

Tính riêng tư cho Định danh số (Privacy for Digital Identity)

1. Giới thiệu về định danh số

Trong xã hội hiện đại, mọi thứ đều có thể là định danh: thẻ căn cước, hộ chiếu, giấy phép lái xe, giấy xác nhận đã tiêm vaccin, thẻ sinh viên, tài khoản Google... Mọi người sử dụng định danh để chứng minh một số thuộc tính của mình. Ví dụ, bằng cách đưa ra thẻ căn cước, một thanh niên có thể chứng minh rằng *anh ta đã hơn 18 tuổi, sống ở quận nội thành Hà Nội, và quê ở Phú Thọ*; Bằng cách đưa ra giấy xác nhận tiêm vaccin, một bệnh nhân có thể chứng minh rằng *anh ta đã tiêm đủ 3 mũi vaxin ngừa Covid*; bằng cách trình thẻ sinh viên, một cô gái có thể chứng minh rằng *cô ấy hiện đang là sinh viên năm cuối*.

Các phát triển gần đây của Blockchain đã tạo ra xu hướng mới về định danh số. Cụ thể, tính minh bạch và công khai của dữ liệu trên Blockchain giúp việc xác minh thuộc tính của định danh trở nên dễ dàng. Bên cấp định danh số sẽ sử dụng Blockchain để lưu trữ các thuộc tính mà định danh sở hữu. Bên sở hữu định danh dùng địa chỉ ví để chứng minh thuộc tính liên quan đến định danh của mình. Bên thứ ba xác minh thuộc tính của định danh thông qua bằng chứng trên Blockchain.

Tuy nhiên, định danh số và việc xác minh như trên có một điểm yếu: người sở hữu định danh bị lộ thông tin trong quá trình chứng minh. Ví dụ, khi bạn trình thẻ căn cước công dân để chứng minh *bạn hơn 18 tuổi*, bạn sẽ bị lộ thông tin về giới tính, tên tuổi, và địa chỉ. Tội tệ hơn, tính công khai của dữ liệu trên blockchain làm các định danh số mất đi tính riêng tư. May mắn thay, điểm yếu này có thể khắc phục bằng kỹ thuật Chứng Minh Không Lộ Tri Thức (CMKLTT). CMKLTT là một kỹ thuật mật mã cho phép chứng minh một khẳng định mà không tiết lộ bất kỳ thông tin gì khác ngoài khẳng định cần chứng minh là đúng. Kỹ thuật này kết hợp với Blockchain tạo ra phương pháp định danh số không lộ tri thức (zk-identity). Mọi thứ diễn ra đơn giản và vô cùng tự nhiên!

Một thư viện định danh số mã nguồn mở có hỗ trợ CMKLTT phổ biến là iden3 (<https://iden3.io>).

2. Bài toán

Thí sinh tham gia sẽ cài đặt một ứng dụng định danh số cho thẻ căn cước công dân (CCCD) dựa trên thư viện nguồn mở iden3 hoặc một thư viện định danh số khác có hỗ trợ CMKLTT. Yêu cầu cụ thể như sau:

- Dữ liệu căn cước công dân bao gồm: *số căn cước công dân, họ tên, năm sinh, giới tính, quốc tịch, quê quán, đặc điểm nhận dạng, ngày cấp, nơi cấp*. Dữ liệu này sẽ được gửi đến Server quản lý CCCD để xác thực.
- Dữ liệu CCCD được băm và lưu lên Blockchain để mọi người có thể chứng minh một cách công khai thuộc tính của mình cho bên thứ 3.
- Việc chứng minh phải đảm bảo không lộ bất cứ thông tin gì ngoài khẳng định cần chứng minh là đúng. Ví dụ: việc chứng minh người dùng X có tuổi lớn hơn 18 sẽ không làm lộ địa chỉ, số tuổi chính xác của X, giới tính, hoặc địa chỉ của X. Việc chứng minh các thuộc tính hạn chế trong một số kiểu: tuổi thuộc khoảng nào, tên là gì, quê quán ở đâu. Tuy nhiên, bạn phải cho phép kết hợp các khẳng định. Ví dụ: *tuổi lớn hơn 18 và quê ở Phú Thọ*.

3. Các công việc chuẩn bị trước

- Cài đặt giao thức Iden3 (<https://iden3.io>) và các thư viện liên quan;
- Thiết kế giao diện gồm hai trang:
 - **Trang đăng ký** cho phép nhập căn cước công dân với thông tin về: *số căn cước công dân, họ tên, năm sinh, giới tính, quốc tịch, quê quán, đặc điểm nhận dạng, ngày cấp, nơi cấp*.
 - **Trang đăng nhập** cho phép thực hiện sinh chứng minh cho thuộc tính cụ thể từ định danh; và nếu chứng minh thỏa mãn điều kiện thì cho phép đăng nhập.
- Thiết kế các thuật toán cho hợp đồng thông minh trên blockchain và phía backend.
- Chuẩn bị bộ dữ liệu test và kịch bản trình diễn kết quả phần mềm.

4. Công việc phải làm tại vòng chung kết

Câu 1 (30 điểm). Lập trình giao diện

Trang đăng ký:

- Nhập dữ liệu về CCCD gồm: *số CCCD, họ tên, năm sinh, giới tính, quốc tịch, quê quán, đặc điểm nhận dạng, ngày cấp, nơi cấp*.
- Tạo định danh là cặp khóa (bí mật, công khai) cho người dùng; và cho phép người dùng lưu trữ cặp khóa trên máy cục bộ dưới dạng file key.json hoặc key.txt.
- Và gửi thông tin cần thiết về **Server quản lý CCCD**.

Trang đăng nhập:

- Sử dụng file key.json và dữ liệu về các thuộc tính của người dùng để sinh chứng minh cho khẳng định "*lớn hơn 18 tuổi và (quê ở Phú Thọ hoặc quê ở Hà Nội hoặc quê Hải Phòng)*" và gửi về **Server đăng nhập**.

- Nhận token để đăng nhập từ Server đăng nhập nếu chứng minh là đúng.

Câu 2 (30 điểm) Cài đặt hợp đồng thông minh

Dữ liệu về các thuộc tính của căn cước công dân được xác thực qua cây Merkle. Các hợp đồng thông minh chỉ nên lưu dữ liệu về Gốc của cây Merkle này để đảm bảo tính riêng tư. Gốc của cây Merkle được cập nhật sau khi đã kiểm tra rằng:

- Dữ liệu cập nhật được ký bởi Server quản lý CCCD;
- Bằng chứng cho việc cập nhật gốc của cây Merkle là hợp lệ.

Ngoài ra, các hợp đồng thông minh cần hỗ trợ hàm verify để kiểm tra thuộc tính của định danh thoả mãn điều kiện nào đó qua bằng chứng không lộ tri thức. Các hợp đồng thông minh này có thể được triển khai trên Blockchain Ethereum Testnet.

Câu 3 (30 điểm). Lập trình server

a. Server quản lý CCCD

Dữ liệu CCCD sẽ được nhập qua giao diện Trang đăng ký và gửi cho Server quản lý CCCD. Server này sẽ :

- xử lý dữ liệu và tính lại cây Merkle;
- tính bằng chứng zk-proof rằng việc cập nhật gốc của cây Merkle là đúng;
- Cập nhật gốc của cây Merkle lên Blockchain bằng cách gửi gốc mới cùng bằng chứng zk-proof.

Với bằng chứng đã được công khai trên mạng blockchain, người dùng sau này có thể tạo ra các chứng minh không lộ tri thức về thuộc tính của mình để xác thực với bên thứ 3.

b. Server đăng nhập

Người dùng (từ frontend) gửi bằng chứng về khẳng định

*“Lớn hơn 18 tuổi và (quê ở Phú Thọ **hoặc** quê ở Hà Nội **hoặc** quê ở Hải Phòng)”*

cho Server đăng nhập. Server sẽ kiểm tra tính đúng đắn của bằng chứng này qua hàm verify của hợp đồng thông minh trên Blockchain; và nếu đúng, Server cấp quyền truy cập cho người dùng qua một token chuẩn, ví dụ: Json Web Token.

Câu 4 (10 điểm). Cải thiện việc nhập liệu

Dùng một thư viện mã nguồn mở OCR (Optical Character Recognition) lấy thông tin từ căn cước công dân để tự động hoá quá trình đăng ký căn cước công dân số trong Trang đăng ký CCCD.

Lưu ý: các nhóm trong quá trình phát triển ứng dụng phải tuân theo các quy trình phát triển phần mềm nguồn mở.