

HỌC VIỆN KỸ THUẬT MẬT MÃ
KHOA AN TOÀN THÔNG TIN



CÔNG NGHỆ BLOCKCHAIN

Đề tài:

**Nghiên cứu một số tiêu chuẩn quốc tế trong triển khai ứng dụng
Blockchain**

Sinh viên thực hiện:

Phạm Anh Minh - AT160148

Phạm Công Hưởng - AT160230

Trần Nhật Nam - AT160536

Giảng viên hướng dẫn: Trương Phi Hồ

Hà Nội, tháng 5 năm 2023

MỤC LỤC

MỤC LỤC	i
DANH MỤC TỪ VIẾT TẮT	vi
DANH MỤC HÌNH ẢNH VÀ BẢNG	vii
TÓM TẮT NỘI DUNG ĐỀ TÀI.....	viii
LỜI NÓI ĐẦU	x
Chương 1. Tổng quan các vấn đề liên quan đến các tiêu chuẩn kỹ thuật Blockchain	1
1.1 Phân tích ban đầu	1
1.1.1 Giới thiệu.....	1
1.1.2 Động lực và phạm vi	2
1.1.3 Phương pháp luận.....	3
1.2 Tổng quan	3
1.2.1 Vai trò phát triển của các tiêu chuẩn.....	3
Box 1: Tiêu chuẩn hành động: email.....	4
1.2.2 Sự phát triển không ngừng của các tiêu chuẩn.....	4
1.2.3 Xem xét kỹ hơn: các tiêu chuẩn blockchain.....	5
1.2.3.1 Cài đặt tiêu chuẩn	5
Box 2: Nghiên cứu điển hình: ICO, CryptoKitties và hơn thế nữa – Tiêu chuẩn mã thông báo ERC	6
1.2.3.2 Phát triển phần mềm.....	7
1.2.3.3 Quản trị mạng	7
1.2.4 Ngoài tiêu chuẩn: định mức ngành.....	8
1.3 Những phát hiện chính	8
1.3.1 Thuật ngữ vẫn không nhất quán	8
1.3.2 Khối lượng hoạt động đã phản ánh sự cường điệu xung quanh công nghệ	10
1.3.3 Phạm vi của các tiêu chuẩn blockchain vẫn chưa rõ ràng.....	10

1.3.4 Có sự chồng chéo trong bối cảnh thiết lập tiêu chuẩn.....	11
1.3.5 Có những khoảng trống và sự phân kỳ trong bối cảnh thiết lập tiêu chuẩn.....	12
1.3.6 Các phương pháp tốt nhất để phổ biến / thực hiện các tiêu chuẩn đang được tranh luận	14
Box 3: Nghiên cứu điển hình: Các tiêu chuẩn để tạo điều kiện thuận lợi cho việc thực hiện quy tắc du lịch của FATF	14
1.3.7 Đại diện địa lý trong các sáng kiến thiết lập tiêu chuẩn khác nhau	16
1.3.8 Chuyên môn và đại diện người tiêu dùng khác nhau	17
1.3.9 Những cân nhắc về sở hữu trí tuệ vẫn chưa rõ ràng.....	17
1.4 Tổng kết	18
Box 4: Những nỗ lực thiết lập tiêu chuẩn chính - quy trình đề xuất	25
Chương 2. Tiêu chuẩn ISO/TC 307.....	26
2.1 Tóm tắt điều hành	26
2.2 Giới thiệu	27
2.2.1 Ủy ban kỹ thuật ISO và lập kế hoạch kinh doanh	27
2.2.2 Tiêu chuẩn hóa quốc tế và vai trò của ISO	27
2.3 Môi trường kinh doanh của ISO / TC	29
2.3.1.1 Mô tả môi trường kinh doanh.....	29
2.3.1.2 Các chỉ tiêu định lượng môi trường kinh doanh	31
2.4 LỢI ÍCH MONG ĐỢI TỪ CÔNG VIỆC CỦA ISO / TC	34
2.5 ĐẠI DIỆN VÀ THAM GIA ISO / TC	35
2.5.1 Thành viên	35
2.5.2 Phân tích sự tham gia	35
2.6 Mục tiêu của ISO / TC và các chiến lược cho thành tích	36
2.6.1 Mục tiêu xác định của ISO/TC	36
2.6.2 Xác định các chiến lược để đạt được các mục tiêu đã xác định của ISO / TC	37

2.7 CÁC YẾU TỐ ẢNH HƯỞNG ĐẾN VIỆC HOÀN THÀNH VÀ THỰC HIỆN CHƯƠNG TRÌNH LÀM VIỆC ISO / TC	37
Chương 3. Tiêu chuẩn DIN SPEC 3104.....	40
3.1 Phạm vi	40
3.2 Tài liệu tham chiếu	41
3.3 Thuật ngữ và định nghĩa	41
Độ chính xác.....	42
Xác thực Blockchain	42
Chứng minh tính chính xác của blockchain	42
Dấu thời gian của blockchain	42
Cây nhị phân đầy đủ.....	42
Mật mã học	42
Chữ ký và chữ ký số.....	42
Dấu thời gian điện tử.....	43
Nút lá	43
Chứng minh tính chính xác	43
Proof of work (PoW).....	43
Phần mềm	43
Trạng thái của blockchain.....	43
Đơn vị thời gian.....	43
Khoảng thời gian	43
Dấu thời gian	43
3.4 Các đặc điểm chung của việc xác thực blockchain	44
3.5 Khung kỹ thuật của quá trình xác thực blockchain	45
3.5.1 Các bước của quá trình xác thực blockchain.....	45
3.5.2 Thành phần mật mã học	45
3.5.2.1 Hàm băm	45
3.5.2.2 Chữ ký kỹ thuật số.....	46
3.5.2.3 Đầu ra của quá trình xác thực blockchain	46
3.6 Khung kỹ thuật của quá trình xác minh xác thực blockchain	47

3.6.1 Giới thiệu.....	47
3.6.2 Các bước của quá trình xác minh xác thực blockchain hiện có	47
3.7 Các yếu tố trong quá trình xác minh một dấu thời gian trên blockchain hiện có	48
3.7.1 Tổng quan và quy tắc ứng dụng	48
3.7.2 Khẳng định	48
3.7.3 Đánh giá tính không thay đổi (dựa trên bằng chứng công việc)	48
3.7.4 Độ chính xác của dấu thời gian trên blockchain	50
Chương 4. Đánh giá và đề xuất	51
4.1 Đánh giá	51
4.1.1 Tổng quan về Bitcoin	51
4.1.1.1 Khái niệm Bitcoin.....	51
4.1.1.2 Kiến trúc của Bitcoin.....	52
4.1.1.3 Giao dịch trong Bitcoin	57
4.1.2 Thực tế và thách thức của Bitcoin	57
4.1.2.1 Các công nghệ mở rộng mạng lưới trong Bitcoin	57
4.1.2.2 Các tấn công vào mạng lưới Bitcoin	60
4.1.2.3 Các hạn chế và thách thức của Bitcoin.....	68
4.1.3 Đánh giá ba tiêu chuẩn cho Bitcoin.....	71
4.1.3.1 Lựa chọn tiêu chuẩn và tiêu chí so sánh tiêu chuẩn	71
4.1.3.2 Ba tiêu chuẩn cho Bitcoin	72
4.2 Đề xuất	92
4.2.1 Quy định	94
4.2.2 Đổi mới và áp dụng blockchain có trách nhiệm.....	94
4.2.2.1 Tuân thủ và gắn kết.....	94
4.2.2.2 Quản trị, minh bạch và trách nhiệm giải trình.....	95
4.2.2.3 Khả năng tương tác.....	95
4.2.2.4 Bảo mật và quyền riêng tư kỹ thuật số	95
4.2.2.5 Giáo dục và phát triển kỹ năng.....	96
4.2.2.6 Tác động môi trường	96

4.2.3 Chính sách quốc gia và hợp tác quốc tế	96
4.2.4 Khuyến nghị chính	98
4.2.4.1 Đối với các thực thể thiết lập tiêu chuẩn	98
4.2.4.2 Đối với đơn vị áp dụng tiêu chuẩn kỹ thuật	101
KẾT LUẬN.....	103
TÀI LIỆU THAM KHẢO	105
PHỤ LỤC.....	107
<i>Phân công công việc</i>	<i>107</i>

DANH MỤC TỪ VIẾT TẮT

STT	Từ viết tắt	Nguyên nghĩa
1	GSMI	Global Standards Mapping Initiative
2	ING	International Netherlands Group
3	SDX	SIX Digital Exchange
4	ZKP	Zero-knowledge proof
5	DLT	Distributed ledger technology

DANH MỤC HÌNH ẢNH VÀ BẢNG

Hình 4.1: Hình ảnh minh họa về cấu trúc của bitcoin	54
Hình 4.2: Cấu trúc bitcoin.....	56
Hình 4.3: Số lượng giao dịch mỗi tháng, theo the logarithmic scale	58
Hình 4.4: Mô hình minh họa blockchain	60
Hình 4.5: Relay attack	63
Bảng 1.1: Ví dụ về ERC Token6	
Bảng 1.2: So sánh định nghĩa "blockchain"	9
Bảng 1.3: Chồng chéo về tiêu chuẩn blockchain.....	13
Bảng 1.4: Khoảng trống trong tiêu chuẩn blockchain	14
Bảng 1.5: Các câu hỏi mẫu được trả lời theo tiêu chuẩn.....	16
Bảng 1.6: Những nỗ lực thiết lập tiêu chuẩn lớn - các tổ chức chính thức	22
Bảng 1.7: Những nỗ lực thiết lập tiêu chuẩn chính - các nhóm ngành.....	25
Bảng 4.1: Dung lượng các phần trong khối.....	53
Bảng 4.2: Dung lượng các phần trong tiêu đề khối	54

TÓM TẮT NỘI DUNG ĐỀ TÀI

Trong đề tài nghiên cứu này, nhóm em chia thành 4 phần như sau:

1. Tổng quan về các vấn đề liên quan tiêu chuẩn Blockchain với Tiêu chuẩn WEFF_GSMI_Technical_Standard_2020

Tiêu chuẩn WEFF_GSMI_Technical_Standard_2020 là một tài liệu quan trọng trong lĩnh vực ứng dụng Blockchain. Tiêu chuẩn này tập trung vào việc xác định các yêu cầu kỹ thuật cơ bản cần thiết cho các ứng dụng Blockchain. Nó cũng đưa ra các hướng dẫn về các tiêu chí đánh giá hiệu suất và tính bảo mật của các ứng dụng Blockchain.

Việc sử dụng tiêu chuẩn này sẽ giúp đảm bảo tính đồng nhất và hiệu quả của các ứng dụng của công ty và tổ chức. Đặc biệt, với những công ty hoạt động trong lĩnh vực tài chính, bảo mật và độ tin cậy là hai yếu tố quan trọng nhất. Tiêu chuẩn WEFF_GSMI_Technical_Standard_2020 cung cấp các hướng dẫn và quy trình kiểm tra để giúp các công ty đảm bảo tính bảo mật và độ tin cậy của ứng dụng Blockchain.

Ngoài ra, tiêu chuẩn này còn bao gồm các định nghĩa và giải thích cho các thuật ngữ cơ bản liên quan đến Blockchain. Điều này giúp cho các nhà phát triển và chuyên gia trong lĩnh vực này hiểu rõ hơn về các khái niệm và thuật ngữ quan trọng liên quan đến Blockchain.

Tóm lại, tiêu chuẩn WEFF_GSMI_Technical_Standard_2020 là một tài liệu quan trọng giúp đảm bảo tính đồng nhất, hiệu quả, bảo mật và độ tin cậy của các ứng dụng Blockchain. Việc sử dụng tiêu chuẩn này sẽ giúp cho các công ty và tổ chức triển khai các ứng dụng Blockchain một cách chuyên nghiệp và hiệu quả hơn.

2. Tiêu chuẩn blockchain ISO/TC 307: là một trong những tiêu chuẩn quan trọng nhất trong lĩnh vực ứng dụng Blockchain hiện nay. Tiêu chuẩn này xác định các yêu cầu kỹ thuật cơ bản cần thiết cho các ứng dụng Blockchain và đưa ra các hướng dẫn về các tiêu chí đánh giá hiệu suất và tính bảo mật của các ứng dụng Blockchain.

Việc sử dụng tiêu chuẩn ISO/TC 307 sẽ giúp đảm bảo tính đồng nhất và hiệu quả của các ứng dụng Blockchain. Đặc biệt, với những công ty hoạt động trong lĩnh vực tài chính, bảo mật và độ tin cậy là hai yếu tố quan trọng nhất. Tiêu chuẩn này cung cấp các hướng dẫn và quy trình kiểm tra để giúp các công ty đảm bảo tính bảo mật và độ tin cậy của ứng dụng Blockchain.

3. Tiêu chuẩn blockchain DIN_SPEC 3104: là một tài liệu quan trọng trong lĩnh vực ứng dụng Blockchain. Tiêu chuẩn này tập trung vào việc xác định các yêu cầu kỹ thuật và quy trình kiểm tra cần thiết cho các ứng dụng Blockchain. Nó cũng cung cấp các hướng dẫn về các tiêu chí đánh giá hiệu suất và tính bảo mật của các ứng dụng Blockchain.

Việc sử dụng tiêu chuẩn này sẽ giúp đảm bảo tính đồng nhất và hiệu quả của các ứng dụng của công ty và tổ chức. Đặc biệt, với các công ty hoạt động trong lĩnh vực tài chính, bảo mật và độ tin cậy là hai yếu tố quan trọng nhất. Tiêu chuẩn DIN_SPEC 3104 cung cấp các hướng dẫn và quy trình kiểm tra để giúp các công ty đảm bảo tính bảo mật và độ tin cậy của ứng dụng Blockchain.

Ngoài ra, tiêu chuẩn này còn bao gồm các định nghĩa và giải thích cho các thuật ngữ cơ bản liên quan đến Blockchain. Điều này giúp cho các nhà phát triển và chuyên gia trong lĩnh vực này hiểu rõ hơn về các khái niệm và thuật ngữ quan trọng liên quan đến Blockchain.

Tiêu chuẩn blockchain DIN_SPEC 3104 là một tài liệu quan trọng giúp đảm bảo tính đồng nhất, hiệu quả, bảo mật và độ tin cậy của các ứng dụng Blockchain. Việc sử dụng tiêu chuẩn này sẽ giúp cho các công ty và tổ chức triển khai các ứng dụng Blockchain một cách chuyên nghiệp và hiệu quả hơn.

4. Đưa ra một số đánh giá và đề xuất những tiêu chuẩn, tiêu chí cốt lõi mà một ứng dụng Blockchain trong thực tế cần tuân thủ. Trong đó bao gồm phần đánh giá về Bitcoin và Khuyến nghị của Hội đồng OECD về Blockchain và Công nghệ Sổ cái phân tán hướng dẫn về việc sử dụng và quản lý công nghệ Blockchain và DLT. Nó khuyến khích sự hiểu biết, tạo môi trường hỗ trợ, và quan trọng nhất là đảm bảo an toàn và bảo vệ quyền lợi của người dùng.

LỜI NÓI ĐẦU

Trong thời đại của sự kết nối kỹ thuật số và sự phát triển nhanh chóng của công nghệ Blockchain, việc đảm bảo các tiêu chuẩn và quy chuẩn hợp lý là một yếu tố cực kỳ quan trọng đối với việc triển khai ứng dụng Blockchain hiệu quả. Với tính chất phân tán và đáng tin cậy của Blockchain, việc có các tiêu chuẩn chung sẽ giúp tăng tính tương thích, khả năng tương tác và sự tin cậy của các hệ thống Blockchain khác nhau. Điều này cũng giúp xây dựng lòng tin và khuyến khích sự chấp nhận và sử dụng công nghệ này trên quy mô rộng hơn.

Bài báo cáo này tập trung vào nghiên cứu về một số tiêu chuẩn trong triển khai ứng dụng Blockchain và nhằm đưa ra một số đánh giá và đề xuất về các tiêu chuẩn và tiêu chí cốt lõi mà một ứng dụng Blockchain trong thực tế cần tuân thủ. Việc xác định và tuân thủ các tiêu chuẩn này là cực kỳ quan trọng để đảm bảo tính tin cậy, bảo mật và hiệu quả của ứng dụng Blockchain trong môi trường thực tế.

Chúng em sẽ bắt đầu bằng một tổng quan về các vấn đề liên quan đến tiêu chuẩn Blockchain, bao gồm sự giải thích về Tiêu chuẩn WEFF_GSMI_Technical_Standard 2020, Tiêu chuẩn blockchain ISO/TC 307 và Tiêu chuẩn blockchain DIN_SPEC 3104. Mỗi tiêu chuẩn này có những ưu điểm và tầm quan trọng riêng, và chúng em sẽ phân tích chúng để hiểu rõ hơn về phạm vi và ứng dụng của từng tiêu chuẩn trong việc triển khai ứng dụng Blockchain.

Tiếp theo, chúng em sẽ đi sâu vào việc đánh giá và đề xuất những tiêu chuẩn và tiêu chí cốt lõi mà một ứng dụng Blockchain trong thực tế cần tuân thủ. Trên cơ sở nghiên cứu và phân tích chi tiết, chúng em sẽ xem xét các yếu tố quan trọng như bảo mật, khả năng mở rộng, tính tương thích và khả năng tương tác với các hệ thống khác. Những đề xuất này sẽ hướng đến việc xác định các tiêu chuẩn cần thiết để đảm bảo tính tin cậy và hiệu quả của ứng dụng Blockchain trong môi trường thực tế.

Việc tuân thủ các tiêu chuẩn và tiêu chí cốt lõi không chỉ đảm bảo tính bảo mật và sự tin cậy của ứng dụng Blockchain, mà còn tạo ra sự tương thích và tương tác tốt hơn giữa các hệ thống và ứng dụng khác nhau. Điều này tạo điều kiện thuận lợi cho việc phát triển và triển khai các ứng dụng Blockchain trong các lĩnh vực như tài chính, chuỗi cung ứng, y tế và quản trị.

Bằng việc đưa ra các đánh giá và đề xuất này, chúng em hi vọng rằng bài báo cáo sẽ đóng góp vào việc thúc đẩy sự phát triển bền vững của công nghệ Blockchain và đảm bảo sự hợp tác và tương thích giữa các ứng dụng Blockchain khác nhau. Chúng em cũng hy vọng rằng nội dung của báo cáo sẽ mang lại giá trị và cung cấp sự hiểu biết sâu hơn về việc triển khai ứng dụng Blockchain trong thực tế.

Xin chân thành cảm ơn sự quan tâm, đồng hành và giúp đỡ của thầy Trương Phi Hồ đối với bài báo cáo này. Chúng em hy vọng rằng nó sẽ mang lại cái nhìn rõ ràng và hữu ích về vai trò và ứng dụng của tiêu chuẩn trong việc phát triển và triển khai các ứng dụng Blockchain.

Nhóm báo cáo

Chương 1. Tổng quan các vấn đề liên quan đến các tiêu chuẩn kỹ thuật Blockchain

Khi công nghệ blockchain tiếp tục phát triển, các yêu cầu về sự minh bạch xung quanh các mô hình kỹ thuật, quy định và quản trị ngày càng lớn hơn. Các quyết định về các yếu tố nền tảng này sẽ định hình quỹ đạo phát triển và tiềm năng của công nghệ blockchain.

Tuy nhiên, có rất ít công việc để lập danh mục và đánh giá nền tảng hiện tại mà hệ sinh thái có thể xây dựng trên đó, mặc dù hoạt động gia tăng trong các lĩnh vực liên quan. Khi các bên tham gia trên toàn thế giới xây dựng các giải pháp sáng tạo để giải quyết những thách thức khó khăn nhất của xã hội, cần có một cơ sở để tạo điều kiện cho sự đổi mới có tác động và có trách nhiệm.

Lập danh mục trạng thái của hàng chục tổ chức và hiệp hội thiết lập tiêu chuẩn cộng với các quy định trên 129 quốc gia, Sáng kiến thiết lập bản đồ tiêu chuẩn toàn cầu (GSMI) thể hiện nỗ lực chưa từng có để lập bản đồ và phân tích bối cảnh hiện tại. Nó được chia thành hai thành phần riêng biệt:

1. Tiêu chuẩn kỹ thuật
2. Pháp luật và hướng dẫn được ban hành bởi các cơ quan có chủ quyền và quốc tế cũng như các thông lệ và tiêu chuẩn tốt nhất của cơ quan ngành (bao gồm tổng quan về các nhóm và hiệp hội ngành).

Công việc này là nỗ lực chung giữa Diễn đàn Kinh tế Thế giới và Hội đồng Kinh doanh Blockchain Toàn cầu, với sự đóng góp đáng kể từ MIT Media Lab, ING, Accenture, SDX và Viện Milken. Nỗ lực liên tổ chức này là một sự hợp tác toàn cầu thực sự, cũng như sự liên kết của các sáng kiến khác nhau trước đây. Điều này được hy vọng sẽ đóng vai trò là một mô hình cho những nỗ lực tương tự trên toàn hệ sinh thái trong tương lai.

1.1 Phân tích ban đầu

1.1.1 Giới thiệu

Trong vài năm qua, blockchain đã trải qua những giai đoạn thối phòng và hoài nghi đáng kể. Ngoài ra, một vài trường hợp sử dụng và ứng dụng đầy hứa hẹn đã xuất hiện và hệ sinh thái đang tiến lên phía trước với việc thiết kế và xây dựng theo quy mô.

Tuy nhiên, vẫn còn một số câu hỏi quan trọng đối với sự thành công - hay thất bại - của blockchain. Như được liệt kê ở nơi khác, sự rõ ràng về quy định vẫn là một trở ngại đáng kể đối với nhiều tổ chức. Ngoài ra, các khía cạnh kỹ thuật và quản trị như khả năng tương tác, bảo mật và các mô hình cộng tác hệ sinh thái sẽ có tác động đáng kể đến công nghệ.

Với việc khám phá các ứng dụng như tiền tệ kỹ thuật số và quản lý chuỗi cung ứng - về cơ bản sẽ thay đổi cách thức tương tác và kinh doanh của chúng ta - nhu cầu về nền tảng chung ngày càng tăng. Chúng ta đang chứng kiến sự xuất hiện của các sáng kiến nhằm mang lại định nghĩa rõ ràng hơn cho các mô hình kinh doanh, nền tảng và cơ sở hạ tầng mới mà blockchain yêu cầu và cho phép.

Chắc chắn có những nơi cần tiêu chuẩn hóa ngay bây giờ - và những nơi khác thì quá sớm. Các cuộc tranh luận triết học về công nghệ vẫn còn. Và điều quan trọng là các phong trào hướng tới tiêu chuẩn hóa không đem lại kết quả là việc đánh giá cẩn thận các đánh đổi liên quan đến kiến trúc kỹ thuật và quản trị.

Các công nghệ phi tập trung cũng giới thiệu những khả năng mới cho việc thiết lập tiêu chuẩn trên toàn hệ sinh thái. Những cách làm việc mới đang thách thức các mô hình hiện có để có thể cung cấp các tính năng hoặc tính linh hoạt độc đáo. Vẫn còn phải xem xét toàn bộ phạm vi ưu và nhược điểm, vì vậy điều quan trọng là phải tiếp tục theo dõi các lĩnh vực mà hiệu quả và rủi ro mới có thể phát huy tác dụng.

Cuối cùng, các tiêu chuẩn có khả năng giúp tạo sân chơi bình đẳng trong quá trình phát triển blockchain - nhưng chỉ khi chúng được thiết kế và triển khai một cách chu đáo. Nếu không chủ động quan tâm đến cách thức tạo ra các tiêu chuẩn và ai tạo ra chúng, có thể chúng sẽ được định hình theo các lợi ích và định hướng cụ thể – và có khả năng là theo hình ảnh của các cường quốc bá quyền hoặc các hệ thống kế thừa.

1.1.2 Động lực và phạm vi

Đã có sự gia tăng hoạt động xung quanh tiêu chuẩn hóa kỹ thuật. Trong phần này sẽ cung cấp một cái nhìn tổng quan về cảnh quan để:

- 1) Lập bản đồ các nỗ lực tiêu chuẩn hóa kỹ thuật đang được tiến hành;
- 2) Xác định các khoảng trống và các khu vực chồng chéo;
- 3) Xác định các bước quan trọng tiếp theo cho hệ sinh thái.

Như chúng ta đã thấy trong quá khứ, việc áp dụng các tiêu chuẩn cuối cùng được quyết định bởi nhiều yếu tố. Bản đồ này được hy vọng sẽ được sử dụng bởi các nhà cung cấp dịch vụ blockchain, các nhà hoạch định chính sách và các tổ chức thiết lập tiêu chuẩn để thông báo cách tiếp cận của họ đối với các hoạt động thiết lập tiêu chuẩn và thực hiện các tiêu chuẩn kỹ thuật.

Bài báo cáo lập bản đồ các tiêu chuẩn tập trung rộng rãi vào công nghệ sổ cái phân tán (DLT) để có cái nhìn toàn diện về sự phát triển của các tiêu chuẩn. Các thuật ngữ “blockchain” và “công nghệ sổ cái phân tán” được sử dụng thay thế cho nhau trong suốt báo cáo để đơn giản và ngắn gọn, mặc dù chúng sự khác biệt thực tế - đặc biệt khi chúng liên quan đến các tiêu chuẩn kỹ thuật.

Đối với mục đích của phần này, “các tiêu chuẩn” được định nghĩa là *các quy ước hướng dẫn việc phát triển và sử dụng DLT*. Chúng được thiết lập bởi các cơ quan tiêu chuẩn hóa công nghiệp và truyền thống.. Bài báo có một cái nhìn bao quát về “các cơ quan thiết lập tiêu chuẩn” hoặc “các thực thể thiết lập tiêu chuẩn” để lập bản đồ hệ sinh thái rộng lớn đóng góp cho các tiêu chuẩn kỹ thuật. Điều này có thể bao gồm các tổ chức phát triển tiêu chuẩn truyền thống (SDO) cũng như các nhóm ngành và cộng đồng nhà phát triển.

1.1.3 Phương pháp luận

1. Một đánh giá tài liệu chuyên sâu khám phá những nỗ lực hiện có đang được thực hiện theo hướng tiêu chuẩn hóa DLT.

2. Các cuộc phỏng vấn kỹ thuật để xác thực các quan sát từ nghiên cứu và hiểu rõ hơn về ý nghĩa của việc phát triển các tiêu chuẩn DLT.

1.2 Tổng quan

1.2.1 Vai trò phát triển của các tiêu chuẩn

Vai trò của tiêu chuẩn hóa trong các cuộc Cách mạng Công nghiệp lần thứ nhất, thứ hai và thứ ba đã được ghi chép rõ ràng – đặc biệt là vai trò của chúng trong việc thiết lập “cơ sở hạ tầng thông tin” để có thể xây dựng các sản phẩm và thị trường mới. Trong khi các tiêu chuẩn sẽ đóng một vai trò trong cuộc Cách mạng Công nghiệp lần thứ tư – trong đó các công nghệ mới nổi đang nhanh chóng thay đổi cuộc sống và chuyển đổi doanh nghiệp và xã hội – các cơ quan thiết lập tiêu chuẩn có những thách thức mới phía trước. Có những cân nhắc độc đáo được đưa ra bởi các lĩnh vực hội tụ công nghệ, đặc biệt khi chúng liên quan đến các ngành dọc được tiêu

chuẩn hóa cao như chăm sóc sức khỏe. Hơn nữa, các công nghệ của Cuộc cách mạng công nghiệp lần thứ tư tạo ra các mô hình hoạt động và thực tế mới. Chẳng hạn, các tiêu chuẩn liên quan đến Blockchain phải vật lộn với quản trị phi tập trung.

Box 1: Tiêu chuẩn hành động: email

Ngày nay, chúng ta có thể gửi email cho bất kỳ ai có địa chỉ hợp lệ – bất kể họ có sử dụng cùng ứng dụng email, tên miền hoặc loại máy tính hay không. Người dùng không chuyên chấp nhận tính nhất quán trong các trải nghiệm gửi và nhận email của chúng ta: các trường *To* và *From*, gửi đến một địa chỉ có ký hiệu “@” và sự khác biệt giữa email đã đọc và chưa đọc.

Trải nghiệm thống nhất này là kết quả của một bộ tiêu chuẩn mạnh mẽ xác định cách xử lý, truyền, truy xuất email, v.v.

Chẳng hạn, có thể gửi email từ tài khoản Outlook đến tài khoản Gmail với các tên miền khác nhau mà không cần thực hiện thêm bất kỳ thao tác hoặc bước nào. Người dùng có thể nhận ra các từ viết tắt như “SMTP”, “DNS”, “POP” và “IMAP”.

Mặc dù đây là một ví dụ quá đơn giản, nhưng nó minh họa cách các tiêu chuẩn kỹ thuật và giao thức tạo điều kiện thuận lợi cho việc liên lạc liền mạch và tạo ra thị trường dịch vụ kỹ thuật.

Có thể hữu ích khi nghĩ về các loại tiêu chuẩn theo chức năng dự định của chúng. *Sơ sánh kiến trúc tham khảo: chức năng của các tiêu chuẩn trong các ngành thâm dụng tri thức* phác thảo cách các tiêu chuẩn có thể đóng góp đến các mục tiêu giảm đa dạng, đặc điểm kỹ thuật về chất lượng và độ tin cậy, cung cấp thông tin liên quan đến hiệu suất và đảm bảo khả năng tương tác.

1.2.2 Sự phát triển không ngừng của các tiêu chuẩn

Các tiêu chuẩn thường được tạo ra và áp dụng theo một trong ba cách (được điều chỉnh từ Sổ tay Đổi mới và Tiêu chuẩn):

Các tiêu chuẩn thường được tạo ra và áp dụng theo một trong ba cách (được điều chỉnh từ Sổ tay Đổi mới và Tiêu chuẩn):

- Theo quy ước (*tiêu chuẩn thực tế*) - một thực tiễn, hành vi hoặc cấu hình được chấp nhận rộng rãi thông qua sự lặp lại và sử dụng, ví dụ, chỉ định phải và trái

- Bồi fiat (*tiêu chuẩn de jure*) - được áp đặt bởi một sắc lệnh hoặc quy định của chính phủ hoặc tổ chức khác. Ví dụ bao gồm các hoạt động của Tiêu chuẩn Úc và các tiêu chuẩn de jure của Ủy ban Chứng khoán và Giao dịch Hoa Kỳ về quản lý mã thông báo.
- Bảng đàm phán - như được thỏa thuận chính thức giữa các bên liên quan trong một hoạt động hoặc doanh nghiệp, chẳng hạn như những người được tạo ra bởi tổ chức phát triển tiêu chuẩn chính thức (SDO) như được thảo luận sau trong bài báo.

1.2.3 Xem xét kỹ hơn: các tiêu chuẩn blockchain

Theo một số cách, blockchain đảo lộn các mô hình thiết lập tiêu chuẩn truyền thống, do quản trị phi tập trung và khả năng nhúng các tiêu chuẩn trong việc xây dựng giao thức. Các khu vực khác đã bắt chước các cấu trúc được sử dụng để tạo ra sự gắn kết trong các hệ thống phân tán như internet.

1.2.3.1 Cài đặt tiêu chuẩn

Các thực thể thiết lập tiêu chuẩn quen thuộc, chẳng hạn như Lực lượng đặc nhiệm kỹ thuật Internet (IETF), Viện Kỹ sư Điện và Điện tử (IEEE) và Tổ chức Tiêu chuẩn hóa Quốc tế (ISO), tiếp tục phát triển các tiêu chuẩn công nghệ thông tin tự nguyện. Một số, chẳng hạn như ISO và IEEE, trong số những người khác, đã thành lập các nhóm làm việc chuyên dụng về blockchain và công nghệ sổ cái phân tán, nhưng các lĩnh vực trọng tâm và đầu ra của họ là giai đoạn đầu.

Áp dụng một mô hình tương tự, một số cơ quan tiêu chuẩn dành riêng cho ngành, chẳng hạn như GS1 (nhóm quản lý không gian tên mã vạch và các tiêu chuẩn chuỗi cung ứng khác) hoặc Hiệp hội Hệ thống Quản lý và Thông tin Chăm sóc Sức khỏe (HIMSS), cũng có các nhóm làm việc blockchain. Trong lĩnh vực blockchain và các ứng dụng liên quan, một vài nhóm ngành, chẳng hạn như Ethereum Enterprise Alliance (EEA), Interwork Alliance (IWA) và Distributed Identity Foundation (DIF), tập trung vào các tiêu chuẩn blockchain.

Các quy trình tiêu chuẩn dành riêng cho giao thức cũng đã được thực hiện theo cách phi tập trung thông qua "các đề xuất cải tiến". Chúng được quản lý bởi cộng đồng nhà phát triển và thường được tạo điều kiện thông qua nền tảng mã nguồn mở GitHub. Một số ví dụ bao gồm Đề xuất cải tiến Bitcoin (BIP), Đề xuất cải tiến Ethereum (EIP) và Đề xuất cải tiến zCash (ZIP).

Box 2: Nghiên cứu điển hình: ICO, CryptoKitties và hơn thế nữa – Tiêu chuẩn mã thông báo ERC

Nhiều ứng dụng được công nhận rộng rãi của Blockchain được kích hoạt theo tiêu chuẩn mã thông báo ERC, xác định động lực, đặc điểm kỹ thuật và triển khai cho mã thông báo dựa trên Ethereum.

Ví dụ về ERC Tokens

Được đặt tên theo mã định danh Ethereum Request for Comment (ERC), các ví dụ đáng chú ý bao gồm (lấy từ tiêu chuẩn token):

Tiêu chuẩn	Tóm tắt	Được biết đến
ERC-20	Tiêu chuẩn cho phép triển khai API tiêu chuẩn cho token trong hợp đồng thông minh. Tiêu chuẩn này cung cấp chức năng cơ bản để chuyển token, cũng như cho phép token được phê duyệt để bên thứ ba khác trên chuỗi có thể sử dụng chúng.	<i>Kích hoạt hợp đồng thông minh và tài chính phi tập trung (DeFi).</i> Ví dụ: Chainlink, Maker, Augur <i>Initial Coin Offerings (ICO)</i> Ví dụ: EOS, Telegram, Tezos <i>Stablecoin</i> Ví dụ: Tether, USDC, Paxos
ERC-721	Tiêu chuẩn sau đây cho phép triển khai giao diện lập trình ứng dụng (API) tiêu chuẩn cho các mã thông báo không thể thay thế (NFT) trong các hợp đồng thông minh. Tiêu chuẩn này cung cấp chức năng cơ bản để theo dõi và chuyển NFT.	<i>Bộ sưu tập và trò chơi Blockchain</i> Ví dụ: CryptoKitties, Gods Unchained

Bảng 1.1: Ví dụ về ERC Token

Các tiêu chuẩn mã thông báo được quản lý thông qua quy trình Đề xuất cải tiến Ethereum (EIP), được chạy trên GitHub.

1.2.3.2 Phát triển phần mềm

Các tập đoàn phát triển phần mềm tập hợp nhiều bên liên quan để chia sẻ và cùng phát triển phần mềm cơ bản cho các mạng này: hãy nghĩ đến Tổ chức Phần mềm Tự do, Quỹ Phần mềm Apache và thậm chí cả Linux Foundation. Thông thường các tập đoàn này không tài trợ cho công việc phát triển hoặc viết mã phần mềm trực tiếp. Thay vào đó, chúng phục vụ chức năng "kiểm soát không lưu" trong việc quản lý các quy trình phát triển phần mềm.

Phần mềm thường là chất kết dính giữa nhiều tiêu chuẩn và người dùng cuối. Tùy thuộc vào cấu trúc của quy trình, phát triển phần mềm có thể không cần định hướng đồng thuận giống như các sáng kiến thiết lập tiêu chuẩn. Ngoài ra, phần mềm được cập nhật liên tục - ví dụ, để thêm các tính năng mới và sửa lỗi - trong khi các tiêu chuẩn có nhiều ràng buộc hơn trong việc phát hành các bản cập nhật.

Cuối cùng, cách tiếp cận quản lý sở hữu trí tuệ (IP) khác nhau. Với phần mềm, IP được đính kèm với các đóng góp kỹ thuật (ví dụ: yêu cầu kéo GitHub), không phải từng thành phần riêng lẻ của một cuộc thảo luận rộng hơn (ví dụ: bình luận trên Slack). Do đó, các mô hình quản trị và hoạt động có thể rất khác nhau giữa các tổ chức này và các cơ quan tiêu chuẩn.

1.2.3.3 Quản trị mạng

Các tiêu chuẩn là tùy chọn theo bản chất - chúng được sử dụng hoặc không. Trong lịch sử, cần có các cơ quan để phân xử các tranh chấp trên một mạng lưới sống, thờ bao gồm nhiều người tham gia và chương trình nghị sự khác nhau.

Các tổ chức như Tập đoàn Internet về Tên và Số được gán (ICANN), hoặc thậm chí các nhóm không chính thức như Nhóm các nhà khai thác mạng Bắc Mỹ (NANOG) đã đẩy mạnh để đáp ứng nhu cầu này. Tham gia nhiều hơn vào chính sách chính thức, các tổ chức này cần cân bằng thời gian hoạt động và khả năng sử dụng với tính toàn diện và giá trị.

Đồng thời, quản trị mạng blockchain giới thiệu một loạt các nhu cầu và khả năng mới. Ở cấp độ giao thức, phần lớn việc xét xử xảy ra trực tiếp trong cộng đồng nhà phát triển. Tuy nhiên, điều này không phải lúc nào cũng mang lại sự đa dạng của những người tham gia và chương trình nghị sự. Hơn nữa, hiện tại không có cấu trúc quản trị liên giao thức nào tạo điều kiện cho sự phối hợp có thể cần thiết cho khả năng tương tác và khả năng mở rộng.

1.2.4 Ngoài tiêu chuẩn: định mức ngành

Như với sự phát triển của bất kỳ công nghệ nào, có một vai trò cho cả các tiêu chuẩn chính thức và các tiêu chuẩn công nghiệp được thiết lập không chính thức hơn. Ví dụ, Quy tắc Ứng xử của Tài chính Kỹ thuật số Toàn cầu, Cơ quan Đăng ký Tiết lộ của Messari và Nguyên tắc Presidio của Diễn đàn Kinh tế Thế giới đều đại diện cho những nỗ lực cấp cơ sở để xác định kỳ vọng và giá trị. Mặc dù các sáng kiến này không được liệt kê các tiêu chuẩn kỹ thuật, nhưng chúng nhằm mục đích ảnh hưởng đến các quyết định quan trọng liên quan đến công nghệ và quản trị.

1.3 Những phát hiện chính

Rõ ràng, có một số cách tiếp cận để tạo ra các tiêu chuẩn cho công nghệ blockchain. Bài viết này thể hiện nỗ lực lập bản đồ hoạt động hiện tại (tính đến tháng 8 năm 2020) và xác định các xu hướng trong hệ sinh thái. Phần này tổng hợp những hiểu biết chính từ việc lập bản đồ hàng chục sáng kiến thiết lập tiêu chuẩn và các hoạt động của chúng bằng cách xác định các thách thức, chồng chéo và khoảng trống trong bối cảnh.

- Sự rõ ràng vẫn là một thách thức vì thuật ngữ vẫn không nhất quán, trong khi phạm vi của các tiêu chuẩn blockchain vẫn chưa rõ ràng.
- Có cả khoảng trống và chồng chéo trong bối cảnh thiết lập tiêu chuẩn.
- Tính đại diện không nhất quán giữa các thuộc tính như địa lý, chuyên môn và vai trò. Thêm vào đó, quyền sở hữu trí tuệ có thể ảnh hưởng đến mức độ cởi mở trong quá trình sáng tạo.

1.3.1 Thuật ngữ vẫn không nhất quán

Các định nghĩa rõ ràng và nhất quán cho các khía cạnh chính của blockchain vẫn là một thách thức (đáng chú ý, đây là một thách thức được xác định trong các tài liệu liên quan đến tiêu chuẩn có từ năm 2017). Giữa và đôi khi trong các cơ quan thiết lập tiêu chuẩn, các định nghĩa cốt lõi có thể khác nhau. Lấy hai ví dụ về thuật ngữ "blockchain":

Định nghĩa	Sổ cái phân tán với các khối được xác nhận được tổ chức trong một chuỗi tuần tự, chỉ nối thêm bằng cách sử dụng các liên kết mật mã. CHÚ THÍCH 1: Blockchain được thiết kế để chống giả mạo và tạo ra các bản ghi sổ cái cuối cùng, dứt khoát và bất biến.	Một loại sổ cái phân tán bao gồm dữ liệu được ghi lại kỹ thuật số được sắp xếp như một chuỗi các khối phát triển liên tiếp với mỗi khối được liên kết mật mã và được củng cố chống giả mạo và sửa đổi
-------------------	---	---

Bảng 1.2: So sánh định nghĩa "blockchain"

Mặc dù các định nghĩa tương tự nhau – nhấn mạnh rằng blockchain là một loại sổ cái phân tán với các khối được liên kết bằng mật mã – các nhà quan sát sắc sảo sẽ lưu ý một số khác biệt. Ví dụ, định nghĩa ISO lưu ý "các blockchain được thiết kế để chống giả mạo và tạo ra các bản ghi sổ cái cuối cùng, dứt khoát và bất biến" thay cho "cứng rắn chống giả mạo và sửa đổi" của ITU-T. Định nghĩa ITU-T mô tả chuỗi là "phát triển liên tiếp", trong khi định nghĩa ISO chọn "chuỗi tuần tự, chỉ nối thêm".

Những phân kỳ này cũng được phản ánh trong kiến trúc tham chiếu. Ví dụ, IEEE tổ chức dự thảo kiến trúc tham chiếu của mình thành năm "miền kiến trúc DLT" (hoặc quan điểm):

- 1) nền tảng;
- 2) dữ liệu;
- 3) quá trình;
- 4) dịch vụ; và
- 5) các ứng dụng.

Trong khi đó, ITU-T đã xác định năm "thành phần chức năng":

- 1) lớp lõi;
- 2) lớp dịch vụ;
- 3) nền tảng dịch vụ ứng dụng;
- 4) Ứng dụng DLT;
- 5) dịch vụ bên ngoài.

Mặc dù những khác biệt này có vẻ tinh tế, nhưng chúng có thể có tác động gọn sóng trong suốt quá trình phát triển và thực hiện các tiêu chuẩn. Mỗi thực thể thiết lập tiêu chuẩn nhất thiết

phải xây dựng dựa trên công việc trong quá khứ, để lại chỗ cho việc giải thích từ những người dùng phân loại tiếp theo, kết hợp những khác biệt này.

1.3.2 Khối lượng hoạt động đã phản ánh sự cường điệu xung quanh công nghệ

Số lượng các nỗ lực thiết lập tiêu chuẩn đã tương ứng với sự cường điệu xung quanh công nghệ. Một số nỗ lực được bắt đầu ở đỉnh cao của tiếng vang xung quanh blockchain đã giảm xuống hoặc vẫn chưa công bố bất kỳ đầu ra đáng kể nào.

1.3.3 Phạm vi của các tiêu chuẩn blockchain vẫn chưa rõ ràng

Cách tiếp cận để phân chia các lớp của ngăn xếp kỹ thuật (ví dụ: các tiêu chuẩn hướng tới mạng so với lớp ứng dụng) khác nhau giữa các tổ chức. Như vậy, các sắc thái và sự phụ thuộc vào các tiêu chuẩn khác có thể bị mất trong hỗn hợp. Hãy xem xét ví dụ về quản lý danh tính kỹ thuật số. Bởi vì nhận dạng kỹ thuật số là nền tảng, nó chắc chắn sẽ chạm vào mọi lớp của ngăn xếp công nghệ. Các câu hỏi có thể bao gồm: *Danh tính được xác minh như thế nào? Mức độ riêng tư nào cần được đảm bảo? Những định dạng dữ liệu nào là cần thiết để đảm bảo khả năng tương tác và tính di động của dữ liệu?* Tiêu chuẩn hóa hiệu quả trong không gian này sẽ yêu cầu sự liên kết trong toàn bộ ngăn xếp và khớp nối rõ ràng các lớp mà các tiêu chuẩn cụ thể sẽ áp dụng.

Một câu hỏi liên quan là làm thế nào các tiêu chuẩn blockchain tương tác với ngành dọc. Ví dụ, các tiêu chuẩn tiền tệ kỹ thuật số phải xem xét các khoản thanh toán và tiêu chuẩn hệ thống tài chính liên quan đến tuân thủ, nhận dạng cá nhân, đại diện dữ liệu và giao tiếp, v.v., ngoài các tiêu chuẩn về lớp kỹ thuật. Trong khi một số cơ quan thiết lập tiêu chuẩn có kết nối chính thức với các luồng công việc liên quan, những cơ quan khác có thể hoạt động độc lập. Điều này cũng thú vị khi xem xét sự hội tụ với các công nghệ Cách mạng công nghiệp lần thứ tư khác như internet vạn vật (IoT), nơi hoạt động thiết lập tiêu chuẩn cũng còn non trẻ.

Cuối cùng, blockchain trùng lặp với các lĩnh vực kỹ thuật và tiêu chuẩn hóa cao khác, chẳng hạn như mật mã. Mật mã bằng chứng không có kiến thức (ZKP) là một ví dụ, vì nó có quy trình tiêu chuẩn hóa tích cực dựa trên cộng đồng. Mặc dù đây không phải là "tiêu chuẩn blockchain" về mặt kỹ thuật, nhưng chúng có ý nghĩa quan trọng đối với các tiêu chuẩn blockchain và quỹ đạo của công nghệ.

1.3.4 Có sự chồng chéo trong bối cảnh thiết lập tiêu chuẩn

Bởi vì có một số cơ quan thiết lập tiêu chuẩn với công việc đang được tiến hành, có một số lĩnh vực tập trung hoạt động cao - và một số chưa được khám phá bởi các tổ chức thiết lập tiêu chuẩn.

Phân tích các tiêu chuẩn được lập bản đồ cho thấy năm lĩnh vực chồng chéo hàng đầu là:

1. **Bảo mật:** Đương nhiên, bảo mật là một lĩnh vực trọng tâm chính cho các tiêu chuẩn kỹ thuật. Do không phải tất cả các blockchain đều được tạo ra theo cùng một cách, việc hiểu cách đảm bảo tính nhất quán trong quản lý bảo mật trên các loại blockchain khác nhau là điều cần thiết để đảm bảo sử dụng bền vững nền tảng. Tuy nhiên, vẫn còn phải xem các yếu tố khác nhau như giao thức đồng thuận và cấp phép sẽ ảnh hưởng đến các tiêu chuẩn này như thế nào.
2. **Internet vạn vật (IoT):** Việc đánh giá sự hội tụ của các công nghệ mới nổi là rất quan trọng đối với tiêu chuẩn hóa tư duy tiên bộ. Các tiêu chuẩn kỹ thuật bao gồm hiểu các yêu cầu đối với các trường hợp sử dụng IoT và blockchain và phân tích các yêu cầu về khả năng tương tác giữa IoT và blockchain.
3. **Nhận dạng:** Được coi là một yếu tố cơ bản và ứng dụng của blockchain, các nguyên tắc cơ bản về nhận dạng kỹ thuật số như giao thức lưu thông, tạo và quản lý khóa và thông số kỹ thuật giao thức cho nguồn gốc nhận dạng lẫn nhau của các khóa / địa chỉ công khai được tạo giữa các mật mã khác nhau là trọng tâm cốt lõi của các cơ quan tiêu chuẩn hóa.
4. **Yêu cầu DLT:** Có công việc đang được tiến hành để xác định các yêu cầu phần mềm và phần cứng để vận hành blockchain. Tuy nhiên, phần lớn hoạt động này là giao thức cụ thể và có thể không nhất thiết trùng với các khía cạnh khác, chẳng hạn như các yêu cầu quản trị.
5. **Phân loại / thuật ngữ DLT:** Vì thuật ngữ là cơ sở cho tất cả các hoạt động thiết lập tiêu chuẩn tiếp theo, hầu hết các thực thể đã bắt đầu từ đây. Nhưng, như đã mô tả trước đó, có sự khác biệt trong định nghĩa và kiến trúc tham chiếu.

Mặc dù sự kết hợp này có thể là dấu hiệu của các lĩnh vực ưu tiên cao để tiêu chuẩn hóa, nhưng nó cũng giới thiệu khả năng chồng chéo hoặc xung đột trong việc thiết lập tiêu chuẩn trong các lĩnh vực này. Ví dụ, ISO, IEEE, ITU-T và Tiêu chuẩn Úc có hơn một chục sáng kiến liên quan đến bảo mật blockchain – bên cạnh các đề xuất cải tiến liên quan đến bảo mật ở cấp độ

giao thức. Như đã nói ở trên, phân loại và thuật ngữ đã chứng minh điều này. Vì mạng lưới giữa các sáng kiến này phần lớn là không chính thức, nên có tiềm năng cho các kết quả đầu ra không hoàn toàn phù hợp.

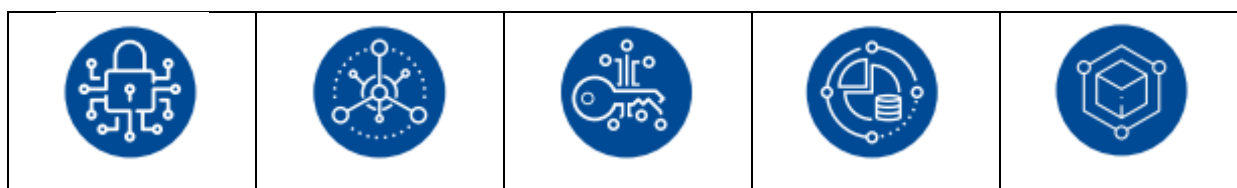
Nhiều tiêu chuẩn được đề cập trong bài viết này vẫn chưa được hoàn thiện, vì vậy rất khó để đánh giá chính xác mức độ chồng chéo trong các lĩnh vực nội dung. Tuy nhiên, các khu vực này cần được theo dõi và phối hợp cẩn thận.

1.3.5 Có những khoảng trống và sự phân kỳ trong bối cảnh thiết lập tiêu chuẩn

Tuy nhiên, vẫn có những khoảng trống trong bối cảnh hiện đang tồn tại do sự kết hợp của sự non nớt về công nghệ, sự phức tạp của chủ đề và sự khác biệt trong các triết lý cơ bản về công nghệ.





Các lỗ hổng được xác định trong thiết lập tiêu chuẩn thường rơi vào bốn loại:

- 1. Khi nào nên áp dụng DLT:** Phần lớn các nỗ lực để lập danh mục các tiêu chí để đánh giá sự phù hợp cho mục đích của blockchain là không chính thức. Các tổ chức có thể được hưởng lợi từ hướng dẫn về kỳ vọng hiệu suất và khuôn khổ để đánh giá các rủi ro chức năng.
- 2. Các yếu tố kỹ thuật cốt lõi:** Các nguyên tắc cơ bản của công nghệ blockchain, chẳng hạn như thuật toán đồng thuận và khả năng tương tác, phần lớn đã phát triển thông qua những người chơi trong ngành và phát triển kỹ thuật, thay vì thông qua chính thức hóa và tiêu chuẩn hóa.
- 3. Kiểm tra hiệu suất DLT:** Hiện tại không có tiêu chuẩn nào cho loại thử nghiệm nào có thể và nên được thực hiện trên nền tảng DLT. Các tiêu chuẩn có thể phác thảo các thông số cho các loại thử nghiệm (ví dụ: kỹ thuật, chức năng, người dùng, căng thẳng hoặc bảo mật) và các khuyến nghị về thủ tục.
- 4. Các ngành dọc liên quan:** Như đã nêu trước đây, các tổ chức thiết lập tiêu chuẩn đã bắt đầu khám phá các kết nối với ngành dọc. Tuy nhiên, một số ngành dọc vẫn là lãnh thổ chưa được khám phá.



Bảo mật	Internet vạn vật (IOT)	Định danh	Các yêu cầu DLT	Phân loại và thuật ngữ
Quản lý bảo mật cho tài sản mật mã của khách hàng trên các sàn giao dịch tiền điện tử Ưu tiên bảo vệ tài sản của khách hàng Khung bảo mật cho hệ thống quản lý truy cập và chia sẻ dữ liệu dựa trên công nghệ sổ cái phân tán	Khả năng tương tác giữa các thiết bị IoT / phần cứng và các giao thức mạng blockchain	Quản lý khóa người dùng cho công nghệ blockchain và sổ cái phân tán	Yêu cầu phần cứng Yêu cầu phần mềm Định dạng dữ liệu	Định nghĩa làm việc cho blockchain Xác định loại, chức năng, thành phần, tương tác người dùng và trường hợp sử dụng của blockchain

Bảng 1.3: Chồng chéo về tiêu chuẩn blockchain

			
Khi nào nên áp dụng DLT	Yếu tố kỹ thuật cốt lõi	Kiểm tra hiệu suất DLT	Ngành dọc liên quan
Đánh giá tính hữu ích của DLT Các loại DLT - tính năng và kỳ vọng về hiệu suất	Mạng ngoài chuỗi (ví dụ: Lightning) Thuật toán đồng thuận Cấu trúc chức năng	Kiểm tra hiệu suất phân loại (ví dụ: kiểm tra kỹ thuật, chức năng, người dùng, căng thẳng,	Giáo dục Phát triển bền vững Quản lý xây dựng Quản lý quyền Đăng ký đất đai

Rủi ro chức năng Heuristics để so sánh đa nền tảng	(ví dụ: blockchain, DAG) Khả năng tương tác DLT	bảo mật) và cách chúng có thể được thực hiện Yêu cầu kiểm tra hiệu suất	
--	--	---	--

Bảng 1.4: Khoảng trống trong tiêu chuẩn blockchain

1.3.6 Các phương pháp tốt nhất để phổ biến / thực hiện các tiêu chuẩn đang được tranh luận

Một số người cho rằng tương phi liên quan đến một số tiêu chuẩn đi ngược lại đặc tính của công nghệ blockchain. Tuy nhiên, các dự án nguồn mở phải đối mặt với những cân nhắc và ràng buộc riêng của họ. Phân cấp và tình trạng hiện tại của blockchain cũng có nghĩa là không có thực thể chuyên dụng nào chịu trách nhiệm phổ biến các tiêu chuẩn và giám sát việc thực hiện chúng, chẳng hạn như ICANN cho internet. Vì vậy, việc thực hiện các tiêu chuẩn phần lớn được để lại cho cấp độ tổ chức và hệ sinh thái. Vì nhiều người tham gia vào blockchain thông qua các tập đoàn, có thể các cấu trúc quản trị này thông báo cho chiến lược tiêu chuẩn tổ chức.

Ngoài ra, sự non trẻ của công nghệ và vô số các cơ quan quan tâm đến tiêu chuẩn có nghĩa là không rõ liệu các lực lượng thúc đẩy việc áp dụng sẽ là lực kéo thị trường, đẩy thị trường hay kết hợp cả hai. Với các tiêu chuẩn truyền thống, việc thực hiện phần lớn là tùy chọn và tùy thuộc vào quyết định của nhóm phát triển cốt lõi. Đối với các tiêu chuẩn được thực hiện thông qua các đề xuất cải tiến, có tùy chọn để phân nhánh chuỗi trong trường hợp có những bất đồng cơ bản (mặc dù quá trình phản hồi nhằm giải thích điều này một cách chủ động).

Hơn nữa, có những dự án kỹ thuật, chẳng hạn như Polkadot và Interledger, tập trung vào các giải pháp được thiết kế để tạo điều kiện cho các tương tác giữa các giao thức. Vì vậy, có thể các giải pháp kỹ thuật thay đổi vai trò của các tiêu chuẩn kỹ thuật trong việc tạo điều kiện cho khả năng tương tác.

Box 3: Nghiên cứu điển hình: Các tiêu chuẩn để tạo điều kiện thuận lợi cho việc thực hiện quy tắc du lịch của FATF

Vào tháng 6 năm 2019, Lực lượng đặc nhiệm hành động tài chính (FATF) đã cập nhật các khuyến nghị chống rửa tiền và chống khủng bố (AML / CFT) để làm rõ các yêu cầu đối với các nhà cung cấp dịch vụ tài sản ảo (VASP). Điều này bao gồm khuyến nghị "quy tắc du lịch", theo

đó các nhà cung cấp dịch vụ sẽ chịu trách nhiệm chia sẻ thông tin nhận dạng về người gửi và người nhận cho các giao dịch giữa các sàn giao dịch vượt quá 3.000 đô la giá trị.


Yêu cầu này đặt ra câu hỏi cho VASP bao gồm, nhưng không giới hạn, các tiêu chuẩn cho nhắn tin liên VASP cũng như để nhận dạng người tiêu dùng và chính VASP. Nhanh chóng nhận ra nhu cầu hợp tác, một số tác nhân trong ngành đã huy động để lấp đầy những khoảng trống này và trả lời các câu hỏi chính.



Những người chơi trong ngành nhấn mạnh tầm quan trọng của sự rõ ràng trong những vấn đề này để có thể giao tiếp hiệu quả và có ý nghĩa giữa các VASP - và tự động hóa việc trao đổi các thông điệp như vậy. Hơn nữa, các tiêu chuẩn sẽ tạo điều kiện thuận lợi cho một thị trường cho những người quan tâm đến việc sản xuất các giải pháp kỹ thuật để tạo điều kiện thuận lợi cho việc nhắn tin giữa các VASP.

Nhóm công tác chung về Tiêu chuẩn nhắn tin InterVASP (JWG-IVMS), do Phòng Thương mại Kỹ thuật số, Tài chính Kỹ thuật số Toàn cầu và Hiệp hội Trao đổi Tài sản Kỹ thuật số Quốc tế dẫn đầu, được thành lập vào tháng 12 năm 2019 và có sự tham gia của hơn 130 chuyên gia kỹ thuật để phát triển Tiêu chuẩn nhắn tin liên VASP IVMS101. Tiêu chuẩn được phát hành vào tháng 5 năm 2020, với hướng dẫn về từ vựng chung, nguyên tắc dữ liệu, kiểu dữ liệu và xác định mô hình dữ liệu, trong số các thành phần khác.

Các câu hỏi mẫu được trả lời theo tiêu chuẩn

Ví dụ về các câu hỏi được trả lời theo tiêu chuẩn có thể gây ra các biến chứng trong giao tiếp giữa các VASP:

Chủ đề	Câu hỏi mẫu	Tiêu chuẩn	Trả lời
Yêu cầu về dữ liệu 	Dữ liệu nào nên được đưa vào để xác định ai đó?	" Cấu trúc 5.2.2.1 NaturalPerson"	Tên, địa chỉ, căn cước công dân, nhận dạng người tiêu dùng, ngày và nơi sinh, quốc gia cư trú
Nhận dạng quốc gia	Hợp chủng quốc Hoa Kỳ nên được	"Giá trị được sử dụng cho quốc gia hiện trường phải có	US

	xác định là US hay USA?	trên mã ISO3166-1 alpha-2 hoặc giá trị XX”	
Thời gian 	Ngày 2020-3-5 đại diện cho ngày 5 tháng 3 hay ngày 3 tháng 5?	“Định nghĩa: Một điểm trong thời gian, được biểu diễn dưới dạng một ngày trong năm dương lịch. Tuân thủ ISO 860 ... Định dạng: YYYY-MM-DD”	5 Tháng Ba 2020

Bảng 1.5: Các câu hỏi mẫu được trả lời theo tiêu chuẩn

Đến nay, các nhà cung cấp giải pháp kỹ thuật bao gồm Sygna của CoolBitX, TRISA, Notabene và Securrency của CipherTrace đã cam kết sử dụng tiêu chuẩn IVMS101.

1.3.7 Đại diện địa lý trong các sáng kiến thiết lập tiêu chuẩn khác nhau

Phần lớn hoạt động thiết lập tiêu chuẩn ngày nay có trụ sở tại Châu Âu, Bắc Mỹ và Trung Quốc. Trong khi một số cơ quan đã cố tình đưa tiếng nói toàn cầu vào các sáng kiến của họ thông qua các nhóm địa phương hoặc đại diện khu vực, nhiều cơ quan không có nhiệm vụ rõ ràng về đại diện địa lý. Ví dụ, trong số 11 nhóm làm việc của ISO, chỉ có một nhóm (nhóm đặc biệt về hướng dẫn đánh giá DLT) có người triệu tập không đến từ Châu Âu, Bắc Mỹ hoặc Úc. Một ví dụ khác là các tác giả và nhà nghiên cứu chính của kiến trúc tham chiếu công nghệ sổ cái phân tán ITU-T đều đến từ Trung Quốc.

Nếu không có sự đại diện này - hoặc tối thiểu, một cơ hội để gửi phản hồi - có thể các tiêu chuẩn không phù hợp liên quan đến cơ sở hạ tầng, quy định và / hoặc thực tế hoạt động trong một số khu vực địa lý nhất định. Hơn nữa, các yếu tố chủ đề cốt lõi của công việc thiết lập tiêu chuẩn như quyền riêng tư chứa nhiều diễn giải và bối cảnh văn hóa.

1.3.8 Chuyên môn và đại diện người tiêu dùng khác nhau

Cho rằng blockchain chạm vào phần mềm, mật mã và kinh tế, một chuyên môn đa dạng là cần thiết trong quá trình phát triển tiêu chuẩn. Tuy nhiên, một số nỗ lực được định hướng hướng tới các ban chỉ đạo "kỹ thuật", có thể ngăn cản các cuộc trò chuyện có ý nghĩa về các ưu đãi và tác động của chúng đối với người dùng cuối.

Ngoài ra, có nhiều mức độ tham gia khác nhau giữa những người tiêu dùng công nghệ. Một số sáng kiến thiết lập tiêu chuẩn đã chính thức hóa quan hệ đối tác với các nhóm định hướng người tiêu dùng. Ví dụ: ISO hợp tác chặt chẽ với Người tiêu dùng Quốc tế.⁴⁰ Trong trường hợp các tiêu chuẩn nguồn mở, định hướng giao thức, những người đóng góp thường là người tiêu dùng sản phẩm. Tối thiểu, các quy trình tiêu chuẩn được thực hiện minh bạch và có thể truy cập thông qua GitHub. Tuy nhiên, tính minh bạch có thể không phải là trọng tâm chính trong quá trình thiết lập tiêu chuẩn, điều này có thể dẫn đến những lo ngại về bảo vệ người tiêu dùng hoặc thậm chí loại trừ và khai thác.

1.3.9 Những cân nhắc về sở hữu trí tuệ vẫn chưa rõ ràng

Một cơ quan tiêu chuẩn hoạt động tốt tạo ra một tiêu chuẩn dễ thực hiện, mà bất kỳ ai cũng có thể thực hiện; Ngoài ra, không nên có vấn đề về bằng sáng chế - hoặc, nếu có, chúng cần được chỉ định rõ ràng.

Tuy nhiên, điều quan trọng cần lưu ý là có thể có sự đánh đổi giữa tính mở và quyền sở hữu IP. Ví dụ, các quy trình mở như các quy trình được sử dụng bởi Bitcoin và Ethereum - bởi vì sự tham gia hoàn toàn công khai mà không có bất kỳ sự chuyển nhượng sở hữu trí tuệ nào - có nguy cơ tạo ra các tiêu chuẩn vi phạm bằng sáng chế thuộc sở hữu của người tham gia. Mặc dù điều này chưa phát sinh như một vấn đề thực chất, nhưng nó có thể là một rủi ro trong tương lai.

Ngược lại, các cơ quan tiêu chuẩn khác chạy các quy trình được cho là "khép kín" hơn theo nghĩa là những người tham gia vào các cuộc trò chuyện đó có thể cần phải đồng ý cấp phép cho bất kỳ IP bằng sáng chế nào mà họ nắm giữ được bảo vệ bởi các tiêu chuẩn đó. Điều này có nghĩa là những cuộc thảo luận đó không thể xảy ra trong môi trường ẩn danh.

1.4 Tổng kết

Rõ ràng, có nhiều nỗ lực đang được tiến hành, mỗi nỗ lực có một bộ yêu cầu thủ tục duy nhất và những điểm mạnh và điểm yếu liên quan.

Để cung cấp một cái nhìn tổng quan về bối cảnh hiện tại, các bảng sau đây tóm tắt một số nỗ lực thiết lập tiêu chuẩn chính đang được tiến hành giữa các tổ chức thiết lập tiêu chuẩn chính thức và các nhóm ngành và thông qua các đề xuất cải tiến.

Tiêu chuẩn	Địa điểm	Mục đích	Chủ đề
IEEE¹	Hoa Kỳ	Mục đích của Viện Kỹ sư Điện và Điện tử (IEEE) là thúc đẩy sự phát triển và ứng dụng công nghệ điện và khoa học đồng minh vì lợi ích của nhân loại, sự tiến bộ của nghề nghiệp và hạnh phúc của các thành viên	Internet vạn vật (IoT); Trao đổi và thanh toán tiền điện tử; Thẻ; Năng lượng; Tài sản kỹ thuật số
ISO²	Thụy Sĩ	Tổ chức Tiêu chuẩn hóa Quốc tế (ISO) là một tổ chức quốc tế độc lập, phi chính phủ, phát triển các tiêu chuẩn để đảm bảo chất lượng, an toàn và hiệu quả của sản phẩm, dịch vụ và hệ thống	Bảo mật; Định danh
W3C³	Hoa Kỳ	Worldwide Web Consortium (W3C) đang phát triển các giao thức và hướng dẫn đảm bảo tăng trưởng lâu dài cho web	Định danh
IRTF⁴	Hoa Kỳ	Lực lượng đặc nhiệm nghiên cứu Internet (IRTF) nhằm mục đích thúc	Định danh; Tài sản kỹ thuật số

¹ <https://standards.ieee.org/>

² <https://www.iso.org/standards.html>

³ <https://www.w3.org/standards/>

⁴ <https://irtf.org/>

		đẩy nghiên cứu cho sự phát triển của internet	
IEC⁵	Thụy Sĩ	Ủy ban Kỹ thuật Điện Quốc tế (IEC) thúc đẩy tiêu chuẩn hóa công nghệ điện, điện tử và các vấn đề liên quan	Internet vạn vật (IoT)
IETF⁶	Hoa Kỳ	Mục đích của Lực lượng đặc nhiệm kỹ thuật Internet (IETF) là tạo ra các tiêu chuẩn tự nguyện để duy trì và cải thiện khả năng sử dụng và khả năng tương tác của internet	Thanh toán bằng tiền điện tử
ITU-T⁷	Thụy Sĩ	Ngành Viễn thông Liên minh Viễn thông Quốc tế (ITU-T) đảm bảo sản xuất hiệu quả và kịp thời các tiêu chuẩn bao gồm tất cả các lĩnh vực viễn thông và công nghệ thông tin truyền thông (ICT) trên cơ sở toàn thế giới, đồng thời xác định các nguyên tắc thuế quan và kế toán cho các dịch vụ viễn thông quốc tế	Bảo mật; IoT; Định danh; Các yêu cầu DTL
BSI⁸	Vương Quốc Anh	Viện Tiêu chuẩn Anh (BSI) là cơ quan tiêu chuẩn quốc gia của Vương quốc Anh. Nó nhằm mục đích chia sẻ kiến thức, đổi mới và phương pháp luận để giúp mọi người và tổ chức biến sự xuất sắc thành thói quen	Các yêu cầu DTL
CEN⁹ CENELEC¹⁰	Bỉ	Ủy ban Tiêu chuẩn hóa Châu Âu (CEN) và Ủy ban Tiêu chuẩn hóa Kỹ	Bảo mật

⁵ <https://www.iec.ch/>

⁶ <https://www.ietf.org/standards/>

⁷ <https://www.itu.int/en/ITU-T/publications/Pages/default.aspx>

⁸ <https://www.bsigroup.com/en-GB/standards/>

⁹ <https://www.cen.eu/Pages/default.aspx>

¹⁰ <https://www.cenelec.eu/>

		thuật Điện Châu Âu (CENELEC) cung cấp một nền tảng để phát triển các tiêu chuẩn Châu Âu và các tài liệu kỹ thuật khác liên quan đến các loại sản phẩm, vật liệu, dịch vụ và quy trình khác nhau	
Standards Australia¹¹	Úc	Tiêu chuẩn Úc điều phối các hoạt động tiêu chuẩn hóa và tạo điều kiện cho sự phát triển của các tiêu chuẩn Úc	Bảo mật; DTL taxonomy
WIPO¹²	Thụy Sĩ	Tổ chức Sở hữu trí tuệ thế giới (WIPO): 1) thúc đẩy việc bảo hộ sở hữu trí tuệ trên toàn thế giới thông qua hợp tác giữa các quốc gia và, khi thích hợp, phối hợp với bất kỳ tổ chức quốc tế nào khác; và 2) đảm bảo hợp tác hành chính giữa các công đoàn	Ứng dụng Blockchain vào sở hữu trí tuệ
ETSI¹³	Pháp	Viện Tiêu chuẩn Viễn thông Châu Âu (ETSI) cung cấp các cơ hội, nguồn lực và nền tảng để hiểu, định hình, thúc đẩy và cộng tác trên các tiêu chuẩn áp dụng toàn cầu	Sổ cái phân tán được phép
SAC¹⁴	Trung Quốc	Cục Tiêu chuẩn hóa Trung Quốc (SAC) thực hiện trách nhiệm hành chính bằng cách thực hiện quản lý, giám sát thống nhất và điều phối tổng thể công việc tiêu chuẩn hóa ở Trung Quốc	Các yêu cầu DTL

¹¹ <https://www.standards.org.au/>

¹² www.wipo.int

¹³ <https://www.etsi.org/standards>

¹⁴ <http://www.sac.gov.cn/sacen/>

BRIBA¹⁵	Trung Quốc	Sáng kiến Vành đai và Con đường (BRI) đã thành lập Liên minh Blockchain Sáng kiến Vành đai và Con đường (BRIBA) để thúc đẩy sự phát triển của BRI bằng cách tận dụng các công nghệ blockchain	Các yêu cầu DTL
CESI¹⁶	Trung Quốc	Viện Tiêu chuẩn hóa Điện tử Trung Quốc (CESI) làm việc với các hoạt động tiêu chuẩn hóa, đánh giá sự phù hợp và đo lường trong lĩnh vực công nghệ thông tin điện tử. Trong vài năm qua, CESI đã đưa ra tầm nhìn giới thiệu ba tiêu chuẩn blockchain về hợp đồng thông minh, quyền riêng tư và tiền gửi trong nỗ lực hướng dẫn tốt hơn sự phát triển của ngành công nghiệp blockchain trong nước	Tokens; Bảo mật
DCSA¹⁷	Hà Lan	Hiệp hội Vận tải Container Kỹ thuật số (DCSA) tìm cách mở đường cho khả năng tương tác trong ngành vận tải container thông qua số hóa và tiêu chuẩn hóa	Khả năng tương tác
Internatuonal Chamber of Commerce (ICC)¹⁸	Pháp	ICC đã thành lập một nhóm làm việc gọi là Sáng kiến Tiêu chuẩn Kỹ thuật số (DSI). Mục đích của DSI là khuyến khích và duy trì khả năng tương tác dựa trên các tiêu chuẩn (giữa các tập	Khả năng tương tác

¹⁵ <https://www.beltandroadblockchain.org/>

¹⁶ <http://www.cc.cesi.cn/english.aspx>

¹⁷ <https://dcsa.org/>

¹⁸ <https://iccwbo.org/>

		đoàn và mạng lưới blockchain và phi blockchain) trong thương mại toàn cầu	
--	--	---	--

Bảng 1.6: Những nỗ lực thiết lập tiêu chuẩn lớn - các tổ chức chính thức

Tiêu chuẩn	Địa điểm	Mục đích	Chủ đề
EEA¹⁹	Hoa Kỳ	Enterprise Ethereum Alliance (EEA) xây dựng, thúc đẩy và hỗ trợ rộng rãi các phương pháp, tiêu chuẩn và kiến trúc tham chiếu dựa trên công nghệ dựa trên Ethereum	Khả năng tương tác; Token
Hyperledger²⁰	Hoa Kỳ	Hyperledger là một cộng đồng mã nguồn mở tập trung vào việc phát triển một bộ khung, công cụ và thư viện ổn định để triển khai blockchain cấp doanh nghiệp	Khả năng tương tác; Token
IWA²¹	Hoa Kỳ	Liên minh InterWork (IWA) đang làm việc để: phát triển các thông số kỹ thuật tương tác dựa trên tiêu chuẩn; giải quyết các yêu cầu của thị trường và các chỉ số hiệu suất; hỗ trợ tiến bộ trên tất cả các công nghệ nền tảng; và cho phép trao đổi nhiều bên	Token; Phân tích
JWG²²	Hoa Kỳ và Vương quốc Anh	Nhóm công tác chung về Tiêu chuẩn nhấn tin interVASP (JWG) đã xác định sự cần thiết của VASP để áp dụng các phương pháp tiếp cận thống nhất và thiết lập các tiêu chuẩn chung để	Token

¹⁹ <https://entethalliance.org/>

²⁰ <https://www.hyperledger.org/>

²¹ <https://interwork.org/>

²² <https://intervasp.org/>

		<p>cho phép họ đáp ứng các nghĩa vụ của mình do các khuyến nghị của FATF khi chúng áp dụng cho các thực thể bị ảnh hưởng</p> <p>Để giải quyết vấn đề này, một nhóm làm việc chung liên ngành, liên ngành gồm các chuyên gia kỹ thuật đã được thành lập vào tháng 12 năm 2019 và một tiêu chuẩn kỹ thuật mới do nhóm phát triển</p>	
National Blockchain and Distributed Accounting Technology Standardization Technical Committee²³	Trung Quốc	<p>Đây là một nhóm các tổ chức đã tham gia một ủy ban quốc gia tập trung vào việc tạo ra các tiêu chuẩn cho công nghệ blockchain</p>	Yêu cầu DLT; Thuật ngữ DLT
GDC ²⁴	Hoa Kỳ	<p>Nhiệm vụ của Phòng Thương mại Kỹ thuật số (CDC) là thúc đẩy việc chấp nhận và sử dụng tài sản kỹ thuật số và công nghệ dựa trên blockchain. Thông qua giáo dục, vận động và làm việc chặt chẽ với các nhà hoạch định chính sách, cơ quan quản lý và ngành công nghiệp, mục tiêu của nó là phát triển một môi trường khuyến khích đổi mới, việc làm và đầu tư</p>	Tài sản kỹ thuật số

²³ <https://tech.sina.com.cn/it/2018-05-10/docihaichqz3607998.shtml>(Chinese)

²⁴ <https://digitalchamber.org/initiatives/>

MOBI²⁵	Hoa Kỳ	Nhóm công tác nhận dạng phương tiện (VIWG) của Mobility Open Blockchain Initiative (MOBI) nhằm mục đích sử dụng DLT để làm cho tính di động an toàn hơn, xanh hơn, rẻ hơn và dễ tiếp cận hơn	Nhận dạng xe; bảo hiểm dựa trên mức sử dụng; tích hợp lưới xe điện; kết nối di động và thị trường dữ liệu; chuỗi cung ứng và tài chính; Chứng khoán hóa và hợp đồng thông minh
GDF²⁶	Vương quốc Anh	Tài chính kỹ thuật số toàn cầu (GDF) là một cơ quan thành viên trong ngành thúc đẩy việc áp dụng các phương pháp hay nhất cho tiền điện tử và công nghệ tài chính kỹ thuật số, thông qua việc phát triển các tiêu chuẩn ứng xử, trong một diễn đàn tham gia chung với những người tham gia thị trường, các nhà hoạch định chính sách và cơ quan quản lý	Các yêu cầu DTL
BIG²⁷	Canada	Tập đoàn Công nghiệp Blockchain (BIG) được dành riêng để thúc đẩy việc áp dụng các công nghệ	Yêu cầu DLT (đang tiến hành)

²⁵ <https://dlt.mobi/>

²⁶ <https://www.gdf.io/>

²⁷ <https://blockchainindustrygroup.org/>

		blockchain và tiền tệ kỹ thuật số bằng cách tích cực hợp tác và thúc đẩy những nỗ lực của cộng đồng blockchain toàn cầu của chúng tôi	
BIA²⁸	Estonia	Liên minh Công nghiệp Blockchain (BIA) tìm cách thúc đẩy các giao dịch và kết nối chéo blockchain. Mục tiêu của liên minh này là tạo ra một tiêu chuẩn được chấp nhận trên toàn cầu để kết nối các blockchain và mang lại những đổi mới lại với nhau	Khả năng tương tác
BITA²⁹	Hoa Kỳ	Blockchain in Transport Alliance (BiTA) đang tìm cách phát triển và nắm lấy một khuôn khổ và tiêu chuẩn chung mà từ đó những người tham gia vận tải / hậu cần / chuỗi cung ứng có thể xây dựng blockchain applications	Khả năng tương tác; Yêu cầu DLT

Bảng 1.7: Những nỗ lực thiết lập tiêu chuẩn chính - các nhóm ngành

Box 4: Những nỗ lực thiết lập tiêu chuẩn chính - quy trình đề xuất

- Đề xuất cải tiến Bitcoin (BIP)³⁰
- Đề xuất cải tiến Ethereum (EIP)³¹
- Đề xuất cải thiện zCash (ZIP)³²
- Sửa đổi sổ cái XRP³³
- Đề xuất cải thiện Libra (LIP)³⁴

²⁸ <https://bialliance.io/>

²⁹ <https://www.bitastudio/>

³⁰ <https://github.com/bitcoin/bips>

³¹ <https://github.com/ethereum/EIPs>

³² <https://github.com/zcash/zips>

³³ <https://xrpl.org/amendments.html>

³⁴ <https://lip.libra.org/overview>

Chương 2. Tiêu chuẩn ISO/TC 307

2.1 Tóm tắt điều hành

Công nghệ Blockchain hứa hẹn sẽ cách mạng hóa không chỉ lĩnh vực tài chính, mà còn toàn bộ mọi thứ từ hòa nhập xã hội đến hiệu quả trong chính phủ, y tế và tất cả các lĩnh vực kinh doanh.

ISO / TC 307, blockchain và công nghệ sổ cái phân tán, đã được thiết lập để đáp ứng nhu cầu tiêu chuẩn hóa ngày càng tăng trong lĩnh vực này bằng cách cung cấp các cách làm việc được quốc tế đồng ý để cải thiện bảo mật, quyền riêng tư và tạo điều kiện sử dụng công nghệ trên toàn thế giới thông qua khả năng tương tác tốt hơn. Điều này đặc biệt có liên quan do số lượng doanh nghiệp vừa và nhỏ, trên nhiều lĩnh vực khác nhau, đang phát triển công nghệ blockchain và sổ cái phân tán như một sản phẩm.

Phạm vi của ISO / TC 307 đọc: "tiêu chuẩn hóa các công nghệ blockchain và công nghệ sổ cái phân tán."

Kể từ ngày 13 tháng 3 năm 2018, công việc tiêu chuẩn hóa ISO / TC 307 đã được chia thành sáu nhóm:

- Cơ sở WG 1;
- WG 2 Bảo mật, quyền riêng tư và danh tính;
- Hợp đồng thông minh WG 3 và các ứng dụng của chúng;
- SG 2 Trường hợp sử dụng;
- Quản trị SG 6;
- SG 7 Khả năng tương tác.

Blockchain và công nghệ sổ cái phân tán là một lĩnh vực phát triển và mở rộng nhanh chóng. Nhu cầu hợp tác và hợp tác đã được xác định và ISO / TC 307 đang liên lạc với các ủy ban ISO và IEC có liên quan, cũng như các tổ chức bên ngoài, để giảm thiểu bất kỳ sự chồng chéo nào.

2.2 Giới thiệu

2.2.1 Ủy ban kỹ thuật ISO và lập kế hoạch kinh doanh

Việc mở rộng kế hoạch kinh doanh chính thức cho Ủy ban kỹ thuật ISO (ISO / TCs) là một biện pháp quan trọng tạo thành một phần của đánh giá lớn về kinh doanh. Mục đích là để điều chỉnh chương trình làm việc ISO với nhu cầu và xu hướng môi trường kinh doanh được thể hiện và cho phép ISO / TCs ưu tiên giữa các dự án khác nhau, xác định lợi ích mong đợi từ sự sẵn có của Tiêu chuẩn quốc tế và đảm bảo nguồn lực đầy đủ cho các dự án trong suốt quá trình phát triển của họ.

2.2.2 Tiêu chuẩn hóa quốc tế và vai trò của ISO

Mục đích quan trọng nhất của tiêu chuẩn hóa quốc tế là tạo thuận lợi cho việc trao đổi hàng hóa và dịch vụ thông qua việc loại bỏ các rào cản kỹ thuật đối với thương mại.

Ba cơ quan chịu trách nhiệm lập kế hoạch, phát triển và áp dụng các tiêu chuẩn quốc tế: ISO (Tổ chức tiêu chuẩn hóa quốc tế) chịu trách nhiệm cho tất cả các lĩnh vực ngoại trừ Kỹ thuật điện, là trách nhiệm của IEC (Ủy ban kỹ thuật điện quốc tế) và hầu hết các Công nghệ Viễn thông, phần lớn là trách nhiệm của ITU (Liên minh Viễn thông Quốc tế).

ISO là một hiệp hội pháp lý, các thành viên trong đó là Cơ quan Tiêu chuẩn Quốc gia (NSB) của khoảng 164 quốc gia (tổ chức đại diện cho lợi ích kinh tế và xã hội ở cấp độ quốc tế), được hỗ trợ bởi Ban Thư ký Trung ương có trụ sở tại Geneva, Thụy Sĩ.

Sản phẩm chính của ISO là Tiêu chuẩn quốc tế.

Một tiêu chuẩn quốc tế thể hiện các nguyên tắc thiết yếu của sự cởi mở và minh bạch toàn cầu, sự đồng thuận và gắn kết kỹ thuật. Chúng được bảo vệ thông qua sự phát triển của nó trong Ủy ban kỹ thuật ISO (ISO / TC), đại diện của tất cả các bên quan tâm, được hỗ trợ bởi giai đoạn bình luận công khai (Yêu cầu kỹ thuật ISO). ISO và các Ủy ban kỹ thuật của nó cũng có thể cung cấp Đặc điểm kỹ thuật ISO (ISO / TS), Thông số kỹ thuật có sẵn công khai ISO (ISO / PAS) và Báo cáo kỹ thuật ISO (ISO / TR) như các giải pháp cho nhu cầu thị trường. Các sản phẩm ISO này đại diện cho mức độ đồng thuận thấp hơn và do đó không có cùng trạng thái với Tiêu chuẩn quốc tế.

ISO cũng cung cấp Thỏa thuận hội thảo quốc tế (IWA) như một sản phẩm nhằm thu hẹp khoảng cách giữa các hoạt động của tập đoàn và quy trình tiêu chuẩn hóa chính thức được đại diện bởi ISO và các thành viên quốc gia. Một sự khác biệt quan trọng là IWA được phát triển bởi

các hội thảo ISO và fora, chỉ bao gồm những người tham gia có lợi ích trực tiếp, và do đó nó không được công nhận là tiêu chuẩn quốc tế.

2.3 Môi trường kinh doanh của ISO / TC

2.3.1.1 Mô tả môi trường kinh doanh

Các động lực chính trị, kinh tế, kỹ thuật, quy định, pháp lý và xã hội sau đây mô tả môi trường kinh doanh của ngành công nghiệp, sản phẩm, vật liệu, kỹ thuật hoặc thực tiễn liên quan đến phạm vi của ISO / TC này và chúng có thể ảnh hưởng đáng kể đến cách tiến hành các quy trình phát triển tiêu chuẩn có liên quan và nội dung của các tiêu chuẩn kết quả.

ISO / TC 307 chịu trách nhiệm tiêu chuẩn hóa liên quan đến blockchain và công nghệ sổ cái phân tán (DLT). Điều này có thể bao gồm các tiêu chuẩn liên quan đến thuật ngữ, kiến trúc tham chiếu, bảo mật và quyền riêng tư, danh tính, hợp đồng thông minh, quản trị và khả năng tương tác cho blockchain và DLT, cũng như các tiêu chuẩn cụ thể cho các ngành công nghiệp và các yêu cầu chung của chính phủ.

Blockchain và DLT vẫn đang trong giai đoạn đầu phát triển và triển khai, nhưng chúng đang phát triển nhanh chóng và cần các tiêu chuẩn nhanh chóng. Chúng cho thấy nhiều tiềm năng vì chúng cung cấp các khả năng thường không thể đáp ứng theo bất kỳ cách nào khác; Nhưng chúng đòi hỏi các công nghệ khác để có thể hoạt động. Chính sự liên kết và phụ thuộc lẫn nhau này với các công nghệ khác đòi hỏi sự phụ thuộc lẫn nhau và khả năng tương tác của các tiêu chuẩn. Các tiêu chuẩn ISO / TC 307 này sẽ tương thích và hỗ trợ các tiêu chuẩn liên quan khác.

Việc triển khai blockchain và DLT hoạt động đã tồn tại ở quy mô lớn với các ứng dụng tiềm năng trên tất cả các lĩnh vực công nghiệp, hệ thống tài chính và thanh toán, kiểm soát biên giới, quản trị và vận hành internet, hậu cần, kiểm soát xuất khẩu, hồ sơ bệnh nhân và hơn thế nữa. Nói chung, bất cứ nơi nào các yêu cầu về truy xuất nguồn gốc, trách nhiệm giải trình, tuân thủ quy định và dữ liệu có thẩm quyền tồn tại, có một yêu cầu tiềm năng đối với blockchain và DLT. Do đó, ưu tiên của ISO / TC 307 là đảm bảo rằng bất kỳ tiêu chuẩn nào được phát triển đều đủ linh hoạt để áp dụng cho nhiều ứng dụng tiềm năng. Các tiêu chuẩn sau đó sẽ cần được cập nhật liên tục trong một vòng phản hồi với các chính phủ và khu vực tư nhân để đảm bảo ISO / TC 307 đang phát triển các tiêu chuẩn đáp ứng nhu cầu của họ. Kế hoạch làm việc cho ISO / TC 307 nên được dẫn dắt theo yêu cầu, dựa trên bối cảnh chiến lược được cập nhật liên tục.

Phạm vi ứng dụng rộng rãi cho blockchain và DLT cũng có nghĩa là khu vực làm việc này có một cơ sở rộng lớn của các bên liên quan bị ảnh hưởng. Điều này bao gồm các chính phủ và khu vực tư nhân nói chung, có liên quan đặc biệt đến ngành tài chính và công nghệ thông tin, cũng

như các nhà sản xuất và nhà cung cấp các sản phẩm và tài sản vật lý và ảo, những người làm việc hoặc chuyên về quản lý dữ liệu và hồ sơ, cũng như công dân và người tiêu dùng.

Phần lớn blockchain và DLT sẽ hoạt động trong các tình huống liên quan đến dữ liệu cá nhân, riêng tư, công ty, chính phủ hoặc dữ liệu nhạy cảm khác, tất cả đều phải tuân theo quy định. Đáng chú ý nhất, là những blockchain và DLT liên quan đến hoạt động tài chính và bảo mật thông tin vì chúng có mặt khắp nơi trên tất cả các tổ chức công nghiệp và chính phủ. Các quy định quan trọng trên toàn cầu ngày nay có liên quan đến blockchain và DLT bao gồm:

- Quy định bảo vệ dữ liệu chung của EU (GDPR), đặt ra tiêu chuẩn cho việc bảo vệ dữ liệu cá nhân và quyền riêng tư. Phạm vi của nó là bất kỳ hệ thống nào bao gồm dữ liệu cá nhân, thậm chí giả mạo. Nó công nhận các yêu cầu về an toàn công cộng và các quyền cơ bản khác của con người;
- Chỉ thị 2 về dịch vụ thanh toán của EU, ảnh hưởng đến tất cả các tổ chức tài chính, tổ chức thương mại và dịch vụ bán lẻ. Nó yêu cầu Xác thực khách hàng mạnh mẽ. Điều này dựa trên các yêu cầu của G20;
- Chỉ thị chống rửa tiền 4 của EU, làm tăng phạm vi và chiều sâu của các biện pháp chống rửa tiền. Nó cũng bao gồm các loại tiền ảo, dựa trên blockchain và DLT. Điều này dựa trên các yêu cầu của G20.

Do đó, các tiêu chuẩn về bảo mật thông tin và quyền riêng tư sẽ rất quan trọng đối với bất kỳ người dùng hoặc nhà phát triển công nghệ nào, bao gồm yêu cầu pháp lý để đảm bảo rằng dữ liệu được cập nhật. Một ứng dụng khác của blockchain và DLT liên quan đến các hợp đồng thông minh; Những điều này đã có ý nghĩa trong lĩnh vực pháp lý, với các vấn đề xung quanh ngôn ngữ được sử dụng, khả năng tương thích với các khung pháp lý hiện có, sự khác biệt về quyền tài phán, khả năng thực thi và nhận thức của các công ty, nhân viên chính phủ và ngành, công dân và người tiêu dùng về tình trạng pháp lý của các hợp đồng thông minh này, cũng như việc sử dụng chúng trong các hệ thống và dịch vụ dựa trên trí tuệ nhân tạo và tự động.

Các mối quan tâm khác liên quan đến blockchain và DLT bao gồm các khía cạnh như lạm dụng tội phạm, tiêu thụ năng lượng, quản trị, bất biến vừa là lợi ích vừa là rủi ro, an toàn công cộng, bảo vệ người tiêu dùng và thiếu hiểu biết của công chúng.

Mặc dù hiện tại không có tiêu chuẩn ISO nào tồn tại cho blockchain và DLT, một số tiêu chuẩn liên quan đã được xác định mà nhóm sẽ cần phải có ý thức trong việc phát triển các tiêu chuẩn cho blockchain và DLT. Chúng bao gồm, tối thiểu:

- Loạt dịch vụ tài chính ISO 20022 - Đề án thông điệp ngành tài chính toàn cầu;
- ISO / IEC 17788 Công nghệ thông tin - Điện toán đám mây - Tổng quan và Từ vựng;
- ISO/IEC 17789 Công nghệ thông tin – Điện toán đám mây – Kiến trúc tham chiếu;
- ISO / IEC 18384 series Công nghệ thông tin - Kiến trúc tham chiếu cho kiến trúc hướng dịch vụ;
- Khung ISO / IEC 19086 Công nghệ thông tin - Điện toán đám mây - Thỏa thuận mức dịch vụ (SLA);
- ISO / IEC 27000 series Công nghệ thông tin - Kỹ thuật bảo mật, với các tiêu chuẩn hồ sơ cho nhiều ngành công nghiệp;
- Loạt ISO 29000 về quản lý danh tính và quyền riêng tư;
- Quản lý rủi ro loạt ISO 31000 - Nguyên tắc và Hướng dẫn;
- ISO 10962 series Chứng khoán và các công cụ tài chính liên quan;
- ISO 6166 series Chứng khoán và các công cụ tài chính liên quan;
- ISO / IEC 38500 series Công nghệ thông tin - Quản trị CNTT cho Tổ chức;
- Tiêu chuẩn ISO / IEC JTC 1 SC 17 về các tài liệu liên quan đến danh tính, bao gồm hộ chiếu và giấy phép lái xe.

ITU-T có các khuyến nghị có liên quan đến ISO / TC 307, đặc biệt là về cấu trúc và hoạt động của mạng, và về an ninh mạng và quản lý sự cố mạng.

IETF, OASIS và W3C cũng có các tiêu chuẩn liên quan đến ISO / TC 307, bao gồm các thông số kỹ thuật chi tiết cho hoạt động của Internet, thông tin về mối đe dọa mạng và truy xuất nguồn gốc chuỗi cung ứng và đảm bảo chất lượng.

2.3.1.2 Các chỉ tiêu định lượng môi trường kinh doanh

Các chỉ số định lượng mô tả môi trường kinh doanh để cung cấp thông tin đầy đủ để hỗ trợ các hành động của ISO / TC. Các chỉ số có thể bao gồm:

- Áp dụng và sử dụng các tiêu chuẩn ISO/TC 307;
- Sự tham gia liên tục của ngành công nghiệp và các bên liên quan với ISO / TC 307;
- Ngành công nghiệp và xu hướng toàn cầu liên quan đến blockchain và DLT.

Để đo lường việc áp dụng và sử dụng các tiêu chuẩn ISO / TC 307 cũng như sự tham gia liên tục của ISO / TC 307 với ngành công nghiệp và các bên liên quan thích hợp, ủy ban kỹ thuật có thể xem xét các chỉ số như:

- Bán các tiêu chuẩn ISO / TC 307 và các sản phẩm khác;

- Số lượng các Cơ quan thành viên ISO tham gia và quan sát về TC và số lượng ủy ban nhân bản hoạt động ở cấp quốc gia;
- Số lượng các tiêu chuẩn được thông qua bởi các cơ quan thành viên ISO và được tham chiếu trong các chương trình quốc gia;
- Cân đối các bên liên quan trong các ủy ban gương quốc gia và trong các đoàn cho các cuộc họp TC;
- Số lượng tổ chức thực hiện hoặc chứng nhận theo tiêu chuẩn;
- Số lượng các tổ chức liên lạc với ISO / TC 307 và tích cực tham gia;
- Số lượng tiêu chuẩn và các sản phẩm phân phối khác được dịch để sử dụng ở các quốc gia Thành viên ISO và các ngôn ngữ địa phương khác;
- Sự tham gia tích cực của các Cơ quan thành viên ISO vào công việc của ISO / TC 307;
- Số lượng tiêu chuẩn được sử dụng trong các quy định hoặc hợp đồng định hướng thị trường ở cấp quốc gia và quốc tế;
- Sự phù hợp của các nhà cung cấp dịch vụ với các tiêu chuẩn ISO / TC 307;
- Số lượng tiêu chuẩn theo chương trình làm việc của ISO / TC 307; và
- Tốc độ xây dựng và cập nhật các tiêu chuẩn trong danh mục ISO / TC 307.

Xu hướng ngành và toàn cầu có thể đóng vai trò là chỉ số định lượng của môi trường kinh doanh có thể bao gồm:

- số lượng ứng dụng trong thế giới thực của blockchain và DLT, vượt ra ngoài giai đoạn chứng minh khái niệm;
- số lượng các công ty, bao gồm cả các doanh nghiệp vừa và nhỏ, cung cấp blockchain hoặc DLT như một sản phẩm hoặc dịch vụ;
- giá trị ước tính của tiền kỹ thuật số được lưu trữ trong blockchain hoặc DLT;
- giá trị ước tính của tài sản được lưu trữ trong blockchain hoặc DLT;
- ước tính số lượng giao dịch đã diễn ra trên blockchain hoặc DLT.

Khi thu thập dữ liệu liên quan đến các lĩnh vực trên, ISO / TC 307 sẽ xem xét thực hiện một cuộc khảo sát các thành viên tham gia và quan sát, để mỗi Cơ quan thành viên ISO hoàn thành. Cuộc khảo sát sẽ thu thập dữ liệu về các khía cạnh như mức độ áp dụng, sử dụng các tiêu chuẩn trên toàn quốc và tình trạng thị trường ở nước họ, trong số các khía cạnh khác như chi tiết ở trên.

Một số dữ liệu có thể khó thu thập hơn, đặc biệt là xung quanh giá trị của tài sản và / hoặc tiền kỹ thuật số được giữ trong blockchain và DLT. ISO / TC 307 sẽ khám phá thông qua cơ sở thành viên của mình mức độ báo cáo công khai có sẵn liên quan đến những điều trên và có thể

cần phải rút ra kết quả của các cuộc khảo sát hoặc nghiên cứu ngành khác được thực hiện có quyền truy cập vào dữ liệu đó.

2.4 LỢI ÍCH MONG ĐỢI TỪ CÔNG VIỆC CỦA ISO / TC

Những lợi ích dự kiến sẽ được thực hiện do tiêu chuẩn hóa cho blockchain và DLT bao gồm:

- Hỗ trợ đổi mới, cạnh tranh, quản trị, phát triển và tăng trưởng trong lĩnh vực này, đặc biệt là trong các kịch bản sử dụng xuyên biên giới, xuyên biên giới để cải thiện dịch vụ cho công dân;
- Thuật ngữ thống nhất và kiến trúc tham chiếu trong lĩnh vực này;
- Tăng sự hiểu biết và sự tự tin áp dụng của blockchain và dlt;
- Một tài liệu tham khảo hoặc kho lưu trữ tiềm năng cho các ứng dụng trường hợp sử dụng để hướng dẫn việc áp dụng;
- Tăng cường áp dụng blockchain và dlt của ngành công nghiệp và chính phủ;
- Tạo điều kiện thuận lợi cho khả năng tương thích giữa công nghệ và khung pháp lý trên một loạt các khu vực pháp lý;
- Hỗ trợ người dùng và người mua có thể xác nhận chất lượng của blockchain và dlt có sẵn trên thị trường;
- Cho các nhà cung cấp dịch vụ, cải thiện niềm tin và danh tiếng, với việc giảm rủi ro nhận thức;
- Khả năng tương tác giữa các công nghệ sổ cái khác nhau và giữa các công nghệ sổ cái và các thành phần hệ thống khác;
- Loại bỏ các rào cản gia nhập bằng cách tạo điều kiện đẩy nhanh thời gian đưa ra thị trường;
- Giảm nguy cơ bị "khóa" vào các phương pháp tiếp cận kỹ thuật hoặc không chuẩn hóa cụ thể có thể chứng minh không thành công hoặc có vấn đề trong tương lai;
- Tăng đầu tư vào blockchain và dlt;
- Cải thiện kết quả bảo mật và quyền riêng tư thông qua việc cung cấp các yêu cầu mạnh mẽ, cũng dẫn đến niềm tin của người tiêu dùng vào các công nghệ này;
- Giảm chi phí thực hiện bằng cách cung cấp các yêu cầu cơ bản minh bạch.

2.5 ĐẠI DIỆN VÀ THAM GIA ISO / TC

2.5.1 Thành viên

Chi tiết về tư cách thành viên và liên lạc viên ISO / TC 307 có thể được tìm thấy trên trang chủ của ủy ban: <https://www.iso.org/committee/6266604.html>

2.5.2 Phân tích sự tham gia

Bảng phân tích và phân tích dưới đây là chính xác tính đến ngày 18 tháng 3 năm 2018. Tham khảo trang chủ thành viên ủy ban để biết thông tin cập nhật: <https://www.iso.org/committee/6266604.html?view=participation>.

- **Phân tích theo khu vực**

Vùng	Thành viên P	Thành viên O
Châu Phi	0	1
Châu Mỹ	4	2
Châu Á - Thái Bình Dương	7	5
Châu Âu	20	4
Trung Đông	0	2

LƯU Ý: Vì mục đích của bảng này, Nga đã được phân loại là một phần của châu Âu.

- **Phân tích**

Từ những điều trên, có thể thấy rằng các thành viên hiện tại của ISO / TC 307 rất ủng hộ các thành viên phát triển, với sự hiện diện thống trị của châu Âu trong số các thành viên tham gia và các thành viên tham gia từ Bắc Mỹ là Hoa Kỳ và Canada. Một xu hướng khác nổi lên là sự hiện diện mạnh mẽ ở khu vực châu Á-Thái Bình Dương, với một số lượng đáng kể các thành viên tham gia và quan sát trên các trạng thái phát triển khác nhau trong khu vực đó.

Đại diện này phản ánh bản chất kỹ thuật cao của công việc, với sự tham gia mạnh mẽ hơn từ các quốc gia có trình độ công nghiệp và chuyên môn cao hơn trong lĩnh vực này, dẫn đến sự mất cân bằng nặng nề đối với các quốc gia phát triển ở châu Âu và Bắc Mỹ, và những quốc gia đang chuyển đổi ở châu Á-Thái Bình Dương. Các thành viên đã lưu ý rằng Estonia nổi bật như một loại trừ khỏi danh sách và đã tìm cách khuyến khích sự tham gia của thành viên này.

Đáng chú ý là có rất ít sự tham gia vào ủy ban từ Trung và Nam Mỹ và Châu Phi, chỉ có Brazil (thành viên P), Jamaica (thành viên P), Nam Phi (thành viên P), Argentina (thành viên O) và Uruguay (thành viên O) đại diện cho các khu vực này. Cho đến nay, Trung Đông cũng có sự

tham gia hạn chế, chỉ có Israel và Iran được liệt kê (cả hai đều là thành viên O). Cần khuyến khích sự tham gia mạnh mẽ hơn ở các khu vực này, và cơ quan thành viên ban thư ký, Úc, có thể muốn xem xét một thỏa thuận kết nghĩa với một thành viên khác để khuyến khích điều này.

Về mặt liên lạc, ISO / TC 307 có năm liên lạc bên ngoài cho đến nay, với SWIFT, Ủy ban Châu Âu, Liên đoàn Khảo sát Quốc tế, Liên minh Viễn thông Quốc tế và Ủy ban Kinh tế Liên Hợp Quốc Châu Âu. Đã có nhiều sự quan tâm từ ngành công nghiệp và các tổ chức bên ngoài trong việc liên lạc với ISO / TC 307; số tiền lãi cho thấy ngành công nghiệp nhận thức được việc thành lập ISO / TC 307 và rất muốn tham gia vào quá trình này. Ngoài ra, ISO / TC 307 đang tích cực tham gia với các tổ chức và cơ quan có liên quan trên thị trường và ngành công nghiệp để khuyến khích liên lạc và đảm bảo rằng công việc được phát triển bởi ISO / TC 307 là và vẫn có liên quan.

Các liên lạc thích hợp đã được thiết lập nội bộ với các ủy ban ISO và ISO / IEC khác, và một lần nữa danh sách này dự kiến sẽ tăng lên một chút theo thời gian. Các thành viên cá nhân của ISO / TC 307 có thể hiện sự háo hức hợp tác với các ủy ban ISO và ISO / IEC khác và tránh mọi sự trùng lặp công việc.

2.6 Mục tiêu của ISO / TC và các chiến lược cho thành tích

2.6.1 Mục tiêu xác định của ISO/TC

ISO/TC 307 sẽ:

- Sản xuất một bộ Tiêu chuẩn và báo cáo quốc tế sẽ khuyến khích việc áp dụng blockchain và DLT và hỗ trợ đổi mới, quản trị và phát triển trong ngành. Các tiêu chuẩn và báo cáo quốc tế này sẽ bao gồm các chủ đề hỗ trợ cả các kịch bản sử dụng xuyên biên giới, xuyên biên giới. Ủy ban đặt mục tiêu có các Tiêu chuẩn và báo cáo quốc tế này không muộn hơn năm 2021;
- Phát triển một thuật ngữ Tiêu chuẩn quốc tế sẽ cung cấp một từ vựng thống nhất cho blockchain và DLT. Ủy ban đặt mục tiêu có tiêu chuẩn này không muộn hơn năm 2020;
- Phát triển một kiến trúc tham chiếu Tiêu chuẩn quốc tế sẽ cung cấp một cái nhìn thống nhất về blockchain và DLT. Ủy ban đặt mục tiêu có tiêu chuẩn này không muộn hơn năm 2021;
- Phát triển một kho lưu trữ các trường hợp sử dụng để hỗ trợ hiểu các ứng dụng và triển khai của blockchain và DLT. Kho lưu trữ này sẽ là một sáng kiến liên tục;

- Xây dựng một gói Tiêu chuẩn và Thông số kỹ thuật quốc tế để giải quyết khả năng tương thích giữa công nghệ và khung pháp lý để hỗ trợ việc áp dụng blockchain và DLT của ngành công nghiệp và chính phủ, sẽ có sẵn vào năm 2021;
- Tạo Báo cáo kỹ thuật trong các lĩnh vực bảo mật, quyền riêng tư và danh tính sau đó điều tra các Tiêu chuẩn quốc tế tiềm năng cần được phát triển vì các khía cạnh được xác định và xác định tốt hơn;
- Giải quyết khả năng tương tác giữa các công nghệ sổ cái khác nhau và giữa các công nghệ sổ cái và các thành phần hệ thống khác vì các khía cạnh được phát triển và xác định tốt hơn.

2.6.2 Xác định các chiến lược để đạt được các mục tiêu đã xác định của ISO / TC

Các chiến lược được ISO / TC 307 sử dụng để đạt được các mục tiêu được liệt kê ở trên bao gồm:

- Ưu tiên các dự án trong ISO / TC 307, chẳng hạn như thuật ngữ và kiến trúc tham chiếu làm khái niệm nền tảng cho các tiêu chuẩn khác để xây dựng;
- Các nhóm nghiên cứu sẽ được thành lập khi thích hợp, để điều tra các lĩnh vực tiềm năng để tiêu chuẩn hóa trong blockchain và DLT;
- Hợp tác với các ủy ban ISO khác, IEC và các SDO khác, để tránh trùng lặp công việc;
- Tận dụng công việc liên quan nếu có, từ cả hai ủy ban ISO và ISO / IEC khác, và từ ngành công nghiệp và thị trường rộng hơn;
- Tiến hành giám sát thị trường và ngành liên tục đối với các trường hợp sử dụng và ứng dụng, để đảm bảo các tiêu chuẩn được phát triển không dành riêng cho các ngành cụ thể;
- Phát triển các báo cáo kỹ thuật nếu có, để hỗ trợ sự hiểu biết về blockchain và DLT.

Ủy ban có thể xem xét việc thành lập các tiểu ban chính thức ở giai đoạn sau.

2.7 CÁC YẾU TỐ ẢNH HƯỞNG ĐẾN VIỆC HOÀN THÀNH VÀ THỰC HIỆN CHƯƠNG TRÌNH LÀM VIỆC ISO / TC

Các yếu tố có khả năng tác động tiêu cực đến công việc của ISO / TC 307 bao gồm những yếu tố đặc trưng của tiêu chuẩn hóa và những yếu tố cụ thể của ngành. Hai loại rủi ro đã được nhóm lại tương ứng dưới đây.

Các yếu tố đặc trưng của tiêu chuẩn hóa có thể ảnh hưởng đến công việc của ISO / TC 307 bao gồm:

- Các vị trí Chủ tịch ủy ban ISO, Thư ký, Người triệu tập hoặc Trưởng dự án còn trống;

- Nguồn lực chuyên gia không đủ sẵn có (đối với một số dự án nhất định);
- Chuyên môn cụ thể cho một dự án còn thiếu, có thể ảnh hưởng đến sự phát triển của dự án cũng như độ tin cậy của tiêu chuẩn kết quả trong cộng đồng doanh nghiệp;
- Việc xác nhận một phương pháp thử nghiệm phụ thuộc vào nguồn tài trợ có sẵn để thực hiện nghiên cứu trước / đồng quy phạm cần thiết;
- Các vấn đề pháp lý / quy định như sự không chắc chắn liên quan đến Chỉ thị EC có thể có hoặc các yêu cầu và xung đột về quyền tài phán, do đó có thể yêu cầu sửa đổi nội dung và ngày mục tiêu cho các dự án trong chương trình làm việc;
- Các thành viên có thể gặp khó khăn trong việc đạt được sự đồng thuận, do các lợi ích địa chính trị và thị trường đa dạng hiện nay.

Các yếu tố cụ thể của ngành có thể ảnh hưởng đến công việc của ISO / TC 307 bao gồm:

- Môi trường thị trường hiện tại cho blockchain và DLT bị chi phối bởi cả các dự án nguồn mở và độc quyền. Các nhóm này có thể không sẵn sàng tuân thủ các tiêu chuẩn ISO và / hoặc thấy ít giá trị khi làm như vậy;
- Các sáng kiến tiêu chuẩn hóa song song do ngành dẫn đầu trong các lĩnh vực thị trường cụ thể có thể dẫn đến trùng lặp hoặc xung đột;
- Lĩnh vực blockchain và DLT là một lĩnh vực thay đổi nhanh chóng, với nhiều công việc sáng tạo đang được thực hiện bởi các công ty khởi nghiệp nhỏ trên toàn cầu. Các nhóm này có thể coi các tiêu chuẩn là kìm hãm sự đổi mới hoặc sáng tạo;
- Ngành công nghiệp blockchain và DLT là một ngành rất phân mảnh, giải quyết nhiều vấn đề khác nhau. Ngoài ra, ngành công nghiệp dựa trên một số công nghệ đã được tiêu chuẩn hóa. Điều này có thể đặt ra một thách thức trong việc có thể tạo ra một bộ tiêu chuẩn gắn kết phù hợp với tất cả các bên liên quan và tương thích và nhận thức được các công nghệ tiêu chuẩn hóa hiện có đang được sử dụng.
- Đối với một số ngành công nghiệp hiện có, có sự kháng cự đối với blockchain và DLT, vì chúng gây ra mối đe dọa cho một số ngành nhất định và có thể gây rối. Ví dụ có thể là trong các lĩnh vực hậu cần hoặc dịch vụ trực tuyến;
- Trong các lĩnh vực như hợp đồng thông minh, có những tác động pháp lý của công nghệ này. Do đó, các Tiêu chuẩn cần đảm bảo chúng tương thích với các yêu cầu lập pháp trên một loạt các khu vực pháp lý. Với tính chất toàn cầu của quy trình tiêu chuẩn ISO và cụ thể là ISO / TC 307, điều này có thể chứng minh một thách thức không thể vượt qua;

- Các ứng dụng trường hợp sử dụng có tỷ lệ giao dịch rất cao, ví dụ như trong Internet of Things hoặc trong Giao dịch tài chính, có thể không sử dụng được công nghệ này, với tiềm năng là các lựa chọn thay thế khác xuất hiện.

Chương 3. Tiêu chuẩn DIN SPEC 3104

3.1 Phạm vi

DIN SPEC 3104 xác định khung kỹ thuật và chức năng của phần mềm xác thực blockchain cho quy trình xác thực blockchain. Đặc biệt, nó cung cấp các yêu cầu và tiêu chí đánh giá cho tính chính xác của blockchain và khía cạnh chức năng đặt thời gian trên blockchain.

Các tiêu chí đánh giá được đưa ra cho proof of work blockchain công khai, vì đây là loại blockchain chính được sử dụng trong phần mềm xác thực blockchain. Các tiêu chí không xác định thời điểm mà đánh dấu thời gian trên blockchain được coi là tốt, mà thay vào đó yêu cầu phần mềm cung cấp đủ thông tin cho người dùng để tự đưa ra đánh giá.

Các khía cạnh chức năng khác của phần mềm xác thực blockchain, đặc biệt là việc nhận dạng người dùng và lưu trữ dữ liệu, cũng như các vấn đề liên quan đến việc phát triển phần mềm chính mình, chẳng hạn như đảm bảo chất lượng, không được bao gồm trong tài liệu này.

DIN SPEC 3104 nhắm đến người dùng phần mềm xác thực blockchain. Việc thảo luận về phần mềm của các proof of work blockchain công khai không thuộc phạm vi của quy định này.

Tài liệu này áp dụng cho việc xác thực dựa trên blockchain nói chung cũng như các ứng dụng cụ thể, chẳng hạn như:

- Chứng minh quyền sở hữu vật lý và trí tuệ (ngoại trừ yêu cầu hình thức),
- Các tuyên bố ý định (ngoại trừ yêu cầu hình thức bằng văn bản),
- Các đăng ký công khai,
- Xác thực trang web và tài liệu kế toán,
- Hỗ trợ xác thực tài liệu dựa trên blockchain trong một môi trường đa quốc gia và
- Mạng năng lượng và công nghệ SmartMeter.

Việc chứng nhận và công chứng tài liệu không thuộc phạm vi của tài liệu này vì các quy trình này được quy định bởi pháp luật quốc gia và châu Âu.

3.2 Tài liệu tham chiếu

Các tài liệu sau được đề cập trong văn bản theo cách mà một phần hoặc toàn bộ nội dung của chúng đáp ứng yêu cầu của tài liệu này. Đối với các tài liệu có ngày đề cập, chỉ áp dụng phiên bản được trích dẫn. Đối với các tài liệu không có ngày đề cập, áp dụng phiên bản mới nhất của tài liệu tham chiếu (bao gồm bất kỳ sửa đổi nào).

ISO/IEC 9796-2, Công nghệ thông tin - Kỹ thuật an ninh - Các phương pháp chữ ký số cho phục hồi thông điệp - Phần 2: Cơ chế dựa trên phân tích số nguyên

ISO/IEC 10118-3, Công nghệ thông tin - Hàm băm - Phần 3: Các hàm băm đặc biệt

ISO/IEC 14888-3, Kỹ thuật bảo mật - Chữ ký số với phụ lục - Phần 3: Cơ chế dựa trên logarithm rời rạc

EN 319 132-1 V1.1.1 (2016-04), Chữ ký điện tử và cơ sở hạ tầng (ESI) - Chữ ký số XAdES - Phần 1: Các khối xây dựng và chữ ký cơ bản XAdES

BSI TR-03111, Mật mã Elliptic Curve, Phiên bản 2.10, 2018-06-01

FIPS 186-4, Tiêu chuẩn Chữ ký số (DSS), Tháng 7 năm 2013

Chính sách của NIST về hàm băm, Tháng 8 năm 2015

PKCS #1 RSA Cryptography Specifications Version 2.2

RFC 3447, Tiêu chuẩn Mật mã Khóa công khai (PKCS) #1: Các thông số Mật mã RSA Phiên bản 2.1, Tháng 2 năm 2003

SOG-IS Crypto Evaluation Scheme Agreed Cryptographic Mechanisms, Phiên bản 1.1, Tháng 6 năm 2018

3.3 Thuật ngữ và định nghĩa

Với mục đích của tài liệu này, các thuật ngữ và định nghĩa được đưa ra trong DIN SPEC 16597 và các thuật ngữ sau đây áp dụng.

DIN và DKE duy trì các cơ sở dữ liệu thuật ngữ để sử dụng trong tiêu chuẩn hóa tại các địa chỉ sau:

DIN-TERMinologieportal: có sẵn tại <https://www.din.de/go/din-term>

DKE-IEV: có sẵn tại <http://www.dke.de/DKE-IEV>

Độ chính xác

Số S của một đơn vị thời gian nào đó sao cho nếu một khối trong blockchain có dấu thời gian T, thì khối này đã được tạo ra trong khoảng thời gian $[T-S, T+S]$.

Lưu ý: Độ chính xác của blockchain được đưa ra theo đơn vị thời gian.

Xác thực Blockchain

Chứng minh tính chính xác của blockchain và dấu thời gian của blockchain.

Chứng minh tính chính xác của blockchain

Thông tin được lưu trữ trên blockchain, là một băm của một mảnh dữ liệu hoặc một gốc của cây Merkle chứa băm của một mảnh dữ liệu, tạo ra bằng chứng về trạng thái cụ thể của mảnh dữ liệu này

Dấu thời gian của blockchain

Dữ liệu kỹ thuật số trong blockchain, liên kết với dữ liệu kỹ thuật số khác trong một khoảng thời gian cụ thể, tạo ra bằng chứng rằng dữ liệu sau tồn tại tại một điểm thời gian nào đó trong khoảng thời gian này

Cây nhị phân đầy đủ

Cây trong đó mỗi phần tử có tối đa hai liên kết đi ra, và mỗi cấp N trong cây, trừ có thể là cấp lớn nhất, có $2N$ phần tử

Mật mã học

Lĩnh vực thể hiện các nguyên tắc, phương tiện và phương pháp để biến đổi dữ liệu nhằm ẩn nội dung ngữ nghĩa của chúng, ngăn chặn việc sử dụng trái phép hoặc ngăn chặn việc sửa đổi không phát hiện được của chúng.

Chữ ký và chữ ký số

Dữ liệu được gắn vào một đơn vị dữ liệu hoặc là một biến đổi mật mã của đơn vị dữ liệu đó, cho phép một thực thể chứng minh nguồn gốc và tính toàn vẹn của đơn vị dữ liệu và bảo vệ khỏi việc giả mạo.

Dấu thời gian điện tử

Dữ liệu dạng điện tử liên kết với dữ liệu dạng điện tử khác vào một thời điểm cụ thể, tạo ra bằng chứng rằng dữ liệu sau tồn tại tại thời điểm đó.

Nút lá

Phần tử của một cây không có bất kỳ nút con nào.

Chứng minh tính chính xác

Thông tin về một mảnh dữ liệu tạo ra bằng chứng về trạng thái cụ thể của mảnh dữ liệu này

Proof of work (PoW)

Cơ chế đồng thuận yêu cầu các thành viên chứng minh mật mã sở hữu một lượng tài nguyên tính toán nhất định để tạo ra các khối mới

Phần mềm

Sáng tạo trí tuệ bao gồm các chương trình, quy trình, quy tắc và bất kỳ tài liệu liên quan nào liên quan đến hoạt động của một hệ thống

Trạng thái của blockchain

Tập hợp tất cả các giao dịch mà khả năng còn lại là một phần của blockchain, sau khi đã đạt được sự đồng thuận, được coi là đủ cao.

Đơn vị thời gian

Khoảng thời gian cụ thể, được sử dụng làm cách tiêu chuẩn để đo hoặc diễn đạt thời gian

Khoảng thời gian

Khoảng cách thời gian bao gồm các điểm thời gian

Dấu thời gian

Tham số được bao gồm trong một khối, chỉ định một thời điểm mà khối đó được tạo ra.

3.4 Các đặc điểm chung của việc xác thực blockchain

Hai dịch vụ, truyền thống được cung cấp bởi các bên thứ ba đáng tin cậy, bao gồm:

- Chứng minh tính chính xác cho một tài liệu và tuyên bố ý định,
- Đánh dấu thời gian điện tử, chứng tỏ rằng tài liệu tồn tại tại một thời điểm cụ thể.

Xác thực blockchain là một quy trình tương tự, trong đó:

- Các nhiệm vụ truyền thống của các bên thứ ba đáng tin cậy được thực hiện bởi phần mềm xác thực blockchain và blockchain,
- Quá trình xác minh có thể được người dùng thực hiện độc lập, sử dụng phần mềm xác thực blockchain và dữ liệu blockchain.

Cụ thể, hai quy trình sau đây được mô tả, được thực hiện bằng blockchain:

- Chứng minh tính chính xác của blockchain,
- Đánh dấu thời gian của blockchain.

Nếu chứng minh tính chính xác của blockchain được áp dụng cho dữ liệu D, thì được chứng thực rằng dữ liệu D đã tồn tại. Nếu dữ liệu D được đánh dấu thời gian trong blockchain với thời điểm T, thì được chứng minh rằng D tồn tại trong một khoảng thời gian, trong đó khoảng thời gian được xác định bởi T và nằm trong độ lệch của độ chính xác của các dấu thời gian blockchain.

Các chức năng của phần mềm xác thực blockchain bao gồm:

- Tạo chứng minh tính chính xác của blockchain cho dữ liệu, đánh dấu thời gian của blockchain cho dữ liệu và một tệp chứa thông tin cần thiết để xác minh việc xác thực blockchain.
- Xác minh chứng minh tính chính xác của blockchain hiện có và các dấu thời gian của blockchain. Điều này bao gồm:
 - Xác minh sự tồn tại của dữ liệu trong blockchain
 - Đánh giá tính không thể thay đổi (đối với chứng minh tính chính xác của blockchain, và
 - Ước tính độ chính xác của các dấu thời gian blockchain (đối với đánh dấu thời gian của blockchain).

Yêu cầu về bảo mật trong việc lưu trữ dữ liệu có thể được thực hiện theo ISO/IEC 27000, ISO/IEC 27001, ISO/IEC 27002, ISO/IEC 27003, ISO/IEC 27004 và ISO/IEC 27005.

3.5 Khung kỹ thuật của quá trình xác thực blockchain

3.5.1 Các bước của quá trình xác thực blockchain

Ban đầu của quá trình xác thực blockchain, người dùng có một mảnh dữ liệu trong định dạng kỹ thuật số. Kết quả của quá trình là người dùng nhận được một dữ liệu kỹ thuật số khác dưới dạng một tệp tin, cùng với dữ liệu blockchain cung cấp chứng minh tính chính xác của blockchain và dấu thời gian của dữ liệu người dùng trên blockchain.

Đầu vào cho quá trình tạo xác thực blockchain là dữ liệu cần được notarize trên blockchain. Dữ liệu này có thể tùy chọn bao gồm chữ ký kỹ thuật số để người dùng có thể chứng minh rằng anh ta sở hữu dữ liệu đó.

Quy trình này tương tự cho cả quá trình chứng minh tính chính xác của blockchain và quá trình đánh dấu thời gian của blockchain. Nó bao gồm các bước sau:

- Phần mềm cho phép người dùng ký kết dữ liệu, để có thể chứng minh rằng anh ta sở hữu dữ liệu đó.
- Phần mềm tạo ra một giá trị băm của dữ liệu.
- Phần mềm tổng hợp một số giá trị băm của các mục dữ liệu khác nhau thành một cây Merkle.
- Phần mềm thực hiện việc notarize dữ liệu trên blockchain, có nghĩa là một số thông tin mật mã được lưu trữ trên blockchain. Thông tin này có thể là giá trị băm của dữ liệu hoặc là gốc Merkle của một cây chứa giá trị băm của dữ liệu. Bước này cung cấp cả chứng minh tính chính xác của blockchain và dấu thời gian trên blockchain.
- Phần mềm xuất ra thông tin cần thiết để chứng minh xác thực blockchain.

3.5.2 Thành phần mật mã học

3.5.2.1 Hàm băm

Hàm băm được sử dụng để tạo ra một dấu vân tay của dữ liệu cần notarize trên blockchain. Hàm băm phải là một trong những hàm được sử dụng trong:

SOG-IS, Mục 2.3 hoặc,
ISO/IEC 10118-3, hoặc
Chính sách của NIST về các hàm băm.

3.5.2.2 Chữ ký kỹ thuật số

Phần mềm xác thực blockchain có thể bao gồm chức năng chữ ký kỹ thuật số. Nếu nhà sản xuất phần mềm chọn cung cấp chức năng này, chữ ký phải thuộc một trong những loại được liệt kê trong phần này. Quyết định sử dụng chức năng chữ ký kỹ thuật số sẽ để cho người dùng có mong muốn chứng minh sở hữu dữ liệu được notarize trên blockchain.

Các chữ ký kỹ thuật số được chấp nhận phải là một trong những loại được liệt kê trong EN 319 132-1 V1.1.1 (2016-04) hoặc trong SOG-IS, phiên bản 2018.

- RSA
 - PSS (PKCS#1v2.1) [RFC3447, PKCS1, ISO/IEC 9796-2]
 - PKCS#1v1.5 [RFC3447, PKCS1, ISO/IEC 9796-2]
- FF-DLOG
 - Schnorr [ISO/IEC 14888-3]
 - DSA [FIPS186-4, ISO/IEC 14888-3]
- EC-DLOG
 - EC-KCDSA [ISO/IEC 14888-3]
 - EC-DSA [FIPS186-4, ISO/IEC 14888-3]
 - EC-GDSA [BSI TR-03111]
 - EC-Schnorr [ISO/IEC 14888-3]

3.5.2.3 Đầu ra của quá trình xác thực blockchain

Phần mềm cung cấp thông tin sau đây cho người dùng dưới dạng một tệp tin để xác minh dữ liệu:

- Chữ ký kỹ thuật số (nếu đã sử dụng);
- Hàm băm được sử dụng;
- Thông tin về cây Merkle, nếu đã sử dụng cây Merkle;
- Blockchain đã được sử dụng trong quá trình;
- Giao dịch chứa thông tin mật mã đã được lưu trữ trên Blockchain;

- Dữ liệu xác minh của chữ ký kỹ thuật số (nếu sử dụng), thời gian đánh dấu thời gian và dữ liệu cụ thể của blockchain và thông tin về người xác thực.

3.6 Khung kỹ thuật của quá trình xác minh xác thực blockchain

3.6.1 Giới thiệu

Trong ngữ cảnh xác thực blockchain, một blockchain chứa các hàm băm của dữ liệu hoặc gốc cây Merkle chứa các hàm băm của dữ liệu.

Hai quy trình phải được thực hiện trong quá trình xác minh xác thực blockchain:

Kiểm tra sự tồn tại: xác minh rằng thông tin mật mã cần thiết (hàm băm của một phần dữ liệu hoặc gốc cây Merkle chứa hàm băm của một phần dữ liệu) đã được bao gồm trong một khối nào đó của blockchain.

Đánh giá tính không thay đổi: blockchain phải không thể thay đổi, có nghĩa là dữ liệu trong các khối không thể được sửa đổi, xóa bỏ hoặc thêm vào.

Những quy trình này là đủ để xác minh blockchain proof of correctness.

Nếu việc xác minh blockchain time-stamping cũng được thực hiện, quy trình sau đây cũng phải được thực hiện:

Ước lượng độ chính xác (đối với blockchain time-stamp): độ chính xác của các dấu thời gian trên blockchain là bao nhiêu?

Tiêu chí đánh giá quan trọng mà phải được sử dụng xem xét mức độ khó khăn để vi phạm tính không thay đổi của blockchain. Độ chính xác của các dấu thời gian trên blockchain phải được thông báo ít nhất cho người dùng bằng phần mềm.

3.6.2 Các bước của quá trình xác minh xác thực blockchain hiện có

Ở đầu quá trình xác minh của một quá trình xác thực blockchain, người dùng cung cấp hai mảnh dữ liệu đầu vào:

- Dữ liệu đã được blockchain notarized trước đó;
- Thông tin được cung cấp bởi phần mềm như kết quả của quá trình xác thực blockchain.

Kết quả của quá trình xác minh, dựa trên dữ liệu đầu vào này, bao gồm:

- Một khẳng định rằng dữ liệu thực sự đã được blockchain notarized;
- Thông tin về việc xác thực blockchain;

- Trong trường hợp yêu cầu một blockchain time-stamp, thông báo từ chối về độ chính xác của dấu thời gian và tùy chọn một ước lượng về độ chính xác cho dấu thời gian.

Các bước của quá trình xác minh xác thực blockchain, để đạt được kết quả trên, là:

- Phần mềm tải xuống thông tin blockchain liên quan.
- Phần mềm xác minh chứng cứ bằng cách sử dụng thông tin blockchain và xuất ra xem liệu dữ liệu có được blockchain notarized và đánh giá tính không thay đổi hay không.

Trong trường hợp blockchain time-stamping, phần mềm sử dụng thêm dữ liệu blockchain để hiển thị dấu thời gian trên blockchain. Ngoài ra, phần mềm phải cung cấp thông báo từ chối về độ chính xác của dấu thời gian và có thể nêu rõ độ chính xác của dấu thời gian.

3.7 Các yếu tố trong quá trình xác minh một dấu thời gian trên blockchain hiện có

3.7.1 Tổng quan và quy tắc ứng dụng

Phần mềm xác minh xác thực blockchain phải bao gồm trong quá trình xác minh cho blockchain proof of correctness những mục được mô tả trong 3.3.2. Nó cũng phải bao gồm những mục được mô tả trong 3.3.3. Nếu được chứng minh một cách thích hợp, có thể có các phương pháp xác minh thay thế. Trong trường hợp xác minh một dấu thời gian trên blockchain, những mục được mô tả trong 6.3.4 cũng phải được thực hiện.

3.7.2 Khẳng định

Phần mềm khẳng định tính hợp lệ của thông tin đã được cung cấp.

- Thông tin đủ để xác minh rằng dữ liệu mật mã được lưu trữ trong khối và giao dịch nào trên blockchain.
- Dữ liệu mật mã thực sự được lưu trữ trong khối đã cho.

3.7.3 Đánh giá tính không thay đổi (dựa trên bằng chứng công việc)

Cơ chế bằng chứng công việc cung cấp thông tin về lượng proof of work ("work") đã được sử dụng để tạo ra một khối. Bằng chứng công việc được sử dụng

như một bằng chứng cho tính không thay đổi. Điều này có thể được thấy thông qua các sự thật sau:

- Chuỗi dài nhất được xác định là chuỗi có số lượng công việc nhiều nhất.
- Một khối được coi là không thể thay đổi trong thực tế sau một số lượng xác nhận phù hợp.
- Các thuật ngữ sau được sử dụng để đánh giá lượng năng lượng (trong watt) cần thiết để tạo ra một khối:
- `block_average_hashes`: số lượng hashes, trung bình, cần thiết để tạo ra một khối.

GHI CHÚ: Thông tin này được bao gồm trong mỗi khối.

- `watt_hash(t)`: lượng watt cần thiết để tính toán một hash cụ thể tại một thời điểm nhất định.

GHI CHÚ: Năng lượng để tính toán một hash khác nhau dựa trên hàm hash và trạng thái của phần cứng hiện đại. Phần mềm phải cung cấp nguồn thông tin mà thông tin này được lấy từ.

- `watt_block(t)`: lượng watt cần thiết, trung bình, tại thời điểm `t` để tạo ra một khối.

Công thức sau đây được suy ra ngay từ những định nghĩa đó:

– $watt_block(t) = watt_hash(t) \cdot block_average_hashes$.

GHI CHÚ: Ví dụ trong Bitcoin, mỗi khối được gắn kết với một giá trị gọi là độ khó [16]. Số lượng hashes ước tính cần thiết để tạo ra một khối trong Bitcoin là [16]: $(difficulty_of_block \cdot 2^{32})$,

Các thuật ngữ sau được sử dụng để đánh giá lượng năng lượng (trong watt) cần thiết để tạo ra một khối và các khối tiếp theo trong một blockchain:

- `H`: chiều cao của khối.
- `D`: độ sâu của khối.
- `watt_block_H_D(t)`: lượng watt tại thời điểm `t` cần thiết, trung bình, để tạo ra tất cả các khối giữa `H` và `D`.
- Công thức sau đây được suy ra từ một phép tính đơn giản:
- $watt_block_H_D(t) = \text{tổng}(watt_block(t) \text{ của tất cả các khối giữa } H \text{ và } H+D)$

- Phần mềm phải trình bày `watt_block_H_D` cho khối chứa dấu thời gian của dữ liệu.

3.7.4 Độ chính xác của dấu thời gian trên blockchain

Dấu thời gian của các khối không hoàn toàn chính xác trên blockchain. Ví dụ, "dấu thời gian Bitcoin có thể chênh lệch trong vài giờ so với thời gian được duy trì bởi các thành viên Bitcoin (nút), và lý thuyết có thể chênh lệch một cách đáng kể so với thời gian thực tế (tức là thời gian bên ngoài mạng Bitcoin)." [18] Nguyên tắc này khác biệt so với các giải pháp đánh dấu thời gian kỹ thuật số không phải là blockchain, trong đó dấu thời gian trên Blockchain là chính xác.

Trong quá trình xác minh một dấu thời gian trên blockchain, phần mềm nên hiển thị cho người dùng:

- Một thông báo miễn trừ trách nhiệm về độ chính xác của dấu thời gian trên Blockchain, và/hoặc
- Một tuyên bố về độ chính xác của dấu thời gian trên Blockchain, và/hoặc
- Một phân tích, hoặc một liên kết đến một phân tích, để ước tính độ chính xác của dấu thời gian trên blockchain.

Chương 4. Đánh giá và đề xuất

4.1 Đánh giá

4.1.1 Tổng quan về Bitcoin

4.1.1.1 Khái niệm Bitcoin

Bitcoin là tập hợp các khái niệm và công nghệ tạo thành nền tảng mạng lưới kỹ thuật số. Đơn vị tiền tệ được gọi là bitcoin được sử dụng để lưu trữ và truyền giá trị giữa những người tham gia mạng bitcoin. Người dùng bitcoin giao tiếp với nhau bằng giao thức bitcoin chủ yếu thông qua internet, mặc dù các mạng vận chuyển khác cũng có thể được sử dụng. Ngăn xếp giao thức bitcoin, có sẵn dưới dạng phần mềm mã nguồn mở, có thể chạy trên nhiều loại thiết bị điện toán, bao gồm cả máy tính xách tay và điện thoại thông minh, giúp công nghệ này có thể truy cập dễ dàng.

Người dùng có thể chuyển bitcoin qua mạng để thực hiện bất kỳ điều gì có thể thực hiện được với các loại tiền tệ thông thường, bao gồm mua và bán hàng hóa, gửi tiền cho mọi người hoặc tổ chức hoặc gia hạn tín dụng. Bitcoin có thể được mua, bán và đổi lấy các loại tiền tệ khác tại các sàn giao dịch tiền tệ chuyên biệt. Theo một nghĩa nào đó, Bitcoin là hình thức kiếm tiền hoàn hảo cho internet vì nó nhanh, an toàn và không biên giới.

Không giống như các loại tiền tệ truyền thống, bitcoin hoàn toàn là ảo. Không có đồng xu vật lý hoặc thậm chí là đồng tiền kỹ thuật số. Các đồng xu được ngụ ý trong các giao dịch chuyển giá trị từ người gửi sang người nhận. Người dùng Bitcoin sở hữu các khóa cho phép họ chứng minh quyền sở hữu bitcoin trong mạng Bitcoin. Với các khóa này, họ có thể ký các giao dịch để mở khóa giá trị và chi tiêu bằng cách chuyển nó cho chủ sở hữu mới. Các khóa thường được lưu trữ trong ví kỹ thuật số trên máy tính hoặc điện thoại thông minh của mỗi người dùng. Sở hữu chìa khóa có thể ký giao dịch là điều kiện tiên quyết duy nhất để chi tiêu bitcoin, đặt quyền kiểm soát hoàn toàn trong tay của mỗi người dùng.

Bitcoin là một hệ thống ngang hàng, phân tán. Như vậy, không có máy chủ hoặc điểm kiểm soát "trung tâm". Bitcoin, tức là các đơn vị bitcoin, được tạo ra thông qua một quá trình gọi là "khai thác", bao gồm việc cạnh tranh để tìm giải pháp cho một vấn đề toán học trong khi xử lý các giao dịch Bitcoin. Bất kỳ người tham gia nào trong mạng Bitcoin (nghĩa là bất kỳ ai sử dụng thiết bị chạy toàn bộ giao thức Bitcoin) đều

có thể hoạt động như một công cụ khai thác, sử dụng sức mạnh xử lý của máy tính để xác minh và ghi lại các giao dịch. Trung bình cứ sau 10 phút, một người khai thác Bitcoin có thể xác thực các giao dịch trong 10 phút qua và được thưởng bằng bitcoin hoàn toàn mới. Về cơ bản, khai thác Bitcoin phi tập trung hóa các chức năng phát hành và thanh toán tiền tệ của một ngân hàng trung ương và thay thế nhu cầu đối với bất kỳ ngân hàng trung ương nào.

Giao thức Bitcoin bao gồm các thuật toán tích hợp điều chỉnh chức năng khai thác trên mạng. Độ khó của nhiệm vụ xử lý mà những người khai thác phải thực hiện được điều chỉnh linh hoạt để trung bình cứ sau 10 phút lại có người thành công bất kể có bao nhiêu người khai thác (và bao nhiêu quá trình xử lý) đang cạnh tranh tại bất kỳ thời điểm nào. Giao thức này cũng giảm một nửa tốc độ tạo bitcoin mới sau mỗi 4 năm và giới hạn tổng số bitcoin sẽ được tạo ở mức tổng cố định chỉ dưới 21 triệu xu. Kết quả là số lượng bitcoin đang lưu hành theo sát một đường cong dễ dự đoán, đạt 21 triệu vào năm 2140. Do tỷ lệ phát hành bitcoin giảm dần, về lâu dài, đồng tiền Bitcoin sẽ giảm phát. Hơn nữa, bitcoin không thể bị lạm phát bằng cách "in".

Đằng sau hậu trường, Bitcoin cũng là tên của giao thức, mạng ngang hàng và đối mới điện toán phân tán. Đồng tiền bitcoin thực sự chỉ là ứng dụng đầu tiên của phát minh này. Bitcoin đại diện cho đỉnh cao của nhiều thập kỷ nghiên cứu về mật mã và hệ thống phân tán, đồng thời bao gồm bốn cải tiến chính được kết hợp với nhau trong một sự kết hợp độc đáo và mạnh mẽ. Bitcoin bao gồm:

Mạng ngang hàng phi tập trung (giao thức Bitcoin)

- Sổ cái giao dịch công khai (blockchain)
- Một bộ quy tắc để xác thực giao dịch độc lập và phát hành tiền tệ (quy tắc đồng thuận)
- Một cơ chế để đạt được sự đồng thuận phi tập trung toàn cầu trên chuỗi khối hợp lệ (thuật toán Proof-of-Work)

4.1.1.2 Kiến trúc của Bitcoin

Cấu trúc một khối

Một khối là một cấu trúc dữ liệu vùng chứa, nó tổng hợp các giao dịch để đưa vào nhật ký công khai, vào chuỗi khối. Khối được tạo thành từ một tiêu đề, chứa siêu

dữ liệu, theo sau là một danh sách dài các giao dịch - chiếm phần lớn kích thước của nó.

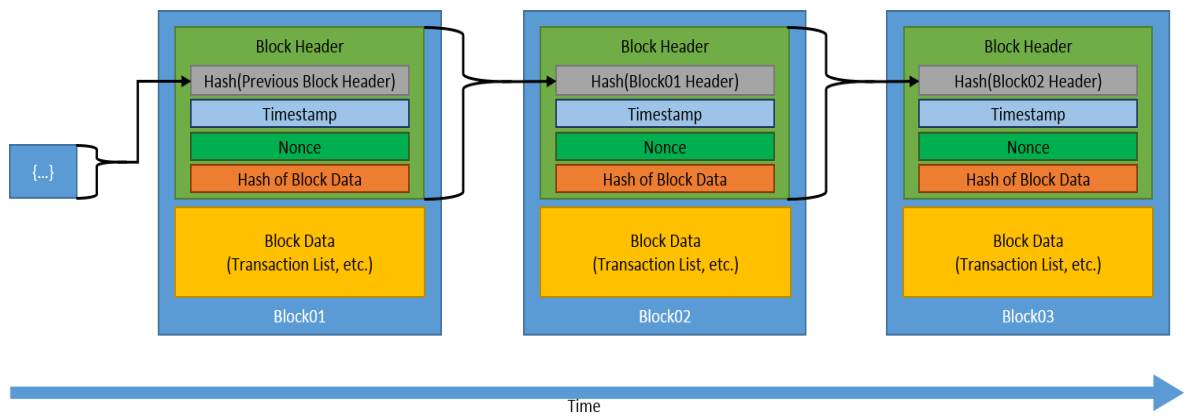
Về dung lượng, phần tiêu đề khối (block header) chiếm 80 byte, trong đó một giao dịch thông thường sẽ chiếm ít nhất 250byte và mỗi khối sẽ chứa hơn 500 giao dịch. Như vậy, mỗi khối hoàn chỉnh kèm theo toàn bộ lịch sử giao dịch sẽ có dung lượng lớn gấp 1000 lần so với tiêu đề khối.

Kích thước	Vùng	Mô tả
4 bytes	Kích thước khối	Kích thước của khối dựa theo trường này, tính bằng bytes;
80 bytes	Tiêu đề khối	Một số trường từ tiêu đề khối;
1-9 bytes (VarInt)	Bộ đếm giao dịch	Nắm bắt lượng giao dịch
Tuỳ biến	Các giao dịch	Nhập ký các giao dịch trong khối này

Bảng 4.1: Dung lượng các phần trong khối

Tiêu đề khối – Block header

Phần tiêu đề khối bao gồm ba bộ siêu dữ liệu khối. Đầu tiên là giá trị băm của tiêu đề khối trước đó, nhằm duy trì kết nối của khối này với chuỗi khối. Tiếp theo là một bộ dữ liệu bao gồm các giá trị sau: Dấu thời gian (timestamp), số nonce và độ khó để tạo ra khối. Cụ thể, dấu thời gian ghi lại thời điểm tạo khối, số nonce là giá trị duy nhất để xác định giữa các khối và độ khó càng thấp chứng tỏ khối này càng khó được tìm ra. Những giá trị này sẽ được đề cập chi tiết hơn ở phần luật đồng thuận Proof-of-Work. Cuối cùng, bộ siêu dữ liệu thứ ba là gốc merkle, có thể coi đây là một hàm băm nhằm tóm tắt tất cả các giao dịch trong khối.



Hình 4.1: Hình ảnh minh họa về cấu trúc của bitcoin

Kích thước	Trường	Mô tả
4 byte	Phiên bản	Gán nhãn phiên bản để theo dõi sự cập nhật của phần mềm hoặc giao thức
32 byte	Hàm băm khối trước	Tham chiếu đến hàm băm của khối trước đó trong chuỗi
32 byte	Gốc merkle	Giá trị băm của các giao dịch trong khối
4 byte	Dấu thời gian	Thời điểm khởi tạo gần chính xác của khối
4 byte	Độ khó	Độ khó của thuật toán Proof-of-Work cho khối này
4 byte	Nonce	Một số duy nhất dùng cho thuật toán PoW

Bảng 4.2: Dung lượng các phần trong tiêu đề khối

Mã định danh khối Giá trị băm tiêu đề khối và chiều cao khối

Mã định danh của một khối chính là hàm băm mật mã của nó: Một dấu vân tay số, được tạo bằng cách băm tiêu đề khối hai lần thông qua thuật toán SHA256. Kết quả của hàm băm 32 bytes được gọi là hàm băm khối nhưng chính xác hơn là hàm băm tiêu đề khối, bởi vì chỉ có tiêu đề khối được sử dụng để tính toán.

Ví dụ:

000000000019d6689c085ae165831e934ff763ae46a2a6c172b3f1b60a8ce26f là hàm băm khối của khối bitcoin đầu tiên từng được tạo. Băm khối xác định một khối duy nhất và rõ ràng và có thể được lấy độc lập bởi bất kỳ nút nào bằng cách băm tiêu đề khối.

Lưu ý rằng hàm băm khối không thực sự được đưa vào bên trong cấu trúc dữ liệu của khối, ngay cả khi khối được truyền trên mạng, cũng như khi nó được lưu trữ trên bộ lưu trữ liên tục của nút như một phần của chuỗi khối. Thay vào đó, hàm băm của khối được tính bởi mỗi nút khi khối được nhận từ mạng. Băm khối có thể được lưu trữ trong một bảng cơ sở dữ liệu riêng biệt như một phần của siêu dữ liệu của khối, để tạo điều kiện lập chỉ mục và truy xuất các khối từ đĩa nhanh hơn.

Cách thứ hai để xác định một khối là theo vị trí của nó trong chuỗi khối, được gọi là chiều cao khối. Khối đầu tiên từng được tạo ở độ cao khối 0 (không) và là cùng một khối đã được tham chiếu trước đó bởi hàm băm khối sau

000000000019d6689c085ae165831e934ff763ae46a2a6c172b3f1b60a8ce26f.

Do đó, một khối có thể được xác định theo hai cách: bằng cách tham chiếu hàm băm khối hoặc bằng cách tham chiếu chiều cao khối. Mỗi khối nối tiếp theo được thêm vào “trên cùng” của khối đầu tiên là một vị trí “cao hơn” trong chuỗi khối, giống như các hộp được xếp chồng lên nhau. Chiều cao khối vào ngày 1 tháng 1 năm 2017 là khoảng 446.000, nghĩa là có 446.000 khối được xếp chồng lên nhau trên khối đầu tiên được tạo vào tháng 1 năm 2009.

Không giống như hàm băm khối, chiều cao khối không phải là mã định danh duy nhất. Mặc dù một khối duy nhất sẽ luôn có chiều cao khối cụ thể và bất biến, nhưng chưa chắc về điều ngược lại - chiều cao khối không phải lúc nào cũng xác định một khối duy nhất. Hai hoặc nhiều khối có thể có cùng chiều cao khối, cùng cạnh tranh cho cùng một vị trí trong chuỗi khối. Chiều cao khối cũng không phải là một phần của cấu trúc dữ liệu khối; nó không được lưu trữ trong khối. Cụ thể, mỗi nút tự động xác định vị trí (chiều cao) của một khối trong chuỗi khối khi nó được nhận từ mạng bitcoin. Chiều cao khối cũng có thể được lưu trữ dưới dạng siêu dữ liệu trong bảng cơ sở dữ liệu được lập chỉ mục để truy xuất nhanh hơn.

Giá trị băm của khối luôn xác định duy nhất một khối. Một khối cũng luôn có một chiều cao cụ thể. Tuy nhiên, không phải lúc nào chiều cao khối cụ thể cũng có thể

xác định một khối duy nhất. Thay vào đó, hai hoặc nhiều khối có thể cạnh tranh cho một vị trí duy nhất trong chuỗi khối.

Khối khởi nguyên

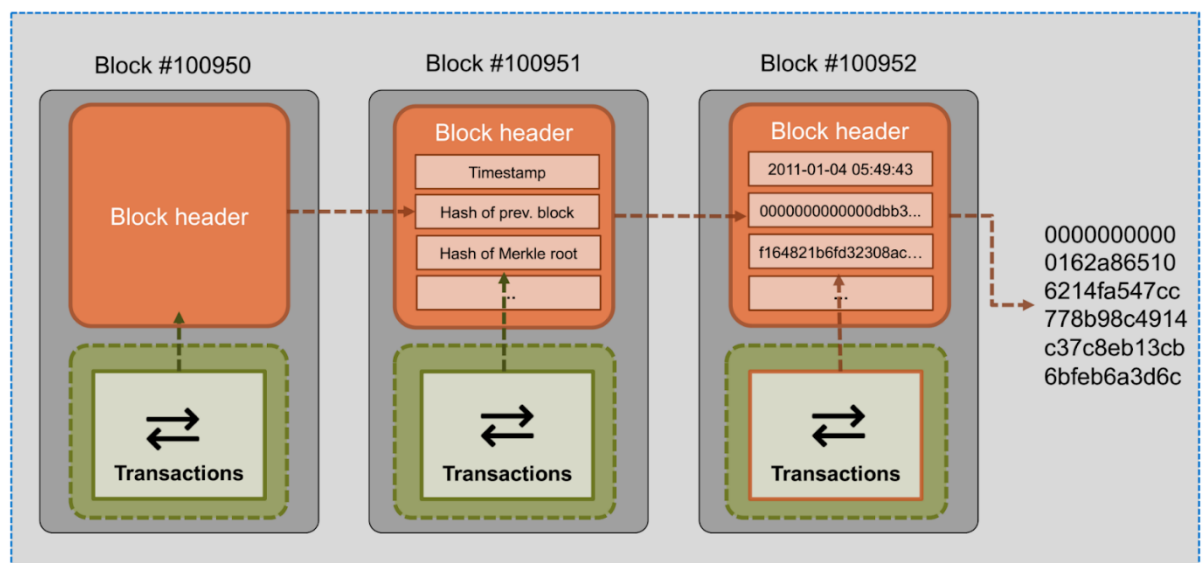
Khối đầu tiên trong chuỗi khối được gọi là khối khởi nguồn (genesis) và được tạo ra vào năm 2009. Nó là tổ tiên chung của tất cả các khối trong chuỗi khối: nếu bạn bắt đầu ở bất kỳ khối nào và đi theo chuỗi ngược thời gian, cuối cùng bạn sẽ đến đích tại khối genesis.

Mỗi nút luôn bắt đầu với một chuỗi khối bao gồm ít nhất một khối - bởi khối gốc đã được mã hóa tĩnh trong phần mềm máy khách bitcoin, do đó không thể thay đổi được. Mọi nút luôn “biết” hàm băm và cấu trúc của khối gốc, dấu thời gian đánh dấu thời điểm khối được tạo và thậm chí là từng giao dịch bên trong. Do đó, tất cả các nút đều có điểm khởi đầu cho chuỗi khối, một “gốc” an toàn để từ đó xây dựng một chuỗi khối đáng tin cậy.

Thông tin thêm về Genesis:

- Được khai thác vào 2009-01-03 18:15:05
- Phần “Hash của khối trước đó” là 0
- Chỉ chứa giao dịch về phần thưởng khai thác được: 50 BTC đầu tiên không bao giờ chi tiêu

Bitcoin Blockchain



Hình 4.2: Cấu trúc bitcoin

4.1.1.3 Giao dịch trong Bitcoin

Giao dịch là phần quan trọng nhất của hệ thống Bitcoin. Mọi thứ khác trong bitcoin được thiết kế để đảm bảo rằng các giao dịch có thể được tạo, lan truyền trên mạng, được xác thực và cuối cùng được thêm vào sổ cái giao dịch toàn cầu (Blockchain).

Giao dịch là cấu trúc dữ liệu mã hóa việc chuyển giao giá trị giữa những người tham gia trong hệ thống Bitcoin.

Mỗi giao dịch Bitcoin bao gồm một người gửi, một người nhận và một số lượng Bitcoin được trao đổi. Khi một giao dịch được tạo ra, nó được phát sóng đến mạng lưới Bitcoin để được xác nhận bởi các nút trong mạng.

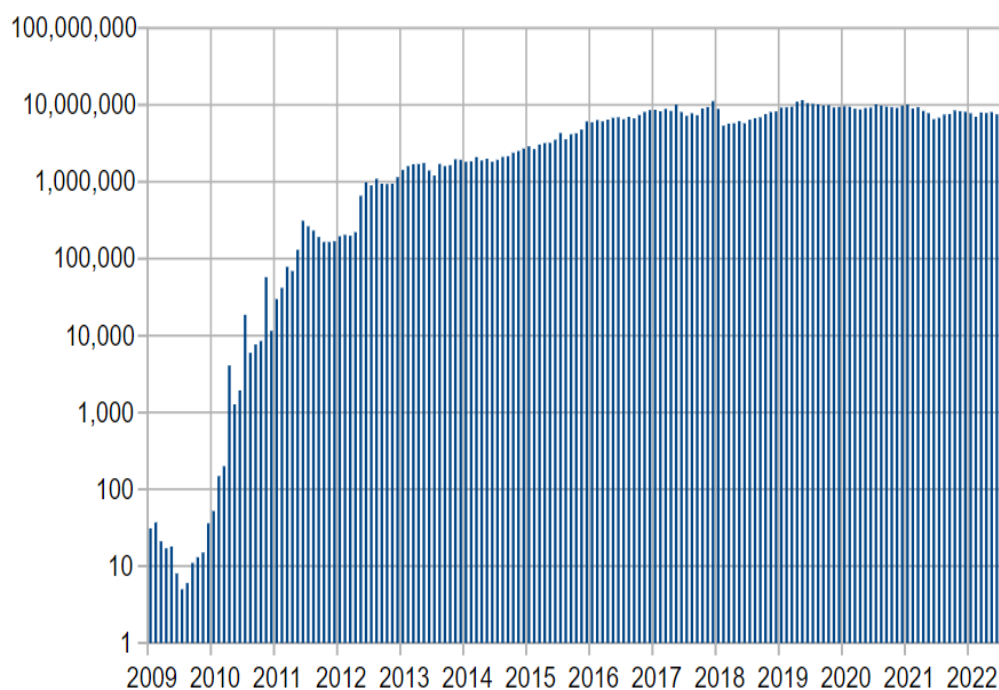
Để xác nhận một giao dịch, các nút trên mạng sẽ sử dụng các phép toán toán học phức tạp để xác minh tính hợp lệ của giao dịch. Khi giao dịch được xác nhận, nó được đưa vào một khối mới trên blockchain và trở thành không thể thay đổi.

4.1.2 Thực tế và thách thức của Bitcoin

4.1.2.1 Các công nghệ mở rộng mạng lưới trong Bitcoin

Vấn đề khả năng mở rộng trong mạng Bitcoin

Vấn đề về khả năng mở rộng của Bitcoin được liên quan đến khả năng giới hạn của mạng Bitcoin trong việc xử lý lượng lớn dữ liệu giao dịch trên nền tảng của nó trong thời gian ngắn. Vấn đề này liên quan đến việc các bản ghi (gọi là khối) trong chuỗi khối Bitcoin có kích thước và tần suất giới hạn.



Hình 4.3: Số lượng giao dịch mỗi tháng, theo the logarithmic scale

Thông lượng tối đa là tốc độ tối đa mà Blockchain có thể xác nhận các giao dịch. Hiện nay, tốc độ tối đa của Bitcoin là 3,3-7 giao dịch/giây. Con số này bị hạn chế bởi kích thước khối tối đa và thời gian giữa các khối.

Các khối của Bitcoin chứa các giao dịch trên mạng Bitcoin. Khả năng xử lý giao dịch trên chuỗi khối của mạng Bitcoin được giới hạn bởi thời gian trung bình tạo khối là 10 phút và giới hạn kích thước khối ban đầu là 1 megabyte. Cả hai yếu tố này cùng gây ra giới hạn truyền thông của mạng. Khả năng xử lý giao dịch tối đa được ước tính sử dụng kích thước giao dịch trung bình là từ 3,3 đến 7 giao dịch mỗi giây. Hiện có nhiều giải pháp đã được đề xuất và triển khai để giải quyết vấn đề này.

- Khi giao dịch được xác minh trên mạng Bitcoin, lý thuyết mỗi nút trong hệ thống phi tập trung phải xác minh mỗi giao dịch.
- Mạng Bitcoin chỉ có thể xử lý một số lượng giao dịch nhất định trong một khung thời gian nhất định, chẳng hạn như trên mỗi khối.
- Về cơ bản, tính mở rộng của mạng đến khả năng xử lý một lượng lớn các giao dịch.
- Trong ngữ cảnh chi tiết hơn, các yếu tố tính mở rộng bao gồm khả năng thông lượng, thời gian giao dịch, độ trễ và bảo mật.

Có một số công nghệ được đề xuất và triển khai để mở rộng mạng Bitcoin. Một số trong số họ là:

- Segregated Witness (SegWit): một soft fork được triển khai vào năm 2017 để tách dữ liệu chữ ký giao dịch khỏi dữ liệu giao dịch, cho phép đưa nhiều giao dịch hơn vào một khối.
- Lightning Network: một giải pháp mở rộng lớp 2 cho phép giao dịch ngoại tuyến nhanh và rẻ bằng cách tạo các kênh thanh toán giữa những người dùng.
- Schnorr signatures: một bản nâng cấp được đề xuất cho thuật toán chữ ký có thể giảm quy mô giao dịch và cho phép nhiều giao dịch hơn được đưa vào một khối.
- Drivechain: một công nghệ sidechain cho phép linh hoạt hơn trong việc mở rộng quy mô bằng cách cho phép tạo các chuỗi khối mới với các quy tắc và tham số của riêng chúng.
- MimbleWimble: một giao thức tập trung vào quyền riêng tư có thể cho phép các giao dịch riêng tư và hiệu quả hơn trên mạng Bitcoin bằng cách xóa dữ liệu không cần thiết.

Light Network

Lightning Network là một giao thức thanh toán hoạt động trên blockchain của Bitcoin. Đó là một mạng lưới các nút phi tập trung cho phép gửi một số lượng lớn các giao dịch (lên đến 1 triệu mỗi giây) cực kỳ nhanh chóng với một mức phí không đáng kể.

Lightning Network lấy các giao dịch ra khỏi blockchain chính và giúp chúng dễ mở rộng và rất rẻ tiền, đối đầu trực tiếp với VISA, MasterCard Lightning Network đạt được điều đó bằng cách thiết lập các kênh thanh toán giữa cặp người dùng thông qua đó các bên có thể thực hiện hoặc nhận thanh toán từ nhau.

Khác với mạng chính Bitcoin, nơi mỗi giao dịch phải được xác minh, trên Lightning Network hai bên có thể gửi và nhận tiền không ngừng với nhau, và chỉ việc mở và đóng các kênh thanh toán như vậy mới được ghi lại trên blockchain chính.

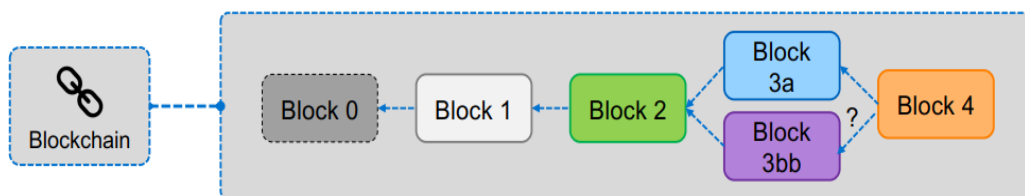
4.1.2.2 Các tấn công vào mạng lưới Bitcoin

Double Spending

Xem xét ví dụ:

Lấy ví dụ, Alice đã tạo một giao dịch để gửi một số tiền Bitcoin cho Bob để mua một tệp nhạc. Một nút an toàn trên mạng nhìn thấy giao dịch này và đưa nó vào một khối. Bob cũng thấy giao dịch này và đã gửi tệp nhạc cho Alice.

Nhưng nếu Alice muốn lừa đảo Bob, cô ấy có thể tạo một giao dịch khác với cùng một số Bitcoin và gửi nó đến một địa chỉ khác. Nếu giao dịch này được xác nhận trước khi giao dịch ban đầu của Alice đến Bob, thì số Bitcoin đã được giao dịch hai lần: một lần cho giao dịch ban đầu của Alice và một lần cho giao dịch mới của cô ấy.



Hình 4.4: Mô hình minh họa blockchain

Hãy xem xét blockchain cơ bản dưới đây:

- Khối xanh (khối 3a) chứa giao dịch hợp lệ của Alice đến Bob.
- Sau khi một nút “an toàn” đề xuất khối này, Alice được chọn để đề xuất khối mới.
- Alice có thể làm gì?
 - Tùy chọn 1: Xây dựng trên khối 3a, cô ấy chấp nhận thực tế rằng giao dịch đã xảy ra. Điều này không phải là điều cô ấy muốn, cô ấy muốn double spend (giao dịch hai lần)!
 - Tùy chọn 2: Xây dựng trên khối 2 một khối mới 3b (màu tím), không chứa giao dịch mà cô ấy đã gửi cho Bob, nhưng là một giao dịch chi tiêu nhưng số tiền đó (số tiền gửi cho Bob) gửi cho chính mình. Điều này được mô tả là forking (phân nhánh).

Điều này có nghĩa là có thể giao dịch 2 lần 1 lúc?

Không, vì không thể tạo ra một khối hoặc blockchain hợp lệ với hai giao dịch sử dụng cùng một UTXO. Những gì xảy ra là tạo ra hai "thực tại" khác nhau. Khối 3a

(màu xanh) tạo ra một thực tại trong đó Bob được thanh toán và khối 3b (màu tím) tạo ra một thực tại khác trong đó Alice tự gửi tiền cho chính mình.

Xung đột này được giải quyết như thế nào?

Khi một nút trong mạng đề xuất một khối mới, nút đó phải chọn khối gốc để tạo khối mới. Vì mỗi khối trong mạng blockchain được liên kết với khối trước đó, các khối càng đi xa khỏi khối gốc sẽ càng ít được chấp nhận bởi mạng. Do đó, nút đề xuất khối mới sẽ phải chọn khối trên chuỗi dài nhất, có nghĩa là chuỗi khối mà có nhiều khối hơn so với các chuỗi khác.

Những khối không được chọn sẽ trở thành "mồ côi", không còn được kết nối với chuỗi khối dài nhất. Không còn liên quan đến mạng nữa.

Khi nào cuộc tấn công thành công?

Nếu Alice thuyết phục mạng rằng khối mà cô ấy tạo ra là khối hợp lệ và nên được thêm vào chuỗi blockchain dài nhất.

Từ ví dụ trên, chúng ta biết rằng khối màu xanh là khối hợp lệ. Tuy nhiên, nếu Alice cố gắng thêm khối của mình (khối màu tím) vào chuỗi blockchain dài nhất và thuyết phục các nút trong mạng rằng khối của cô ấy là khối hợp lệ, thì cuộc tấn công sẽ thành công.

a. Giới thiệu

Mạng Bitcoin là một hệ thống tiền điện tử phi tập trung, cho phép các giao dịch được thực hiện mà không cần trung gian. Tuy nhiên, hệ thống này cũng có thể trở thành mục tiêu của các cuộc tấn công mạng, trong đó một trong những cuộc tấn công phổ biến nhất là Double Spending.

Double Spending là một kỹ thuật tấn công trong đó kẻ tấn công cố gắng sử dụng cùng một đồng Bitcoin để thực hiện nhiều giao dịch khác nhau mà không phải trả bất kỳ chi phí nào. Khi kẻ tấn công thực hiện Double Spending, họ đang cố gắng phá vỡ tính toàn vẹn của hệ thống Bitcoin.

b. Cách thức hoạt động của Double Spending

Để thực hiện Double Spending, kẻ tấn công phải thực hiện hai giao dịch Bitcoin khác nhau cùng một lúc. Trong giao dịch đầu tiên, họ gửi một số lượng Bitcoin đến một địa chỉ Bitcoin bình thường. Tuy nhiên, trước khi giao dịch này được xác nhận và được lưu trữ trong blockchain, kẻ tấn công sẽ thực hiện một giao dịch khác với cùng một số lượng Bitcoin nhưng gửi đến một địa chỉ khác.

Nếu kẻ tấn công có thể khai thác thành công một khối mới trong blockchain, họ sẽ thêm giao dịch của họ vào khối này và phát hành nó cho mạng. Nếu giao dịch thứ hai được xác nhận trước giao dịch đầu tiên, kẻ tấn công sẽ có thể hoàn tất Double Spending và có được quyền sử dụng số Bitcoin đó hai lần.

c. Hậu quả của Double Spending

- Mất niềm tin: Một cuộc tấn công double spending thành công có thể làm giảm niềm tin của người dùng vào hệ thống tiền điện tử. Nếu hệ thống không thể bảo vệ chống lại double spending, người dùng có thể mất niềm tin vào khả năng của đồng tiền để hoạt động như một phương tiện trao đổi an toàn và đáng tin cậy.
- Thiệt hại tài chính: Một cuộc tấn công double spending có thể gây ra thiệt hại tài chính cho các bên bị ảnh hưởng, chẳng hạn như các nhà bán lẻ hoặc nhà cung cấp dịch vụ. Nếu kẻ tấn công quản lý để sử dụng cùng một loại tiền điện tử cho nhiều giao dịch, người nhận được tiền "double-spent" có thể chịu mất mát vì tiền chỉ được công nhận là hợp lệ cho một giao dịch.
- Giảm sự lựa chọn: Do thiệt hại tài chính tiềm ẩn và mất niềm tin gây ra bởi cuộc tấn công double spending, một loại tiền điện tử có thể đối mặt với tỷ lệ lựa chọn giảm. Cả người dùng và nhà bán lẻ có thể do dự tham gia vào một hệ thống dễ bị tấn công như vậy, làm chậm sự phát triển của hệ sinh thái tiền điện tử.
- Tổn hại danh tiếng: Danh tiếng của đồng tiền kỹ thuật số và các nhà phát triển của nó có thể bị tổn thương nếu một cuộc tấn công chi tiêu kép xảy ra. Điều này có thể làm khó cho đội ngũ phát triển thu hút nhà đầu tư hoặc người dùng mới, hoặc hợp tác với các thực thể khác trong không gian tiền điện tử.
- Giảm giá trị thị trường: Nếu một cuộc tấn công chi tiêu kép được công khai rộng rãi hoặc ảnh hưởng đáng kể đến hoạt động của đồng tiền kỹ thuật số, nó có thể dẫn đến giảm giá trị thị trường của đồng tiền, vì nhà đầu tư và người dùng có thể mất lòng tin vào tính ổn định và an ninh của đồng tiền.

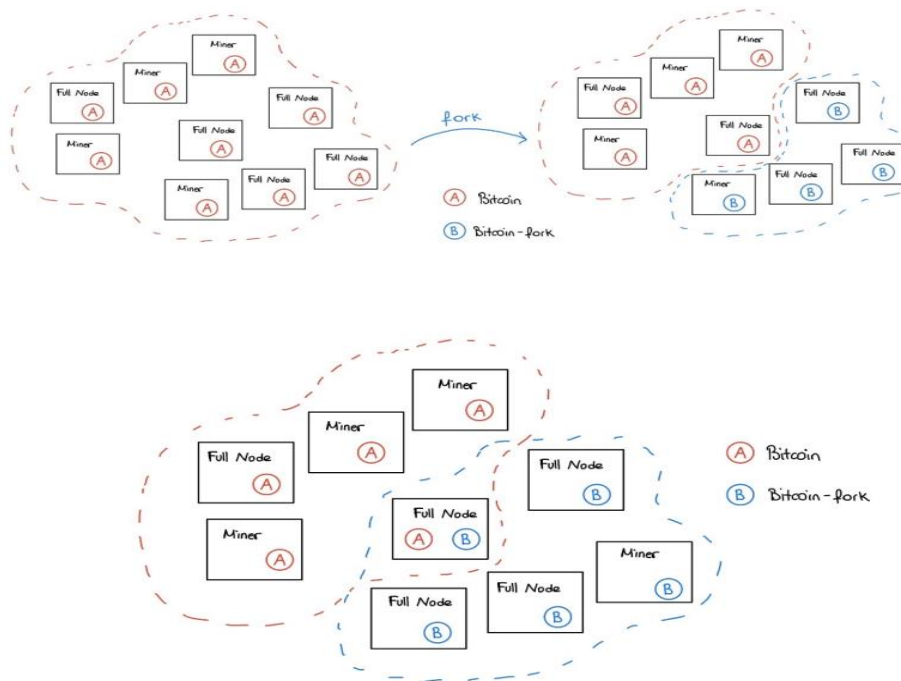
d. Phương pháp ngăn chặn

- Sử dụng Nonce để chống **Replay Attacks**: Nonce là một giá trị mật mã khó phải được băm trước khi có thể khai thác một khối. Giá trị của nonces chỉ có thể được sử dụng một lần. Chúng giúp bảo mật chuỗi khối trước các cuộc tấn công lặp lại vì giá trị của chúng không thể bị trùng lặp. Nonces duy trì tính toàn vẹn của mỗi khối.

- **Timestamps:** Mỗi giao dịch thành công có một dấu thời gian. Dấu thời gian chứng minh rằng một khối cụ thể đã được thêm vào chuỗi tại một thời điểm cụ thể. Một khối trở nên không thể đảo ngược thời điểm nó được đánh dấu thời gian. Bất kỳ giao dịch xung đột nào cố double spending tiền điện tử trong khối được đánh dấu thời gian mà người dùng thông thường đều không thành công.
- **Xác nhận giao dịch:** Một cách đơn giản để ngăn chặn Double Spending là yêu cầu xác nhận từ một số người dùng khác trước khi giao dịch được hoàn tất. Trong Bitcoin, các giao dịch được xác nhận thông qua quá trình khai thác mỏ và xác thực giao dịch, khi một giao dịch được xác nhận, nó được thêm vào blockchain và trở thành không thể thay đổi.
- **Giám sát giao dịch:** Các hệ thống thanh toán trực tuyến cũng có thể giám sát các giao dịch và phát hiện Double Spending thông qua các thuật toán giám sát.
- **Điều chỉnh lại thời gian chờ xác nhận:** Trong Bitcoin, thời gian chờ xác nhận giao dịch có thể được điều chỉnh để tăng tính an toàn, ví dụ như tăng thời gian chờ xác nhận trước khi cho phép các giao dịch tiếp theo

Replay Attack

Xem xét ví dụ sau:



Hình 4.5: Relay attack

Giả sử Alice sở hữu một số lượng Bitcoin.

- Tuy nhiên, blockchain sắp trải qua một cuộc phân nhánh cứng (hard fork) sẽ chia blockchain thành hai phần: phiên bản cũ và phiên bản mới.
- Sau khi phân nhánh xảy ra, Alice sở hữu số tiền tương tự trên cả hai phiên bản và cô quyết định gửi 5 Bitcoins cho Bob trên phiên bản cũ để trả nợ.
- Giao dịch cuối cùng được bao gồm trong một khối trên phiên bản cũ và Bob nhận được số tiền của mình.
- Tuy nhiên, Bob nhận ra rằng anh ta có thể nhận được thêm tiền bằng cách nhân bản giao dịch của Alice trên phiên bản mới.
- Vì địa chỉ không thay đổi, việc "lặp lại" giao dịch này được xác nhận bởi các thợ đào trên phiên bản mới.
- Với điều này, Bob đã thành công trong việc thực hiện một cuộc tấn công tái sử dụng (replay attack).
- Lưu ý: Người tham gia vào mạng sau khi phân nhánh cứng đã xảy ra không dễ bị tấn công tái sử dụng vì địa chỉ của họ không có lịch sử giao dịch trên bất kỳ phiên bản nào của blockchain.

a. Giới thiệu

Là một loại cuộc tấn công trong đó kẻ tấn công ghi lại một giao dịch hợp lệ và sau đó tái sử dụng nó để thực hiện các giao dịch giả mạo.

b. Cách thức hoạt động

Replay Attack có thể xảy ra khi các chuỗi khối đang thay đổi hoặc nâng cấp các giao thức của chúng, một quá trình được gọi là hard fork. Trong khi hard fork đang diễn ra, cả hai phiên bản của giao thức vẫn tiếp tục được thực hiện, điều đó có nghĩa là bất kỳ giao dịch nào được coi là hợp lệ trên phiên bản trước cũng sẽ hợp lệ trên sổ cái mới.

Khi tin tặc thực hiện một cuộc tấn công lặp lại, chúng có thể sử dụng hard fork để mô phỏng các giao dịch trên phiên bản trước, sau đó, số tiền tương tự có thể được chuyển vào ví thêm một lần nữa. Các cuộc tấn công lặp lại có thể được thực hiện vô số lần trừ khi mạng dừng lại.

c. Hậu quả

- Truy cập trái phép: Trong cuộc tấn công phát lại, kẻ tấn công có thể truy cập trái phép vào hệ thống hoặc mạng bằng cách gửi lại một thông điệp xác thực hợp lệ

được chụp trước đó. Điều này có thể đe dọa an ninh và tính toàn vẹn của hệ thống và cho phép kẻ tấn công truy cập vào dữ liệu nhạy cảm hoặc thực hiện các hoạt động độc hại.

- Trộm danh tính: Kẻ tấn công có thể gửi một thông điệp đã được phát lại như là đã được gửi bởi người dùng hợp lệ, dẫn đến việc trộm cắp danh tính. Điều này có thể dẫn đến mất tiền, hư hại danh tiếng và mất thông tin cá nhân cho nạn nhân.
- Chi phối dữ liệu: Kẻ tấn công có thể chi phối thông tin và dữ liệu nhạy cảm bằng cách phát lại các truyền thông dữ liệu, làm cho người nhận khó phân biệt giữa các thông điệp chính thức và gian lận.
- Mất tiền: Cuộc tấn công phát lại có thể dẫn đến mất tiền cho các doanh nghiệp và cá nhân, vì kẻ tấn công có thể chi phối các giao dịch tài chính hoặc thực hiện các giao dịch trái phép bằng cách gửi lại các thông điệp đã được chụp trước đó.
- Sự gián đoạn dịch vụ: Các tin nhắn được gửi lại, đặc biệt là ở số lượng lớn, có thể làm quá tải hệ thống và dẫn đến gián đoạn dịch vụ hoặc thậm chí là cuộc tấn công từ chối dịch vụ

d. Phương pháp ngăn chặn Replay Attack

- Cách đầu tiên để ngăn chặn các cuộc tấn công phát lại là gắn dấu thời gian hoặc số thứ tự cho mỗi tin nhắn đã gửi. Điều này sẽ cho phép người nhận loại bỏ bất kỳ tin nhắn nào có dấu thời gian hoặc số thứ tự lặp lại.
- Một phương pháp hay nhất khác là sử dụng chữ ký số. Chữ ký số cho phép người nhận xác thực người gửi.
- Một thực tiễn tốt nhất khác để giảm thiểu các cuộc tấn công phát lại là sử dụng các khóa phiên ngẫu nhiên. Các khóa phiên ngẫu nhiên thường cụ thể theo thời gian. Do đó, các khóa này sẽ thay đổi theo thời gian, khiến kẻ tấn công mạng khó đánh lừa được người nhận.
- Mật khẩu một lần là một phương pháp hay nhất tuyệt vời khác cũng có thể được sử dụng để giảm thiểu các cuộc tấn công lặp lại. Mật khẩu dùng một lần là một chuỗi ký tự gồm chữ và số được tạo tự động để xác thực người dùng chỉ cho một giao dịch hoặc phiên đăng nhập. Mật khẩu một lần an toàn hơn nhiều so với mật khẩu thông thường.

51% Attack

a. Giới thiệu

51% Attack là một dạng tấn công đối với mạng blockchain. Khi một nhóm tấn công chiếm được hơn 50% sức mạnh tính toán của một mạng blockchain, họ có thể kiểm soát toàn bộ quá trình giao dịch trên mạng đó. Điều này có nghĩa là họ có thể thực hiện các giao dịch giả mạo, đánh cắp tiền của người dùng và lợi dụng các thông tin cá nhân. Ngoài ra, 51% Attack còn có thể phá vỡ tính toàn vẹn của mạng blockchain và làm giảm độ tin cậy của nó.

b. Cơ chế hoạt động của 51% Attack

51% Attack là kết quả của sự tập trung quá mức của sức mạnh tính toán trên mạng blockchain. Khi một nhóm tấn công sở hữu hơn 50% sức mạnh tính toán của mạng đó, họ có thể thực hiện các giao dịch giả mạo trên mạng đó. Điều này có thể đánh cắp tiền của người dùng bằng cách thực hiện các giao dịch chuyển tiền không hợp lệ hoặc lặp lại các giao dịch đã thực hiện trước đó để chiếm lấy lợi nhuận.

Họ cũng có thể ngăn chặn các giao dịch của người dùng bằng cách không bao gồm chúng vào các khối mới trong chuỗi khối của mạng đó. Điều này có thể gây ra sự phân cực trong cộng đồng của mạng blockchain bị tấn công, khi một số người dùng chấp nhận các giao dịch giả mạo và khối mới được thêm vào chuỗi khối, trong khi các người dùng khác không chấp nhận và sẽ không sử dụng các giao dịch và khối này.

c. Hậu quả

Khi cuộc tấn công này được thực hiện một số hậu quả có thể bao gồm:

- Đánh cắp tiền của người dùng: Những kẻ tấn công có thể thực hiện các giao dịch giả mạo trên mạng đó để đánh cắp tiền của người dùng. Họ cũng có thể lợi dụng thông tin cá nhân của người dùng và thực hiện các hành động xấu khác.
- Phá vỡ tính toàn vẹn của mạng blockchain: Nếu một nhóm tấn công chiếm được hơn 50% sức mạnh tính toán của mạng blockchain, họ có thể phá vỡ tính toàn vẹn của mạng đó bằng cách thay đổi thông tin trong các khối trước đó hoặc ngăn chặn các giao dịch mới được thêm vào chuỗi khối.
- Giảm độ tin cậy của mạng blockchain: Nếu một mạng blockchain bị tấn công bởi 51% Attack, điều này sẽ làm giảm độ tin cậy của mạng đó và khiến người dùng mất niềm tin vào tính bảo mật và độ tin cậy của nó.

- Gây ra sự phân cực trong cộng đồng: Nếu một nhóm tấn công thực hiện 51% Attack trên một mạng blockchain, điều này có thể gây ra sự phân cực trong cộng đồng của mạng đó. Một số người dùng có thể chấp nhận các giao dịch giả mạo và khối mới được thêm vào chuỗi khối, trong khi các người dùng khác không chấp nhận và sẽ không sử dụng các giao dịch và khối này. Điều này có thể gây ra sự khác biệt và xung đột trong cộng đồng và ảnh hưởng đến sự phát triển của mạng blockchain.

d. Các cách ngăn chặn cuộc tấn công 51%

Giới hạn 50% cho một người khai thác

Chuỗi khối phải đảm bảo rằng không có công cụ khai thác hoặc nhóm công cụ khai thác nào kiểm soát hơn 50% sức mạnh băm. Sẽ không thể để một người khai thác hoặc một nhóm tấn công mạng bằng cách xây dựng chuỗi khối được xác thực lâu nhất. Để thực hiện được cuộc tấn công, điều đó có nghĩa là kẻ tấn công phải sở hữu phần cứng mạnh mẽ và yêu cầu năng lượng cực lớn. Ngoài ra, kẻ tấn công có thể cần may mắn vì quá trình khai thác sẽ là ngẫu nhiên.

Một ví dụ điển hình là Bitcoin, nơi mạng lưới và tỷ lệ băm của nó đủ lớn và phức tạp để trở thành khoản đầu tư ban đầu đáng kể cho kẻ tấn công thuê thiết bị khai thác. Mặt khác, Ethereum Classic dễ bị tấn công hơn vì tỷ lệ băm tổng thể của nó tương đối nhỏ so với Bitcoin.

Sử dụng Proof of Stake

Một người khai thác duy nhất có thể trở thành người chơi đa số trong một mạng chuỗi khối nhỏ. Tất cả các mạng blockchain sử dụng PoW đều có chính sách rằng các thợ đào phải nâng cấp thiết bị của họ thường xuyên. Việc không làm như vậy có thể dẫn đến việc họ không nhận được phần thưởng khối và họ sẽ bị tụt lại phía sau những người khai thác khác trong mạng.

Để tránh nguy cơ bị tấn công 51%, chuỗi khối có thể sử dụng Proof of Stake (PoS), đây là một sự đồng thuận an toàn hơn PoW. Trong hầu hết các trường hợp, các ưu đãi PoS được kiểm soát bởi hầu hết những người dùng giàu có không có khả năng thực hiện cuộc tấn công. Tuy nhiên, các chuỗi khối đã chuyển từ cấu trúc này và chúng thích các lựa chọn thay thế phi tập trung hơn như Chứng minh cổ phần được ủy quyền (DPoS).

Cộng đồng mạng mạnh mẽ

Khi sử dụng PoS hoặc DPoS, người dùng có mức cổ phần tối thiểu trong mạng được bình chọn là người xác thực khối. Các trình xác nhận được cộng đồng bình chọn. Trong trường hợp thông đồng để xâm phạm mạng, họ sẽ bị cộng đồng ném ra khỏi mạng.

Cách tiếp cận này ngăn chặn sự xuất hiện của một cuộc tấn công 51%. Nó cũng hiệu quả trong việc tránh chi tiêu gấp đôi vì các quy tắc dành cho trình xác thực độc hại được mã hóa vào chuỗi khối

4.1.2.3 Các hạn chế và thách thức của Bitcoin

Hạn chế

- Mặc dù Bitcoin được coi là một công nghệ tiên tiến và có nhiều ưu điểm, nhưng nó cũng có một số hạn chế, bao gồm:
- Khả năng mở rộng hạn chế: Bitcoin có khả năng xử lý một số giao dịch trong một khoảng thời gian nhất định. Điều này có nghĩa là khi số lượng người dùng và giao dịch tăng lên, thì việc xử lý các giao dịch sẽ trở nên chậm hơn và có thể tăng chi phí.
- Khả năng đào Bitcoin càng ngày càng khó: Một trong những điều hấp dẫn của Bitcoin là việc đào tiền ảo này để tạo ra Bitcoin mới. Tuy nhiên, quá trình đào Bitcoin ngày càng khó khăn và tốn kém hơn. Điều này làm cho việc đào Bitcoin trở nên khó khăn hơn đối với các thợ đào Bitcoin.
- Sự không ổn định về giá: Giá Bitcoin thay đổi liên tục và rất khó để dự đoán. Điều này làm cho việc sử dụng Bitcoin như một phương tiện thanh toán không ổn định và có thể gây ra rủi ro cho các nhà đầu tư.
- An ninh còn đang trong giai đoạn phát triển: Mặc dù các giao dịch Bitcoin được mã hóa và an toàn, nhưng việc bảo mật hệ thống Bitcoin vẫn còn đang trong giai đoạn phát triển. Các vụ tấn công và vi phạm bảo mật đã xảy ra trong quá khứ và có thể xảy ra trong tương lai.
- Sự phụ thuộc vào mạng lưới internet: Bitcoin hoạt động trên mạng lưới internet, do đó nó phụ thuộc vào việc có kết nối internet ổn định để thực hiện các giao dịch. Nếu mạng lưới internet gặp sự cố hoặc bị tấn công, thì sẽ ảnh hưởng đến hoạt động của Bitcoin.

- Tiêu thụ điện năng: Quá trình đào Bitcoin cần sử dụng rất nhiều năng lượng điện. Việc này không chỉ làm tăng chi phí cho việc đào Bitcoin mà còn gây ra tác động tiêu cực đến môi trường vì phải sử dụng các nguồn năng lượng không thân thiện với môi trường.
- Tốc độ giao dịch chậm: Việc xác nhận một giao dịch Bitcoin có thể mất từ vài phút đến vài giờ. Điều này có thể làm chậm quá trình thanh toán và giao dịch.
- Phí giao dịch cao: Bitcoin yêu cầu người dùng trả phí giao dịch cho các thợ đào để xác nhận giao dịch. Các khoản phí này có thể rất cao đối với các giao dịch lớn.
- Khả năng lạm dụng: Do Bitcoin không được quản lý hoặc kiểm soát bởi bất kỳ tổ chức nào, nó có thể được sử dụng cho các hoạt động phi pháp hoặc bất hợp pháp.
- Không được chấp nhận rộng rãi: Mặc dù Bitcoin đang được chấp nhận bởi một số doanh nghiệp và tổ chức, nhưng nó vẫn chưa được chấp nhận rộng rãi như tiền tệ truyền thống.
- Không có sự bảo đảm: Bitcoin không được bảo đảm bởi bất kỳ tổ chức tài chính nào, điều này có nghĩa là nếu bạn mất khóa riêng tư của mình, bạn không thể lấy lại tiền của mình.
- Khó khăn trong việc sửa đổi: Bitcoin là một nền tảng phần mềm mã nguồn mở, nghĩa là không có một tổ chức nào kiểm soát và sửa đổi mã nguồn. Điều này có thể tạo ra khó khăn trong việc thực hiện các sửa đổi cần thiết để cải thiện tính năng hoặc sửa lỗi trong hệ thống.
- Tiềm ẩn nguy cơ phân mảnh: Bitcoin là một mạng lưới phân cấp, có nghĩa là nó phụ thuộc vào các nút và thợ đào đang tham gia vào mạng. Nếu có quá ít nút hoặc thợ đào tham gia vào mạng, thì nó có thể dẫn đến một sự phân mảnh trong mạng lưới, gây ảnh hưởng đến tính toàn vẹn và an ninh của hệ thống.
- Không thể hoàn toàn ẩn danh: Mặc dù các giao dịch Bitcoin không tiết lộ thông tin cá nhân của người dùng, nhưng tất cả các giao dịch đều được lưu trữ trên blockchain công khai, điều này có nghĩa là các giao dịch có thể được truy tìm lại về sau.

Thách thức

Bitcoin đang đối mặt với nhiều thách thức, bao gồm:

- Sự phát triển chậm của công nghệ: Mặc dù Bitcoin là công nghệ tiên tiến và được sử dụng rộng rãi, nhưng nó đang đối mặt với sự phát triển chậm của công nghệ. Các nhà phát triển cần phải liên tục cập nhật và phát triển các tính năng mới để giải quyết các vấn đề hiện tại của Bitcoin.
- Cạnh tranh từ các đồng tiền ảo khác: Các đồng tiền ảo khác đang ngày càng trở nên phổ biến và có tính năng cải tiến hơn so với Bitcoin. Điều này tạo ra một sự cạnh tranh trong thị trường tiền ảo và đặt Bitcoin vào một vị trí không ổn định.
- Sự cần thiết phải tuân thủ các quy định pháp lý: Các quy định pháp lý đang được áp dụng đối với tiền ảo và Bitcoin không phải là ngoại lệ. Việc phải tuân thủ các quy định pháp lý có thể làm tăng chi phí và ảnh hưởng đến sự phát triển của Bitcoin.
- Sự bảo mật của hệ thống: Mặc dù Bitcoin được mã hóa và an toàn, nhưng các vụ tấn công và vi phạm bảo mật đã xảy ra trong quá khứ và có thể xảy ra trong tương lai. Việc bảo vệ hệ thống Bitcoin cần phải được thực hiện liên tục và nghiêm ngặt để đảm bảo tính an toàn của các giao dịch Bitcoin.
- Mức độ sử dụng thấp: Mặc dù Bitcoin đã được sử dụng rộng rãi, tuy nhiên mức độ sử dụng của nó vẫn thấp so với các phương tiện thanh toán truyền thống. Điều này gây ảnh hưởng đến tính tiện lợi và khả năng chấp nhận của Bitcoin.
- Khả năng sử dụng cho mục đích phi pháp: Vì Bitcoin không được quản lý hoặc kiểm soát bởi các tổ chức tài chính hay chính phủ, nên có khả năng sử dụng cho mục đích phi pháp như rửa tiền, trốn thuế hoặc tài trợ cho các hoạt động tội phạm.
- Khả năng bị cấm hoặc hạn chế sử dụng: Các chính phủ có thể cấm hoặc hạn chế sử dụng Bitcoin trong một số trường hợp như sự cố về an ninh quốc gia, kiểm soát vốn chuyển ra nước ngoài hoặc chống lại các hoạt động phi pháp. Việc này có thể làm giảm khả năng sử dụng và tính bền vững của Bitcoin.

- Sự cạnh tranh từ các đồng tiền mã hóa khác: Hiện nay, có hàng trăm đồng tiền mã hóa khác ngoài Bitcoin được sử dụng và phát triển trên toàn cầu. Các đồng tiền này cạnh tranh với Bitcoin về tính khả dụng và giá trị và có thể làm giảm khả năng sử dụng và giá trị của Bitcoin.
- Vấn đề về quyền riêng tư: Mặc dù Bitcoin được cho là không thuộc về bất kỳ ai, nhưng mọi giao dịch Bitcoin đều được lưu trữ trên blockchain và có thể được truy xuất. Điều này đặt ra câu hỏi về quyền riêng tư và an ninh thông tin.
- Thách thức về quy định và luật pháp: Bitcoin không được quản lý hoặc kiểm soát bởi bất kỳ tổ chức tài chính hay chính phủ nào, điều này đặt ra thách thức về quy định và luật pháp. Các quy định và chính sách pháp lý khác nhau ở từng quốc gia và khu vực có thể gây ảnh hưởng đến sự phát triển và sử dụng của Bitcoin.
- Rủi ro bảo mật: Một số rủi ro bảo mật như vi rút máy tính, tấn công mạng và các cuộc tấn công hacker có thể gây ảnh hưởng đến tính bảo mật của Bitcoin và làm giảm độ tin cậy của nó.

4.1.3 Đánh giá ba tiêu chuẩn cho Bitcoin

4.1.3.1 Lựa chọn tiêu chuẩn và tiêu chí so sánh tiêu chuẩn

Lựa chọn tiêu chuẩn

Đối với đề tài này, nhóm chỉ chọn các công trình được công bố từ các tổ chức chuyên về tiêu chuẩn hóa, như ISO, và không xem xét những bản thảo ở bất kỳ giai đoạn nào, vì nội dung của chúng có thể thay đổi trước khi phiên bản phát hành cuối cùng được công khai. Tương tự, nhóm không xem xét các giao thức hoặc quy trình cụ thể của các công ty, mà đôi khi được gọi là "tiêu chuẩn" một cách sai lầm, và chỉ áp dụng duy nhất trong Ethereum dưới dạng Token cụ thể, vì những thực hiện như vậy chỉ liên quan đến các giải pháp cá nhân và không phải là tiêu chuẩn áp dụng toàn cầu độc lập với nền tảng blockchain được chọn. Những yếu tố như vậy không liên quan đến đề tài này. Việc lựa chọn các nỗ lực tiêu chuẩn hóa được trình bày trong bài báo này dựa trên hai phương pháp. Trước tiên, nhóm đã tìm hiểu các công bố và hoạt động của các tổ chức tiêu chuẩn hóa nổi tiếng và tổ chức làm việc cụ thể hơn về an ninh thông tin. Đối với phương pháp thứ hai, nhóm mở rộng nghiên cứu và phạm vi tiêu

chuẩn hóa bằng cách bao gồm thông tin bổ sung mà nhóm có thể thu thập thông qua các tài liệu tham khảo liên quan.

Tiêu chí so sánh tiêu chuẩn

Vì việc lựa chọn các tiêu chuẩn và khuyến nghị sẽ được thảo luận và so sánh trong công việc này rất rộng, với đa dạng mục tiêu của các tài liệu liên quan, các tiêu chí so sánh cũng cần phản ánh sự đa dạng này. Hơn nữa, mức độ chi tiết mà các tiêu chuẩn cung cấp khác nhau rất lớn, đặc biệt là đối với các vấn đề đặc biệt như tuân thủ GDPR và tích hợp các vấn đề pháp lý. Tuy nhiên, ngay cả từ quan điểm kỹ thuật và quản lý, các điểm tập trung khác nhau của các tiêu chuẩn làm cho việc so sánh trở nên khó khăn và không thể sử dụng một chỉ số duy nhất. Hơn nữa, cần lưu ý rằng không phải tất cả các tài liệu được đề cập trong phần này thực sự tập trung vào blockchain hoặc công nghệ sổ cái kỹ thuật số, đối với một số tài liệu này chỉ là một vấn đề phụ được xem xét, nhưng không phải là chủ đề chính. Tuy nhiên, những tài liệu như vậy có thể rất có giá trị, đặc biệt khi chúng tập trung vào các thực tiễn tốt nhất trong một lĩnh vực ứng dụng cụ thể, do đó có ý nghĩa đối với lĩnh vực đang nghiên cứu.

Các tiêu chuẩn và thực tiễn tốt đã được chọn được cấu trúc theo các tiêu chí sau, được nhóm thành bốn nhóm: (i) Tiêu chí phản ánh về tài liệu, khả năng áp dụng, thông tin siêu và lĩnh vực chính của nó (tiêu chí tài liệu), và (ii) tiêu chí phản ánh nội dung thực tế của tài liệu (tiêu chí nội dung). Phải nhắc lại rằng nhóm chỉ xem xét các tiêu chuẩn đã được công bố dưới dạng cuối cùng, không bao gồm bản thảo hoặc kết quả thảo luận trung gian, vì (a) chúng thường không phổ biến và (b) có thể thay đổi đáng kể trước khi phát hành cuối cùng.

4.1.3.2 Ba tiêu chuẩn cho Bitcoin

Ba tiêu chuẩn cho Bitcoin được nhóm lựa chọn gồm:

WEF_GSMI_Technical_Standards_2020, ISO/TC 307, DIN SPEC 3104.

Đánh giá tiêu chuẩn WEF_GSMI_Technical_Standards_2020 cho Bitcoin

Đánh giá tiêu chuẩn WEF_GSMI_Technical_Standards_2020 cho Bitcoin sẽ dựa vào những tiêu chí sau: khả năng tương tác, bảo mật, quyền riêng tư, quản trị, quản lý dữ liệu, tuân thủ.

a. Khả năng tương tác

Tương thích và Tương tác:

- Đánh giá sự tương thích của Bitcoin với các mạng dựa trên blockchain khác. Đánh giá khả năng tương tác và giao tiếp của Bitcoin với các giao thức và tiêu chuẩn khác nhau.
- Xem xét xem Bitcoin có thể tích hợp một cách liền mạch với các mạng blockchain khác mà không gặp các rào cản kỹ thuật đáng kể hay vấn đề về tương thích.

Tiêu chuẩn và Giao thức tương thích:

- Đánh giá mức độ tiêu chuẩn và giao thức tương thích được triển khai trong Bitcoin. Tìm kiếm các tiêu chuẩn cho phép giao tiếp và trao đổi dữ liệu qua mạng lưới.
- Xem xét xem Bitcoin tuân thủ các tiêu chuẩn tương thích được chấp nhận rộng rãi, như giao dịch nguyên tử, cầu nối giữa các chuỗi, hoặc các giao thức tương thích như Polkadot hoặc Cosmos.

Giao dịch qua Chuỗi:

- Đánh giá khả năng hỗ trợ giao dịch qua chuỗi của Bitcoin. Đánh giá xem nó có cho phép người dùng chuyển tài sản hoặc giá trị giữa Bitcoin và các mạng blockchain khác không.
- Xem xét các cơ chế và công nghệ có sẵn để thực hiện giao dịch qua chuỗi một cách an toàn, như giao dịch phi tập trung hoặc các giao thức tương thích.

Trao đổi Dữ liệu:

- Đánh giá khả năng trao đổi dữ liệu của Bitcoin với các mạng blockchain khác.
- Xem xét xem Bitcoin có hỗ trợ các định dạng dữ liệu tương thích hay có cơ chế chia sẻ và đồng bộ dữ liệu với các mạng khác không.
- Đánh giá xem Bitcoin có cho phép việc trao đổi tương thích của các hợp đồng thông minh, tài sản số hoặc các yếu tố dữ liệu khác giữa các mạng dựa trên blockchain khác nhau không.

Khi đánh giá tính tương thích của Bitcoin, quan trọng là đánh giá sự tương thích của nó với các mạng khác, mức độ tiêu chuẩn tương thích được triển khai và khả năng hỗ trợ giao dịch qua chuỗi và trao đổi dữ liệu. Phân tích này sẽ cung cấp thông tin về khả năng hợp tác và giao tiếp của Bitcoin với các hệ sinh thái blockchain

b. Bảo mật

Thuật toán mã hóa:

- Phân tích các thuật toán mã hóa được sử dụng trong Bitcoin, chẳng hạn như hàm băm (SHA-256) và ký tự số (ECDSA). Đánh giá tính mạnh mẽ và khả năng chống lại các cuộc tấn công mật mã đã biết.
- Xem xét xem Bitcoin có theo kịp các tiến trình trong mã học và áp dụng các thuật toán an toàn để bảo vệ giao dịch và dữ liệu người dùng.

Cơ chế đồng thuận:

- Đánh giá cơ chế đồng thuận được sử dụng trong Bitcoin, đó là Proof-of-Work - PoW. Phân tích các cam kết bảo mật mà PoW mang lại trong quá trình ngăn chặn tiêu cực gian lận và duy trì tính toàn vẹn của blockchain.
- Xem mức độ phi tập trung được đánh giá là đạt được thông qua cơ chế đồng thuận và xem liệu nó có hiệu quả chống lại các cuộc tấn công hay không.

Lịch sử các sự cố bảo mật:

- Đánh giá sự cố về bảo mật và lỗi theo dõi trong lịch sử của mạng Bitcoin. Tìm hiểu về các cuộc tấn công đáng lưu ý như Double Spending, Replay) Attack, 51% Attack.
- Đánh giá tác động của những sự cố này, phản hồi từ cộng đồng Bitcoin và các biện pháp được thực hiện để giảm thiểu rủi ro trong tương lai.

Biện pháp bảo mật:

- Phân tích các biện pháp bảo mật được phát triển khai thác trong mã nguồn Bitcoin và cơ sở hạ tầng mạng. Đánh giá việc sử dụng các phương pháp tốt nhất, như mã hóa mạng ngang hàng, mã hóa mạng ngang hàng và bảo vệ chống lại các hướng tấn công thông thường.
- Xem xét xem Bitcoin đã trải qua các cuộc kiểm tra bảo mật hoặc kiểm tra xâm nhập để phát hiện ra các lỗ hổng và đảm bảo một cơ sở bảo mật chắc chắn.

Việc đánh giá các tính năng bảo mật của mạng Bitcoin là rất quan trọng, bao gồm các thuật toán mã hóa mật mã, cơ chế đồng thuận và khả năng chống lại các cuộc tấn công. Việc đánh giá lịch sử các sự cố và lỗ hổng bảo mật cung cấp thông tin chuyên sâu về khả năng phục hồi của mạng. Ngoài ra, việc phân tích các biện pháp bảo mật được triển khai trong cơ sở mã và cơ sở hạ tầng mạng của Bitcoin giúp đánh giá mức độ bảo vệ và giảm thiểu rủi ro tại chỗ.

c. Chính sách

Mô hình giao dịch ẩn danh (Pseudonymous Transaction Model):

- Đánh giá mức độ bảo vệ sự riêng tư được cung cấp bởi mô hình giao dịch giấu danh của Bitcoin, có nghĩa là các giao dịch không được liên kết trực tiếp với danh tính trong thế giới thực.
- Xem xét mức độ mà Bitcoin bảo vệ sự riêng tư của người dùng bằng cách cho phép họ thực hiện giao dịch mà không tiết lộ thông tin cá nhân.

Tính ẩn danh và không liên kết:

- Đánh giá mức độ ẩn danh và không liên kết của các giao dịch trên mạng Bitcoin. Phân tích độ khó khăn trong việc theo dõi các giao dịch trở lại người gửi và người nhận.
- Xem xét tiềm năng của phân tích đồ thị giao dịch và khả năng phát hiện các mẫu hoặc liên kết các giao dịch với người dùng cụ thể.

Công nghệ tăng cường sự riêng tư:

- Đánh giá các biện pháp được Bitcoin thực hiện để tăng cường sự riêng tư, chẳng hạn như việc áp dụng các công nghệ tăng cường sự riêng tư như CoinJoin hoặc Confidential Transactions.
- Phân tích tính hiệu quả của các công nghệ này trong việc che giấu chi tiết giao dịch và bảo vệ sự riêng tư của người dùng.

Chính sách và Hướng dẫn về Sự riêng tư:

- Đánh giá bất kỳ chính sách hoặc hướng dẫn về sự riêng tư nào được thiết lập bởi cộng đồng hoặc nhóm phát triển Bitcoin. Xem xét liệu các chính sách này có giải quyết được các vấn đề về sự riêng tư và thúc đẩy các phương pháp tốt nhất để bảo vệ sự riêng tư của người dùng hay không.

Giáo dục và Nhận thức của người dùng:

- Xem xét những nỗ lực của cộng đồng Bitcoin để giáo dục người dùng về các phương pháp tốt nhất để bảo vệ sự riêng tư. Đánh giá liệu có sẵn các tài nguyên để giúp người dùng hiểu và tăng cường sự riêng tư khi sử dụng Bitcoin hay không.

Bằng cách đánh giá mức độ bảo vệ sự riêng tư được cung cấp bởi mô hình giao dịch giấu danh của Bitcoin, xem xét mức độ ẩn danh và không liên kết của các giao dịch và đánh giá các biện pháp được thực hiện để tăng cường sự riêng tư, có thể có

được những thông tin sâu sắc về các tính năng về sự riêng tư của mạng. Điều quan trọng cũng là cần xem xét việc áp dụng các công nghệ tăng cường sự riêng tư và bất kỳ chính sách hoặc hướng dẫn về sự riêng tư nào được thiết lập để đảm bảo sự riêng tư của người dùng.

d. Quản trị

Mô hình Quản trị phi tập trung:

- Phân tích mô hình quản trị phi tập trung của Bitcoin, có nghĩa là quyền ra quyết định được phân phối giữa các bên tham gia thay vì được kiểm soát bởi một thực thể duy nhất.
- Đánh giá mức độ mà mô hình quản trị cho phép một loạt các bên liên quan tham gia trong các quyết định quản trị.

Tham gia của cộng đồng:

- Đánh giá mức độ tham gia của cộng đồng trong quản trị Bitcoin. Xem xét liệu cộng đồng có cơ chế để đề xuất và thảo luận về các thay đổi hoặc cải tiến cho giao thức Bitcoin hay không.
- Đánh giá mức độ truy cập vào các quyết định quản trị và mức độ mà các thành viên trong cộng đồng có thể đóng góp ý tưởng và quan điểm của mình.
- Cơ chế xây dựng đồng thuận:
- Phân tích các cơ chế xây dựng đồng thuận được sử dụng bởi cộng đồng Bitcoin để đạt được sự đồng thuận về các thay đổi hoặc nâng cấp cho mạng.
- Xem xét tính hiệu quả của các cơ chế này trong việc đạt được đồng thuận và duy trì tính ổn định và tính toàn vẹn của giao thức Bitcoin.

Các sự cố và tranh chấp liên quan đến quản trị:

- Đánh giá lịch sử các sự cố và tranh chấp liên quan đến quản trị đã xảy ra trong hệ sinh thái Bitcoin. Điều này có thể bao gồm các cuộc tranh luận, xung đột lợi ích hoặc tranh cãi về các thay đổi đề xuất hoặc quy trình ra quyết định.
- Xem xét tác động của những sự cố này đến cộng đồng và tính đàn hồi của mô hình quản trị trong việc đối phó và giải quyết những thách thức này.

Sự minh bạch và trách nhiệm:

- Đánh giá mức độ minh bạch và trách nhiệm trong các quy trình quản trị của Bitcoin. Đánh giá liệu quyết định được thực hiện một cách minh bạch, có sự truyền thông rõ ràng và tài liệu về các đề xuất và thảo luận hay không.

- Xem xét sự tồn tại của các cơ chế để đưa ra trách nhiệm cho các bên tham gia và đảm bảo rằng các quyết định phù hợp với lợi ích của cộng đồng Bitcoin nói chung.

Bằng cách phân tích mô hình quản trị phi tập trung của Bitcoin, đánh giá sự tham gia của cộng đồng và các cơ chế xây dựng đồng thuận, cân nhắc các sự cố và tranh chấp liên quan đến quản trị, bạn có thể có được những thông tin sâu sắc về cách quản trị được cấu trúc và thực hiện trong hệ sinh thái Bitcoin. Ngoài ra, đánh giá các khía cạnh về sự minh bạch và trách nhiệm có thể cung cấp một cái nhìn tốt hơn về quy trình ra quyết định và sự phù hợp với lợi ích của cộng đồng.

e. Quản lý dữ liệu

Cấu trúc dữ liệu:

- Đánh giá cấu trúc dữ liệu được sử dụng trong Bitcoin, dựa trên một blockchain. Hiểu cách dữ liệu được tổ chức và lưu trữ trong các khối và cách các khối được liên kết với nhau để tạo thành blockchain.
- Đánh giá tính phù hợp của cấu trúc dữ liệu của Bitcoin để lưu trữ và truy xuất dữ liệu giao dịch một cách hiệu quả.

Cơ chế lưu trữ:

- Phân tích các cơ chế lưu trữ được sử dụng bởi Bitcoin để lưu trữ dữ liệu blockchain của nó. Xem xét liệu Bitcoin có sử dụng mô hình lưu trữ phân tán hay phụ thuộc vào các máy chủ tập trung để lưu trữ dữ liệu hay không.
- Đánh giá tính bền bỉ và tính dự phòng của các cơ chế lưu trữ của Bitcoin để đảm bảo tính toàn vẹn và khả dụng của dữ liệu.

Biện pháp đảm bảo tính toàn vẹn dữ liệu:

- Đánh giá các biện pháp được triển khai bởi Bitcoin để đảm bảo tính toàn vẹn dữ liệu trong blockchain. Điều này có thể bao gồm việc sử dụng các thuật toán mật mã để xác nhận dữ liệu và bảo vệ chống lại sự can thiệp.
- Đánh giá tính hiệu quả của các biện pháp này trong việc duy trì độ chính xác và nhất quán của dữ liệu được lưu trữ trong blockchain.

Khả năng mở rộng:

- Đánh giá khả năng mở rộng của Bitcoin đối với việc quản lý dữ liệu. Xem xét mạng có thể xử lý một lượng lớn giao dịch mà không gây ra sự giảm hiệu suất đáng kể hay không.

- Đánh giá các giải pháp hoặc kỹ thuật mở rộng mà Bitcoin đã triển khai để giải quyết thách thức về tăng khối lượng giao dịch và duy trì kích thước của blockchain.

Đồng bộ hóa và xác thực dữ liệu:

- Phân tích tính hiệu quả và tính hiệu quả của quy trình đồng bộ hóa và xác nhận dữ liệu của Bitcoin. Xem xét tốc độ lan truyền giao dịch mới trong toàn mạng và mức độ hiệu quả của quá trình xác nhận.
- Đánh giá cơ chế đồng thuận (ví dụ: Proof of Work) được sử dụng bởi Bitcoin để đảm bảo sự đồng ý về trạng thái của blockchain và tính hợp lệ của các giao dịch.

Bằng cách đánh giá cấu trúc dữ liệu, cơ chế lưu trữ, biện pháp đảm bảo tính toàn vẹn dữ liệu, khả năng mở rộng và quy trình đồng bộ hóa và xác nhận dữ liệu của Bitcoin, có thể có được những thông tin sâu sắc về cách Bitcoin quản lý dữ liệu và xử lý yêu cầu ngày càng tăng của việc xử lý giao dịch.

f. Tuân thủ

Tuân thủ Pháp lý và Quy định:

- Đánh giá sự tuân thủ của Bitcoin đối với các khung pháp lý và quy định liên quan ở các khu vực khác nhau. Xem xét cách Bitcoin đối phó với các quy định tài chính, luật chứng khoán, nghĩa vụ thuế và các luật pháp khác có liên quan.
- Đánh giá mức độ mà thiết kế và chức năng của Bitcoin tuân thủ các yêu cầu pháp lý và quy định này.

Phòng chống rửa tiền (AML) và xác minh khách hàng (KYC):

(Anti-Money Laundering (AML) and Know-Your-Customer (KYC))

- Xem xét các biện pháp đã triển khai bởi Bitcoin để đáp ứng các quy định về AML và KYC. Đánh giá mức độ minh bạch và các thủ tục xác minh được sử dụng để giảm thiểu rủi ro của các hoạt động bất hợp pháp và rửa tiền.
- Đánh giá tính hiệu quả của các biện pháp này trong việc ngăn chặn truy cập trái phép, gian lận và lạm dụng mạng Bitcoin.

Sự minh bạch và khả năng kiểm toán của giao dịch:

- Đánh giá tính minh bạch và khả năng kiểm toán của các giao dịch Bitcoin. Xem xét liệu chi tiết giao dịch, bao gồm địa chỉ người gửi và người nhận và số

tiền giao dịch, có được công khai truy cập và xác minh trên blockchain hay không.

- Đánh giá mức độ mà lịch sử giao dịch của Bitcoin có thể được kiểm toán cho mục đích tuân thủ, chẳng hạn như xác minh nguồn tiền hoặc điều tra các hoạt động đáng ngờ.

Công cụ tuân thủ và Đối tác:

- Xem xét tính sẵn có của các công cụ và dịch vụ tuân thủ trong hệ sinh thái Bitcoin. Đánh giá liệu có các nhà cung cấp bên thứ ba uy tín cung cấp các giải pháp tuân thủ, chẳng hạn như phân tích blockchain hoặc dịch vụ xác minh danh tính hay không.
- Đánh giá bất kỳ liên kết hoặc hợp tác nào với các cơ quan quản lý, tổ chức tài chính hoặc tổ chức tuân thủ nào cho thấy cam kết của Bitcoin với tuân thủ và hợp tác với các cơ quan có liên quan.

Thách thức và tranh chấp pháp lý:

- Phân tích các trường hợp trong quá khứ mà Bitcoin đã gặp phải thách thức hoặc tranh chấp pháp lý. Xem xét bất kỳ hành động pháp lý, cảnh báo quy định hoặc các sự cố liên quan đến tuân thủ nào có thể ảnh hưởng đến uy tín hoặc hoạt động của Bitcoin.
- Đánh giá cách mà Bitcoin đã đáp ứng với những thách thức này và các biện pháp được thực hiện để giải quyết bất kỳ khoảng trống hoặc mớilộn ngai về tuân thủ nào được đưa ra bởi các cơ quan quản lý.

Bằng cách đánh giá sự tuân thủ của Bitcoin với các yêu cầu pháp lý và quy định, các biện pháp AML và KYC, tính minh bạch và khả năng kiểm toán của các giao dịch, và cách tiếp cận của Bitcoin đối với các thách thức pháp lý, bạn có thể đánh giá mức độ phù hợp của Bitcoin cho các giao dịch tài chính tuân thủ và khả năng của nó để hoạt động trong các khung pháp lý khác nhau.

Đánh giá tiêu chuẩn ISO/TC 307 cho Bitcoin

Đánh giá tiêu chuẩn WEF_GSMI_Technical_Standards_2020 cho Bitcoin sẽ dựa vào những tiêu chí sau: công nghệ blockchain, khả năng mở rộng, bảo mật, chính sách và bảo vệ dữ liệu, quản trị và tuân thủ, khả năng tương tác.

a. Công nghệ blockchain

Khi đánh giá Bitcoin thông qua tiêu chuẩn ISO/TC 307, việc đánh giá cách Bitcoin sử dụng công nghệ blockchain và việc tuân thủ các nguyên tắc và yêu cầu được đề ra trong tiêu chuẩn về công nghệ blockchain và sổ cái phân tán là rất quan trọng.

Đầu tiên, phân tích cách Bitcoin triển khai các khái niệm cơ bản của blockchain, chẳng hạn như sự đồng thuận phi tập trung, tính không thể thay đổi và bảo mật mật mã. Xem xét cơ chế đồng thuận được sử dụng bởi Bitcoin, chẳng hạn như proof-of-work (PoW), và đánh giá tính hiệu quả của nó trong việc đạt được sự đồng thuận giữa các thành viên trong mạng lưới.

Tiếp theo, đánh giá cách Bitcoin đáp ứng các yêu cầu chính được đề ra trong tiêu chuẩn ISO/TC 307. Những yêu cầu này có thể bao gồm tính toàn vẹn dữ liệu, tính minh bạch, khả năng kiểm tra và tính truy xuất. Đánh giá cách Bitcoin đảm bảo tính toàn vẹn của dữ liệu giao dịch của nó, độ minh bạch của blockchain và khả năng kiểm tra và truy xuất giao dịch một cách hiệu quả.

Xem xét cách Bitcoin xử lý các vấn đề về khả năng mở rộng trong blockchain của nó. Đánh giá xem Bitcoin có sử dụng các kỹ thuật như gom giao dịch, giải pháp lớp hai hoặc các giao thức off-chain để cải thiện khả năng mở rộng mà vẫn đảm bảo tính toàn vẹn của blockchain hay không.

Ngoài ra, đánh giá cách Bitcoin tiếp cận với quản trị và xây dựng sự đồng thuận. Phân tích các quy trình ra quyết định, sự tham gia của cộng đồng và các cơ chế giải quyết xung đột hoặc giới thiệu nâng cấp cho giao thức. Xem xét mô hình quản trị của Bitcoin có phù hợp với các nguyên tắc và hướng dẫn được đưa ra trong tiêu chuẩn ISO/TC 307 hay không.

Cuối cùng, xem xét bất kỳ tiến bộ hoặc đổi mới nào mà Bitcoin đã triển khai để cải thiện tính bảo mật, riêng tư và tương thích của blockchain của nó. Đánh giá xem Bitcoin có tích hợp các công nghệ tăng cường quyền riêng tư, chẳng hạn như chứng minh không có kiến thức hoặc chữ ký vòng, để bảo vệ quyền riêng tư của người dùng hay không. Xem xét tính tương thích của Bitcoin với các mạng blockchain khác và mức độ mà nó hỗ trợ tương tác giữa các chuỗi khối.

Bằng cách đánh giá kỹ lưỡng cách Bitcoin sử dụng công nghệ blockchain và việc tuân thủ các nguyên tắc và yêu cầu được đề ra trong tiêu chuẩn ISO/TC 307, bạn có thể có cái nhìn về tính phù hợp của nó với các thực tiễn tốt nhất trong ngành và xác

định các điểm mạnh và điểm yếu của Bitcoin trong bối cảnh rộng hơn của công nghệ blockchain.

b. Khả năng mở rộng

Khi đánh giá khả năng mở rộng của Bitcoin thông qua tiêu chuẩn ISO/TC 307, việc đánh giá các giải pháp mở rộng được sử dụng bởi Bitcoin và sự phù hợp của chúng với các nguyên tắc và khuyến nghị về khả năng mở rộng được cung cấp trong tiêu chuẩn là rất quan trọng.

Đầu tiên, phân tích khả năng xử lý giao dịch hiện tại của Bitcoin và khả năng xử lý một lượng lớn giao dịch. Đánh giá lưu lượng giao dịch trên mạng và đánh giá xem nó có đáp ứng các yêu cầu khả năng mở rộng được đề ra trong tiêu chuẩn ISO/TC 307 hay không.

Xem xét các giải pháp mở rộng được triển khai bởi Bitcoin, chẳng hạn như gom giao dịch, Segregated Witness (SegWit) hoặc các giao thức lớp hai như Lightning Network. Đánh giá tính hiệu quả của các giải pháp này trong việc cải thiện khả năng mở rộng của giao dịch trong khi vẫn đảm bảo an ninh và tính toàn vẹn của blockchain.

Đánh giá cách Bitcoin đối phó với các thách thức của tắc nghẽn mạng và các khoản phí giao dịch cao, vì những yếu tố này có thể ảnh hưởng đến khả năng mở rộng của nó. Xem xét bất kỳ kỹ thuật hoặc cơ chế đổi mới nào mà Bitcoin sử dụng để giảm thiểu các vấn đề này và cải thiện khả năng mở rộng của mạng.

Ngoài ra, đánh giá mức độ nghiên cứu và phát triển được tiến hành bởi cộng đồng Bitcoin để giải quyết các vấn đề về khả năng mở rộng. Xem xét việc áp dụng các công nghệ mới hoặc nâng cấp giao thức được đề xuất nhằm cải thiện khả năng mở rộng của mạng trong khi đảm bảo tính tương thích và sự đồng thuận giữa các thành viên trong mạng.

Thêm vào đó, phân tích cách các giải pháp khả năng mở rộng của Bitcoin phù hợp với các nguyên tắc và khuyến nghị về khả năng mở rộng được cung cấp trong tiêu chuẩn ISO/TC 307. Xem xét xem các giải pháp được triển khai có tuân thủ các thực tiễn tốt nhất và các tiêu chuẩn ngành để đạt được khả năng mở rộng trong công nghệ blockchain và số cái phân tán hay không.

Bằng cách đánh giá kỹ lưỡng các giải pháp khả năng mở rộng của Bitcoin và sự phù hợp của chúng với tiêu chuẩn ISO/TC 307, bạn có thể đánh giá khả năng của mạng trong việc xử lý một lượng lớn giao dịch một cách hiệu quả. Đánh giá này sẽ

cung cấp thông tin về khả năng mở rộng của Bitcoin và sự tuân thủ của nó với các nguyên tắc và khuyến nghị ngành trong bối cảnh khả năng mở rộng.

c. Bảo mật

Khi đánh giá tính bảo mật của Bitcoin theo tiêu chuẩn ISO/TC 307, việc phân tích các biện pháp bảo mật được triển khai trong mạng là rất quan trọng. Điều này bao gồm đánh giá các thuật toán mã hóa được sử dụng, cơ chế đồng thuận được sử dụng và các cơ chế bảo vệ chống lại các cuộc tấn công đã biết như double spending và 51% attacks.

Bắt đầu bằng việc xem xét các thuật toán mã hóa được sử dụng bởi Bitcoin, chẳng hạn như SHA-256 cho phép băm và mã hóa đường cong elip cho việc tạo khóa và xác minh chữ ký. Đánh giá tính bền vững của các thuật toán này và đánh giá sự tuân thủ của chúng với các yêu cầu bảo mật được đề ra trong tiêu chuẩn ISO/TC 307.

Tiếp theo, phân tích cơ chế đồng thuận của Bitcoin, hiện tại được dựa trên proof-of-work (PoW). Đánh giá các tính năng bảo mật của PoW, bao gồm sự kháng cự với các cuộc tấn công Sybil và ngăn chặn các tác nhân độc hại kiểm soát mạng. Đánh giá xem cơ chế đồng thuận của Bitcoin có phù hợp với các yêu cầu bảo mật được đặt ra trong tiêu chuẩn ISO/TC 307 hay không.

Xem xét cách Bitcoin bảo vệ chống lại các cuộc tấn công đã biết, đặc biệt là double spending và 51% attacks. Đánh giá sự kháng cự của mạng trước các cuộc tấn công này và các biện pháp để phát hiện và ngăn chặn chúng. Đánh giá xem các biện pháp bảo mật của Bitcoin có phù hợp với các yêu cầu được quy định bởi tiêu chuẩn ISO/TC 307 về bảo vệ chống lại các cuộc tấn công này hay không.

Ngoài ra, kiểm tra sự tuân thủ của Bitcoin với các yêu cầu bảo mật của tiêu chuẩn ISO/TC 307. Đánh giá xem mạng triển khai các thực tiễn và giao thức bảo mật được khuyến nghị, chẳng hạn như quản lý khóa, kiểm soát truy cập và các kênh truyền thông an toàn. Đánh giá mức độ tuân thủ các yêu cầu này để xác định tổng thể tình trạng bảo mật của Bitcoin.

d. Chính sách và bảo vệ dữ liệu

Khi đánh giá mức độ bảo mật thông tin và bảo vệ dữ liệu mà mô hình giao dịch của Bitcoin cung cấp, việc xem xét sự tuân thủ của Bitcoin với các tiêu chuẩn bảo mật thông tin được đề ra bởi ISO/TC 307 là rất quan trọng, bao gồm các nguyên tắc như giảm thiểu dữ liệu, sự đồng ý của người dùng và xử lý dữ liệu an toàn.

Bắt đầu bằng việc đánh giá phương pháp giảm thiểu dữ liệu của Bitcoin. Giảm thiểu dữ liệu tập trung vào việc thu thập và lưu trữ chỉ các dữ liệu cần thiết để xử lý giao dịch. Đánh giá xem Bitcoin có tuân thủ nguyên tắc này bằng cách phân tích thông tin được bao gồm trong các giao dịch và đánh giá xem liệu dữ liệu không cần thiết có được tránh.

Tiếp theo, xem xét sự tuân thủ của Bitcoin đối với yêu cầu sự đồng ý của người dùng. Sự đồng ý của người dùng là rất quan trọng để đảm bảo các cá nhân có quyền kiểm soát việc tiết lộ và xử lý thông tin cá nhân của họ. Đánh giá xem Bitcoin cung cấp cơ chế cho người dùng để đưa ra sự đồng ý thông tin và xem xét xem liệu họ có khả năng quản lý việc chia sẻ và xử lý dữ liệu của mình.

Đánh giá cách Bitcoin xử lý và bảo mật dữ liệu. Xem xét các biện pháp được triển khai để bảo vệ thông tin nhạy cảm, chẳng hạn như các giao thức mã hóa và truyền dữ liệu an toàn. Đánh giá xem các thực tiễn xử lý dữ liệu của Bitcoin có phù hợp với các khuyến nghị về bảo mật và quyền riêng tư được đề ra bởi ISO/TC 307 hay không.

Ngoài ra, xem xét bất kỳ công nghệ tăng cường quyền riêng tư nào được áp dụng bởi Bitcoin. Các công nghệ này có thể bao gồm các kỹ thuật như CoinJoin hoặc giao dịch bảo mật, nhằm tăng cường quyền riêng tư của các giao dịch và bảo vệ tính không liên kết của danh tính người dùng. Đánh giá mức độ mà Bitcoin tích hợp các công nghệ này và hiệu quả của chúng trong bảo vệ quyền riêng tư.

Bằng cách đánh giá sự tuân thủ của Bitcoin đối với các tiêu chuẩn bảo mật thông tin được đề ra bởi ISO/TC 307, chẳng hạn như giảm thiểu dữ liệu, sự đồng ý của người dùng và xử lý dữ liệu an toàn, bạn có thể đánh giá mức độ bảo vệ quyền riêng tư và bảo vệ dữ liệu mà mô hình giao dịch của Bitcoin cung cấp. Đánh giá này sẽ giúp xác định liệu Bitcoin có phù hợp với các tiêu chuẩn quyền riêng tư được khuyến nghị và tuân thủ các thực tiễn tốt nhất trong bảo vệ quyền riêng tư và bảo vệ dữ liệu.

Cũng quan trọng là cần xem xét bất kỳ sự cố bảo mật hoặc lỗ hổng nào đã xảy ra trong quá khứ và cách cộng đồng Bitcoin đã giải quyết chúng. Đánh giá khả năng đáp ứng của mạng trước các vấn đề bảo mật và việc triển khai các bản vá hoặc nâng cấp kịp thời.

Bằng cách phân tích kỹ lưỡng các biện pháp bảo mật được triển khai trong Bitcoin, bao gồm các thuật toán mã hóa, cơ chế đồng thuận và bảo vệ chống lại các

cuộc tấn công đã biết, và đánh giá sự tuân thủ của nó với các yêu cầu bảo mật của tiêu chuẩn ISO/TC 307, bạn có thể có được một hiểu biết toàn diện về tình trạng bảo mật của Bitcoin và sự phù hợp của nó với các tiêu chuẩn ngành cho các công nghệ blockchain.

e. Quản trị và tuân thủ

Khi đánh giá việc quản trị và tuân thủ của Bitcoin, việc đánh giá mô hình quản trị, quy trình ra quyết định và tuân thủ các quy định pháp lý liên quan là rất quan trọng. Ngoài ra, cần xem xét cách Bitcoin đáp ứng các nguyên tắc quản trị được đề ra bởi tiêu chuẩn ISO/TC 307, chẳng hạn như tính minh bạch, trách nhiệm và tính bao gồm.

Bắt đầu bằng việc phân tích mô hình quản trị của Bitcoin. Đánh giá xem quy trình ra quyết định của Bitcoin có phân tán và bao gồm đại diện đa dạng, cho phép đại diện rộng rãi và đa dạng tham gia và đại diện. Đánh giá các cơ chế được thiết lập cho các bên liên quan để đưa ra ý kiến của họ và đóng góp vào quá trình ra quyết định. Xem xét mức độ minh bạch của cơ cấu quản trị và xem liệu thông tin về quyết định được công khai.

Tiếp theo, đánh giá sự tuân thủ của Bitcoin đối với các quy định pháp lý liên quan. Xem xét việc tuân thủ các quy định chống rửa tiền (AML) và xác minh khách hàng (KYC), cũng như bất kỳ quy định tài chính và bảo vệ người tiêu dùng nào khác. Đánh giá liệu Bitcoin đã triển khai các biện pháp để đảm bảo tuân thủ các quy định này và xác minh danh tính người dùng khi cần thiết hay không.

Xem xét cách Bitcoin đáp ứng các nguyên tắc quản trị được đề ra bởi tiêu chuẩn ISO/TC 307. Điều này bao gồm các nguyên tắc như tính minh bạch, đòi hỏi cung cấp thông tin rõ ràng về quy trình quản trị và quyết định, và trách nhiệm, đòi hỏi các cá nhân hoặc tổ chức chịu trách nhiệm cho hành động của mình. Đánh giá mức độ Bitcoin thể hiện các nguyên tắc này trong các thực tiễn quản trị của mình.

Ngoài ra, đánh giá cách Bitcoin tiếp cận tính bao gồm trong quản trị. Xem xét liệu Bitcoin có khuyến khích sự tham gia đa dạng và đại diện, và tính toàn vẹn của quyết định, lấy ý kiến của các bên liên quan và đảm bảo quyết định công bằng.

Bằng cách đánh giá mô hình quản trị của Bitcoin, quy trình ra quyết định và sự tuân thủ các quy định pháp lý liên quan, cũng như sự tuân thủ các nguyên tắc quản trị được đề ra bởi tiêu chuẩn ISO/TC 307, bạn có thể đánh giá tính hiệu quả và sự mạnh

mẽ của quản trị của Bitcoin và đánh giá sự phù hợp của nó với các thực tiễn quản trị được khuyến nghị.

f. Khả năng tương tác

Khi đánh giá tính tương thích của Bitcoin, việc đánh giá khả năng tương thích và khả năng tương tác với các mạng và hệ thống dựa trên blockchain khác là rất quan trọng. Xem xét việc tuân thủ các tiêu chuẩn và giao thức tương thích được đề ra bởi tiêu chuẩn ISO/TC 307 để tích hợp mượt mà với các hệ sinh thái blockchain đa dạng.

Bắt đầu bằng việc đánh giá tính tương thích của Bitcoin với các mạng blockchain khác. Đánh giá khả năng của Bitcoin để giao tiếp và trao đổi dữ liệu với các nền tảng blockchain khác nhau một cách hiệu quả, cho phép tương thích và giao dịch qua các chuỗi khối. Xem xét mức độ tiêu chuẩn hóa và giao thức được áp dụng bởi Bitcoin để đảm bảo tích hợp mượt mà.

Đánh giá sự tuân thủ của Bitcoin đối với các tiêu chuẩn tương thích ISO/TC 307. Những tiêu chuẩn này cung cấp hướng dẫn cho tích hợp mượt mà của các hệ sinh thái blockchain. Đánh giá mức độ phù hợp của Bitcoin với các tiêu chuẩn và giao thức này, bao gồm khả năng trao đổi thông tin, chia sẻ tài sản và thực hiện các giao dịch với các mạng blockchain khác.

Xem xét các khía cạnh công nghệ hỗ trợ tính tương thích. Đánh giá sự khả dụng của các giao diện lập trình ứng dụng (API) và các công cụ tích hợp khác cho phép truyền thông mượt mà giữa Bitcoin và các mạng blockchain khác. Đánh giá liệu cấu trúc dữ liệu, cơ chế đồng thuận và khả năng hợp đồng thông minh của Bitcoin có hỗ trợ yêu cầu tương thích hay không.

Ngoài ra, xem xét các sáng kiến hoặc sự hợp tác liên tục mà Bitcoin đã thực hiện để nâng cao tính tương thích. Tìm kiếm các đối tác hoặc dự án nhằm kết nối các mạng blockchain khác nhau hoặc tạo điều kiện cho giao dịch qua chuỗi khối. Những nỗ lực này thể hiện sự cam kết của Bitcoin đối với tính tương thích và sự sẵn lòng hợp tác với các hệ sinh thái blockchain khác.

Bằng cách đánh giá tính tương thích, sự tuân thủ các tiêu chuẩn tương thích và khả năng công nghệ cho tích hợp mượt mà, bạn có thể đánh giá tính hiệu quả của Bitcoin trong việc tạo điều kiện cho tính tương thích với các mạng và hệ thống dựa trên blockchain khác. Đánh giá này là rất quan trọng để hiểu tiềm năng của Bitcoin

trong việc hợp tác và khả năng tận dụng các lợi ích của một hệ sinh thái blockchain kết nối.

Đánh giá tiêu chuẩn DIN SPEC 3014 cho Bitcoin

Đánh giá tiêu chuẩn WEF_GSMI_Technical_Standards_2020 cho Bitcoin sẽ dựa vào những tiêu chí sau: quản trị và tổ chức, công nghệ và kiến trúc, bảo mật và phục hồi sau sự cố, khả năng tương tác và tương thích, quyền riêng tư và bảo vệ dữ liệu.

a. Quản trị và tổ chức

Cơ chế đồng thuận: Phân tích cơ chế đồng thuận được sử dụng bởi Bitcoin, chẳng hạn như Proof of Work (PoW). Đánh giá tính hiệu quả của những cơ chế này trong việc đạt được sự đồng thuận và duy trì tính toàn vẹn của mạng. Xem xét liệu cơ chế đồng thuận có phù hợp với các nguyên tắc được đề ra trong DIN SPEC 3014 hay không.

Sự tham gia của cộng đồng: Đánh giá mức độ tham gia của cộng đồng trong hệ sinh thái Bitcoin. Đánh giá liệu có kênh để các thành viên trong cộng đồng thể hiện ý kiến, đóng góp vào quy trình ra quyết định và tham gia vào việc phát triển và cải thiện giao thức hay không.

Nguyên tắc quản trị: Đánh giá sự tuân thủ của Bitcoin đối với các nguyên tắc quản trị được đề ra trong DIN SPEC 3014. Những nguyên tắc này có thể bao gồm tính minh bạch, trách nhiệm và tính bao gồm. Đánh giá liệu Bitcoin có cung cấp các cơ chế để đảm bảo tính minh bạch trong quyết định, đảm bảo trách nhiệm của các bên liên quan và thúc đẩy tính bao gồm bằng cách chào đón các quan điểm đa dạng.

Sự cố và tranh cãi liên quan đến quản trị: Xem xét bất kỳ sự cố hoặc tranh cãi liên quan đến chính phủ nào đã xảy ra trong hệ sinh thái Bitcoin. Đánh giá cách xử lý các sự cố này và liệu chúng có ảnh hưởng đến cấu trúc chính phủ hoặc quy trình ra quyết định hay không. Đánh giá liệu Bitcoin đã thực hiện các bước để học hỏi từ các sự cố trong quá khứ và cải thiện các thực hành quản trị của mình.

Bằng cách đánh giá chính phủ và tổ chức của Bitcoin dựa trên những khía cạnh này và áp dụng các tiêu chí được đề ra trong DIN SPEC 3014, bạn có thể có được cái nhìn về mức độ tuân thủ của Bitcoin đối với các nguyên tắc quản trị được đề xuất và đánh giá tính hiệu quả và độ bền của chính phủ tổng thể của nó.

b. Công nghệ và kiến trúc

Công nghệ blockchain: Đánh giá công nghệ blockchain cơ bản được sử dụng bởi Bitcoin. Phân tích thiết kế, cấu trúc và chức năng của blockchain, bao gồm cấu trúc dữ liệu, cơ chế đồng thuận và quy trình xác thực giao dịch. Đánh giá liệu blockchain của Bitcoin có phù hợp với các hướng dẫn và yêu cầu được chỉ định trong DIN SPEC 3014 hay không.

Công nghệ Stack: Phân tích tổng thể công nghệ stack của Bitcoin, bao gồm cơ sở hạ tầng mạng, phần mềm khách hàng và các đặc tả giao thức. Đánh giá liệu công nghệ stack của Bitcoin có đáp ứng các hướng dẫn và yêu cầu được đề xuất trong DIN SPEC 3014 hay không, đặc biệt là tính đáng tin cậy, khả năng mở rộng, tương tác và bảo mật.

Quản trị công nghệ: Xem xét các khía cạnh quản trị liên quan đến công nghệ và kiến trúc của Bitcoin. Đánh giá cách ra quyết định liên quan đến các thay đổi và nâng cấp công nghệ và liệu có cơ chế để đảm bảo tính minh bạch và tham gia của cộng đồng trong sự tiến hóa của công nghệ.

Bằng cách đánh giá công nghệ và kiến trúc của Bitcoin dựa trên những khía cạnh này và áp dụng các tiêu chí được đề ra trong DIN SPEC 3014, bạn có thể có được cái nhìn về mức độ phù hợp của công nghệ của Bitcoin với các hướng dẫn và yêu cầu được đề xuất và đánh giá tính ổn định, bảo mật và khả năng mở rộng của công nghệ tổng thể của nó.

c. Bảo mật và phục hồi sau sự cố

Thuật toán mật mã: Phân tích các thuật toán mật mã được sử dụng bởi Bitcoin để bảo vệ giao dịch, đảm bảo tính riêng tư và duy trì tính toàn vẹn của blockchain. Đánh giá tính mạnh mẽ và hiệu quả của các thuật toán này trong việc bảo vệ dữ liệu nhạy cảm và kháng các cuộc tấn công mật mã.

Cơ chế đồng thuận: Đánh giá các biện pháp bảo mật có sẵn trong cơ chế đồng thuận của Bitcoin, hiện tại là Proof of Work (PoW). Đánh giá tính kháng lại của cơ chế đồng thuận với các cuộc tấn công đã biết như double spending và 51% attacks. Xem xét liệu cơ chế đồng thuận có phù hợp với các yêu cầu bảo mật được đề xuất trong DIN SPEC 3014 hay không.

Cơ sở hạ tầng mạng: Đánh giá các biện pháp bảo mật được triển khai trong cơ sở hạ tầng mạng của Bitcoin. Điều này bao gồm phân tích các giao thức, kênh truyền thông và quy trình xác thực được sử dụng trong mạng. Đánh giá liệu các biện pháp này

có đảm bảo đủ để bảo vệ khỏi truy cập trái phép, gian lận dữ liệu và các mối đe dọa bảo mật khác hay không.

Bảo mật mã nguồn: Đánh giá các biện pháp bảo mật được triển khai trong mã nguồn của Bitcoin. Đánh giá liệu mã nguồn này có được kiểm định bảo mật định kỳ, đánh giá lỗ hổng và xem xét đồng nghiệp để xác định và khắc phục các điểm yếu bảo mật tiềm ẩn hay không. Xem xét việc sử dụng các thực hành mã hóa an toàn và áp dụng các phương pháp tốt nhất cho việc phát triển phần mềm an toàn.

Khả năng ứng phó sự cố: Xem xét khả năng phản ứng của mạng Bitcoin trong trường hợp xảy ra sự cố. Đánh giá các quy trình và cơ chế được triển khai để phát hiện, giảm thiểu và khôi phục khỏi các sự cố bảo mật hoặc gián đoạn mạng. Đánh giá tính ứng phó sự cố đối với các cuộc tấn công, sự cố mạng và các gián đoạn tiềm ẩn khác.

Bằng cách đánh giá tính bảo mật và khả năng kháng cự của Bitcoin dựa trên những khía cạnh này và áp dụng các tiêu chí được đề ra trong DIN SPEC 3014, bạn có thể có được cái nhìn về các biện pháp bảo mật được triển khai trong Bitcoin, khả năng kháng lại các cuộc tấn công và khả năng kháng cự tổng thể của nó đối với các mối đe dọa bảo mật tiềm ẩn. Bạn có thể cung cấp thêm thông tin về DIN SPEC 3014 không?

d. Khả năng tương tác và tương thích

Tiêu chuẩn và giao thức tương thích: Đánh giá mức độ tiêu chuẩn và giao thức tương thích được triển khai bởi Bitcoin. Đánh giá liệu Bitcoin tuân thủ các hướng dẫn được đề xuất trong DIN SPEC 3014 để tích hợp mượt mà với các hệ thống và mạng dựa trên blockchain khác. Xem xét việc sử dụng các định dạng dữ liệu chung, giao thức truyền thông và khả năng tương tác đồng thuận để tạo điều kiện cho tính tương thích.

Tương tác với các blockchain khác: Đánh giá khả năng tương tác của Bitcoin với các nền tảng và hệ thống blockchain khác. Xem xét tính tương thích của Bitcoin với các cơ chế đồng thuận khác nhau, các ngôn ngữ hợp đồng thông minh và định dạng giao dịch được sử dụng bởi các blockchain khác. Đánh giá liệu Bitcoin có thể trao đổi tài sản, dữ liệu hoặc thực hiện các giao dịch qua mạng blockchain khác một cách hiệu quả.

Trao đổi và tích hợp dữ liệu: Đánh giá khả năng trao đổi và tích hợp dữ liệu của Bitcoin với các hệ thống bên ngoài. Xem xét tính dễ dàng trong việc truy cập và lấy dữ

liệu từ blockchain Bitcoin cho các ứng dụng hoặc dịch vụ bên ngoài. Đánh giá tính tương thích của cấu trúc dữ liệu và API của Bitcoin với các tiêu chuẩn và thực hành tốt nhất trong lĩnh vực tương tác dữ liệu.

Tính năng chạy trên nhiều nền tảng: Đánh giá liệu Bitcoin có thể hoạt động hiệu quả trên các hệ điều hành khác nhau, cấu hình phần cứng và môi trường phần mềm khác nhau. Xem xét tính độc lập nền tảng của việc triển khai phần mềm Bitcoin và tính tương thích của nó với các ứng dụng khách và phần mềm ví khác nhau.

Giao tiếp giữa các blockchain: Xem xét các cơ chế và giao thức được sử dụng bởi Bitcoin để hỗ trợ giao tiếp giữa các blockchain. Đánh giá khả năng của Bitcoin để trao đổi thông tin, tài sản hoặc thực hiện các giao dịch an toàn qua các blockchain khác nhau, bao gồm các mạng riêng tư hoặc được cho phép.

Bằng cách đánh giá tính tương thích và tương tác của Bitcoin dựa trên những khía cạnh này và áp dụng các tiêu chí được đề ra trong DIN SPEC 3014, bạn có thể có được cái nhìn về khả năng tương tác của Bitcoin với các hệ thống và mạng dựa trên blockchain khác, cũng như với các ứng dụng bên ngoài, tạo điều kiện cho tính tích hợp và trao đổi dữ liệu trong hệ sinh thái blockchain rộng lớn hơn.

e. Quyền riêng tư và bảo vệ dữ liệu

Tối thiểu hoá dữ liệu: Đánh giá liệu Bitcoin tuân thủ nguyên tắc tối thiểu hoá dữ liệu, có nghĩa là chỉ thu thập và lưu trữ các dữ liệu cần thiết để xác nhận giao dịch và hoạt động mạng. Đánh giá xem Bitcoin có tránh việc lưu trữ dữ liệu không cần thiết để giảm thiểu rủi ro về sự riêng tư không.

Sự đồng thuận của người dùng: Xem xét mức độ mà mô hình giao dịch của Bitcoin tôn trọng sự đồng thuận của người dùng. Đánh giá liệu người dùng có kiểm soát được thông tin cá nhân của mình và liệu có yêu cầu sự đồng ý của họ trước khi tiến hành xử lý hoặc tiết lộ dữ liệu nào hay không.

Xử lý dữ liệu an toàn: Đánh giá các biện pháp mà Bitcoin đã thực hiện để đảm bảo việc xử lý dữ liệu an toàn. Điều này bao gồm đánh giá việc sử dụng các kỹ thuật mã hóa và giao thức truyền thông an toàn để bảo vệ dữ liệu giao dịch khỏi truy cập hoặc gián đoạn trái phép.

Ẩn danh và giả danh: Đánh giá mức độ ẩn danh và giả danh được cung cấp bởi mô hình giao dịch của Bitcoin. Xem xét liệu Bitcoin có cho phép người dùng thực hiện giao dịch mà không tiết lộ danh tính thực sự của họ, từ đó bảo vệ sự riêng tư của họ.

Công nghệ tăng cường sự riêng tư: Đánh giá liệu Bitcoin sử dụng các công nghệ tăng cường sự riêng tư như CoinJoin hoặc Confidential Transactions, nhằm cải thiện sự riêng tư bằng cách che giấu chi tiết giao dịch và tăng cường tính không liên kết giữa các đầu vào và đầu ra giao dịch.

Tuân thủ các tiêu chuẩn về sự riêng tư: Đánh giá sự tuân thủ của Bitcoin với các tiêu chuẩn về sự riêng tư được đề ra trong DIN SPEC 3014. Xem xét liệu Bitcoin tuân thủ các hướng dẫn và yêu cầu được đề xuất trong tiêu chuẩn để đảm bảo bảo vệ và sự riêng tư đủ đáp ứng cho người dùng của nó.

Bằng cách đánh giá tính bảo vệ dữ liệu và sự riêng tư của Bitcoin dựa trên những khía cạnh này và xem xét các tiêu chí được đề ra trong DIN SPEC 3014, bạn có thể đánh giá mức độ bảo vệ dữ liệu và sự riêng tư được cung cấp bởi mô hình giao dịch của Bitcoin và xác định sự tuân thủ của nó với các tiêu chuẩn và thực hành tốt nhất về sự riêng tư.

So sánh ba tiêu chuẩn khi áp dụng đánh giá cho Bitcoin

Tính tương thích:

- WEF_GSMI_Technical_Standards_2020: Đánh giá tính tương thích và khả năng tương tác của Bitcoin với các mạng dựa trên blockchain khác, nhấn mạnh các tiêu chuẩn và giao thức tương thích.
- ISO/TC 307: Đánh giá cách Bitcoin sử dụng công nghệ blockchain và tuân thủ các nguyên tắc và yêu cầu về tính tương thích được chỉ định trong tiêu chuẩn.
- DIN SPEC 3104: Đánh giá tính tương thích và khả năng tương tác của Bitcoin với các hệ thống và mạng dựa trên blockchain khác, xem xét việc tuân thủ hướng dẫn về tính tương thích được cung cấp bởi tiêu chuẩn.

Bảo mật:

- WEF_GSMI_Technical_Standards_2020: Phân tích các tính năng bảo mật của Bitcoin, bao gồm các thuật toán mật mã, cơ chế đồng thuận và khả năng chống lại các cuộc tấn công.
- ISO/TC 307: Đánh giá các biện pháp bảo mật được triển khai trong Bitcoin, bao gồm các thuật toán mật mã, cơ chế đồng thuận và bảo vệ chống lại các cuộc tấn công đã biết.

- DIN SPEC 3104: Phân tích các biện pháp bảo mật được triển khai trong Bitcoin, bao gồm các thuật toán mật mã, cơ chế đồng thuận và bảo vệ chống lại các cuộc tấn công như double spending và 51% attacks.

Sự riêng tư:

- WEF_GSMI_Technical_Standards_2020: Đánh giá mức độ sự riêng tư được cung cấp bởi mô hình giao dịch giả danh của Bitcoin và đánh giá các biện pháp được thực hiện để tăng cường sự riêng tư.
- ISO/TC 307: Xem xét việc tuân thủ của Bitcoin đối với các tiêu chuẩn về sự riêng tư được đề ra trong tiêu chuẩn, bao gồm tối thiểu hoá dữ liệu, sự đồng ý của người dùng và xử lý dữ liệu an toàn.
- DIN SPEC 3104: Đánh giá mức độ bảo vệ dữ liệu và sự riêng tư được cung cấp bởi mô hình giao dịch của Bitcoin và đánh giá việc tuân thủ của nó với các tiêu chuẩn bảo vệ dữ liệu và sự riêng tư được đề ra trong tiêu chuẩn.

Quản trị:

- WEF_GSMI_Technical_Standards_2020: Phân tích mô hình quản trị phi tập trung của Bitcoin, quy trình ra quyết định và sự tham gia của cộng đồng.
- ISO/TC 307: Đánh giá mô hình quản trị của Bitcoin, quy trình ra quyết định và tuân thủ các quy định và yêu cầu pháp lý liên quan.
- DIN SPEC 3104: Đánh giá cấu trúc quản trị của Bitcoin, bao gồm quy trình ra quyết định, cơ chế đồng thuận và sự tham gia của cộng đồng.
- Quản lý dữ liệu:
- WEF_GSMI_Technical_Standards_2020: Đánh giá cấu trúc dữ liệu của Bitcoin, cơ chế lưu trữ, khả năng mở rộng và hiệu quả của quy trình đồng bộ hóa và xác thực dữ liệu.
- ISO/TC 307: Đánh giá cấu trúc dữ liệu của Bitcoin, cơ chế lưu trữ và các giải pháp mở rộng khả dụng phù hợp với các hướng dẫn và khuyến nghị của tiêu chuẩn.
- DIN SPEC 3104: Đánh giá cấu trúc dữ liệu của Bitcoin, cơ chế lưu trữ, khả năng mở rộng và hiệu quả của quy trình đồng bộ hóa và xác thực dữ liệu.

Tuân thủ:

- WEF_GSMI_Technical_Standards_2020: Đánh giá sự tuân thủ của Bitcoin đối với các yêu cầu pháp lý và quy định liên quan, đặc biệt là các quy định chống rửa tiền (AML) và biết khách hàng (KYC).
- ISO/TC 307: Xem xét sự tuân thủ của Bitcoin đối với các yêu cầu pháp lý và quy định liên quan trong các phạm vi pháp lý khác nhau, bao gồm các quy định chống rửa tiền (AML) và biết khách hàng (KYC).
- DIN SPEC 3104: Đánh giá sự tuân thủ của Bitcoin đối với các quy định và yêu cầu pháp lý liên quan, đặc biệt là các nguyên tắc quản trị như minh bạch, trách nhiệm và tính bảo đảm.

Tóm lại, mặc dù có thể có các khu vực đánh giá chồng chéo, mỗi tiêu chuẩn tiếp cận việc đánh giá Bitcoin từ một góc độ khác nhau, nhấn mạnh các tiêu chí và yêu cầu khác nhau. WEF_GSMI_Technical_Standards_2020 cung cấp một khung đánh giá toàn diện bao gồm các khía cạnh khác nhau. ISO/TC 307 tập trung đặc biệt vào công nghệ blockchain và các công nghệ sổ cái phân tán và sự tuân thủ của chúng đối với các nguyên tắc của tiêu chuẩn. DIN SPEC 3104 bao phủ một loạt các khía cạnh, bao gồm quản trị, công nghệ, bảo mật và tính tương thích.

4.2 Đề xuất

XEM XÉT rằng Blockchain và các công nghệ sổ cái phân tán khác (DLT) có thể tạo điều kiện thuận lợi cho việc lưu giữ hồ sơ có thể theo dõi và chuyển giao giá trị và dữ liệu, cũng như các công cụ sáng tạo như "hợp đồng thông minh" và các trường hợp sử dụng tiềm năng, ví dụ như mã hóa tài sản, có thể độc lập hoặc tạo thành một thành phần của các giải pháp công nghệ rộng lớn hơn trên các khu vực tư nhân và công cộng trong các lĩnh vực đa dạng như nhận dạng kỹ thuật số, dịch vụ tài chính, dịch vụ công và chuỗi cung ứng;

XEM XÉT rằng Blockchain có thể có tiềm năng đóng góp vào sự đổi mới, năng suất, khả năng phục hồi, minh bạch, thẩm định trong chuỗi cung ứng, tính toàn vẹn của dữ liệu, cạnh tranh, hợp tác nhiều bên liên quan, trách nhiệm giải trình và đảm bảo một sân chơi bình đẳng, và do đó có thể thúc đẩy niềm tin và sự tự tin vào các tổ chức và thúc đẩy hành vi kinh doanh có trách nhiệm và các Mục tiêu Phát triển Bền vững;

THỪA NHẬN rằng Blockchain mang những hạn chế và rủi ro nhất định, một số trong đó dành riêng cho Blockchain trong khi những người khác có liên quan đến công

nghe kỹ thuật số rộng hơn, ví dụ như rủi ro liên quan đến quyền riêng tư và bảo mật, lưu ký thông tin truy cập và lỗ hổng mật mã;

THỪA NHẬN rằng danh tính kỹ thuật số có thể kiểm chứng của Blockchain là một thành phần của nhiều ứng dụng Blockchain, đồng thời, bản thân Blockchain có thể là một yếu tố hỗ trợ nhận dạng kỹ thuật số có thể kiểm chứng;

THỪA NHẬN rằng các khung chính sách, pháp lý và quy định quốc gia và quốc tế áp dụng cho Blockchain và các ứng dụng của nó và Blockchain và các ứng dụng của nó sẽ cần được đánh giá định kỳ để đảm bảo tính phù hợp, đặc biệt là đối với các Blockchain hoạt động xuyên biên giới;

THỪA NHẬN tầm quan trọng của tính trung lập về công nghệ cả về chính sách, pháp lý và quy định, khuôn khổ, cũng như khi xác định công nghệ và ứng dụng phù hợp và phù hợp nhất để đáp ứng nhu cầu và yêu cầu của một tình huống nhất định;

THỪA NHẬN rằng tư vấn, thu hút và trao quyền cho các bên liên quan là một phần thiết yếu trong việc thúc đẩy niềm tin của công chúng trong việc áp dụng thích hợp các ứng dụng Blockchain;

THỪA NHẬN rằng sự phát triển và ứng dụng nhanh chóng của Blockchain đã tạo ra nhu cầu trên toàn cầu về hướng dẫn chính sách rõ ràng và mạch lạc cho việc đổi mới và áp dụng Blockchain nhằm ngăn ngừa và giảm thiểu rủi ro, đồng thời duy trì các động lực để đổi mới, hợp tác và cạnh tranh, đồng thời tính đến bối cảnh cụ thể của khu vực và quốc gia;

HỖ TRỢ sử dụng bền vững các ứng dụng Blockchain, đồng thời xác định và giảm thiểu mọi tác động tiêu cực đến môi trường;

THỪA NHẬN rằng cách tiếp cận dựa trên giá trị đối với đổi mới và áp dụng Blockchain có trách nhiệm có thể giúp khuyến khích đổi mới, giảm bất bình đẳng kinh tế, xã hội, giới tính và các bất bình đẳng khác, thúc đẩy việc làm chất lượng và an toàn, thúc đẩy tài chính toàn diện, bảo vệ nhà đầu tư và người tiêu dùng, hỗ trợ khả năng phục hồi hệ thống tài chính, cạnh tranh công bằng và toàn vẹn thị trường, trao quyền cho các cá nhân và khuyến khích chuyển đổi công bằng và phát triển kỹ năng, tăng cường bảo mật kỹ thuật số và bảo vệ dữ liệu, xây dựng niềm tin vào nền kinh tế và xã hội số, bảo vệ môi trường tự nhiên và khuyến khích sử dụng năng lượng hiệu quả, từ đó hỗ trợ tăng trưởng bao trùm, hạnh phúc, ứng xử kinh doanh minh bạch và có trách nhiệm, quyền con người và các giá trị cơ bản khác.

4.2.1 Quy định

'**Blockchain**' đề cập đến tất cả các loại công nghệ Blockchain và công nghệ sổ cái phân tán (DLT), bao gồm các lớp giao thức, mạng và ứng dụng. Công nghệ Blockchain và DLT là một phần của hệ sinh thái công nghệ rộng lớn hơn. DLT là sự kết hợp của các công nghệ cùng nhau tạo ra một sổ cái kỹ thuật số, chia sẻ và tự cập nhật các giao dịch hoặc thông tin đã được xác minh giữa các bên trong mạng dựa trên các công nghệ cơ sở dữ liệu tiên tiến, bao gồm cả công nghệ blockchain. DLT sử dụng nhiều loại cơ chế đồng thuận đa bên khác nhau để xác thực và ghi lại các giao dịch và có nhiều hệ thống quản trị khác nhau, từ các mô hình "tập trung" cho đến các trường hợp có thể không có sự kiểm soát của (các) cơ quan trung ương (còn được gọi là "phi tập trung").

'**Các bên liên quan đến Blockchain**' đề cập đến tất cả các tổ chức và cá nhân liên quan đến việc sử dụng, đổi mới liên quan đến hoặc bị ảnh hưởng bởi Blockchain, trực tiếp hoặc gián tiếp, bao gồm nhưng không giới hạn ở chính phủ, doanh nghiệp, công nhân, nhà phát triển, học giả, người tiêu dùng và công dân.

'**Tác nhân Blockchain**' đề cập đến các bên liên quan Blockchain đóng vai trò tích cực trong hệ sinh thái Blockchain, bao gồm cả việc thiết lập các thực tiễn và chính sách, và bao gồm các tổ chức, tập đoàn và cá nhân, bao gồm nhưng không giới hạn ở các chính phủ, phát triển hoặc vận hành Blockchain hoặc các ứng dụng của chúng.

4.2.2 Đổi mới và áp dụng blockchain có trách nhiệm

KHUYẾN NGHỊ rằng các Thành viên và những người không phải là Thành viên đã tuân thủ Khuyến nghị này (sau đây gọi là "Tuân thủ") khuyến khích cách tiếp cận có đạo đức và có trách nhiệm đối với việc đổi mới và áp dụng Blockchain nhằm khai thác các cơ hội và giảm thiểu rủi ro và KÊU GỌI tất cả các Tác nhân Blockchain, phù hợp với vai trò và sự tham gia của họ vào Blockchain, thực hiện cách tiếp cận như vậy, bằng cách:

4.2.2.1 Tuân thủ và gắn kết

Đưa ra các cơ chế để đánh giá và đảm bảo sự tuân thủ và gắn kết của các ứng dụng Blockchain với các yêu cầu chính sách, pháp lý và quy định có liên quan, bao gồm cả những yêu cầu hoạt động xuyên biên giới.

4.2.2.2 Quản trị, minh bạch và trách nhiệm giải trình

Thực hiện các bước sao cho các khung quản trị của Blockchain và các ứng dụng của chúng được minh bạch và được xác định rõ ràng, phù hợp với các nghĩa vụ pháp lý và quy định, bao gồm:

a) Thực hiện cách tiếp cận toàn diện, nhiều bên liên quan để quản trị Blockchain, bao gồm phát triển các biện pháp để đảm bảo trách nhiệm giải trình, bao gồm cả trong trường hợp kết thúc Blockchain hoặc các ứng dụng của nó;

b) Cung cấp sự minh bạch, khi thích hợp, cho các bên liên quan đến Blockchain về việc sử dụng Blockchain, thiết kế và vận hành của họ, khung quản trị của họ, các cơ chế khuyến khích liên quan và về danh tính, vai trò và trách nhiệm của các Tác nhân Blockchain có liên quan đến bất kỳ Blockchain nào, đặc biệt là liên quan đến trách nhiệm giải trình đối với các nghĩa vụ tuân thủ của họ;

c) Thực hiện các đánh giá ban đầu và thường xuyên về Blockchain liên quan đến việc tuân thủ Khuyến nghị này, nhằm xác minh và xác nhận liên tục trong vòng đời của chúng thông qua các phương pháp tiếp cận tương xứng, ví dụ, đánh giá theo thiết kế và thúc đẩy tính minh bạch của kết quả đánh giá đó đến mức tối đa phù hợp, cũng như cung cấp biện pháp khắc phục nếu có; và

d) Tiết lộ bất kỳ thay đổi nào đối với khung quản trị hoặc mã của Blockchain một cách có trách nhiệm và kịp thời.

4.2.2.3 Khả năng tương tác

Tạo điều kiện cho khả năng tương tác của Blockchain, bao gồm thông qua các tiêu chuẩn mở và với các hệ thống không phải Blockchain và với các hệ thống công nghệ thông tin (CNTT) hiện có, để hỗ trợ luồng dữ liệu và cải thiện bảo vệ và kiểm soát cá nhân dữ liệu cá nhân.

4.2.2.4 Bảo mật và quyền riêng tư kỹ thuật số

Cung cấp bảo mật kỹ thuật số và bảo vệ quyền riêng tư trong ứng dụng Blockchain, bao gồm: a) Thực hiện các biện pháp để hiểu và giảm thiểu các rủi ro liên quan đến bảo mật kỹ thuật số và quyền riêng tư liên quan đến Blockchain và các ứng dụng của chúng, bao gồm các rủi ro liên quan đến quản lý danh tính kỹ thuật số, kiểm soát truy cập, quản trị và cơ sở hạ tầng; b) Chịu trách nhiệm quản lý rủi ro, được hỗ trợ

bởi tính liên tục của doanh nghiệp và phù hợp với các tiêu chuẩn bảo mật kỹ thuật số và quyền riêng tư có liên quan và các chức năng quản lý rủi ro, bao gồm bằng cách hành động minh bạch, ví dụ, bằng cách cung cấp các báo cáo kịp thời về các sự cố bảo mật kỹ thuật số bao gồm cả những sự cố ảnh hưởng đến quyền riêng tư; và c) Do các tính năng cụ thể của nhiều Blockchain, bao gồm tính bất biến, tuổi thọ và tính chất phân tán hoặc tập trung của chúng, chỉ thu thập và lưu trữ dữ liệu cá nhân khi thực sự cần thiết cho mục đích dự định của ứng dụng Blockchain và tuân thủ các khung chính sách, pháp lý và quy định có liên quan.

4.2.2.5 Giáo dục và phát triển kỹ năng

a) Thúc đẩy sự hiểu biết về Blockchain và các ứng dụng, lợi ích và rủi ro tiềm năng của nó giữa tất cả các bên liên quan đến Blockchain, bao gồm cả việc ra quyết định diễn ra ở đâu và như thế nào trong các khuôn khổ quản trị phi tập trung và tập trung, và để ngăn chặn sự xuất hiện của khoảng cách kỹ thuật số;

b) Hỗ trợ một môi trường làm việc công bằng và an toàn bằng cách đảm bảo người lao động được thông báo và tư vấn phù hợp về cách triển khai Blockchain tại nơi làm việc của họ; và

c) Nỗ lực cung cấp các cơ hội và đào tạo có liên quan để xây dựng các kỹ năng, cũng như đánh giá tác động tiềm năng và hỗ trợ chuyển đổi công bằng cho những người bị thay thế bởi các ứng dụng Blockchain.

4.2.2.6 Tác động môi trường

Hỗ trợ việc sử dụng bền vững Blockchain, đồng thời xác định và giảm thiểu mọi tác động tiêu cực đến môi trường

4.2.3 Chính sách quốc gia và hợp tác quốc tế

KHUYẾN NGHỊ rằng khi thiết lập hoặc thực hiện các biện pháp chính sách liên quan đến đổi mới và áp dụng Blockchain, có tính đến tầm quan trọng của tính trung lập về công nghệ và phù hợp với các quy định trên, Tuân thủ:

1. Phát triển các phương pháp tiếp cận chính sách phối hợp, cụ thể là:

a) Phát triển một cách tiếp cận tích hợp giữa các cấp chính quyền để giải quyết những thách thức và cơ hội tiềm năng do Blockchain mang lại, khi thích hợp, cho các

nền kinh tế và xã hội rộng hơn, có tính đến giao điểm với các công nghệ khác và các chính sách áp dụng, cũng như ý nghĩa xuyên biên giới của nó; và

b) Xem xét Blockchain như một công cụ tiềm năng để đạt được các mục tiêu chính sách khi thích hợp, bao gồm cả việc cung cấp dịch vụ và quản lý của chính phủ cũng như trong hợp tác quốc tế.

2. Thúc đẩy một môi trường hỗ trợ đổi mới công nghệ, chẳng hạn như nghiên cứu và phát triển Blockchain, với sự hợp tác nhiều bên liên quan (ví dụ: với các khu vực công cộng, tư nhân và học thuật), sẽ cung cấp một môi trường hỗ trợ, trong số những thứ khác, việc sử dụng công nghệ Blockchain của các doanh nghiệp và doanh nhân vừa và nhỏ và sử dụng nó trong cơ sở hạ tầng và cung cấp dịch vụ, khi thích hợp.

3. Phân đầu xây dựng năng lực con người bằng cách hỗ trợ giáo dục và đào tạo cho tất cả các bên liên quan đến Blockchain về các kỹ năng cần thiết để hiểu và làm việc với Blockchain, khi thích hợp, bao gồm hỗ trợ chuyển đổi công bằng cho những người có công việc bị gián đoạn và thay thế.

4. Hỗ trợ môi trường chính sách thuận lợi cho đổi mới công nghệ, cụ thể bằng cách:

a) Thu thập đầu vào đa dạng khi hình thành chính sách công liên quan đến Blockchain dựa trên tính minh bạch và đối thoại đa bên toàn diện; và

b) Phát triển năng lực thể chế và cơ chế kiểm tra các ứng dụng Blockchain tiềm năng nhằm:

- i. đảm bảo sự gắn kết của họ với các yêu cầu chính sách, pháp lý và quy định;
- ii. đánh giá nhu cầu, lợi ích và rủi ro để thích ứng với các yêu cầu đó cũng như các biện pháp kiểm soát quản lý rủi ro đầy đủ và thực hiện các sửa đổi khi cần thiết và phù hợp;
- iii. hỗ trợ, khi thích hợp, nghiên cứu, phát triển và / hoặc triển khai Blockchain, bao gồm thông qua, ví dụ, hộp cát quy định hoặc phòng thí nghiệm đổi mới.

5. Hợp tác quốc tế, cụ thể bằng cách:

a) Làm việc cùng nhau để tiến tới hợp tác toàn cầu trên các khuôn khổ đổi mới và áp dụng Blockchain và do đó khai thác tốt nhất các cơ hội tiềm năng của nó, đồng thời ngăn ngừa hoặc giảm thiểu rủi ro;

b) Làm việc cùng nhau trong OECD và các diễn đàn quốc tế và khu vực khác để thúc đẩy việc chia sẻ kiến thức và tăng cường hợp tác và hợp tác xuyên biên giới trên và thông qua Blockchain và các ứng dụng của nó; và

c) Thúc đẩy các quy trình mở và đa bên liên quan, hướng đến sự đồng thuận và để phát triển các tiêu chuẩn kỹ thuật và đạo đức toàn cầu cho Blockchain và các ứng dụng của nó.

4.2.4 Khuyến nghị chính

Cho rằng các hoạt động thiết lập tiêu chuẩn đang ở giai đoạn đầu, có nhiều ẩn số. Tuy nhiên, điều quan trọng là phải lập kế hoạch chủ động để đảm bảo rằng các sáng kiến thiết lập tiêu chuẩn khuyến khích triển khai blockchain có trách nhiệm.

Đối với tất cả các tác nhân, điều quan trọng là việc sử dụng blockchain và các nỗ lực tiêu chuẩn hóa có mục đích rõ ràng. Những người tham gia hệ sinh thái nên xác định các trường hợp sử dụng có giá trị cao của blockchain cho nhu cầu của họ và sau đó xác định nơi các tiêu chuẩn có thể tăng tốc hoặc giải quyết các lỗ hổng trong việc phát triển các giải pháp cho các trường hợp sử dụng đó.

4.2.4.1 Đối với các thực thể thiết lập tiêu chuẩn

Theo nhiều cách, các thực tiễn tốt nhất để tạo và thực hiện các tiêu chuẩn sẽ phản ánh những tiêu chuẩn được sử dụng trong suốt lịch sử lâu dài của việc tạo ra các tiêu chuẩn kỹ thuật. Ví dụ, các nguồn lực hiện đang tồn tại để đánh giá nhu cầu về các tiêu chuẩn (so với việc sử dụng hoặc điều chỉnh một tiêu chuẩn hiện có), nâng cao vai trò của người dùng và các kỹ thuật chung để tạo ra tiêu chuẩn kỹ thuật.

Dựa trên đánh giá, các khuyến nghị cụ thể về DLT bao gồm:

1. Đảm bảo sự phối hợp và hợp tác hơn nữa giữa các tổ chức thiết lập tiêu chuẩn. Như đã xác định trong bài báo này, có cả khoảng trống và chồng chéo trong bối cảnh hiện tại. Điều này có thể được giảm bớt thông qua việc tăng cường hợp tác giữa các thực thể - ví dụ, thông qua hội đồng quản trị hoặc đối thoại hoặc tham vấn định kỳ giữa các nhà lãnh đạo nhóm làm việc. Điều này có thể tạo điều kiện thuận lợi

cho việc liên kết các tiêu chuẩn, bao gồm nhưng không giới hạn ở: 1) thuật ngữ hài hòa và định nghĩa làm việc; 2) trình tự thích hợp của việc xây dựng tiêu chuẩn; và 3) giảm thiểu dư thừa và tối đa hóa tiềm năng thúc đẩy khả năng tương tác.

Cho đến nay, phần lớn sự hợp tác này là trên cơ sở song phương, chẳng hạn như quan hệ đối tác giữa Hyperledger và Ethereum Enterprise Alliance, hoặc thông qua tư cách thành viên chung trong các ủy ban thiết lập tiêu chuẩn hoặc các nhóm làm việc. Hướng tới một cách tiếp cận phối hợp hơn sẽ rất quan trọng trong việc chủ động xác định các ưu tiên chiến lược cho hệ sinh thái cũng như xác định các quy trình tạo và xem xét phù hợp.

Ví dụ, một sáng kiến lập bản đồ tiêu chuẩn như bài báo này có thể được thực hiện bởi một cơ quan như vậy và được cập nhật thường xuyên để tăng tính minh bạch và giao tiếp giữa các tổ chức thiết lập tiêu chuẩn.

2. Xác định và chỉ định nơi các cuộc trò chuyện về tiêu chuẩn hóa có thể là sớm - và nơi các tiêu chuẩn chính thức là không cần thiết. Có thể có những khía cạnh kỹ thuật của DLT chưa đủ trưởng thành để tiêu chuẩn hóa. Tiến tới tiêu chuẩn hóa quá sớm có thể kìm hãm sự đổi mới hoặc dẫn đến các ưu đãi sai lệch hoặc bất lợi. Như vậy, khung thời gian trong đó các tiêu chuẩn được phát triển là rất quan trọng. Điều quan trọng là phải cẩn thận xem xét các khía cạnh này có thể là gì và xác định dòng thời gian dự kiến để xem xét lại các chủ đề.

Trong việc xác định một lộ trình tiềm năng, các cuộc trò chuyện về sự phát triển của công nghệ và phát triển các tiêu chuẩn tương ứng có thể tiếp tục song song. Khi công nghệ phát triển, các thực thể thiết lập tiêu chuẩn có thể chọn cách tiếp cận dựa trên nguyên tắc - đầu tiên xác định các nguyên tắc cấp cao, sau đó ban hành hướng dẫn liên quan. Cuối cùng, các tiêu chuẩn có thể được quy định rõ hơn và hệ thống hóa tại thời điểm các khía cạnh kỹ thuật đã đạt đến độ chín đủ.

Đồng thời, có thể có các khía cạnh kỹ thuật mà thị trường sẽ giải quyết. Nhiều điều có thể học được từ sự phát triển của internet trong việc đánh giá nơi cần can thiệp và không cần thiết.

3. Đảm bảo rằng ngôn ngữ và mục đích sử dụng là chính xác. Như đã nêu, vẫn còn tranh luận về các lựa chọn thuật ngữ và thiết kế kỹ thuật chính trong hệ sinh thái DLT. Do đó, điều quan trọng là phải đảm bảo rằng các tiêu chuẩn nêu rõ đối tượng và ý định dự định của họ càng rõ ràng càng tốt - ví dụ: xác định lớp có liên quan trong

ngăn xếp công nghệ hoặc, khi thích hợp, (các) giao thức hoặc (các) ngành dọc nào đang được giải quyết trong một nỗ lực tiêu chuẩn hóa cụ thể.

Ngoài ra, trong trường hợp tiêu chuẩn hóa trên các định nghĩa làm việc không được thực hiện trong thời gian tới, điều quan trọng là các tiêu chuẩn thiết lập đó phải minh bạch về các định nghĩa được sử dụng làm cơ sở cho các hoạt động của đơn vị.

4. Chủ động lập kế hoạch cho vai trò của phân cấp trong việc xây dựng và thực hiện các tiêu chuẩn - và đổi mới cho phù hợp. Những người sản xuất các tiêu chuẩn DLT sẽ cần phải xem xét ý nghĩa của quản trị phi tập trung đối với việc tạo và thực hiện các tiêu chuẩn. Ví dụ, nhiều giao thức phi tập trung thực hiện các thay đổi thông qua các đề xuất cải tiến dựa trên cộng đồng. Quá trình này khác nhau về mặt kiến trúc và người tham gia từ việc thực hiện các tiêu chuẩn kỹ thuật được quản lý tập trung.

Do đó, các tiêu chuẩn kỹ thuật nên được thiết kế với việc thực hiện trong tâm trí - chủ động xác định nơi có thể có thách thức hoặc thích ứng trong mô hình truyền thống. Ví dụ: Có bước mới nào trong việc tạo và triển khai nên thêm không? Có cộng đồng nhà phát triển cụ thể nào mà nên tham gia không – và bằng cách nào? Làm thế nào có thể giải thích cho sự hội tụ với các công nghệ Cách mạng công nghiệp lần thứ tư khác?

5. Tiếp tục tìm kiếm đầu vào đa dạng trong việc phát triển và triển khai các tiêu chuẩn. Nhiều cơ quan xây dựng tiêu chuẩn cho phép xem xét công khai các tiêu chuẩn được soạn thảo, và một loạt các quốc gia và lĩnh vực tổ chức đang được đại diện trong việc phát triển các tiêu chuẩn DLT. Đảm bảo sự đại diện đa dạng là rất quan trọng để duy trì tính toàn vẹn của các tiêu chuẩn - tạo ra một quy trình mà các tiêu chuẩn không được thiết kế theo hình ảnh của các sản phẩm, triết lý hoặc lợi ích địa chính trị cụ thể.

Cho rằng các tổ chức thiết lập tiêu chuẩn chủ yếu có trụ sở tại châu Âu và Bắc Mỹ, các khu vực địa lý khác phải được đưa vào một cách thận trọng và cẩn thận. Ngoài ra, điều quan trọng là phải xem xét các quan điểm từ nhiều lĩnh vực chuyên môn, bao gồm mật mã và kinh tế cũng như người tiêu dùng. Bước đầu tiên hướng tới mục tiêu này có thể là đo lường và xác định bất kỳ khoảng trống nào trong đại diện.

6. Giáo dục ngành công nghiệp và các nhà hoạch định chính sách về các kỹ thuật tốt nhất để thực hiện các tiêu chuẩn. Với sự non trẻ của DLT, các tiêu chuẩn có tiềm năng định hình tương lai của công nghệ trên cả hai mặt sản phẩm và chính

sách. Tuy nhiên, hiệu quả của các tiêu chuẩn cuối cùng sẽ phụ thuộc vào cách chúng được hiểu và thực hiện.

Các tổ chức thiết lập tiêu chuẩn nên theo dõi việc triển khai và tạo điều kiện thuận lợi cho việc tạo ra các công cụ hoặc tài nguyên thân thiện với người dùng để thực hiện các tiêu chuẩn. Ví dụ, các cơ quan thiết lập tiêu chuẩn có thể tạo ra các hướng dẫn từng bước và / hoặc nắm bắt các nghiên cứu điển hình để minh họa vai trò của các tiêu chuẩn kỹ thuật trong thực tế.

4.2.4.2 Đối với đơn vị áp dụng tiêu chuẩn kỹ thuật

1. Chủ động mở rộng mức độ tương tác mong muốn với việc thiết lập tiêu chuẩn. Như đã nêu trong bài báo, có một số cơ chế để đóng góp hoặc bình luận về phát triển tiêu chuẩn. Các đơn vị nên chủ động xác định chiến lược tham gia (hoặc không) vào các hoạt động này. Điều này có thể bao gồm, nhưng không giới hạn, xác định các chủ đề hoặc lĩnh vực ảnh hưởng mong muốn, tham gia các nhóm hành động cụ thể của ngành hoặc chỉ định các chuyên gia kỹ thuật cho các nhóm làm việc trong giai đoạn đầu.

Tính toán lợi tức đầu tư sẽ khác nhau; Tuy nhiên, các thực thể nên tuân theo các hoạt động thiết lập tiêu chuẩn đang diễn ra để duy trì thông tin về bối cảnh đang phát triển ở mức tối thiểu. Các thực thể không theo dõi hoạt động này có thể bị bỏ lại phía sau trong những phát triển quan trọng, chẳng hạn như những phát triển liên quan đến mật mã, bảo mật hoặc khả năng tương tác

2. Phối hợp với các tổ chức khác để thiết lập chương trình nghị sự cho việc thiết lập tiêu chuẩn. Như đã chứng minh trong suốt bài báo, việc phát triển các tiêu chuẩn blockchain là sự kết hợp của các đề xuất chủ động và phản hồi đối với các nhu cầu hoặc nhu cầu cụ thể của ngành. Như vậy, các tổ chức có thể được hưởng lợi từ việc tham gia hoặc học hỏi từ một tập đoàn công nghiệp. Các hệ sinh thái có cách tiếp cận hợp tác có khả năng xác định những khoảng trống có giá trị cao nhất trong cảnh quan và địa điểm thích hợp nhất cho bài tập thiết lập tiêu chuẩn. Hơn nữa, cách tiếp cận này có thể giúp giảm thiểu sự dư thừa và cho phép một bộ tùy chọn mạnh mẽ cho người tiêu dùng.

3. Xác định quy trình ra quyết định và thông qua. Do sự khác biệt trong kiến trúc kỹ thuật và quản trị trên DLT, việc thực hiện các tiêu chuẩn sẽ khác nhau rất nhiều

giữa các thực thể. Các tổ chức nên chủ động quét và hiểu hoạt động diễn ra trong bối cảnh tiêu chuẩn để lập kế hoạch và quản lý việc thực hiện mong muốn. Điều này sẽ đảm bảo rằng các bước thích hợp được thực hiện không chỉ về mặt kỹ thuật, mà còn về mặt quản lý thay đổi và ra quyết định chiến lược.

Như đã thảo luận, các tiêu chuẩn có thể sẽ đóng góp vào các tính năng chính của công nghệ, bao gồm khả năng tương tác và khả năng mở rộng ngoài khả năng mở khóa các sản phẩm và thị trường mới. Những tổ chức không có chiến lược có thể bị bỏ lại phía sau.

Các tiêu chuẩn rất quan trọng đối với việc hỗ trợ các tính năng quan trọng của DLT, chẳng hạn như khả năng tương tác và khả năng mở rộng. Một bộ tiêu chuẩn mạnh mẽ có tiềm năng mở khóa các sản phẩm và thị trường mới như một phần của hệ sinh thái lớn hơn. Tuy nhiên, những nỗ lực hiện nay vẫn còn thiếu sự rõ ràng, đại diện và phối hợp đúng đắn. Nhận ra những rào cản này là bước đầu tiên để vượt qua chúng. Các thực thể thiết lập tiêu chuẩn phải đa dạng và chủ động, và cố gắng tạo ra nhận thức và hiểu biết. Các thực thể áp dụng tiêu chuẩn cũng phải thực hiện phần việc của mình bằng cách tham gia vào quá trình phát triển tiêu chuẩn và rất quan trọng trong việc lựa chọn của họ. Cùng với nhau, một quỹ đạo tích cực cho DLT có thể được thiết lập và tiềm năng của nó được nhận ra.

KẾT LUẬN

Trong bài báo cáo này, chúng em đã tiến hành nghiên cứu về một số tiêu chuẩn trong triển khai ứng dụng Blockchain và đề xuất một số tiêu chuẩn và tiêu chí cốt lõi mà một ứng dụng Blockchain trong thực tế cần tuân thủ. Các tiêu chuẩn và tiêu chí này đóng vai trò quan trọng trong việc đảm bảo tính tin cậy, bảo mật và hiệu quả của ứng dụng Blockchain.

Trước hết, chúng em đã tổng quan về các vấn đề liên quan đến tiêu chuẩn Blockchain. Chúng em đã trình bày các tiêu chuẩn quan trọng bao gồm Tiêu chuẩn WEFF_GSMI_Technical_Standard_2020, Tiêu chuẩn blockchain ISO/TC 307 và Tiêu chuẩn blockchain DIN_SPEC 3104. Mỗi tiêu chuẩn đều có phạm vi và ưu điểm riêng, và chúng em đã phân tích, so sánh và đánh giá từng tiêu chuẩn để hiểu rõ hơn về ưu điểm và ứng dụng của chúng.

Tiếp theo, chúng em đã đề xuất một số tiêu chuẩn và tiêu chí cốt lõi mà một ứng dụng Blockchain trong thực tế cần tuân thủ. Bằng cách xem xét các yếu tố như bảo mật, khả năng mở rộng, tính tương thích và khả năng tương tác với các hệ thống khác, chúng em đã nhận thức được những yếu tố quan trọng để đảm bảo tính tin cậy và hiệu quả của ứng dụng Blockchain. Những tiêu chuẩn và tiêu chí này giúp xác định các yêu cầu cần thiết và hướng dẫn cho việc triển khai thành công một ứng dụng Blockchain trong thực tế.

Qua việc tuân thủ các tiêu chuẩn và tiêu chí cốt lõi này, một ứng dụng Blockchain có thể đạt được những lợi ích quan trọng. Đầu tiên, tính bảo mật được đảm bảo, giúp ngăn chặn các cuộc tấn công và đảm bảo an toàn thông tin. Thứ hai, khả năng mở rộng cho phép ứng dụng mở rộng quy mô một cách linh hoạt để đáp ứng nhu cầu ngày càng tăng. Thứ ba, tính tương thích và khả năng tương tác giữa các hệ thống khác nhau tạo điều kiện thuận lợi cho việc kết nối và tích hợp với các ứng dụng và dịch vụ khác. Điều này giúp tạo ra một hệ sinh thái Blockchain phong phú và đa dạng, đồng thời tăng cường khả năng tương tác và hợp tác giữa các bên liên quan.

Tuy nhiên, chúng em nhận thấy rằng công nghệ Blockchain vẫn đang tiếp tục phát triển và tiến hóa. Do đó, các tiêu chuẩn và tiêu chí cốt lõi cần được cập nhật và điều chỉnh theo sự thay đổi của môi trường kỹ thuật và yêu cầu của người dùng. Sự hợp tác và giao lưu giữa các tổ chức, cộng đồng và các chuyên gia trong lĩnh vực

Blockchain là rất quan trọng để xây dựng và duy trì các tiêu chuẩn chất lượng cao và phù hợp với thực tế.

Tổng kết lại, việc nghiên cứu và tuân thủ các tiêu chuẩn trong triển khai ứng dụng Blockchain đóng vai trò quan trọng trong việc đảm bảo tính tin cậy, bảo mật và hiệu quả của công nghệ này. Chúng em hy vọng bài báo cáo này đã góp phần vào việc khám phá và thảo luận về vai trò của các tiêu chuẩn trong việc phát triển và triển khai các ứng dụng Blockchain. Chúng em tin rằng việc tuân thủ các tiêu chuẩn và tiêu chí cốt lõi đề xuất sẽ giúp tạo ra một môi trường tin cậy và khung làm việc chung cho sự phát triển bền vững của công nghệ Blockchain.

Chúng em xin chân thành cảm ơn sự quan tâm và đồng hành của quý thầy cô trong việc nghiên cứu và đọc bài báo cáo này. Hy vọng rằng nội dung của bài báo cáo đã cung cấp cái nhìn sâu hơn về vai trò và ứng dụng của tiêu chuẩn trong việc triển khai ứng dụng Blockchain trong thực tế. Chúng em mong rằng thông qua việc tuân thủ các tiêu chuẩn và tiêu chí cốt lõi, ứng dụng Blockchain sẽ trở thành một công nghệ mạnh mẽ và đáng tin cậy, mang lại nhiều lợi ích cho xã hội và kinh tế.

TÀI LIỆU THAM KHẢO

- [1] World Economic Forum (08/2020), *Global Standards Mapping Initiative: An overview of blockchain technical standards*
- [2] ISO/TC 307 (2016), *Blockchain and distributed ledger technologies*
- [3] RON, EYAL, *A survey of blockchain notary services*, 2018. Cryptom Technologies. Available from: <http://blog.cryptom.eu/?p=23>
- [4] ISO/IEC 2382:2015, *Information technology — Vocabulary*
- [5] ETSI TS 119 142-3 V1.1.1 (2016-12), *Electronic Signatures and Infrastructures (ESI); PAdES digital signatures; Part 3: PAdES Document Time-stamp digital signatures (PAdES-DTS)*
- [6] DIN SPEC 16597:2018-02, *Terminologie für Blockchains*
- [7] IEC 61499-1:2012, *Function blocks - Part 1: Architecture*
- [8] ISO/IEC 27000, *Information technology - Security techniques - Information security management systems - Overview and vocabulary*
- [9] ISO/IEC 27001, *Information technology - Security techniques - Information security management systems - Requirements*
- [10] ISO/IEC 27002, *Information technology - Security techniques - Code of practice for information security controls*
- [11] ISO/IEC 27003, *Information technology - Security techniques - Information security management systems - Guidance*
- [12] ISO/IEC 27004, *Information technology - Security techniques - Information security management - Monitoring, measurement, analysis and evaluation*
- [13] ISO/IEC 27005, *Information technology - Security techniques - Information security risk management*
- [14] NARAYANAN, ARVIND, BONNEAU, JOSEPH, FELTEN, EDWARD, MILLER, ANDREW, GOLDFEDER, STEVEN, *Bitcoin and Cryptocurrency Technologies: A Comprehensive Introduction.*, Princeton University Press, 2016
- [15] NAKAMOTO, S., *Bitcoin: A Peer-to-Peer Electronic Cash System*, 2008. Available from: <https://bitcoin.org/bitcoin.pdf>

- [16]Bitcoin.it, *Confirmation*, [viewed on: October 30, 2018]. Available from:
<https://en.bitcoin.it/wiki/Confirmation>
- [17]Bitcoin.org, *Bitcoin Developer Guide* [viewed on October 30, 2018]. Available from: <https://bitcoin.org/en/developer-guide#term-proof-of-work>
- [18]Bitcoin.it, *Difficulty* [viewed on October 30, 2018]. Available from:
- [19] <https://en.bitcoin.it/wiki/Difficulty>
- [20]Culubas, *Timejacking & Bitcoin*, 2011. Available
- [21]from: https://culubas.blogspot.com/2011/05/timejacking-bitcoin_802.html
- [22]SZALACHOWSKI, PAWEL, "*Towards More Reliable Bitcoin Timestamps*," Proceedings of Crypto Valley Conference on Blockchain Technology (CVCBT), 2018. Available from:
<https://arxiv.org/abs/1803.09028>
- [23] Organisation for Economic Co-operation and Development (10/06/2022), *Recommendation Of The Council On Blockchain And Other Distributed Ledger Technologies*, Meeting of the Council at Ministerial Level.

PHỤ LỤC

Phân công công việc

Tên thành viên	Phân công công việc
Phạm Anh Minh – AT160148	1. Chương 1. Tổng quan các vấn đề liên quan đến các tiêu chuẩn kỹ thuật Blockchain 2. Chương 4. Đánh giá và đề xuất: Đề xuất 3. Tổng hợp và chỉnh sửa báo cáo, slide
Phạm Công Hưởng – AT160230	1. Chương 3. Tiêu chuẩn DIN SPEC 3104 2. Chương 4. Đánh giá và đề xuất: Đánh giá 3. Thiết kế slide
Trần Nhật Nam – AT16056	Chương 2. Tiêu chuẩn ISO/TC 307