AgriCarbonDEX

1. Bối cảnh

Biến đổi khí hậu và phát thải nhà kính đang là thách thức toàn cầu, đòi hỏi mỗi quốc gia, doanh nghiệp và cá nhân cùng hành động. Tín chỉ carbon và dữ liệu ESG (môi trường – xã hội – quản trị) ngày càng trở thành tài sản có giá trị cao, được giao dịch như một phần của chiến lược giảm phát thải và tài chính bền vững.

Tuy nhiên, thị trường tín chỉ carbon hiện nay đối mặt với các vấn đề lớn:

- Khó xác minh nguồn gốc và tính minh bạch của dữ liệu môi trường.
- Nguy cơ "greenwashing" khi doanh nghiệp tuyên bố xanh nhưng không có bằng chứng kiểm chứng.
- Dữ liệu bị phân mảnh, khó theo dõi xuyên suốt chuỗi giá trị.

2. Giải thích các khái niệm

- DT (Digital Twin): là bản sao kỹ thuật số của một đối tượng, hệ thống hoặc quá trình trong thế giới thực. DT mô phỏng hành vi, trạng thái và hiệu suất của đối tượng thật theo thời gian thực.
- Dữ liệu DT: là dữ liệu được thu thập từ cảm biến hoặc nguồn thực tế, phản ánh trạng thái hiện tại hoặc lịch sử của đối tượng.
- Tín chỉ carbon: Là một chứng chỉ đại diện cho quyền phát thải 1 tấn khí CO_2 (hoặc tương đương). Các doanh nghiệp gây ô nhiễm có thể mua tín chỉ từ các bên thực hiện các dự án giảm phát thải, như trồng rừng, năng lượng tái tạo, vv.
- DID (Decentralized Identifier): Là định danh phi tập trung, cho phép các đối tượng (người, tổ chức, thiết bị, vv.) tự xác định danh tính của mình không cần trung gian.
- Greenwashing: Là hành vi tung hô sai sự thật hoặc phóng đại những nỗ lực bảo vệ môi trường của một công ty hoặc tổ chức, nhằm đánh bóng hình ảnh.
- ESG (Environmental, Social, Governance): Là khung đánh giá mức độ bền vững của doanh nghiệp dựa trên môi trường, xã hội và quản trị. ESG ngày càng quan trọng trong đầu tư và đánh giá tác động dài hạn của tổ chức.
- RAG (Retrieval-Augmented Generation): Là kỹ thuật AI kết hợp truy xuất dữ liệu từ nguồn ngoài với khả năng tạo văn bản của mô hình ngôn ngữ. Nhờ đó, câu trả lời được tạo ra chính xác và có căn cứ hơn, đặc biệt hữu ích khi cần trích dẫn thông tin từ tài liệu cụ thể.

3. Mục tiêu

Dự án AgriCarbonDEX được xây dựng nhằm:

- Tạo ra một nền tảng phi tập trung (DEX) cho phép giao dịch tín chỉ carbon, dữ liệu môi trường, và tài sản ESG một cách minh bạch và đáng tin cậy.
- Ứng dụng Digital Twin (DT) để mô phỏng hành vi môi trường của từng thực thể (trang trại, nhà máy, vùng sinh thái), đảm bảo rằng tín chỉ được tạo ra dựa trên dữ liệu thật.
- Tích hợp AI Agent (LLM) để hỗ trợ tư vấn về ESG, phân tích hành vi môi trường, và hỗ trợ minh bạch hóa quy trình phát hành và đánh giá tín chỉ.
- Xác minh nguồn gốc phát thải / hấp thụ và nguồn gốc của tín chỉ carbon.

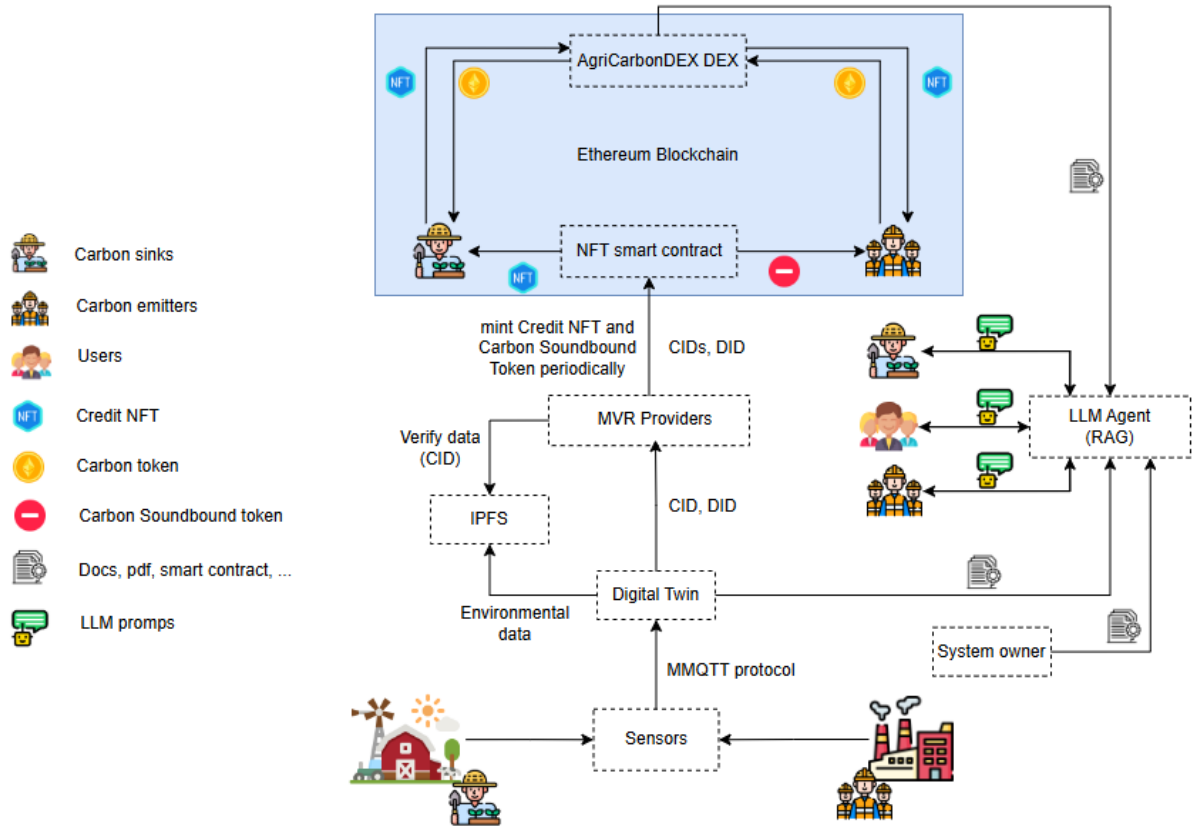
4. Phạm vi ứng dụng

- Nông nghiệp tái sinh, trang trại trồng rừng, nhà máy xanh: tạo và giao dịch tín chỉ carbon thật sự.
- Tổ chức tài chính, nhà đầu tư ESG: đánh giá minh bạch tài sản môi trường.
- Chính quyền địa phương và trung ương: giám sát phát thải, hỗ trợ ra quyết định chính sách.
- Người dân: truy xuất dữ liệu môi trường gần họ, khuyến khích tiêu dùng xanh.

5. Giá trị kỳ vọng

- Đảm bảo tín chỉ carbon phát hành từ dữ liệu thật, có thể kiểm tra.
- Tạo ra thị trường giao dịch minh bạch, phi tập trung, khuyến khích doanh nghiệp phát triển bền vững.
- Đưa dữ liệu ESG vào tài chính hóa, phục vụ các quỹ đầu tư xanh và nhà hoạch định chính sách.
- Nâng cao vai trò của công nghệ Việt Nam trong xây dựng hạ tầng tài chính môi trường.

6. Kiến trúc hệ thống



Trong hình trên, các thành phần trong hệ thống có thể chia thành 5 Lớp:

- **End devices:** Các cảm biến thu thập từ các trang trại trồng rừng hoặc các xí nghiệp.
- **Edge:** DT đặt ở cạnh nguồn dữ liệu với độ trễ thấp và phản hồi ngay lập tức với dữ liệu thô sơ.
- **Fog:** Các DT đặt ở gần trung tâm hơn, có tài nguyên tính toán mạnh nên có khả năng phân tích phức tạp.
- **Control center:** Trung tâm giám sát, xác minh và báo cáo (MVR) cùng với chatbox LLM agent và mô đun ML/DL phát hiện số liệu DT bất thường.
- **Cloud:** Hệ thống blockchain Ethereum với các hợp đồng thông minh.

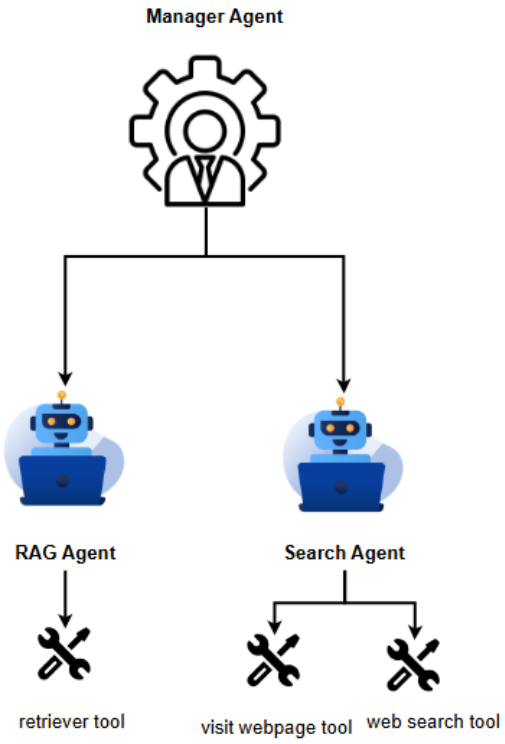
Vai trò của các thành phần:

- **DT:** Mô hình hóa động mỗi thực thể phát thải – cập nhật trạng thái thời gian thực, đo lường bằng dữ liệu cảm biến, vệ tinh, hoặc đầu vào mô phỏng.
- **Ethereum Blockchain:** Ghi nhận quá trình tạo, xác minh và giao dịch tín chỉ carbon. Tạo NFT dữ liệu môi trường (air quality, emission log…). Gắn DID (danh tính số) với tổ chức phát hành.
- **LLM Agent:** Trợ lý AI hỗ trợ tư vấn ESG, diễn giải dữ liệu twin, giải thích quy định carbon, cảnh báo hành vi bất thường (risk of greenwashing).
- **DEX layer:** Sàn giao dịch token carbon (ERC-20) hoặc dữ liệu môi trường NFT (ERC-721) giữa các bên có nhu cầu.

Các loại token trong mạng:

- **Credit NFT:** Được cấp cho các bên có ảnh hưởng tốt, tích cực đến môi trường như các trang trại trồng rừng, doanh nghiệp tái chế, dự án năng lượng tái tạo. Credit NFT đại diện cho một lượng carbon đã được loại bỏ hoặc tránh phát thải, và có thể chuyển nhượng hoặc bán cho các bên khác để phục vụ mục đích bù đắp khí thải carbon.
- **Carbon Soundbound Token:** Cấp cho các bên có ảnh hưởng xấu, tiêu cực đến môi trường như các xí nghiệp, nhà máy sản xuất, công ty khai thác tài nguyên. Token này phản ánh lượng khí thải carbon mà tổ chức phát ra và không thể chuyển nhượng hoặc mua bán, nhằm gắn liền trách nhiệm môi trường vào danh tính kỹ thuật số của tổ chức.
- **Carbon Token:** Là tài sản kỹ thuật số được sử dụng để mua Credit NFT, thường được phát hành và sử dụng bởi các bên gây phát thải như nhà máy, doanh nghiệp sản xuất, công ty vận tải hoặc các tổ chức muốn bù đắp lượng khí thải carbon của mình.

6.1) LLM Agent



Hệ thống hiện tại được xây dựng dựa trên kiến trúc **Multi-agent**, tức là một tập hợp gồm nhiều tác nhân thông minh có khả năng tương tác, phối hợp hoặc hoạt động độc lập nhằm giải quyết các tác vụ phức tạp trong môi trường năng động.

Cụ thể, hệ thống hiện tại bao gồm **một Manager Agent** đóng vai trò điều phối và hai tác nhân chức năng chính:

- **RAG Agent**: Được sử dụng khi người dùng có các câu hỏi liên quan đến hệ thống AgriCarbonDex, chẳng hạn như: “Tại sao AgriCarbonDex được đề xuất?” hoặc “AgriCarbonDex được ứng dụng trong lĩnh vực nào?” Tác nhân này sử dụng kỹ thuật kết hợp giữa truy xuất và tạo sinh (Retrieval-Augmented Generation) để cung cấp câu trả lời chính xác và có căn cứ.
- **Search Agent**: Được kích hoạt khi người dùng đặt ra các câu hỏi vượt ngoài phạm vi hệ thống, ví dụ như: “ESG là gì?” hoặc “ERC20 hoạt động như thế nào?” Tác nhân này tìm kiếm và tổng hợp thông tin từ các nguồn bên ngoài nhằm hỗ trợ người dùng hiểu các khái niệm nền tảng.

Định Hướng Phát Triển (Future Work)

Trong giai đoạn tiếp theo, chúng tôi định hướng mở rộng hệ thống theo hướng đa nhiệm, linh hoạt và thông minh hơn, nhằm nâng cao khả năng hỗ trợ tư vấn ESG, phân tích dữ liệu carbon và cung cấp giá trị thực tiễn cho người dùng doanh nghiệp. Cụ thể, các hạng mục phát triển bao gồm:

a) Mở rộng hệ thống với các Tác nhân Chuyên biệt (Specialized Agents)

- **Regulation Agent**: Chịu trách nhiệm giải thích các chính sách, quy định ESG và Carbon đang áp dụng, đồng thời cập nhật liên tục từ các nguồn dữ liệu uy tín như IPCC, UNFCCC hoặc hệ thống pháp luật của từng quốc gia. Tác nhân này hỗ trợ người dùng hiểu rõ nghĩa vụ pháp lý liên quan đến phát thải và tín chỉ carbon.
- **ESG Risk Agent**: Thực hiện phân tích nội dung để phát hiện và cảnh báo các rủi ro liên quan đến hành vi "greenwashing" (ngụy tạo ESG) hoặc sai lệch trong báo cáo ESG.
- **Twin Interpretation Agent**: Chuyên đảm nhiệm việc giải thích các dữ liệu được sinh ra từ mô hình Digital Twin, giúp người dùng không chuyên dễ dàng tiếp cận và hiểu rõ các chỉ số đo lường phát thải, xu hướng biến động carbon theo thời gian thực.

b) Tăng cường năng lực phối hợp tác nhân (Agent Collaboration)

Hiện tại, các tác nhân hoạt động chủ yếu theo chỉ dẫn của Manager Agent. Trong tương lai, chúng tôi dự kiến phát triển cơ chế **phối hợp linh hoạt giữa các agent**, cho phép các tác nhân tự động giao tiếp và phân chia nhiệm vụ thông qua một giao thức điều phối chung.

Ví dụ: Khi người dùng đặt câu hỏi như “Tác động của carbon footprint trong chuỗi cung ứng nông nghiệp là gì?”, hệ thống sẽ tự động:

- **RAG Agent**: Cung cấp thông tin nền liên quan đến AgriCarbonDex và khái niệm carbon footprint.
- **Search Agent**: Thu thập và trích xuất số liệu, dữ liệu thực tế từ các nguồn bên ngoài.
- **Twin Interpretation Agent**: Trình bày dữ liệu dưới dạng trực quan, dễ hiểu.
- **ESG Risk Agent**: Phân tích các rủi ro ESG liên quan đến chuỗi cung ứng cụ thể.

- **Manager Agent**: Tổng hợp đầu ra từ các tác nhân trên và trình bày cho người dùng một câu trả lời toàn diện, mạch lạc.

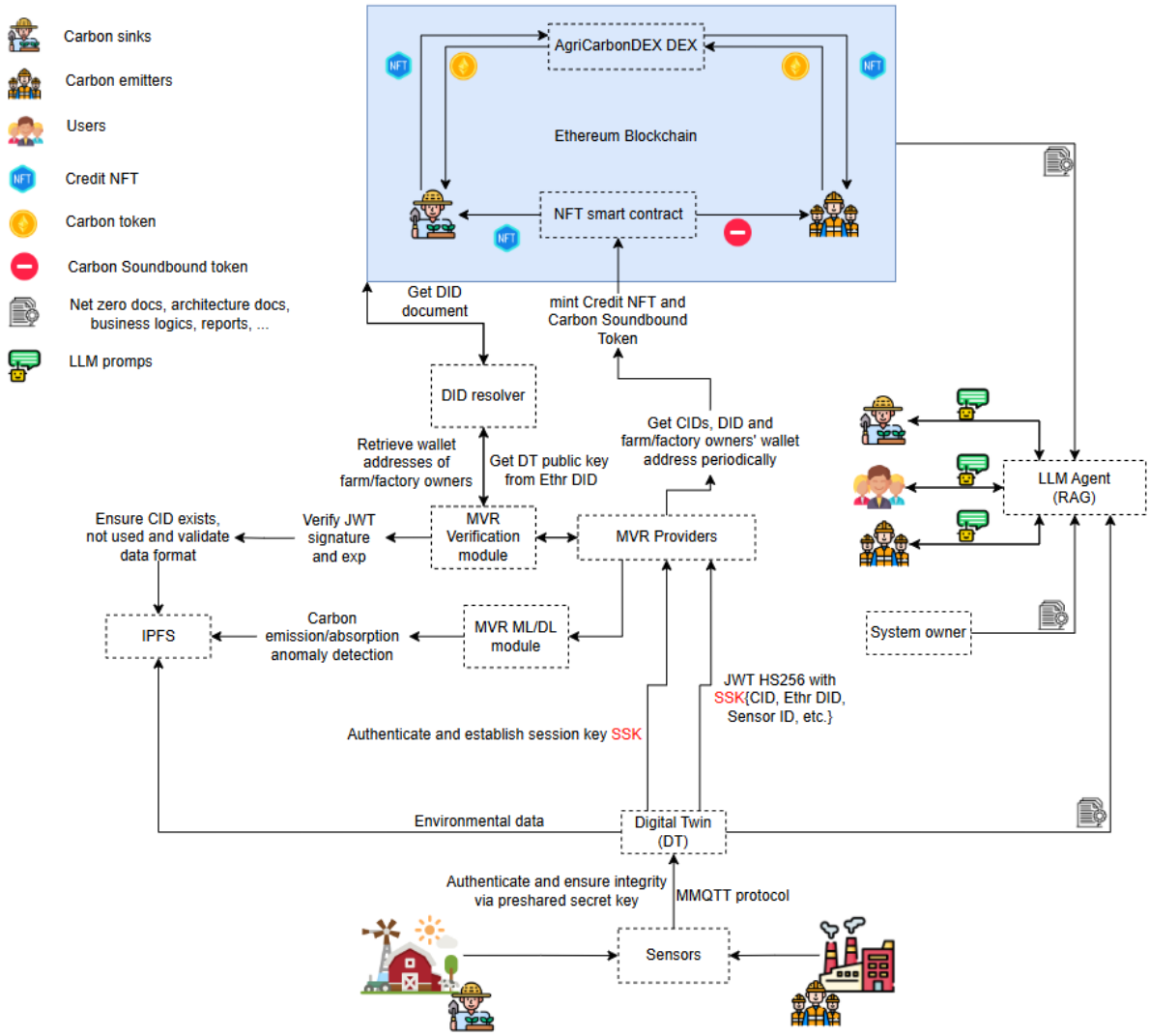
7. Quản lý, định danh các DT và dữ liệu

Các DT trong hệ thống của chúng tôi liên tục tạo ra dữ liệu theo thời gian thực. Để đảm bảo tính hiệu quả và tiết kiệm chi phí, thay vì lưu trữ dữ liệu gốc trực tiếp lên blockchain, chúng tôi sử dụng IPFS để lưu trữ phân tán, sau đó lấy Content Identifier (CID) làm đại diện duy nhất cho từng phiên bản dữ liệu DT.

Tuy nhiên, do mỗi CID chỉ đại diện cho một bản snapshot cụ thể của dữ liệu, chúng tôi sử dụng Decentralized Identifiers (DID) để định danh lâu dài cho từng DT. DID giúp truy xuất lịch sử và xác minh nguồn gốc dữ liệu một cách minh bạch và đáng tin cậy.

Khi thực hiện mint NFT tín chỉ carbon, chúng tôi nhóm một lô các CID liên quan và liên kết chúng với DID của DT tương ứng. Điều này cho phép chứng minh nguồn gốc dữ liệu và danh tính của bên phát thải hoặc hấp thụ carbon, đồng thời giảm đáng kể chi phí gas nhờ không cần ghi dữ liệu lớn trực tiếp lên blockchain hay liên lục mint từng NFT riêng lẻ.

8. Ngữ cảnh giả mạo và hướng giải quyết



- Kẻ tấn công sinh DID và gửi thông tin DT về MVR: Chỉ chấp nhận những DID đã được đăng kí trước.
- Kẻ tấn công giả mạo một DT hợp lệ bằng cách giả mạo DID: Xác minh chữ kí ứng với khóa công khai trong DID document.
- DT đã xác minh gửi thông tin giả: Dùng ML/DL để phát hiện số liệu bất thường và MVR có trách nhiệm giám sát, quản lý cảm biến.

9. Giao thức xác thực giữa DT và MVR

a. Tổng quan

Trong hệ thống này, vì các dữ liệu DT cần được công khai để xác thực nên không cần đảm bảo tính bí mật mà thay vào đó, chúng ta cần xác thực các

thành phần tham gia và đảm bảo tính toàn vẹn của dữ liệu. Trong đó, đối với việc gửi dữ liệu từ cảm biến lên DT, chúng ta có thể sử dụng PSK (Preshared Secret Key) để xác thực và kiểm tra tính toàn vẹn thông qua HMAC vì DT nằm gần nguồn dữ liệu. Tuy nhiên, đối với việc gửi dữ liệu từ DT lên MVR, chúng ta không nên dùng PSK để xác thực và đảm bảo tính toàn vẹn vì khoảng cách xa khiến cho việc triển khai PSK trở nên khó khăn hơn khi muốn mở rộng hệ thống và cập nhật khóa. Do đó, chúng ta sẽ sử dụng hệ mã hóa khóa công khai và chữ kí số. Vì dữ liệu được gửi từ DT lên MVR theo thời gian thực nên chúng ta cần xác thực DT và đồng thuận khóa phiên SSK (Session Key) trước rồi dùng SSK đó để đảm bảo tính toàn vẹn của dữ liệu. Việc xác thực DT, MVR và các bên liên quan, chúng tôi không dùng chứng chỉ X.509 với TLS mà tận dụng DID đã trình bày, cụ thể là Ethr DID. Ethr DID cho phép chủ tài khoản thêm hoặc xóa các khóa công khai thông qua hợp đồng Ethr DID Registry, giúp linh động hơn khi triển khai.

b. Giao thức xác thực và đồng thuận khóa phiên

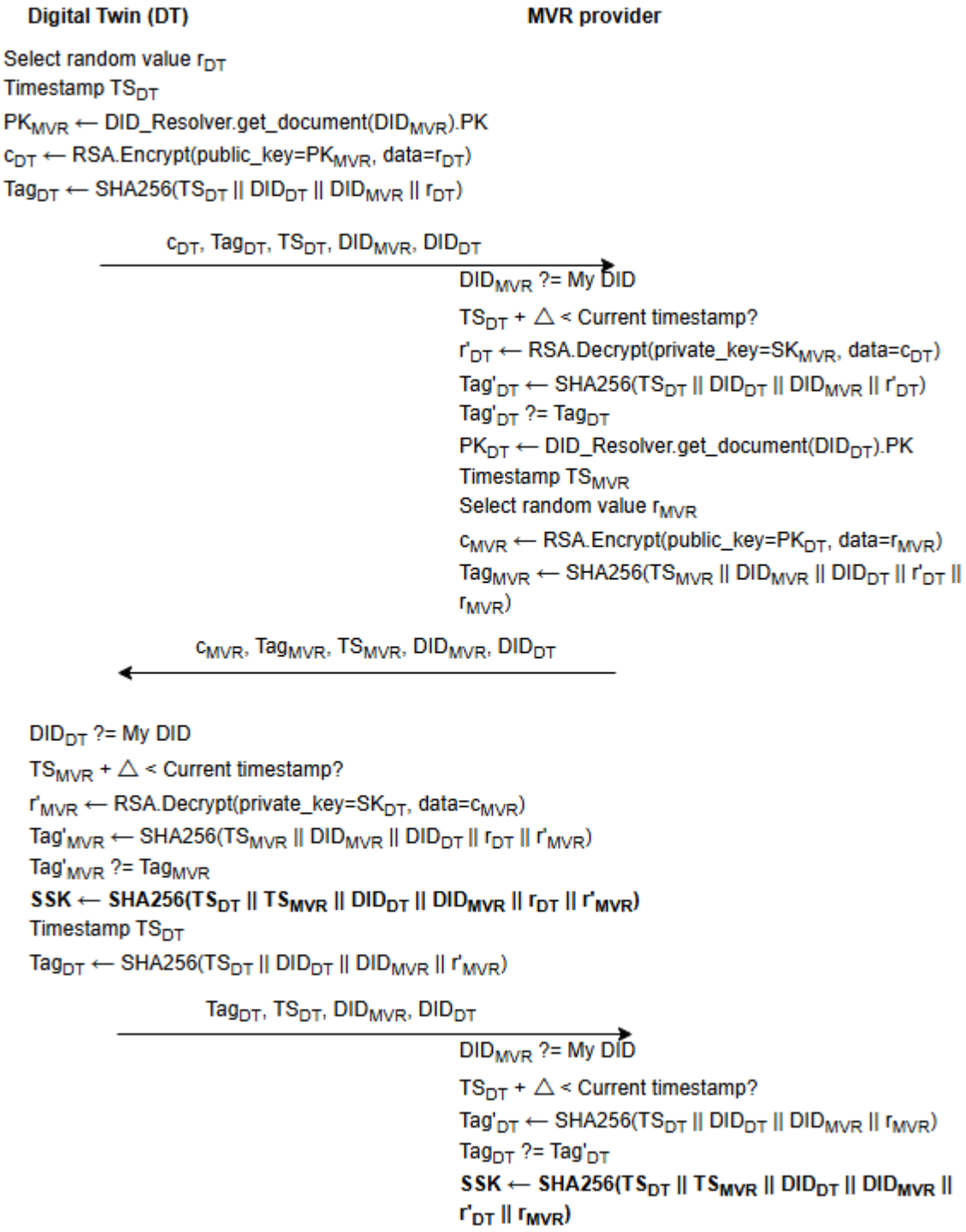
Pha thiết lập (Setup) và đăng kí:

MVR và các DT sẽ tạo DID, đồng thời sinh cặp khóa RSA và thêm khóa công khai vào DID document. Vì kiến trúc mạng có dạng hình sao (các DT gửi dữ liệu về MVR để xác minh), MVR tiến hành đăng kí cho các DT bằng cách lưu lại các thông tin DID, địa chỉ IP, vv.

Trong trường hợp muốn mở rộng hệ thống, cho phép xác thực và đồng thuận khóa phiên đối với 2 thành phần bất kỳ (Kiến trúc mạng ngang hàng thay vì hình sao), chúng ta sẽ cần đến một bên trung gian là Trust Authority (TA) để mapping danh tính của tổ chức (DT, MVR, vv.) sang DID, đóng vai trò như Certificate Authority trong TLS và chứng chỉ X.509. Việc này có thể thực hiện thông qua môt hợp đồng thông minh chỉ cho phép TA mới có quyền thêm, xóa hoặc sửa.

Xác thực và đồng thuận khóa phiên SSK:

Quá trình xác thực và đồng thuận khóa phiên SSK của DT và MVR provider được mô tả như hình bên dưới:



c. Xác thực và đảm bảo tính toàn vẹn của dữ liệu gửi đi thông qua SSK

Sau khi thành lập được khóa phiên SSK, chúng tôi dùng nó để xác thực DT và đảm bảo tính toàn vẹn của dữ liệu gửi lên MVR. Lý do cần sử dụng SSK thay

cho chữ kí số là vì tốc độ xác minh chữ kí số thông qua mật mã bất đối xứng lâu hơn nhiều so với việc kiểm tra HMAC, trong khi dữ liệu DT gửi lên MVR theo thời gian thực nên cần phải tối ưu. Ngoài ra, để đơn giản và thuận tiện cho việc triển khai, chúng tôi sử dụng JWT (JSON Web Token) với thuật toán HS256 để gửi lên các thông tin như CID của dữ liệu DT, ID của cảm biến hay thời gian hiện tại, vv.