ĐẠI HỌC QUỐC GIA THÀNH PHỐ HỒ CHÍ MINH
TRƯỜNG ĐẠI HỌC KHOA HỌC TỰ NHIÊN
KHOA: CÔNG NGHỆ THÔNG TIN

Nguyễn Hải Tuyên - 21127474
Trần Minh Đạt - 21127570

HỆ THỐNG UY TÍN XÁC THỰC HỒ SƠ VÀ ĐÁNH GIÁ KỸ NĂNG

KHÓA LUẬN TỐT NGHIỆP CỬ NHÂN
CHƯƠNG TRÌNH CHẤT LƯỢNG CAO

GIẢNG VIÊN HƯỚNG DẪN
PGS. TS. Nguyễn Đình Thúc

Tp. Hồ Chí Minh, tháng 8 năm 2025

Lời cảm ơn

Mục lục

Chương 1

Giới thiệu chung

1.1 Đặt vấn đề

Trong quá trình tuyển dụng nguồn nhân lực hiện nay đối với các ngành nghề, đặc biệt là Công nghệ thông tin, việc xác thực trình độ học vấn, kỹ năng và kinh nghiệm của một cá nhân vẫn còn gặp nhiều khó khăn. Hiện nay, các nhà tuyển dụng và doanh nghiệp thường dựa vào chứng chỉ, bằng cấp hoặc thông tin do ứng viên cung cấp để đánh giá năng lực. Tuy nhiên, những thông tin này **có thể bị làm giả** hoặc không phản ánh chính xác thực lực của ứng viên.

Bên cạnh đó, nhiều cá nhân có kỹ năng thực tế nhưng lại không có cách nào để chứng minh năng lực của mình ngoài những hồ sơ truyền thống. Điều này làm hạn chế cơ hội phát triển và nâng cao giá trị của bản thân trong lĩnh vực. Vì vậy, cần có một giải pháp minh bạch, khách quan và đáng tin cậy để xác thực trình độ của mỗi cá nhân, đồng thời hỗ trợ doanh nghiệp đánh giá năng lực của ứng viên một cách thuận lợi và chính xác hơn.

Theo đó, ý tưởng về một **Hệ thống uy tín xác thực hồ sơ và đánh giá kỹ năng** được phát triển dựa trên công nghệ blockchain, cung cấp một nền tảng giúp cá nhân có thể chứng minh năng lực của mình một cách minh bạch, công khai và không thể thay đổi. Hệ thống cho phép người dùng tham gia các thử thách để kiểm tra và chứng minh kỹ năng, đồng thời áp dụng cơ chế đánh giá phi tập trung để đảm bảo tính khách quan.

Thay vì chỉ dựa vào văn bằng, chứng chỉ hay lời khai của ứng viên, hệ

thống này sẽ ghi nhận kết quả đánh giá được tích lũy lên blockchain và hệ thống lưu trữ phi tập trung, giúp tạo ra một hồ sơ uy tín đáng tin cậy, có thể sử dụng trên nhiều nền tảng khác nhau. Cộng đồng chuyên gia và nhà tuyển dụng có thể tham gia vào quá trình đánh giá để đảm bảo chất lượng, đồng thời giúp thúc đẩy sự phát triển của một hệ sinh thái xác thực năng lực trong lĩnh vực Công nghệ thông tin.

1.2 Mục tiêu

Đề tài nhằm xây dựng một hệ thống uy tín phi tập trung ứng dụng công nghệ blockchain để xây dựng và xác thực kỹ năng và hồ sơ cá nhân, bước đầu giới hạn trong lĩnh vực Công nghệ thông tin. Hệ thống sẽ cung cấp một môi trường và phương thức đánh giá minh bạch, khách quan và không thể thay đổi, giúp cá nhân chứng minh năng lực thực tế một cách đáng tin cậy, đồng thời hỗ trợ tổ chức và doanh nghiệp trong việc xác thực trình độ ứng viên.

Hệ thống hướng đến việc **tạo lập một môi trường đánh giá công bằng**, nơi mà năng lực của cá nhân được thể hiện thông qua kết quả thực tế, thay vì chỉ dựa vào chứng chỉ hoặc hồ sơ tự khai. Bên cạnh đó, việc ứng dụng blockchain giúp đảm bảo dữ liệu được bảo mật, minh bạch và có thể truy xuất dễ dàng, góp phần nâng cao độ tin cậy và hiệu quả trong quy trình tuyển dụng và đánh giá nhân sự.

Ngoài việc giải quyết bài toán xác thực hồ sơ, hệ thống còn tạo động lực để cá nhân **phát triển kỹ năng liên tục**, khi họ có thể tham gia các thử thách để cải thiện năng lực và nhận được sự công nhận từ cộng đồng. Với tiềm năng mở rộng, mô hình này có thể được áp dụng cho nhiều lĩnh vực khác, đóng góp vào xu hướng phát triển của các giải pháp phi tập trung trong tương lai.

1.3 Các nghiên cứu liên quan

1.3.1 Nghiên cứu trong nước

Bài nghiên cứu "Quản Lý Định Danh Phi Tập Trung"[1] là xuất phát điểm quan trọng của đề tài. Ý tưởng chính của bài nghiên cứu là việc xây dựng một thống quản lý định danh số nơi người dùng (chủ thể định danh) có toàn quyền kiểm soát đối với thông tin định danh của mình, thay vì phụ thuộc vào các nhà cung cấp dịnh vụ (Service Provider). Bài nghiên cứu đã đề xuất việc sử dụng công nghệ blockchain để xây dựng hệ thống định danh, bao gồm hai chủ thể chính: người dùng (chủ thể định danh) và nhà cung cấp dịnh vụ. Dữ liệu định danh của người dùng được lưu trữ cục bộ trên chính thiết bị của người dùng dưới dạng mã hóa và tham chiếu đến dữ liệu được lưu trên blockchain. Để quản lý dữ liệu mã hóa, cả chủ thể định danh và nhà cung cấp dịch vụ cần sử dụng giao thức tương tác DataTX. Chủ thể định danh có toàn quyền đối với dữ liệu của mình, có thể quản lý quyền truy cập thông qua giao thức tương tác AccessTx.

Bài nghiên cứu cũng đã định nghĩa về uy tín (reputation) như sau: "Uy tín được hình thành và biến đổi qua những thành công hay thất bại thực thể khi thực thi các nhiệm vụ cụ thể"[1, 2]. Có thể hiểu rằng, uy tín không phải là thực thể bất biến, mà luôn thay đổi theo thời gian và từng ngữ cảnh cụ thể. Không chỉ dừng lại ở một khái niệm lý thuyết đơn thuần, bài nghiên cứu đã đề xuất một hướng tiếp cận cụ thể để tính toán và số hóa khái niệm trừu tượng này bằng cách dựa vào hành vi (behavior) của các Node trong mạng, bao gồm người dùng (chủ thể định danh) và nhà cung cấp dịch vụ. Niềm tin của một thực thể (Node) được thiết lập là "giá trị kỳ vọng về hành vi tốt của Node trong tương lai"[1]. Kỳ vọng này chính là xác suất p trong phân phối Bernoulli, được tính bằng cách đếm số hành động của Node để tính xấp xỉ xác suất. [3, 1]

1.3.2 Nghiên cứu ngoài nước

Chúng tôi đã tham khảo từ các bài báo của dự án Rebooting the Web Of Trust (RWOT) [4, 5, 6]. Các công trình này đã đưa ra một khung khái niệm (conceptual framework) cơ bản cho một hệ thống uy tín, đặc biệt

trong việc đánh giá kỹ năng của một cá nhân khi tham gia vào mạng.

Bài báo [4] đã đề xuất một quy trình chung gồm các bước thao tác của các thực thể trong một hệ thống uy tín:

- Mỗi cá nhân tham gia vào mạng bằng một mã định danh phi tập trung (DID - Distributed Identifier).
- Chủ thể cần xây dựng uy tín sẽ tạo một tuyên bố (Assertion) và ký bằng khóa bí mật (Private Key) của mình.
- Để tăng tính thuyết phục của tuyên bố, chủ thể có thể tạo một bằng chứng (Evidence) và ký bằng khóa bí mật của mình, sau đó bổ sung tuyên bố ban đầu bằng cách tham chiếu đến bằng chứng vừa tạo.
- Các chủ thể khác tạo một bài đánh giá (Evaluation), ký bằng khóa bí mật của mình và tham chiếu đến tuyên bố của chủ thể cần xây dựng uy tín. Một bài đánh giá có thể ủng hộ hoặc thách thức tuyên bố gốc, có thể tham chiếu đến các bằng chứng (Evidence) để tăng tính thuyết phục.
- Cộng đồng sẽ tham gia bình chọn cho các bài đánh giá. Họ có thể lựa chọn đồng tình hoặc không đồng tình với bài đánh giá.

Bài báo [5] đã chỉ ra các yếu tố cốt lõi cần xem xét khi xây dựng một hệ thống uy tín phi tập trung, bao gồm bối cảnh (Context); sự tham gia của cộng đồng (Participation); sự đồng thuận của người dùng (User Consent); tính bảo mật (Confidentiality), khả năng tạo giá trị (Value Generation); hiệu suất hệ thống (Performance); tính bền vững của hệ thống (Sustainability); vòng đời của các tuyên bố (Claim Lifecycle); tính phục hồi sau các cuộc tấn công mạng (Resilience) và khía cạnh pháp lí (Legal).

Và bài báo [6] đã tập trung vào việc tìm kiếm giải pháp để số hóa khái niệm trừu tượng uy tín. Uy tín của một chủ thể phụ thuộc vào rất nhiều yếu tố và ngữ cảnh khác nhau, vì vậy việc biến những dữ liệu thô đầu vào thành dữ liệu đầu ra nhất quán, có thể xử lý được (actionable output) là một phần quan trọng trong một hệ thống uy tín. Cụ thể hơn, bài báo đã đưa ra một quy trình tuần tự, bao gồm việc xác định dữ liệu đầu ra (output), xác định dữ liệu thô đầu vào (raw input), xác định chất

lượng đầu vào và biên độ lỗi, chuẩn hóa dữ liệu để đưa về một dạng nhất quán, và cuối cùng là xử lý dữ liệu.

Nhìn chung, các nghiên cứu, bài báo mà chúng tôi đã tham khảo từ trong và ngoài nước đã định hình một ý tưởng sơ khai về một hệ thống uy tín phi tập trung. Các nghiên cứu, bài báo đã đề xuất những quy trình xử lý, cách thức tương tác giữa các chủ thể trong hệ thống, kiến trúc hệ thống, cũng như các khía cạnh cần xem xét trong một hệ thống uy tín. Qua đó, đã tạo tiền đề cho bài nghiên cứu này về việc xây dựng và triển khai một hệ thống uy tín trong thực tiễn.

1.4 Cách tiếp cận

Từ ý tưởng rút ra từ các nghiên cứu và bài báo đã tiến hành theo hướng đề tài này, chúng tôi có hướng tiếp cận tới hệ thống này như sau:

1.4.1 Các thành phần công nghệ chính

- Blockchain: sổ cái phi tập trung, có vai trò lưu trữ dữ liệu quan trọng trên chuỗi (on-chain) như thông tin người dùng, danh sách thử thách, danh sách giải pháp, chỉ số uy tín, quyền truy cập vào dữ liệu của người dùng,... Dữ liệu có thể chứa các tham chiếu (CID) của các dữ liệu lưu ngoài chuỗi (off-chain).

- Smart Contract: hợp đồng thông minh tương tác với blockchain để quản lý dữ liệu on-chain, đồng thời thực thi các tiến trình quan trọng như: tính toán chỉ số uy tín, cập nhật kết quả lưu trên chuỗi, thực hiện các biện pháp thưởng phạt theo quy ước.

- Kho lưu trữ dữ liệu phi tập trung (dStorage): dịch vụ lưu trữ phi tập trung dùng để lưu trữ dữ liệu người dùng, nội dung của các *thử thách*, các *giải pháp* của nó, và các dữ liệu lớn cần lưu trữ ngoài chuỗi.

1.4.2 Các chủ thể tương tác

- *Người đóng góp* (Contributor): là những người dùng tạo các thử thách, có trách nhiệm đóng góp ngân hàng thử thách của hệ thống.
- *Người kiểm duyệt* (Moderator): là những người có trách nhiệm kiểm duyệt các thử thách do người đóng góp tạo ra, thực hiện phân loại, đánh giá, và kiểm định chất lượng của thử thách. Để trở thành người kiểm duyệt, người dùng phải thỏa mãn các điều kiện cụ thể được quy định bởi hệ thống.
- *Người dùng* (User): là những người có nhu cầu xây dựng uy tín, có thể tìm kiếm các thử thách, tham gia và đưa ra các giải pháp cho thử thách tương ứng.
- *Người đánh giá* (Evaluator): là những người tham gia vào quá trình đánh giá giải pháp mà người dùng đưa ra cho một thử thách.
- *Phòng tuyển dụng của các công ty* (Companies' recruitment department): là đội ngũ tuyển dụng của các công ty có nhu cầu tuyển dụng những ứng viên phù hợp.

1.4.3 Các tập dữ liệu

- Ngân hàng thử thách: kho tàng các thử thách được đóng góp bởi các Contributor, mỗi thử thách sẽ có tiêu đề, mô tả, loại thử thách, lượng token treo thưởng, v.v.
- Bộ kết quả kiểm duyệt: một thử thách sẽ nhận được nhiều điểm số từ nhiều Moderator khác nhau trước khi nó được công khai cho User tham gia.
- Bộ danh sách giải pháp: một thử thách sẽ có nhiều giải pháp khác nhau được cung cấp bởi nhiều User khác nhau.
- Bộ kết quả đánh giá: một giải pháp sẽ nhận được nhiều điểm số từ nhiều Evaluator khác nhau.

- Danh sách bài tuyển dụng: các bài tuyển dụng được đăng tải bởi các đội ngũ tuyển dụng, mỗi bài tuyển dụng sẽ có tiêu đề, mô tả công việc, yêu cầu về điểm uy tín, v.v.
- Bộ thông tin ứng tuyển: một bài tuyển dụng sẽ được nhiều User khác nhau ứng tuyển.
- Danh sách các cuộc họp trực tuyến: những buổi gặp mặt trực tuyến được lên lịch bởi đội ngũ tuyển dụng dành cho một User cho một bài tuyển dụng nhất định.
- Hồ sơ người dùng:
  - Thông tin cá nhân, chẳng hạn như địa chỉ ví, tên, email, ảnh đại diện, v.v.
  - Chỉ số uy tín của người dùng trên hệ thống
  - Lịch sử tham gia thử thách
- Thông tin giao dịch token: phản ánh việc đóng góp và tham gia thử thách, đánh giá giải pháp, đăng bài tuyển dụng và ứng tuyển, và sự biến động về chỉ số uy tín.

1.4.4 Kịch bản tương tác giữa các chủ thể

- **Tạo thử thách**
  - Người đóng góp (Contributor) tạo và đăng tải các thử thách lên hệ thống. Nội dung của thử thách được lưu trữ và chia sẻ lên dStorage.
  - Mỗi thử thách phải thuộc về một loại thử thách nhất định (ví dụ: Khoa học máy tính, An ninh mạng, Phát triển phần mềm, v.v.)
  - Hệ thống lưu nội dung của thử thách ở dStorage. Smart Contract cập nhật danh sách các thử thách trên chuỗi chứa các CID tham chiếu đến nội dung của thử thách ở dStorage.

  - Các thử thách vừa tạo ở trạng thái chưa kiểm duyệt, cần phải thông qua ý kiến của những người kiểm duyệt (Moderator).
  - Sau giai đoạn kiểm duyệt, nếu thử thách đạt mức độ và được hội đồng tán thành sẽ chuyển sang trạng thái đã kiểm duyệt. Những người cần xây dựng uy tín có thể tham gia vào thử thách.

- **Kiểm duyệt thử thách**
  - Những người kiểm duyệt (Moderator) đọc nội dung của thử thách, kiểm tra chất lượng và mức độ phù hợp của thử thách. Sau đó, những người kiểm duyệt tiến hành bỏ phiếu về các thông tin như: phân loại của thử thách, độ khó, mức độ phù hợp . . .
  - Smart Contract tổng hợp đánh giá của những Moderator, dựa trên một công thức tính đã quy định sẵn để tổng hợp ra kết quả cuối cùng.
  - Smart Contract cập nhật thông tin liên quan của thử thách đã lưu trên chuỗi.

- **Tham gia thử thách và đánh giá**
  - Người dùng (User) trả một khoản token nhất định cho Contributor để tham gia thử thách.
  - Hệ thống tự động tạo một không gian làm việc nơi User có thể tạo giải pháp của mình.
  - User thiết lập một phiên đánh giá với số lượng tối đa Người đánh giá (Evaluator) cố định có thể tham gia chấm điểm. Evaluator có thể đánh giá bằng cách tham gia vào phiên.
  - Sau khi hoàn thành đánh giá, mỗi Evaluator sẽ nộp số điểm.
  - Smart Contract thu thập tất cả điểm số từ Evaluator, áp dụng thuật toán tính điểm để xác định số điểm cuối cùng.
  - Những Evaluator có điểm số gần với kết quả chính xác nhất sẽ nhận thêm điểm uy tín cho bản thân. Evaluator có điểm số

lệch xa với kết quả nhất (hoặc biên độ lệch vượt quá giới hạn đã quy định sẵn) sẽ bị trừ đi điểm uy tín.

  - Smart Contract sau đó cập nhật kết quả lên blockchain để đảm bảo tính minh bạch và không thể chỉnh sửa.
  - Điểm số của giải pháp sẽ làm thay đổi chỉ số uy tín của User trong một loại thử thách cụ thể.

- **Đăng bài tuyển dụng và ứng tuyển**
  - Đội ngũ tuyển dụng của các công ty tạo và đăng tải các bài tuyển dụng kèm theo yêu cầu về chỉ số uy tín của ứng viên.
  - Ứng viên tiến hành ứng tuyển vào các bài tuyển dụng.
  - Nhà tuyển dụng lúc này có thể xem được chỉ số uy tín của ứng viên và có thể truy cập lịch sử tham gia thử thách.
  - Smart Contract cập nhật dữ liệu quyền truy cập lưu trên chuỗi (nếu có).
  - Nhà tuyển dụng có thể lên lịch các cuộc họp trực tuyến để phỏng vấn ứng viên.
  - Đội ngũ tuyển dụng xem xét và quyết định tuyển dụng đối với User. Nếu có, công ty cần trả một khoản token cho hệ thống.

1.5 Đóng góp của đề tài

Đề tài mang lại những đóng góp chính sau:

- **Đề xuất một mô hình hệ thống uy tín phi tập trung** ứng dụng công nghệ blockchain để xác thực kỹ năng và hồ sơ cá nhân một cách minh bạch, khách quan và không thể thay đổi. Mô hình này hướng đến việc xây dựng một chuẩn đánh giá năng lực mới trong lĩnh vực Công nghệ thông tin.
- **Thiết kế kiến trúc hệ thống đầy đủ** với các thành phần chính như Smart Contract, blockchain, dịch vụ lưu trữ phi tập trung (dStorage), cùng luồng tương tác rõ ràng giữa các chủ thể trong hệ thống

như người dùng, người đóng góp, người kiểm duyệt, người đánh giá và nhà tuyển dụng.

- **Xây dựng cơ chế đánh giá dựa trên cộng đồng (community-driven assessment)** kết hợp với hệ thống tính điểm uy tín nhằm đảm bảo tính công bằng, chống gian lận và khuyến khích sự tham gia tích cực từ nhiều bên liên quan.
- **Triển khai một hệ thống minh họa (prototype)** hoạt động được ở môi trường cục bộ, bao gồm giao diện người dùng, backend tích hợp Smart Contract, khả năng lưu trữ dữ liệu phi tập trung và cơ chế đánh giá thử thách.
- **Đóng góp vào hướng nghiên cứu về hệ thống đánh giá phi tập trung và quản lý danh tiếng**, mở ra khả năng mở rộng mô hình cho các lĩnh vực khác ngoài Công nghệ thông tin, phù hợp với xu hướng ứng dụng công nghệ blockchain trong quản lý dữ liệu và xác thực hồ sơ.

Chương 2

Các hệ thống và công nghệ liên quan

2.1 ReGreT

ReGreT [7] là một mô hình đánh giá uy tín trong xã hội nhiều tác nhân (multi-agent society), được xây dựng nhằm mô phỏng cách con người hình thành và sử dụng danh tiếng trong các tương tác xã hội. Mô hình này mở rộng so với các mô hình trước bằng cách đưa ra ba chiều chính (dimension) của uy tín: chiều cá nhân, chiều xã hội, và chiều bản thể học (ontological).

2.1.1 Chiều cá nhân

Đây là mức độ cơ bản nhất của uy tín, dựa trên trải nghiệm trực tiếp giữa hai tác nhân. Khi hai tác nhân tương tác, mỗi bên ghi nhận *kết quả* (outcomes) từ tương tác đó, bao gồm những gì đã được thỏa thuận và những gì thực sự xảy ra. Dựa vào những kết quả này, mỗi tác nhân hình thành *ấn tượng cá nhân* (impressions), từ đó tính ra *uy tín chủ quan* (subjective reputation). Bên cạnh đó, cũng sẽ một *độ tin cậy* (reliability) đối với uy tín chủ quan này. Những ấn tượng gần thời điểm hiện tại hơn sẽ được ưu tiên cao hơn thông qua hàm trọng số thời gian.

Từ đó, ReGreT định nghĩa cách tính uy tín trực tiếp của một tác nhân

a đối với tác nhân b (chiều cá nhân) như sau:

$$R_{a \to b}(subject)$$

2.1.2 Chiều xã hội

ReGreT mô hình hóa hiện tượng phổ biến trong xã hội con người: một cá nhân mang theo uy tín của nhóm mà họ thuộc về. Nếu không có đủ thông tin trực tiếp, ta có thể dựa vào uy tín nhóm để ước lượng hành vi của một tác nhân. Tương tự như cách một cá nhân có thể bị ảnh hưởng bởi uy tín của nhóm mà mình thuộc về, bản thân cá nhân đó cũng sẽ dựa vào *trải nghiệm* (experiences) của những người trong chính nhóm của mình để bổ sung và củng cố hiểu biết cá nhân về một thực thể. Nói cách khác, những gì mà các thành viên trong nhóm từng trải qua với một thực thể cụ thể (hoặc với nhóm của thực thể đó) sẽ góp phần định hình và làm phong phú thêm nhận định của mỗi thành viên trong nhóm.

Do đó, để tính giá trị uy tín của mình đối với một tác nhân theo chiều xã hội, ReGreT mở rộng thêm ba nguồn thông tin mới. Bên cạnh tương tác trực tiếp với chính tác nhân, giờ đây phải xem xét thêm tương tác với các thành viên trong nhóm mà tác nhân đó thuộc về, thông tin mà nhóm của mình đối với tác nhân đó, và cuối cùng là thông tin mà nhóm của mình đối với nhóm của tác nhân đó.

Trải nghiệm cá nhân

Giả sử ta tính giá trị uy tín của một tác nhân a thuộc về nhóm $\mathcal{A}$ đối với tác nhân b thuộc về nhóm $\mathcal{B}$. Đầu tiên, ta đã biết uy tín trực tiếp giữa hai tác nhân như sau:

$$R_{a \to b}(subject)$$

Tiếp theo, sự tương tác của a đối với các thành viên khác của nhóm $\mathcal{B}$ được biểu diễn như sau:

$$R_{a \to \mathcal{B}}(subject) = \sum_{b_i \in \mathcal{B}} \omega^{ab_i} \cdot R_{a \to b_i}(subject)$$

trong đó, $\sum_{b_i \in \mathcal{B}} \omega^{ab_i} = 1$. Vì đang trong trường hợp uy tín chủ quan,

chúng ta cần phương thức để thể thiện độ tin cậy của uy tín này:

$$RL_{a\to\mathcal{B}}(subject) = \sum_{b_i\in\mathcal{B}} \omega^{ab_i} \cdot RL_{a\to b_i}(subject)$$

Trải nghiệm nhóm

Một khi đã có được trải nghiệm của cá nhân a, ta sẽ xem xét đến trải nghiệm của nhóm $\mathcal{A}$ đối với tác nhân b và cả nhóm $\mathcal{B}$.

Đầu tiên, ta tính uy tín chủ quan của nhóm $\mathcal{A}$ đối với tác nhân b cùng với độ tin cậy của uy tín như sau:

$$R_{\mathcal{A}\to b}(subject) = \sum_{a_i\in\mathcal{A}} \omega^{a_i b} \cdot R_{a_i\to b}(subject)$$

$$RL_{\mathcal{A}\to b}(subject) = \sum_{a_i\in\mathcal{A}} \omega^{a_i b} \cdot RL_{a_i\to b}(subject)$$

trong đó, $\sum_{a_i\in\mathcal{A}} \omega^{a_i b} = 1$.

Tương tự, để biết được uy tín của nhóm $\mathcal{A}$ đối với nhóm $\mathcal{B}$, ta tính như sau:

$$R_{\mathcal{A}\to\mathcal{B}}(subject) = \sum_{a_i\in\mathcal{A}} \omega^{a_i\mathcal{B}} \cdot R_{a_i\to\mathcal{B}}(subject)$$

$$RL_{\mathcal{A}\to\mathcal{B}}(subject) = \sum_{a_i\in\mathcal{A}} \omega^{a_i\mathcal{B}} \cdot RL_{a_i\to\mathcal{B}}(subject)$$

trong đó, $\sum_{a_i\in\mathcal{A}} \omega^{a_i\mathcal{B}} = 1$.

Tổng hợp tất cả thông tin lại với nhau

Cuối cùng, ReGreT định nghĩa cách tính uy tín của tác nhân a đối với tác nhân b theo chiều xã hội như sau:

$$\begin{aligned} SR_{a\to b}(subject) = {} & \xi_{ab} \cdot R_{a\to b}(subject) + \\ & \xi_{a\mathcal{B}} \cdot R_{a\to\mathcal{B}}(subject) + \\ & \xi_{\mathcal{A}b} \cdot R_{\mathcal{A}\to b}(subject) + \\ & \xi_{\mathcal{A}\mathcal{B}} \cdot R_{\mathcal{A}\to\mathcal{B}}(subject) \end{aligned}$$

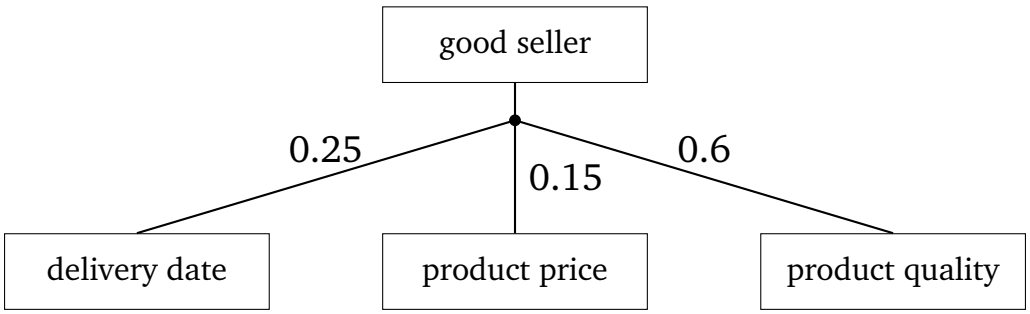
$$
\begin{aligned}
SRL_{a\to b}(subject) = \xi_{ab} \cdot RL_{a\to b}(subject) + \\
\xi_{a\mathcal{B}} \cdot RL_{a\to \mathcal{B}}(subject) + \\
\xi_{\mathcal{A}b} \cdot RL_{\mathcal{A}\to b}(subject) + \\
\xi_{\mathcal{A}\mathcal{B}} \cdot RL_{\mathcal{A}\to \mathcal{B}}(subject)
\end{aligned}
$$

trong đó, $\xi_{ab} + \xi_{a\mathcal{B}} + \xi_{\mathcal{A}b} + \xi_{\mathcal{A}\mathcal{B}} = 1$.

2.1.3 Chiều bản thể học

Trong hai chiều cá nhân và xã hội, mỗi lần đánh giá uy tín chỉ tập trung vào một khía cạnh đơn lẻ. Tuy nhiên, trong thực tế, các khía cạnh này thường liên quan đến nhau và cần được kết hợp cùng *trọng số* của từng khía cạnh lại để hình thành một khái niệm uy tín phức tạp hơn – đó chính là mục tiêu của **chiều bản thể học**.

Ở chiều này, mô hình ReGreT sử dụng cấu trúc đồ thị để mô tả mối quan hệ giữa các khía cạnh khác nhau của uy tín. Ví dụ, *một người bán hàng tốt* (good seller) có thể bao gồm các yếu tố: giao hàng nhanh, giá cả hợp lý, và chất lượng sản phẩm cao, ta có cấu trúc đồ thị bản thể như hình 2.1 để mô hình hóa mối quan hệ giữa các khía cạnh trong ví dụ này.



Hình 2.1: Cấu trúc đồ thị bản thể cho “một người bán hàng tốt”

Vì vậy, khi muốn tính một uy tín phức hợp theo chiều bản thể học, một tác nhân cần tính uy tín của từng khía cạnh liên quan. Mỗi khía cạnh này có thể lại là một nút trong một đồ thị con, nơi nó cũng được cấu thành từ các khía cạnh nhỏ hơn nữa.

Đối với những nút cuối cùng trong đồ thị (các khía cạnh cơ bản nhất của hành vi, gọi là *atomic aspect*), thì uy tín của chúng được tính dựa trên chiều cá nhân và chiều xã hội.

Sau khi có điểm uy tín cho từng nút con, điểm uy tín của một nút bất kỳ i trong đồ thị bản thể sẽ được tính bằng cách kết hợp các giá trị của các nút con của nó theo một công thức:

$$OR_{a\to b}(i) = \sum_{j\in children(i)} w_{ij} \cdot OR_{a\to b}(j)$$

$$ORL_{a\to b}(i) = \sum_{j\in children(i)} w_{ij} \cdot ORL_{a\to b}(j)$$

trong đó, $OR_{a\to b}(j) = SR_{a\to b}(j)$ khi j là một khía cạnh cơ bản.

Đối với ví dụ ở hình 2.1, ta có thể tính giá trị uy tín của b (người bán hàng tốt) từ góc nhìn của a bằng công thức:

$$\begin{aligned} OR_{a\to b}(good\ seller) = {} & 0.25 \cdot SR_{a\to b}(delivery\ date) + \\ & 0.15 \cdot SR_{a\to b}(product\ price) + \\ & 0.6 \cdot SR_{a\to b}(product\ quality) \end{aligned}$$

2.2 EigenTrust

Mạng chia sẻ tập tin ngang hàng (P2P) đang ngày càng trở nên phổ biến nhờ ưu điểm không cần máy chủ trung tâm, có khả năng mở rộng tốt và cung cấp nhiều dữ liệu đa dạng. Tuy nhiên, đặc tính ẩn danh và mở của P2P cũng khiến hệ thống này dễ bị lạm dụng, không ai chịu trách nhiệm rõ ràng cho nội dung mà họ chia sẻ. Kết quả là tệp tin giả mạo, virus, hoặc nội dung bị chỉnh sửa có thể được phát tán rộng rãi, các peer độc hại có thể dễ dàng lừa người dùng tải về nội dung sai.

EigenTrust [8] được giới thiệu là một thuật toán giảm thiểu khả năng tải về các tập tin độc hại bằng cách gán mỗi peer một *giá trị tin cậy toàn cục* (global trust value) duy nhất, dựa trên lịch sử tải lên của peer đó. Mỗi peer trong mạng cùng tham gia tính toán điểm tin cậy của nhau theo cách phân tán và đối xứng. Khi tải tập tin về, các peer sẽ ưu tiên chọn nguồn tải là những peer có điểm tin cậy cao, giúp giảm đáng kể số lượng tập tin không xác thực.

2.2.1 Giá trị tin cậy cục bộ

Mỗi peer trong hệ thống mạng P2P cho phép theo dõi lịch sử giao dịch của nhau và đánh giá lẫn nhau sau mỗi giao dịch. Ví dụ, mỗi khi peer i tải tập tin từ peer j, nó có thể gán điểm tích cực $(tr(i,j) = 1)$ nếu hài lòng, hoặc điểm tiêu cực $(tr(i,j) = -1)$ nếu gặp vấn đề như tập tin bị hỏng, giả mạo hoặc quá trình tải thất bại. Từ các đánh giá này, một *giá trị tin cậy cục bộ* (local trust value) có thể được tính bằng cách cộng các điểm đánh giá mà peer i đã gán cho j, biểu diễn là $s_{ij} = \sum tr_{ij}$.

Ngoài ra, có thể biểu diễn giá trị này bằng cách lưu số lượng giao dịch hài lòng $sat(i,j)$ và không hài lòng $unsat(i,j)$, rồi tính:

$$st_{ij} = sat(i,j) - unsat(i,j)$$

2.2.2 Chuẩn hóa giá trị tin cậy cục bộ

Trước tiên, cần chuẩn hóa các giá trị tin cậy cục bộ sat_{ij} để đảm bảo tính công bằng. Nếu không chuẩn hóa, một peer độc hại có thể đánh giá tích cực cho các peer độc hại khác và đánh giá tiêu cực cho các peer có uy tín cao. Để chuẩn hóa, ta chỉ xét các đánh giá tích cực, và tính xác suất chọn mỗi peer j khi được peer i tin tưởng như sau:

$$c_{ij} = \frac{max(s_{ij}, 0)}{\sum_j max(s_{ij}, 0)}$$

Cách làm này đảm bảo các giá trị c_{ij} nằm trong khoảng $[0, 1]$ và có thể được hiểu như một xác suất trong mô hình ngẫu nhiên (chú ý: nếu $\sum_j max(s_{ij}, 0) = 0$ thì c_{ij} sẽ không xác định, vấn đề này sẽ được giải quyết sau đó). Tuy nhiên, có một số hạn chế: nếu $c_{ij} = c_{ik}$, ta chỉ biết peer j và k được i đánh giá ngang nhau, chứ không biết là tốt hay trung bình. Dù vậy, việc chuẩn hóa theo cách này giúp quá trình tính toán hiệu quả hơn và dễ dàng áp dụng mô hình xác suất.

2.2.3 Tổng hợp các giá trị tin cậy cục bộ

Sau khi chuẩn hóa, mục tiêu là tổng hợp các đánh giá cục bộ để thu được cái nhìn rộng hơn về độ tin cậy của từng peer. Điều này được thực hiện bằng cách áp dụng **transitive trust** (tạm dịch: niềm tin chuyển tiếp) – nghĩa là peer i sẽ hỏi ý kiến những người mà nó tin tưởng, và kết hợp đánh giá của họ với trọng số tương ứng.

Quá trình tổng hợp này dẫn đến một biểu thức dạng:

$$t_{ik} = \sum_j c_{ij} c_{jk}$$

trong đó, t_{ik} thể hiện niềm tin của peer i đối với k sau khi hỏi bạn bè của nó (j), mỗi người bạn của i lại đánh giá k một cách riêng (c_{jk}). Ta có thể biểu diễn biểu thức trên thành ma trận: nếu ta gọi C là ma trận $[c_{ij}]$ và $\vec{t_i}$ là vector chứa các giá trị t_{ik}, khi đó ta có $\vec{t_i} = C^T \vec{c_i}$.

Ma trận trên có thể mở rộng khi peer i hỏi thêm những người bạn của bạn mà i đã hỏi ($(C^T)^2, (C^T)^3, ..., (C^T)^n$), và khi n đủ lớn, vector $\vec{t_i}$ sẽ hội tụ về một vector *duy nhất cho mỗi peer* i – đó chính là vector riêng chính của ma trận tin cậy chuẩn hóa C. Nói cách khác, $\vec{t}$ là *vector tin cậy toàn cục* (global trust vector) trong mô hình này, và mỗi phần tử của nó, $\vec{t_j}$, định lượng mức độ tin cậy của hệ thống nói chung đặt vào peer j.

2.2.4 Giải thích về xác suất

Cách hiểu xác suất cung cấp một góc nhìn trực quan cho quá trình lan truyền uy tín trong mạng. Tưởng tượng có một tác nhân ngẫu nhiên đi lang thang trong mạng P2P để tìm peer đáng tin. Tại mỗi bước, khi đang đứng ở peer i, nó sẽ chuyển đến peer j với xác suất là c_{ij} – tức là mức độ mà i tin tưởng j. Quá trình này tạo thành một **xích Markov** [9] với ma trận chuyển xác suất là ma trận tin cậy chuẩn hóa C. Sau nhiều bước di chuyển, tác nhân sẽ thường xuyên rơi vào những peer đáng tin hơn – và xác suất dừng lại ở mỗi peer chính là mức độ danh tiếng toàn cục.

Điều này giống như mô hình "Random Surfer" [10] trong PageRank: dù đi lung tung, người dùng sẽ thường ghé lại các trang web đáng tin và phổ biến hơn.

2.2.5 Phiên bản EigenTrust cơ bản

Trong phiên bản đơn giản nhất, ta giả sử có một máy chủ trung tâm lưu trữ tất cả giá trị c_{ij}, mục tiêu chính là tính được giá trị tin cậy toàn cục $\vec{t} = C^T\vec{e}$, với vector khởi đầu là $\vec{e}$ thể hiện phân bố xác suất đồng đều của toàn bộ m peer, tức $e_i = 1/m$. Chi tiết tại thuật toán 1.

Algorithm 1 Thuật toán EigenTrust đơn giản

$\vec{t}^{(0)} = \vec{e}$
repeat
  $\vec{t}^{(k+1)} = C^T\vec{t}^{(k)}$
  $\delta = ||\vec{t}^{(k+1)} - \vec{t}^{(k)}||$
until $\delta < \epsilon$

Tuy nhiên, có ba vấn đề thực tiễn mà thuật toán 1 không thể xử lý: nhóm peer có uy tín sẵn, những peer không hoạt động, và các peer độc hại hợp tác với nhau.

Nhóm peer có uy tín sẵn. Một hệ thống mạng P2P chỉ có một vài peer là có uy tín cao, thường là những người đầu tiên tham gia hệ thống, chẳng hạn như những nhà phát triển hay những người dùng truy cập sớm. Ta định nghĩa tập hợp P là các peer có uy tín sẵn (pre-trusted peers) và $\vec{p}$ là vector khởi đầu thay cho $\vec{e}$, với:

$$p_i = \begin{cases} 1/|P|, & \text{nếu } i \in P \\ 0, & \text{ngược lại} \end{cases}$$

điều này giúp hội tụ nhanh hơn, cũng như loại bỏ được các peer độc hại.

Những peer không hoạt động. Nếu peer i chưa từng tương tác với ai, thì không thể tính được c_{ij} (do không thể chia hết cho 0). Khi đó, ta sẽ sử dụng p_j thay thế cho c_{ij}, tức là nếu peer i không tương tác với ai, không tin tưởng ai thì sẽ chọn peer có uy tín sẵn.

Các peer độc hại hợp tác với nhau. Có khả năng sẽ xuất hiện nhiều nhóm peer độc hại mà chúng biết lẫn nhau, bọn chúng sẽ đánh giá cao lẫn nhau và đánh giá thấp những peer có uy tín. Để ngăn chặn điều này, ta trộn thêm $\vec{p}$ vào mỗi vòng lặp:

$$\vec{t}^{(k+1)} = (1-a)C^T\vec{t}^{(k)} + a\vec{p}$$

trong đó, a là một hằng số nhỏ hơn 1. Việc này giúp "kéo" giá trị $\vec{c_i}$ của các peer về phía nhóm peer P nhằm phá vòng lặp tin tưởng nội bộ của nhóm độc hại.

Cuối cùng, ta hoàn thiện thuật toán EigenTrust cơ bản như sau:

Algorithm 2 Thuật toán EigenTrust cơ bản

$\vec{t}^{(0)} = \vec{p}$
repeat
  $\vec{t}^{(k+1)} = C^T \vec{t}^{(k)}$
  $\vec{t}^{(k+1)} = (1-a)\vec{t}^{(k+1)} + a\vec{p}$
  $\delta = ||\vec{t}^{(k+1)} - \vec{t}^{(k)}||$
until $\delta < \epsilon$

2.2.6 EigenTrust phân tán

Ở đây, bài toán được mở rộng để không cần máy chủ trung tâm, mà mỗi peer tự tính toán uy tín của chính mình bằng thông tin từ những peer từng tương tác với nó. Yêu cầu đầu tiên của bài toán này là mỗi peer i phải lưu trữ vector tin cậy cục bộ $\vec{c_i}$ và giá trị tin cậy toàn cục t_i của chính nó. Mỗi peer có thể tính giá trị tin cậy toàn cục của mình như sau:

$$t_i^{(k+1)} = (1-a)(c_{1i}t_1^{(k)} + ... + c_{ni}t_n^{(k)}) + ap_i$$

Từ đó, ta có được thuật toán EigenTrust phân tán cơ bản được thể hiện ở thuật toán 3. Vì mỗi peer chỉ tương tác với một số peer nhỏ (không phải toàn mạng), việc tính toán và truyền tin cũng nhẹ nhàng và hiệu quả. Trong trường hợp một mạng lưới có nhiều peer hoạt động mạnh, ta có thể duy trì những lợi ích trên bằng cách giới hạn số lượng giá trị tin cậy cục bộ c_{ij} mà mỗi peer có thể báo cáo.

Algorithm 3 Thuật toán EigenTrust phân tán

Definitions

- A_i: set of peers which have downloaded files from peer i
- B_i: set of peers from which peer i has downloaded files

Algorithm

Each peer i do {

Query all peers $j \in A_i$ for $t_j^0 = p_j$;

repeat

Compute $t_i^{(k+1)} = (1-a)(c_{1i}t_1^{(k)} + c_{2i}t_2^{(k)} + ... + c_{ni}t_n^{(k)}) + ap_i$

Send $c_{ij}t_i^{(k+1)}$ to all peers $j \in B_i$

Compute $\delta = |t^{(k+1)} - t^{(k)}|$

Wait for all peers of $j \in A_i$ to return $c_{ji}t_j^{(k+1)}$

until $\delta < \epsilon$

}

Chương 3

Hệ thống SkillChain

Chương 4

Kết quả

Chương 5

Kết luận

Tài liệu tham khảo

[1] N. Đình Thúc, "Quản lý Định danh phi tập trung." Tài liệu nội bộ được cung cấp bởi giảng viên hướng dẫn.

[2] T. Grandison and M. Sloman, "A survey of trust in internet applications," *IEEE Communications Surveys and Tutorials*, vol. 3, pp. 2–16, 01 2000.

[3] N. Đình Thúc, Đặng Hải Vân, and L. Phong, *Thống kê máy tính*. Nhà xuất bản Khoa học và kỹ thuật, 2010.

[4] C. Allen, T. Daubenschütz, M. Sporny, N. Thorp, H. Wood, G. Willen, and A. Voto, "Portable reputation toolkit use cases." GitHub Repository, 2017. A White Paper from Rebooting the Web of Trust III Design Workshop.

[5] A. C. de Crespigny, D. Khovratovich, F. Blondeau, K. Sok, P. Honigman, N. Alexopoulos, F. Petitcolas, and S. Conway, "Design considerations for decentralized reputation systems." GitHub Repository, 2017. A White Paper from the Rebooting the Web of Trust IV Design Workshop.

[6] A. Brock, K. Hamlin, G. R. Rachmany, and J. Lanc, "Reputation interpretation." GitHub Repository, 2019. A white paper from Rebooting the Web of Trust IX.

[7] J. Sabater and C. Sierra, "Regret: reputation in gregarious societies," in *Proceedings of the Fifth International Conference on Autonomous Agents*, AGENTS '01, (New York, NY, USA), p. 194–195, Association for Computing Machinery, 2001.

[8] S. D. Kamvar, M. T. Schlosser, and H. Garcia-Molina, "The eigentrust algorithm for reputation management in p2p networks," in *Proceedings of the 12th International Conference on World Wide Web*, WWW '03, (New York, NY, USA), p. 640–651, Association for Computing Machinery, 2003.

[9] Wikipedia contributors, "Markov chain — Wikipedia, the free encyclopedia," 2025. [Online; accessed 25-June-2025].

[10] P. Chebolu and P. Melsted, "Pagerank and the random surfer model.," in *SODA*, vol. 8, pp. 1010–1018, 2008.

Phụ lục