**BỘ GIÁO DỤC VÀ ĐÀO TẠO**

**TRƯỜNG ĐẠI HỌC ĐẠI NAM**

Logo, company name

Description automatically generated

**BÀI TẬP LỚN**

**TÊN HỌC PHẦN: CÔNG NGHỆ BLOKCHAIN**

**ĐỀ TÀI: RÚT THĂM TRÚNG THƯỞNG LỚP HỌC**

**Giáo viên hướng dẫn: Trần Đăng Công**

**Sinh viên thực hiện:**  **Nhóm 9**

|  |  |  |  |
| --- | --- | --- | --- |
| **Stt** | **Mã sv** | **Họ và tên** | **Lớp** |
| 1 | 1571020216 | Vũ Mạnh Quân | CNTT 15-03 |
| 2 | 1571020057 | Nguyễn Tiến Đạt | CNTT 15-03 |
| 3 | 1571020210 | Nguyễn Duy Quang | CNTT 15-03 |

**Hà Nội, năm 2025**

**BỘ GIÁO DỤC VÀ ĐÀO TẠO**

**TRƯỜNG ĐẠI HỌC ĐẠI NAM**

Logo, company name

Description automatically generated

**BÀI TẬP LỚN**

**TÊN HỌC PHẦN: CÔNG NGHỆ BLOKCHAIN**

**ĐỀ TÀI: RÚT THĂM TRÚNG THƯỞNG LỚP HỌC**

|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
| **STT** | **Mã Sinh Viên** | **Họ và Tên** | **Ngày Sinh** | **Điểm** | |
| **Bằng Số** | **Bằng Chữ** |
| **1** | **1571020216** | **Vũ Mạnh Quân** | **16/01/2003** |  |  |
| **2** | **1571020057** | **Nguyễn Tiến Đạt** | **02/02/2003** |  |  |
| **3** | **1571020210** | **Nguyễn Duy Quang** | **19/09/2003** |  |  |

**CÁN BỘ CHẤM THI 1 CÁN BỘ CHẤM THI 2**

**Hà Nội, Ngày 4 Tháng 6 năm 2025**

**LỜI NÓI ĐẦU**

Trong các hoạt động học tập, sinh hoạt ngoại khóa hay tổ chức sự kiện trong môi trường lớp học, rút thăm trúng thưởng là một hình thức giải trí phổ biến, góp phần tăng sự tương tác và gắn kết giữa các thành viên. Tuy nhiên, hình thức rút thăm truyền thống thường dựa vào giấy bốc thăm hoặc phần mềm đơn giản, dẫn đến những nghi ngờ về tính ngẫu nhiên, minh bạch hoặc sự can thiệp chủ quan của người tổ chức.

Trong thời đại công nghệ số phát triển nhanh chóng, blockchain – một nền tảng công nghệ nổi bật với đặc trưng minh bạch, bất biến và phân tán – được xem là giải pháp tiềm năng để gia tăng độ tin cậy cho các hệ thống cần đảm bảo công bằng và chống gian lận. Việc đưa blockchain vào một hoạt động nhỏ như rút thăm trúng thưởng lớp học là một hướng tiếp cận sáng tạo và có ý nghĩa giáo dục công nghệ thực tiễn.

Xuất phát từ đó, đề tài “Blockchain rút thăm trúng thưởng lớp học” được xây dựng nhằm mô phỏng một hệ thống rút thăm ngẫu nhiên dựa trên hàm băm (hash function) – một thành phần quen thuộc trong blockchain – để tạo ra kết quả công bằng và không thể bị thao túng. Giao diện hệ thống cho phép người dùng nhập tên đăng ký tham gia, lưu lại danh sách, và khi nhấn nút “Rút thăm”, hệ thống sẽ sử dụng một chuỗi giả lập ngẫu nhiên (random hash) để chọn ra người trúng thưởng một cách minh bạch.

Hệ thống này tuy đơn giản nhưng mang tính giáo dục cao, giúp người học làm quen với cách thức hoạt động của các thuật toán chọn ngẫu nhiên, khái niệm hash, và đặc biệt là tư duy minh bạch của blockchain – nền tảng đang được ứng dụng rộng rãi trong tài chính, quản lý, bảo mật và nhiều lĩnh vực khác.

Qua đề tài này, nhóm thực hiện không chỉ mong muốn tạo ra một công cụ hữu ích và vui nhộn cho lớp học, mà còn truyền tải tinh thần đổi mới sáng tạo trong việc ứng dụng công nghệ để giải quyết các bài toán đời sống hàng ngày theo cách hiện đại và đáng tin cậy hơn.

**MỤC LỤC**

[CHƯƠNG 1: GIỚI THIỆU 7](#_Toc634)

[1.1 Giới thiệu đề tài 7](#_Toc25075)

[1.2 Mục tiêu nghiên cứu 7](#_Toc31584)

[1.3 Lý do chọn đề tài 8](#_Toc14465)

[1.4 Phạm vi nghiên cứu 8](#_Toc4624)

[CHƯƠNG 2: CƠ SỞ LÝ THUYẾT 10](#_Toc2810)

[2.1 Khái niệm công nghệ Blockchain 10](#_Toc9771)

[2.2 Hàm băm (Hash Function) 10](#_Toc16062)

[2.3 Tạo tính ngẫu nhiên trên Blockchain 11](#_Toc709)

[2.4 Hợp đồng thông minh (Smart Contract) 12](#_Toc26846)

[CHƯƠNG 3: PHÂN TÍCH YÊU CẦU ĐỀ TÀI 13](#_Toc19892)

[3.1 Yêu cầu chức năng 13](#_Toc4287)

[3.1.1 Chức năng đăng ký người tham gia 13](#_Toc3623)

[3.1.2 Hiển thị danh sách người tham gia 13](#_Toc12485)

[3.1.3 Chức năng rút thăm 13](#_Toc27932)

[3.1.4 Hiển thị kết quả người thắng 13](#_Toc11639)

[3.1.5 Chức năng làm mới danh sách 14](#_Toc9844)

[3.2 Yêu cầu bổ sung về giao diện và hệ thống 14](#_Toc32450)

[3.2.1 Giao diện thân thiện, dễ hiểu 14](#_Toc6068)

[3.2.2 Minh bạch và dễ theo dõi 14](#_Toc25662)

[3.2.3 Ngẫu nhiên, không bị thao túng 15](#_Toc432)

[3.2.4 Hoạt động mượt mà, không bị lỗi 15](#_Toc1182)

[3.2.5 Dễ dàng triển khai và sử dụng 15](#_Toc31925)

[CHƯƠNG 4: THIẾT KẾ VÀ TRIỂN KHAI HỆ THỐNG 16](#_Toc6587)

[4.1 Giao diện người dùng (UI) 16](#_Toc23284)

[4.2 Cấu trúc dữ liệu 17](#_Toc5592)

[4.2.1 Danh sách người tham gia (participants) 17](#_Toc21298)

[4.2.2 Dữ liệu ngẫu nhiên đầu vào (random seed) 17](#_Toc21512)

[4.2.3 Hàm băm (hash function) 17](#_Toc24073)

[4.2.4 Tính toán người thắng 18](#_Toc13546)

[4.2.5 Kết quả hiển thị 18](#_Toc16970)

[CHƯƠNG 5: KẾT QUẢ THỰC HIỆN 19](#_Toc21009)

[5.1 Code hợp đồng thông minh 19](#_Toc28982)

[5.2 Code giao diện 21](#_Toc1486)

[CHƯƠNG 6 : KẾT LUẬN 25](#_Toc6562)

[6.1 Tổng kết đề tài 25](#_Toc12861)

[6.2 Đánh giá kết quả đạt được 25](#_Toc20821)

[6.3 Hạn chế 26](#_Toc18881)

**MỤC LỤC HÌNH ẢNH**

[Image 1 : Hợp đồng thông minh 19](#_Toc29839)

[Image 2 : Giao diện 21](#_Toc26153)

[Image 3 : Kết nối đến ví MetaMask 22](#_Toc13972)

[Image 4 : Tải file danh sách sinh viên lên 22](#_Toc222)

[Image 5 : Hiển thị danh sách sinh viên 23](#_Toc188)

[Image 6 : Rút thăm tìm ra người may mắn 23](#_Toc31063)

[Image 7 : Mã hash và thông tin người thắng được gửi lên blockchain 24](#_Toc24482)

[Image 8 : Đồng thời được lưu trên firebase để dễ dàng quản lý 24](#_Toc19504)

**CHƯƠNG 1: GIỚI THIỆU**

**1.1** **Giới thiệu đề tài**

Trong môi trường học tập hiện nay, những hoạt động như rút thăm trúng thưởng, chia nhóm ngẫu nhiên hay chọn đại diện tham gia trò chơi thường xuyên được tổ chức để tạo sự hứng thú và gắn kết giữa các thành viên trong lớp. Tuy nhiên, phần lớn các hoạt động này vẫn được thực hiện theo cách thủ công – ví dụ như viết tên ra giấy rồi bốc thăm – hoặc thông qua một số công cụ đơn giản như vòng quay may mắn, random tên bằng Excel... Điều này tuy tiện lợi nhưng đôi khi lại khiến mọi người nghi ngờ về tính công bằng hoặc cho rằng có sự can thiệp từ người tổ chức.

Từ thực tế đó, nhóm chúng em nảy ra ý tưởng xây dựng một hệ thống rút thăm ứng dụng nguyên lý của blockchain – một công nghệ hiện đại đang được ứng dụng rất nhiều trong các lĩnh vực như tài chính, quản lý, xác minh danh tính... Mục tiêu là tạo ra một ứng dụng đơn giản, dễ sử dụng trong lớp học nhưng vẫn đảm bảo được tính ngẫu nhiên, minh bạch và công bằng.

Thông qua việc sử dụng hàm băm (hash function) để mô phỏng việc chọn người thắng một cách ngẫu nhiên, hệ thống không chỉ đơn thuần là một công cụ giải trí mà còn giúp người dùng hiểu thêm về cách công nghệ có thể giải quyết những vấn đề tưởng chừng rất đời thường như “ai sẽ là người được chọn hôm nay”. Hơn nữa, đây cũng là cơ hội để chúng em áp dụng kiến thức về lập trình, thiết kế giao diện và tư duy logic vào một tình huống thực tế.

**1.2 Mục tiêu nghiên cứu**

Với đề tài này, nhóm em đặt ra một số mục tiêu cụ thể như sau:

Xây dựng một giao diện đơn giản để người tham gia có thể nhập tên đăng ký vào hệ thống.

Tạo cơ chế lưu danh sách người tham gia một cách rõ ràng, không trùng lặp.

Thiết kế nút “Rút thăm” giúp hệ thống chọn ra một người thắng hoàn toàn ngẫu nhiên, dựa trên thuật toán sử dụng hàm băm hoặc mô phỏng cơ chế giống blockchain.

Hiển thị kết quả rút thăm rõ ràng, không thể bị thay đổi sau khi công bố.

Đảm bảo hệ thống dễ sử dụng cho cả giáo viên và học sinh, và có thể áp dụng cho nhiều tình huống thực tế khác nhau.

**1.3 Lý do chọn đề tài**

Chúng em lựa chọn đề tài này không chỉ vì nó mang tính thực tế cao mà còn bởi nhiều lý do ý nghĩa:

Thứ nhất, trong thực tế lớp học, những hoạt động rút thăm trúng thưởng hoặc chọn người đại diện rất phổ biến, nhưng thường thiếu công cụ hỗ trợ minh bạch. Việc áp dụng công nghệ sẽ giúp giải quyết vấn đề này một cách hiệu quả.

Thứ hai, blockchain là một chủ đề đang rất "hot" trong lĩnh vực công nghệ hiện đại. Việc áp dụng một phần nguyên lý của blockchain vào bài toán nhỏ này giúp chúng em tiếp cận khái niệm mới một cách dễ hiểu và gần gũi hơn.

Thứ ba, đề tài này cho phép chúng em kết hợp nhiều kỹ năng đã học như lập trình frontend, xử lý dữ liệu, làm việc với thuật toán ngẫu nhiên và giao tiếp giữa các thành phần trong hệ thống.

Cuối cùng, đây là một sản phẩm tuy đơn giản nhưng thiết thực. Nó có thể dùng thật trong lớp học, mang lại niềm vui, sự công bằng và một chút “hi-tech” trong mỗi lần rút thăm.

**1.4 Phạm vi nghiên cứu**

Do điều kiện thời gian và phạm vi đề tài, nhóm em chỉ tập trung phát triển hệ thống ở mức cơ bản, mô phỏng rút thăm ngẫu nhiên trong phạm vi lớp học. Cụ thể:

Về chức năng:

Người dùng có thể nhập tên để đăng ký tham gia.

Hệ thống sẽ lưu danh sách này và sử dụng thuật toán random (kết hợp với hash mô phỏng) để chọn người thắng.

Giao diện có thể hiển thị danh sách và kết quả một cách rõ ràng.

Về công nghệ:

Ứng dụng hoạt động trên nền tảng web đơn giản (có thể dùng HTML/CSS/JS hoặc Python Flask).

Sử dụng thuật toán tạo hash ngẫu nhiên để mô phỏng tính bất biến và ngẫu nhiên của blockchain (không triển khai blockchain thực tế).

Về quy mô sử dụng:

Dành cho lớp học hoặc nhóm nhỏ từ 10–50 người.

Hệ thống chạy cục bộ, không cần kết nối internet, đảm bảo dễ triển khai trong điều kiện lớp học thông thường.

Giới hạn đề tài:

Không sử dụng mạng blockchain thật (như Ethereum hay BNB Chain).

Không kết hợp với hệ thống lưu trữ vĩnh viễn hoặc phân phối phần thưởng tự động.

Tính ngẫu nhiên mang tính mô phỏng, không đạt mức bảo mật cao như hệ thống blockchain thực tế.

# **CHƯƠNG 2: CƠ SỞ LÝ THUYẾT**

## **2.1 Khái niệm công nghệ Blockchain**

Công nghệ blockchain hay còn gọi là “chuỗi khối” là một trong những bước tiến quan trọng của kỷ nguyên số hiện đại. Nếu phải mô tả một cách ngắn gọn, thì blockchain giống như một cuốn sổ ghi chép điện tử, nơi mọi dữ liệu được ghi lại theo từng “khối” (block) và những khối này được liên kết với nhau tạo thành một “chuỗi”.

Điều đặc biệt ở blockchain là: một khi dữ liệu đã ghi vào khối, gần như không thể sửa đổi được. Bởi mỗi khối đều chứa một mã băm (hash) riêng, và mã băm này lại được tạo ra từ nội dung của khối đó cộng với mã băm của khối trước. Nếu có ai đó cố tình chỉnh sửa một khối trong chuỗi, toàn bộ các khối sau sẽ bị sai lệch, và các nút mạng (node) trong hệ thống sẽ phát hiện ra ngay lập tức.

Công nghệ blockchain thường được ứng dụng trong các hệ thống tài chính phi tập trung như Bitcoin, Ethereum… nhưng thật ra nó có thể áp dụng vào rất nhiều lĩnh vực khác như quản lý chuỗi cung ứng, bỏ phiếu điện tử, lưu trữ hồ sơ y tế, xác minh danh tính, và thậm chí là những thứ gần gũi như hệ thống rút thăm trúng thưởng.

Trong đề tài này, nhóm chúng em chọn blockchain không phải để làm một hệ thống quá phức tạp, mà là để ứng dụng một phần nguyên lý của nó – cụ thể là sử dụng tính minh bạch, không thể sửa đổi và ngẫu nhiên – để rút thăm một cách công bằng trong lớp học.

## **2.2 Hàm băm (Hash Function)**

Hàm băm là một thành phần cơ bản và vô cùng quan trọng trong công nghệ blockchain. Nó giống như một "cỗ máy nghiền dữ liệu" – bạn đưa vào một chuỗi bất kỳ (có thể là tên, số, câu văn...), và máy sẽ trả ra một chuỗi mã hóa cố định, nhìn rất “khó hiểu”, không đoán được từ đầu ra mà ngược lại về đầu vào.

Một số tính chất nổi bật của hàm băm gồm:

Không thể đảo ngược: Nghĩa là khi đã băm ra kết quả rồi, không thể lấy kết quả đó để tìm lại được dữ liệu gốc ban đầu.

Rất nhạy cảm với thay đổi: Chỉ cần thay đổi một ký tự nhỏ trong dữ liệu đầu vào (ví dụ “Nguyen Van A” thành “Nguyen Van a”), kết quả băm sẽ khác hoàn toàn.

Đầu ra có độ dài cố định: Bất kể đầu vào dài ngắn thế nào, kết quả băm vẫn có độ dài cố định (ví dụ SHA-256 luôn ra 64 ký tự hex).

Ví dụ cụ thể:

Hash("Nguyen Van A") → 51f3...e2c

Hash("Nguyen Van a") → b6a2...8d0

Trong đề tài, chúng em sử dụng hàm băm để chọn ra người thắng. Cách làm là lấy danh sách người chơi, kết hợp với một chuỗi ngẫu nhiên (ví dụ thời gian hoặc số may mắn do người dùng chọn), rồi đưa toàn bộ vào hàm băm. Sau đó, lấy kết quả hash để suy ra chỉ số người thắng. Cách này đơn giản nhưng vẫn đảm bảo tính bất ngờ, minh bạch và khó gian lận.

## **2.3 Tạo tính ngẫu nhiên trên Blockchain**

Một điều tưởng chừng đơn giản như "lấy ngẫu nhiên 1 người" thật ra lại là một bài toán rất khó trong thế giới blockchain. Nguyên nhân là vì blockchain là hệ thống phi tập trung, tức không có máy chủ trung tâm nào điều khiển mọi thứ. Tất cả đều minh bạch, ai cũng có thể đọc được dữ liệu. Chính vì thế, nếu muốn tạo ra một kết quả "ngẫu nhiên", thì phải đảm bảo không ai biết trước được, và cũng không ai có thể can thiệp vào quá trình chọn lựa.

Một số kỹ thuật tạo ngẫu nhiên phổ biến trong các hệ thống blockchain thật gồm:

Lấy timestamp (thời gian tạo block) làm cơ sở random.

Dựa vào hash của block gần nhất: vì không ai đoán được hash trước khi nó được tạo ra.

Sử dụng dịch vụ Oracle: lấy dữ liệu từ bên ngoài như số xổ số, nhiệt độ thời tiết, v.v.

Tuy nhiên, trong phạm vi đề tài này, nhóm em không triển khai blockchain thật mà chỉ mô phỏng lại cơ chế này bằng các công cụ đơn giản:

Sử dụng Math.random(), Date.now() hoặc crypto.randomUUID() làm dữ liệu ngẫu nhiên đầu vào.

Băm dữ liệu này bằng hàm hash (ví dụ SHA-256), rồi dùng kết quả để chọn người thắng (ví dụ: lấy số cuối chia cho số người tham gia → chọn người ở vị trí đó).

Nhờ đó, kết quả hoàn toàn ngẫu nhiên, không ai đoán trước được, và đặc biệt là không ai có thể chỉnh sửa sau khi đã bấm “Rút thăm”.

## **2.4 Hợp đồng thông minh (Smart Contract)**

Hợp đồng thông minh (smart contract) là một đoạn mã được lập trình chạy trên blockchain, có khả năng tự thực thi các điều kiện đã định sẵn, không cần ai can thiệp hay điều khiển.

Ví dụ, nếu có một hợp đồng quy định: "Nếu A gửi cho B 1 ETH, thì B sẽ giao hàng cho A", thì smart contract có thể kiểm tra, xác minh và tự động hoàn tất giao dịch đó khi đủ điều kiện, mà không cần người trung gian.

Tính chất nổi bật của smart contract:

Tự động: Chỉ cần đúng điều kiện, hệ thống sẽ thực thi.

Không thể sửa đổi: Một khi đã đưa lên blockchain, hợp đồng không thể bị chỉnh sửa tùy ý.

Công khai và minh bạch: Ai cũng có thể kiểm tra nội dung hợp đồng.

Trong đề tài này, nhóm em chưa triển khai smart contract thật vì nó phức tạp và vượt quá phạm vi lớp học. Tuy nhiên, việc nghiên cứu smart contract giúp chúng em hình dung rằng:

Nếu phát triển lên tầm cao hơn, việc rút thăm trúng thưởng hoàn toàn có thể được thực hiện trên blockchain thật, bằng hợp đồng thông minh.

Điều này sẽ giúp loại bỏ mọi nghi ngờ, đảm bảo công bằng tuyệt đối.

Đồng thời, hệ thống có thể tự động trao thưởng (token, NFT...) mà không cần người trung gian điều phối.

# **CHƯƠNG 3: PHÂN TÍCH YÊU CẦU ĐỀ TÀI**

## **3.1 Yêu cầu chức năng**

Để đảm bảo hệ thống rút thăm hoạt động đúng mục tiêu ban đầu và có thể áp dụng thật trong lớp học, nhóm chúng em đã xác định rõ các chức năng mà hệ thống cần phải có. Các chức năng này vừa đảm bảo tính tiện lợi, vừa phải công bằng và minh bạch – đúng tinh thần mà blockchain hướng tới.

**3.1.1 Chức năng đăng ký người tham gia**

Đây là bước đầu tiên của hệ thống. Học sinh hoặc người tham gia sẽ nhập tên của mình vào ô đăng ký.

Sau khi bấm nút “Thêm”, tên sẽ được lưu lại trong danh sách người chơi.

Hệ thống cần kiểm tra trùng tên, tránh việc một người nhập tên nhiều lần để tăng cơ hội trúng. Nếu phát hiện trùng, sẽ báo lỗi ngay.

**3.1.2 Hiển thị danh sách người tham gia**

Sau khi đăng ký, hệ thống sẽ hiển thị toàn bộ danh sách người đã nhập tên.

Danh sách này được sắp xếp đơn giản, có thể đánh số thứ tự để dễ theo dõi.

Danh sách được hiển thị công khai, ai cũng thấy, tạo cảm giác minh bạch và rõ ràng.

**3.1.3 Chức năng rút thăm**

Khi đã có đủ danh sách người tham gia, người tổ chức sẽ bấm nút “Rút thăm”.

Hệ thống sẽ tự động lấy danh sách hiện tại, kết hợp với một yếu tố ngẫu nhiên như thời gian hiện tại (timestamp) hoặc chuỗi ngẫu nhiên (random string).

Từ đó, hệ thống sẽ đưa chuỗi đó vào hàm băm (hash function) để tạo ra một dãy mã không thể đoán trước.

Dựa vào dãy mã đó, hệ thống sẽ tính toán để chọn ra một người thắng duy nhất, ví dụ bằng cách lấy 2–3 số cuối của hash rồi chia cho tổng số người để xác định vị trí.

**3.1.4 Hiển thị kết quả người thắng**

Sau khi hệ thống chọn xong, tên người trúng thưởng sẽ được hiển thị nổi bật lên màn hình, có thể kèm hiệu ứng như chữ to, màu nổi bật hoặc biểu tượng vui nhộn.

Kèm theo đó, có thể hiển thị thêm thông tin kỹ thuật như hash được tạo ra, cách chọn người thắng… để người xem thấy rõ quá trình là minh bạch.

**3.1.5 Chức năng làm mới danh sách**

Sau mỗi lần rút thăm xong, hệ thống cần có nút “Làm mới” để xóa hết dữ liệu cũ.

Người tổ chức có thể bắt đầu một lượt rút thăm mới mà không bị lẫn với danh sách cũ.

## **3.2 Yêu cầu bổ sung về giao diện và hệ thống**

Ngoài các chức năng chính nêu trên, hệ thống còn cần những yếu tố bổ sung để dễ sử dụng hơn, thân thiện hơn với người dùng và đảm bảo hoạt động mượt mà trong môi trường lớp học.

**3.2.1 Giao diện thân thiện, dễ hiểu**

Do hệ thống dùng trong lớp học, với nhiều người không rành công nghệ, nên giao diện phải cực kỳ đơn giản và trực quan.

Mọi thành phần nên được bố trí rõ ràng:

Một ô để nhập tên

Một danh sách hiển thị tên đã đăng ký

Một nút lớn để “Rút thăm”

Một khu vực nổi bật để hiển thị kết quả

Màu sắc nên tươi sáng, chữ rõ, dễ đọc trên máy chiếu hoặc màn hình lớn.

**3.2.2 Minh bạch và dễ theo dõi**

Toàn bộ quá trình nên được hiển thị công khai: từ danh sách người tham gia cho đến người trúng thưởng.

Nếu có thể, nên cho người dùng xem cả dữ liệu đầu vào và kết quả băm, để chứng minh rằng kết quả là ngẫu nhiên và không thể bị can thiệp.

**3.2.3 Ngẫu nhiên, không bị thao túng**

Thuật toán chọn người thắng không được viết theo kiểu “nếu tên là Nguyễn Văn A thì cho thắng”. Phải dùng dữ liệu không ai đoán trước được như thời gian hiện tại, chuỗi random...

Mã hash phải thay đổi mỗi lần rút thăm, đảm bảo người xem không thể dự đoán kết quả trước khi bấm nút.

**3.2.4 Hoạt động mượt mà, không bị lỗi**

Hệ thống cần chạy mượt cả trên laptop, trình duyệt Chrome/Edge và màn hình chiếu.

Không bị đơ khi nhập quá nhiều người.

Nếu có lỗi nhập trùng, sai tên... phải báo rõ ràng, dễ hiểu để người dùng biết mà sửa.

**3.2.5 Dễ dàng triển khai và sử dụng**

Hệ thống nên viết bằng các công nghệ đơn giản như HTML/CSS/JS hoặc Python Flask.

Không yêu cầu cài đặt phức tạp. Chỉ cần tải file và chạy là dùng được ngay, phù hợp với môi trường lớp học.

Nếu có thời gian, có thể mở rộng thêm tính năng tải danh sách về, hoặc kết nối ví blockchain để rút thăm thực sự bằng smart contract.

**CHƯƠNG 4: THIẾT KẾ VÀ TRIỂN KHAI HỆ THỐNG**

## **4.1 Giao diện người dùng (UI)**

Mục tiêu thiết kế giao diện

Vì hệ thống hướng đến sử dụng trực tiếp trong lớp học, nên giao diện cần đảm bảo các tiêu chí:

Dễ nhìn – dễ dùng: Không gây rối mắt, thao tác đơn giản, dễ hiểu cho cả học sinh và giáo viên.

Chạy tốt trên mọi thiết bị: Laptop, máy chiếu, trình duyệt phổ biến như Chrome/Edge.

Giao diện trực quan, rõ ràng: Mỗi phần nên tách biệt, người dùng dễ nhận biết mình đang làm gì.

Các thành phần chính trong giao diện

Khung nhập tên người tham gia

Gồm một ô input (textbox) để người dùng nhập tên.

Nút “Thêm” hoặc “Đăng ký” bên cạnh để đưa tên vào danh sách.

Danh sách người tham gia

Hiển thị bên dưới ô nhập, gồm các tên đã được thêm vào.

Có thể đánh số thứ tự, mỗi dòng là một người.

Có thể hiển thị theo dạng bảng (table) đơn giản.

Nút “Rút thăm”

Đây là nút quan trọng nhất, thường được làm to, nổi bật.

Khi nhấn, hệ thống sẽ thực hiện thuật toán chọn người thắng dựa trên hash.

Khu vực hiển thị kết quả

Sau khi rút thăm, tên người thắng được hiển thị lớn ở giữa màn hình.

Có thể thêm hiệu ứng đơn giản như đổi màu, phóng to chữ, biểu tượng chúc mừng.

Nếu cần, hiển thị thêm thông tin như giá trị hash, thời gian, chỉ số chọn ra người thắng.

Nút “Làm mới”

Dùng để xóa danh sách cũ và bắt đầu một lượt rút thăm mới.

**4.2 Cấu trúc dữ liệu**

Vì đây là một ứng dụng đơn giản, nhóm em sử dụng các cấu trúc dữ liệu cơ bản để lưu trữ và xử lý thông tin. Dưới đây là các thành phần chính của dữ liệu được sử dụng trong hệ thống:

**4.2.1 Danh sách người tham gia (participants)**

Dạng: Mảng (Array) hoặc Danh sách (List)

Mỗi phần tử trong mảng là một chuỗi (String) chứa tên người dùng.

participants = ["Nguyễn Văn A", "Trần Thị B", "Lê Hoàng C"];

Trong phiên bản mở rộng, có thể chuyển sang dạng đối tượng để lưu thêm thời gian đăng ký, ID người dùng…

**4.2.2 Dữ liệu ngẫu nhiên đầu vào (random seed)**

Dùng để tạo độ ngẫu nhiên cho việc rút thăm.

Có thể lấy theo thời gian hiện tại (Date.now()), chuỗi UUID, hoặc chuỗi người tổ chức nhập vào.

randomSeed = Date.now().toString(); // Ví dụ: "1717449553001"

**4.2.3 Hàm băm (hash function)**

Sử dụng hàm băm như SHA-256 (qua thư viện crypto-js hoặc hashlib nếu dùng Python).

Đầu vào sẽ là danh sách người tham gia + random seed.

Đầu ra là một chuỗi hash dạng hex.

hashResult = SHA256(participants.join(",") + randomSeed);

**4.2.4 Tính toán người thắng**

Lấy 3 hoặc 4 ký tự cuối cùng trong hash để chuyển sang số.

Dùng phép chia dư cho tổng số người để xác định chỉ số người thắng.

let index = parseInt(hashResult.slice(-3), 16) % participants.length;

let winner = participants[index];

**4.2.5 Kết quả hiển thị**

Dạng đối tượng:

{

"winner": "Lê Hoàng C",

"index": 2,

"hash": "3ab1d0f6a7c9e2...",

"random\_seed": "1717449553001",

"timestamp": "2025-06-01 10:21:33"

}

# **CHƯƠNG 5: KẾT QUẢ THỰC HIỆN**

## **5.1 Code hợp đồng thông minh**

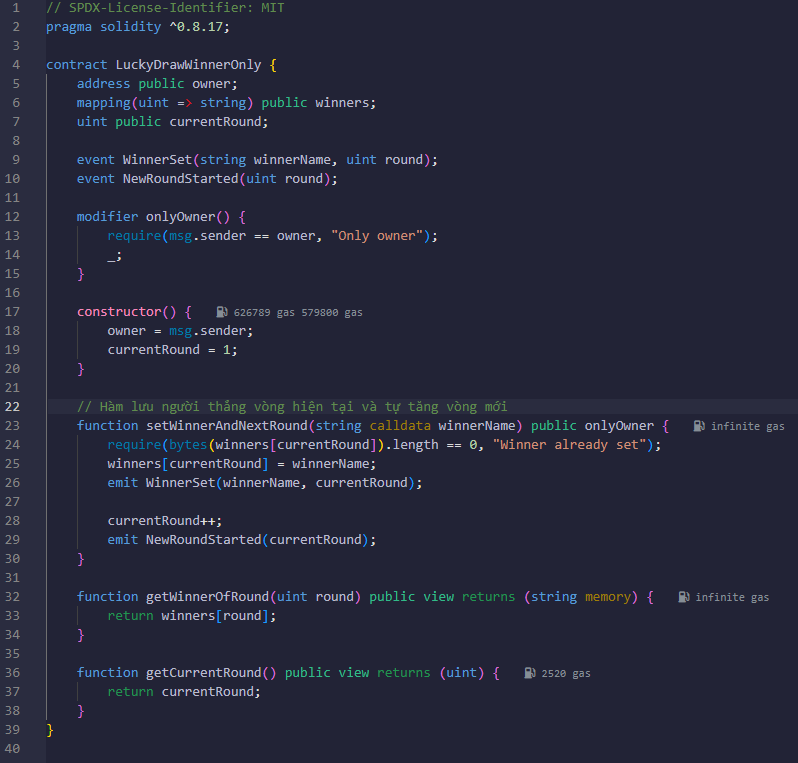


Image 1: Hợp đồng thông minh

**Mục đích hợp đồng:**

Ghi nhận người trúng thưởng theo từng vòng rút thăm, mỗi vòng chỉ có 1 người thắng, và chỉ chủ sở hữu (owner) được quyền cập nhật người thắng.

**Thành phần chính:**

Owner: địa chỉ người tạo hợp đồng, chỉ người này mới có quyền chọn người thắng.

currentRound: số thứ tự vòng rút thăm, bắt đầu từ 1 và tự tăng sau mỗi lượt.

winners: mapping lưu tên người thắng ứng với từng vòng.

**Hàm quan trọng:**

setWinnerAndNextRound(string winnerName)

Chỉ owner mới gọi được (onlyOwner).

Nếu vòng hiện tại chưa có người thắng, hàm sẽ:

Lưu tên người thắng vào winners[currentRound]

Phát sự kiện WinnerSet

Tăng currentRound lên 1 và phát sự kiện NewRoundStarted

getWinnerOfRound(uint round)

Trả về tên người thắng của một vòng cụ thể.

getCurrentRound()

Trả về số vòng hiện tại.

**Ví dụ hoạt động:**

currentRound = 1

Gọi setWinnerAndNextRound("Nguyen Van A")

→ Lưu "Nguyen Van A" là người thắng vòng 1

→ Tự động tăng currentRound = 2

**Quyền hạn:**

Ghi người thắng: chỉ owner

Xem kết quả: ai cũng xem được

## **5.2 Code giao diện**

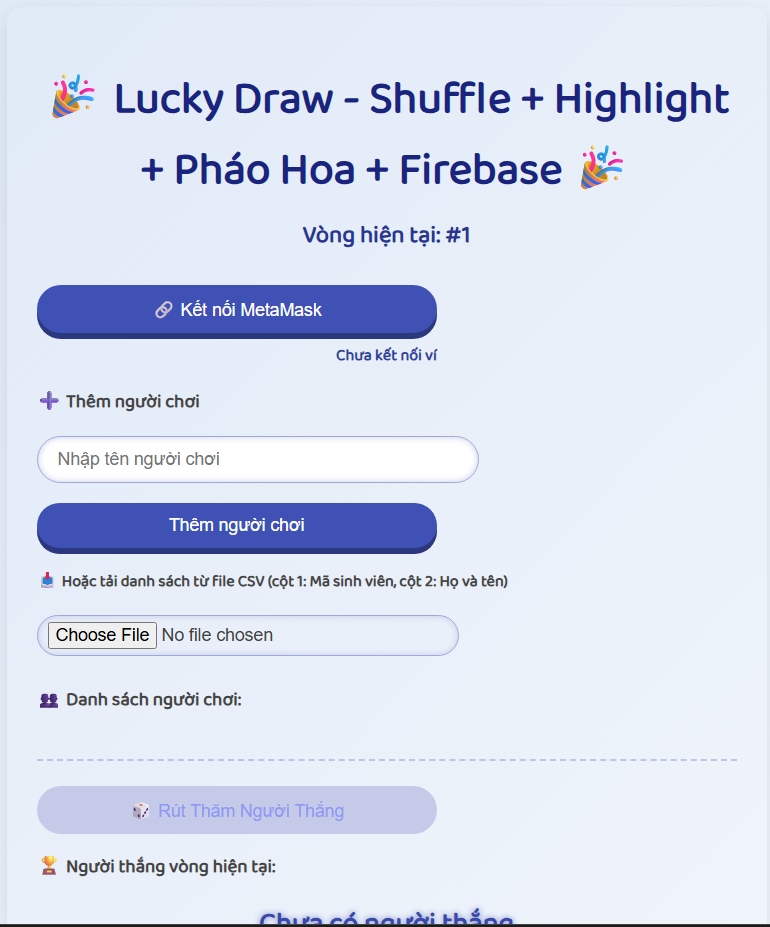


Image 2: Giao diện

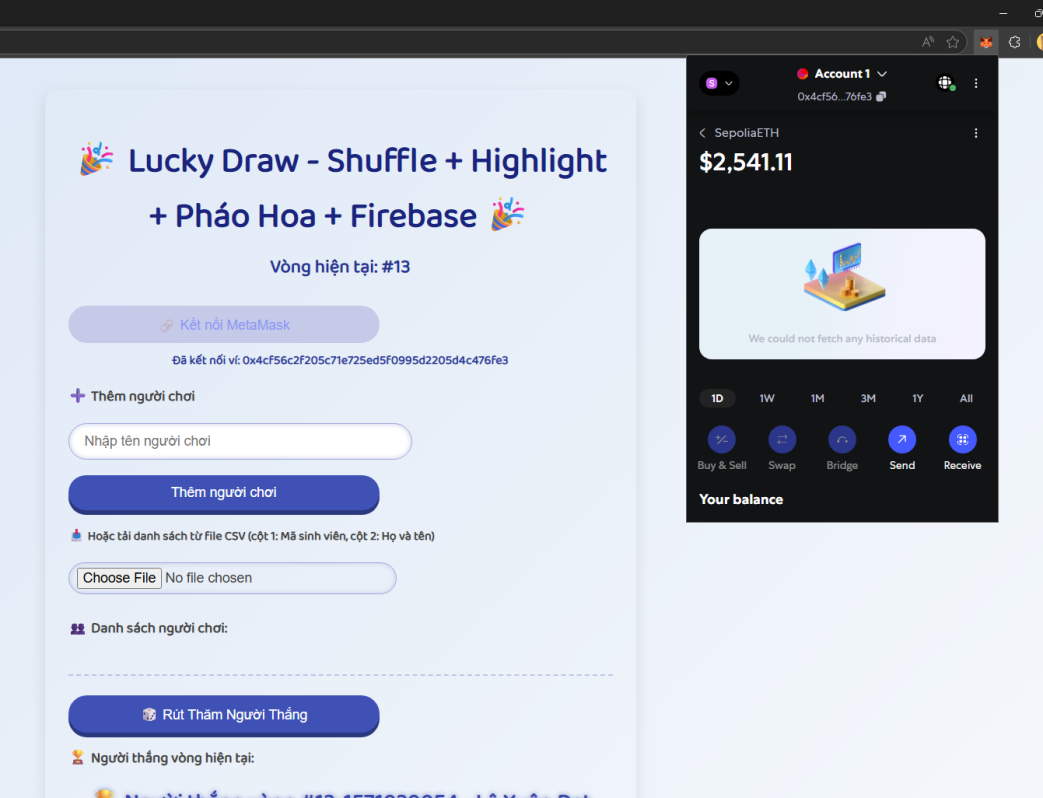


Image 3: Kết nối đến ví MetaMask

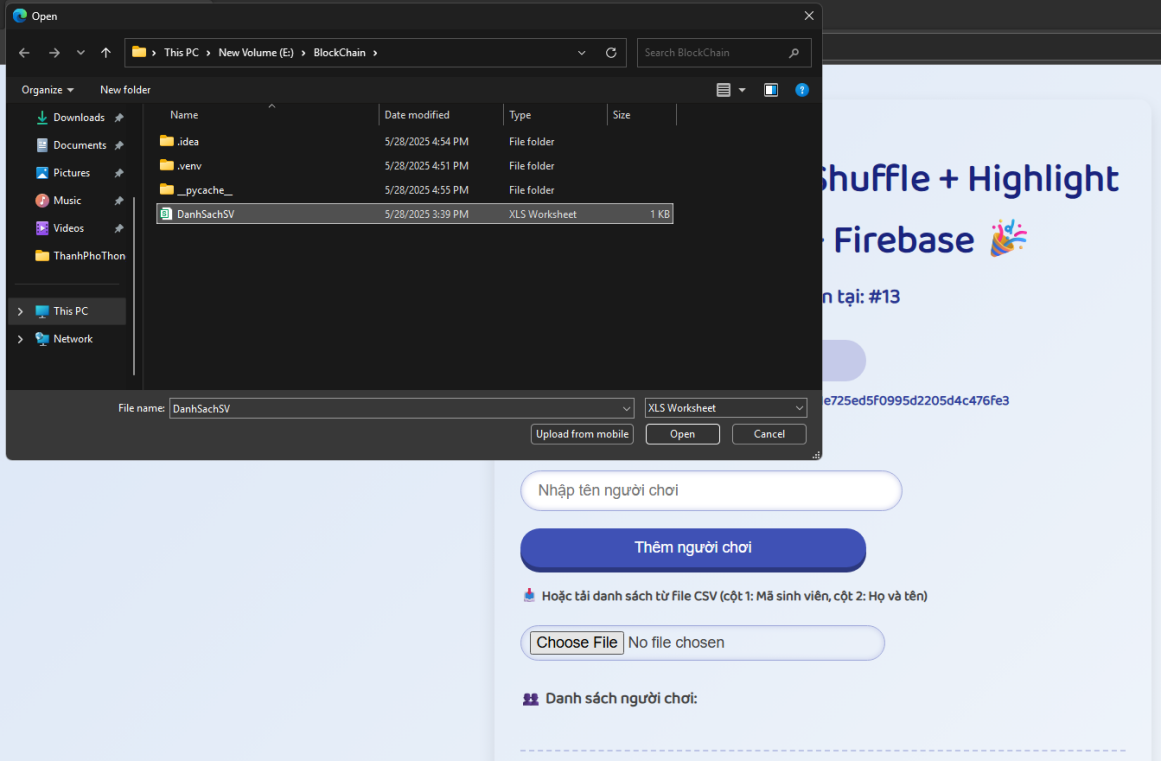


Image 4: Tải file danh sách sinh viên lên

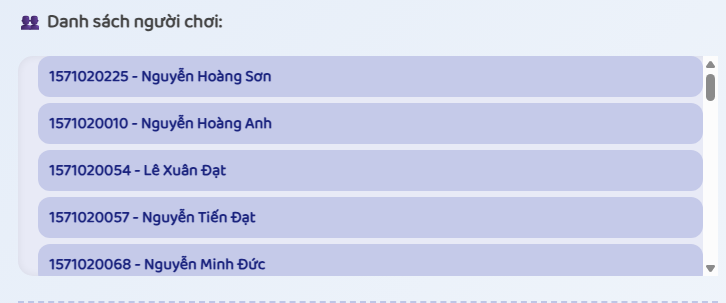


Image 5: Hiển thị danh sách sinh viên



Image 6: Rút thăm tìm ra người may mắn

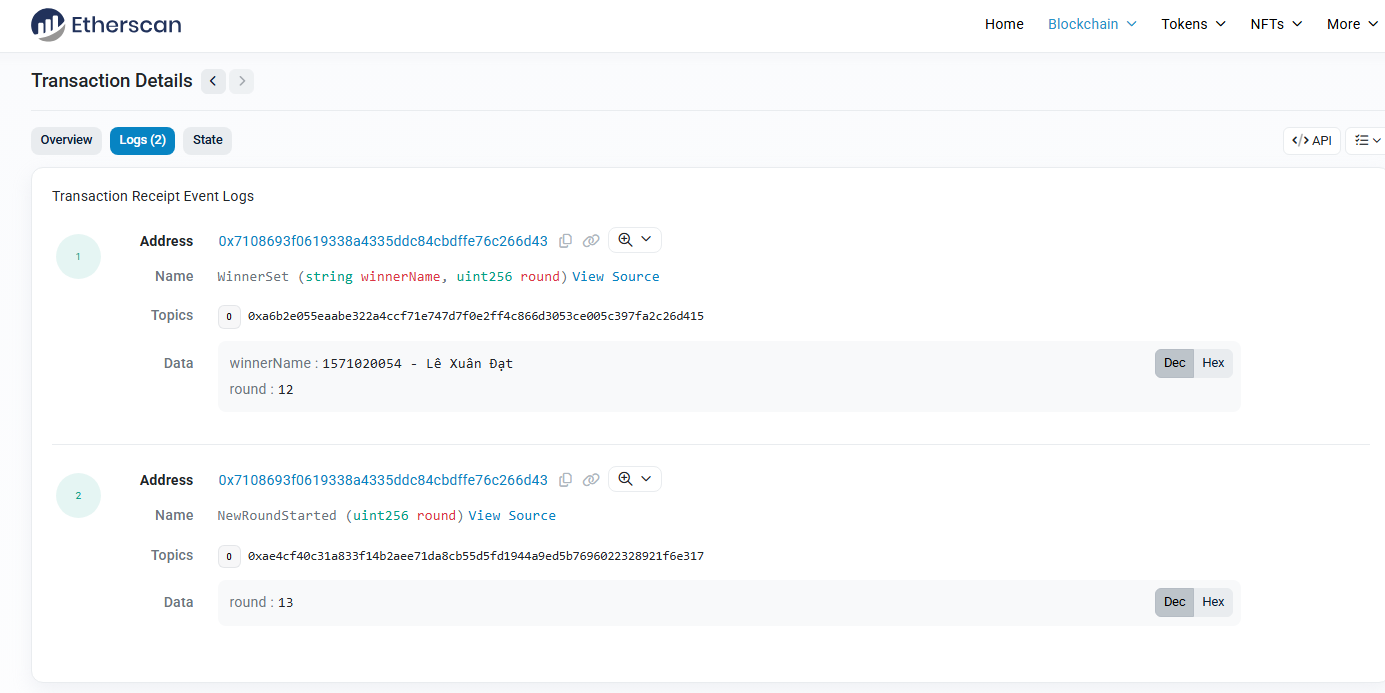


Image 7: Mã hash và thông tin người thắng được gửi lên blockchain

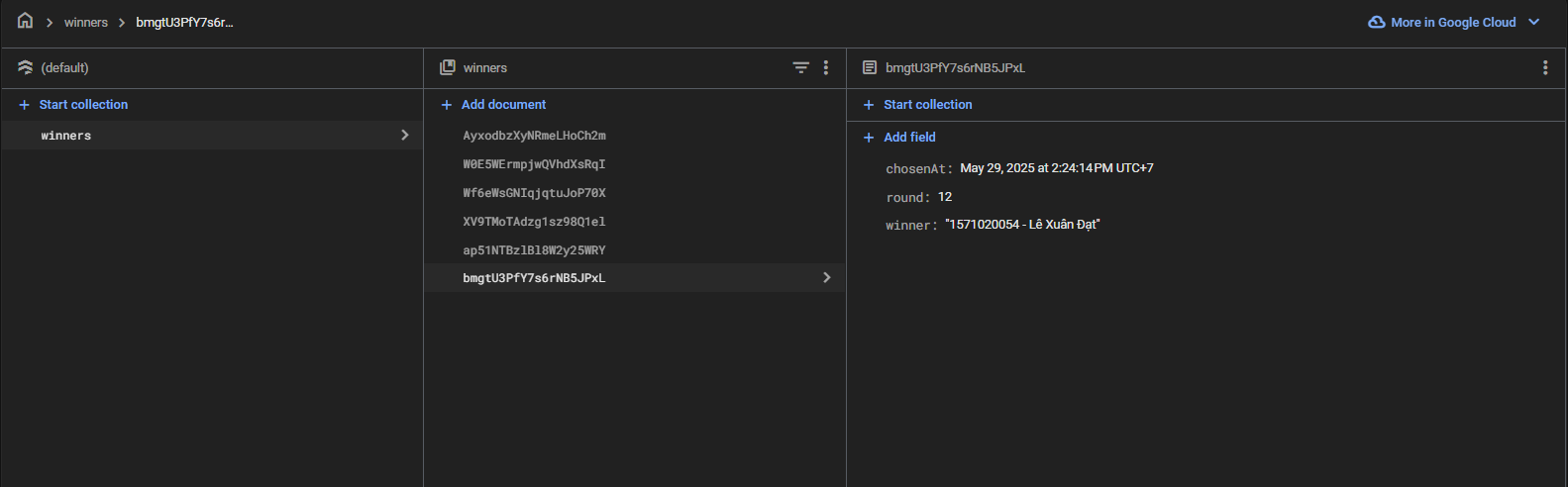


Image 8: Đồng thời được lưu trên firebase để dễ dàng quản lý

# **CHƯƠNG 6 : KẾT LUẬN**

**6.1 Tổng kết đề tài**

Trong suốt quá trình thực hiện đề tài “Blockchain rút thăm trúng thưởng lớp học”, nhóm chúng em đã xây dựng được một hệ thống đơn giản nhưng mang lại hiệu quả rõ ràng, dễ áp dụng trong thực tế lớp học. Với giao diện thân thiện, dễ sử dụng và thuật toán chọn người thắng mô phỏng dựa trên hàm băm – hệ thống đã đáp ứng được các tiêu chí đề ra từ ban đầu: công bằng, minh bạch và không thể gian lận.

Chúng em đã lần lượt:

Tìm hiểu và ứng dụng các khái niệm nền tảng của blockchain như hàm băm, ngẫu nhiên, và hợp đồng thông minh.

Thiết kế giao diện trực quan, dễ thao tác, phù hợp với không gian lớp học.

Triển khai thuật toán chọn người thắng dựa trên hash và yếu tố ngẫu nhiên.

Mô phỏng khả năng nâng cấp hệ thống lên blockchain thật thông qua smart contract.

Mặc dù không triển khai trực tiếp trên mạng blockchain như Ethereum, nhưng hệ thống của nhóm đã thể hiện rõ nguyên lý hoạt động, đồng thời tạo tiền đề cho việc mở rộng trong tương lai nếu có nhu cầu áp dụng ở quy mô lớn hơn.

**6.2 Đánh giá kết quả đạt được**

Ưu điểm nổi bật:

Giao diện đơn giản, thân thiện, dễ triển khai trong thực tế.

Thuật toán minh bạch, người dùng không thể can thiệp kết quả.

Tái hiện được tư duy blockchain thông qua cách lưu trữ và chọn người thắng bằng hash.

Có khả năng mở rộng và kết nối với hợp đồng thông minh thật trong tương lai.

Khả năng áp dụng thực tế:

Sử dụng trong các hoạt động sinh hoạt lớp, tổ chức sự kiện nội bộ, chọn nhóm ngẫu nhiên...

Là công cụ giúp học sinh – sinh viên tiếp cận công nghệ blockchain một cách dễ hiểu và gần gũi.

**6.3 Hạn chế**

Dù đạt được nhiều kết quả tích cực, hệ thống vẫn còn một số điểm hạn chế:

Chưa tích hợp trực tiếp với blockchain thật như Ethereum hoặc BNB Chain.

Thuật toán tạo ngẫu nhiên còn phụ thuộc vào dữ liệu nội bộ (timestamp hoặc chuỗi giả lập).

Chưa có tính năng lưu dữ liệu lâu dài (chỉ lưu tạm trong session).