Journal of educational equipment: Education management, Volume 1, Issue 296 (September 2023)
ISSN 1859 - 0810

Ứng dụng công nghệ blockchain trong tải dữ liệu đáng tin cậy trên các node internet of things

Hoàng Quốc Việt*

**Học viện Hành chính Quốc Gia*

Received: 30/7/2023; Accepted: 7/8/2023; Published: 14/8/2023

Abstract: *The article introduces the background and importance of "Blockchain in downloading data on Internet of Things nodes" and suggests that in the period of rapid development of artificial intelligence, a large number of communication devices Information technology has virtually no ability to protect data during the digital transformation process, and access to devices, data transmission lines, and data platforms is easily susceptible to impersonation, theft, and interference. It seriously affects the security and reliability of the Internet of Things environment in general. At the same time, due to the customization and diversification of Internet of Things terminals and applications, it has brought more security risks to Internet of Things business. Therefore, more attention is paid to the reliability of data. Faced with the above problems, the article suggests that reliable data transmission is an effective solution.*

Keywords*: Blockchain technology, data download, trust, internet of things node*

1. Giới thiệu

Khi trí tuệ nhân tạo (AI) đã bước vào kỷ nguyên 2.0[1], tầm quan trọng và ảnh hưởng của nó đối với trí tuệ dữ liệu lớn, hệ thống mạng toàn cầu, trí tuệ nhân tạo, đa phương tiện, trí tuệ giữa người máy và hệ thống thông minh AI đã bắt đầu nổi lên như một hiện tượng. Được phát triển mạnh mẽ, cùng với 5G, Internet vạn vật và chuỗi khối, đang hình thành các công nghệ, sản phẩm, định dạng và ngành mới, giúp quy trình sản xuất trở nên thông minh hơn, sự kết hợp giữa cung và cầu được tối ưu hóa hơn, do đó tạo ra những thay đổi lớn trong cơ cấu kinh tế và thúc đẩy hiệu suất làm việc. Trí thông minh nhân tạo là lĩnh vực then chốt của thế hệ AI mới. Trong môi trường Internet, trí thông minh của con người và máy móc hỗ trợ lẫn nhau nó làm tăng hiệu quả và tạo thành một "nhóm không gian trí tuệ" tích hợp giữa người máy và đối tượng để thể hiện đầy đủ trí tuệ nhân tạo.

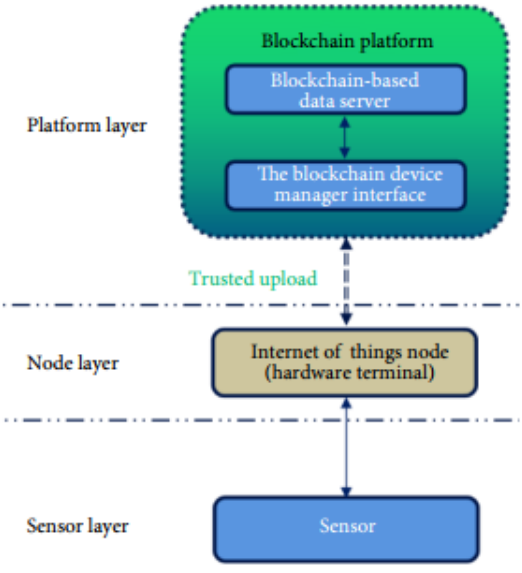
Bản chất của nó là cốt lõi trí tuệ của hệ sinh thái đổi mới khoa học và công nghệ Internet, lan tỏa đến các tổ chức bao gồm toàn bộ quá trình đổi mới từ nghiên cứu và phát triển công nghệ đến vận hành thương mại[2]. Do đó, nghiên cứu về trí thông minh nhân tạo không chỉ thúc đẩy đổi mới lý thuyết và công nghệ của AI mà còn đổi mới về ứng dụng, quản lý, hệ thống và kinh doanh của toàn xã hội thông tin.

Trong quá trình phát triển trí tuệ nhân tạo, cần có một kho dữ liệu lớn để hỗ trợ. Tuy nhiên, rủi ro bảo mật được tìm thấy trong các liên kết khác nhau, chẳng hạn như thu thập, truyền tải và chia sẻ dữ liệu. Bảo mật dữ liệu cũng là một trở ngại đối với sự phát triển của nền kinh tế kỹ thuật số. Do đó, bài báo này đề xuất một sơ đồ tải dữ liệu lên đáng tin cậy của các nút IoT dựa trên chuỗi khối, áp dụng tải lên đáng tin cậy để làm cho dữ liệu an toàn và đáng tin cậy, tạo môi trường dữ liệu lành mạnh và giúp phát triển trí thông minh nhân tạo ngày càng phát triển hơn.

2. Nội dung nghiên cứu

2.1. Sơ đồ thiết kế kiến trúc tổng thể

Kiến trúc hệ thống trong sơ đồ 2.1. Hệ thống tải lên đáng tin cậy bao gồm ba lớp: Platform layer, Note layer và Sensor layer.



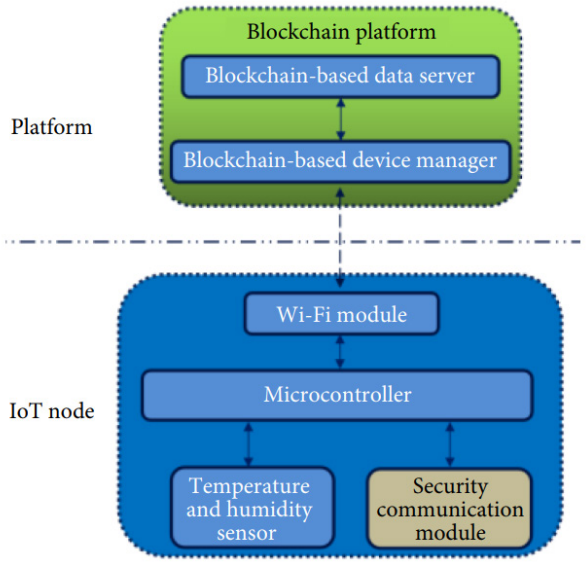
Sơ đồ 2.1. Sơ đồ kiến trúc hệ thống tổng thể

2.2. Thiết kế cho việc tải dữ liệu lên dựa trên công nghệ blockchain

Nền tảng Blockchain[3] là một thuật ngữ trong lĩnh vực công nghệ thông tin. Về bản chất, đó là một cơ sở dữ liệu được chia sẻ, với dữ liệu hoặc thông tin được lưu trữ dưới dạng "không thể giả mạo", "đầy đủ dấu vết", "có thể theo dõi", "mở và minh bạch", và "bảo trì". Dựa trên những đặc điểm này, công nghệ blockchain đã xây dựng một nền tảng "tin cậy" vững chắc, tạo ra một cơ chế "hợp tác" đáng tin cậy và thể ứng dụng rộng rãi. Các lợi ích của công nghệ blockchain bao gồm phi tập trung, mở cửa, tự trị, ẩn danh và thông tin không thể thay đổi. Trong số đó, khả năng không thể can thiệp vào thông tin là một lợi thế nổi bật. Hơn nữa, tính ổn định và bảo mật của dữ liệu rất cao. Nền tảng dữ liệu dựa trên công nghệ blockchain được áp dụng để thay thế nền tảng truyền thống, nhằm đảm bảo thêm tính đáng tin cậy của dữ liệu trên nền tảng.

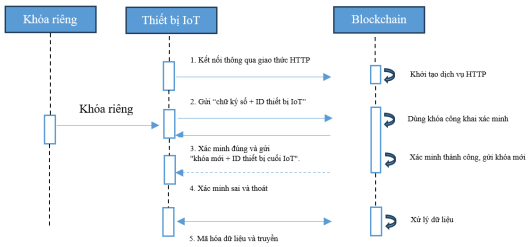
2.3. Triển khai tải dữ liệu lên

Triển khai phần cứng để xác nhận tải lên đáng tin cậy của các node IoT dựa trên blockchain. Việc triển khai tổng thể được trình bày trong sơ đồ 2.2. Cấu trúc lớp của Node: Vi điều khiển[4, mô-đun Wi-Fi. Thông tin chi tiết về lớp Node: Vi điều khiển giao tiếp với từng mô-đun để thực hiện các chức năng sau đây.



Sơ đồ 2.2. Sơ đồ tổng quan của hệ thống tải dữ liệu đáng tin cậy

Giao diện SPI được sử dụng để giao tiếp với mô-đun truyền thông an toàn để tạo cặp khóa SM2, chữ ký, mã hóa và giải mã, và mã hóa và giải mã SM4.

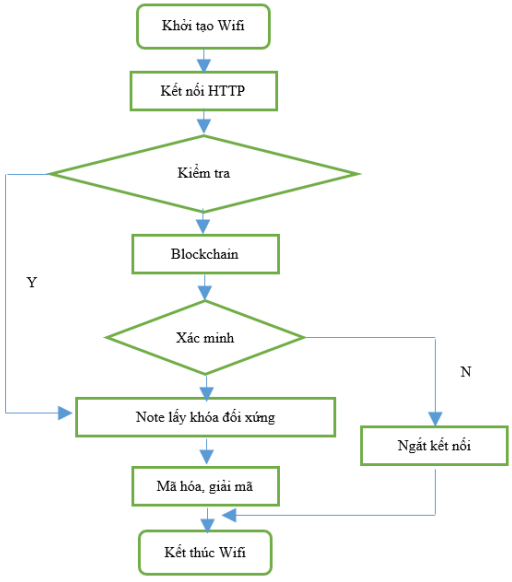


Sơ đồ 2.3. Biểu đồ luồng tương tác phần mềm của hệ thống tải dữ liệu lên

Giao diện USART được sử dụng để giao tiếp với mô-đun Wi-Fi và tiến hành giao tiếp dữ liệu với nền tảng cấu trúc. Cấu trúc lớp của nền tảng dựa trên quản lý thiết bị công nghệ blockchain và máy chủ dữ liệu công nghệ blockchain tạo nên nền tảng blockchain. Thông tin chi tiết về lớp nền tảng: Dựa trên quản lý thiết bị công nghệ blockchain, thiết lập một kết nối truyền tin tin cậy với node, đóng gói dữ liệu mã hóa của nó và gửi nó đến máy chủ dữ liệu công nghệ blockchain.

Triển khai phần mềm Quá trình tương tác phần mềm của hệ thống tải lên đáng tin cậy được hiển thị trong sơ đồ 2.3. Giao thức truyền thông mạng sử dụng HTTP, trong khi định dạng trao đổi dữ liệu sử dụng JSON. Quá trình cụ thể như sau.

(1) Vi điều khiển trong node giao tiếp với mô-đun truyền thông an toàn để tạo ra cặp khóa không đối xứng. Các node tiến hành chia một phần văn bản thuần để thu được bản tóm tắt, sau đó ký số cho bản tóm tắt. Gửi cùng lúc văn bản thuần, chữ ký số, khóa công khai và số ID duy nhất 15 byte đến nền tảng. (Nền tảng tìm khóa công khai tương ứng của node dựa trên ID duy nhất và kiểm tra giá trị chữ ký).



Sơ đồ 2.4. Biểu đồ luồng tác vụ Wi-Fi

(2) Nền tảng sử dụng khóa công khai để kiểm tra giá trị chữ ký. Nếu kiểm tra thành công, thì nền tảng đã kích hoạt node thành công. Tiếp theo, thực hiện việc kết nối node, và khóa công khai tương ứng với ID thiết bị. Phản hồi kết nối node một giá trị ngẫu nhiên làm muối dữ liệu mã hóa đối xứng sau này + số ID duy nhất 15 byte (vì khóa là số ngẫu nhiên, cần một giá trị cố định để xác nhận rằng khóa ngẫu nhiên đúng). Nền tảng sử dụng khóa công khai của node để mã hóa khóa và ID của chính nó; khi mã hóa văn bản nó sẽ được gửi trở lại node để xác minh. Nếu xác minh thất bại, kết nối sẽ bị ngắt.

```
----------------------------------------------------------Received http_post_chain
=== =
=== ==
HTTP/1.1 200
Content-Type: application/json;charset=UTF-8
Transfer-Encoding: chunked
Date: Wed, 23 Mar 2022 04:56:12 GMT

6c
{"code":200,"message":"","data":{"txId":"bdeb40b464b3ac8756b8b591068657be5a5a8f641e1f17823b0116ad2e087875"}}
0


---result_code->valueint = 200

http_post_data---OK

==================================

txId = bdeb40b464b3ac8756b8b591068657be5a5a8f641e1f17823b0116ad2e087875

==================================
```

Hình 2.2. Truy vấn kết quả dữ liệu được liên kết

(3) Node sử dụng quy trình giải mã bằng khóa riêng tư của mình (2) để thu được khóa đối xứng, được sử dụng cho mã hóa và tải lên dữ liệu. Khi hệ thống được bật, nó trước tiên khởi tạo từng phần ngoại vi và hệ điều hành, sau đó tạo ra các nhiệm vụ chờ, Wi-Fi, cảm biến và cuối cùng khởi động lõi. Nhiệm vụ Wi-Fi được hiển thị trong sơ đồ 2.4. Trước hết, thiết lập một kết nối HTTP để truy vấn xem cờ kích hoạt kết nối đã được đặt. Sau đó, thực hiện giải mã truyền thông. Nếu cờ kiểm tra chưa được đặt, thì gửi yêu cầu chữ ký và kích hoạt kết nối đến nền tảng, nền tảng sẽ kiểm tra và xử lý yêu cầu kích hoạt kết nối. Nếu kiểm tra thành công, thì node giải mã văn bản mã hóa để thu được khóa đối xứng và đặt cờ kích hoạt kết nối để thực hiện truyền thông mã hóa và giải mã. Nếu xác minh thất bại, kết nối sẽ bị ngắt.

2.4. Kết quả tải dữ liệu mã hóa

Nếu tải lên thành công, thì gói phản hồi HTTP chứa định dạng txID duy nhất; nếu tải lên thất bại, thì gói phản hồi không chứa txID. Dữ liệu kết quả của chuỗi có thể được truy vấn thông qua txID. Kết quả tải lên thành công được hiển thị như trong hình 2.1. Kết quả truy vấn dữ liệu được hiển thị như trong hình 2.2.

```
----------------------------------------------------------Received http_query_data

HTTP/1.1 200
Content-Type: application/json;charset=UTF-8
Transfer-Encoding: chunked
Date: Wed, 23 Mar 2022 06:04:30 GMT

2da
{"code":200,"message":"","data":[{"txId":"4d0dd7556d5aa5d1d20a9f69016d6a754d35980d50250a23254df71b70a0b226","blockHeight":1374,"senderOrgId":"wx-org3.chainmaker.org","senderPk":"f1157b03aad05f2112ca3e4d8baf2d702570a0bb9f11de5af00b08b5e9b31902","appEnableSyncNotify":0,"ruleId":"1498579715282366464","ruleVersion":3,"ruleEnableSyncNotify":0,"openId":"evidence","version":1,"timestamp":1648015464945,"bizParamsHash":"4aab3c87a90e84831a61f9f9f27053177d85de1fbc662f5fb295de2cb116bb59","bizData":{"rawData":{"appId":"130180","businessIdentification":"xyp130180","businessType":1,"businessUser":"iot_2.0","dataType":"A","equipmentId":"X00000000000001","humidity":"28.79","temperature":"20.31"}},"ruleName":"iot_ciphertextDataUpchain"}]}
```

Hình 2.1. Kết quả của chuỗi dữ liệu thành công

3. Kết luận

Bài báo này đề xuất một thiết kế cho hệ thống tải dữ liệu đáng tin cậy dựa trên nền tảng IoT, được thiết kế dựa trên ba khía cạnh của phần cứng node, liên kết truyền thông và nền tảng để thực hiện việc tải dữ liệu lên đáng tin cậy. Từ đó nguy cơ truy cập từ các thiết bị trái phép đến nền tảng dữ liệu được kiểm soát hiệu quả, đảm bảo tính hợp pháp của nguồn dữ liệu IoT. Thông qua cơ chế xác nhận khóa giữa các node IoT và nền tảng dữ liệu dựa trên blockchain, tính bảo mật của liên kết truyền thông có thể được đảm bảo trong khi đồng thời tránh được việc ăn cắp và tấn công. So với việc lưu trữ dữ liệu tập trung như bình thường, nền tảng dữ liệu dựa trên blockchain giảm thiểu mạnh mẽ rủi ro về việc tiết lộ thông tin riêng tư và can thiệp cố ý, giải quyết vấn đề nghẽn băng thông và tăng cường khả năng mở rộng của việc lưu trữ dữ liệu.

Tài liệu tham khảo

[1]. F. Wu, C. Lu, M. Zhu, H. Chen, J. Zhu, K. Yu, L. Li, M. Li, Q. Chen, X. Li, et al., Towards a new generation of artificial intelligence in China, Nat. Mach. Intell., vol. 2, no. 6, pp. 312–316, 2020

[2]. Y. Chai, C. Miao, B. Sun, Y. Zheng, and Q. Li, Crowd science and engineering: concept and research framework, International Journal of Crowd Science, vol. 1, no. 1, pp. 2-8, 2017.

[3]. K. Salah, N. Nizamuddin, R. Jayaraman, and M Omar, Blockchainbased soybean traceability in agricultural supply chain, IEEE Access, vol. 7, pp. 73295–73305, 2019

[4]. M. Gautschi, P. D. Schiavone, A. Traber, I. Loi, A. Pullini, D. Rossi, E. Flamand, F. K. Gürkaynak,