**BLOCKCHAIN VÀ ĐO LƯỜNG PHÁP ĐỊNH :**

**CÁC ỨNG DỤNG VÀ KHẢ NĂNG**

*Wilson S.Melo Jr.*

*Brazinlian National Institute of Metrology, Quality and Technology*

*OIML Boulletin LXII. Number 3. July 2021*

**Tóm tắt**

Blockchain là một công nghệ đang phát triển có tiềm năng to lớn làm nhanh hơn chuyển đổi số của các bộ phận khác nhau. Trong bối cảnh đo lường pháp định, blockchain có thể tác động mạnh đến nhiều áp dụng và hoạt động liên quan đến quản lý thông tin, tự động hóa quy trình làm việc, độ tin cậy của phương tiện đo và hệ thống đo. Ngoài ra, blockchain phụ thuộc vào các thiết bị tiên tri nuôi hệ thống với thông tin từ thế giới bên ngoài. Khi một người xem xét tài sản vật chất, các dụng cụ đo thông minh sẽ trở thành những thiết bị tiên tri này, và kết quả là, blockchain sẽ cần phải có các quy định và hoạt động đo lường pháp định cụ thể. Trong bài báo này, chúng tôi thảo luận về sự phụ thuộc lẫn nhau đó, mô tả các áp dụng tiềm năng và những kết quả nghiên cứu đã công bố. Những chủ đề này là chìa khóa để tạo ra nhận thức khoa học và nhận thức đo lường đối với những áp dụng và những tác động của công nghệ blockchain đến đo lường pháp định trong những năm sắp tới.

**1 Lời nói đầu**

Khái niệm chuyển đổi số trong đo lường liên quan đến quá trình áp dụng và tích hợp ngày càng tăng một tập hợp lớn các công nghệ mới [1]-[8]. Chúng ta gọi chúng là “Công nghệ 4.0”, trong sự tham chiếu rõ ràng tới cuộc cách mạng công nghiệp lần thứ tư và tới các ý tưởng, quá trình, phương pháp và công cụ mới của nó [9]. Thực vậy, Công nghiệp 4.0 là chuyển đổi số của công nghiệp thế kỷ 21 dưới ảnh hưởng của 9 “trụ cột” công nghệ : dữ liệu lớn (big data), điện toán đám mây (cloud computing), tự động hóa robot (robot automation), tích hợp ngang và dọc (horizontal and vertical integration), internet vạn vật (the Internet of Things (IoT)), sản xuất phụ gia (additive manufacturing), thực tế tăng cường (augmented reality), mô phỏng (simulation), và an ninh mạng (cybersecurity). Tuy nhiên, điều đáng chú ý là những công nghệ này cũng đang làm biến đổi các lĩnh vực khác bên cạnh công nghiệp. Điện lưới thông minh (smart grids), giao tiếp xe cộ (vehicular communication) (ví dụ V2V và V2I), y tế điện tử (e-health), và thành phố thông minh (smart cities) là những ví dụ về các hệ thống phức tạp sinh ra từ chuyển đổi số trong sản xuất/phân bố năng lượng, vận chuyển, chăm sóc sức khỏe, và quản lý không gian đô thị [9]. Như vậy chúng ta có thể thấy những công nghệ này đang tạo ra một “xã hội 4.0” đích thực từ khi chuyển đổi số có những áp dụng sâu sắc trong tất cả các hoạt động của con người. Do đó, đo lường pháp định cũng là một mục tiêu của những công nghệ này và sẽ trải qua những thay đổi quan trọng trong nhiều năm sắp tới [7].

Thông tin là nhiên liệu nguyên tố trong chuyển đổi số [7], [9]. Vì vậy, các công nghệ có khả năng quản lý thông tin và tích hợp các công nghệ khác đang nổi lên như là các công cụ hiệu quả và đột phá. Blockchain là một trong những công nghệ này. Trong thập kỷ trước, blockchain đã lôi cuốn sự chú ý của các bên liên quan trong nhiều lĩnh vực khác nhau, chủ yếu là do thành công về mặt diễn đạt như là một nền tảng của tiền điện tử [10]-[13]. Tuy nhiên, blockchain có thể làm nhiều hơn việc quản lý các ví bitcoin. Thực vậy, người ta có thể mô tả blockchain như là một nhà tích hợp thực sự giữa các công nghệ số khác nhau như điện toán đám mây, dữ liệu lớn, và IoT. Các chủ đề sau đây tóm tắt quan niệm này :

+ Áp dụng blockchain dựa vào một mạng lưới thiết bị ngang hàng độc lập làm việc hợp tác chặt chẽ, thường là trong môi trường dựa trên điện toán đám mây.

+ Blockchain làm việc như là các hệ thống lưu trữ dữ liệu tin cậy và không thể thay đổi, như vậy chúng cũng có thể hỗ trợ và củng cố các ứng dụng dữ liệu lớn.

+ Blockchain sử dụng các liên hệ thông minh để tự động hóa quy trình làm việc, cho phép tích hợp ngang và dọc giữa các hệ thống khác nhau.

+ Một trong những đặc điểm chính của blockchain là tạo niềm tin giữa các bên không tin tưởng lẫn nhau, tăng cường an ninh mạng.

Khả năng áp dụng blockchain cho các quá trình chuyển đổi số là không tính đếm được [11], [13]. Trong một khảo sát gần đây về các áp dụng dựa trên cơ sở blockchain, Dai et al. [11] trích dẫn các dự án đang tiến hành trong những lĩnh vực khác nhau ví dụ như mua bán năng lượng, quản lý vòng đời xe, và bảo vệ dữ liệu bệnh nhân trong bệnh viện. Ta có thể nhận thấy tất cả những áp dụng này đều đang mở rộng trong “thế giới mạng” (ở đó thông tin chỉ là một giá trị số hóa) và đang tích hợp trong “thế giới hữu hình” (ở đó thông tin liên quan đến những yếu tố cụ thể và các đại lượng vật lý). Phát hiện này giới thiệu một thách thức mới (và nhiều cơ hội) mà chúng ta có thể tổng hợp trong các trình bày dưới đây :

+ Đo lường pháp định cần blockchain khi mà nhiều quá trình liên quan đến mua bán hàng hóa, sức khỏe con người, an toàn cộng đồng, và môi trường sẽ trở thành những áp dụng dựa trên cơ sở blockchain;

+ Blockchain cần đo lường pháp định hỗ trợ vì nhiều thông tin thế giới-thực đòi hỏi chuyển đổi thành những phép đo các đại lượng vật lý.

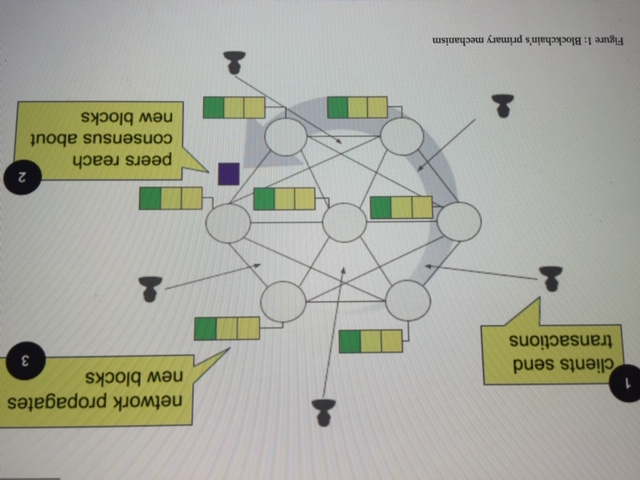
Bài báo này đề xuất một khái niệm là có mối liên hệ cộng sinh có ích giữa đo lường pháp định và blockchain. Chúng tôi trình bày bằng chứng hỗ trợ ý tưởng này bằng cách mô tả một số phát hiện nghiên cứu về các áp dụng dựa trên cơ sở blockchain trong phạm vi liên quan đến các hệ thống đo theo quy định. Những ví dụ này chứng minh blockchain có thể nâng cao các hoạt động đo lường pháp định, giảm chi phí và cải thiện hiệu lực của nó. Hơn nữa, blockchain phụ thuộc vào thông tin tin cậy từ thế giới thực, và các hệ thống đo chịu sự kiểm soát luật pháp là những thiết bị được chỉ định nhiều nhất để lấp đầy khoảng trống này. Chúng tôi kết luận blockchain có thể là một công cụ đặc biệt để làm nhanh chuyển đổi số của đo lường pháp định, đưa các hoạt động của nó tới trình độ công nghệ mới.

**2 Blockchain trong một tóm tắt ngắn gọn**

Ta có thể định nghĩa blockchain như là một cấu trúc dữ liệu chỉ-nối thêm được phân phối (a distributed append-only data structure) (gọi là sổ cái) có thể lưu trữ dữ liệu và phần mềm tự-thực thi gọi là hợp đồng thông minh [10], [11], [13]. Những đặc điểm này tạo cho blckchain không chỉ là một giải pháp lưu trữ mà còn là một nền tảng dịch vụ-định hướng hoàn chỉnh. Hơn nữa, blockchain cung cấp một cơ chế để đạt được sự tin tưởng giữa các bên không tin tưởng lẫn nhau không cần có bên thứ ba được tin tưởng (a third strusted party - TTP). Khía cạnh cuối cùng này dẫn đến hai nguyên nhân chính để chấp nhận blockchain : a) không sẵn có TTP để dùng, hoặc b) chi phí về TTP quá cao [14].

Sự thực hiện blockchain dựa vào mạng lưới người ngang hàng xuất phát từ các tổ chức độc lập đảm bảo độ tin cậy của thông tin. Hình 1 trình bày cơ chế cơ bản của blockchain, bao gồm những khách hàng đang gửi giao dịch tới mạng để thiết lập những giao dịch này vào hộp và tái tạo các hộp này giữa tất cả những người ngang hàng đang tham gia. Quá trình quyết định hộp tiếp theo được gọi là đồng thuận. Mạng cũng đảm bảo thứ tự giao dịch bằng mật mã khớp nối từng hộp tới hộp trước đó, tạo ra “chuỗi các hộp” (“chain of blocks”).

Theo Cachin và Vukolic [10], bốn quy tắc kỹ thuật hoạt động như là nền tảng trong cấu trúc của blockchain là : mật mã, đồng thuận, tái tạo, logic kinh doanh. Mật mã cần thiết để đảm bảo tính xác thực và toàn vẹn của thông tin đối với từng giao dịch



**Hình 1**. *Cơ chế cơ bản của blockchain* *(1) khách hàng gửi các giao dịch; (2) những người ngang hàng đạt được sự đồng thuận về các hộp mới; (3) mạng lan truyền các hộp mới.*

kể từ khi người gửi đánh dấu các yêu cầu của họ, và những người ngang hàng cũng đánh dấu hiệu lực từng hộp. Đồng thuận là vấn đề kinh điển trong khoa học máy tính và nó cần thiết để xác định thứ tự tổng thể của giao dịch và từng nội dung hộp [12]. Tiếp theo, tái tạo là chìa khóa để lan truyền các hộp và đạt được sự nhất quán dữ liệu trong tất cả những người ngang hàng. Cuối cùng, logic kinh doanh đến từ các hợp đồng thông minh, trong thực tế, chúng là các phần mềm được nhúng vào blockchain. Các hợp đồng thông minh cung cấp một cơ chế linh hoạt để tự động hóa quy trình làm việc, áp dụng kinh doanh kiểu blockchain.

Ngày nay, có một sự đa dạng về áp dụng blockchain, chúng ta gọi chúng là các nền tảng (platform) [15],[16]. Chấp nhận một nền tảng blockchain thường là một quyết định khôn ngoan do sự phức tạp của việc áp dụng blockchain từ điểm xuất phát. Tuy nhiên, mỗi nền tảng blockchain có đặc điểm riêng và thậm chí là triết lý hoạt động riêng của nó. Có hai loại nền tảng chính theo phân loại thực tế : blockchain cho phép (hoặc blockchain riêng tư) và blockchain không-cho phép (cũng được gọi là blockchain công cộng) [10],[13]. Hai loại này khác nhau ở chỗ blockchain cho phép cần có sự nhận dạng của người ngang hàng tham gia vào sự đồng thuận, còn blockchain không-cho phép thì không cần. Sự khác nhau này cũng ảnh hưởng đến cơ chế đồng thuận trong mạng. Blockchain cho phép có thể chấp nhận các giao thức đồng thuận dựa vào bỏ phiếu, thường nó thực hiện tốt hơn các giao thức đồng thuận dựa vào bằng chứng. Ngược lại, blockchain không-cho phép tạo thành các nền tảng truy cập-tự do được phân quyền cao và là lý tưởng đối với ví tiền điện tử và các áp dụng đào tạo [10], [12].

Các giao thức đồng thuận dựa vào phiếu bầu phụ thuộc vào số đại biểu theo quy định cần thiết cuả nghững người ngang hàng có khả năng quyết định thứ tự các giao dịch và tạo ra bất kỳ hộp mới nào. Hiện nay, các giao thức đồng thuận chịu-lỗi (fault-tolerant consensus protocols) là sự lựa chọn hứa hẹn nhất, đặc biệt là về độ tin cậy và hiệu suất. Người ta phân loại các giao thức này thành chịu lỗi-sự cố (CFT - crash-fault tolerant) và chịu lỗi-phức tạp (BFT – byzantine-fault tolerant). Trong thực tế, chúng ta có thể nói đồng thuận BFT tin cậy hơn CFT vì BFT bao gồm tất cả các đặc điểm của CFT. Tuy nhiên, BFT cũng phức tạp hơn và chịu đựng được các cuộc tấn công thông đồng của không quá một phần ba những người ngang hàng tích hợp số đại biểu tối thiểu cần thiết đồng thuận, trong khi chịu lỗi CFT chịu đựng được không quá một nửa những người ngang hàng thỏa hiệp.

**3 Vì sao đo lường pháp định lại cần các blockchain**

Sự tin cậy là một yêu cầu thiết yếu trong đo lường pháp định**.** Nó cũng là giao điểm chính xác với công nghệ blockchain. Dù đo lường pháp định có các phương pháp hiệu quả để nhận được những phép đo với độ không đảm bảo thấp, nhưng việc sử lý thông tin kỹ thuật số có thể là một vấn đề khi phép đo và thông tin liên quan đến pháp lý là mục tiêu của các cuộc tấn công mạng của những thực thể độc hại [6], [17], [18].

Các nước có mối quan tâm khác nhau đối với vấn đề an ninh mạng của phương tiện đo. Ví dụ, Mỹ có thể quan tâm đến khủng bố mạng chống lại các cơ sở hạ tầng quan trọng phụ thuộc vào cảm biến và độ tin cậy của máy đo. Các nước khác ở châu Âu thường trao đổi các vấn đề về quyền riêng tư mỗi khi máy đo có thể phát hiện thông tin nhạy cảm của người tiêu dùng. Ở nhiều nước đang phát triển, gian lận đo lường là thách thức chính đòi hỏi hành động liên tục của cơ quan được thông báo. Trong tất cả các lĩnh vực này, blockchain có thể làm tăng đáng kể độ tin cậy của phương tiện đo và bảo vệ phần mềm và các đặc trưng liên quan đến luật pháp.

Mặt khác, chuyển đổi số nhanh trong đo lường pháp định [7] làm tăng đòi hỏi đối với các công nghệ đột phá (disruptive technologies) để giảm độ không đảm bảo và tăng cường bảo vệ phương tiện đo [4], [6]. Như đã thảo luận ở trên, blockchain là một trong số các công nghệ đó và rất khó để không đồng ý với xác nhận này. Tuy nhiên có nhiều câu hỏi và nghi ngờ về việc chúng ta cần phải sử dụng blockchain như thế nào để cải tiến hiệu lực của đo lường pháp định.

Áp dụng dựa trên cơ sở-blockchain phổ biến đầu tiên là Bitcoin [15], được đề xuất năm 2008. Vào thập kỷ trước, blockchain phát triển mạnh mẽ phù hợp với tiền điện tử và chỉ vài năm sau, người ta bắt đầu quan tâm đến việc sử dụng blockchain trong các lĩnh vực khác bên cạnh lĩnh vực tài chính. Năm 2017 chúng tôi đã có công trình kỹ thuật đầu tiên đề xuất việc blockchain có thể giúp cải tiến hoạt động đo lường pháp định [19]. Năm 2018, ấn phẩm độc lập của PTB (Viện đo lường quốc gia Đức và INMETRO (Viện đo lường quốc gia Brazil) đã đề xuất các áp dụng và thực nghiệm thực tế đầu tiên dựa trên cơ sở blockchain cho đo lường pháp định [20], [21]. Trong cùng năm, NIST (Viện đo lường quốc gia Mỹ) đã công bố một báo cáo kỹ thuật về blockchain nhưng không đề xuất bất cứ ứng dụng thực tế nào trong lĩnh vực đo lường [13]. Kể từ đó, những ý tưởng khác nhau đã khám phá ra các thuộc tính của blockchain trong những áp dụng liên quan đến việc quản lý máy đo thông minh, đơn giản hóa phê duyệt mẫu, giám sát hiện trường các thiết bị theo quy định [18], [22]-[24]. Trong các phần sau chúng tôi trình bày tóm tắt những công việc này.

**3.1 Bắt đầu từ những áp dụng thông thường**

Tính năng blockchain cơ bản nhất là dữ liệu được lưu trữ. Hơn nữa, bộ nhớ này được phân phối, phi tập trung và bất biến. Khi người ta xem xét các đặc tính này, ý tưởng đầu tiên là sử dụng blockchain để lưu trữ dữ liệu nhạy cảm thuộc phạm vi kiểm soát pháp luật của phương tiện đo và phép đo [20]. Như vậy, blockchain có thể hoạt động như các kho chứa những tham số liên quan đến luật pháp của máy đo, giấy chứng nhận hiệu chuẩn, và cập nhật phần mềm cho các máy đo thông minh.

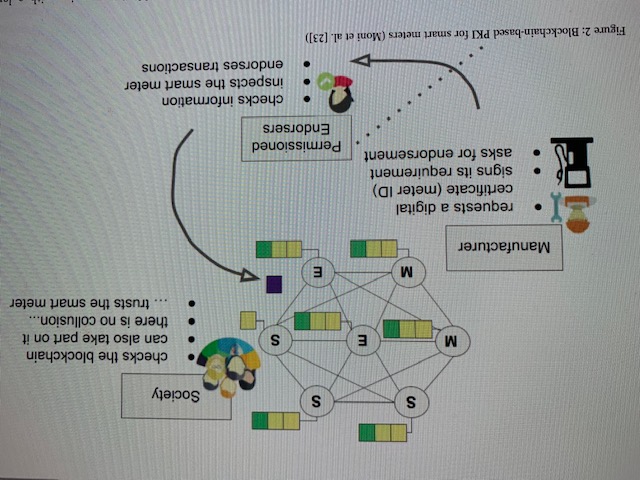
Một sáng kiến thực tế liên quan đến blockchain và đo lường pháp định đã xuất hiện trong phạm vi dự án Đám mây đo lường châu Âu (EMC) [7]. EMC bao gồm một số Viện đo lường quốc gia (NMI) châu Âu và thiết lập một cấu trúc quy chiếu liên quan đến chuyển đổi số trong đo lường. Đề án dự kiến trước sự chấp nhận các blockchain được cấp phép như là một thay thế trong các quy trình kỹ thuật số đòi hỏi sự tin tưởng. Thiel và Wertlich [8] đã đề cập đến việc quản lý các danh tính quản trị và nhật ký sự kiện một cách rõ ràng.

**3.2** **Cơ sở hạ tầng khóa-công khai cho phương tiện đo**

Cơ sở hạ tầng khóa-công khai (PKI - A Public-Key Infrastructure) là một cơ chế để quản lý giấy chứng nhận kỹ thuật số, tạo thành một mô hình giải pháp cổ điển cho các áp dụng sử dụng chỉ thị mật mã chuyên sâu (ví dụ chữ ký kỹ thuật số) [20], [23]. Sự thực hiện truyền thống của nó là phân cấp và tin tưởng vào các Cơ quan chứng nhận (CA - Certification Authorities). Về bản chất, một chức năng của CA là cấp và xác minh giấy chứng nhận kỹ thuật số, nhận thực rằng khóa công khai đã cho là thuộc về thực thể tương ứng.

PKI dựa trên CA thường tốn kém do nhu cầu về quản lý , kiểm tra xác nhận, và sự hủy bỏ giấy chứng nhận kỹ thuật số. Vì vậy, sự áp dụng truyền thống có thể không phù hợp trong trường hợp với số lượng lớn thiết bị giá thấp (ví dụ thiết bị IoT và phương tiện đo). Ngược lại, PKI dựa trên blockchain có thể tạo thành một sự thay thế rẻ hơn để cung cấp các dịch vụ tương tự không phụ thuộc vào các CA [23]. Trong PKI dựa trên blockchain, nếu một thiết bị có khóa công khai được lưu giữ trong sổ cái, những người tham gia khác có thể tiếp cận nó và kiểm tra tính xác thực và toàn vẹn của mọi thông tin được đánh dấu. Hơn nữa, sổ cái không thể thay đổi cung cấp tính không thể bác bỏ được mà không cần chứng chỉ kỹ thuật số.

Hình 2 mô tả một cấu trúc PKI dựa trên blockchain được áp dụng bởi Moni và cộng sự [23]. Trong đề nghị của họ, những người chứng thực được phép (ví dụ các cơ quan khai báo) chịu trách nhiệm kiểm soát mọi phương tiện đo mới, tách ra khóa công khai của nó, và đưa nó vào blockchain. Một khi khóa công khai ở đó, phương tiện có thể đánh dấu bất kỳ thông tin liên quan luật pháp nào bằng cách sử dụng khóa riêng tương ứng. Mọi thực thể tiếp cận blockchain có thể viện dẫn một hợp đồng thông minh để kiểm tra chữ ký này mà không cần đến CA hoặc bất kỳ TTP nào.



**Hình 2 :** *PKI dựa trên blockchain cho máy đo thông minh (****Nhà sản xuất*** *: \*yêu cầu một giấy chứng nhận kỹ thuật số (sự nhận dạng máy đo); \*đánh dấu yêu cầu của nó; \*yêu cầu sự chứng thực.* ***Người chứng thực được phép*** *: \*kiểm soát thông tin; \* kiểm tra máy đo thông minh; \*chứng thực hợp đồng.* ***Xã hội :*** *\*kiểm soát blockchain; \*cũng có thể tham gia vào nó; \*không có sự thông đồng…; … tin tưởng máy đo thông minh)*

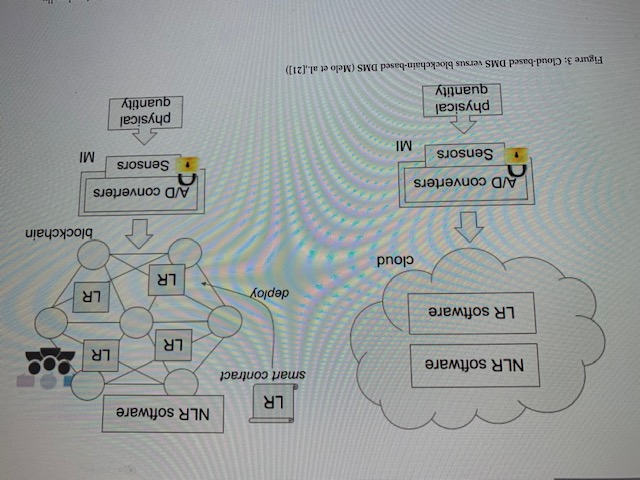
Loại áp dụng này có thể là cần thiết đối với máy đo thông minh. Các phương tiện khác đã sử dụng mật mã khóa công khai để đảm bảo tính toàn vẹn và tính xác thực của các phép đo và dữ liệu liên quan luật pháp. Tuy nhiên, không có chứng chỉ kỹ thuật số, người ta không thể xác nhận tính không thể bác bỏ được của phép đo do phương tiện đo được luật pháp kiểm soát thực hiện. PKI dựa trên blockchain có thể thu hẹp khoảng cách này một cách thiết thực và hiệu quả.

**3.3 Các hệ thống đo phân tán**

Hiện nay một số công trình đã đưa ra các giải pháp sử dụng tài nguyên tính toán từ xa để chạy phần mềm liên quan luật pháp trong các áp dụng đo lường [21], [25]. Chúng ta đặt tên cho loại phương tiện này là các Hệ thống đo phân tán (DMS - Distributed Measuring System). DMS có các đặc trưng lý thú khi so sánh với cấu trúc của phương tiện đo truyền thống. Nó làm giảm độ phức tạp của việc đánh giá phần mềm trong khi cho phép các nhà sản xuất tận dụng công nghệ tính toán hiện đại (ví dụ tính toán đám mây và ảo hóa).

DMS sử dụng blockchain thậm chí tạo ra nhiều hơn các khả năng mới : người ta có thể áp dụng phần mềm liên quan đến luật pháp như là các hợp đồng thông minh, biến blockchain thành một công cụ bảo vệ phần mềm. Hơn nữa, blockchain có thể giảm chi phí liên quan đến việc giám sát đo lường các máy đo, bao gồm việc giám sát tiếp thị và giám sát hiện trường [21].

Hình 3 tóm tắt so sánh giữa DMS dựa trên đám mây như được mô tả theo Opperman et al. [25] và DMS dựa trên blockchain được áp dụng theo Melo et al. [21].



**Hình 3 :** *DMS dựa trên đám mây so với DMS dựa trên blockchain (Melo et al.[21])*

Về bản chất, cả hai có cùng cấu trúc liên quan đến việc dựa vào một máy đo thông minh rất nhỏ để tập hợp dữ liệu thô, đánh dấu chúng và gửi chúng đến blockchain. Sự khác biệt xảy ra sau khi máy đo gửi dữ liệu. Đám mây xử lý dữ liệu và cung cấp các phép đo sử dụng modul phần mềm liên quan đến luật pháp (LR) và không liên quan đến luật pháp (NLR) được lắp đặt như một dịch vụ đám mây nhưng vẫn chịu sự kiểm soát của một thực thể cụ thể (tức là người sở hữu dịch vụ đám mây). Ngược lại, DMS dựa trên blockchain áp dụng phần mềm LR và NLR như là các hợp đồng thông minh. Sự ngang hàng khác nhau từ các tổ chức độc lập thực hiện các hợp đồng thông minh như nhau (thủ tục này là một phần của dự phòng blockchain) và phải đồng ý về kết quả đo chính xác. Hơn nữa, các hợp đồng thông minh được viết trong sổ cái, đảm bảo tính nguyên vẹn của nó và chống lại sự xáo trộn.

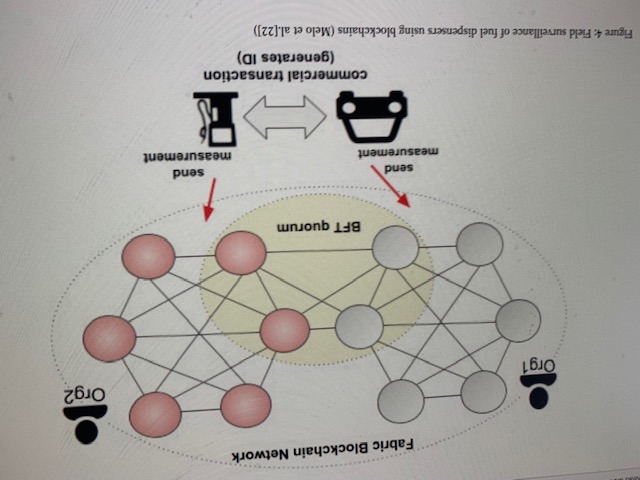
DMS dựa trên blockchain làm việc như sau. Nhà sản xuất cài đặt phương tiện đo của mình từ hai modul cơ bản : một modul phần cứng an toàn cảm nhận đại lượng vật lý và gửi nó đến blockchain theo hình thức một giao dịch, và một hợp đồng thông minh cài đặt phép tính đo lường (thường được thực hiện bằng một phần mềm liên quan luật pháp). Sau khi xử lý với phê duyệt loại cho cả hai modul, cơ quan được thông báo viết một hợp đồng thông minh trên blockchain, vì vậy bất cứ modul phần cứng nào đang sử dụng đều có thể gửi giao dịch của nó. Blockchain có trách nhiệm thực hiện một phép tính đo lường trọn vẹn. Nó cũng đảm bảo tính toàn vẹn phần mềm vì mã trở thành một hợp đồng thông minh bất biến, có liên quan về mặt pháp lý trong sổ cái.

**3.4 Cập nhật phần mềm liên quan pháp lý**

Nhà sản xuất phát triển phần mềm liên quan pháp lý cho các phương tiện chịu sự kiểm soát pháp lý cần đệ trình từng phiên bản phần mềm mới cho quá trình phê duyệt loại. Nhà thiết kế phần mềm có thể tận dụng các cơ chế khác nhau đảm bảo để thiết bị đo chỉ nhận phiên bản phần mềm được phê duyệt đúng đắn. Tuy nhiên, blockchain có thể tạo ra một giải pháp hữu hiệu [20]. Trong áp dụng này, nhà sản xuất lập trình các thiết bị đo của mình để tìm (và chỉ chấp nhận) các cập nhật phần mềm được công bố trên blockchain. Cơ quan được thông báo có trách nhiệm tải lên blockchain mọi phiên bản phần mềm mới. Trong lúc ấy, người sử dụng thiết bị đo có thể theo dõi các cập nhật phần mềm và kiểm tra thiết bị của họ xem có phù hợp với phiên bản được phê duyệt gần nhất không.

**3.5 Giám sát hiện trường bằng cách sử dụng blockchain**

Thật đáng tiếc, sự gian lận trong đo lường là một thực tế phổ biến, và vấn đề xuất hiện chủ yếu là do thu nhập có lãi mà thực thể độc hại có thể kiếm được [6], [26]. Nhiều khi sự gian lận là rất tinh vi về tài nguyên và hành vi lén lút [17].



**Hình 4** : *Giám sát hiện trường máy rút nhiên liệu sử dụng blockchain*

Máy rút nhiên liệu là một ví dụ điển hình về sự gian lận mà các thực thể độc hại thông đồng với nhau và thậm chí có thể làm hư hỏng các đại lý của cơ quan được thông báo. Leitao et al. [17] phân tích độ tin cậy của các máy rút nhiên liệu ở Brazil và mô tả hơn 20 chiến lược gian lận điện tử khác nhau, hầu hết trong số đó là phần cứng để phát hiện và phơi bày ngay cả bởi các kỹ thuật viên có kinh nghiệm. Ngoài ra, Rodrigues Filho và Goncalves [26] đánh giá chỉ riêng ở Brazil, gian lận trong đo nhiên liệu làm xã hội thất thoát tới 300 triệu USD mỗi năm.

Một trong các công việc của chúng tôi hiện nay là sử dụng blockchain như là một công cụ để cải tiến giám sát hiện trường các máy rút nhiên liệu [22]. Ý tưởng cốt lõi đằng sau đề xuất này là để thu hút các thực thể khác nhau vào những hoạt động giám sát đo lường. Blockchain phục vụ như là một nền tảng tin cậy để lưu trữ thông tin từ các nguồn khác nhau. Ví dụ, người ta mong đợi máy rút nhiện liệu đăng nhập mọi sự kiện nạp lại vào blockchain. Nhưng người lái xe có thể làm như thế bằng cách sử dụng cảm biến gắn vào xe cộ để thiết lập lượng nhiên liệu ở mỗi lần nạp lại. Dù những cảm biến này không đủ chính xác và tin cậy, nhưng thông tin của chúng trở thành rất có ích sau một số lớn các sự kiện. Hơn nữa, các thực thể tham gia như là các bên liên quan trong blockchain có thể thực hiện việc phân tích thống kê bằng cách áp dụng các hợp đồng thông minh. Blockchain cung cấp sự bảo vệ quan trọng chống lại các cuộc tấn công thông đồng, điều này ngăn chặn nhiều hành vi gian lận. Hình 4 trình bày dự kiến áp dụng của chúng tôi sử dụng nền tảng Hyperledger Fabric và đồng thuận BFT.

**3.6 Quản lý thử nghiệm thành thạo**

Thử nghiệm thành thạo (PT - Proficiency Testing) là phương pháp đánh giá việc thực hiện của một tập hợp các bên tham gia - thường là các phòng thí nghiệm hoặc các thực thể thực hiện thử nghiệm đo lường – dựa trên chuẩn mực được thiết lập trước. Chúng là một công cụ đặc biệt để kiểm tra năng lực được chứng minh bởi các phòng thí nghiệm này trong việc tiến hành các phép thử, thí nghiệm, và thực nghiệm.

Blockchain có thể cung cấp một nền tảng hiệu quả để quản lý PT bằng cách tự động hóa việc thực hiện quá trình đánh giá và cung cấp sự lưu trữ thông tin an toàn. Chúng ta có thể thực hiện áp dụng này như sau. Người tổ chức PT (tức tổ chức chịu trách nhiệm điều hành PT) công bố một khóa mật mã công khai trên blockchain. Từng thành viên tham gia tạo ra các kết quả so sánh lẫn nhau của mình, mã hóa các phép đo tương ứng bằng cách sử dụng khóa công khai của người tổ chức, và viết chúng lên blockchain. Sau bước này, những người tham gia không thể thay đổi bất kỳ phép đo nào của họ nữa. Ngay khi tất cả các bên tham gia đã cung cấp các phép đo (mã hóa) của họ, người tổ chức công bố khóa riêng. Hành động này khởi phát một hợp đồng thông minh giải mã tự động các phép đo của từng bên tham gia và tính toán kết quả PT cuối cùng. Ngoài ra, kết quả này có thể trải qua đánh giá ở mọi thời điểm từ khi sổ cái lưu giữ vĩnh viễn tất cả thông tin có ảnh hưởng tới nó.

**4 Vì sao blockchain cần có đo lường pháp định**

Dù hầu hết mọi người hiểu rõ vì sao blockchain cần thiết cho đo lường pháp định, số ít người phát hiện điều ngược lại cũng là đúng : blockchain cần có đo lường pháp định. Sự phụ thuộc này sẽ trở thành rõ ràng hơn trong những năm sắp tới do một nhóm diễn viên thiết yếu : các nhà tiên tri của blockchain [27]. Trong hệ sinh thái blockchain, các nhà tiên tri là những thực thể có thể tin cậy nuôi dưỡng mạng lưới blockchain bằng thông tin từ thế giới bên ngoài. Thông tin này là cần thiết cho các mục đích khác nhau, nhưng có hai mục đích liên quan hơn : a) quản lý sự liên kết giữa tài sản hữu hình và đại diện kỹ thuật số của nó; và b) cung cấp thông tin cho các quá trình quyết định của hợp đồng thông minh [28], [29].

**4.1 Phương tiện đo có thể hoạt động như các nhà tiên tri**

Blockchain là rất tốt khi quản lý tài sản kỹ thuật số (ví dụ ví tiền điện tử, tài liệu, giấy chứng nhận). Tuy nhiên, những tài sản này thường là đại diện kỹ thuật số của điều gì đó trong thế giới vật lý : một tài sản hữu hình. Nhiều khi tài sản hữu hình này cũng là một tài sản vật lý. Khi điều này sảy ra, các nhà tiên tri sẽ cần có các phép đo để mô tả tài sản vật lý và cung cấp thông tin về nó. Chúng ta có thể trình bày khái niệm này từ các áp dụng dựa trên blockchain sau :

**Giao dịch năng lượng** : Một số công việc đã đề xuất blockchain là nền tảng để giao dịch tự do giữa các máy phát điện siêu nhỏ trong lưới điện thông minh. Tuy nhiên, blockchain cần một chứng thực vật lý về sự tồn tại của lượng năng lượng giao dịch. Trong thực tế, chứng thực này sẽ phát ra từ đồng hồ năng lượng thông minh làm việc như một nhà tiên tri và thông tin cho blockchain năng lượng người bán thực sự sản xuất là bao nhiêu.

**Giao dịch tài sản** : dân chúng có thể quan tâm đến việc bán hoặc cho thuê tài sản (ví dụ một căn hộ) bằng cách sử dụng blockchain. Các đề xuất liên quan tới loại áp dụng này thường tận dụng cơ hội tạo ra những nền tảng giao tiếp trực tiếp giữa người bán và người mua không cần có TTP. Tuy nhiên, người mua hoặc người thuê thường hỏi thông tin cụ thể như kích thước tài sản, tình trạng bảo tồn của nó hoặc vị trí chính xác để xác định sự tới của ánh sáng tự nhiên. Đồng hồ đo thông minh và thiết bị IoT có thể cung cấp tất cả thông tin này, phục vụ như các nhà tiên tri tin cậy.

**Liên kết chuẩn dược phẩm được kiểm soát** : Áp dụng này thật hấp dẫn do nó có thể quản lý một chu trình sống đầy đủ của dược phẩm được kiểm sóat (nghĩa là sản xuất, phân phối, và tiêu dùng). Một lần nữa, các quá trình liên quan lại yêu cầu những phép đo các đại lượng vật lý khác nhau. Ví dụ, phòng thí nghiệm sản xuất có thể sử dụng thiết bị đo để chứng thực tỷ lệ của từng thành phần hóa học. Lần lượt, các phòng thí nghiệm kiểm tra có thể dùng phương tiện tia-X để kiểm tra tính chất hóa học thể rắn. Trong thực tế, các loại hệ thống đo khác nhau nuôi blockchain bằng thông tin về sản phẩm (nghĩa là tài sản vật lý).

Điều tương tự khi chúng ta nói về những đồng thông minh quyết định các quá trình. Sự khác nhau là ở chỗ hợp đồng thông minh có thể phụ thuộc vào thông tin không mô tả tài sản vật lý nhưng xác định các điều kiện cụ thể liên quan đến việc hoàn thành giao dịch. Lần nữa, những điều kiện này có thể phụ thuộc vào các phép đo tin cậy. Các ví dụ sau đây giúp hiểu rõ sự phụ thuộc này :

**Giao dịch thực phẩm lạnh** : Các áp dụng blockchain có thể hỗ trợ hợp đồng thông minh để xác định giá thực phẩm theo nhiệt độ bảo quản nó. Trong thực tế, một nhiệt kế giám sát nhiệt độ thực phẩm trong quá trình vận chuyển. Sự thay đổi nhiệt độ (nghĩa là nhiệt độ vượt quá một ngưỡng cụ thể) ảnh hưởng đến giá cuối cùng của sản phẩm.

**Giám sát tình trạng bệnh nhân** : Người ta có thể áp dụng hợp đồng thông minh trong các hệ thống giám sát sức khỏe dựa trên blockchain để ghi nhu cầu đối với các thủ tục y tế cụ thể tùy theo tình trạng bệnh nhân. Các cảm biến thân thể (ví dụ máy đo huyết áp, khí kế) có thể cung cấp thông tin thời gian-thực tới một hợp đồng thông minh để khởi động các thông báo hoặc báo động về tình trạng không bình thường. Sổ đăng ký này bảo vệ cả bệnh nhân và nhân viên khỏe mạnh một khi nó là bằng chứng không thể thay đổi để xác minh các thủ tục y tế.

**4.2 Đảm bảo độ tin cậy của lời tiên tri**

Phương tiện đo sẽ thực hiện lời tiên tri trong những áp dụng dựa trên blockchain khác nhau, thi hành những chức năng liên quan pháp lý trong nhiều kịch bản này. Vì vậy, những thiết bị đo này cũng có thể đòi hỏi kiểm soát và giám sát đo lường. Ngay cái nhìn đầu tiên, người ta có thể cho là các hoạt động cần thiết sẽ giống như các hoạt động mà cơ quan được thông báo đã áp dụng khi kiểm tra phương tiện đo trong các ứng dụng điển hình. Tuy nhiên, sự tin tưởng này có thể là không chính xác. Người ta phải xem xét các nhân tố khác nhau có thể ảnh hưởng đến độ tin cậy của lời tiên tri, nhiều trong số các nhân tố đó đòi hỏi một sự phân tích sâu hơn.

Trước hết, blockchain có thể yêu cầu các tính năng mới mà thiết bị đo thông minh tiêu chuẩn không áp dụng. Do những tính năng này có thể ảnh hưởng đến các chức năng liên quan luật pháp, chúng cũng có thể áp đặt yêu cầu kỹ thuật và các chỉ dẫn phương tiện đo mới. Có cơ hội tốt để các NMI sẽ cần áp dụng các chương trình quy định mới dự tính các cấp khác nhau của lời tiên tri trong môi trường kỹ thuật hoàn toàn mới. Khía cạnh thú vị thứ hai là blockchain có thể tạo ra một bộ phận dịch vụ mới cho các nhà sản xuất thiết bị đo thông minh. Khi chúng ta đánh giá những kỳ vọng blockchain ngày càng tăng, chúng ta thấy số các áp dụng sẽ tăng lên trong những bộ phận dịch vụ đa dạng hơn. Ở đâu mà các áp dụng blockchain quản lý tài sản vật lý, các nhà tiên tri sẽ là cần thiết, và thiết bị đo thông minh sẽ đáp ứng nhu cầu này.

**5 Thách thức và cơ hội nghiên cứu**

Blockchain là một công nghệ còn trẻ. Nên có nhiều nghi ngờ và lo âu về việc công nghệ này sẽ thay đổi thế nào cho tới khi trưởng thành. Sự không đảm bảo này cũng tác động đến mọi áp dụng trong lĩnh vực đo lường pháp định. Không thể tránh được, chúng ta phải giải quyết những vấn đề này trước khi các áp dụng blockchain trở thành một sự thay thế có thể dự đoán hơn. Đồng thời, những thách thức này tạo ra các cơ hội đặc biệt cho nghiên cứu và phát minh của các nhà khoa học đo lường trên toàn thế giới. Dưới đây chúng tôi nêu rõ bốn trong số những thách thức này : đồng thuận - consensus, hiệu suất – performance, bảo mật - privacy , và xác nhận lời tiên tri - oracles’ authentication.

**5.1 Chúng ta nên sử dụng đồng thuận nào ?**

Cho đến nay, thực tế là tất cả các công việc về blockchain và các áp dụng trong đo lường pháp định đều đề xuất các blockchain được phép như là một thay thế phù hợp nhất. Thiel và Weztlich [8] thảo luận về việc tích hợp blockchain tới tài liệu tham khảo kiến trúc EMC và khẳng định việc chọn các blockchain được phép bằng cách lập luận rằng trong EMC (i) không có TTP, (ii) có những người sử dụng phức tạp và không biết, và (iii) người sử dụng có thể là không đáng tin cậy. Trong các thực nghiệm được INMETRO và PTB phát triển, những blockchain được phép là một tiền đề trong tất cả các kịch bản được khảo sát. Khía cạnh này có liên quan vì nó ảnh hưởng trực tiếp đến các đồng thuận blockchain.

Trong blockchain được phép, một câu hỏi liên quan là về việc chấp nhận đồng thuận CFT hoặc BFT. Như chúng ta đã thảo luận ở trên, BFT có thể ảnh hưởng đáng kể đến tài sản bảo mật trong mạng lưới blockchain thật sự phi tập trung. Nhiều kịch bản thực tế trong đo lường pháp định có thể phụ thuộc loại đồng thuận này để đảm bảo sự công bằng khi quyết định thứ tự giao dịch và các hộp mới. Tuy nhiên, việc triển khai nó vẫn còn là một thách thức. Hầu hết các nền tảng blockchain được phép không áp dụng đồng thuận BFT một cách tự nhiên. Mặt khác, các giải pháp sử dụng đồng thuận CFT được phổ biến nhiều hơn, như trường hợp của giao thức Raft. Một số thực nghiệm đã công bố của chúng tôi đã sử dụng Raft để phối hợp các đồng thuận giữa những máy phục vụ ở Đức và Brazil. Bước cần thiết tiếp theo là so sánh giữa các lựa chọn thay thế CFT và BFT.

**5.2 Mạng blockchain của tôi có hoạt động chính xác không ?**

Hiệu suất có lẽ là nút cổ chai blockchain tại thời điểm này. Các nền tảng blockchain hiện có xử lý một số lượng tương đối thấp các giao dịch trong một giây (tps) so với các giải pháp độc lập. Ngoài ra, blockchain còn có vấn đề nghiêm trọng về khả năng mở rộng, nghĩa là chúng ta không thể tăng hiệu suất đơn giản bằng thêm nhiều người ngang hàng hơn. Giới hạn này liên quan tới thuộc tính nội tại từ giao thức đồng thuận. Dù giao thức đồng thuận bỏ phiếu (phù hợp với blockchain được phép) thực hiện tốt hơn dựa trên bằng chứng, chúng vẫn kém hiệu quả hơn nhiều so với các giải pháp tập trung.

Chỉ để đưa ra một ý tưởng về các con số, những nền tảng blockchain được phép nổi tiếng như Bitcoin và Ethereum 1.0 có thể thực hiện khoảng 7 và 30 tps. Trong một blockchain được phép, chúng ta có Hyperledger Fabric phân phối khoảng 2 000 tps trong môi trường tiêu chuẩn [16], mặc dù, trong triển khai của chúng tôi, chúng tôi nhận được giá trị xấp xỉ 400 tps [18], [21], [22]. Ngay cả như vậy, những tỷ lệ hiệu suất này có thể đủ để thực hiện các ứng dụng điều chỉnh. Chúng tôi có thể chứng minh lập luận này từ những tìm tòi trong công việc trước đây của chúng tôi, trong đó chúng tôi thiết kế áp dụng blockchain đáp ứng đòi hỏi của một DMS tốc độ xe giả định, đếm trên các đồng hồ đo tốc độ 1,000 và một dòng xe cộ lớn hơn 2 500 xe/giờ [21].

Người ta có thể khẳng định một cách an toàn rằng, trong những năm sắp tới, hiệu suất sẽ là một chủ đề nghiên cứu hàng đầu về blockchain. Chúng ta cũng có thể hy vọng rằng các nền tảng blockchain sẽ tăng hiệu suất hiện nay và xử lý các ứng dụng quy mô lớn hơn.

**5.3 Blockchain có đảm bảo bí mật dữ liệu của tôi không ?**

Bảo mật là một câu hỏi lớn khi nói về blockchain. Trước hết, chúng ta cần nhớ rằng những ứng dụng thực tế blockchain đầu tiên đã khuyến khích mạnh mẽ triết lý công khai thông tin. Người ta thường tin Bicoin vì mọi người có thể kiểm tra từng giao dịch và đánh giá mọi ví tiền (mặc dù về lý thuyết người sở hữu chúng là ẩn danh). Tuy nhiên, khái niệm này còn lâu mới trở thành xu thế chủ đạo về mặt quản lý thông tin. Bảo mật là bắt buộc trong hầu hết các kịch bản thực tế, đặc biệt là trong thời đại của pháp luật và các quy định chẳng hạn như Quy định bảo vệ dữ liệu chung (GDPR).

Bảo mật phép đo là mối quan tâm trong lĩnh vực đo lường pháp định, đặc biệt là khi có rủi ro bộc lộ thông tin nhậy cảm con người [25]. Điều đó sẩy ra với đồng hồ đo năng lượng thông minh có thể bộc lộ ra thói quen của người trong nhà hoặc cảm biến thân thể giám sát dữ liệu sức khỏe. Vì vậy nếu chúng ta có ý định sử dụng blockchain để lưu trữ thông tin nhạy cảm, chúng ta cần trao đổi xem áp dụng đặc điểm này thế nào. Tuy vậy, các giải pháp là không tầm thường vì chúng đối lập với tính chất “mở” của blockchain (ví dụ khả năng kiểm toán, minh bạch) với những ràng buộc riêng tư (ví dụ tính bí mật, kiểm soát truy cập).

Kiểm soát truy cập là đặc điểm mà nhiều nền tảng blockchain được phép đã bao gồm theo mặc định. Ví dụ, trong Hyperledger Fabric, người ngang hàng có thể gồm những kênh khác nhau (nghĩa là các ví dụ sổ cái khác nhau) và xác định chính sách truy cập cụ thể cho mỗi người trong số họ [16]. Tuy nhiên, chính sách bảo mật có thể cần nhiều ràng buộc hạn chế hơn chính sách truy cập. Trong trường hợp này, các chỉ dẫn mật mã là sự thay thế phù hợp hơn. PTB đã phát triển một tuyến điều tra tiên phong bao gồm các hệ thống mã hóa đồng cấu hoàn toàn để đảm bảo bí mật [18], [24]. Những cơ chế này cho phép tính toán dữ liệu trong miền mật mã (nghĩa là chúng ta có thể thao tác toán học trên dữ liệu mà không cần giải mã nó), có những áp dụng trong các hệ thống đám mây và blockchain. Bất chấp khía cạnh đầy hứa hẹn của nó, nghiên cứu này đối diện những thách thức nghiêm trọng vì sự mã hóa đồng cấu vẫn đòi hỏi một chi tiêu đáng kể của tài nguyên tính toán và có thể bị cấm trong nhiều kịch bản thực tế.

**5.4 Tôi có thể cải tiến thế nào để dụng cụ đo của tôi là một nhà tiên tri tin cậy ?**

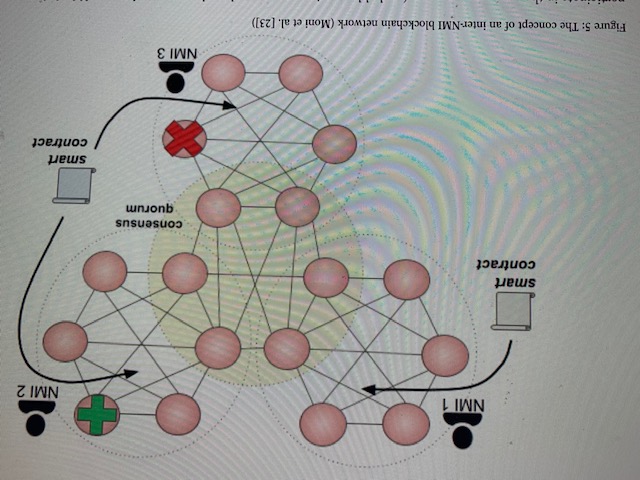
Người làm việc trên bất kỳ hoạt động nào liên quan đến sản xuất dụng cụ đo thông minh chú ý đến mục 4.1 có lẽ sẽ tự hỏi chuyển đổi những dụng cụ đo này thành các nhà tiên tri blockchain thế nào. Câu hỏi này là xác đáng, đặc biệt là khi người ta xem các nhà tiên tri hoạt động trước dòng thông tin blockchain, như vậy các chỉ dẫn an toàn blockchain không áp dụng cho các thiết bị này [27]. Đồng thời, nếu các nhà tiên tri là không đáng tin, cũng không là blockchain. Phát hiện này ảnh hưởng sâu sắc đến việc đánh giá độ tin cậy của blockchain. Blockchain sẽ cần những cơ chế độc lập để chứng nhận độ tin cậy của các nhà tiên tri, bao gồm cả sự xác nhận của chúng.

Đầu tiên, chúng ta phải nhớ rằng đo lường pháp định đã thiết lập các hướng dẫn và khuyến nghị để bảo vệ những thành phần phương tiện đo liên quan về mặt luật pháp và chứng nhận độ tin cậy của chúng. Tuy nhiên, ý nghĩ về các nhà tiên tri như là các thiết bị có thể tin cậy cô lập chuyển chúng thành một TTP, mà blockchain không muốn phụ thuộc vào. Các nhà tiên tri có lẽ sẽ là những thiết bị dự phòng và bổ xung, như vậy các quyết định blockchain sẽ tin vào thông tin được chứng thực bằng một tập hợp các nhà tiên tri thay vì một nhà tiên tri cô lập [30].

Đã có công trình khoa học đề xuất các giao thức xác thực tiên tri, một số trong đó dựa vào giao thức bỏ phiếu [28], [29]. Tuy nhiên, với hiểu biết tốt nhất của chúng tôi, chưa có nghiên cứu nào thảo luận tích hợp các dụng cụ đo thông minh vào các giao thức thực tế của chứng thực nhiều bên. Khảo sát này rõ ràng là một đề tài đáng chú ý m\*à các nhà khoa học đo lường có thể giải quyết trong nhiều nghiên cứu của họ những năm sắp tới.

**5.5 Nhu cầu đối với mạng blockchain liên-NMI**

Khi chúng ta xem xét rất nhiều khả năng và cơ hội đối với các áp dụng dựa vào-blockchain trong đo lường, điều tự nhiên dẫn đến là các nhà khoa học và các nhà đo lường sẽ cần có một môi trường thích hợp để thực nghiệm các giải pháp. Nhằm mục đích lan truyền ý tưởng này, PTB và INMETRO đã làm việc cùng nhau thay mặt cho mạng blockchain liên-NMI [23]. Hình 5 trình bày đề xuất này như là một mạng blockchain được phép. Các NMI tích hợp mạng cần cung cấp sự ngang hàng để thực hiện các áp dụng quan tâm chung cho những người tham gia khác. Các NMI cũng có thể tham gia vào số đại biểu quy định đồng thuận (có lẽ là một thay thế dựa trên bỏ phiếu : CFT hoặc BFT).



**Hình 5** : *Khái niệm về mạng blockchain liên-NMI (Moni et all. [23])*

Chúng ta hình dung mạng blockchain liên-NMI như là một nền tảng định hướng-hợp đồng thông minh. Như vậy người tham gia có thể viết và thực hiện các áp dụng của họ bằng cách sử dụng những hợp đồng thông minh như là một cơ sở phát triển. Hơn nữa, mạng được phân cấp. Từng người tham gia có thể quản lý những người ngang hàng của họ một cách độc lập, thêm vào hoặc loại bỏ người ngang hàng theo nhu cầu của họ.

Mạng liên-NMI là một sự khởi đầu lớn mở ra các cơ hội cho cộng tác và đóng góp trên phạm vi thế giới. Chi tiết hơn xin xem công trình của Moni et al, [23]. Nếu viện của bạn muốn tham gia mạng, chúng tôi mong bạn liên hệ với chúng tôi để có chi tiết hơn về dự án.

**6 Kết luận**

Trong bài báo này, chúng tôi đã trình bày những khái niệm chính liên kết đo lường pháp định tới công nghệ blockchain. Blockchain là một công cụ đẩy nhanh chuyển đổi kỹ thuật số trong nhiều lĩnh vực. Nhu cầu đối với các áp dụng dựa trên blockchain sẽ tăng lên trong những năm sắp tới, và đo lường pháp định cũng có thể tận dụng điều đó. Hơn nữa, blockchain cũng sẽ cần sự giúp đỡ của đo lường pháp định để quản lý các tài sản vật lý một cách đúng đắn. Thuận lợi và sự phụ thuộc lẫn nhau này có thể tăng cường tính chất đáng tin cậy của blockchain và đẩy mạnh chuyển đổi kỹ thuật số trong các quá trình đo lường pháp định về cơ bản phụ thuộc vào tính bất biến của thông tin, độ tin cậy và tự động hóa quyết định.

**7 Tài liệu tham khảo**

[1] E. V. Dudukalov, V. D. Munister, A. L. Zolkin, S. A. Galanskiy, e S. G. Rudnev, “Metrological support integration in conditions of digital transformation”, J. Phys. Conf. Ser., vol. 1889, no 3, p. 032012, 2021, doi: 10.1088/1742-6596/1889/3/032012.

[2] T. Mustapää, P. Nikander, D. Hutzschenreuter, e R. Viitala, “Metrological challenges in collaborative sensing: Applicability of digital calibration certificates”, Sens. Switz., vol. 20, no 17, p. 1–19, 2020, doi: 10.3390/s20174730.

[3] T. Mustapaa, J. Autiosalo, P. Nikander, J. E. Siegel, e R. Viitala, “Digital Metrology for the Internet of Things”, in GIoTS 2020 - Global Internet of Things Summit, Proceedings, 2020, p. 1–6. doi: 10.1109/GIOTS49054.2020.9119603.

[4] A. Oppermann, S. Eickelberg, e J. Exner, “Toward Digital Transformation of Processes in Legal Metrology for Weighing Instruments”, in Proceedings of the 2020 Federated Conference on Computer Science and Information Systems, FedCSIS 2020, 2020, vol. 21, p. 559–562. doi: 10.15439/2020F77.

[5] M. Peterek e B. Montavon, “Prototype for dual digital traceability of metrology data using X.509 and IOTA”, CIRP Ann., vol. 69, no 1, p. 449–452, 2020, doi: 10.1016/j.cirp.2020.04.104.

[6] A. E. R. Rincon, W. S. Melo, C. M. Farias, e L. F. R. C. Carmo, “Securing Smart Meters through Physical Properties of their Components”, IEEE Trans. Instrum. Meas., vol. 70, p. 1–11, 2020, doi: 10.1109/TIM.2020.3041098.

[7] F. Thiel, “Digital transformation of legal metrology - The European Metrology Cloud”, OIML Bull., vol. 59, no 1, p. 10–21, 2018.

[8] F. Thiel e J. Wetzlich, “The European Metrology Cloud: Impact of European Regulations on Data Protection and the Free Flow of Non-Personal Data”, in 19th International Congress of Metrology, 2019, p. 39. doi: 10.1051/metrology/201901001.

[9] A. Ustundag e E. Cevikcan, Industry 4.0: Managing The Digital Transformation. Cham, Switzerland: Springer, 2018. doi: 10.1007/978-3-319-57870-5.

[10] C. Cachin e M. Vukoli , “Blockchain Consensus Protocols in the Wild”, in 31 International Symposium on Distributed Computing, 2017, p. 16. doi: 10.4230/LIPIcs.DISC.2017.1.

[11] H.-N. Dai, Z. Zheng, e Y. Zhang, “Blockchain for Internet of Things: A Survey”, IEEE Internet Things J., vol. 6, no 5, p. 8076— – 8094, 2019.

[12] Y. Xiao, N. Zhang, W. Lou, e Y. T. Hou, “A Survey of Distributed Consensus Protocols for Blockchain Networks”, IEEE Commun. Surv. Tutor., vol. 22, no 2, p. 1432–1465, 2020.

[13] D. Yaga, P. Mell, N. Roby, e K. Scarfone, “Blockchain Technology Overview”, 2018. doi: 10.6028/NIST.IR.8202.

[14] K. Wüst e A. Gervais, “Do you Need a Blockchain?”, in 2018 Crypto Valley Conference on Blockchain Technology (CVCBT), 2018, p. 45–54. doi: 10.1109/CVCBT.2018.00011.

[15] S. Nakamoto, “Bitcoin: A Peer-to-Peer Electronic Cash System”, Www.Bitcoin.Org, 2008. doi: 10.1007/s10838- 008-9062-0.

[16] E. Androulaki et al., “Hyperledger Fabric: A Distributed Operating System for Permissioned Blockchains”, Porto, Portugal, 2018. doi: 10.1145/3190508.3190538.

[17] F. O. Leitão, M. T. Vasconcellos, e P. C. R. Brandão, “Hardware and Software Countermeasures on High Technology Fraud at Fuel Dispensers under the Scope of Legal Metrology”, in IX Simposio Internacional “Metrologia 2014”, Havana, 2014, p. 1–10.

[18] D. Peters et al., “IT Security for Measuring Instruments: Confidential Checking of Software Functionality”, in Advances in Intelligent Systems and Computing, vol. 1129 AISC, Springer, Cham, 2020, p. 701–720. doi: 10.1007/978-3-030-39445-5\_51.

[19] W. S. Melo Jr., A. Bessani, e L. F. R. C. Carmo, “How Blockchains can help Legal Metrology”, in SERIAL ‘17 Proceedings of the 1st Workshop on Scalable and Resilient Infrastructures for Distributed Ledgers, New York, NewYork, USA, 2017, p. 1–2. doi: 10.1145/3152824.3152829.

[20] D. Peters, J. Wetzlich, F. Thiel, e J. Seifert, “Blockchain Applications for Legal Metrology”, in IEEE International Instrumentation and Measurement Technology Conference, Houston, Texas, USA, 2018, p. 6.

[21] W. S. Melo Jr., A. Bessani, N. Neves, A. O. Santin, e L. F. R. C. Carmo, “Using Blockchains to Implement Distributed Measuring Systems”, IEEE Trans. Instrum. Meas., vol. 68, no 5, p. 1503–1512, 2019, doi: 10.1109/TIM.2019.2898013.

[22] W. S. Melo, L. V. Tarelho, B. A. Rodrigues, A. N. Bessani, e L. F. R. C. Carmo, “Field surveillance of fuel dispensers using IoT-based metering and blockchains”, J. Netw. Comput. Appl., vol. 175, no February 2021, p. 102914, 2020, doi: 10.1016/j.jnca.2020.102914.

[23] M. Moni, W. Melo, D. Peters, e R. Machado, “When measurements meet blockchain: On behalf of an internmi network”, Sensors, vol. 21, no 5, p. 1–24, 2021, doi: 10.3390/s21051564.

[24] A. Yurchenko, M. Moni, D. Peters, J. Nordholz, e F. Thiel, “Security for Distributed Smart Meter : Blockchain-based Approach , Ensuring Privacy by Functional Encryption”, in Proceedings of the 10th International Conference on Cloud Computing and Services Science - CLOSER, 2020, p. 292–301. doi: 10.5220/0009377702920301.

[25] A. Oppermann, F. G. Toro, F. Thiel, e J.-P. Seifert, “Secure Cloud Computing: Reference Architecture for Measuring Instrument under Legal Control”, Secur. Priv., vol. 1, no 3, p. 1–26, 2018, doi: 10.1002/spy2.18.

[26] B. A. Rodrigues Filho e R. F. Gonçalves, “Measuring the economic impact of metrological frauds in trade metrology using an Input-Output Model”, IFIP Adv. Inf. Commun. Technol., vol. 488, 2016, doi: 10.1007/978-3- 319-51133-7.

[27] K. Mammadzada, M. Iqbal, F. Payman Milani, L. GarcíaBañuelos, e R. Matulevi ius, Blockchain Oracles: A Framework for Blockchain-Based Applications (SLR Protocol and Results). University of Tartu, 2020. doi: 10.15155/re-112.

[28] J. Adler, R. Berryhill, A. Veneris, Z. Poulos, N. Veira, e A. Kastania, “Astraea: A decentralized blockchain oracle”, in 2018 IEEE International Conference on Internet of Things (iThings) and IEEE Green Computing and Communications (GreenCom) and IEEE Cyber, Physical and Social Computing (CPSCom) and IEEE Smart Data (SmartData), 2018, p. 1145–1152. [Online]. Disponível em: <http://arxiv.org/abs/1808.00528>

[29] F. Zhang, E. Cecchetti, K. Croman, A. Juels, e E. Shi, “Town Crier: An authenticated data feed for smart contracts”, in 23rd ACM Conference on Computer and Communications Security, CCS 2016, 2016, p. 270–282. doi: 10.1145/2976749.2978326.

[30] L. Ma, K. Kaneko, S. Sharma, e K. Sakurai, “Reliable decentralized oracle with mechanisms for verification and disputation”, in 7th International Symposium on Computing and Networking Workshops, CANDARW 2019, 2019, p. 346–352. doi: 10.1109/CANDARW.2019.00067.