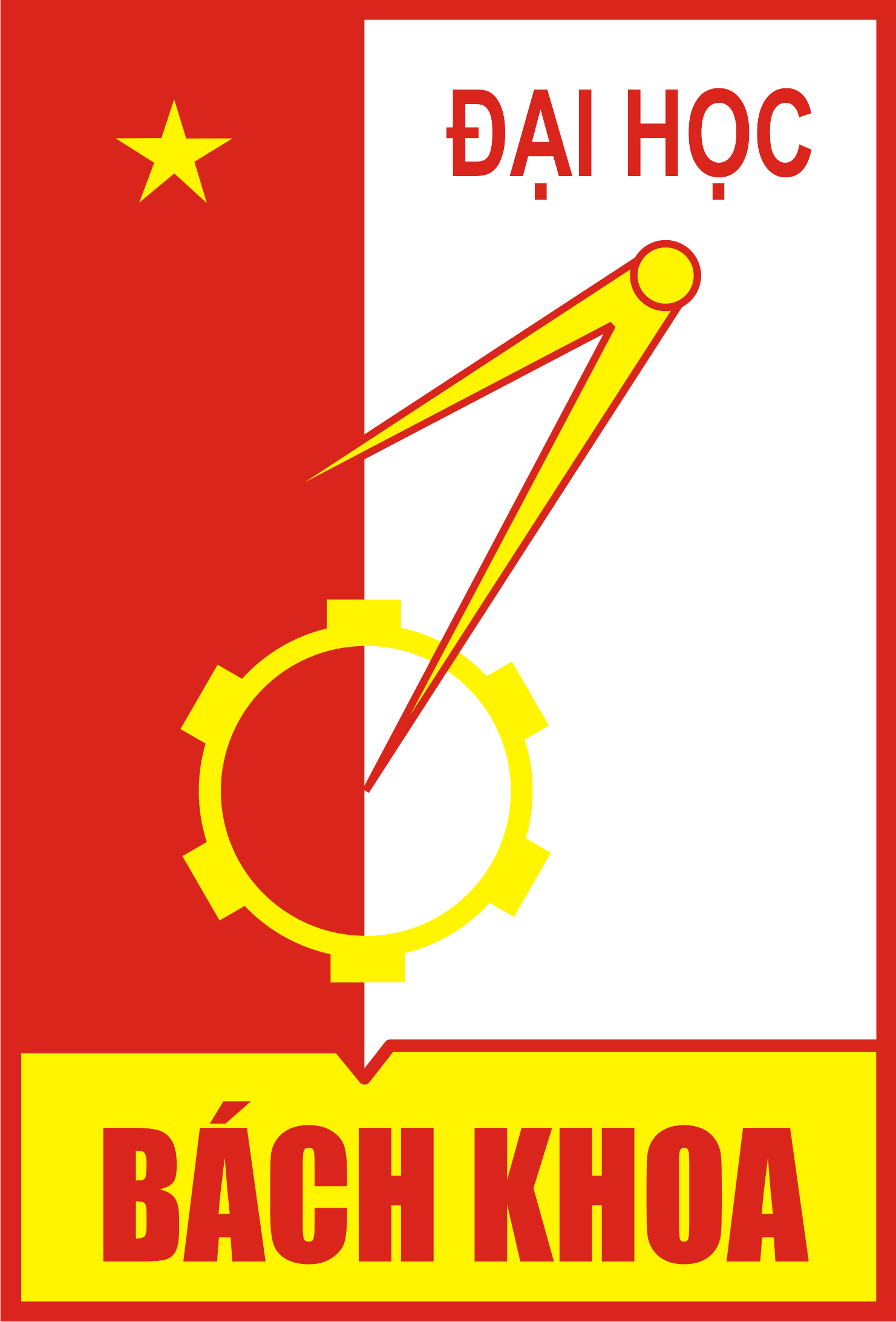
TRƯỜNG ĐẠI HỌC BÁCH KHOA HÀ NỘI

VIỆN CÔNG NGHỆ THÔNG TIN VÀ TRUYỀN THÔNG

──────── \* ───────



BÁO CÁO: An toàn trong giao dịch điện tử

Đề tài: Xổ số Online

Giảng viên hướng dẫn: TS. Trần Vĩnh Đức

Sinh viên thực hiện: Trần Cảnh Tuấn – 20154144

Lê Văn Mạnh – 20152395

***Hà Nội, tháng 12 năm 2019***

**Lời nói đầu**

Thế kỷ XXI với trọng tâm phát triển là cách mạng công nghiệp 4.0 lấy Công nghệ thông tin làm chủ đạo. Không riêng gì các nhóm ngành thuần công nghệ áp dụng các kỹ thuật về công nghệ thông tin, mà cả các nhóm ngành khác như trồng trọt, chăn nuôi, … cũng có thể áp dụng công nghệ thông tin, giúp việc quản lý và vận hành trở nên thuận tiện và đơn giản hơn, đồng thời cũng mang lại được kết quả cao hơn so với cách thức tiếp cận và quản lý truyền thống. Lấy ví dụ trong trồng trọt, việc phun thuốc chống sâu bệnh có thể được thực hiện thông qua các thiết bị bay không người lái, kết nối với thiết bị điều khiển trung tâm thông qua mạng di động hoặc mạng wifi, quản lý về tốc độ bay, lượng thuốc được phun, áp suất và gió thông qua phần mềm. Độ ẩm của đất cũng có thể được thu thập bằng các cảm biến, sau đó truyền thông tin qua giao tiếp mạng đến thiết bị quản lý trung tâm để có thể điều chỉnh lượng nước, phân kịp thời. Trong chăn nuôi có thể ứng dụng công nghệ thông tin vào việc quản lý nhập xuất đàn, thời gian tiêm thuốc định kỳ, nhiệt độ trong các chuồng trại, … Gần hơn là các cửa hàng có thể tạo một gian hàng trên các trang thương mại điện tử, giúp cho sản phẩm của mình đến gần hơn với người tiêu dùng mà không mất thêm nhiều chi phí, quản lý đơn hàng và bán hàng cũng dễ dàng hơn, … Và còn rất nhiều ứng dụng nữa của công nghệ thông tin. Nhưng nếu nhìn kỹ, chúng ta sẽ thấy tất cả đều xoay quanh thông tin. Thông tin thu thập từ các cảm biến, thông tin giao dịch của các đơn hàng, xa hơn là thông tin vận hành của các công ty hay doanh nghiệp, thông tin của quốc gia, … Vậy điều gì xảy ra nếu các thông tin được đưa lên là giả mạo, hay một ai đó cố ý làm sai lệch những thông tin này? Nhận thấy nguy cơ tiềm ẩn về vấn đề này, một công nghệ mới xuất hiện và nổi lên trong thời gian gần đây, đó là Blockchain. Với công nghệ này đảm bảo một thông tin nếu đã được xuất bản theo lý thuyết thì không thể bị chỉnh sửa. Nó cũng giúp minh bạch hóa các tác vụ đã được thực hiện và chỉ đích danh người thực hiện nó. Nhận thấy đây là một lĩnh vực mới và nhiều tiềm năng, trong học phần này nhóm quyết định nghiên cứu và trình bày ví dụ về một ứng dụng của Blockchain thông qua một trò chơi là Xổ Số.

Trong quá trình thực hiện đề tài, nhóm rất cảm ơn thầy Trần Vĩnh Đức đã có những góp ý vô cùng thiết thực giúp nhóm có thể hoàn thiện được sản phẩm tốt hơn. Báo cáo chắc hẳn vẫn còn nhiều thiếu sót, rất mong nhận được ý kiến đóng góp của thầy.

Nội dung

[Giới thiệu 5](#_Toc27083790)

[1. Giới thiệu Xổ số 6](#_Toc27083791)

[2. Thiết kế hệ thống 7](#_Toc27083792)

[3. Minh họa 9](#_Toc27083793)

[Tài liệu tham khảo 10](#_Toc27083794)

# Giới thiệu

Chơi xổ số là một hình thức không còn xa lạ gì đối với mọi người. Nhưng với thời đại của công nghệ phát triển, mọi người không có nhiều thời gian để theo dõi, tham gia không chỉ xổ số mà bất cứ một trò chơi truyền thống nào. Vì vậy để có thể tiếp cận tốt hơn, rộng hơn, các trò chơi có xu hướng Online hóa để có thêm nhiều người chơi. Nhưng việc tham gia trên môi trường mạng tiềm ẩn nhiều rủi ro, đồng thời thông tin cũng khó thể nào minh bạch, xác nhận rằng thông tin đó là chính người chơi đó tạo ra mà không phải là một người nào khác. Và giả sử khi trao thưởng thì không thể có một người khác với thông tin không phù hợp mà lại được nhận thưởng. Những vấn đề này trong đề tài Xổ số Online, nhóm sẽ giải quyết bằng cách sử dụng công nghệ Blockchain.

Trò chơi sẽ được viết dựa trên mạng Blockchain Ethereum, đây là một nền tảng có cung cấp các hàm lập trình để có thể lập trình các đoạn mã tương tác với mạng. Ngôn ngữ được sử dụng là Python. Trò chơi sẽ cho phép người chơi thao tác thông qua một giao diện web, chơi và kiểm tra số dư trong ví của mình. Trong các phần tiếp theo của báo cáo nhóm sẽ trình bày kĩ hơn về cách xây dựng trò chơi online này và cách tương tác với mạng Blockchain để minh bạch và đảm bảo thông tin của người chơi.

# 1. Giới thiệu Xổ số

Xổ số là một trò chơi liên quan đến chọn các con số cho một giải thưởng. Xổ số có nhiều hình thức. Ví dụ, giải thưởng có thể là một số tiền mặt cố định hoặc hàng hoá. Trong hình thức này, có nguy cơ người tổ chức sẽ bị lỗ nếu không bán được đủ số vé. Một cách khác phổ biến hơn là quỹ giải thưởng sẽ là một tỷ lệ phần trăm cố định của tổng số tiền vé (phổ biến là 50% tiền vé). Nhiều loại xổ số gần đây cho phép người mua lựa chọn số trên vé số, dẫn đến việc có thể có nhiều người chiến thắng trong một kỳ quay số.

Hiểu đơn giản, người chơi sẽ tiến hành chọn con số mà mình mong muốn trước giờ quay số trúng thưởng, sau giờ quay số người chơi sẽ không được tham gia nữa. Đến giờ quay số cơ quan chủ quản tổ chức sẽ tiến hành quay số và thông báo kết quả. Người chơi nào có số đã chọn trùng với số mà cơ quan chủ quản thông báo sẽ nhận được giải thưởng. Khi đưa trò chơi lên hình thức Online sẽ gặp một số vấn đề

* Có thể thay đổi thông tin phía server để giả mạo người trúng thưởng để nhận thưởng
* Có thể bị từ chối trả thưởng do nhà cái giả thông tin trúng thưởng và submit trước người trúng thưởng thật

Khi áp dụng mạng Blockchain vào trò chơi này sẽ không thể bị giả mạo kết quả và thông tin đã tham gia chơi của người chơi.

# 2. Thiết kế hệ thống

Để tham gia trò chơi, đầu tiên người chơi sẽ tiến hành nhập các thông tin cần thiết, bao gồm

* Con số muốn chơi
* Số tiền muốn cược

Server sẽ tiến hành lấy những thông tin này, kèm theo thông tin về thời gian. Yếu tố thời gian quan trọng vì cần có một thời gian cụ thể để tiến hành quay số, từ thời gian này trở đi người chơi sẽ không thể tham gia chơi. Hệ thống được thiết kế để thời gian cố định này là 18h30p, và từ 18h00 hệ thống sẽ đóng lại và người chơi sẽ không thể tham gia chơi nữa. Tức nếu hợp lệ, server sẽ nắm các thông tin

* Con số muốn chơi
* Số tiền muốn cược
* Thời gian chơi

Các thông tin này sẽ được đẩy lên Blockchain, sau đó mạng sẽ trả về một transaction ID. Người chơi cần lưu lại thông tin này để nếu có trúng thưởng thì sẽ nhập thông tin transaction này để nhận thưởng.

Khi đến thời gian đã cài đặt trước (ở đây là 18h30p), hệ thống sẽ tự lấy thông tin từ web xổ số, trích xuất để xác định con số trúng thưởng. Con số này sẽ được đẩy lên smartcontract để lưu. Hệ thống được thiết kế sao cho mô phỏng giống nhất so với chơi xổ số ở ngoài đời thực, theo đó người chơi nếu trúng sẽ phải tự mình nhập thông tin transaction ID phía trên vào hệ thống để nhận thưởng. Khi thông tin này được đẩy lên mạng, sẽ được kiểm tra với con số trúng thưởng đã lưu phía trước bằng cách chạy smartconstract. Nếu thông tin nhận thưởng là phù hợp, tiền sẽ được chuyển về ví cho người chơi. Minh họa bằng hình ảnh sau

A close up of a map

Description automatically generated

# 3. Minh họa

Kiểm tra số tiền hiện có trong tài khoản trước khi chơi

A screenshot of a cell phone

Description automatically generated

Người chơi đặt con số kèm các thông tin cần thiết

A screenshot of a cell phone

Description automatically generated

Kiểm tra ví sau khi biết đã trúng thưởng

A screenshot of a cell phone

Description automatically generated

Bảng thực nghiệm chi phí khi chạy các hàm cần thiết

|  |  |  |
| --- | --- | --- |
| **Function** | **Giá ETH** | **Giá $** |
| buile smartcontract | 0.000636 | ~ $0.09 |
| set\_number\_win | 0.000042 | ~ $0.006 |
| submit | 0.000081 | ~ $0.01 |
| post\_to\_blockchain | 0.00000005 | ~ $0.000007 |

# Tài liệu tham khảo

1. *Ethereum Documentation* < <https://ethereum.org/developers/> >.

[Ngày truy cập: 12/12/2019].

1. *Top 100 Cryptocurrencies by Market Capitalization* < <https://coinmarketcap.com/?fbclid=IwAR1Aa86Whi29wFGvYRr9PM6Ls2brAMTXmutypq-omvqwvE3QwUIaQOGXuFY> >

[Ngày truy cập: 12/12/2019].