo mật cho các nút, các thành viên, các hợp đồng thông minh và những người dùng (xem 6.2).

Quản lý cho mỗi mục tiêu sẽ là khác nhau:

Việc quản lý cấu hình bao gồm cấu hình ban đầu cho triển khai và cập nhật cấu hình trên một cơ sở liên tục trong một hoặc nhiều nút, các hợp đồng thông minh, các sổ cái, các ứng dụng, hoặc các người dùng.

Quản lý triển khai bao gồm việc triển khai và loại bỏ các nút, các mạng, các hợp đồng thông minh, các sổ cái, các cơ sở dữ liệu và các ứng dụng xuyên suốt một mạng phân tán của các hệ thống vật lý, các hệ thống ảo và các hệ thống DLT. Quy mô và các sự phụ thuộc có thể là những thách thức ở đây.

Quản lý vận hành bao gồm:

- khởi động các nút và các ứng dụng.

- dừng các nút và các ứng dụng, và

- thay đổi các kết nối mạng.

Giám sát bao gồm:

- giám sát hiệu năng của các nút và các mạng truyền thông,

- giám sát trạng thái và tính sẵn sàng của các nút và các mạng truyền thông, và

- giám sát các số liệu nghiệp vụ đặc trưng cho quản trị.

Bảo trì bao gồm việc thực thi và triển khai các thay đổi liên tục đối với bất kỳ phần tử nào của các hệ thống DLT, các mạng, và các ứng dụng. Việc đưa các thay đổi được triển khai trên khắp hàng nghìn nút một cách kịp thời mà không gây gián đoạn tính sẵn sàng và khả năng liên tác của các API có thể là một thách thức.

Việc loại bỏ bao gồm việc cho ngừng hoạt động hoặc việc xóa bất kỳ phần tử nào khỏi hệ thống DLT. Làm điều này mà không gây ra sự gián đoạn với hệ thống DLT là quan trọng.

Quản lý và quản trị các hệ thống DLT cần được điều phối cẩn thận. Như một ví dụ, quy trình quản trị có thể quyết định rằng mã của nền tảng DLT cần được cập nhật, giả sử để khắc phục một vấn đề bảo mật – quy trình quản lý cần đảm bảo rằng tất cả các nút trong hệ thống DLT được cập nhật một cách tương ứng, hoặc nếu không vấn đề bảo mật có thể vẫn còn tồn lại.

Phần mềm cho các nền tảng DLT có thể được cập nhật để sửa các lỗi và thay đổi các quy tắc, bao gồm cơ chế đồng thuận, giao thức truyền thông giữa các nút DLT, cấu trúc dữ liệu, kích thước của khối, và độ khó cho Bằng chứng công việc và. v.v. Có hai loại hình chuyển đổi khác nhau liên quan đến cập nhật phần mềm được gọi là phân nhánh cứng và phân nhánh mềm.

Một phân nhánh cứng là một sự thay đổi mà không giữ tính tương thích ngược. Nó yêu cầu tất cả các nút DLT cập nhật lên phiên bản mới của phần mềm. Các nút DLT không được cập nhật không thể chấp nhận các giao dịch hoặc dữ liệu sổ cái mà được tạo ra bởi các nút DLT được cập nhật theo các quy tắc mới. Bởi vậy, các nút DLT không được cập nhật không có khả năng duy trì một kết nối đến mạng của các nút DLT được cập nhật. Các phân nhánh cứng có thể gây ra sự phân kỳ vĩnh viễn của các sổ cái giữa các nút DLT không được cập nhật và các nút DLT được cập nhật. Loại phân kỳ này được gọi là “chia tách sổ cái” hay “phân nhánh”. Các phân nhánh cứng có thể được gây ra một cách có chủ ý hoặc tình cờ.

Một phân nhánh mềm là một sự thay đổi để giữ tính tương thích ngược. Nó là một cách để khuyến khích các nút DLT cập nhật lên phiên bản phần mềm mới. Các nút DLT cũ không được cập nhật và các nút DLT mới được cập nhật cùng tồn tại trên cùng một mạng DLT. Các nút DLT cũ có thể chấp nhận các giao dịch hoặc dữ liệu sổ cái mà được tạo bởi các nút DLT mới, nhưng mặt khác, các nút DLT mới có thể từ chối những thứ được tạo bởi các nút DLT cũ. Nếu một phần lớn các nút DLT cập nhật lên phần mềm mới, được kỳ vọng rằng các nút DLT cũ khác sẽ cũng cập nhật vì các giao dịch và dữ liệu sổ cái của chúng có thể được chấp nhận bởi một số lượng lớn hơn các nút DLT.

6.7 Tính liên tác

Các hệ thống DLT đang được đề xuất cho nhiều mục đích khác nhau, trong đó các hệ thống DLT sẽ cần phải làm việc cùng với các hệ thống DLT khác và với các hệ thống phi DLT. Nhìn vào sự phát triển của thẻ tín dụng và trao đổi dữ liệu điện tử (EDI), các hệ thống DLT đại diện cho tài sản mã hóa sẽ cần phải liên tác với các hệ thống tài sản mã hóa khác. Việc nhập thông tin vào và việc xuất thông tin từ các hệ thống DLT sẽ được thuận lợi bởi các định dạng thông tin và ngữ nghĩa thông tin chung. Điều này cũng đúng khi hoạt động liên tác như một phần của sự trao đổi thông tin trong chuỗi cung ứng.

Tính liên tác phải được phân biệt với tính di động, tính có thể thay thế cho nhau hoặc tính đồng dạng. Tính di động hàm ý khả năng di chuyển các ứng dụng hoặc thông tin từ hệ thống này sang hệ thống khác, thay vì trao đổi thông tin. Tính có thể thay thế cho nhau ngụ ý khả năng thay thế một hệ thống bằng một hệ thống khác để đáp ứng các yêu cầu giống nhau. Tính đồng dạng ngụ ý sự giống nhau của thiết kế. Tính liên tác tập trung vào trao đổi thông tin, nơi mà thông tin có thể được trao đổi hiệu quả để các hệ thống khác nhau có thể làm việc cùng nhau.

Có nhiều quan điểm khác nhau của tính liên tác cần được xem xét. Các quan điểm này được gọi là "phương diện" (facets). Có mô hình 5 phương diện, được mô tả chi tiết trong ISO/IEC 19941. Năm phương diện đó là:

1. Tính liên tác truyền tải (xem 3.23)

DLT thường được nghĩ đến như hoạt động trong môi trường dựa trên Internet; tuy nhiên, DLT cũng có thể hoạt động trong các môi trường mạng khác. Phương diện truyền tải liên quan đến hạ tầng truyền thông - cách thức lấy các byte dữ liệu từ hệ thống này sang hệ thống khác.

Điều này bao gồm phần cứng mạng: Ethernet, Wi-Fi, Băng thông rộng (xDSL), Vệ tinh, v.v. Nó cũng bao gồm giao thức truyền tải được sử dụng: HTTP(S), AMQP, MQTT, Kafka, v.v.

Nếu các phương diện truyền tải không tương thích, thì một vài hình thức chuyển đổi giao thức nào đó có thể sẽ được yêu cầu.

2. Tính liên tác cú pháp (xem 3.22)

Trọng tâm vào "cú pháp của dữ liệu". Lý tưởng nhất là cú pháp của dữ liệu phải giống nhau đối với dịch vụ nguồn và dịch vụ đích. Tuy nhiên, nếu cú pháp không khớp, ví dụ: nguồn sử dụng cú pháp JSON nhưng đích sử dụng XML, nó có thể ánh xạ dữ liệu bằng cách sử dụng các công cụ sẵn có phổ biến. Các môi trường EDI đã tận dụng nhiều cú pháp được tiêu chuẩn hóa.

3. Tính liên tác ngữ nghĩa dữ liệu (xem 3.20)

Ngữ nghĩa học liên quan đến các khái niệm trong một lĩnh vực, các thuộc tính, thuật ngữ, từ vựng và các mối quan hệ cấu trúc giữa chúng. Ngữ nghĩa học cũng liên quan đến tính chính xác tính hợp lệ và tính đầy đủ của dữ liệu.

Trọng tâm vào "ngữ nghĩa của dữ liệu". Ngữ nghĩa của dữ liệu thường được biểu diễn bằng một bản thể luận. Các bản thể luận tương thích giúp đơn giản hóa việc chuyển đổi dữ liệu giữa các dịch vụ nguồn và đích. Nếu các bản thể luận không tương thích, có thể áp dụng các nguồn lực bổ sung để phát hiện các điểm không nhất quán. Các điểm không nhất quán này có thể được giải quyết, hoặc các yêu cầu về tính liên tác ngữ nghĩa dữ liệu có thể được nới lỏng để cho phép dữ liệu được mang chuyển.

4. Tính liên tác hành vi (xem 3.3)

Cần phải đặc tả cách giao diện dịch vụ sử dụng dữ liệu được trao đổi cùng với các điều kiện và ràng buộc liên quan.

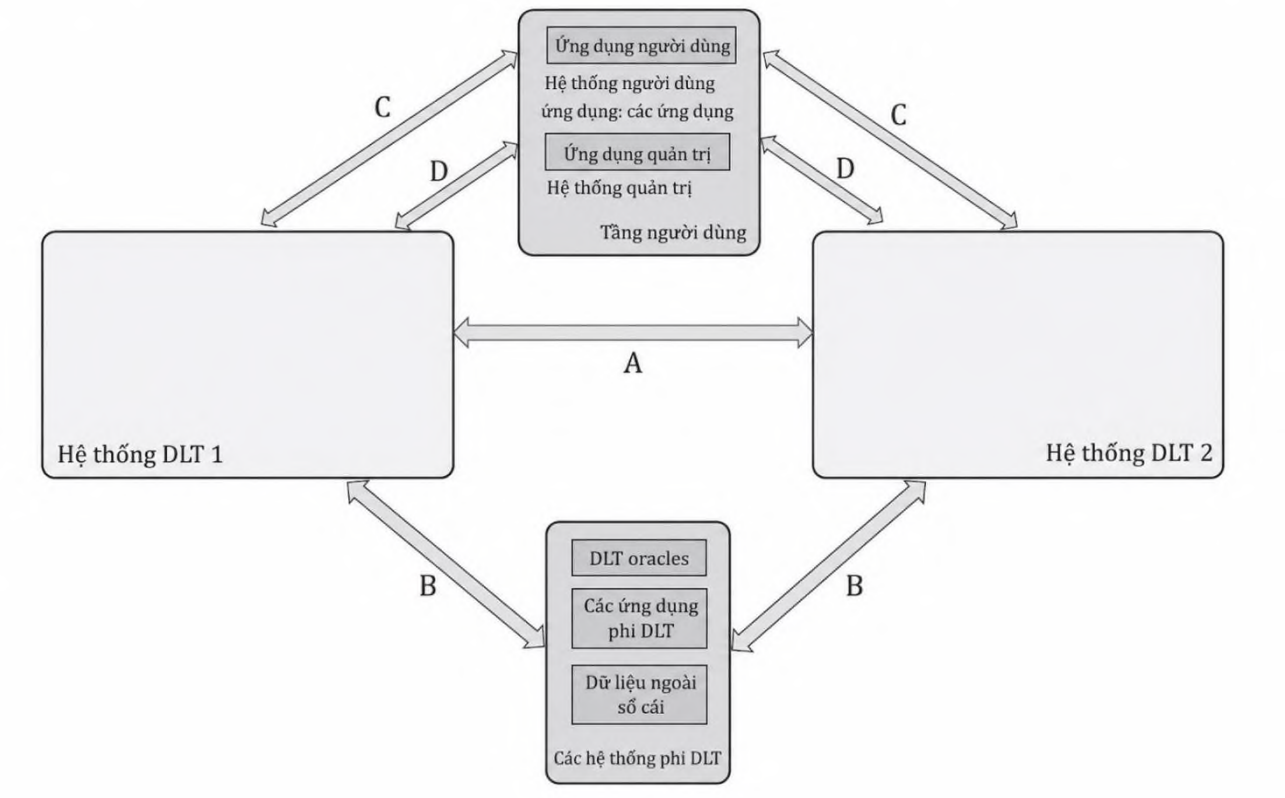
5. Tính liên tác chính sách () (xem 3.16)

Mô hình 5 phương diện cũng được sử dụng trong ISO/IEC 21823-1. Năm phương diện này áp dụng để hiểu về tính liên tác trong các hệ thống phân tán khắp nơi như hệ thống điện toán đám mây và hệ thống DLT.

Ngoài năm phương diện nêu trên, cần phải hiểu rõ các hệ thống hoặc ứng dụng nào có liên quan trong các hệ thống DLT - những thực thể nào đang giao tiếp và bản chất của sự giao tiếp đó là gì.

Khi xem xét tính liên tác đối với tài sản kỹ thuật số, điều quan trọng là phải đảm bảo khái niệm về các đặc tính kế thừa.

Khi xem xét tính liên tác, có 4 tương tác giữa các thực thể trong hệ thống DLT là có liên quan, như được minh họa trong Hình 2, trong đó các chi tiết về các thực thể hoàn toàn nằm trong nội bộ các hệ thống DLT đã được lược bỏ.



Hình 2 - Giao diện tính liên tác – Hệ thống người dùng DLT, hệ thống quản trị DLT

Hình 2 xác định bốn giao diện tiềm năng nơi tính liên tác có thể được áp dụng:

A - trực tiếp giữa 2 (hoặc nhiều hơn) hệ thống DLT;

B - giữa các hệ thống DLT và các hệ thống phi DLT bên ngoài;

C - giữa các ứng dụng người dùng và các hệ thống DLT;

D - giữa các ứng dụng quản trị và các hệ thống DLT.

Các ví dụ về tính liên tác giữa nhiều hệ thống bao gồm:

- Hệ thống 1 liên tác với Hệ thống 2 với một tập con các chức năng và thuộc tính chung của hai hệ thống;

- Hệ thống 2 và Hệ thống 3 liên tác với các chức năng và thuộc tính chung của hai hệ thống;

- Hệ thống 1 và Hệ thống 3 có thể liên tác với một tập con các chức năng và thuộc tính chung của ba hệ thống.

Sự khám phá DLT hỗ trợ tính liên tác giữa các hệ thống DLT. Sự khám phá bao gồm các hoạt động mà một hệ thống DLT thực hiện để chia sẻ thông tin về bản thân và chức năng của nó. Một hệ thống DLT có thể truyền đạt thông tin này - ví dụ thông qua một thư mục dịch vụ hoặc danh mục dịch vụ - đến các thực thể khác nhằm tạo thuận lợi cho sự tham gia của chúng hoặc để trao đổi dữ liệu và dịch vụ. Một Dịch vụ đặt tên sổ cái (LNS) tùy chọn có thể được triển khai trong một hệ thống DLT theo cách tương tự như Dịch vụ tên miền (DNS) được sử dụng trên Internet để xác định kết nối mạng của một dịch vụ sổ cái. Điều này có thể cho phép các ứng dụng liên sổ cái liên tác thuận tiện với nhau. Một quy ước đặt tên cũng có thể được tiêu chuẩn hóa. Các định nghĩa chi tiết cho các khái niệm và các mối quan hệ khả năng có thể khám phá là nằm ngoài phạm vi của tiêu chuẩn này.

Nó có thể là hữu ích để tạo thuận lợi cho tự động hóa quá trình làm các hệ thống DLT khác nhau có tính liên tác với nhau - thay vì phải tìm kiếm, đánh giá, kết nối và ánh xạ thông tin giữa các hệ thống theo cách thức riêng lẻ mỗi lần; một phương tiện cho phép các hệ thống DLT quảng bá thông tin khám phá của chúng để các hệ thống khác có thể xác định tính tương thích và mức độ phù hợp là điều có giá trị. Việc chuẩn hóa siêu dữ liệu có tính đến mô hình 5 phương diện có thể hữu ích để cho phép diễn giải thông tin khám phá.

Một số ví dụ về thông tin khám phá của hệ thống DLT có thể bao gồm: các quy trình và mục đích, thông tin và dịch vụ có thể được cung cấp hoặc tiêu thụ, bảo mật, đảm bảo, truy cập, chi phí, quảng bá, thông tin vận hành, yêu cầu quản trị, các đặc tính phi chức năng, các hạn chế về khu vực và pháp lý, và các thuộc tính hữu ích khác nhằm tạo thuận lợi cho tích hợp thủ công hoặc tự động.

Các kịch bản tích hợp khác nhau có thể yêu cầu các thông tin khác nhau trong quá trình khám phá, tích hợp hoặc tham gia, cụ thể là:

- các ứng dụng bên ngoài đang tìm kiếm để hiểu rõ các năng lực, yêu cầu và uy tín của các hệ thống và dịch vụ DLT hiện có với tư cách là người dùng; và

- các nút tiềm năng đang tìm kiếm sổ cái của một hệ thống DLT, trong đó các đối tác hiện có còn ít hơn và từ vựng chưa được thiết lập đầy đủ.

6.8 Luồng dữ liệu

Việc am hiểu luồng dữ liệu (xem 3.5) là thiết yếu để bảo vệ quyền riêng tư và tính bảo mật của dữ liệu trong các hệ thống DLT.

Trong một cấp độ hệ thống, các luồng dữ liệu của hệ thống DLT có thể được phân chia thành các luồng nội bộ và các luồng bên ngoài. Có năm luồng dữ liệu cơ bản liên quan đến các hệ thống DLT như được minh họa trong Hình 3:

- Luồng dữ liệu Z: dữ liệu lưu chuyển giữa các nút trong hệ thống DLT;

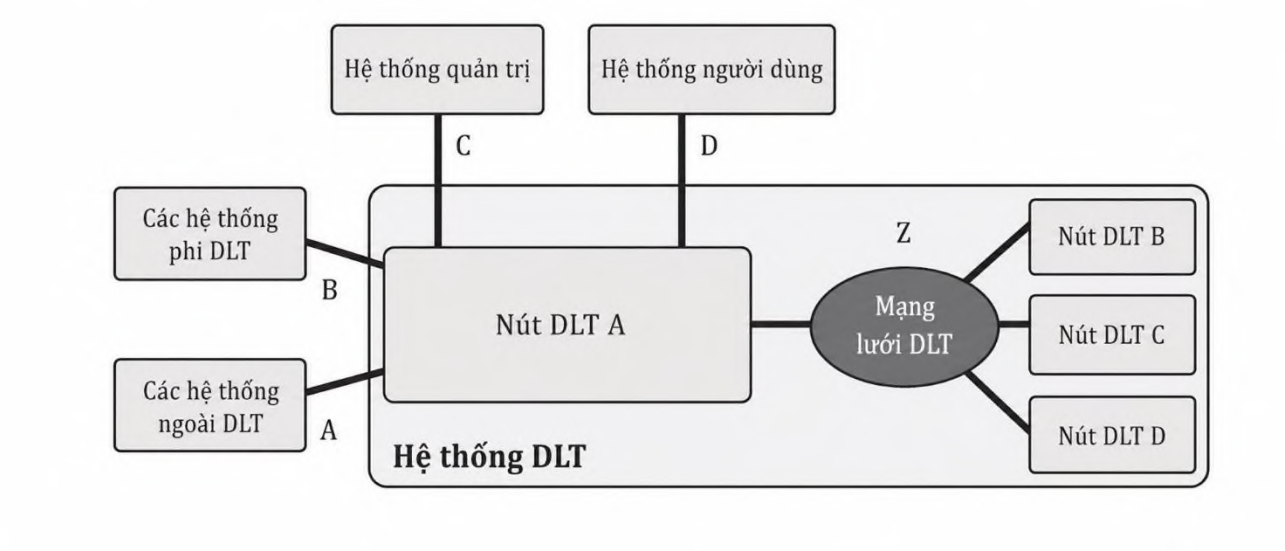
- Luồng dữ liệu A: dữ liệu lưu chuyển giữa hai hệ thống DLT riêng biệt khi chúng liên tác với nhau;

- Luồng dữ liệu B: dữ liệu lưu chuyển giữa một hệ thống DLT và các hệ thống phi DLT được kết nối với nó;

- Luồng dữ liệu C: dữ liệu lưu chuyển giữa các ứng dụng quản trị và một hệ thống DLT;

- Luồng dữ liệu D: dữ liệu lưu chuyển giữa các ứng dụng người dùng và một hệ thống DLT.

Tuy nhiên, các luồng dữ liệu trong các ứng dụng thực tế thường phức tạp và khó am hiểu. Các luồng dữ liệu trong các hệ thống DLT thường được khởi phát bởi các thao tác liên quan đến dữ liệu của các bên liên quan. Cụ thể, dữ liệu DLT có thể lưu chuyển giữa các hệ thống thuộc về hoặc có liên quan đến các bên liên quan khác nhau. Bên cạnh đó, việc sử dụng các thiết bị là phổ biến trong các hệ thống DLT, bao gồm nhiều loại thiết bị khác nhau như thiết bị di động và thiết bị IoT. Ngoài ra, trong một số trường hợp, các dịch vụ điện toán đám mây được sử dụng để cung cấp các khả năng như lưu trữ, điều này làm cho các luồng dữ liệu trong các hệ thống DLT trở nên phức tạp hơn.



Hình 3 – Dòng dữ liệu DLT

7 Các loại hệ thống DLT

Sự phân biệt giữa các hệ thống DLT công khai và các hệ thống DLT riêng tư là về việc ai có thể đọc các bản ghi giao dịch trên sổ cái. Một hệ thống DLT công khai có các bản ghi giao dịch có thể được đọc bởi bất kỳ ai (tức là bởi công chúng nói chung). Ngược lại, một hệ thống DLT riêng tư có các bản ghi giao dịch không thể được đọc bởi bất kỳ ai - quyền truy cập đọc vào các bản ghi giao dịch bị giới hạn một cách có chủ đích - các bản ghi là riêng tư ở mức độ quyền truy cập đọc được giới hạn ở một nhóm cụ thể nào đó.

Chỉ quyền truy cập đọc vào các bản ghi giao dịch mới được đề cập ở đây. Nó có thể là trường hợp bổ sung các bản ghi giao dịch vào sổ cái cũng được mở cho tất cả, hoặc cũng có thể là việc bổ sung các bản ghi giao dịch vào sổ cái bị giới hạn vài nhóm cụ thể nào đó. Cả hai khả năng đều có thể xảy ra đối với các hệ thống DLT công khai.

Các cụm từ "hệ thống DLT không cấp phép" và "hệ thống DLT có cấp phép" liên quan đến việc liệu có cần thiết phải có quyền để sử dụng hệ thống hay không (sự cho phép hàm ý một hình thức xác thực và ủy quyền nào đó đối với người dùng liên quan). Một hệ thống DLT không cấp phép không yêu cầu sự cho phép để sử dụng hoặc vận hành hệ thống. Một hệ thống DLT cần cấp phép yêu cầu sự cho phép để thực hiện một số thao tác nhất định của hệ thống. Các thao tác ở đây bao gồm các chức năng DLT cơ bản như đọc bản ghi giao dịch, bổ sung bản ghi giao dịch và xác thực bản ghi giao dịch.

Có bốn tổ hợp của các khái niệm này cần được hiểu rõ:

1. Hệ thống DLT công khai không cần cấp phép (public permissionless DLT system)

Đây là hệ thống DLT mở cho bất kỳ ai sử dụng và không yêu cầu sự cho phép để thực hiện bất kỳ thao tác nào trên hệ thống, bao gồm cả việc tham gia vào các cơ chế đồng thuận và xác thực các giao dịch. Đây là một trong những trường hợp điển hình của chuỗi khối - Bitcoin và Ethereum là các ví dụ điển hình.

2. Hệ thống DLT công khai cần cấp phép (public permissioned DLT system)

Đây thường là trường hợp quyền truy cập đọc vào các bản ghi giao dịch được mở cho bất kỳ ai, nhưng các thao tác khác trên hệ thống yêu cầu sự cho phép ở một mức độ nào đó - ví dụ: bất kỳ ai cũng có thể đọc nhưng chỉ những người cụ thể mới có thể bổ sung bản ghi giao dịch. Một ví dụ về hệ thống DLT như vậy là hệ thống cho phép người tiêu dùng xác minh nguồn gốc xuất xứ của các mặt hàng thực phẩm - họ có thể đọc các bản ghi giao dịch về lịch sử của mặt hàng từ trang trại đến bàn ăn, nhưng chỉ những người như nông dân, công ty vận chuyển, v.v. mới được phép tạo ra các bản ghi giao dịch đó.

3. Hệ thống DLT riêng tư cần cấp phép (private permissioned DLT system)

Đây là trường hợp điển hình và phổ biến, trong đó tất cả các thao tác trên hệ thống DLT đều bị giới hạn ở các nhóm cụ thể và yêu cầu sự cho phép để thực hiện bất kỳ thao tác nào trên hệ thống, kể cả việc đọc bản ghi giao dịch. DLT có cấp quyền có thể đảm bảo khả năng hiển thị đối với những chủ sở hữu khác nhau của các nút vận hành mạng DLT. Các trường hợp như vậy có thể được xử lý bằng cách sử dụng các hệ thống DLT mã nguồn mở cần cấp phép. Hyperledger Fabric là một ví dụ về hệ thống DLT riêng tư cần cấp phép.

4. Hệ thống DLT riêng tư không cần cấp phép (private permissionless DLT system)

Trong trường hợp này, các thao tác trên hệ thống DLT bị giới hạn ở các nhóm cụ thể, nhưng không yêu cầu sự cho phép để thực hiện các thao tác đó - điều này có thể được thực hiện bằng cách sử dụng các phương tiện khác để hạn chế sự tham gia, chẳng hạn như cài đặt hệ thống DLT trên một mạng riêng tư.

8 Các cân nhắc kiến trúc đối với hệ thống DLT

8.1 Các đặc tính và mối quan hệ

Để hiểu rõ các hệ thống DLT, việc xác định một tập hợp giới hạn các đặc tính và hiểu rõ các mối quan hệ giữa chúng với nhau như được thể hiện trong [Bảng 1] là điều hữu ích. Các công nghệ được phân loại theo bốn đặc tính sau:

- kiến trúc lưu trữ sổ cái (ledger storage architecture);

- kiến trúc điều khiển sổ cái (ledger control architecture);

- phân tập sổ cái (ledger subsetting);

- quyền truy cập sổ cái (ledger permissions).

Rất ít giải pháp sẽ tồn tại hoàn toàn "trên chuỗi" (on-chain), vì vậy việc nhận biết các thành phần bao quanh sổ cái trong một giải pháp đầu cuối (end-to-end solution) cũng là điều quan trọng. Một

sổ cái được triển khai trên hạ tầng - cơ sở tính toán, mạng và lưu trữ cần được thiết lập để xử lý việc tiếp nhận các thông điệp. Trong một số hệ thống, một số loại dữ liệu nhất định như dữ liệu phương tiện (hình ảnh, video, âm thanh) không được đưa lên sổ cái mà thay vào đó được lưu trong kho lưu trữ riêng biệt. Một số dữ liệu khác có thể không phù hợp để đưa lên sổ cái vì các dữ liệu đó, ví dụ như thông tin nhận dạng cá nhân (PII), chịu sự điều chỉnh của các quy định bảo vệ dữ liệu, chẳng hạn như GDPR của Liên minh Châu Âu, và trong trường hợp này, tính bất biến cùng tính minh bạch được coi là những yếu tố bất lợi. Do đó, loại dữ liệu này thường sẽ được lưu trữ trong kho dữ liệu ngoài sổ cái (off-ledger data store).

Trong bối cảnh các hệ thống DLT, kiến trúc lưu trữ (storage architecture) khác với kiến trúc kiểm soát (control architecture) (ví dụ: cơ chế đồng thuận), và lưu trữ sổ cái (ledger storage) khác với lưu trữ nội dung dữ liệu (data content storage) (ví dụ: dữ liệu phương tiện). Do đó, các đặc tính liên quan đến kiến trúc lưu trữ sổ cái và kiến trúc điều khiển sổ cái có thể được tách biệt như sau.

CHÚ THÍCH - Các công nghệ sổ cái tập trung được đưa vào Bảng 1 và các mục tiếp theo nhằm mục đích đầy đủ và dễ hiểu. Các hệ thống sổ cái tập trung nằm ngoài phạm vi của tài liệu này.

Bảng 1 - Loại hình hệ thống DLT dựa trên một tập hợp giới hạn các đặc tính

Công nghệ sổ cái	**Kiến trúc lưu trữ sổ cái**	**Kiến trúc điều khiển sổ cái**	**Phân tập sổ cái**	**Quyền truy cập sổ cái**
Công nghệ sổ cái tập trung *(tức là sổ cái truyền thống)*	Kiến trúc (lưu trữ sổ cái) tập trung *(tức là lưu trữ tập trung)*	Kiến trúc (điều khiển sổ cái) tập trung *(tức là kiểm soát tập trung)*	**Bản sao đầy đủ của sổ cái** *(tức là sao chép toàn bộ)*	**Không cấp quyền** hoặc **có cấp quyền**
Công nghệ sổ cái phân tán (DLT)	Kiến trúc (lưu trữ sổ cái) phân tán *(tức là lưu trữ phân tán)*	Kiến trúc (điều khiển sổ cái) phi tập trung *(tức là kiểm soát phi tập trung, dựa trên cơ chế đồng thuận)*	**Tập con của sổ cái** *(tức là bản sao một phần)*	
			Bản sao đầy đủ của sổ cái	

Hiệu suất giao dịch là một yếu tố then chốt và bị ảnh hưởng trực tiếp bởi kiến trúc của mạng.

8.2 Công nghệ sổ cái

Các công nghệ sổ cái được thiết kế để hỗ trợ và triển khai các sổ cái. Chúng có thể là tập trung hoặc phân tán.

8.3 Kiến trúc lưu trữ sổ cái

Kiến trúc lưu trữ sổ cái có thể là:

- Kiến trúc (lưu trữ sổ cái) tập trung: có một máy chủ trung tâm (bộ môi giới) lưu trữ một phiên bản đầy đủ và duy nhất của sổ cái;

- Kiến trúc (lưu trữ sổ cái) phân tán: là kiến trúc trong đó mỗi nút có thể lưu trữ một bản sao đầy đủ hoặc một phần của sổ cái phân tán.

8.4 Kiến trúc điều khiển sổ cái

Kiến trúc điều khiển sổ cái có thể là:

- Kiến trúc (điều khiển sổ cái) tập trung: là kiến trúc trong đó một thực thể trung tâm duy nhất (máy chủ hoặc cơ quan có thẩm quyền) kiểm soát việc ra quyết định liên quan đến sổ cái phân tán, tức là việc xác thực các khối bản ghi mới;

- Kiến trúc (điều khiển sổ cái) phân tán: là kiến trúc trong đó tất cả các thành phần kiến trúc - đặc biệt là các nút trong hệ thống DLT - kiểm soát việc ra quyết định liên quan đến sổ cái phân tán, dựa trên cơ chế đồng thuận được vận hành bởi hệ thống phân tán (xem ISO 22739:2020, 3.32);

- Kiến trúc (điều khiển sổ cái) phi tập trung: là kiến trúc trong đó nhiều nút (hoặc cơ quan có thẩm quyền) trong hệ thống DLT kiểm soát việc ra quyết định liên quan đến sổ cái phân tán, dựa trên cơ chế đồng thuận vận hành như một hệ thống phi tập trung (xem ISO 22739:2020, 3.19).

Điều khiển sổ cái được liên kết với cơ chế/mô hình đồng thuận sổ cái. Cơ chế/mô hình này có thể được mô tả trong phần mềm lõi DLT (DLT core software) hoặc phần mềm máy khách DLT (DLT client software).

8.5 Phân tập sổ cái

Trong bối cảnh các hệ thống DLT, phân tập sổ cái có thể là:

- tập con của sổ cái, tức là bản sao một phần;

- toàn bộ sổ cái, tức là bản sao đầy đủ.

8.6 Sự cho phép sổ cái

Các loại sự cho phép được áp dụng cho sổ cái là không cần cấp phép hoặc cần cấp phép.

9 Các góc nhìn kiến trúc của kiến trúc tham chiếu

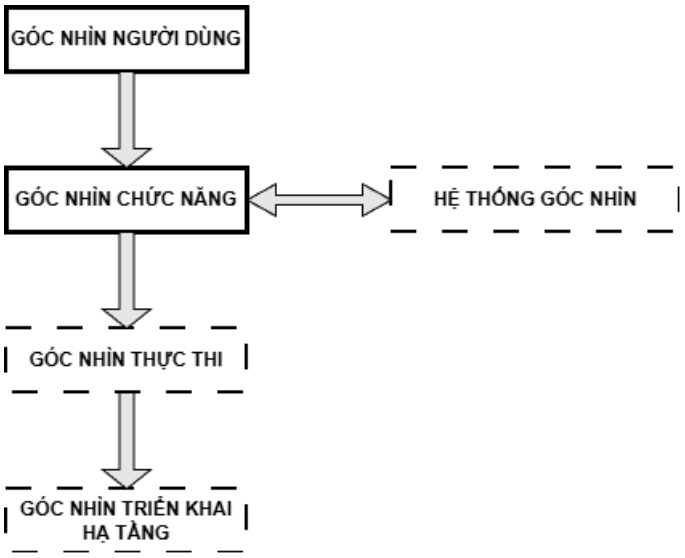
9.1 Tổng quan

9.1.1 Năm góc nhìn kiến trúc

Các hệ thống DLT có thể được mô tả bằng phương pháp tiếp cận dựa trên các góc nhìn. Có năm góc nhìn riêng biệt có thể được sử dụng để mô tả một kiến trúc tham chiếu, bao gồm:

- Góc nhìn người dùng (User view);
- Góc nhìn chức năng (Functional view);
- Góc nhìn hệ thống (System view);
- Góc nhìn thực thi (Implementation view);
- Góc nhìn triển khai hạ tầng (Deployment view).

Hình 4 minh họa các khả năng chuyển đổi giữa các góc nhìn này, và Bảng 2 cung cấp mô tả cho từng góc nhìn.



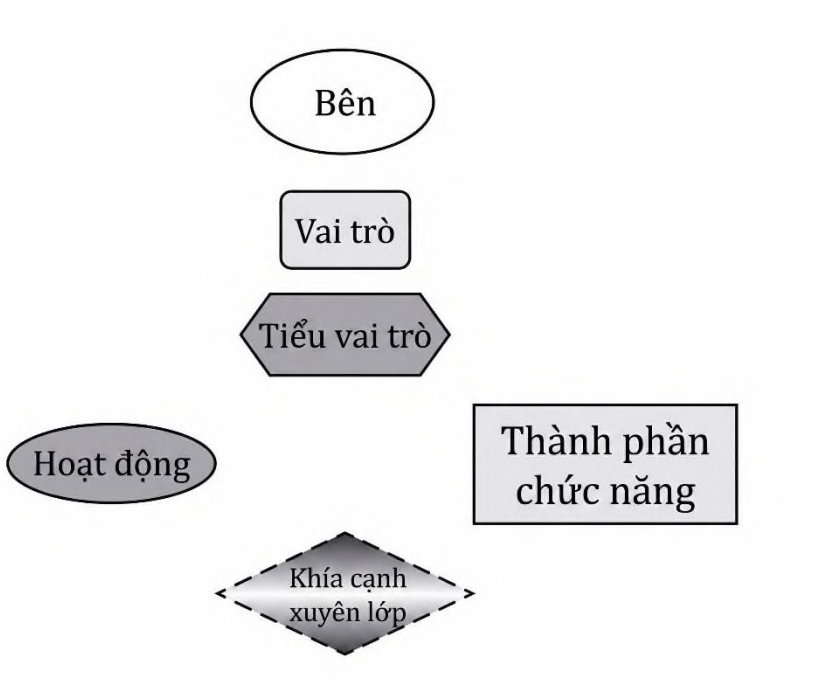
Hình 4: Sự chuyển đổi giữa các góc nhìn kiến trúc

Bảng 2- Các góc nhìn kiến trúc tham chiếu

Góc nhìn kiến trúc tham chiếu (RA)	Mô tả góc nhìn kiến trúc tham chiếu
Góc nhìn người dùng (*User view*)	Bối cảnh hệ thống, các bên liên quan, các vai trò, các tiểu vai trò và các hoạt động của hệ thống DLT
Góc nhìn chức năng (*Functional view*)	Các chức năng cần thiết để hỗ trợ các hoạt động của hệ thống DLT
Góc nhìn hệ thống (*System view*)	Góc nhìn thay thế của góc nhìn chức năng, nhấn mạnh các mối quan hệ giữa các thành phần khác nhau và vị trí tương đối của chúng trong hệ thống
Góc nhìn thực thi (*Implementation view*) [a]	Các chức năng cần thiết để triển khai hệ thống DLT trong các phần dịch vụ và/hoặc các phần hạ tầng
Góc nhìn triển khai (*Deployment view*) [a]	Cách thức các chức năng của DLT được triển khai về mặt kỹ thuật trong các thành phần hạ tầng hiện có hoặc trong các thành phần mới được đưa vào hạ tầng đó
[a] Góc nhìn thực thi và góc nhìn triển khai nằm ngoài phạm vi của tài liệu này.	

9.1.2 Ký hiệu của các sơ đồ

Các quy ước sau đây được áp dụng. Các sơ đồ được sử dụng xuyên suốt tài liệu này nhằm giúp minh họa kiến trúc tham chiếu. Hình 5 cung cấp các quy ước được sử dụng liên quan đến nội dung của các sơ đồ.



CHÚ THÍCH: "Khía cạnh" (Aspect) được hiểu là tham chiếu đến khía cạnh xuyên lớp (Cross-cutting aspect).

Hình 5: Chú giải các sơ đồ sử dụng trong tài liệu

Kiến trúc tham chiếu trong Tiêu chuẩn này sử dụng thuật ngữ ICT và hệ thống ICT. Thuật ngữ này được sử dụng nhằm làm rõ rằng kiến trúc tham chiếu bao phủ không chỉ các công nghệ tính toán và lưu trữ liên quan đến hệ thống máy tính, mà còn cả các mạng truyền thông liên kết các hệ thống với nhau.

Các bên liên quan trong một hệ thống DLT là các bên có lợi ích liên quan (stakeholders) của hệ thống đó. Một bên có thể đảm nhận nhiều hơn một vai trò tại bất kỳ thời điểm nào và có thể tham gia vào một tập con cụ thể các hoạt động của vai trò đó. Ví dụ về các bên bao gồm, nhưng không giới hạn ở, các cá nhân, doanh nghiệp và cơ quan chính phủ.
Các tiểu vai trò (sub-roles) khác nhau có thể chia sẻ các hoạt động DLT liên quan đến một vai trò nhất định. Mô tả về các vai trò và tiểu vai trò DLT được cung cấp tại 9.2.

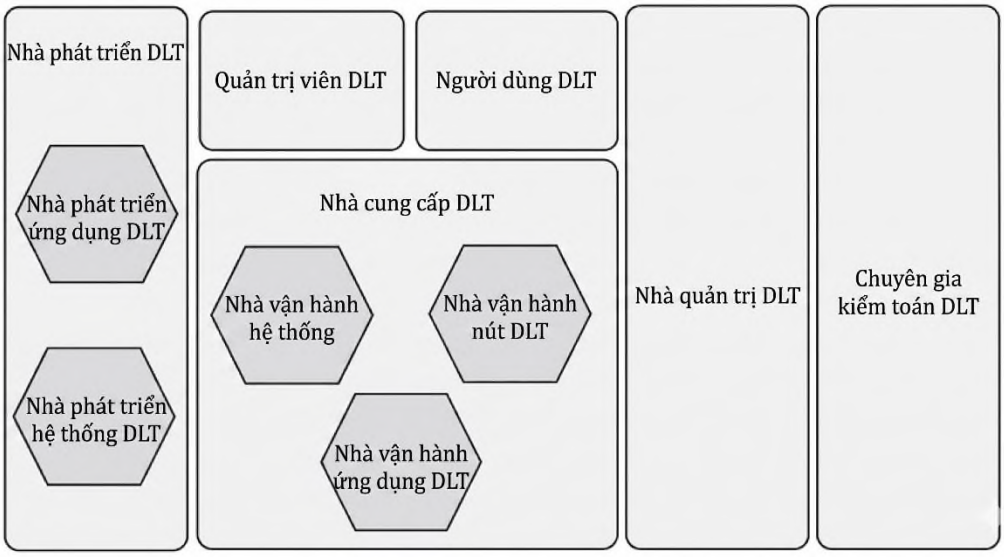
9.2 Góc nhìn người dùng

9.2.1 Tổng quan

Tiêu chuẩn này mô tả một tập hợp các vai trò và tiểu vai trò nhằm giải quyết các hoạt động chính gắn liền với hệ thống DLT. Như được thể hiện trong Hình 6, các vai trò và tiểu vai trò của hệ thống DLT bao gồm:

- người dùng DLT
- quản trị viên DLT
- nhà cung cấp DLT:
  - nhà vận hành hệ thống DLT
  - nhà vận hành nút DLT
  - nhà vận hành ứng dụng DLT
- Nhà phát triển DLT:

  - nhà phát triển ứng dụng DLT (cho người dùng DLT và nhà cung cấp DLT)
  - nhà phát triển hệ thống DLT (cho nhà cung cấp DLT)
- nhà quản lý DLT
- chuyên gia kiểm toán DLT



Hình 6 – Hệ thống các vai trò và các tiểu vai trò DLT

Để xác định ranh giới trách nhiệm trong một hệ thống DLT, cần hiểu không chỉ vai trò và tiểu vai trò mà còn cả các hoạt động một cách chi tiết. Mỗi hoạt động được trình bày trong tiểu mục tương ứng của vai trò và tiểu vai trò. Không phải tất cả các vai trò/tiểu vai trò này đều nhất thiết tồn tại trong mọi hệ thống DLT.

Điều quan trọng cần lưu ý là trong một số trường hợp, một cá nhân hoặc một tổ chức có thể đảm nhận nhiều vai trò/tiểu vai trò. Cũng có thể xảy ra trường hợp các vai trò/tiểu vai trò khác nhau được phân chia giữa các tổ chức khác nhau.

CHÚ THÍCH: Tất cả các hoạt động cần được thực hiện trên cơ sở bảo vệ quyền riêng tư.

9.2.2 Người dùng DLT

Người dùng DLT là vai trò sử dụng giải pháp DLT. Vai trò này có thể đại diện cho một cá nhân, một tổ chức, một thiết bị hoặc một hệ thống.
Thông thường, người dùng DLT sử dụng hệ thống DLT thông qua ứng dụng DLT hoặc mã nguồn ngoài sổ cái tương tác với API DLT, thay vì tương tác trực tiếp với nút DLT. Điều này đúng với người dùng DLT là các hệ thống tự động thay vì người dùng là con người trong đó sự tương tác thường diễn ra thông qua API do ứng dụng DLT cung cấp.
Các hoạt động bao gồm:

- sử dụng các ứng dụng người dùng DLT: tương tác phù hợp với các hệ thống nghiệp vụ;
- cài đặt ứng dụng người dùng;
- cấu hình các ứng dụng người dùng DLT;
- cài đặt máy khách hoặc ứng dụng để tương tác với hệ thống DLT;
- xử lý các ngoại lệ hoặc sự cố.

9.2.3 Quản trị viên DLT

Quản trị viên DLT thực hiện các hoạt động quản trị cụ thể, đặc biệt là trong lĩnh vực cấu hình bảo mật. Phạm vi của các quản trị viên sẽ khác nhau trong các hệ thống và các mạng khác nhau - một số chỉ giới hạn ở các nút DLT và một số khác có thể hoạt động ở mức các giải pháp DLT.
Các hoạt động bao gồm:

- quản lý chính sách bảo mật;
- quản lý khóa mật mã;
- xử lý các ngoại lệ;
- cài đặt các ứng dụng người dùng;
- cấu hình các ứng dụng người dùng DLT và các ứng dụng quản trị;
- quản lý các kiểm soát truy cập dựa trên vai trò đối với việc tạo, triển khai và gọi các hợp đồng thông minh.

9.2.4 Nhà cung cấp DLT

9.2.4.1 Tổng quan

Nhà cung cấp DLT đóng vai trò có thể sở hữu và vận hành một hoặc nhiều nút trong các hệ thống DLT và các mạng DLT. Các nhà cung cấp DLT đồng ý tạo/khởi tạo các nút, tham gia các mạng, chi trả và xử lý các thỏa thuận pháp lý để tham gia mạng. Đây là vai trò của bên có lợi ích kinh doanh liên quan.

Các tiểu vai trò bao gồm:

- nhà vận hành hệ thống DLT;
- nhà vận hành nút DLT;
- nhà vận hành ứng dụng DLT.

9.2.4.2 Nhà vận hành hệ thống DLT

Nhà vận hành hệ thống DLT đóng vai trò quản lý và vận hành các hệ thống vật lý và ảo cùng các mạng lưu trữ và chạy các thành phần của các hệ thống DLT và các nền tảng DLT tại các nút DLT. Vai trò này xử lý các kết nối mạng và các kết nối nhiều nút, đảm bảo tính liên tác giữa các nút và thực thi các chính sách giữa các nút.

Các hoạt động bao gồm:

- quản lý các mạng truyền thông cho hệ thống DLT;
- triển khai các hệ thống vật lý và ảo hóa;
- thiết lập các môi trường và quy trình.

9.2.4.3 Nhà vận hành nút DLT

Nhà vận hành nút DLT đóng vai trò quản lý và vận hành một hoặc nhiều nút trong hệ thống DLT cho nhà cung cấp DLT. Các nhà vận hành nút chịu trách nhiệm về vòng đời của nút, có thể bao gồm các trách nhiệm kinh doanh, chuẩn bị triển khai, vận hành các nút, quản lý và bảo trì các nút.

Các hoạt động bao gồm:

- xử lý các vấn đề kinh doanh, bao gồm các quan hệ khách hàng và các quy trình tài chính, cùng các thống kê kinh doanh;

- chuẩn bị triển khai, bao gồm xác định các quy trình triển khai, thiết kế các cơ chế đảm bảo tính liên tục của hệ thống và lựa chọn các yêu cầu kiểm toán;
- vận hành và khai thác, bao gồm chuẩn bị các hệ thống, thực hiện các quy trình triển khai, vận hành các sổ cái, các hợp đồng thông minh và các cơ chế đồng thuận trong các môi trường thực thi an toàn, thực hiện tính liên tục của hệ thống và đáp ứng các yêu cầu của người dùng;
- quản lý, bảo mật và điều hành, bao gồm vận hành và giám sát các hệ thống, khôi phục các nút, quản lý các tài sản và quản lý bảo mật và rủi ro;
- duy trì việc cập nhật phù hợp cho các hệ thống DLT.

CHÚ THÍCH: Nhà vận hành có thể nhận chỉ đạo từ cơ quan quản lý nhà nước hoặc các nhà quản trị tùy theo phạm vi.

9.2.4.4 Nhà vận hành ứng dụng DLT

Nhà vận hành ứng dụng DLT là vai trò quản lý, sở hữu, vận hành và bảo trì các hệ thống ứng dụng DLT để cung cấp các dịch vụ DLT cho người dùng DLT, một cách trực tiếp hoặc gián tiếp. Nhà vận hành ứng dụng DLT có thể cung cấp các dịch vụ DLT bằng cách sở hữu hoặc vận hành một nút DLT, hoặc có thể cung cấp các dịch vụ nghiệp vụ DLT thông qua các dịch vụ do chủ sở hữu nút DLT cung cấp.

Các hoạt động bao gồm:

- cung cấp, giám sát và quản lý các dịch vụ nghiệp vụ DLT;

- quản lý kinh doanh;

- bảo vệ quyền riêng tư;

- quản lý bảo mật và rủi ro;

- thu thập các báo cáo kiểm toán;

- xử lý sự cố;

- đảm bảo tuân thủ.

9.2.5 Những nhà phát triển DLT

9.2.5.1 Tổng quan

Nhà phát triển DLT là vai trò tạo ra và duy trì mã nguồn và thiết bị chuyên dụng cho bất kỳ bộ phận hoặc thực thi nào của các hệ thống DLT hoặc các ứng dụng DLT. Nhà phát triển DLT có hai tiểu vai trò:

- nhà phát triển ứng dụng DLT;

- nhà phát triển hệ thống DLT.

9.2.5.2 Những nhà phát triển ứng dụng DLT

Nhà phát triển ứng dụng DLT là vai trò tạo ra và duy trì các ứng dụng DLT và các hợp đồng thông minh hoạt động kết hợp với các hệ thống DLT. Vai trò này cũng có thể bao gồm các ứng dụng chạy bên ngoài các nút của hệ thống DLT, tương tác với chúng thông qua API người dùng do các nút

cung cấp. Các ứng dụng DLT có thể được sử dụng, lưu trữ và vận hành bởi người dùng DLT hoặc các nhà cung cấp DLT.

Việc phát triển các hợp đồng thông minh đôi khi đòi hỏi các công cụ và kỹ năng đặc biệt, vì hợp đồng thông minh thường đại diện cho một quy trình nghiệp vụ có thể đơn giản như một giao dịch cơ bản giữa hai bên đến các kịch bản phức tạp trong các lĩnh vực như dịch vụ tài chính hay chuỗi cung ứng. Điều quan trọng là chỉ các hợp đồng thông minh tuân theo các luồng quy trình nghiệp vụ đã được phê duyệt mới được phép triển khai lên ngăn xếp DLT trong một môi trường nhất định. Các phương thức trong các hợp đồng thông minh này đại diện cho các hành động có thể được thực hiện trong phạm vi hợp đồng bởi các danh tính/định danh được gán cho các vai trò đặc thù theo lĩnh vực, ví dụ: các chủ sở hữu, các người mua, v.v. Các tổ chức có thể chỉ cho phép một số danh tính/định danh nhất định được triển khai các ứng dụng và các thể hiện mới của hợp đồng thông minh lên các thực thi sổ cái của họ. Việc tạo hợp đồng thông minh có thể được quản trị ở cấp độ ứng dụng, cấp độ nền tảng DLT hoặc cấp độ hợp đồng thông minh. Các nhà phát triển ứng dụng DLT và hợp đồng thông minh cần tính đến các vai trò và các yêu cầu truy cập liên quan đến chúng.

Các hoạt động bao gồm:

- thiết kế, tạo ra, tích hợp và duy trì các hệ thống nghiệp vụ dựa trên các hệ thống DLT;

- thiết kế, tạo ra và duy trì các thành phần hoặc các hợp đồng thông minh trong các hệ thống DLT.

9.2.5.3 Nhà phát triển hệ thống DLT

Nhà phát triển hệ thống DLT đảm nhận các vai trò phát triển các hệ thống vật lý và ảo hóa lưu trữ và chạy các thành phần của các hệ thống DLT và các nền tảng DLT tại các nút DLT.

Các hoạt động bao gồm:

- phát triển các thành phần nền tảng DLT;

- kiểm thử các thành phần của các hệ thống DLT cho các nhà vận hành nút và những người dùng nút.

9.2.6 Nhà quản trị DLT

Các nhà quản trị DLT chịu trách nhiệm quản trị toàn bộ các hệ thống DLT và các mạng DLT, nhưng không nhất thiết là toàn bộ giải pháp DLT. Các hệ thống DLT có thể được xem như hạ tầng, trong khi các giải pháp DLT được xây dựng trên đó được xem như các ứng dụng nghiệp vụ. Cả hai đều có các cơ chế quản trị riêng, nhưng có thể và thông thường do các cơ quan quản trị khác nhau thực hiện. Quản trị các hệ thống phi tập trung có thể đòi hỏi các cấu trúc quản trị mới và có thể thay đổi theo thời gian. Trong một số hệ thống DLT, quản trị không do một cơ quan quản trị duy nhất thực hiện, mà thay vào đó do một tập hợp các bên liên quan cùng thực hiện. Cần có một vai trò quản trị toàn bộ các hệ thống DLT và duy trì khả năng hoàn thành các mục tiêu mà các hệ thống DLT được thiết lập để phục vụ.

Các hoạt động bao gồm:

- xây dựng các chính sách DLT có tính đến các luật và các quy định áp dụng;

- trao đổi các chính sách với các bên có lợi ích liên quan;

- giải quyết các xung đột và quản lý các thay đổi;

- xác định các chính sách cho các cơ chế đồng thuận;

- xác định các chính sách cho các nút được phép tham gia vào các mạng DLT, bao gồm các yêu cầu bảo mật tối thiểu;

- làm việc với các nhà cung cấp DLT;

- làm việc với các nhà vận hành nút DLT để đảm bảo việc giám sát và quản trị được thực thi.

9.2.7 Chuyên gia kiểm toán DLT

Các chuyên gia kiểm toán DLT đảm bảo rằng các chính sách, quản trị và các quy định được tuân thủ trong các hệ thống DLT. Họ có thể làm việc với các nhà vận hành, các cơ quan quản lý nhà nước, các nhà quản trị, v.v..

Các hoạt động bao gồm:

- thu thập các bằng chứng phục vụ kiểm toán nhằm đáp ứng các yêu cầu, các tiêu chí, các khung quy định hoặc các phương án được lựa chọn;

- thực hiện kiểm toán các hệ thống DLT và các ứng dụng DLT;

- báo cáo các kết quả kiểm toán.

CHÚ THÍCH 1: Các hoạt động liên quan đến kiểm toán cần được thực hiện trên cơ sở bảo vệ quyền riêng tư.

CHÚ THÍCH 2: Có nhiều loại kiểm toán, tùy chọn và bắt buộc, có thể được áp dụng ở đây.

9.3 Góc nhìn chức năng

9.3.1 Khung phân loại chức năng

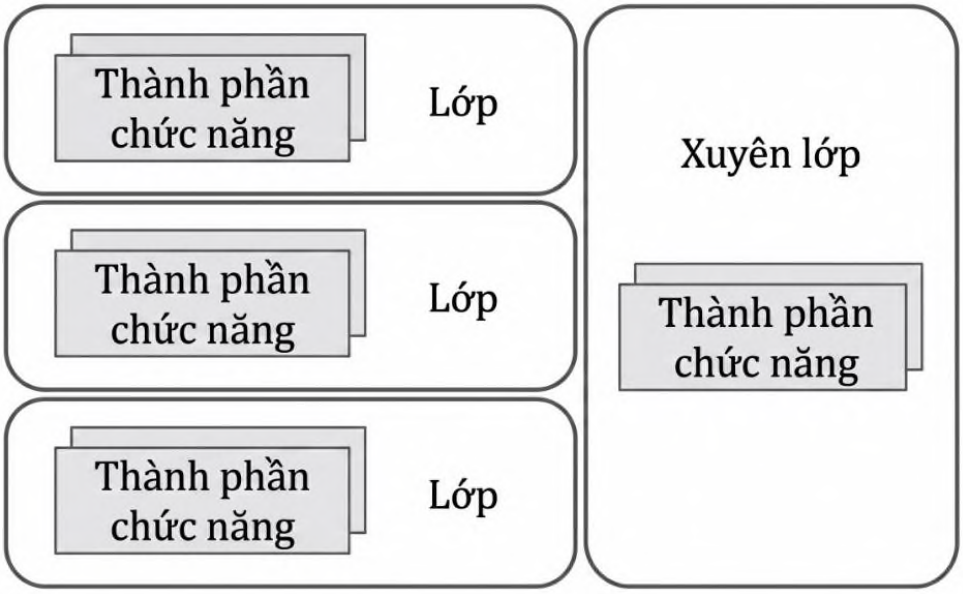
Góc nhìn chức năng là góc nhìn trung lập về công nghệ đối với các chức năng cần thiết để cấu thành một hệ thống DLT. Góc nhìn chức năng mô tả sự phân bổ các chức năng cần thiết để hỗ trợ các hoạt động trong các hệ thống DLT. Kiến trúc chức năng cũng xác định các quan hệ phụ thuộc giữa các chức năng. Góc nhìn chức năng đề cập đến các khái niệm sau của hệ thống DLT:

- các thành phần chức năng (functional components);

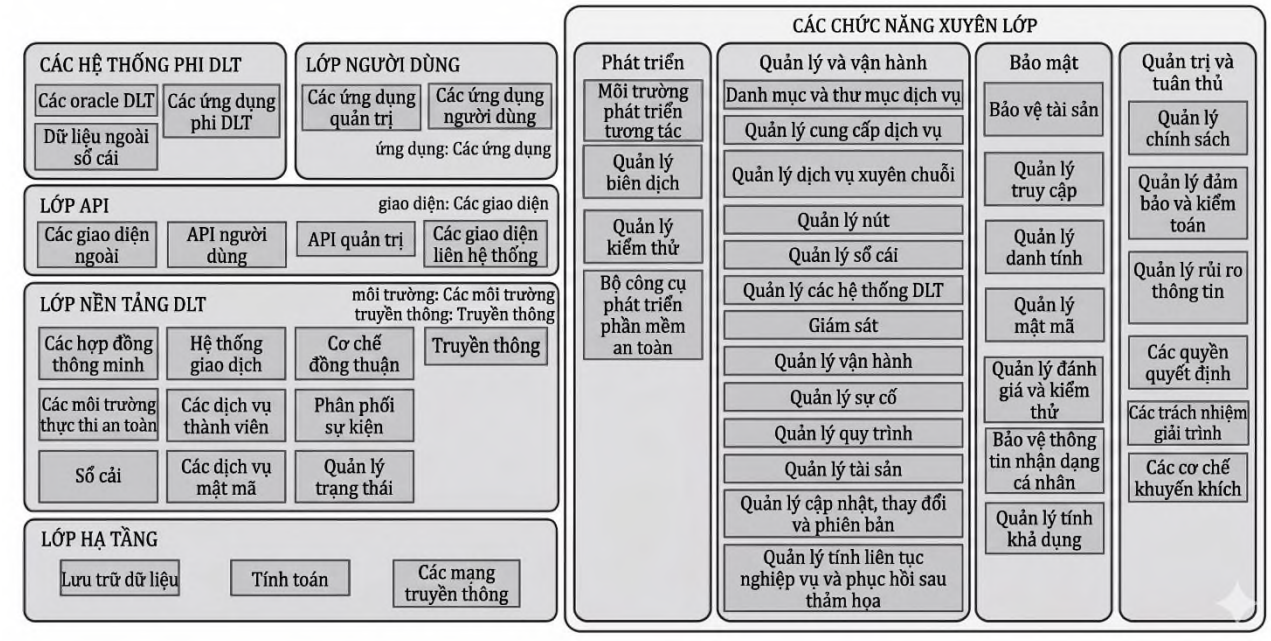
- các lớp chức năng (functional layers);

- các chức năng xuyên lớp (cross-layer functions).

Hình 7 minh họa các khái niệm về các chức năng, các lớp và các thành phần chức năng.



Hình 7 – Các lớp chức năng



Hình 8 – Các thành phần chức năng

Hình 8 bao gồm các hệ thống phi DLT và bốn lớp, cùng với một tập hợp các chức năng xuyên lớp bao phủ tất cả các lớp đó. Bốn lớp đó như sau:

- Lớp người dùng,
- Lớp API,
- Lớp nền tảng DLT,
- Lớp hạ tầng.

9.3.2 Các hệ thống phi DLT

Lớp các hệ thống phi DLT chứa các hệ thống nằm bên ngoài hệ thống DLT mà hệ thống DLT giao tiếp nhằm thực hiện các mục tiêu nghiệp vụ của mình. Lớp này bao gồm các thành phần sau:

- Các oracle DLT (DLT oracles): Các oracle DLT là các hệ thống đáng tin cậy được thiết kế để cung cấp dữ liệu bên ngoài cho hệ thống DLT hoặc để phản hồi các sự kiện từ các hệ thống DLT. Logic chuyển đổi và các dịch vụ có thể được sử dụng để thực hiện việc chuyển đổi cần thiết nhằm truyền thông dữ liệu đến và từ các hệ thống DLT. Các oracle DLT có thể cho phép các hợp đồng thông minh tiếp nhận dữ liệu thực tế trong quá trình thực thi mã.

- Các ứng dụng phi DLT (Non-DLT applications): Các ứng dụng phi DLT là bất kỳ ứng dụng nào nằm bên ngoài hệ thống DLT mà hệ thống DLT giao tiếp, dù là để gửi hay nhận dữ liệu. Cho dù là báo cáo và phân tích dữ liệu hay học máy, có nhiều ngữ cảnh trong đó việc phân tích được thực hiện trên dữ liệu sổ cái. Một ứng dụng như vậy có thể cung cấp dữ liệu và dịch vụ cho các ứng dụng DLT thông qua giao diện lập trình ứng dụng, hoặc có thể tiếp nhận dữ liệu từ hệ thống DLT để cung cấp các dịch vụ bổ trợ.

- Dữ liệu ngoài sổ cái (Off-ledger data): Dữ liệu ngoài sổ cái là bất kỳ dữ liệu nào được lưu trữ bên ngoài hệ thống DLT có thể chứa dữ liệu liên quan đến hệ thống DLT theo một cách nào đó. Một ví dụ có thể là cơ sở dữ liệu lưu giữ dữ liệu bổ sung liên quan đến các giao dịch được lưu trên sổ cái.

9.3.3 Lớp người dùng

Lớp người dùng chứa các chức năng nhằm cho phép các khách hàng DLT tương tác với các lớp khác và các chức năng xuyên lớp.

Các ứng dụng người dùng là các ứng dụng chạy tách biệt khỏi các hệ thống DLT. Chúng hoạt động như các máy khách đối với các hệ thống DLT và được người dùng sử dụng, thông thường để thực hiện các hoạt động đặc thù theo lĩnh vực hoặc đặc thù theo ứng dụng.

Các ứng dụng quản trị là các ứng dụng chạy tách biệt khỏi các hệ thống DLT, hoạt động như máy khách đối với hệ thống DLT, được các quản trị viên sử dụng để hỗ trợ các khả năng duy trì và/hoặc cập nhật các ứng dụng và hệ thống.

CHÚ THÍCH: Cả vai trò người dùng DLT và vai trò quản trị viên DLT đều sử dụng lớp người dùng. Xem 9.2 - Góc nhìn người dùng để hiểu rõ hơn về các nhiệm vụ mà các vai trò, người dùng/nhà vận hành/quản trị viên thực hiện và cần các API tương ứng.

9.3.4 Lớp API

Lớp API chứa các chức năng cung cấp khả năng truy cập đáng tin cậy và hiệu quả vào hệ thống DLT cho các ứng dụng, người dùng và các hệ thống phi DLT, thông qua việc gọi các thành phần chức năng trong lớp nền tảng DLT, và từ đó truy cập vào các dịch vụ bên dưới của lớp nền tảng và các chức năng xuyên lớp.

- Các giao diện ngoài (External interfaces) - các dịch vụ truy cập ngoài sổ cái cung cấp các phương tiện an toàn để truyền thông giữa hệ thống DLT và các hệ thống phi DLT bên ngoài;

- API người dùng (User API) - giao diện lập trình ứng dụng cung cấp quyền truy cập vào các chức năng đặc thù theo lĩnh vực;

- API quản trị (Admin API) - giao diện lập trình ứng dụng cung cấp quyền truy cập vào các chức năng của quản trị viên và nhà vận hành;

- Các giao diện liên hệ thống (Intersystem interfaces) - một nút trong hệ thống DLT có thể giao tiếp với nút khác trong một hệ thống DLT riêng biệt bằng cách sử dụng các giao diện liên hệ thống.

9.3.5 Lớp nền tảng DLT

Lớp nền tảng DLT chứa các chức năng cốt lõi của các hệ thống DLT có thể chạy trong một nút DLT. Lớp này cũng liên quan đến truyền thông giữa các nút.
Các khả năng chính bao gồm:

- các cơ chế đồng thuận phối hợp dữ liệu và các bản ghi tài khoản DLT trong sổ cái giữa các nút;
- truyền thông giữa các nút DLT và các hệ thống DLT thông qua các sự kiện và các giao thức an toàn;
- các dịch vụ mật mã bao gồm mã hóa, chữ ký số và các khả năng khác nhằm đảm bảo tuân thủ bảo mật và khả năng Kháng can thiệp trái phép của các hệ thống DLT;
- các hợp đồng thông minh chạy trong môi trường thực thi an toàn có thể tự động thực thi logic đã được lập lịch, có thể được bổ sung có chọn lọc theo các yêu cầu khác nhau của các ứng dụng;
- các chức năng nhằm tăng cường hiệu năng thông qua bộ nhớ đệm hiệu quả, lưu trữ đáng tin cậy và cân bằng tải.

Lớp nền tảng DLT kết nối phần cứng hoặc hạ tầng mạng do lớp hạ tầng cung cấp với các dịch vụ hỗ trợ chức năng liên quan trong lớp API. Các khả năng được lớp nền tảng DLT hỗ trợ bao gồm:

- hợp đồng thông minh,
- các môi trường thực thi an toàn,
- sổ cái,
- hệ thống giao dịch,
- các dịch vụ thành viên,
- các dịch vụ mật mã,
- cơ chế đồng thuận,
- phân phối sự kiện,
- quản lý trạng thái, và
- giao tiếp an toàn liên nút.

Để mô tả chi tiết hơn các khả năng này:
- Hợp đồng thông minh
Hợp đồng thông minh là một chương trình máy tính được lưu trữ trong hệ thống DLT, trong đó kết quả của bất kỳ lần thực thi nào của chương trình đều được ghi lại trên sổ cái phân tán. Các hợp đồng thông minh cung cấp chức năng lập trình cho người dùng của các hệ thống DLT. Người dùng tương tác với các hợp đồng thông minh bằng cách khởi tạo các sự kiện giao dịch tham chiếu đến địa chỉ hợp đồng.
Trong các hệ thống DLT công khai, các hợp đồng thông minh hầu như hoàn toàn mang tính chất phân tán; trong các hệ thống DLT riêng, chúng có thể mang tính chất phân tán hoặc tập trung. Khi được tập trung hóa, có một số yếu tố tin cậy gắn liền với các hợp đồng thông minh tập trung, ví dụ như chạy mỗi hợp đồng trong một môi trường thực thi đáng tin cậy được tách biệt để đáp ứng yêu cầu của các bên tham gia giao dịch trong mạng. Các hợp đồng thông minh phản ánh quá trình đạt được sự đồng thuận về một kết quả nhiều hơn là tư cách pháp lý của kết quả đó. Kết quả đó có thể có tính ràng buộc pháp lý.
CHÚ THÍCH: Các hợp đồng thông minh (còn được gọi là mã chuỗi , tài sản có thể lập trình hoặc hợp đồng có thể lập trình) được khởi tạo dưới dạng các chương trình máy tính thực thi trong môi trường thực thi an toàn khi người dùng gửi một giao dịch thuộc loại cụ thể đến hệ thống DLT.

- Các môi trường thực thi an toàn

Trong quá trình thực thi, một giao dịch có thể gọi các hợp đồng thông minh, vốn đòi hỏi việc thực thi mã một cách an toàn. Môi trường thực thi an toàn đảm bảo việc thực thi mã có thể được xác minh một cách an toàn. Môi trường thực thi an toàn có thể tận dụng cả các giải pháp bảo mật phần mềm lẫn phần cứng. Một ví dụ là việc sử dụng một container an toàn chứa một tập hợp các thành phần thực thi đã được ký số, chẳng hạn như hệ điều hành an toàn, các thư viện cho các ngôn ngữ lập trình được DLT hỗ trợ, các môi trường thực thi tương ứng của chúng và các thành phần tương tự.

- Sổ cái

Sổ cái (xem 6.1) là một kho thông tin lưu giữ các bản ghi giao dịch cuối cùng và xác định. Sổ cái hỗ trợ các khả năng lưu trữ dữ liệu. Các khả năng lưu trữ dữ liệu hỗ trợ ghi và truy vấn các loại dữ liệu khác nhau được tạo ra trong quá trình vận hành hệ thống DLT, chẳng hạn như sổ cái, thông tin giao dịch, v.v. Việc triển khai kỹ thuật có thể là cơ sở dữ liệu quan hệ, cơ sở dữ liệu cặp khóa-giá trị, cơ sở dữ liệu tệp, v.v. Trong trường hợp phân mảnh cơ sở dữ liệu (database sharding) được hỗ trợ, hệ thống cần hỗ trợ các khả năng phân mảnh và định tuyến dữ liệu.

- Hệ thống giao dịch

Hệ thống giao dịch là thành phần quản lý việc bổ sung các bản ghi giao dịch vào sổ cái. Hệ thống giao dịch có thể chứa một vùng dữ liệu tạm thời để lưu trữ các giao dịch chưa được xác nhận, được gọi là bể giao dịch (transaction pool). Sau khi một giao dịch được xác thực, giao dịch đó được đưa vào bể giao dịch nếu hợp lệ. Các giao dịch cần được ghi vào sổ cái được chọn từ bể giao dịch. Khi các giao dịch được xác nhận là đã được ghi vào sổ cái, chúng có thể được xóa khỏi bể giao dịch. Mỗi nút DLT có thể có bể giao dịch riêng của mình.

- Các dịch vụ thành viên

Các dịch vụ thành viên là các dịch vụ quản lý danh tính, quyền riêng tư, tính bảo mật và khả năng kiểm tra trong hệ thống DLT. Các dịch vụ thành viên chỉ áp dụng cho các hệ thống DLT có cấp phép.

- Các dịch vụ mật mã

Thành phần các dịch vụ mật mã cung cấp cho hệ thống DLT quyền truy cập vào các thuật toán mật mã cần thiết, hoặc trực tiếp hoặc bằng cách cung cấp giao diện đến phần cứng hoặc phần mềm triển khai các thuật toán đó. Hàm băm và chữ ký số là các ví dụ về thuật toán thường được sử dụng trong các hệ thống DLT. Hàm băm thường được sử dụng để bảo vệ sổ cái khỏi các sửa đổi. Bất kỳ thay đổi nào đối với thông tin trong sổ cái sẽ dẫn đến một giá trị băm được tính toán khác với giá trị băm đã được tính toán và lưu trữ trước đó cho sổ cái. Một giá trị băm mới được tính toán mỗi khi một giao dịch, hoặc trong trường hợp chuỗi khối là một khối (có thể chứa nhiều giao dịch), được thêm vào sổ cái. Chữ ký số đảm bảo rằng người nhận nhận được các giao dịch mà không có bên trung gian nào sửa đổi hoặc giả mạo nội dung giao dịch, đồng thời đảm bảo rằng các giao dịch xuất phát từ những người gửi có quyền truy cập vào các khóa riêng.

- Cơ chế đồng thuận

Khi đồng thuận đã đạt được và giao dịch được ghi vào sổ cái phân tán, giao dịch đó được coi là cuối cùng, xác định và bất biến. Điều này đòi hỏi việc triển khai các cơ chế đồng thuận - tức là các quy tắc và quy trình mà thông qua đó đồng thuận được đạt được.

Các quy tắc và quy trình này, vốn cho phép hệ thống DLT duy trì và cập nhật sổ cái phân tán và đảm bảo tính đáng tin cậy của các bản ghi trong sổ cái, tức là tính tin cậy, tính xác thực và tính chính xác của chúng, có sự khác biệt đáng kể về cách tiếp cận triển khai.

Các ví dụ về cơ chế đồng thuận bao gồm: phương pháp Nakamoto với Bằng chứng công việc (PoW), Bằng chứng cổ phần (PoS), Bằng chứng cổ phần ủy quyền (DPoS) hoặc Bằng chứng tầm quan trọng, và các Phương pháp thỏa thuận Byzantine bao gồm Khả năng chịu lỗi Byzantine thực tế (PBFT), Thỏa thuận Byzantine liên kết (FBA) và Byzantine Paxos. Cần lưu ý rằng các phương pháp đồng thuận lai kết hợp PoW và PBFT cũng đã được đề xuất (ví dụ như Đồng thuận Zilliqa).

- Phân phối sự kiện

Thành phần phân phối sự kiện xử lý việc phân phối các sự kiện được tạo ra trong nền tảng DLT.

- Quản lý trạng thái

Thành phần quản lý trạng thái theo dõi trạng thái của các tài sản được lưu giữ trên sổ cái, cập nhật trạng thái đó khi các giao dịch mới được cam kết vào sổ cái.

- Giao tiếp an toàn liên nút

Thành phần Giao tiếp an toàn liên nút xử lý việc truyền thông giữa các nút qua mạng, cho phép vận hành sổ cái phân tán. Giao thức liên nút, còn được gọi là giao thức xương sống, vận hành thông qua thành phần này.

9.3.6 Lớp hạ tầng

Lớp hạ tầng cung cấp môi trường vận hành, bao gồm các thành phần mạng, tính toán và lưu trữ cần thiết cho hoạt động bình thường của hệ thống DLT. Lớp này chứa các tài nguyên bao gồm lưu trữ dữ liệu, các container thực thi và các mạng truyền thông. Lớp này cung cấp các nền tảng cơ sở cần thiết cho việc triển khai hệ thống DLT. Lớp này có thể được cung cấp dưới dạng một tập hợp các tài nguyên điện toán đám mây hoặc dưới dạng thiết bị tại chỗ.

- Lưu trữ dữ liệu

Vị trí vật lý để lưu trữ dữ liệu cho sổ cái và đáp ứng các yêu cầu lưu trữ dữ liệu khác. Chức năng lưu trữ dữ liệu phải đáp ứng các yêu cầu sau:

- có thể được triển khai và sử dụng bởi mỗi nút trong mạng P2P;

- có thể được triển khai theo phương thức phân tán hoặc cục bộ;

- có thể hỗ trợ chủ quyền dữ liệu phù hợp;

- có thể cung cấp các dịch vụ ghi và truy vấn dữ liệu một cách hiệu quả, an toàn và ổn định.

- Tính toán

Chức năng tính toán cung cấp các khả năng thực thi cho hoạt động của hệ thống DLT, bao gồm nhưng không giới hạn ở công nghệ container, công nghệ máy ảo và công nghệ điện toán đám mây. Thông thường, môi trường thực thi cần được cung cấp cho mỗi nút trong hệ thống DLT.

- Mạng truyền thông

Các mạng truyền thông là cần thiết cho việc kết nối mạng P2P của các nút hệ thống DLT, cũng như cho truyền thông giữa hệ thống DLT và các thực thể trong lớp người dùng và trong các hệ thống phi DLT.

9.3.7 Các chức năng xuyên lớp

9.3.7.1 Tổng quan

Các chức năng xuyên lớp hỗ trợ các thành phần trên tất cả các lớp chức năng. Ví dụ, bảo mật là cần thiết cho lớp người dùng, lớp API và lớp nền tảng DLT, do đó bảo mật là một thành phần chức năng xuyên lớp. Các chức năng xuyên lớp cũng có thể hỗ trợ lẫn nhau. Chi tiết hơn, các chức năng được nhóm thành các hạng mục: phát triển; quản lý và vận hành; bảo mật; và quản trị và tuân thủ.

9.3.7.2 Phát triển

Các thành phần chức năng phát triển hỗ trợ các hoạt động của nhà phát triển hệ thống DLT, bao gồm phát triển triển khai ứng dụng và hệ thống, quản lý xây dựng và quản lý kiểm thử.

Các thành phần chức năng phát triển bao gồm:

- môi trường phát triển tích hợp (IDE),

- quản lý xây dựng,

- quản lý kiểm thử, và

- bộ công cụ phát triển phần mềm an toàn.

Để mô tả chi tiết hơn các thành phần này:

- Môi trường phát triển tích hợp (IDE)

Các thành phần chức năng IDE cung cấp các công cụ cho việc phát triển các hợp đồng thông minh, DLT và các ứng dụng liên quan, bao gồm việc phát triển các mô-đun hỗ trợ. Các thành phần chức năng IDE hỗ trợ việc sử dụng các khả năng được cung cấp bởi nền tảng DLT, bao gồm truy cập thông qua các API, quản lý nút và các khả năng phân phối sự kiện. IDE cho phép sử dụng các chức năng trong lớp API và lớp nền tảng DLT, cũng như lớp hạ tầng.

Thành phần chức năng IDE hỗ trợ việc tạo siêu dữ liệu liên quan đến cấu hình cho việc phát triển hợp đồng thông minh; hỗ trợ chuẩn bị hoặc tạo các tập lệnh cấu hình hợp đồng thông minh và các thành phần được nhà vận hành và môi trường thực thi trên các nút sử dụng.

- Quản lý xây dựng

Các thành phần chức năng quản lý xây dựng được sử dụng để xây dựng các gói phần mềm có thể công bố. Gói phần mềm có thể được nộp cho chủ sở hữu hoặc nhà vận hành nút DLT và được triển

khai trong môi trường. Gói phần mềm có thể chứa phần mềm cho các triển khai hợp đồng thông minh cũng như siêu dữ liệu cấu hình và các tập lệnh cấu hình.

Các tính năng quản lý xây dựng bao gồm:

- hỗ trợ chức năng xây dựng tự động gói phần mềm;

- cung cấp chức năng biên dịch tự động;

- cung cấp thông báo lỗi khi xảy ra lỗi trong quá trình xây dựng;

- thực hiện kiểm toán trong quá trình xây dựng;

- hệ thống xây dựng cung cấp hỗ trợ đa ngôn ngữ;

- hệ thống xây dựng cung cấp hỗ trợ đa nền tảng.

- Quản lý kiểm thử

Các thành phần chức năng quản lý kiểm thử hỗ trợ kiểm thử tất cả các chức năng của hệ thống DLT. Các thành phần này cần tạo các báo cáo kiểm thử và cung cấp chúng cùng với phần mềm triển khai hệ thống cho chủ sở hữu hoặc nhà vận hành nút. Các bài kiểm thử thường được thực hiện trong các môi trường thực thi biệt lập được thiết kế để mô phỏng chính xác các môi trường sản xuất. Công việc kiểm thử cũng có thể được thực hiện trong môi trường sản xuất mà không ảnh hưởng đến môi trường sản xuất. Môi trường kiểm thử cần được cung cấp bởi các nhà cung cấp DLT, đặc biệt là nhà vận hành hệ thống DLT.

Một khung kiểm thử được triển khai đầy đủ cần bao gồm các khả năng sau:

- hỗ trợ quản lý kế hoạch kiểm thử, báo cáo kiểm thử, trường hợp kiểm thử và các nội dung tương tự;

- hỗ trợ tạo báo cáo kiểm thử tự động;

- khi kiểm thử được thực hiện trong môi trường tích hợp của môi trường kiểm thử thì môi trường sản xuất không bị ảnh hưởng;

- hỗ trợ tự động hóa quy trình kiểm thử;

- cung cấp thư viện trường hợp kiểm thử và các chức năng quản lý cơ sở dữ liệu kiểm thử;

- tích hợp liên tục/triển khai liên tục (CI/CD) để cho phép nhiều bên yêu cầu, xem xét và phê duyệt mã.

Điều này bao gồm sự kết hợp của quản lý xây dựng, quản lý kiểm thử và quản trị để cung cấp các khả năng kiểm thử này.

- Bộ công cụ phát triển phần mềm an toàn

Các dịch vụ được cung cấp ở đây hỗ trợ việc phát triển mã an toàn bằng cách cung cấp các dịch vụ soát xét mã tự động, kiểm thử tự động và tái sử dụng mã. Các công cụ phát triển phần mềm an toàn có thể bao gồm các công cụ để soát xét mã, kiểm thử, thư viện, ghi nhật ký và giám sát.

9.3.7.3 Quản lý và vận hành

Các thành phần chức năng quản lý và vận hành bao gồm một tập hợp các chức năng để quản lý và kiểm soát hệ thống DLT nhằm cung cấp các khả năng vận hành của hệ thống.

Các thành phần chức năng quản lý và vận hành bao gồm:

- thư mục và danh mục dịch vụ,

- quản lý phân phối,

- quản lý dịch vụ liên chuỗi,

- quản lý nút,

- quản lý sổ cái,

- quản lý hệ thống DLT,

- giám sát,

- quản lý vận hành,

- quản lý sự cố,

- quản lý tài sản,

- quản lý cập nhật, thay đổi và phiên bản, và

- quản lý duy trì nghiệp vụ và khôi phục sau thảm họa.

Để mô tả chi tiết hơn các thành phần này:

- Thư mục và danh mục dịch vụ: Chức năng thư mục dịch vụ cung cấp danh sách tất cả các khả năng DLT, hợp đồng thông minh, dịch vụ và/hoặc API của một hệ thống DLT, nhà cung cấp hoặc nút cụ thể. Danh sách này bao gồm/tham chiếu đến thông tin kỹ thuật về triển khai, cung cấp và vận hành hợp đồng thông minh, dịch vụ hoặc API DLT. Các chức năng danh mục cung cấp quyền truy cập vào thông tin liên quan đến kiến trúc bảo mật và thông tin liên quan đến các dịch vụ, quy trình và công cụ. Danh mục có thể được sử dụng để hỗ trợ việc tạo và lựa chọn một kiến trúc và các thành phần của kiến trúc đó. Các công cụ thư mục và danh mục bao gồm các công cụ để quản lý thuật ngữ, mô hình, cơ sở dữ liệu sản phẩm và thư viện tham chiếu.

- Quản lý phân phối: Chức năng quản lý phân phối cung cấp chức năng quản lý việc phân phối hệ thống DLT, được thực hiện dưới hình thức triển khai hệ thống và điểm đầu cuối truy cập. Đồng thời, chức năng này cung cấp các quy trình công việc cần thiết để đảm bảo các phần tử được cung cấp theo đúng thứ tự.

- Quản lý dịch vụ liên chuỗi: Quản lý dịch vụ liên chuỗi giám sát và duy trì các kết nối, truyền thông và tương tác giữa hai hoặc nhiều hệ thống DLT khác nhau.

- Quản lý nút: Chức năng quản lý nút cung cấp chức năng quản lý việc triển khai nút nền tảng DLT bao gồm hiệu năng và tính sẵn sàng, thường trên một hệ thống logic hoặc ảo. Các nền tảng DLT có thể hỗ trợ các chính sách quản lý, bao gồm khả năng sử dụng Kiểm soát truy cập dựa trên vai trò (RBAC) để quản lý việc tạo và thao tác các tài nguyên.

- Quản lý sổ cái: Chức năng quản lý sổ cái cung cấp chức năng quản lý sổ cái phân tán.

- Quản lý hệ thống DLT: Chức năng quản lý hệ thống DLT cung cấp chức năng quản lý các hệ thống DLT, đặc biệt là về hiệu năng và tính sẵn sàng.

- Giám sát: Các chức năng giám sát bao gồm các công cụ giám sát, phân tích và tự động hóa được sử dụng để phản hồi các thay đổi trong hệ thống DLT và môi trường. Các chức năng này có thể bao gồm phát hiện và khắc phục các vấn đề cũng như phản hồi các thay đổi về dung lượng hệ thống cần thiết và phân tích lỗi.

- Quản lý vận hành: Các dịch vụ này bao gồm các quy trình để đảm bảo hoạt động an toàn của hệ thống DLT và khôi phục hệ thống DLT từ trạng thái lỗi, sự cố hoặc vấn đề.

- Quản lý sự cố: Chức năng quản lý sự cố là một tập hợp các quy trình để phát hiện, báo cáo, đánh giá, phản hồi, xử lý và rút kinh nghiệm từ các sự cố. Sự cố và vấn đề có thể được phát hiện và báo cáo bởi nút DLT, nhà cung cấp DLT hoặc người dùng DLT. Các công cụ quản lý sự cố bao gồm các công cụ phát hiện sự cố, báo cáo, phân tích, điều tra số, ghi nhật ký và giám sát.

- Quản lý tài sản: Các dịch vụ này đạt được và duy trì quyền sở hữu và giám sát phù hợp đối với các tài sản của tổ chức. Các công cụ quản lý tài sản bao gồm các công cụ để kiểm soát kiểm kê tài sản và theo dõi quyền sở hữu tài sản.

- Quản lý cập nhật, thay đổi và phiên bản: Quản lý cập nhật, thay đổi và phiên bản cung cấp các dịch vụ, quy trình và công cụ để đảm bảo rằng phần cứng và phần mềm được duy trì cập nhật; được nâng cấp lên phiên bản mới nhất; rằng các thay đổi được cấp phép và quản lý; và rằng các bản ghi về cập nhật, thay đổi và triển khai được lưu giữ. Các công cụ hỗ trợ cho lĩnh vực này bao gồm quản lý thay đổi và cập nhật, cơ sở dữ liệu quản lý cấu hình, kho lưu trữ phần mềm và các công cụ kiểm thử.

- Quản lý liên tục nghiệp vụ và khôi phục sau thảm họa: Các dịch vụ này hỗ trợ việc ngăn chặn, phát hiện và khôi phục từ sự gián đoạn dịch vụ, sự cố hoặc thảm họa. Trong các hệ thống phân tán, chẳng hạn như DLT, các nút có thể không đòi hỏi các dịch vụ này; nếu một nút ngừng hoạt động, khi nút đó hoạt động trở lại, nó sẽ tự động nhận thông tin mới nhất. Các công cụ hỗ trợ cho lĩnh vực này bao gồm các tài sản và quy trình quan trọng để chuyển đổi dự phòng.

9.3.7.4 Bảo mật

Các thành phần chức năng bảo mật chủ yếu nhằm cung cấp các thuộc tính bảo mật như xác thực, ủy quyền, tính bảo mật, tính toàn vẹn, tính sẵn sàng và kiểm soát truy cập cho tất cả các lớp chức năng của hệ thống DLT và các giao thức giữa các nút. Các tính năng bảo mật này được sử dụng

rộng rãi trong xác thực danh tính người dùng và nút, thiết kế giao thức giao dịch, bảo vệ tài sản, mã hóa kênh truyền thông và kiểm soát truy cập dữ liệu ứng dụng.

Các thành phần chức năng bảo mật bao gồm:

- bảo vệ tài sản;

- quản lý truy cập;

- quản lý danh tính;

- quản lý mật mã;

- quản lý đánh giá và kiểm tra;

- bảo vệ thông tin nhận dạng cá nhân;

- quản lý tính sẵn sàng.

Trong hệ thống DLT, bảo mật thông tin, bảo vệ tính bảo mật, tính toàn vẹn và tính sẵn sàng của thông tin và bảo vệ thông tin nhận dạng cá nhân (PII) bao trùm nhiều hơn sổ cái; đây là khía cạnh xuyên suốt bao gồm người dùng, các hệ thống phi DLT, API, nền tảng DLT, hạ tầng và các chức năng xuyên lớp khác. Do bảo mật là một khía cạnh xuyên suốt, nó hỗ trợ các lớp khác trong kiến trúc.

- Bảo vệ tài sản: Các dịch vụ trong lĩnh vực này cung cấp sự bảo vệ logic và vật lý cho các tài sản cấu thành hoặc kết nối với các hệ thống DLT. Các dịch vụ và công cụ bảo vệ tài sản bao gồm kiểm soát truy cập, bảo mật ứng dụng, bảo mật nền tảng, bảo mật mạng và bảo mật vật lý. Một số hệ thống DLT công khai hoặc không cấp phép có thể không có khả năng bảo vệ các khóa mật mã.

- Quản lý truy cập: Quản lý truy cập phù hợp với các hệ thống DLT có cấp phép và thông thường không phù hợp với các hệ thống DLT không cấp phép. Các dịch vụ có thể bao gồm các quy trình xác nhận và/hoặc xác minh danh tính của người dùng trước khi họ thực hiện giao dịch sử dụng sổ cái, hoặc để hạn chế các hành động mà người dùng có thể thực hiện sau khi được xác thực thành công. Trước khi thực hiện giao dịch, người dùng hệ thống DLT thường đăng nhập vào một nút; các dịch vụ và quy trình trong lĩnh vực này sẽ cung cấp xác thực và ủy quyền để người dùng đó đăng nhập thành công vào nút và sau đó thực hiện giao dịch. Các dịch vụ thành viên trong lớp nền tảng DLT được sử dụng bởi chức năng quản lý truy cập. Quản lý truy cập có thể bao gồm nhận dạng, xác thực, ủy quyền, kiểm soát truy cập và nhật ký truy cập.

- Quản lý danh tính: Các dịch vụ trong lĩnh vực này bao gồm các chức năng hỗ trợ vòng đời của danh tính. Lĩnh vực này bao gồm việc tạo tài khoản DLT và thiết lập các thuộc tính và giá trị liên quan đến tài khoản DLT, ví dụ như định danh, vai trò và thông tin xác thực. Lĩnh vực này bao gồm các thực thể và vai trò trong hệ thống DLT và có thể bao gồm các hệ thống phi DLT được kết nối với hệ thống DLT. Các dịch vụ, quy trình và công cụ quản lý danh tính bao gồm quản lý vai trò, ví kỹ thuật số và ghi nhật ký.

- Quản lý mật mã: Các dịch vụ trong lĩnh vực này bao gồm các quy trình để triển khai mật mã trong hệ thống DLT. Các công cụ hỗ trợ quản lý mật mã bao gồm quản lý khóa và ghi nhật ký.

- Quản lý đánh giá và kiểm tra: Các dịch vụ được cung cấp ở đây cho phép các nhóm nội bộ soát xét hiệu năng của các quy trình và phần mềm theo định kỳ, bổ sung cho các chức năng và hoạt động kiểm toán và đảm bảo. Đánh giá và kiểm tra thông thường được thực hiện bởi các nhóm nội bộ; các báo cáo cũng mang tính nội bộ của tổ chức và có thể liên quan đến dự án hoặc phát triển phần mềm. Các công cụ đánh giá và kiểm tra bao gồm kiểm tra hiệu năng, xác nhận, kiểm tra xâm nhập (penetration testing), ghi nhật ký và giám sát.

- Bảo vệ thông tin nhận dạng cá nhân: Việc bảo vệ PII thông thường liên quan đến một tập hợp kiểm soát rộng hơn so với bảo mật thông tin (ví dụ, ISO/IEC 27701 và ISO/IEC 29151:2017 liệt kê các kiểm soát bổ sung ngoài những kiểm soát được quy định trong ISO/IEC 27001). Chức năng này cung cấp các dịch vụ có thể được sử dụng để bảo vệ PII. Các công cụ hỗ trợ bảo vệ PII bao gồm kiểm soát truy cập, mã hóa, ẩn danh hóa, phi nhận dạng hóa (de-identification), hủy, ghi nhật ký và giám sát. Đối với các tài sản kỹ thuật số, có thể cần xem xét các tính năng không thể thay thế (non-fungible) khi xác định liệu PII có tồn tại hay không. PII có thể được suy luận khi nhiều tập dữ liệu đã được phi nhận dạng hóa được kết hợp. Việc sử dụng dữ liệu đã được phi nhận dạng hóa vẫn cần được xem xét đối với PII nếu nhiều loại dữ liệu/trường được sử dụng để khám phá. Xem ISO/TR 23244 để có thảo luận chi tiết hơn về PII trong ngữ cảnh các hệ thống DLT (ví dụ như các hệ thống chuỗi khối).

- Quản lý tính sẵn sàng: Các dịch vụ quản lý tính sẵn sàng đảm bảo rằng các chức năng và dịch vụ liên quan đến hệ thống chuỗi khối hoặc DLT sẵn sàng để sử dụng và đáp ứng các yêu cầu được nêu trong hợp đồng, thỏa thuận mức độ dịch vụ hoặc tài liệu khác. Các công cụ hỗ trợ quản lý tính sẵn sàng bao gồm quản lý năng lực, cung cấp, độ tin cậy, khả năng bảo trì, ghi nhật ký và giám sát.

9.3.7.5 Quản trị và tuân thủ

Các thành phần chức năng quản trị và tuân thủ cho phép các hệ thống DLT tuân thủ các đặc tính được quản trị và có thể kiểm tra dựa trên các yêu cầu quản trị và tuân thủ của chủ sở hữu và nhà vận hành nút DLT. Quản trị có thể giúp ngăn chặn các mạng DLT vi phạm các luật, quy định và quy tắc ngành (chẳng hạn như trở thành công cụ cho rửa tiền, tài trợ bất hợp pháp hoặc các giao dịch tội phạm). Chúng bao gồm các chức năng sau:

- quản lý chính sách;

- quản lý đảm bảo và kiểm toán;

- quản lý rủi ro thông tin;

- quyền quyết định;

- trách nhiệm giải trình;

- Cơ chế khuyến khích.

Để mô tả chi tiết hơn các chức năng này:

- Quản lý chính sách: Chức năng quản lý chính sách xác định, truy xuất và cập nhật các chính sách cho các hệ thống DLT và quản lý của chúng. Các chính sách này bao gồm bản thân hệ thống DLT và các khía cạnh nghiệp vụ, công nghệ, bảo mật, quản lý, quyền riêng tư và xác thực của nó.

- Quản lý đảm bảo và kiểm toán: Chức năng hỗ trợ kiểm toán chủ yếu được sử dụng để đạt được kiểm soát nội bộ kiểm toán, xác định trách nhiệm, truy xuất sự kiện và các yêu cầu khác của một giải pháp DLT hoàn chỉnh bao gồm hệ thống DLT, vốn cần các phương tiện kỹ thuật hiệu quả cùng với các tiêu chuẩn ngành nghiệp vụ để kiểm toán chính xác. Kiểm toán bảo mật là việc xem xét và kiểm tra độc lập các bản ghi và hoạt động hệ thống nhằm kiểm tra tính đầy đủ của các kiểm soát hệ thống, đảm bảo tuân thủ các chính sách và quy trình vận hành đã được thiết lập, phát hiện các vi phạm bảo mật và khuyến nghị các thay đổi được chỉ định trong kiểm soát, chính sách và quy trình (xem ISO 7498-2:1989). Đảm bảo bảo mật giúp chứng minh sự tin tưởng rằng một yêu cầu về việc đáp ứng các mục tiêu bảo mật đã được hoặc sẽ được đạt được (xem ISO/IEC TR 15443-1:2012). Các dịch vụ này cung cấp hỗ trợ cho kiểm toán bên ngoài và có thể dẫn đến các phát hiện được lập thành tài liệu có thể được chia sẻ cả trong và ngoài tổ chức.

- Quản lý rủi ro thông tin: Các dịch vụ quản lý rủi ro thông tin cung cấp các quy trình và công cụ để xác định, phân tích và xử lý các rủi ro thông tin. Các dịch vụ này cũng bao gồm báo cáo và tích hợp với các khung quản lý rủi ro khác. Các công cụ cần thiết bao gồm đánh giá rủi ro, xử lý rủi ro và báo cáo.

- Quyền quyết định: Việc phân bổ quyền quyết định trong môi trường phi tập trung có thể kém rõ ràng và tường minh hơn so với các môi trường được quản trị tập trung truyền thống. Người dùng DLT và các bên liên quan khác bị ảnh hưởng bởi các quyết định quản trị DLT chịu tác động bởi cách thức các quyền quyết định này được phân bổ. Quyền quyết định có thể là ngầm định hoặc tường minh. Quyền quyết định ngầm định có thể ít sẵn sàng hơn để được kiểm tra, mặc dù nó có thể mang lại sự linh hoạt bổ sung cho các hệ thống DLT để thích ứng với các thách thức quản trị không lường trước. Các tuyên bố tường minh về quyền quyết định có thể được ghi lại trong chính hệ thống DLT hoặc thông qua tham chiếu đến một tuyên bố bên ngoài về quyền quyết định và trách nhiệm giải trình. Việc phân bổ và tính tường minh của quyền quyết định hệ thống DLT có thể phát triển trong suốt vòng đời của hệ thống DLT - ví dụ, chúng có thể bắt đầu ở trạng thái tập trung ngầm định và phát triển để trở nên phi tập trung tường minh khi hệ thống DLT trưởng thành.

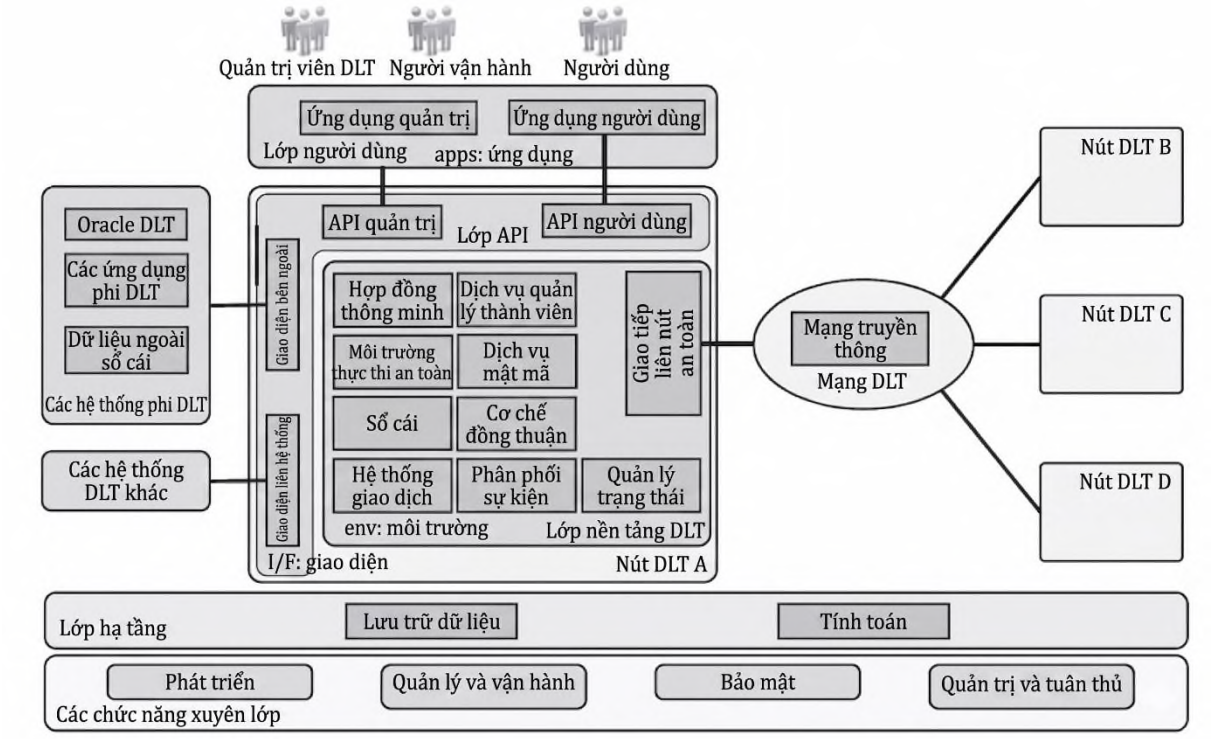
- Trách nhiệm giải trình: Để tăng cường tính minh bạch cho người dùng DLT hiện tại và tương lai cũng như các bên liên quan khác, các trách nhiệm giải trình của các bên trong các hệ thống DLT nên được công bố và làm rõ ràng. Điều này cho phép các bên tham gia hiểu được quyền hạn nằm ở đâu và như thế nào, đồng thời giảm sự không chắc chắn cho cả người dùng DLT và các bên liên quan khác trong việc đánh giá các rủi ro liên quan đến hoạt động của các hệ thống DLT. Nếu không có các tuyên bố và phân bổ trách nhiệm giải trình tường minh, hệ thống DLT có thể đối mặt với các thách thức phát sinh từ sự thiếu vắng thẩm quyền hợp pháp được chính thức hóa và rủi ro rằng các quyết định quan trọng sẽ được đưa ra mà không có trách nhiệm giải trình. Các ví dụ bao gồm việc giải quyết xung đột và thay đổi các quy tắc đồng thuận và cơ chế Cơ chế khuyến khích. Nếu không tuyên bố vị trí thẩm quyền đối với các quyết định vận hành và quản trị quan trọng, các bên thực sự nắm giữ quyền kiểm soát đó thường thực hiện mà không có trách nhiệm giải trình được chính thức hóa, khiến các bên tham gia không thể có ngay cả sự truy đòi hạn chế đối với sự giám sát và các ràng buộc pháp lý trong trường hợp xảy ra thất bại quản trị. Các ví dụ bao gồm lạm dụng quyền lực, chiếm đoạt tài sản hệ thống hoặc các quyết định không phù hợp với lợi ích của một tỷ lệ đáng kể người dùng DLT. Điều này đặt ra thách thức cho các bên liên quan của các hệ thống DLT, khiến họ có ít phương tiện truy đòi để yêu cầu những người ra quyết định có thẩm quyền ngầm định chịu trách nhiệm giải trình đối với các quyết định vi phạm các quy tắc, nguyên tắc hoặc thông lệ của hệ thống DLT, hoặc lợi ích chung của người dùng DLT và các bên liên quan khác.

- Cơ chế khuyến khích: Cơ chế khuyến khích trong các hệ thống DLT có thể đóng vai trò quan trọng trong việc định hướng hành vi của nhiều đối tượng người dùng DLT và các bên liên quan khác. Cơ chế khuyến khích có thể khuyến khích việc thực hiện các hoạt động cần thiết cho sự vận hành và quản trị liên tục của hệ thống. Nếu các cơ chế khuyến khích dành cho người dùng và các bên liên quan khác không được điều chỉnh phù hợp, chúng có thể dẫn đến các hành vi gây bất lợi về lâu dài cho người dùng hoặc các bên liên quan, có khả năng gây nguy hại cho sự vận hành bền vững của hệ thống. Cơ chế khuyến khích trong các hệ thống DLT có thể thúc đẩy việc đạt được đồng thuận giữa những người ra quyết định, giải quyết xung đột và đưa ra các quyết định liên quan đến quản trị, thiết kế và vận hành liên tục của hệ thống.

9.4 Góc nhìn hệ thống

9.4.1 Tổng quan

Hình 9 cung cấp một góc nhìn thay thế về các thành phần chức năng của một hệ thống DLT - đó là góc nhìn hệ thống về các thành phần chức năng. Góc nhìn hệ thống nhấn mạnh các mối quan hệ giữa các thành phần khác nhau và vị trí tương đối của chúng trong hệ thống.



Hình 9 – Hệ thống các thành phần chức năng của hệ thống Công nghệ sổ cái phân tán

Như được minh họa trong Hình 9, các loại giao diện phổ biến được sử dụng trong các hệ thống DLT có thể bao gồm:

- giao diện bên ngoài,

- giao diện liên hệ thống,

- API người dùng,

- API quản trị.

Góc nhìn hệ thống tổ chức các thành phần chức năng thành các nhóm sau:

- các nút DLT;

- các hệ thống ứng dụng - phục vụ cho quản trị và người dùng;

- các hệ thống phi DLT;

- các hệ thống DLT khác;

- các chức năng xuyên lớp.

9.4.2 Các nút DLT

Hệ thống DLT được xây dựng dưới dạng một tập hợp các nút giao tiếp với nhau, còn được gọi là các nút ngang hàng, vận hành theo phương thức phân tán. Mỗi nút có thể bao gồm một phần hoặc toàn bộ các thành phần chức năng trong lớp nền tảng DLT của Hình 9, cùng với các thành phần trong lớp API.

9.4.3 Các hệ thống ứng dụng

Hệ thống ứng dụng bao gồm cả ứng dụng người dùng cung cấp các khả năng cho người dùng cuối, và ứng dụng quản trị cung cấp các chức năng quản lý và điều hành hệ thống DLT. Các ứng dụng này truy cập hệ thống DLT thông qua User API và Admin API tương ứng của một nút.

9.4.4 Hệ thống phi DLT

Các hệ thống phi DLT bao gồm các oracle DLT, các ứng dụng phi DLT và dữ liệu ngoài sổ cái (off-ledger data). Các hệ thống này được kết nối với một nút DLT thông qua thành phần giao diện bên ngoài.

9.4.5. Các hệ thống DLT khác

Các hệ thống DLT khác là các hệ thống DLT riêng biệt tương tác với hệ thống DLT. Các hệ thống này được kết nối với một nút DLT thông qua các giao diện liên hệ thống.

9.4.6 Các chức năng xuyên lớp

Các chức năng xuyên lớp bao gồm thành phần phát triển, thành phần quản lý và vận hành, thành phần bảo mật và thành phần quản trị và tuân thủ. Các thành phần chức năng này trải rộng trên tất cả các phần tử của hệ thống DLT và được thể hiện trong Hình 9 như một nhóm trải rộng qua phần dưới của sơ đồ.

Phụ lục A

(Thông tin)

Xem xét về các token, tiền ảo, tiền mã hóa, đồng tiền và các khái niệm liên quan

Về mặt lịch sử, trong các hệ thống phi DLT, các token vật lý (chẳng hạn như đồng xu, chip hoặc vé) đã được sử dụng từ lâu trong các môi trường hệ thống đóng cục bộ. Tiền tệ và đồng tiền có thể có giá trị nội tại (giá trị này có thể thay đổi đáng kể). Các token, chip, vé, tem, vòng đeo tay và các thiết bị khác được phát hành cho các mục đích sử dụng cục bộ, chẳng hạn như tại rạp chiếu phim, cho hệ thống tàu điện ngầm, tại lễ hội âm nhạc, cho trò chơi điện tử, sòng bạc hoặc để sử dụng máy giặt và máy sấy tại tiệm giặt đồ - nhằm đơn giản hóa việc xử lý tiền mặt trong hệ thống và giảm thiểu các rủi ro liên quan đến việc xử lý tiền tệ; vì các mục đích tâm lý như giảm tâm lý e ngại khi chi tiêu, giảm rủi ro token bị đánh cắp để sử dụng ở nơi khác, và tăng rào cản chuyển đổi token trở lại thành tiền mặt.

Các token mật mã, cả ảo lẫn vật lý, cũng đã được sử dụng từ lâu trong nhiều môi trường hệ thống phân tán khác nhau, chủ yếu để truy cập vào một hệ thống; chúng đã đảm nhận nhiều vai trò mới trong môi trường DLT, nơi các quyền của người nắm giữ không được giám sát tập trung.

Tài liệu tham khảo sử dụng thuật ngữ đồng tiền điện tử thay vì token cho đơn vị tiền mã hóa chính được mô tả trong tài liệu đó. Trang web Bitcoin.org mặt khác tham chiếu các token như là các vật phẩm vật lý, hữu hình mà ai đó có thể nắm giữ và có thể được liên kết với các khóa riêng tư Bitcoin.

Trong khi Bitcoin là một đồng tiền điện tử được thiết kế chủ yếu cho các hệ thống thanh toán, thì Ether tập trung cả vào giá trị nội tại lẫn việc được sử dụng như "nhiên liệu" cho các dịch vụ của các ứng dụng được thiết kế theo khung Ethereum. Trong khung Ethereum, các nhà phát triển cũng có thể tạo ra các token riêng của mình cho nhiều mục đích sử dụng khác, chủ yếu đại diện cho các hàng hóa có thể giao dịch và có tính khả hoán.

Hàng nghìn loại tiền mã hóa, đồng tiền và token khác đã được phát triển kể từ đó, một số là các dự án phái sinh và một số khác vì mục đích riêng của chúng. Các loại này có thể thuộc một số hạng mục rộng, được gọi chung là token ở đây ngay cả khi người tạo ra chúng không gọi là token. Mặc dù các token này chủ yếu được coi là đặc thù của chuỗi khối, song các token ngày càng được sử dụng trong DLT không phải chuỗi khối.

Các hạng mục này bao gồm:

- Token có giá trị nội tại: Là loại token mà giá trị của nó được dựa thuần túy vào nhu cầu đối với chính token đó, nơi nó trở thành "đơn vị tiền tệ bản địa" trong một môi trường nhất định. Các cơ quan quản lý đang có nhiều cuộc thảo luận về các token này, chẳng hạn như liệu các token đó có phải được xử lý như tiền tệ hay như chứng khoán (ví dụ, phải chịu việc tính toán lãi lỗ) khi được giao dịch hay không. Chúng được thiết kế để là các kho lưu trữ giá trị có tính thanh khoản và dễ dàng chuyển nhượng, chẳng hạn sang các loại tiền tệ khác. Hiệu ứng tâm lý là quy tụ một nhóm đa dạng các bên tham gia để nhận thấy giá trị của token tăng lên và, chủ yếu trong môi trường không cấp phép, để bỏ ra công sức và tài nguyên nhằm cải thiện môi trường (ví dụ: đào - mining).

Cho đến nay, các hoạt động xung quanh các token có giá trị nội tại tập trung vào các hoạt động tích lũy liên quan đến các token và số dư của các thay đổi; không tồn tại các token riêng lẻ mà vì một lý

do nào đó có thể thu được giá trị sưu tầm khác biệt so với token khác, chẳng hạn như vì mục đích sưu tập hoặc đầu tư; chúng có tính thay thế.

- Token có giá trị ngoại tại: Là loại token mà giá trị của nó được dựa trên một điểm tham chiếu bên ngoài. Giống như các token vật lý, nơi có thể đổi đồng xu hoặc vé để lấy đồ uống có cồn, hoặc để sử dụng dịch vụ rửa xe, hoặc để quay bánh roulette, token là một đại diện thay thế cho thứ khác: một token khác, một tài sản vật lý (ví dụ: vàng, giá trị vốn cổ phần/cổ phiếu), hoặc các tài sản ảo (quyền đỗ xe trong bãi đỗ xe, khả năng bỏ phiếu về một quyết định kinh doanh, quyền lợi một phần trong dòng tiền bản quyền).

Giống như các token có giá trị nội tại, cho đến nay, các token này tập trung vào các hàng hóa có giá trị có tính thay thế, tức là quyền đổi lấy giá trị liên quan. Tuy nhiên, DLT cũng có thể được sử dụng cho việc nhận dạng cụ thể các hàng hóa có thể sưu tầm hoặc các hàng hóa có giá trị khác.

- Token đại diện (không mang giá trị): Mặc dù trọng tâm hiện nay là các token như tiền tệ hoặc như đại diện thay thế cho thứ khác mà giá trị có thể được trao đổi, song các token có thể được thiết kế cho nhiều mục đích khác trong một hệ thống, giống như chúng đã làm trong thế giới vật lý, nơi mục tiêu chính không bị giới hạn trong việc trao đổi giá trị. Thế giới vật lý có các luật và thông lệ phân biệt giữa quyền sở hữu, quyền chiếm hữu và các quyền liên quan; hầu hết các ứng dụng DLT là để đại diện cho việc chuyển nhượng quyền sở hữu của một hàng hóa có thể giao dịch có tính thay thế, và không tập trung vào việc theo dõi quyền chiếm hữu hoặc các quyền khác.

Các token có thể được sử dụng như các thiết bị theo dõi. Một tổ chức (ví dụ: công ty cho thuê ô tô hoặc hãng hàng không) có thể muốn theo dõi tài sản của mình tốt hơn; các đối tượng bán hàng hóa có giá trị cao hoặc các hàng hóa khác đòi hỏi theo dõi (đồ trang sức đắt tiền, nhạc cụ có thể sưu tầm, vũ khí, thực phẩm hoặc dược phẩm) có thể được theo dõi. Theo dõi kiểm toán và lịch sử vật phẩm có thể được ghi lại. Tương tự, một tổ chức hoặc mạng lưới có thể sử dụng các token để truy cập URL, API hoặc các tài nguyên khác, trong khi các cơ quan quản lý có thể công bố thông tin để theo dõi quyền. Ví dụ, điều này có thể cho phép chủ sở hữu kiểm soát việc chia sẻ xe đạp, vào bãi đỗ xe hoặc công viên quốc gia, hoặc công bố thông tin giấy phép, chẳng hạn như danh sách các chuyên gia được phép hành nghề. Các quyền có thể có giá trị xã hội hoặc tiền tệ, nhưng một số quyền không thể được giao dịch - ví dụ, quyền bỏ phiếu trong một cuộc bầu cử cụ thể.

Tiền ảo có thể được phân loại là tiền tệ thay thế kỹ thuật số, trong đó tiền tệ thay thế là các loại hàng hóa khác nhau được sử dụng để trao đổi hàng hóa và dịch vụ. Đặc điểm chính của chúng là có tính kỹ thuật số, tức là được đại diện bởi một số thực thể và hệ thống kỹ thuật số thay vì các vật thể vật lý. Tuy nhiên, khả năng đại diện chúng một cách vật lý thông qua giấy, kim loại hoặc các vật liệu khác không bị loại trừ.

Tiền ảo dựa trên DLT dựa vào các kỹ thuật mật mã để triển khai các tính năng liên quan nhất của chúng; trong trường hợp này, chúng được gọi là tiền mã hóa, là một loại tiền ảo đặc biệt theo quan điểm hình thức. Trong tài liệu này, cả hai thuật ngữ tiền ảo và tiền mã hóa đều được sử dụng, thuật ngữ đầu tiên theo nghĩa rộng hơn và thuật ngữ thứ hai chỉ đề cập đến tập con các loại tiền tệ sử dụng mật mã.

Báo cáo của ECB năm 2012 được đề cập tại 5.14 phân loại tiền ảo thành ba hạng mục sau:

1. Sơ đồ tiền ảo đóng: Thường được sử dụng trong các trò chơi điện tử trực tuyến để thưởng cho việc thực hiện các nhiệm vụ hoặc sứ mệnh (ví dụ: trong các trò chơi mô phỏng cuộc sống ảo, nơi

chúng cần thiết để mua các hàng hóa và khả năng mới) và không gắn kết với nền kinh tế thực; loại tiền ảo này chỉ tồn tại và có thể sử dụng trong thế giới ảo gắn liền với trò chơi. Tuy nhiên, mức độ phổ biến và sử dụng của chúng không thể bỏ qua vì, đặc biệt đối với các trò chơi điện tử rất phổ biến, số lượng người dùng có thể dễ dàng đạt đến vài triệu người. Mặt khác, do việc sử dụng của chúng bị giới hạn trong thế giới ảo, tác động trực tiếp của chúng đến cuộc sống thực của người dùng vẫn còn hạn chế. Ví dụ, trong trường hợp gian lận, chúng có thể có tác động tâm lý đến cuộc sống thực của người chơi, nhưng việc sử dụng của chúng bị giới hạn đến một chức năng cụ thể đến mức thiệt hại hoặc hoạt động bất hợp pháp có thể được coi là không đáng kể.

2. Sơ đồ tiền ảo với luồng một chiều (chiều vào): Tiền ảo có thể được mua để sử dụng mua hàng hóa và dịch vụ ảo (ngoại lệ cả hàng hóa thực). Loại sơ đồ này có ứng dụng đầu tiên trong thế giới trò chơi điện tử, nơi người chơi có thể sử dụng thẻ tín dụng của mình để mua "tín dụng ảo" nhằm sau đó có được các tính năng và dịch vụ mới giúp nâng cao hiệu suất chơi game. Mô hình này ngày nay còn được ứng dụng trong các lĩnh vực thương mại khác, nơi người dùng có thể mua các tín dụng cụ thể, sau đó có thể được sử dụng để truy cập các dịch vụ trực tuyến. Hiện tượng thẻ quà tặng ảo được giới thiệu bởi ví dụ Amazon™ [1)] là một ví dụ khác về tiền ảo với luồng một chiều: người dùng, sử dụng thẻ tín dụng của mình, mua một lượng tín dụng ảo tương đương và sau đó chuyển cho người dùng thứ ba (ví dụ: như một món quà). Bên thứ ba sẽ có thể sử dụng tín dụng này để mua trên thị trường Amazon™ một lượng hàng hóa thực tương đương, nhưng sẽ không được phép chuyển đổi ngược các tín dụng nhận được thành tiền thực. Nhìn chung, các loại tiền tệ này vẫn nằm trong hệ sinh thái được kiểm soát của chúng và tuân theo các luồng đơn giản, điều này hạn chế rủi ro đầu cơ và lạm dụng bất hợp pháp. Tuy nhiên, các rủi ro trở nên rõ ràng hơn khi tồn tại một liên kết giữa thế giới thực và thế giới ảo và liên kết này thường được xác định bởi thẻ tín dụng được sử dụng để chuyển đổi tiền thành tín dụng ảo. Nhìn chung, các loại tiền tệ này được các công ty cung cấp dịch vụ trực tuyến (bao gồm cửa hàng trực tuyến) áp dụng và các sơ đồ chuyển đổi và sử dụng được biết đến rộng rãi. Ở đây, rủi ro đối với người dùng chủ yếu nằm ở cách thức quản lý và lưu giữ thông tin liên quan đến "liên kết vật lý" (tức là thẻ tín dụng). Tác động có thể rất lớn, có khả năng ảnh hưởng đến hàng trăm triệu người dùng cuối, ví dụ trong trường hợp các nền tảng trực tuyến phổ biến. Tuy nhiên, hiện nay các ngân hàng và công ty thẻ tín dụng đã được trang bị khá đầy đủ để bảo vệ người dùng cuối khỏi loại mối đe dọa này.

[1)] AMAZON là nhãn hiệu thương mại của Amazon Services LLC và/hoặc các công ty liên kết của hãng. Thông tin này được cung cấp vì sự tiện lợi của người dùng Tiêu chuẩn này và không cấu thành sự chứng thực của ISO đối với sản phẩm được đề cập.

3. Sơ đồ tiền ảo với luồng hai chiều: Giống như bất kỳ loại tiền tệ có thể chuyển đổi nào khác, có hai tỷ giá hối đoái và có thể mua cả hàng hóa và dịch vụ ảo lẫn thực. Đây thực sự là hạng mục tiền ảo quan trọng nhất về tác động đến thế giới thực. Khả năng chuyển đổi hai chiều giữa tiền tệ thực và tiền ảo trên thực tế mở ra cho tiền ảo một phạm vi rộng hơn các trường hợp sử dụng nghiệp vụ. Tuy nhiên, các loại tiền tệ này, nhờ những đặc điểm riêng của chúng và thực tế là chúng thường không được quản lý bởi bất kỳ cơ quan đáng tin cậy nào, đang ngày càng trở nên hấp dẫn đối với các hoạt động bất hợp pháp. Tính hai chiều, tự bản thân nó, không phải là một đặc điểm tiêu cực; tuy nhiên, phần lớn các tiền ảo hoạt động trong lĩnh vực này không được quản lý, dựa trên các cơ chế chưa được nghiên cứu và phân tích kỹ lưỡng, và sự bảo vệ người dùng cuối không được cung cấp như một tính năng bắt buộc. Hệ quả là hạng mục tiền ảo này hiện nay là loại đang phơi bày người dùng cuối, và nhìn chung là xã hội, trước nhiều mối đe dọa nhất.

Từ phân loại trên, có thể thấy rõ rằng tiền ảo hai chiều có tác động lớn nhất đến cuộc sống thực của người dùng và vì lý do này, chúng cần được nghiên cứu và phân tích chuyên sâu hơn.

Phụ lục B

(Thông tin)

Các ví dụ về triển khai sổ cái

Phụ lục này cung cấp một số ví dụ về các triển khai sổ cái [2)].

Trong bối cảnh của các hệ thống DLT, các ví dụ về triển khai sổ cái bao gồm nhưng không giới hạn ở:

- DLT chuỗi khối: Bằng chứng công việc (Proof of Work): Không cấp phép (Permissionless) (BTC, ZEC, ETH);
- DLT chuỗi khối: Bằng chứng cổ phần (Proof of Stake): Không cấp phép (Permissionless) (ETH Constantinople);
- DLT chuỗi khối: Kết hợp (PoW/pBFT): Không cấp phép (Permissionless) (ZIL);
- DLT không phải chuỗi khối: PBFT: Có cấp phép (Permissioned) (XRP);
- DLT không phải chuỗi khối: FBA: Gần cấp phép (Pseudo-permissioned) (XLM);
- DLT không phải chuỗi khối: Tangle: Có cấp phép (Permissioned) (IOTA);
- Khung DLT doanh nghiệp: <đa dạng>: Có cấp phép (Permissioned) (Hyperledger/Corda).

Các từ viết tắt và thuật ngữ viết tắt được sử dụng ở trên có các nghĩa như sau:

- BTC - Bitcoin;
- ZEC - Zcash;
- ETH - Ethereum;
- Constantinople - Một bản cập nhật Ethereum trong quá trình chuyển đổi sang Bằng chứng cổ phần;
- PBFT - Practical Byzantine Fault Tolerance - Một giao thức đồng thuận chịu lỗi Byzantine;
- ZIL - Zilliqa - Một nền tảng chuỗi khối;
- XRP - Tiền mã hóa được sử dụng bởi mạng thanh toán Ripple;
- XLM - Tiền mã hóa được sử dụng bởi mạng Stellar;
- Tangle - Giao thức DLT dựa trên Đồ thị có hướng không có chu trình (Directed Acyclic Graphs);
- IOTA - Một sổ cái mã nguồn mở dựa trên Tangle.

[2)] Bitcoin, Zcash, Ethereum, Constantinople, Zilliqa, Ripple, Stellar, Hyperledger và Corda là các ví dụ về các sản phẩm phù hợp hiện có trên thị trường thương mại. Thông tin này được cung cấp vì sự tiện lợi của người dùng tài liệu này và không cấu thành sự chứng thực của ISO đối với các sản phẩm này.

Thư mục tài liệu tham khảo

[1] NAKAMOTO Satoshi Bitcoin: A Peer-to-Peer Electronic Cash System

https://bitcoin.org/bitcoin.pdf

[2] European Central Bank 2012), Virtual currency schemes

https://www.ecb.europa.eu/pub/pdf/other/virtualcurrencyschemes201210en.pdf

[3] ISO 5127:2017, Information and documentation - Foundation and vocabulary

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

[5] ISO/IEC 14772-2:2004, Information technology - Computer graphics and image processing - The Virtual Reality Modeling Language (VRML) - Part 2: External authoring interface (EAI)

[6] ISO/IEC/TR 15443-1:2012, Information technology - Security techniques - Security assurance framework - Part 1: Introduction and concepts

[7] ISO 16484-2:2004, Building automation and control systems (BACS) - Part 2: Hardware

[8] ISO/TR 18307, Health informatics - Interoperability and compatibility in messaging and communication standards - Key characteristics

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

[10] ISO/IEC 17789:2014, Information technology - Cloud computing - Reference architecture

[11] ISO/IEC 19941:2017, Information technology - Cloud computing - Interoperability and portability

[12] ISO/TS 21089, Health informatics - Trusted end-to-end information flows

[13] ISO/IEC 21823-1:2019, Internet of things (IoT) - Interoperability for IoT systems - Part 1: Framework

[14] ISO 22300, Security and resilience - Vocabulary

[15] ISO/IEC TS 23167, Information technology - Cloud computing - Common technologies and techniques

[16] ISO/TR 23244, Blockchain and distributed ledger technologies - Privacy and personally identifiable information protection considerations

[17] ISO/TR 23455:2019, Blockchain and distributed ledger technologies - Overview of and interactions between smart contracts in blockchain and distributed ledger technology systems

[18] ISO/TS 23635, Blockchain and distributed ledger technologies - Guidelines for governance

[19] ISO/IEC 24760-1, IT Security and Privacy - A framework for identity management - Part 1: Terminology and concepts

[20] ISO/IEC/IEEE 24765:2017, Systems and software engineering - Vocabulary

[21] ISO/IEC 27000, Information technology - Security techniques - Information security management systems - Overview and vocabulary

[22] ISO/IEC 27001, Information technology - Security techniques - Information security management systems - Requirements

[23] ISO/IEC 27018, Information technology - Security techniques - Code of practice for protection of personally identifiable information (PII) in public clouds acting as PII processors

[24] ISO/IEC 27031:2011, Information technology - Security techniques - Guidelines for information and communication technology readiness for business continuity

[25] ISO/IEC 29100, Information technology - Security techniques - Privacy framework

[26] ISO/IEC 29134, Information technology - Security techniques - Guidelines for privacy impact assessment

[27] ISO/IEC 29151, Information technology - Security techniques - Code of practice for personally identifiable information protection

[28] ISO/IEC 30141, Internet of Things (IoT) - Reference Architecture

[29] ISO/IEC 38500:2015, Information technology - Governance of IT for the organization

[30] ISO/IEC 29100:2011/Amd 1:2018, Information technology - Security techniques - Privacy framework - Amendment 1: Clarifications

[31] ISO/IEC 18033-1, Information security - Encryption algorithms - Part 1: General

[32] ISO/IEC/IEEE 42010:2011, Systems and software engineering - Architecture description

[33] ISO/IEC/IEEE 24748-1:2018, Systems and software engineering - Life cycle management - Part 1: Guidelines for life cycle management

[34] ISO/IEC 27050-1:2019, Information technology - Electronic discovery - Part 1: Overview and concepts

[35] ISO 37101:2016, Sustainable development in communities - Management system for sustainable development - Requirements with guidance for use

---