| TCVN | TIÊU CHUẨN QUỐC GIA |
|---|---|

DỰ THẢO

# TCVN XXXXX:2026
# ISO/TR 24374:2023-04

**Xuất bản lần 1**

# DỊCH VỤ TÀI CHÍNH – THÔNG TIN BẢO MẬT CHO PKI TRONG CÁC TRIỂN KHAI BLOCKCHAIN VÀ DLT

***Financial services - Security information for PKI in blockchain and DLT implementations***

**HÀ NỘI – 2026**

# MỤC LỤC

## Lời nói đầu

TCVN XXXXX:2026 hoàn toàn tương đương với ISO/TR 24374:2023-04.

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

Mặc dù các giải pháp dựa trên DLT/Blockchain vẫn đang ở giai đoạn đầu của quá trình áp dụng diện rộng và vẫn còn nhiều thách thức lớn, nhưng chúng chứa đựng tiềm năng [7] cho các cơ hội lớn trên nhiều lĩnh vực. Trong khi ngành tài chính đã thể hiện sự quan tâm rộng rãi từ sớm đối với DLT/Blockchain, các tổ chức khác trong khu vực công và tư nhân – những nơi dựa vào việc lưu giữ hồ sơ và quản lý các giao dịch bảo mật – cũng được hưởng lợi từ công nghệ này. DLT/Blockchain cũng mang lại cơ hội trong các lĩnh vực chăm sóc sức khỏe, dược phẩm, sáng tạo, và thực phẩm.

Trước mối quan tâm ngày càng tăng đối với DLT/Blockchain, các nỗ lực xây dựng tiêu chuẩn đã được đẩy mạnh, đặc biệt với việc thành lập Ủy ban kỹ thuật ISO về Blockchain và các công nghệ sổ cái phân tán (ISO/TC 307 Blockchain and distributed ledger technologies). Thông tin chi tiết có thể xem tại: https://www.iso.org/committee/6266604.html

ISO/DTR 23245 đã nêu rõ rằng:

“(i) Nội dung cốt lõi của việc quản lý vòng đời khóa đối với blockchain tương tự như trong hệ thống PKI thông thường.

(ii) Một số ứng dụng blockchain không có quy trình thu hồi cặp khóa. Trong những trường hợp đó, cần một quy trình quản lý khóa khác.”

Việc xem xét các hệ quả chính và tác động của DLT/Blockchain đối với việc triển khai hạ tầng khóa công khai (PKI) hiện hành trong dịch vụ tài chính là thiết yếu nhằm giảm thiểu mọi sự gián đoạn tiềm ẩn.

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

# Dịch vụ tài chính – Thông tin bảo mật cho PKI trong các triển khai Blockchain và DLT

*Financial services - Security information for PKI in blockchain and DLT implementations*

## 1 Phạm vi áp dụng

Tiêu chuẩn này áp dụng cho việc mô tả việc quản lý các khóa mật mã trong một chuỗi khối hoặc hệ thống phân tán được sử dụng trong lĩnh vực tài chính.

Mục tiêu của tiêu chuẩn này xem xét tác động của các quy trình quản lý khóa khác nhau cần thiết cho việc triển khai Cơ sở hạ tầng khóa công khai (PKI) trong các dự án chuỗi khối và công nghệ sổ cái phân tán (DLT).

## 2 Tài liệu viện dẫn

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

## 3 Thuật ngữ và định nghĩa

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

**3.1**

**chuỗi khối** (blockchain)

*sổ cái phân tán* (3.4) với các khối đã được xác nhận, được tổ chức thành một chuỗi tuần tự, chỉ cho phép ghi nối tiếp vào, thông qua việc sử dụng các liên kết mật mã.

CHÚ THÍCH 1: Các chuỗi khối được thiết kế để chống giả mạo và tạo ra các *bản ghi sổ cái* mang tính hoàn tất, xác quyết và bất biến.

**3.2**

**sự đồng thuận** (consensus)

thỏa thuận giữa các nút DLT rằng:

a) một giao dịch đã được xác thực; và

b) *sổ cái phân tán* (3.4) chứa một tập hợp nhất quán và *một trình tự xác định* của các giao dịch đã được xác thực.

**3.3**

**cơ chế đồng thuận** (consensus mechanism)

các quy tắc và quy trình để đạt được *đồng thuận* (3.2).

**3.4**

**sổ cái phân tán** (distributed ledger)

*sổ cái* (3.9) được chia sẻ trên một tập hợp các nút DLT và được đồng bộ hóa giữa các nút DLT bằng *cơ chế đồng thuận* (3.3).

[Nguồn: ISO 22739:2020, 3.44]

**3.5**

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

hệ thống triển khai một *sổ cái phân tán* (3.4).

**3.6**

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

công nghệ cho phép vận hành và sử dụng các *sổ cái phân tán* (3.4).

**3.7**

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

thiết bị hoặc quy trình của hệ thống công nghệ sổ cái phân tán, tham gia vào một mạng và lưu trữ bản sao toàn phần hoặc một phần của các *bản ghi sổ cái* (3.10).

**3.8**

**mô đun bảo mật phần cứng** (hardware security module - HSM)

triển khai phần cứng của bộ xử lý mật mã an toàn, sử dụng chứng thư ITU-T X.509 và khóa riêng để cung cấp xác thực an toàn (mức an toàn 3 trở lên theo ISO/IEC 19790:2012).

**3.9**

**sổ cái** (ledger)

kho lưu trữ thông tin chứa các bản ghi giao dịch, được thiết kế sao cho mang tính cuối cùng, xác quyết và bất biến.

**3.10**

**bản ghi sổ cái** (ledger record)

bản ghi sổ cái bao gồm các giá trị băm của bản ghi giao dịch hoặc các tham chiếu đến bản ghi giao dịch, được lưu trên *chuỗi khối* (3.1) hoặc hệ thống sổ cái phân tán.

[Nguồn: ISO 22739:2020, 3.30]

## 4 Ký hiệu và các thuật ngữ viết tắt

| | | |
|---|---|---|
| API | Application Program Interface | Giao diện lập trình ứng dụng |
| BCP | Business Continuity Plan | Kế hoạch duy trì hoạt động kinh doanh |
| BTC | Bitcoin | Bitcoin |
| CA | Certificate Authority | Thẩm quyền chứng thực |
| CRL | Certificate Revocation List | Danh sách thu hồi chứng thư |
| DHT | Distributed Hash Table | Bảng băm phân tán |
| DTR | Draft Technical Report | Dự thảo báo cáo kỹ thuật |

| | | |
|---|---|---|
| ETL | Extract, Transfer, and Load | Trích xuất, chuyển đổi và tải |
| HSM | Hardware Security Module | Mô-đun bảo mật phần cứng |
| KYC | Know Your Customer | Định danh khách hàng |
| LDAP | Lightweight Directory Access Protocol | Giao thức truy cập thư mục nhẹ |
| MITM | Man-In-The-Middle | Tấn công xen giữa |
| OCSP | Online Certificate Status Protocol | Giao thức trạng thái chứng thư trực tuyến |
| PAX | Paxos Standard | Chuẩn Paxos |
| PKI | Public Key Infrastructure | Cơ sở hạ tầng khóa công khai |
| VPN | Virtual Private Network | Mạng riêng ảo |
| WoT | Web of Trust | Mạng lưới tin cậy |

# 5 Các vấn đề liên quan – Công nghệ sổ cái phân tán (DLT) / Blockchain và PKI

## 5.1 Các mối quan ngại về an toàn dữ liệu và quyền riêng tư DLT/Blockchain

### 5.1.1 Tổng quan

Chuỗi khối và các hệ thống DLT bao gồm các nút ngang hàng trong một mạng, dữ liệu lưu trữ trên mạng đó có tính xác quyết được thống nhất thông qua cơ chế đồng thuận. Mỗi nút có một mô đun mật mã để thực hiện các phép toán mật mã theo đúng quy định trong giao thức nền tảng. Mặc dù các mạng lưới và dịch vụ chuỗi khối không có một máy chủ trung tâm, điều đó không có nghĩa là các nút không cần được bảo vệ. Các nỗ lực cao nhất để bảo vệ từng nút chính là yếu tố then chốt để đảm bảo an toàn cho toàn bộ hệ thống dựa trên chuỗi khối.

Về cơ bản, các dự án công nghệ chuỗi khối là một sổ cái phân tán hoặc cơ sở dữ liệu phân tán dựa trên nền tảng ngang hàng được tổ chức bởi một tập hợp kết hợp với chuỗi khối, tức là một loạt các tập dữ liệu được mã hóa dùng để ghi lại các thay đổi mang tính bất biến theo thời gian.

Một trong những giá trị cơ bản của chuỗi khối là bản chất phân tán ghi-một-lần, thêm-nhiều-lần; nó có thể dễ dàng triển khai trên các nút khác nhau trên web, nhưng mỗi bản ghi chứa giá trị băm của chính nó, khiến nó có tính bất biến.
Để đạt được mục đích này, mật mã là phương tiện chính để bảo vệ các ứng dụng, các mạng, cơ sở hạ tầng và dịch vụ khỏi các mối đe dọa mạng. Tuy nhiên, cơ sở hạ tầng khóa công khai (PKI) hiện tại dựa trên một trung tâm là Thẩm quyền chứng thực (CA), có thể trở thành nút thắt cổ chai, ảnh hưởng đến hiệu quả của các giao thức mật mã do chi phí phát sinh từ việc xác minh chữ ký và chứng thư mật mã. Gần đây, chuỗi khối cũng đã được tận dụng để hỗ trợ PKI mà không cần Thẩm quyền chứng thực. Tuy nhiên, nó cũng tạo ra những thách thức bảo mật độc đáo được mô tả trong Điều 5.

### 5.1.2 Từ tập trung đến phi tập trung

Chuỗi khối chuyển dịch việc lưu trữ và bảo vệ dữ liệu từ một mô hình tập trung sang một mô hình phi tập trung. Trong các mô hình tập trung truyền thống, các phương pháp an toàn có thể được hợp nhất với các sản phẩm công nghệ mà chúng phục vụ. Tuy nhiên, chuỗi khối đòi hỏi các biện pháp an toàn đổi mới để bảo vệ các sản phẩm tài chính năng động và phân tán cao mà công nghệ này hướng đến hỗ trợ. Như với bất kỳ cơ sở hạ tầng dựa trên mật mã nào, việc bảo vệ khóa là yếu tố tối quan trọng để đảm bảo an toàn cho hệ thống chuỗi khối.

Một hệ thống chuỗi khối thành công cần có các phương pháp giao tiếp có độ tin cậy cao với các thực tiễn bảo vệ khóa mạnh được cung cấp bởi HSM, các phần tử an toàn và các môi trường tính toán khác được thiết kế để thực thi mã một cách an toàn - và tất cả những yếu tố này mang lại khả năng mở rộng và tính linh hoạt mà một mô hình chuỗi khối phi tập trung cần có.

### 5.1.3 Khai thác tức thời

Bất kỳ ai có thu được khóa đều có thể tức thời khai thác và trục lợi từ tài sản đó. Như đã thấy trong các vụ vi phạm bảo mật trên các nền tảng chuỗi khối công khai, chẳng hạn như Bitfinex, Mt. Gox và các nền tảng khác, việc chuyển giao giá trị mang tính gian lận có thể diễn ra tức thời, không thể đảo ngược và đáng kể. Những người tham gia vào các hệ thống này đã mất hàng triệu đô la do hệ thống an toàn bị xâm phạm.
Tuy nhiên, cần lưu ý rằng các cuộc tấn công này đã khai thác các lỗ hổng ở tầng ứng dụng – cụ thể là các ví điện tử lưu giữ khóa truy cập tài sản – chứ không phải giao thức chuỗi khối nền tảng. Cho đến nay, bản thân công nghệ chuỗi khối đã chứng minh được khả năng chống giả mạo, trong phạm vi được xác định bởi cơ chế đồng thuận được áp dụng bởi mạng.

### 5.1.4 Bảo vệ khóa là yếu tố then chốt

Khả năng thêm các giao dịch vào một cơ sở dữ liệu giao dịch giúp mở rộng khả năng ứng dụng của công nghệ.
PKI truyền thống là dựa trên CA, do đó sự an toàn của hệ thống PKI sẽ bị đe dọa nếu một CA bị xâm phạm. Ví dụ, một khung giảm thiểu các vấn đề với PKI chẳng hạn như các khó khăn với sự thu hồi chứng thư nhanh chóng, sự loại bỏ các điểm lỗi đơn lẻ và các sự cố của các CA. Lưu ý rằng nếu CA gốc bị xâm phạm, kẻ tấn công có thể chiếm quyền kiểm soát toàn bộ PKI và làm tổn hại sự tin cậy của toàn bộ hệ thống, bao gồm bất kỳ hệ thống con nào phụ thuộc vào PKI. [1]

## 5.2 Các vấn đề và tấn công liên quan đến hệ thống PKI

### 5.2.1 Những thách thức hiện tại của Cơ sở hạ tầng khóa công khai (PKI)

Cách tiếp cận được sử dụng phổ biến nhất đối với các PKI là Web PKI. Đây là một hệ thống dựa trên Thẩm quyền chứng thực (CA) và vận hành trên một cơ sở hạ tầng tin cậy tập trung. Mục đích của PKI là tạo điều kiện thuận lợi cho việc truyền tải thông tin điện tử an toàn cho nhiều hoạt động mạng như thương mại điện tử, ngân hàng trực tuyến và bảo mật email. Cần xác minh danh tính của bên mà kết nối an toàn được thiết lập cùng. Nhiệm vụ quan trọng nhất là thiết lập sự tương ứng giữa danh tính (dữ liệu nhận dạng) và khóa công khai của người dùng. Vấn đề này được giải quyết bằng cách sử dụng chứng thư khóa công khai - một tài liệu điện tử được sử dụng để chứng minh quyền sở hữu khóa công khai. Chứng thư chứa khóa công khai, thông tin xác thực của người dùng và chữ ký điện tử của bên đáng tin cậy xác minh người dùng. Để đảm bảo tính toàn vẹn và tính xác thực của chứng thư, nó được ký bởi một bên đáng tin cậy – Thẩm quyền chứng thực.

Các giải pháp Web PKI tập trung tồn tại một số vấn đề nghiêm trọng:
a) Có những thách thức trong việc thông báo kịp thời khi khóa bị xâm phạm, vì việc tạo và phân phối danh sách chứng thư bị thu hồi có thể mất từ vài phút đến một giờ, trừ khi sử dụng các giao thức xác minh đồng bộ như OCSP. Do đó, không có gì đảm bảo 100% rằng khóa này vẫn còn hợp lệ. Vấn đề này cũng liên quan đến các hệ thống DLT, nơi một giao dịch có thể được ký bằng khóa không còn hợp lệ hoặc không còn nằm dưới trách nhiệm kiểm soát duy nhất của chủ sở hữu. Nếu chứng thư được xác minh trực tuyến (bằng cách gửi yêu cầu đến CA), thì quyền riêng tư của người dùng sẽ bị xâm phạm, vì CA sẽ biết toàn bộ lịch sử tương tác của người dùng.

b) Việc xác định danh sách các CA đáng tin cậy trong một hệ thống PKI có thể rất phức tạp và đòi hỏi một số cơ chế quản lý đặc thù ngoài giao thức, mặc dù đã có các hợp tác thành công tạo ra các môi trường liên kết cao, như Danh sách dịch vụ đáng tin cậy của Châu Âu (European Trusted Services List). Một hệ thống phi tập trung cũng có thể bị ảnh hưởng bởi vấn đề này.

c) Trung tâm của hệ thống luôn là mục tiêu tấn công và nếu chứng thư gốc bị xâm phạm thì toàn bộ hệ thống sẽ bị lộ ra hàng loạt lỗ hổng bảo mật.

d) Việc quản lý định danh thuộc về một tổ chức tập trung và không phải của chính chủ sở hữu định danh.

Có nhiều nguyên nhân dẫn đến thất bại của PKI mà cả cộng đồng người dùng lẫn giới nghiên cứu bảo mật máy tính truyền thống đều chưa thực sự tham gia giải quyết. Cụ thể, đã có những sự cố cho thấy các điểm yếu mang tính hệ thống trong thực tiễn tổ chức, tạo ra rủi ro cho tất cả những ai dựa vào PKI. Tuy nhiên, vẫn có các lựa chọn tổ chức và cấu hình có thể giúp tránh hoặc giảm thiểu một số rủi ro này. [15]

Trong PKI phi tập trung, chuỗi khối có thể hoạt động như một kho lưu trữ khóa – giá trị phi tập trung. Nó có khả năng bảo vệ việc đọc dữ liệu để ngăn chặn các cuộc tấn công trung gian MITM (Man-In-The-Middle) và giảm thiểu quyền của các bên thứ ba.

### 5.2.2 Các cuộc tấn công vào PKI

PKI phải đối mặt với các rủi ro xuất phát từ các lỗ hổng tiềm ẩn của các bên Thẩm quyền chứng thực (CA), dẫn đến có thể bị lợi dụng để cấp phát chứng thư trái phép cho người dùng cuối. Nhiều vụ vi phạm đã cho thấy nếu một CA bị xâm phạm, sự an toàn của người dùng cuối tương ứng sẽ gặp rủi ro. Có nhiều trường hợp các lỗi hoặc những sự vi phạm của CA dẫn đến các chứng thư trái phép được phát hành.[12]

Một điểm yếu quan trọng khác của các PKI liên quan đến độ tin cậy và tính bảo mật của danh sách thu hồi chứng thư (CRL) hoặc các máy chủ OCSP liên quan, được sử dụng để đảm bảo quản lý vòng đời chứng thư chính xác, đặc biệt là việc thu hồi, và cần được truy vấn bất cứ khi nào chứng thư được sử dụng. Một cách điển hình, CRL cho một tập hợp các chứng thư được duy trì bởi cùng một (và duy nhất) CA mà đã cấp các chứng thư đó, và điều này tạo ra một điểm lỗi đơn trong hệ thống.

Trong thực tế, các CRL không hoạt động theo thời gian thực; chúng thường được cập nhật định kỳ bởi CA cấp phát, và có thể xảy ra độ trễ giữa sự vi phạm an toàn và bản cập nhật CRL tiếp sau, dẫn đến việc sử dụng tạm thời các chứng thư đã bị xâm phạm. CA có thể không phát hiện việc chứng thư và khóa riêng liên quan bị đánh cắp; trong trường hợp đó, chứng thư sẽ không bị thu hồi.[10] Xem Phụ lục A cho các giải pháp khả thi.

### 5.3 Các mục tiêu an toàn

Các DLT sử dụng PKI mật mã như cơ chế an toàn có khả năng chống lại các tác nhân tấn công không sở hữu khóa thích hợp. Điều này, cùng với việc dữ liệu được chia sẻ và đặc tính kháng can thiệp trái phép của các giải pháp chuỗi khối, có nghĩa là các DLT có mức an toàn cao. Vì lý do này, nếu các biện pháp kiểm soát chẳng hạn như quản lý khóa xem Phụ lục B tuân theo đúng thông lệ tốt nhất của ngành thì hệ thống DLT có tiềm năng vững chắc hơn từ góc độ an ninh mạng so với các hệ thống dựa trên an toàn vật lý hoặc mạng, hoặc các hệ thống được bảo vệ bằng mật khẩu tạo thủ công thay vì các khóa mã riêng. DLT cũng gặp thách thức trong việc tích hợp với các mô đun bảo mật phần cứng (HSM) dùng để lưu trữ và tạo khóa, cũng như với các hạ tầng bảo mật như mạng riêng ảo (VPN).

Các HSM chỉ cung cấp các cơ chế hạn chế để phát hiện việc sử dụng khóa sai mục đích, ví dụ: mã hóa dữ liệu so với mã hóa PIN, hoặc giữa khóa ký với khóa mã hóa. Các DLT có thể được xây dựng dựa trên các lược đồ mật mã mà không nhất thiết được hỗ trợ bởi các HSM, các phần tử an toàn cũng như các thành phần bảo mật khác hỗ trợ hoặc quản lý đúng cách, nhưng vẫn cần phải sử dụng và xử lý thông tin được ký bằng khóa đó, điều này tạo ra rủi ro về an ninh và quản lý khóa.  Hơn nữa, nếu kẻ tấn công chiếm quyền kiểm soát hệ thống hoặc ứng dụng có quyền sử dụng khóa trong HSM, hoặc nếu một kẻ nội gián lạm dụng các quyền này, điều này sẽ cho phép chúng ký các giao dịch tiền mã hóa gian lận. Chỉ một chữ ký như vậy cũng đủ để rút sạch toàn bộ tiền mã hóa trong một địa chỉ cụ thể.[10]

Các thách thức trong việc tích hợp với các hệ thống sổ cái phân tán DLT có liên quan đến mô hình an toàn của chúng, vốn chủ yếu dựa trên PKI (Cơ sở hạ tầng khóa công khai ).[10] Các quyền truy cập để ghi dữ liệu trạng thái chuỗi khối thường yêu cầu các giao dịch dữ liệu được ký bởi một khóa riêng cụ thể, trong khi quyền đọc dữ liệu trạng thái chuỗi khối đòi hỏi quyền truy cập vào tệp sổ cái (được lưu trên nhiều máy chủ) hoặc quyền truy cập vào các cơ chế giao diện được thiết lập trên dữ liệu chuỗi khối. Các giao diện này thường được bảo vệ thông qua hệ thống xác thực mạng (được liên kết với thư mục doanh nghiệp) hoặc cơ chế xác thực mật khẩu tùy chỉnh. Lưu ý điều này khác nhau giữa các hệ thống DLT và trên thực tế không tồn tại với các hệ thống DLT công khai không cần quyền.

Các cơ chế bảo mật là một yếu tố quan trọng cần được xem xét khi tích hợp các giao thức bảo mật chuỗi khối có độ an toàn cao, dựa trên mật mã, với các quy tắc truy cập và kiểm soát khác, có thể lỏng lẻo hơn trong các hệ thống kế thừa hiện có. Tích hợp xét từ góc độ dữ liệu tương đối đơn giản thông qua các giao diện lập trình chuẩn, với giả định rằng việc tích hợp dữ liệu diễn ra trong khuôn khổ an toàn đã được thiết lập và các quy trình ETL tiêu chuẩn. Một khi các hệ thống chuỗi khối có một giao diện tiêu chuẩn an toàn (được định nghĩa sau), chúng về cơ bản trở thành một thành một phần doanh nghiệp khác, mặc dù với những đặc tính đặc trưng của DLT – cụ thể là bản ghi giao dịch bất biến trong mạng phi tập trung nơi các nút ngang hàng chia sẻ dữ liệu, các tài sản và giá trị.

Chuỗi khối cũng có thể được sử dụng để bảo vệ dữ liệu trong các hệ thống khác. Ví dụ, các bản sao lưu cơ sở dữ liệu có thể gắn dấu thời gian bằng hàm băm của dữ liệu để đảm bảo tính toàn vẹn của bản sao lưu cho các mục đích pháp lý.

Các phương pháp mật mã học như cây Merkle, [18] cho phép bảo mật lượng lớn dữ liệu ở mức chi phí thấp. Cây Merkle tách biệt việc xác thực dữ liệu khỏi bản thân dữ liệu - cây Merkle có thể nằm cục bộ, hoặc trên một tổ chức đáng tin cậy, hoặc chính nó cũng có thể nằm trên một hệ thống phân tán.

### 5.4 Tóm tắt việc sử dụng mật mã khóa phi đối xứng trong mạng chuỗi khối

Dưới đây là tóm tắt cách sử dụng mật mã khóa phi đối xứng trong nhiều mạng chuỗi khối:

- Khóa riêng được sử dụng để tạo ký số cho các giao dịch.

- Khóa công khai được sử dụng để dẫn xuất địa chỉ.
- Khóa công khai được sử dụng để xác minh chữ ký được tạo bằng khóa riêng.
- Mật mã phi đối xứng cung cấp khả năng xác minh rằng người dùng thực hiện việc chuyển giá trị sang người dùng khác đang sở hữu khóa riêng có khả năng ký giao dịch đó.

Một số mạng chuỗi khối được cấp phép (permissioned blockchain) có thể tận dụng Cơ sở hạ tầng khóa công khai (PKI) hiện có của doanh nghiệp để cung cấp thông tin xác thực cho người dùng – thay vì yêu cầu mỗi người dùng trong mạng chuỗi khối phải tự quản lý cặp khóa phi đối xứng của mình. Điều này được thực hiện bằng cách sử dụng các dịch vụ thư mục (directory services) hiện có và sử dụng thông tin đó trong mạng chuỗi khối. Các mạng chuỗi khối sử dụng dịch vụ thư mục hiện có có thể truy cập thông qua các giao thức hiện có, chẳng hạn như Giao thức truy cập thư mục nhẹ (LDAP) [10], và sử dụng trực tiếp thông tin từ thư mục, hoặc nhập thông tin đó vào Thẩm quyền chứng thực nội bộ trong mạng chuỗi khối.[5]

### 5.5 Lưu trữ khóa bí mật

Nếu người dùng mất khóa riêng, thì mọi tài sản số liên kết với khóa đó cũng sẽ bị mất, vì việc tái tạo cùng một khóa riêng là không khả thi về mặt tính toán. Nếu khóa riêng bị đánh cắp, kẻ tấn công sẽ có toàn quyền truy cập vào tất cả các tài sản số được kiểm soát bởi khóa riêng đó.

Do tầm quan trọng của việc bảo mật khóa riêng nên nhiều người dùng sử dụng phần cứng bảo mật chuyên dụng để lưu trữ khóa; hoặc, người dùng có thể tận dụng các dịch vụ lưu ký gửi khóa riêng, một lĩnh vực đang phát triển.

Các dịch vụ lưu ký khóa này cũng có thể tuân thủ các quy định về xác minh danh tính khách hàng (KYC) ngoài chức năng lưu trữ khóa riêng, vì người dùng phải cung cấp bằng chứng về danh tính khi tạo tài khoản. Việc lưu trữ khóa riêng là một khía cạnh vô cùng quan trọng của công nghệ chuỗi khối. Khi có thông tin trên báo chí rằng “tiền mã hóa XYZ đã bị đánh cắp từ…”, (một trong những vụ trộm tiền mã hóa lớn nhất từng xảy ra) [13], điều đó gần như chắc chắn có nghĩa là một số khóa riêng đã bị phát hiện và được sử dụng để ký một giao dịch chuyển tiền sang tài khoản mới, chứ không phải mạng chuỗi khối bị tấn công. Lưu ý rằng vì dữ liệu chuỗi khối nhìn chung không thể thay đổi nên một khi tội phạm đánh cắp khóa riêng và công khai thực hiện chuyển số tiền liên quan sang tài khoản khác, giao dịch đó nhìn chung không thể hoàn tác.

## 6 Các hoạt động bảo mật và bảo vệ quyền riêng tư

### 6.1 Các công cụ mật mã

Tính bảo mật của một cơ chế là yếu tố then chốt đối với sự an toàn và ổn định của hệ thống tài chính.

Các công cụ mật mã học, chẳng hạn như mật mã khóa công khai, đóng vai trò trung tâm trong việc bảo đảm an ninh cho các hệ thống hiện có, và có tầm quan trọng thiết yếu trong các cơ chế DLT.

Mặc dù các công cụ mật mã học hiện nay được xem là hiệu quả và được sử dụng rộng rãi, nhưng những tiến bộ công nghệ trong tương lai có thể khiến các công cụ mật mã hiện tại trở nên kém an toàn và kém hiệu quả hơn. Vấn đề này đặc biệt đáng lo ngại đối với các cơ chế có cấu trúc quản trị yếu [3], không thể phản ứng đủ nhanh trước các vấn đề và mối đe dọa bảo mật mới xuất hiện. Việc tích hợp công nghệ DLT vào hạ tầng hiện có, hoặc chuyển đổi từ hệ thống truyền thống sang hệ thống dựa trên DLT, cũng có thể phát sinh các lỗ hổng bảo mật, không phải do công nghệ DLT gây ra, nhưng lại có tác động vận hành đáng kể. Do đó, các cơ chế không chỉ phụ thuộc vào các công cụ mật mã, mà còn có thể áp dụng phương pháp tiếp cận bảo mật theo lớp và tận dụng các công cụ bổ sung.

Các câu hỏi cần được xem xét bao gồm:

- Những rủi ro vận hành chính đối với hệ thống là gì, đặc biệt là những rủi ro có thể ảnh hưởng đến khả năng phục hồi và độ tin cậy, bảo mật, năng lực vận hành và khả năng mở rộng? Hệ thống quản lý các rủi ro này như thế nào?

- Những rủi ro này và cách quản lý chúng khác với các hệ thống truyền thống như thế nào, nếu có?
- Cơ chế cần thích nghi như thế nào để áp dụng bảo mật theo lớp để thoát ra khỏi sự phụ thuộc vào mật mã học?

### 6.2 Hoạt động quản trị

Các cấu trúc quản trị có thể tăng cường tính an toàn của một cơ chế (ví dụ, bằng cách nâng cao năng lực ra quyết định liên quan đến thiết kế và cải tiến công nghệ của hệ thống, hoặc thông qua việc tham gia của hàng loạt các bên liên quan), hoặc cũng có thể làm suy yếu nó (ví dụ, bằng cách làm chậm phản ứng trước các sự cố vận hành trong trường hợp cấu trúc quản trị quá phức tạp). Một cơ chế liên quan đến chia sẻ thông tin và duy trì sổ cái sẽ cần có một cấu trúc quản trị đặc biệt được cân nhắc kỹ lưỡng. Những thách thức quản trị gần đây liên quan đến nhiều trường hợp sử dụng DLT không cần cấp phép đã làm nổi bật tầm quan trọng then chốt của việc hiểu rõ cơ chế quản trị, bao gồm: quản lý thay đổi, quản lý sự cố và thực thi các quyết định quản trị [4].
Ngành công nghiệp có kỳ vọng rất cao về các ứng dụng chuỗi khối như một công cụ mới giúp giảm chi phí trung gian và mang lại giá trị gia tăng như niềm tin và bảo mật. Những kỳ vọng cao từ cộng đồng về chủ đề này tạo ra rủi ro cho các ứng dụng trong tương lai, cũng như đối với cách chuỗi khối đang tác động đến xã hội. [16]

### 6.3 Hoạt động vận hành

Công nghệ sổ cái phân tán đặt ra những thách thức trong việc tích hợp với các mô đun bảo mật phần cứng (HSM) để lưu trữ và tạo khóa, cũng như với hạ tầng bảo mật như mạng riêng ảo (VPN). Các HSM thông thường không cung cấp các cơ chế phát hiện việc sử dụng sai khóa và không có cơ chế phê duyệt đa phương cho việc sử dụng khóa.. [17]
Các giải pháp DLT trong một tổ chức tài chính cũng có khả năng phải tích hợp với các hệ thống tài chính kế thừa đang chạy trên các nền tảng khác nhau, chẳng hạn như máy chủ mainframe, máy chủ web, máy chủ cơ sở dữ liệu và gần đây là các dịch vụ web hoặc microservices RESTful [19]
Các vấn đề liên quan đến tích hợp hệ thống kế thừa vẫn là thách thức liên tục đối với các tổ chức tài chính. Ví dụ, một tổ chức đang vận hành ứng dụng mainframe cần đến dịch vụ screen-scraping để cung cấp giao diện tự động với dữ liệu, đồng thời vẫn phải đảm bảo các quy tắc nghiệp vụ đã được xây dựng suốt hàng thập kỷ vẫn được áp dụng chính xác cho dữ liệu thô khi nhập vào hoặc trích xuất khỏi hệ thống.

Hầu hết các vấn đề tích hợp cần khắc phục liên quan đến hạ tầng DLT, mô hình bảo mật và độ phức tạp trong việc cho phép các hợp đồng thông minh chấp nhận dữ liệu từ các nguồn bên ngoài chuỗi.
Việc giải quyết các vấn đề này đòi hỏi một kiến trúc bảo mật thống nhất, có khả năng liên kết hệ thống tên người dùng và mật khẩu cũ (kế thừa) với hệ thống thư mục và Cơ sở hạ tầng khóa công khai (PKI) dành riêng cho DLT.
Điều quan trọng là thành phần bảo mật cao nhất (ví dụ, hạ tầng phần cứng PKI chống giả mạo) không bị tổn hại do việc triển khai bảo mật kém ở các nơi khác chẳng hạn như cơ sở dữ liệu mật khẩu không được mã hóa, kho khóa không an toàn, hoặc giao diện lập trình ứng dụng (API) mở.
Về bảo mật vật lý và môi trường, điều này thường bao gồm việc sử dụng các mô-đun bảo mật phần cứng (HSM), cùng với các biện pháp bảo vệ vật lý như camera giám sát (CCTV), rào chắn vật lý, các cơ chế bảo vệ bằng chìa  khóa truyền thống, và kiểm soát truy cập vật lý.

## 7 Kiểm soát đối với Blockchain và DLT

### 7.1 Kiểm soát kỹ thuật

Sự tồn tại của chuỗi khối không loại bỏ nhu cầu về các biện pháp kiểm soát kỹ thuật (xem Phụ lục B) trong tổ chức.
Các biện pháp kiểm soát như ISO/IEC 27001 (Hệ thống quản lý an toàn thông tin - ISMS) sẽ tiếp tục được áp dụng.

# 8 Quy trình bảo mật và quyền riêng tư

## 8.1 Tổng quan

Xem Bảng 1 để so sánh sự khác biệt giữa chuỗi khối công khai (public blockchain) và chuỗi khối riêng tư (private blockchain).

**Bảng 1 – Chuỗi khối công khai so với chuỗi khối riêng tư**

| | Chuỗi khối công khai | Chuỗi khối riêng tư |
|---|---|---|
| Tham gia vào mạng | Mở | Đóng |
| Bảo mật giao dịch | Các giao dịch thường được giả danh hóa và chỉ được liên kết trực tiếp với khóa công khai. Các giao dịch thực sự ẩn danh chỉ giới hạn ở một số ít dự án. | Tương tự chuỗi khối công khai, nhưng quyền riêng tư thường có thể được cải thiện bằng các phương pháp phù hợp hơn với chuỗi khối được cấp phép. |
| Khuyến khích kinh tế để tham gia | Được tích hợp sẵn | Được tổ chức theo hợp đồng |
| Tập trung hóa | Hoàn toàn phi tập trung | Mức độ phi tập trung khác nhau |
| Các mục đích sử dụng phổ biến | Thanh toán, chuyển tiền, thị trường dự đoán, lưu trữ phân tán, mạng xã hội trả phí | Dịch vụ tài sản, ngoại hối (FX), truy xuất nguồn gốc, tài trợ thương mại, y tế, hợp đồng bảo hiểm |

## 8.2 Khuyến nghị tiêu chuẩn về các quy trình bảo mật và quyền riêng tư của tổ chức

### 8.2.1 Tổng quan

Điều nhỏ này đưa ra khuyến nghị về phân tích rủi ro đối với chuỗi khối riêng tư (private blockchain) và chuỗi khối công khai (public blockchain).

### 8.2.2 Khuyến nghị tiêu chuẩn về phân tích rủi ro

Hồ sơ rủi ro của chuỗi khối công khai và chuỗi khối riêng tư khác nhau đáng kể. Là một công nghệ mới, chuỗi khối mang theo các rủi ro đặc thù mà các hệ thống CNTT khác không gặp phải, xem Bảng 2. Việc không đưa các rủi ro đặc thù của chuỗi khối vào đánh giá công nghệ có thể dễ dàng khiến các doanh nghiệp bị vi phạm bảo mật.

**Bảng 2 - Rủi ro và mối đe dọa đối với chuỗi khối công khai và riêng tư**

| Những rủi ro | Mối đe dọa | Biện pháp giảm thiểu |
|---|---|---|
| Chiến lược | Mạng được lựa chọn<br>Nền tảng cơ sở | |
| Cơ chế đồng thuận và quản lý mạng | Nguy cơ các giao dịch không phù hợp, không được phép, | Các biện pháp kiểm soát |

| Những rủi ro | Mối đe dọa | Biện pháp giảm thiểu |
|---|---|---|
| | hoặc không chính xác được ghi vào chuỗi khối | |
| An toàn thông tin | Chiếm đoạt tài khoản;<br>Tác nhân độc hại chiếm hơn 51% các node trong mạng | |
| Mật mã học, quản lý khóa và mã hóa token | Đánh cắp khóa riêng | Các quy trình đảm bảo quản lý những khóa này một cách phù hợp. Giám sát các nỗ lực truy cập trái phép vào khóa riêng. |
| Quản lý quyền truy cập chuỗi và quyền riêng tư | Việc sử dụng bởi các bên không được phép gây ra rủi ro nghiêm trọng đối với tính toàn vẹn và quyền riêng tư của chuỗi khối cũng như các giao dịch được ghi lại | Các chuỗi khối riêng tư yêu cầu xác thực danh tính của các thành viên tham gia, bên cạnh các chính sách và quy trình quản lý quyền truy cập người dùng. |
| Quản lý và phân tách dữ liệu | Quản lý tất cả các khía cạnh của dữ liệu, bao gồm tính bảo mật, tính toàn vẹn và tính sẵn sàng của dữ liệu | Dữ liệu được quản lý phù hợp. |
| Tính liên tác và tích hợp | Dữ liệu sai được ghi vào chuỗi khối | Kiểm tra toàn diện khả năng liên tác và tích hợp. Phát triển các biện pháp kiểm soát cho quy trình quản lý thay đổi và kiểm thử chuỗi khối.<br>Kiểm tra tính đầy đủ và chính xác. |
| Khả năng mở rộng và hiệu năng | Chuỗi khối phải hoạt động ổn định dưới áp lực của môi trường vận hành thực tế | Đánh giá liệu giải pháp có đủ năng lực triển khai thực tế hay không, và liệu nó có thể được mở rộng quy mô để phát triển và phù hợp với các trường hợp sử dụng trong tương lai hay không. |
| Tính liên tục hoạt động kinh doanh và khôi phục sau thảm họa | Phụ thuộc vào các thành viên khác của mạng chuỗi khối để duy trì chức năng hoạt động<br>Sự cố về công nghệ, vận hành cũng như các cuộc tấn công mạng. | Xây dựng kế hoạch đảm bảo tính liên tục hoạt động kinh doanh và khôi phục sau thảm họa.<br>Chính sách và tiêu chuẩn. |
| Quản trị, rủi ro và tuân thủ | Thay đổi phần mềm chuỗi khối, bổ sung nút mới hoặc các hoạt động khác | Xác định rõ ràng và tài liệu hóa vai trò, trách nhiệm và cơ chế giải trình.<br>Rà soát các yêu cầu và tiêu chuẩn pháp lý rộng hơn, bao gồm các quy định chuyên ngành và quy định áp dụng chung. |

### 8.3 Các yếu tố thiết kế kỹ thuật

Trong các giải pháp có liên quan đến Cơ sở hạ tầng khóa công khai (PKI), kế hoạch duy trì hoạt động kinh doanh (BCP) bao gồm việc đảm bảo tính toàn vẹn kỹ thuật của các cơ chế sinh khóa (các Thẩm quyền chứng thực - CA, các mô-đun bảo mật phần cứng - HSM), các quy trình nghiệp vụ liên quan đến việc vận chuyển an toàn khóa riêng, và lớp phân quyền xung quanh các cơ chế này.

Ngoài ra, các kế hoạch khôi phục hoạt động kinh doanh cần giải quyết các vấn đề như dự phòng và phòng tránh mất dữ liệu hoặc gián đoạn dịch vụ mà không làm tăng bề mặt tấn công và không làm giảm an toàn vận hành.

BCP cần có sự tham gia của các nhóm an ninh nội bộ, và có thể kết hợp sự thẩm định của các chuyên gia bên ngoài, để đảm bảo tuân thủ các thông lệ tốt nhất trong suốt quá trình thiết lập, triển khai và kiểm thử [11].

### 8.4 Rủi ro pháp lý

Việc có một cơ sở pháp lý có căn cứ đầy đủ, rõ ràng, minh bạch và có thể thực thi là yếu tố cốt lõi của các cơ chế thanh toán, bù trừ và quyết toán [5].
DLT có thể làm gia tăng rủi ro pháp lý nếu tồn tại sự mơ hồ hoặc thiếu chắc chắn về cơ sở pháp lý của cơ chế đó. Do việc áp dụng công nghệ này vào các hoạt động thanh toán, bù trừ và quyết toán còn mới, nền tảng pháp lý căn bản cho một số hoạt động chưa được xây dựng vững chắc như nền tảng pháp lý của các hệ thống truyền thống - ví dụ trong việc xác định quyền tài phán áp dụng hoặc các luật có liên quan.
Ngược lại, DLT có thể được sử dụng để giúp giảm thiểu một số rủi ro pháp lý nhất định. Ví dụ, tự động hóa một số điều khoản và điều kiện của các thỏa thuận có tính ràng buộc pháp lý - chẳng hạn như tự động hóa việc thanh toán lãi suất theo quy định của thỏa thuận hợp đồng - có thể giảm thiểu rủi ro các điều khoản hợp đồng không được thực thi đúng như quy định trong thỏa thuận trong khoảng thời gian đã thỏa thuận [4].

## 9 Triển khai PKI dựa trên Chuỗi khối

Dạng cho phép
Về loại quyền truy cập của chuỗi khối, tài liệu này trình bày về chuỗi khối không cần cấp phép (permission-less blockchain) và chuỗi khối được cấp phép (permissioned blockchain). Chuỗi khối không cần cấp phép, đôi khi còn được gọi là chuỗi khối công khai (public blockchain), được triển khai cho các ứng dụng quy mô Internet, chẳng hạn như xác minh chủ sở hữu tên miền. Ngược lại, chuỗi khối được cấp phép, hay còn gọi là chuỗi khối riêng tư (private blockchain), phù hợp hơn với các trường hợp sử dụng quy mô nhỏ, nơi chỉ có một số lượng hạn chế các bên tham gia. Do đó, cả hai loại chuỗi khối - được cấp phép và không cần cấp phép - đều có thể được sử dụng, tùy thuộc vào trường hợp ứng dụng và số lượng bên tham gia. Đối với phần lớn các ứng dụng triển khai Cơ sở hạ tầng khóa công khai (PKI) quy mô lớn, chuỗi khối không cần cấp quyền (công khai) thường được ưu tiên sử dụng nhằm nâng cao tính ổn định, bảo mật, minh bạch và mức chấp nhận của người dùng cuối.

Thu hồi chứng thư (Revocation):
Hỗ trợ việc thu hồi chứng thư là yếu tố bắt buộc trong một hệ thống PKI. Thu hồi là cơ chế duy nhất đảm bảo tính hợp lệ lâu dài của chứng thư số. Theo mô hình truyền thống, quá trình thu hồi được quản lý bởi các bên thứ ba đáng tin cậy. Khi ứng dụng công nghệ chuỗi khối, niềm tin này được phân tán cho tất cả các thực thể trong mạng lưới. Do đó, việc chia sẻ thông tin thu hồi thông qua chuỗi khối là hoàn toàn khả thi trên thực tế.

Định dạng chứng thư (Certificate Format):
Cần giới hạn số lượng phần mở rộng tùy chỉnh ở mức tối thiểu để hỗ trợ định dạng chứng thư tiêu chuẩn.

Loại PKI (PKI Type):
Các trường hợp sử dụng theo miền ứng dụng cụ thể, thường có tính phi tập trung, có thể được hưởng lợi từ cấu trúc PKI phân cấp.

Loại lưu trữ (Storage Type):
Chỉ lưu trữ lượng dữ liệu tối thiểu trên chuỗi khối vì lý do chi phí và hiệu năng

Khóa có thể cập nhật (Updatable Key):
Các ứng dụng dài hạn cần hỗ trợ chức năng cập nhật khóa của thẩm quyền phát hành (CA phát hành)

Quyền riêng tư (Privacy):
Chọn nguyên tắc bảo vệ quyền riêng tư ngay từ khâu thiết kế (Privacy by design) và các công nghệ tăng cường quyền riêng tư (privacy-enhancing technologies) phù hợp. Yêu cầu đối với các công nghệ tăng cường quyền riêng tư phụ thuộc vào từng trường hợp sử dụng. Cần xem xét các yêu cầu pháp lý về quyền riêng tư, ví dụ như trong trường hợp PKI liên kết các cá nhân với dữ liệu nhận dạng cá nhân.
Cơ chế khuyến khích (Incentives):
Các cơ chế khuyến khích cho người tham gia là cần thiết để thiết lập một cơ sở hạ tầng ổn định trên các chuỗi khối tùy chỉnh. Cũng lưu ý rằng hai điểm hạn chế được xác định là: thiếu quyền riêng tư và thiếu cơ chế kiểm định. Quyền riêng tư là yếu tố thiết yếu do các yêu cầu pháp lý liên quan đến cá nhân chịu sự điều chỉnh của luật bảo vệ dữ liệu. Tham khảo thêm tại [8].

# Phụ lục A

(Tham khảo)

## A.1 Các trường hợp sử dụng tham khảo

a) Một dịch vụ ví tiền mã hóa lớn đã triển khai sản phẩm cho vay mới dành cho tất cả người dùng, không chỉ riêng các tổ chức. Dịch vụ cho vay tiền mã hóa này được triển khai tới người dùng tại hơn 180 quốc gia.

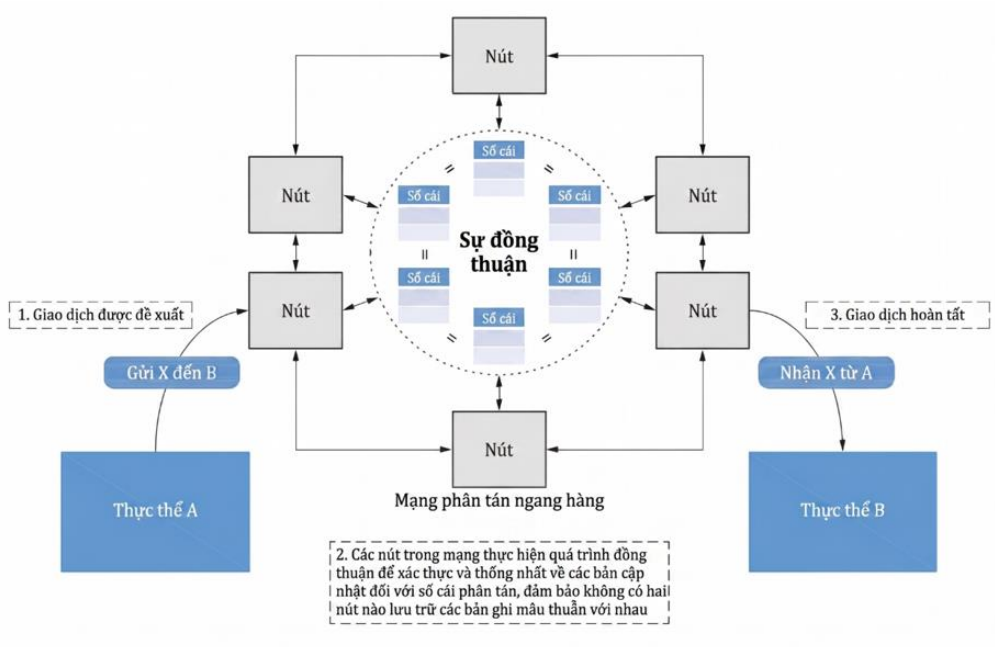
b) Một sàn giao dịch tiền mã hóa có trụ sở tại Hoa Kỳ công bố việc mở rộng sang lĩnh vực giao dịch ngoại hối truyền thống, với chín cặp tiền pháp định mới được giao dịch trực tiếp từ ngày 12 tháng 3 năm 2020. Người dùng trên toàn thế giới - ngoại trừ cư dân Hoa Kỳ - sẽ có thể sử dụng nền tảng này để giao dịch trực tiếp giữa Euro, đô la Mỹ, đô la Canada, yên Nhật, bảng Anh và franc Thụy Sĩ.
c) Người dùng ứng dụng di động của một công ty cà phê sắp tới sẽ được cung cấp tùy chọn thanh toán đồ uống. Công ty này đang xem xét các ứng dụng bán lẻ.

d) Sơ đồ mô phỏng hóa một hệ thống thanh toán dựa trên DLT được thể hiện tại Hình A.1. Trong ví dụ tại Hình A.1, quy trình giao dịch bao gồm ba bước chính:

1. Để khởi tạo thanh toán, thực thể A sử dụng các công cụ mật mã để ký số điện tử một bản cập nhật đề xuất cho sổ cái chung, nhằm chuyển tiền từ tài khoản của mình trên sổ cái sang tài khoản của thực thể B.

2. Khi nhận được yêu cầu chuyển tiền, các nút khác xác thực danh tính của thực thể A và xác nhận tính hợp lệ của giao dịch bằng cách kiểm tra để đảm bảo rằng thực thể A có đủ thông tin xác thực mật mã cần thiết để thực hiện cập nhật cho bản ghi liên quan. Quá trình xác thực bao gồm, nhưng không giới hạn ở, việc kiểm tra xem thực thể A có đủ tiền để thực hiện thanh toán hay không. Các nút cũng tham gia vào quá trình đồng thuận để thống nhất về các khoản thanh toán được đưa vào bản cập nhật tiếp theo của trạng thái sổ cái.

3. Sau khi bản cập nhật được các nút chấp nhận, thuộc tính của tài sản được sửa đổi để tất cả các giao dịch liên quan đến tài sản trong tương lai sẽ được khởi tạo bằng thông tin xác thực mật mã của thực thể B.




**Hình A.1 – Sơ đồ xử lý mô phỏng của hệ thống thanh toán dựa trên DLT**

## A.2 Kế hoạch duy trì hoạt động kinh doanh (BCP) với Cơ sở hạ tầng khóa công khai (PKI)

Trong các giải pháp có liên quan đến PKI, BCP bao gồm việc đảm bảo tính toàn vẹn kỹ thuật của các cơ chế tạo khóa - Thẩm quyền chứng thực (CA), các mô-đun bảo mật phần cứng (HSM) - các quy trình nghiệp vụ liên quan đến việc chuyển giao khóa riêng một cách an toàn, và lớp phân quyền bao quanh các cơ chế này. Ngoài ra, các kế hoạch khôi phục hoạt động kinh doanh cần giải quyết các vấn đề như dự phòng và ngăn ngừa mất dữ liệu hoặc gián đoạn dịch vụ mà không làm tăng bề mặt tấn công và không làm suy giảm bảo mật vận hành. BCP cần có sự tham gia của các nhóm an ninh nội bộ, đồng thời có thể cần xác nhận từ các chuyên gia bên ngoài, nhằm đảm bảo các thực hành tốt nhất được tuân thủ trong suốt quá trình thiết lập, triển khai và kiểm thử.

Chuỗi khối vẫn chưa được kiểm nghiệm ở quy mô rộng trong các môi trường chịu sự quản lý nghiêm ngặt. Các sàn giao dịch, ngân hàng và công ty quản lý quỹ đều đã từng bị ảnh hưởng bởi tội phạm mạng, và các cơ quan quản lý yêu cầu các tổ chức tài chính này phải đảm bảo rằng cả hệ thống bảo vệ an ninh mạng nội bộ của họ lẫn các biện pháp bảo vệ an ninh mạng tại các nhà cung cấp dịch vụ đều đáp ứng các tiêu chuẩn phù hợp.

## A.3 Triển khai Cơ sở hạ tầng khóa công khai (PKI) và Blockchain

Dù kết quả cuối cùng vẫn chưa được xác định, nhưng hiện nay người ta cho rằng công nghệ Chuỗi khối hưởng lợi từ PKI và các công nghệ định danh khác, hơn là thay thế chúng. Về bản chất, Chuỗi khối là một sổ cái chia sẻ - cung cấp cơ chế để nhiều bên tham gia đạt được sự đồng thuận về nội dung của sổ cái theo cách phi tập trung. Các bên tham gia này thường được gọi là mạng lưới Chuỗi khối.

Việc sử dụng hệ mật mã khóa công khai hay còn gọi là mật mã khóa phi đối xứng cùng với Chuỗi khối yêu cầu khóa riêng phải được bảo vệ ở mức cao nhất - bởi vì nếu mất khóa riêng trong Bitcoin, điều đó về cơ bản đồng nghĩa với việc mất tiền. Với tất cả những thông tin trên, rõ ràng Chuỗi khối có ý nghĩa đáng kể trong một số ứng dụng nhất định. Các thử nghiệm do ngành ngân hàng thực hiện là ví dụ điển hình cho thấy cách Chuỗi khối có thể bảo mật các giao dịch chuyển tiền ngân hàng. Tuy nhiên, vì Chuỗi khối vẫn là công nghệ mới nên vẫn còn nhiều tiềm năng phát triển và cải tiến. Trong Chuỗi khối của

Bitcoin, sổ cái chứa các giao dịch liên quan đến việc trao đổi tiền tệ, nhưng trong trường hợp tổng quát hơn, nội dung sổ cái có thể là bất cứ thứ gì.

Đối với Cơ sở hạ tầng khóa công khai PKI, người ta cho rằng cấu trúc cơ bản vẫn sẽ giữ nguyên. Điều này có nghĩa là CA sẽ phát hành và quản lý các chứng thư số cần thiết cho các danh tính số đáng tin cậy nhằm thực hiện xác thực mạnh, chữ ký số và mã hóa dữ liệu. Tuy nhiên, thay vì vận hành hạ tầng trên một máy tính riêng đòi hỏi nhiều công tác bảo trì, CA sẽ được vận hành trên Chuỗi khối - thay thế một máy tính riêng lẻ bằng một nhóm máy tính kết nối, nơi nội dung sổ cái có thể được truy cập bởi bất kỳ ai, từ đó làm cho PKI trở nên đáng tin cậy và vững chắc hơn.

Việc triển khai PKI trên Chuỗi khối mang lại nhiều ưu điểm vượt trội so với PKI truyền thống, bao gồm:
- Các chứng thư số không cần ký, dẫn đến kích thước nhỏ hơn, từ đó giảm thời gian truyền chứng thư được xác nhận bởi chuỗi chứng thư CA.
- Việc xác thực một chứng thư số và chuỗi chứng thư CA của nó là rất quan trọng. Tuy nhiên, vì Chuỗi khối là sổ cái phân tán, bên xác thực có bản sao cục bộ của toàn bộ chuỗi khối và có thể tra cứu các giá trị băm của chứng thư trong kho lưu trữ trên chuỗi khối - do đó không cần xác minh chữ ký. Lưu ý rằng phương pháp thiết kế này cần được giải thích thêm.
- PKI dựa trên Chuỗi khối [6] giải quyết một vấn đề tồn tại lâu dài của PKI truyền thống nhờ không cần sử dụng danh sách thu hồi chứng thư (CRL) hoặc các phản hồi từ giao thức trạng thái chứng thư trực tuyến (OCSP) [11]. Điều này là do nhờ sự đồng bộ hóa chuỗi khối giữa các nút trong mạng, bất kỳ thay đổi nào đối với trạng thái của chứng thư sẽ được thông báo ngay lập tức tới tất cả các nút. Đây là một lợi thế đáng kể, bởi các danh sách CRL có thể tiêu tốn lượng lớn dữ liệu, gây ảnh hưởng đến hiệu suất xử lý tổng thể.

### A.4 Cách chuỗi khối khắc phục các hạn chế của Cơ sở hạ tầng khóa công khai (PKI)

Cơ sở hạ tầng khóa công khai truyền thống có những hạn chế nhất định - bao gồm việc nó dựa trên thiết kế lỗi thời và mang lại sự phức tạp cho bất kỳ doanh nghiệp nào trong quá trình quản lý [14]. Chuỗi khối đang nổi lên như một nền tảng cho thế hệ ứng dụng tiếp theo, cung cấp nền tảng hiện đại cho doanh nghiệp nhằm giúp PKI hoạt động hiệu quả hơn. Thiết kế ứng dụng đã thay đổi đáng kể kể từ khi PKI xuất hiện. Với điện toán đám mây và tính di động, nhân viên không còn bị ràng buộc vào bàn làm việc khi truy cập các dịch vụ máy tính. Do đó, một nền tảng mới là cần thiết để bảo vệ các ứng dụng như vậy, vì không còn tồn tại kết nối tập trung đơn giản từ thiết bị đầu cuối đến máy chủ.

Chuỗi khối được xây dựng để đáp ứng nhu cầu kinh doanh ngày nay. Kiến trúc của nó [3] dựa trên một cơ sở dữ liệu phân tán, duy trì một danh sách bản ghi được sắp xếp theo thứ tự và liên tục tăng thêm, gọi là các khối. Vì Chuỗi khối chạy đồng thời trên hàng chục nghìn máy tính, thiết kế này loại bỏ các rủi ro vốn tồn tại trong các hệ thống PKI thế hệ cũ.

Chuỗi khối có kiến trúc mở, minh bạch và an toàn. Người dùng được xác thực trên Chuỗi khối có thể đọc toàn bộ nội dung của nó. Tính năng này loại bỏ các vấn đề tiềm ẩn xuất phát từ việc phải phụ thuộc vào hành động của các CA bên thứ ba. Các công ty không còn cần đặt niềm tin vào các CA có thể có hành vi gian lận hoặc dễ xảy ra lỗi khi tạo khóa công khai và khóa riêng. Mọi sự kiện xảy ra trên Chuỗi khối đều có thể được xem bởi tất cả người dùng. Do đó, nếu một CA phát hành khóa dưới tên người khác, thông tin sẽ được mọi người trong chuỗi nhìn thấy. Mọi thông tin đều được gắn dấu thời gian, và một bản ghi sẽ được tạo mỗi khi có cập nhật - do đó có thể xác định rõ ràng ai đã thực hiện hành động gì và vào thời điểm nào. Việc thay đổi bản ghi giao dịch trên sổ cái là điều không thể: một kẻ tấn công sẽ phải thay đổi mọi mục trong Chuỗi khối thay vì chỉ một bản ghi. Giải pháp này bảo vệ thông tin theo cách phân tán an toàn và phù hợp hơn với nhu cầu hiện nay so với các hệ thống PKI truyền thống.

Các giải pháp triển khai PKI trên Chuỗi khối đang dần xuất hiện từ các nhà cung cấp. PKI từng là lựa chọn khả thi khi các ứng dụng được xử lý trên các máy chủ tập trung. Khi ngành công nghiệp chuyển sang mô hình xử lý phân tán, nhu cầu về một phương pháp tiếp cận mới trở nên rõ ràng. Chuỗi khối cung cấp một nền tảng vững chắc để xây dựng giải pháp bảo mật phân tán, và sự quan tâm của các tổ chức đối với công nghệ này đang không ngừng gia tăng.

## A.5 Ví dụ về các giải pháp

Các giải pháp hiện có cho các vấn đề được liệt kê trong mục 5.2.1 có thể được phân thành ba nhóm chính, như sau.

Nhóm thứ nhất bao gồm các giải pháp dựa trên việc tạo ra một hoặc nhiều máy chủ hoạt động song song với các máy chủ đã có sẵn (ví dụ: các máy chủ OCSP). Nhiệm vụ của chúng là trả lời các câu hỏi về tính hợp lệ của chứng thư số. Các máy chủ này cần có hiệu năng cao, hoạt động nhanh, an toàn và đơn giản. Trong nhóm này có mô hình PKI dựa trên nhật ký (log), trong đó các máy chủ nhật ký công khai có tính sẵn sàng cao sẽ giám sát và công bố nhật ký các chứng thư số được cấp bởi CA, bảo đảm rằng chỉ những chứng thư số được liệt kê trong nhật ký đã công bố mới được chấp nhận và tin cậy bởi người dùng cuối. Đã có các đề xuất mở rộng nhật ký để bao gồm cả chứng thư số bị thu hồi, nhưng chưa có giải pháp nào được triển khai rộng rãi. Nhóm này cũng bao gồm các giải pháp OCSP nhằm hỗ trợ CRL hoặc các cơ chế xử lý lỗi khác liên quan đến thu hồi chứng thư số. Ý tưởng ở đây là tạo ra một siêu CA (super-CA) có nhiệm vụ phối hợp và hỗ trợ hoạt động của các CA khác. Tuy nhiên, các giải pháp này vẫn gặp phải những điểm yếu vốn có của PKI truyền thống, vì kiến trúc cơ bản về bản chất không thay đổi.

Nhóm thứ hai bao gồm các giải pháp xuất phát từ các mạng ngang hàng (peer-to-peer) phi tập trung, được gọi là Mạng lưới tin cậy (Web of Trust — WoT). Trong mô hình này, chức năng tin cậy được xây dựng dựa trên mạng xã hội để thay thế cho khái niệm thẩm quyền và CA truyền thống. Chức năng tin cậy này có thể được sử dụng để áp đặt giá trị của một chứng thư số trong mối liên kết giữa một chủ thể và khóa công khai của nó. Một người dùng sẽ tích lũy chứng thư số chứa khóa công khai của mình cùng với các chữ ký số từ các thực thể khác nhìn nhận họ là đáng tin cậy.

Nhóm thứ ba sử dụng DLT để xây dựng một phương thức triển khai mới cho việc quản lý chứng thư số X.509 dựa trên Chuỗi khối, nhằm giải quyết vấn đề quản lý tin cậy trong khi vẫn duy trì phần lớn hạ tầng PKI hiện có. Giải pháp này yêu cầu:

- Một cộng đồng các nút độc lập, trong đó mỗi thành viên đều kiểm tra các chứng thư số;
- Kết quả của quá trình kiểm tra được chia sẻ trong cộng đồng, thông qua cơ chế phê duyệt;
- Các kết quả thu được được lưu giữ bất biến và chống giả mạo.

Với cách tiếp cận này, có thể phát hiện chính xác mọi hành vi sai trái của các tác nhân trong hệ sinh thái PKI. Các lỗi có thể được phân biệt rõ ràng với các cuộc tấn công, và các cuộc tấn công đã đề cập trước đó có thể được giảm thiểu. Để biết thêm thông tin, xem [10]

# Phụ lục B

(Tham khảo)

## B.1 Kiểm soát đối với Chuỗi khối và công nghệ sổ cái phân tán (DLT)

### B.1.1 Kiểm soát kỹ thuật

Việc triển khai chuỗi khối không loại bỏ nhu cầu áp dụng các biện pháp kiểm soát kỹ thuật trong tổ chức. Các biện pháp kiểm soát theo ISO/IEC 27001 (Hệ thống quản lý an toàn thông tin) sẽ tiếp tục được áp dụng.

Các biện pháp kiểm soát điển hình mà tổ chức áp dụng công nghệ chuỗi khối cần tuân thủ bao gồm:

- Chính sách an toàn thông tin. Ai có quyền truy cập dữ liệu? Mục đích của nền tảng là gì? Dữ liệu được lưu trữ có mức độ nhạy cảm như thế nào? Có yêu cầu bắt buộc về thời hạn lưu trữ và tiêu hủy dữ liệu không? Đây chỉ là một số trong nhiều vấn đề liên quan đến chính sách an toàn thông tin mà tổ chức cần giải quyết.
- Kiểm soát an ninh nhân sự. Đây là các quy trình đảm bảo quyền truy cập vào hệ thống chuỗi khối được cập nhật khi nhân viên rời khỏi tổ chức hoặc thay đổi vị trí công tác.
- Kiểm soát quản lý tài sản và xây dựng hướng dẫn xác định quyền sở hữu hệ thống DLT. Bao gồm hướng dẫn làm rõ quyền sở hữu thiết bị vật lý (dùng để lưu trữ khóa ký) và máy tính xách tay được cài đặt chứng thư bảo mật.
- Kiểm soát truy cập trên chuỗi khối. Bao gồm các vai trò và phân quyền bảo mật, cùng các kiểm soát nhằm đảm bảo các quy trình phê duyệt được tuân thủ khi cấp quyền tạo, đọc, cập nhật hoặc xóa dữ liệu trên chuỗi khối.
- Kiểm soát an ninh vật lý và môi trường. DLT sẽ yêu cầu quản lý khóa chuyên biệt.
- Kiểm soát an ninh vận hành. Bao gồm các biện pháp kiểm soát hạ tầng tiêu chuẩn như lịch trình kiểm tra vi-rút, khắc phục lỗ hổng zero-day, lịch bảo trì, quản lý dung lượng và sao lưu. Một nút sổ cái phân tán trong chuỗi khối riêng tư vẫn là sự kết hợp giữa dữ liệu và phần mềm chạy trên một hoặc nhiều máy chủ, thường nằm trong mạng riêng ảo (VPN). Các biện pháp kiểm soát tiêu chuẩn sẽ tiếp tục được áp dụng cho môi trường vận hành.
- Kiểm soát mật mã. Đặc biệt quan trọng trên các nền tảng mà việc xác thực dựa trên sở hữu khóa mật mã.
- Kiểm soát quản lý sự cố an toàn thông tin. Trong trường hợp xảy ra vi phạm bảo mật, các biện pháp kiểm soát này áp dụng cho quy trình báo cáo, leo thang và ứng phó sự cố, và có vai trò quan trọng trong việc triển khai DLT một cách an toàn.

CHÚ THÍCH rằng trong mô hình quản trị chia sẻ điển hình, việc thiết lập một bộ tiêu chuẩn các biện pháp kiểm soát giữa tất cả các bên là điều thiết yếu.

Các giao diện này thường được bảo vệ thông qua hệ thống xác thực thông tin mạng (liên kết với thư mục nội bộ doanh nghiệp) hoặc cơ chế xác thực mật khẩu tùy chỉnh. Các cơ chế bảo mật đa lớp này cần hoạt động mà không làm gia tăng bề mặt tấn công, đồng thời vẫn đảm bảo an ninh cho hệ thống có khả năng chứa dữ liệu của nhiều tổ chức khác nhau theo mô hình liên minh vốn phổ biến trong hầu hết các triển khai chuỗi khối.

Phần lớn các vấn đề tích hợp cần được giải quyết liên quan đến hạ tầng DLT, mô hình bảo mật và sự phức tạp trong việc cho phép các hợp đồng thông minh tiếp nhận các nguồn dữ liệu ngoài chuỗi. Việc xử lý các vấn đề này đòi hỏi một kiến trúc bảo mật thống nhất, kết hợp cả hệ thống tên người dùng và mật khẩu kế thừa với các hệ thống thư mục và Cơ sở hạ tầng khóa công khai (PKI) đặc thù của DLT. Điều tối quan trọng là thành phần bảo mật nhất — tức là hạ tầng phần cứng PKI chống giả mạo — không bị làm suy yếu bởi việc triển khai bảo mật kém ở các thành phần khác, chẳng hạn như: cơ sở dữ liệu mật khẩu không được mã hóa, kho khóa không được bảo vệ, hoặc các Giao diện lập trình ứng dụng (API) để mở.

## Thư mục tài liệu tham khảo

[1] ISO/DTR 23245 Blockchain and distributed ledger technologies — Security risks, threats, and vulnerabilities. Geneva: ISO

[2] ISO 22739:2024 Blockchain and distributed ledger technologies — Vocabulary and ISO 23257:2022 Blockchain and distributed ledger technologies — Reference architecture. Geneva: ISO

[3] ISO/TS 23635:2022 Blockchain and distributed ledger technologies — Guidelines for governance. Geneva: ISO, 2022.

[4] TREAT, David B. Blockchain security made simple [online]. Accenture Consulting, 2017. Available from: https://www.accenture.com/gb-en/service-blockchain-security

[5] COMMITTEE ON PAYMENTS AND MARKET INFRASTRUCTURES. Distributed ledger technology in payment, clearing and settlement [online]. Bank for International Settlements (BIS), 2017. Available from: https://www.bis.org/cpmi/publ/d157.htm

[6] LEWISON, K. and CORELLA, F. Backing rich credentials with a blockchain PKI. Pomcor [online]. 2016. Available from: https://pomcor.com/techreports/BlockchainPKI.pdf

[7] DE VRIES, Dennis. Realizing blockchain's potential [online]. KPMG International, 2017. Available from: https://assets.kpmg/content/dam/kpmg/xx/pdf/2018/09/realizing-blockchains-potential.pdf

[8] BRUNNER, Clemens, KNIRSCH, Fabian, UNTERWEGER, Andreas and ENGEL, Dominik. A Comparison of Blockchain-based PKI Implementations. In: Center for Secure Energy Informatics [online]. Salzburg University of Applied Sciences, 2020. Available from: https://www.en-trust.at/papers/Brunner20a.pdf

[9] COMMITTEE ON PAYMENTS AND MARKET INFRASTRUCTURES. Distributed ledger technology in payment, clearing and settlement [online]. Bank for International Settlements (BIS), 2017. Available from: https://www.bis.org/cpmi/publ/d157.htm

[10] TALAMO, Maurizio, ARCIERI, Franco, DIMITRI, Andrea and SCHUNCK, Christian H. A Blockchain based PKI Validation System based on Rare Events Management. Future Internet [online]. 2020, 12(2), 40. Available from: https://www.researchgate.net/publication/339345769_A_Blockchain_based_PKI_Validation_System_based_on_Rare_Events_Management

[11] LIU, Yang, HE, Debiao, OBAIDAT, Mohammad S., KUMAR, Neeraj, KHAN, Muhammad Khurram and CHOO, Kim-Kwang Raymond. Blockchain-based identity management systems: A review. Journal of Network and Computer Applications [online]. 2020, 166. Available from: https://www.sciencedirect.com/science/article/pii/S1084804520302058

[12] SOULSKILL. CAs compromised. Slashdot [online]. 28 October 2011. Available from: https://tech.slashdot.org/story/11/10/28/1954201/four-cas-have-been-compromised-since-june

[13] CNBC. One of the biggest crypto heists. CNBC [online]. 11 August 2021. Available from: https://www.cnbc.com/2021/08/11/cryptocurrency-theft-hackers-steal-600-million-in-poly-network-hack.html

[14] PROTOCOL BY REMME. How Blockchain Addresses Public Key Infrastructure Shortcomings. Infosecurity Magazine [online]. 2020. Available from: https://www.infosecurity-magazine.com/opinions/blockchain-pki-shortcomings-1-1/

[15] HADAN, Hilda, SERRANO, Nicolas and CAMP, L. Jean. A holistic analysis of web-based public key infrastructure failures: comparing experts' perceptions and real-world incidents. Journal of Cybersecurity [online]. 2021, 7(1), tyab025. Available from: https://doi.org/10.1093/cybsec/tyab025

[16] TASCA, Paolo and TESSONE, Claudio J. A taxonomy of blockchain technologies: Principles of identification and classification. Ledger [online]. 2019, 4. DOI: 10.5195/ledger.2019.140

[17] DVORIN, Tova. Points of Failure: Why HSMs Fall Short for Securing Digital Assets. Medium [online]. 2019. Available from: https://medium.com/block-to-basics/points-of-failure-why-hsms-fall-short-for-securing-digital-assets-db5c076d6126

[18] NIST. Merkle tree. In: Dictionary of Algorithms and Data Structures [online]. National Institute of Standards and Technology. Available from: https://xlinux.nist.gov/dads/HTML/MerkleTree.html

[19] RESTful microservices [online]. Available from: https://openliberty.io/docs/latest/test-microservices.html