**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 BLOCKCHAIN**

**ĐỀ TÀI: KHÓA THỜI GIAN BIỂU QUYẾT**

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

**Sinh viên thực hiện:**  **Nhóm 5**

|  |  |  |  |
| --- | --- | --- | --- |
| **Stt** | **Mã sinh viên** | **Họ và tên** | **Lớp** |
| 1 | 1571020025 | Nguyễn Việt Châu | CNTT 15-01 |
| 2 | 1571020264 | Vũ Ngọc Tuấn | CNTT 15-01 |
| 3 | 1571020009 | Nguyễn Đức Anh | CNTT 15-01 |

**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 BLOCKCHAIN**

**ĐỀ TÀI: KHÓA THỜI GIAN BIỂU QUYẾT**

|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
| STT | Mã Sinh Viên | Họ và Tên | Ngày Sinh | Điểm | |
| Bằng Số | Bằng Chữ |
| 1 | 1571020025 | Nguyễn Việt Châu | 17/04/2003 |  |  |
| 2 | 1571020264 | Vũ Ngọc Tuấn | 11/02/2003 |  |  |
| 3 | 1571020009 | Nguyễn Đức Anh | 18/09/2003 |  |  |

### 

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

**Hà Nội, năm 2025**

**LỜI NÓI ĐẦU**

Kính gửi thầy Công,

Trong thời đại công nghệ số phát triển mạnh mẽ như hiện nay, Blockchain đã trở thành một trong những nền tảng công nghệ quan trọng, mang lại tính minh bạch, bảo mật và phi tập trung trong nhiều lĩnh vực, đặc biệt là trong các hệ thống biểu quyết điện tử. Với mong muốn tìm hiểu sâu hơn về ứng dụng của công nghệ này, em đã chọn thực hiện đề tài **"Khóa thời gian biểu quyết trong Blockchain"** trong khuôn khổ bài tập lớn môn học *Blockchain*.

Đề tài tập trung vào việc xây dựng một hệ thống biểu quyết dựa trên hợp đồng thông minh, trong đó chỉ cho phép người dùng thực hiện quyền bỏ phiếu trong một khoảng thời gian nhất định. Việc giới hạn thời gian giúp nâng cao tính bảo mật, công bằng và đảm bảo tính toàn vẹn của dữ liệu biểu quyết. Ngoài ra, đề tài còn tích hợp giao diện đếm ngược thời gian biểu quyết nhằm nâng cao trải nghiệm người dùng và minh bạch hóa quá trình bỏ phiếu.

Trong quá trình thực hiện đề tài, em đã có cơ hội áp dụng các kiến thức về Blockchain, Solidity, giao tiếp giữa frontend và smart contract, cũng như triển khai hợp đồng trên mạng thử nghiệm (testnet). Đây là cơ hội quý báu để em củng cố kiến thức và rèn luyện kỹ năng thực hành công nghệ mới.

Em xin chân thành cảm ơn **Tiến sĩ Trần Đăng Công** – giảng viên hướng dẫn môn *Blockchain* tại **Trường Đại học Đại Nam** – người đã tận tình truyền đạt kiến thức, định hướng và hỗ trợ em trong suốt quá trình học tập và thực hiện đề tài.

Tuy đã rất cố gắng, nhưng do thời gian và kiến thức còn hạn chế, bài báo cáo chắc chắn không tránh khỏi thiếu sót. Em rất mong nhận được sự góp ý, nhận xét từ thầy cô để hoàn thiện hơn trong những lần nghiên cứu tiếp theo.

Trân trọng,

Mục lục

[**LỜI NÓI ĐẦU** 3](#_Toc199967167)

[CHƯƠNG I: TỔNG QUAN ĐỀ TÀI 8](#_Toc199967168)

[1.1. Đặt vấn đề 8](#_Toc199967169)

[**1.2.** **Mục tiêu đề tài** 10](#_Toc199967170)

[1.2.1. Xây dựng hợp đồng thông minh (Smart Contract) cho phép người dùng bỏ phiếu, chỉ khi thời gian hiện tại nằm trong khoảng thời gian cho phép 10](#_Toc199967171)

[1.2.2. Từ chối mọi phiếu bầu được gửi sau thời điểm kết thúc thời gian biểu quyết 11](#_Toc199967172)

[1.2.3. Thiết kế giao diện người dùng có tích hợp đồng hồ đếm ngược giúp hiển thị thời gian còn lại cho đến thời điểm kết thúc 11](#_Toc199967173)

[1.2.4. Triển khai hệ thống trên mạng thử nghiệm (Testnet) và thực hiện kiểm thử chức năng 12](#_Toc199967174)

[**1.3.** **Phạm vi thực hiện** 13](#_Toc199967175)

[ Công nghệ sử dụng 13](#_Toc199967176)

[ Chức năng chính 13](#_Toc199967177)

[**1.4.** **Ý nghĩa của đề tài** 14](#_Toc199967178)

[ Tăng cường tính minh bạch và công bằng 14](#_Toc199967179)

[ Loại bỏ hành vi gian lận và thao túng 15](#_Toc199967180)

[ Giá trị thực tiễn cao 15](#_Toc199967181)

[ Khả năng mở rộng và phát triển 16](#_Toc199967182)

[CHƯƠNG II: CƠ SỞ LÝ THUYẾT 17](#_Toc199967183)

[2.1. Tổng quan về Blockchain 17](#_Toc199967184)

[2.1.1. Khái niệm Blockchain 17](#_Toc199967185)

[2.1.2. Đặc điểm của Blockchain 18](#_Toc199967186)

[2.1.3. Ứng dụng của Blockchain 19](#_Toc199967187)

[**2.2. Hợp đồng thông minh (Smart Contract)** 25](#_Toc199967188)

[**2.2.1. Định nghĩa** 25](#_Toc199967189)

[2.2.2. Quy trình hoạt động của hợp đồng thông minh 26](#_Toc199967190)

[**2.2.3. Ngôn ngữ lập trình Solidity** 27](#_Toc199967191)

[2.3. Biểu quyết trên nền tảng Blockchain 27](#_Toc199967192)

[2.3.1. Cơ chế hoạt động của một hệ thống e-voting trên Blockchain 27](#_Toc199967193)

[2.3.2. Lợi ích của biểu quyết trên nền tảng Blockchain 29](#_Toc199967194)

[CHƯƠNG III: THỰC HIỆN VÀ TRIỂN KHAI 31](#_Toc199967195)

[3.1. Mục đích xây dựng giao diện 31](#_Toc199967196)

[3.2. Cấu trúc giao diện 31](#_Toc199967197)

# CHƯƠNG I: TỔNG QUAN ĐỀ TÀI

## Đặt vấn đề

Công nghệ Blockchain đã trở thành một trong những đột phá quan trọng nhất của thế kỷ 21, hứa hẹn một cuộc cách mạng trong nhiều lĩnh vực từ tài chính, chuỗi cung ứng, y tế đến quản lý dữ liệu. Bản chất phân tán, bất biến và minh bạch của blockchain đã tạo ra một mô hình tin cậy mới, loại bỏ sự cần thiết của các bên trung gian tập trung. Tuy nhiên, cùng với sự phát triển nhanh chóng và khả năng ứng dụng rộng rãi, blockchain cũng phải đối mặt với nhiều thách thức cố hữu, đặc biệt là trong các cơ chế quản trị và ra quyết định. Một trong những thách thức nổi bật nhất chính là việc đảm bảo tính công bằng, hiệu quả và chống lại các hành vi thao túng trong quá trình **biểu quyết** – một yếu tố then chốt quyết định sự phát triển và định hướng của bất kỳ hệ thống phi tập trung nào.

Trong một hệ sinh thái blockchain, các quyết định quan trọng liên quan đến nâng cấp giao thức, thay đổi tham số mạng, hoặc phân bổ tài nguyên thường được đưa ra thông qua cơ chế biểu quyết của cộng đồng. Mặc dù các cơ chế này được thiết kế để dân chủ hóa quá trình ra quyết định, chúng lại tiềm ẩn nhiều rủi ro. Các vấn đề như **tỷ lệ tham gia thấp**, **sự chi phối của các cá voi** (whale – những người nắm giữ lượng lớn token), hoặc **khả năng tấn công bằng 51%** vẫn luôn là mối lo ngại thường trực. Đặc biệt, việc các chủ thể lớn có thể tập trung quyền lực và bỏ phiếu theo ý muốn của mình mà không bị ràng buộc về thời gian hoặc trách nhiệm, có thể dẫn đến những quyết định không tối ưu, làm mất đi tính phi tập trung và gây tổn hại đến lợi ích chung của mạng lưới.

Hơn nữa, trong nhiều trường hợp, quá trình biểu quyết diễn ra tức thời hoặc trong một khoảng thời gian ngắn, tạo điều kiện cho các chiến lược bỏ phiếu "chụp giật" hoặc các hành vi thao túng kết quả. Sự thiếu vắng một cơ chế ràng buộc thời gian hiệu quả đã làm giảm đi tính bền vững và sự ổn định của các quyết định được đưa ra. Điều này đặt ra một câu hỏi lớn: Làm thế nào để thiết kế một hệ thống biểu quyết trên blockchain vừa đảm bảo tính dân chủ, vừa khuyến khích sự tham gia có trách nhiệm và ngăn chặn các hành vi gây hại?

Trong bối cảnh đó, ý tưởng về **"Khóa thời gian biểu quyết" (Voting Time-Lock)** nổi lên như một giải pháp tiềm năng, mang lại một phương pháp tiếp cận mới mẻ để giải quyết các vấn đề trên. Cơ chế này đề xuất việc ràng buộc quyền biểu quyết với một khoảng thời gian khóa nhất định. Điều đó có nghĩa là, để có quyền tham gia biểu quyết hoặc để phiếu bầu của họ có trọng số cao hơn, người tham gia cần phải khóa một lượng token của họ trong một khoảng thời gian nhất định. Thời gian khóa càng dài, hoặc lượng token được khóa càng lớn, trọng số phiếu bầu có thể càng cao. Điều này không chỉ khuyến khích những người tham gia có tầm nhìn dài hạn và cam kết với sự phát triển của dự án, mà còn tạo ra một rào cản kinh tế đối với các hành vi thao túng ngắn hạn.

Việc triển khai "Khóa thời gian biểu quyết" không chỉ giúp tăng cường tính bảo mật và chống lại các cuộc tấn công, mà còn thúc đẩy sự gắn kết của cộng đồng, tạo ra một môi trường biểu quyết công bằng và minh bạch hơn. Nó buộc các chủ thể phải suy nghĩ kỹ lưỡng về quyết định của mình, bởi vì hành động bỏ phiếu của họ sẽ đi kèm với một cam kết về tài sản trong tương lai. Điều này có thể dẫn đến những quyết định được cân nhắc kỹ lưỡng hơn, phản ánh lợi ích dài hạn của mạng lưới thay vì những lợi ích ngắn hạn.

Tuy nhiên, việc thiết kế và triển khai một hệ thống "Khóa thời gian biểu quyết" hiệu quả cũng không hề đơn giản. Cần phải nghiên cứu sâu rộng để xác định các tham số tối ưu như độ dài thời gian khóa, cơ chế tăng trọng số phiếu bầu, và cách thức xử lý các trường hợp đặc biệt. Làm thế nào để cân bằng giữa việc khuyến khích tham gia và không tạo ra rào cản quá lớn cho người dùng mới? Làm thế nào để đảm bảo rằng cơ chế này không vô tình tập trung quyền lực vào tay một số ít chủ thể có khả năng khóa token trong thời gian dài? Những câu hỏi này đòi hỏi một cách tiếp cận đa chiều, kết hợp giữa lý thuyết kinh tế, khoa học máy tính và thiết kế cơ chế.

Chính vì những lý do trên, đề tài **"Nghiên cứu về Khóa thời gian biểu quyết trong Blockchain"** trở nên cấp thiết và có ý nghĩa to lớn. Mục tiêu của nghiên cứu này là khám phá sâu hơn về cơ chế "Khóa thời gian biểu quyết", đánh giá tiềm năng của nó trong việc cải thiện quản trị phi tập trung, đồng thời phân tích những thách thức và đề xuất các giải pháp tối ưu. Thông qua việc tìm hiểu các mô hình đã có và phát triển những ý tưởng mới, chúng em hy vọng sẽ đóng góp vào việc xây dựng các hệ thống blockchain mạnh mẽ, bền vững và thực sự phi tập trung trong tương lai.

* 1. **Mục tiêu đề tài**

Đề tài "Khóa thời gian biểu quyết trong Blockchain" được định hướng với mục tiêu chính là **xây dựng một mô hình biểu quyết điện tử ứng dụng công nghệ Blockchain hiệu quả, minh bạch và có khả năng kiểm soát chặt chẽ về thời gian**. Mô hình này sẽ giải quyết những hạn chế cố hữu của các hệ thống biểu quyết truyền thống và cả một số cơ chế biểu quyết blockchain hiện tại, đặc biệt là việc đảm bảo tính công bằng và chống thao túng thông qua ràng buộc thời gian.

Cụ thể, đề tài sẽ tập trung vào việc đạt được các mục tiêu sau:

### 1.2.1. Xây dựng hợp đồng thông minh (Smart Contract) cho phép người dùng bỏ phiếu, chỉ khi thời gian hiện tại nằm trong khoảng thời gian cho phép

Mục tiêu cốt lõi của đề tài là **thiết kế và phát triển một hoặc nhiều Smart Contract trên nền tảng Blockchain** có khả năng quản lý toàn bộ quy trình biểu quyết. Smart Contract này sẽ không chỉ đơn thuần ghi nhận phiếu bầu mà còn đóng vai trò là "người gác cổng" về thời gian. Điều này có nghĩa là, hợp đồng thông minh sẽ được lập trình để **chỉ chấp nhận các phiếu bầu được gửi đi trong một khoảng thời gian được định trước và rõ ràng**. Khoảng thời gian này sẽ bao gồm thời điểm bắt đầu biểu quyết và thời điểm kết thúc biểu quyết. Mục tiêu này đòi hỏi sự hiểu biết sâu sắc về ngôn ngữ lập trình Smart Contract (ví dụ: Solidity cho Ethereum) và các cơ chế quản lý thời gian trên blockchain để đảm bảo rằng mọi giao dịch gửi phiếu bầu đều được xác thực dựa trên timestamp của block, từ đó loại bỏ khả năng gian lận thời gian hoặc bỏ phiếu ngoài khung giờ quy định.

### 1.2.2. Từ chối mọi phiếu bầu được gửi sau thời điểm kết thúc thời gian biểu quyết

Để đảm bảo tính toàn vẹn và công bằng của quá trình biểu quyết, một mục tiêu quan trọng khác là **phát triển cơ chế để Smart Contract tự động từ chối (reject) hoặc không ghi nhận (ignore) bất kỳ phiếu bầu nào được gửi đến sau khi thời điểm kết thúc biểu quyết đã được thiết lập**. Điều này sẽ ngăn chặn các hành vi bỏ phiếu muộn, cố ý thay đổi kết quả sau cùng hoặc tạo ra sự bất ổn trong hệ thống. Việc triển khai mục tiêu này đòi hỏi logic kiểm tra thời gian chặt chẽ trong Smart Contract, đảm bảo rằng mọi giao dịch liên quan đến việc bỏ phiếu đều được kiểm tra điều kiện thời gian một cách nghiêm ngặt trước khi được xử lý và ghi vào sổ cái. Mục tiêu này cũng bao gồm việc cung cấp các thông báo hoặc mã lỗi rõ ràng cho người dùng khi phiếu bầu của họ bị từ chối do quá thời hạn.

### 1.2.3. Thiết kế giao diện người dùng có tích hợp đồng hồ đếm ngược giúp hiển thị thời gian còn lại cho đến thời điểm kết thúc

Để tăng cường trải nghiệm người dùng (UX) và tính minh bạch của hệ thống, đề tài sẽ **thiết kế và phát triển một giao diện người dùng (User Interface - UI) trực quan và thân thiện**. Giao diện này không chỉ cho phép người dùng dễ dàng xem thông tin về các cuộc biểu quyết, đề xuất đang diễn ra, mà còn tích hợp một **đồng hồ đếm ngược (countdown timer) nổi bật**. Đồng hồ này sẽ hiển thị chính xác thời gian còn lại cho đến khi cuộc biểu quyết kết thúc, giúp người dùng nắm bắt thông tin nhanh chóng và kịp thời đưa ra quyết định của mình. Mục tiêu này đòi hỏi việc kết nối giao diện với dữ liệu thời gian từ Smart Contract trên blockchain một cách linh hoạt, đảm bảo tính đồng bộ và chính xác. Một giao diện người dùng tốt sẽ khuyến khích sự tham gia của cộng đồng và giúp họ cảm thấy tự tin hơn vào tính công bằng của hệ thống.

### 1.2.4. Triển khai hệ thống trên mạng thử nghiệm (Testnet) và thực hiện kiểm thử chức năng

Cuối cùng, để kiểm chứng tính khả thi và ổn định của mô hình đã xây dựng, đề tài sẽ tiến hành **triển khai toàn bộ hệ thống biểu quyết điện tử (bao gồm Smart Contract và giao diện người dùng) trên một mạng thử nghiệm (Testnet)** của blockchain (ví dụ: Ropsten, Goerli, Sepolia cho Ethereum). Việc triển khai trên Testnet cho phép kiểm thử các chức năng một cách an toàn mà không tốn chi phí thực tế. Sau khi triển khai, nhóm nghiên cứu sẽ **thực hiện kiểm thử chức năng (functional testing) một cách toàn diện**, bao gồm kiểm thử các trường hợp bỏ phiếu hợp lệ trong thời gian cho phép, kiểm thử các trường hợp bỏ phiếu sau thời gian kết thúc, kiểm thử sự chính xác của đồng hồ đếm ngược, và kiểm thử khả năng xử lý các tình huống biên. Mục tiêu này không chỉ đảm bảo rằng hệ thống hoạt động đúng theo thiết kế mà còn giúp phát hiện và khắc phục các lỗi tiềm ẩn, từ đó nâng cao độ tin cậy và sẵn sàng cho các ứng dụng thực tế trong tương lai.

Thông qua việc đạt được những mục tiêu trên, đề tài này không chỉ cung cấp một giải pháp kỹ thuật cụ thể cho vấn đề quản trị phi tập trung mà còn đóng góp vào việc thúc đẩy sự phát triển của công nghệ Blockchain trong các ứng dụng thực tiễn, đặc biệt là trong lĩnh vực biểu quyết và ra quyết định công bằng.

* 1. **Phạm vi thực hiện**

### Công nghệ sử dụng

Để đảm bảo tính khả thi và hiệu quả trong quá trình phát triển, đề tài sẽ tập trung vào các công nghệ phổ biến và mạnh mẽ trong hệ sinh thái blockchain:

* **Hợp đồng thông minh (Smart Contract):** Chúng em sẽ sử dụng ngôn ngữ **Solidity** để phát triển các hợp đồng thông minh. Solidity là ngôn ngữ lập trình hàng đầu cho việc xây dựng các ứng dụng phi tập trung (DApps) trên nền tảng tương thích EVM (Ethereum Virtual Machine), mang lại sự linh hoạt và khả năng tương tác cao.
* **Kết nối giao diện frontend:** Để tương tác với các hợp đồng thông minh đã triển khai, chúng em sẽ sử dụng thư viện **Ethers.js** hoặc **Web3.js**. Cả hai đều là các thư viện JavaScript mạnh mẽ, cung cấp API để kết nối ứng dụng web với blockchain, cho phép gửi giao dịch, đọc dữ liệu từ hợp đồng và quản lý tài khoản ví.
* **Giao diện người dùng (Frontend):** Giao diện của hệ thống biểu quyết sẽ được xây dựng một cách đơn giản nhưng trực quan, sử dụng các công nghệ web cơ bản như **HTML, CSS và JavaScript**. Ngoài ra, chúng em cũng có thể xem xét sử dụng framework **ReactJS** để tạo ra một giao diện động và dễ bảo trì hơn, tùy thuộc vào yêu cầu cụ thể và thời gian thực hiện.

### Chức năng chính

Hệ thống biểu quyết được xây dựng sẽ tập trung vào các chức năng cốt lõi sau:

* **Khởi tạo biểu quyết với thời gian giới hạn:** Người quản trị hoặc người được ủy quyền sẽ có khả năng khởi tạo một cuộc biểu quyết mới trên blockchain, trong đó xác định rõ thời gian bắt đầu và thời gian kết thúc của quá trình biểu quyết.
* **Chấp nhận phiếu bầu trong thời gian hợp lệ:** Hợp đồng thông minh sẽ đảm bảo rằng chỉ những phiếu bầu được gửi đi trong khoảng thời gian đã định mới được ghi nhận. Mọi phiếu bầu được gửi trước thời gian bắt đầu hoặc sau thời gian kết thúc sẽ bị từ chối.
* **Hiển thị thời gian còn lại bằng đồng hồ đếm ngược:** Giao diện người dùng sẽ tích hợp một đồng hồ đếm ngược trực quan, hiển thị chính xác thời gian còn lại cho đến khi cuộc biểu quyết kết thúc, giúp người dùng dễ dàng theo dõi và kịp thời đưa ra quyết định.
  1. **Ý nghĩa của đề tài**

Đề tài "Khóa thời gian biểu quyết trong Blockchain" không chỉ là một bài toán kỹ thuật thuần túy về việc xây dựng một hệ thống biểu quyết điện tử. Việc tích hợp cơ chế giới hạn thời gian biểu quyết mang ý nghĩa sâu sắc, giải quyết nhiều vấn đề cốt lõi trong các hệ thống ra quyết định, từ đó nâng cao tính bảo mật, công bằng và hiệu quả kiểm soát quy trình. Dưới đây là những ý nghĩa chính mà đề tài mang lại:

### Tăng cường tính minh bạch và công bằng

Trong bất kỳ hệ thống biểu quyết nào, sự minh bạch và công bằng là yếu tố tối quan trọng. Với cơ chế **khóa thời gian biểu quyết**, hệ thống sẽ đảm bảo rằng **chỉ những phiếu bầu được gửi trong khung thời gian đã định trước và rõ ràng mới được coi là hợp lệ và được ghi nhận**. Điều này loại bỏ hoàn toàn sự nhập nhằng về thời gian, vốn có thể dẫn đến tranh chấp hoặc sự nghi ngờ về kết quả. Mọi người tham gia đều biết chính xác khi nào cuộc biểu quyết bắt đầu và kết thúc, tạo ra một sân chơi bình đẳng. Điều này đặc biệt có ý nghĩa trong các hệ thống phi tập trung, nơi niềm tin được xây dựng dựa trên sự minh bạch và các quy tắc được thực thi tự động bởi hợp đồng thông minh.

### Loại bỏ hành vi gian lận và thao túng

Một trong những vấn đề lớn nhất của các hệ thống biểu quyết truyền thống, và cả một số hệ thống blockchain chưa tối ưu, là khả năng bị thao túng hoặc gian lận. Kẻ gian có thể cố gắng gửi phiếu bầu sau khi thời gian đã hết, hoặc lợi dụng sự thiếu rõ ràng về thời gian để điều chỉnh kết quả. Cơ chế **giới hạn thời gian biểu quyết** được tích hợp chặt chẽ trong hợp đồng thông minh sẽ **tự động từ chối mọi phiếu bầu được gửi đến sau thời điểm kết thúc**. Điều này tạo ra một rào cản kỹ thuật vững chắc, **ngăn chặn mọi hành vi cố ý lợi dụng thời gian để gây ảnh hưởng đến kết quả cuối cùng**. Nó buộc người tham gia phải đưa ra quyết định trong một khung thời gian cụ thể, tăng tính cam kết và trách nhiệm của mỗi phiếu bầu.

### Giá trị thực tiễn cao

Mô hình biểu quyết điện tử với tính năng khóa thời gian biểu quyết do đề tài này xây dựng mang lại **giá trị ứng dụng thực tiễn cao và đa dạng**. Nó có thể được triển khai hiệu quả cho các cuộc biểu quyết nội bộ trong nhiều loại hình tổ chức:

* **Công ty:** Để ra quyết định về chiến lược, chính sách nội bộ, bầu cử ban lãnh đạo.
* **Trường học/Đại học:** Tổ chức bầu cử hội học sinh, ban đại diện, hoặc các quyết định liên quan đến hoạt động học thuật.
* **Tổ chức phi chính phủ (NGOs):** Để biểu quyết về các dự án, phân bổ quỹ, hoặc các vấn đề quản trị.
* **Cộng đồng phi tập trung (DAO):** Là một giải pháp quản trị cơ bản nhưng hiệu quả cho các tổ chức tự trị phi tập trung.

Việc triển khai trên blockchain cũng giúp **giảm đáng kể chi phí vận hành** so với các hệ thống biểu quyết truyền thống, vốn thường đòi hỏi hạ tầng phức tạp, nhân sự giám sát và quy trình kiểm tra tốn kém.

### Khả năng mở rộng và phát triển

Mô hình "Khóa thời gian biểu quyết" được đề xuất trong đề tài này không chỉ là một giải pháp độc lập mà còn là **nền tảng vững chắc cho việc phát triển các tính năng nâng cao hơn trong tương lai**. Một khi cơ chế kiểm soát thời gian và tính toàn vẹn của phiếu bầu được đảm bảo, chúng ta có thể dễ dàng tích hợp thêm:

* **Xác thực người dùng nâng cao:** Ngoài việc kiểm tra địa chỉ ví, có thể tích hợp các cơ chế xác thực danh tính để tăng cường tính bảo mật.
* **Bỏ phiếu ẩn danh:** Phát triển các kỹ thuật mã hóa (như Zero-Knowledge Proofs) để đảm bảo quyền riêng tư của người bỏ phiếu mà vẫn giữ được tính minh bạch của kết quả.
* **Phân quyền quản trị:** Thiết lập các cấp độ quyền hạn khác nhau cho người dùng và quản trị viên, cho phép các nhóm cụ thể khởi tạo hoặc tham gia vào các loại biểu quyết nhất định.
* **Cơ chế trọng số phiếu bầu:** Áp dụng các quy tắc về trọng số phiếu bầu dựa trên lượng token nắm giữ, thời gian khóa token, hoặc các yếu tố khác để phản ánh mức độ cam kết của người tham gia.

Tóm lại, đề tài này không chỉ cung cấp một giải pháp kỹ thuật cụ thể mà còn góp phần xây dựng niềm tin vào các hệ thống biểu quyết phi tập trung, mở đường cho những ứng dụng rộng lớn hơn của công nghệ blockchain trong việc kiến tạo các quy trình ra quyết định công bằng, minh bạch và hiệu quả.

# CHƯƠNG II: CƠ SỞ LÝ THUYẾT

## 2.1. Tổng quan về Blockchain

### 2.1.1. Khái niệm Blockchain

Trong thời đại số hóa, một công nghệ đã âm thầm xuất hiện làm thay đổi cách thức chúng ta giao dịch, lưu trữ thông tin trên Internet, đó chính là blockchain.

Blockchain là một hệ thống cơ sở dữ liệu phân tán, hoạt động trên cơ chế chuỗi khối (blockchain), trong đó thông tin được lưu trữ trong các khối (block) và liên kết chặt chẽ với nhau thành một chuỗi (chain) liên tục, với các thông tin được mã hóa bằng thuật toán phức tạp.

Mỗi khối (block) trong chuỗi chứa:

* Dữ liệu (thông tin giao dịch, phiếu bầu,...)
* Mã băm của khối hiện tại
* Mã băm của khối trước đó
* Dấu thời gian

Blockchain là các khối dữ liệu được mã hóa và kết nối với nhau thành một chuỗi (Ảnh minh họa: Adobe).

### 2.1.2. Đặc điểm của Blockchain

 **Sổ cái phân tán (Distributed Ledger):** Đây là đặc điểm nổi bật nhất. Thay vì một cơ quan tập trung (như ngân hàng, chính phủ) nắm giữ và quản lý một sổ cái duy nhất, Blockchain phân phối bản sao của sổ cái đó đến tất cả các máy tính (nút mạng) tham gia vào mạng lưới. Mỗi nút đều có một bản sao đầy đủ và cập nhật của toàn bộ chuỗi khối. Khi một giao dịch mới xảy ra, nó sẽ được truyền bá đến tất cả các nút và được thêm vào bản sao sổ cái của mỗi nút sau khi được xác thực. Điều này loại bỏ điểm lỗi đơn lẻ và tăng cường khả năng chống chịu của hệ thống. Nếu một hoặc nhiều nút gặp sự cố, hệ thống vẫn tiếp tục hoạt động bình thường nhờ vào sự đồng thuận của các nút còn lại.

 **Bất biến (Immutable):** Một khi dữ liệu (giao dịch) đã được ghi vào một khối và khối đó đã được thêm vào chuỗi, rất khó hoặc gần như không thể thay đổi hoặc xóa bỏ dữ liệu đó. Điều này là do tính chất mã hóa của Blockchain: mỗi khối chứa một hàm băm (hash) của khối trước đó. Nếu bất kỳ dữ liệu nào trong một khối bị thay đổi, hàm băm của khối đó cũng sẽ thay đổi, làm mất hiệu lực của tất cả các khối tiếp theo trong chuỗi. Để thay đổi một giao dịch cũ, kẻ tấn công sẽ phải tính toán lại hàm băm của khối đó và tất cả các khối tiếp theo, sau đó giành quyền kiểm soát phần lớn sức mạnh tính toán của mạng lưới (tấn công 51%), điều này là cực kỳ khó khăn và tốn kém đối với các mạng lưới lớn. Tính bất biến tạo ra một mức độ tin cậy và an toàn cao cho dữ liệu.

 **Phi tập trung (Decentralized):** Blockchain không có một máy chủ trung tâm hay một cơ quan điều hành duy nhất. Thay vào đó, nó hoạt động dựa trên mạng ngang hàng (peer-to-peer). Mọi giao dịch và quy trình xác thực đều được thực hiện bởi chính các thành viên trong mạng lưới thông qua một cơ chế đồng thuận (ví dụ: Proof of Work, Proof of Stake). Sự phi tập trung loại bỏ sự phụ thuộc vào các bên trung gian tin cậy, giảm thiểu nguy cơ tham nhũng, kiểm duyệt và các điểm yếu tập trung. Quyền lực được phân tán, và quyết định được đưa ra bởi sự đồng thuận của cộng đồng.

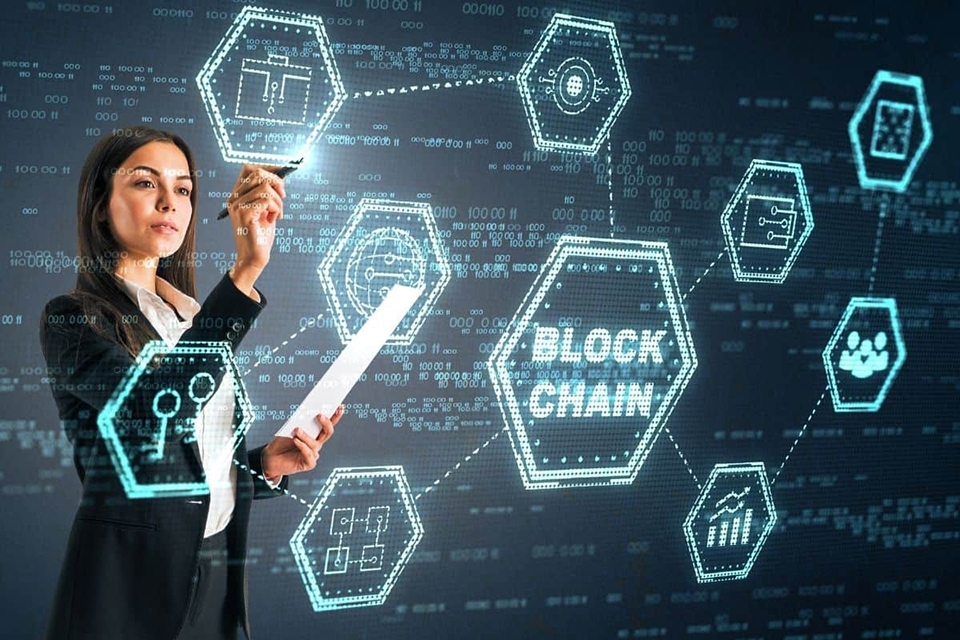
 **Minh bạch (Transparent):** Mặc dù danh tính thực của người dùng có thể được ẩn danh (thông qua địa chỉ ví công khai thay vì tên thật), tất cả các giao dịch trên Blockchain đều được công khai và có thể được bất kỳ ai kiểm tra. Mọi người đều có thể xem lịch sử giao dịch của bất kỳ địa chỉ ví nào. Tính minh bạch này giúp xây dựng niềm tin, cho phép kiểm toán độc lập và giảm thiểu rủi ro gian lận.

 **Bảo mật bằng mật mã học (Cryptographically Secured):** Các giao dịch trên Blockchain được bảo mật bằng các kỹ thuật mật mã tiên tiến. Mỗi giao dịch được ký bằng khóa riêng (private key) của người gửi và được xác minh bằng khóa công khai (public key) của họ. Dữ liệu trong các khối được liên kết với nhau bằng các hàm băm mật mã (cryptographic hash functions), tạo ra một chuỗi liên kết chặt chẽ và không thể giả mạo.

 **Đồng thuận (Consensus Mechanism):** Để đảm bảo tất cả các nút trong mạng lưới đều có cùng một bản sao sổ cái và đồng ý về tính hợp lệ của các giao dịch, Blockchain sử dụng các thuật toán đồng thuận. Các thuật toán này quy định cách thức các khối mới được tạo ra và thêm vào chuỗi. Ví dụ phổ biến nhất là Proof of Work (PoW) được sử dụng bởi Bitcoin và Ethereum (trước đây), nơi các thợ đào cạnh tranh để giải quyết một bài toán mật mã khó, và Proof of Stake (PoS) được sử dụng bởi Ethereum 2.0, nơi người xác thực được chọn dựa trên lượng tài sản mà họ nắm giữ và "đặt cọc" vào hệ thống.

### 2.1.3. Ứng dụng của Blockchain

Ban đầu, Blockchain được biết đến rộng rãi thông qua sự ra đời của Bitcoin, đóng vai trò là nền tảng cho một hệ thống tiền tệ phi tập trung. Tuy nhiên, theo thời gian, tiềm năng của công nghệ này đã vượt xa khỏi lĩnh vực tài chính, mở ra cánh cửa cho hàng loạt ứng dụng đột phá trong nhiều ngành công nghiệp khác nhau. Bản chất phi tập trung, bất biến, minh bạch và an toàn của Blockchain đã chứng minh khả năng giải quyết các vấn đề về lòng tin, hiệu quả và bảo mật dữ liệu trong nhiều lĩnh vực mà trước đây đòi hỏi sự can thiệp của các bên trung gian tốn kém và kém hiệu quả.



Dưới đây là một số ứng dụng nổi bật và tiềm năng của Blockchain:

#### Tài chính và Ngân hàng (FinTech)

Đây là lĩnh vực đầu tiên và rõ ràng nhất mà Blockchain tạo ra ảnh hưởng.

* **Tiền tệ mã hóa (Cryptocurrency):** Bitcoin, Ethereum và hàng ngàn loại tiền điện tử khác đã chứng minh khả năng tạo ra một hệ thống tiền tệ phi tập trung, không chịu sự kiểm soát của chính phủ hay ngân hàng trung ương. Các giao dịch được thực hiện trực tiếp giữa các bên, loại bỏ phí trung gian và đẩy nhanh tốc độ xử lý xuyên biên giới.
* **Thanh toán và Chuyển tiền xuyên biên giới:** Blockchain có thể cách mạng hóa các dịch vụ chuyển tiền quốc tế bằng cách giảm thiểu thời gian xử lý từ vài ngày xuống còn vài phút hoặc thậm chí vài giây, đồng thời cắt giảm đáng kể chi phí. Các dự án như Ripple (XRP) tập trung vào việc tạo ra các giải pháp thanh toán tức thời và chi phí thấp cho các tổ chức tài chính.
* **Cho vay và Vay mượn phi tập trung (DeFi Lending):** Các nền tảng tài chính phi tập trung (Decentralized Finance - DeFi) sử dụng Smart Contract để tự động hóa các khoản vay, cho vay và quản lý tài sản mà không cần đến ngân hàng. Người dùng có thể khóa tài sản kỹ thuật số của họ làm tài sản thế chấp và nhận các khoản vay bằng stablecoin hoặc các loại tiền điện tử khác.
* **Bảo hiểm:** Blockchain có thể tự động hóa quy trình bồi thường thông qua Smart Contract khi các điều kiện được thiết lập trước được đáp ứng (ví dụ: bồi thường tự động khi chuyến bay bị hủy). Điều này tăng cường tính minh bạch, giảm gian lận và tăng tốc độ xử lý yêu cầu.
* **Giao dịch chứng khoán và tài sản:** Blockchain có thể rút ngắn thời gian thanh toán các giao dịch chứng khoán từ T+2 hoặc T+3 xuống gần như tức thời, giảm rủi ro đối tác và tăng hiệu quả thị trường. Token hóa tài sản (asset tokenization) cho phép chia nhỏ quyền sở hữu các tài sản truyền thống như bất động sản, tác phẩm nghệ thuật thành các token kỹ thuật số, mở ra cơ hội đầu tư cho nhiều người hơn.

#### Chuỗi cung ứng và Logistics

Tính minh bạch và khả năng truy xuất nguồn gốc của Blockchain cực kỳ hữu ích trong việc quản lý chuỗi cung ứng phức tạp.

* **Truy xuất nguồn gốc sản phẩm:** Ghi lại mọi giai đoạn của sản phẩm từ nguyên liệu thô đến tay người tiêu dùng trên Blockchain, giúp xác định nguồn gốc sản phẩm, chống hàng giả và đảm bảo chất lượng. Ví dụ: IBM Food Trust sử dụng Blockchain để theo dõi thực phẩm từ nông trại đến bàn ăn.
* **Quản lý tồn kho và vận chuyển:** Cung cấp cái nhìn toàn diện, theo thời gian thực về vị trí và trạng thái của hàng hóa trong chuỗi cung ứng, giúp tối ưu hóa logistics và giảm thất thoát.
* **Minh bạch trong đạo đức sản xuất:** Xác minh các tuyên bố về lao động công bằng, nguồn gốc bền vững hoặc sản phẩm hữu cơ bằng cách ghi lại các chứng nhận trên chuỗi khối.

#### Quản lý danh tính số và Bảo mật dữ liệu

Blockchain có thể trao quyền kiểm soát dữ liệu cá nhân lại cho người dùng.

* **Danh tính tự chủ (Self-Sovereign Identity - SSI):** Cho phép cá nhân kiểm soát danh tính kỹ thuật số của mình, quyết định ai có thể truy cập dữ liệu nào và khi nào. Thay vì lưu trữ thông tin cá nhân trên các máy chủ tập trung dễ bị tấn công, thông tin được xác minh và lưu trữ một cách an toàn trên Blockchain.
* **Bảo mật hồ sơ y tế:** Lưu trữ hồ sơ bệnh án một cách an toàn và chỉ cho phép những người được ủy quyền truy cập, đồng thời vẫn đảm bảo tính riêng tư của bệnh nhân.
* **Quản lý quyền sở hữu trí tuệ:** Ghi nhận và xác minh quyền sở hữu tác phẩm nghệ thuật, âm nhạc, sáng chế, bảo vệ quyền của tác giả và người tạo nội dung.

#### Bầu cử và Quản trị phi tập trung (Decentralized Governance)

Đây là lĩnh vực liên quan trực tiếp đến đề tài của bạn.

* **Bầu cử điện tử:** Cung cấp một hệ thống bầu cử minh bạch, an toàn và chống gian lận. Mỗi phiếu bầu được ghi lại trên Blockchain, đảm bảo tính bất biến và có thể kiểm tra được. Điều này giúp tăng cường niềm tin vào kết quả bầu cử.
* **Quản trị DAO (Decentralized Autonomous Organization):** Blockchain, đặc biệt là thông qua Smart Contract, là xương sống của các tổ chức tự trị phi tập trung. Các quy tắc quản trị, quyết định về phát triển dự án, phân bổ quỹ, đều được mã hóa thành Smart Contract và thực thi thông qua biểu quyết của cộng đồng, mà không cần một ban điều hành trung tâm. Điều này dân chủ hóa quá trình ra quyết định.

#### Bất động sản và Đăng ký tài sản

* **Đăng ký quyền sở hữu:** Ghi lại quyền sở hữu đất đai, nhà cửa trên Blockchain, giúp đơn giản hóa quy trình chuyển nhượng, giảm chi phí và rủi ro gian lận. Các hợp đồng mua bán có thể được tự động hóa bằng Smart Contract.
* **Token hóa bất động sản:** Chia nhỏ quyền sở hữu bất động sản thành các token, cho phép các nhà đầu tư nhỏ tham gia vào thị trường bất động sản.

#### Năng lượng và Lưới điện thông minh

* **Giao dịch năng lượng ngang hàng (Peer-to-Peer Energy Trading):** Cho phép các hộ gia đình có năng lượng mặt trời dư thừa bán trực tiếp cho hàng xóm thông qua mạng lưới Blockchain, không cần qua các công ty điện lực truyền thống.
* **Theo dõi và xác minh năng lượng sạch:** Ghi lại lượng năng lượng tái tạo được sản xuất và tiêu thụ, giúp các công ty tuân thủ quy định và người tiêu dùng có thể lựa chọn nguồn năng lượng bền vững.

#### Giải trí và Trò chơi (Gaming)

* **Tài sản trong game (In-game Assets):** Người chơi có thể thực sự sở hữu các vật phẩm, nhân vật trong game dưới dạng NFT (Non-Fungible Token) trên Blockchain, cho phép họ mua bán, trao đổi hoặc sử dụng các tài sản này trên nhiều nền tảng game khác nhau.
* **Xác minh bản quyền và phân phối nội dung:** Giúp nghệ sĩ, nhạc sĩ có thể trực tiếp phân phối tác phẩm của mình và nhận tiền bản quyền minh bạch, không cần qua các bên trung gian.

#### Y tế và Chăm sóc sức khỏe

* **Quản lý dữ liệu bệnh nhân:** Blockchain có thể tạo ra một sổ cái an toàn và minh bạch cho hồ sơ sức khỏe bệnh nhân, giúp các nhà cung cấp dịch vụ y tế truy cập thông tin cần thiết một cách nhanh chóng và an toàn khi được ủy quyền.
* **Nghiên cứu lâm sàng:** Cải thiện tính toàn vẹn và minh bạch của dữ liệu trong các thử nghiệm lâm sàng, giảm gian lận và tăng tốc độ phát triển thuốc mới.

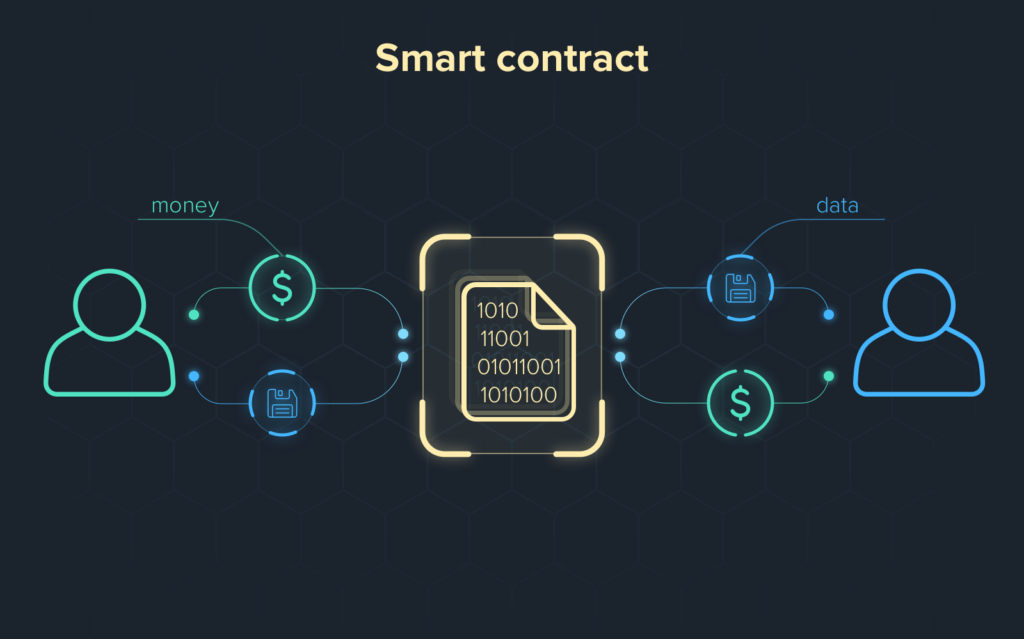
Nhìn chung, Blockchain đang mở ra một kỷ nguyên mới của sự tin cậy và hiệu quả trong thế giới kỹ thuật số. Từ việc định hình lại hệ thống tài chính toàn cầu đến việc tối ưu hóa chuỗi cung ứng, dân chủ hóa quản trị và trao quyền kiểm soát dữ liệu cho cá nhân, tiềm năng ứng dụng của công nghệ này vẫn đang tiếp tục được khám phá và mở rộng. Đây là một công nghệ nền tảng, có khả năng thay đổi cách chúng ta tương tác, giao dịch và tổ chức các hoạt động xã hội.

**2.2. Hợp đồng thông minh (Smart Contract)**

**2.2.1. Định nghĩa**

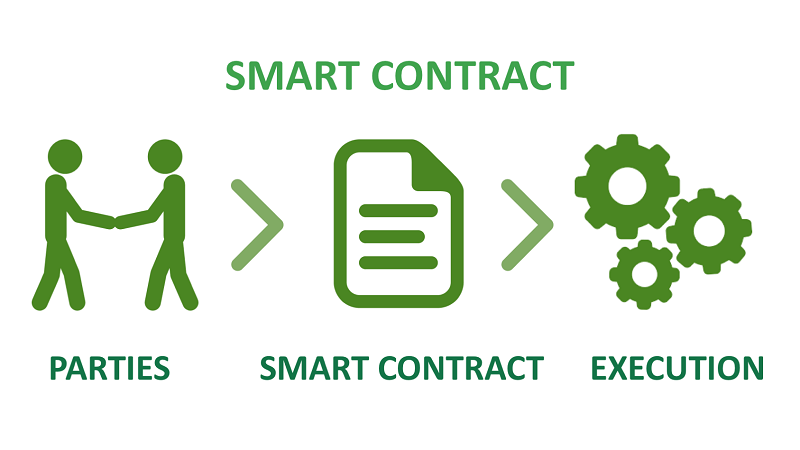
Hợp đồng thông minh (hay Smart Contract) là một ứng dụng phi tập trung nhằm xử lý các logic kinh doanh để đáp ứng tùy theo các sự kiện trên mạng lưới Blockchain. Việc thực hiện hợp đồng thông minh có thể bao gồm việc giao dịch tiền, cung cấp dịch vụ, mở khóa các nội dung được bảo vệ bởi quyền quản lý kỹ thuật số hoặc việc thay đổi các dữ liệu ví dụ như sang tên chủ sở hữu đất. Hợp đồng thông minh cũng có thể được sử dụng để bảo vệ quyền riêng tư, chẳng hạn như việc tạo điều kiện để công bố một vài dữ liệu cá nhân có chọn lọc để đáp ứng một số yêu cầu nhất định.

Các ứng dụng hợp đồng thông minh có nhiều kiến trúc nền tảng khác nhau về cách chúng được phát triển, phân phối, quản lý và cập nhật. Chúng có thể được lưu trữ như là một phần của một blockchain hoặc các công nghệ sổ cái phân tán (distributed ledger) khác. Chúng cũng được tích hợp vào nhiều phương thức thanh toán và trao đổi kỹ thuật số khác nhau có thể bao gồm cả bitcoin và các loại tiền ảo khác.



Mặc dù tên gọi là “thông minh”, tuy nhiên hợp đồng thông minh không phải là hợp đồng có ràng buộc về mặt pháp lý. Chức năng chính của chúng là xử lý các logic kinh doanh nhằm thực hiện các tác vụ, quy trình hoặc giao dịch khác nhau đã được lập trình sẵn để đáp ứng các điều kiện nhất định. Các bước về vấn đề pháp lý phải được thực hiện để liên kết việc xử lý hợp đồng thông minh này với các ràng buộc về pháp lý giữa các bên.

### 2.2.2. Quy trình hoạt động của hợp đồng thông minh



* Bước 1: Các bên tham gia giao kết smart contract bằng cách sử dụng chữ ký số để xác nhận danh tính và sự đồng ý của mình. Hợp đồng thông minh được viết bằng ngôn ngữ lập trình và được mã hóa chuyên biệt.
* Bước 2: Hợp đồng thông minh được tải lên blockchain và được phân phối, sao chép bằng các node trong mạng lưới. Mỗi node sẽ kiểm tra tính hợp lệ của hợp đồng và xác nhận nó vào một khối mới.
* Bước 3: Khi có lệnh triển khai, hợp đồng sẽ tự động thực thi đúng như các điều khoản đã lập trình. Một mạng máy tính sẽ thực hiện các hành động khi đáp ứng được điều kiện xác minh. Các hành động có thể là: chi trả tiền, đăng ký phương tiện, xuất hóa đơn, gửi thông báo…
* Bước 4: Sau khi hoàn thành các hành động, kết quả sẽ được ghi lại và cập nhật trên blockchain. Các bên có quyền truy cập có thể xem kết quả và không thể tự ý thay đổi giao dịch.

**2.2.3. Ngôn ngữ lập trình Solidity**

**Solidity** là ngôn ngữ lập trình chính được sử dụng để viết smart contract trên nền tảng Ethereum. Nó có cú pháp tương tự như JavaScript và hỗ trợ các tính năng như:

* Kiểu dữ liệu: uint, address, mapping, struct, v.v.
* Hàm: có thể là public, private, view, pure, payable.
* Sự kiện (Events): Gửi thông báo đến frontend.
* Modifier: Kiểm tra điều kiện trước khi chạy hàm.

## 2.3. Biểu quyết trên nền tảng Blockchain

### 2.3.1. Cơ chế hoạt động của một hệ thống e-voting trên Blockchain

Một hệ thống biểu quyết điện tử ứng dụng Blockchain được thiết kế để đảm bảo tính toàn vẹn và độ tin cậy của từng phiếu bầu. Cơ chế hoạt động cơ bản của nó có thể được mô tả qua các bước và thành phần chính sau:

* **Người dùng (cử tri) kết nối ví và bỏ phiếu:** Đây là điểm khởi đầu của mọi hoạt động biểu quyết. Người dùng, hay cử tri, sẽ tương tác với hệ thống thông qua một giao diện người dùng (ví dụ: một ứng dụng web). Để tham gia biểu quyết, họ cần có một **ví tiền mã hóa (cryptocurrency wallet)** được kết nối với mạng lưới blockchain tương ứng (ví dụ: MetaMask cho Ethereum). Ví này không chỉ là nơi lưu trữ tài sản số mà còn đóng vai trò là danh tính kỹ thuật số của người dùng trên blockchain. Khi người dùng muốn bỏ phiếu cho một lựa chọn nào đó, họ sẽ thực hiện một giao dịch từ ví của mình để gửi thông tin về phiếu bầu đến **Smart Contract** của cuộc biểu quyết. Giao dịch này thường đi kèm với một khoản phí nhỏ (gas fee) để được xử lý bởi mạng lưới.
* **Smart Contract lưu trữ kết quả và kiểm soát quyền vote:** Trung tâm của hệ thống e-voting trên blockchain chính là **Smart Contract (Hợp đồng thông minh)**. Đây là một đoạn mã tự thực thi được triển khai vĩnh viễn trên blockchain. Smart Contract chịu trách nhiệm chính trong việc:
  + **Lưu trữ kết quả biểu quyết:** Khi một phiếu bầu hợp lệ được gửi đến, Smart Contract sẽ ghi nhận và cập nhật số lượng phiếu cho từng lựa chọn. Dữ liệu này được lưu trữ trực tiếp trên blockchain.
  + **Kiểm soát quyền bỏ phiếu (Voting Eligibility):** Smart Contract được lập trình để xác định ai có quyền bỏ phiếu. Điều này có thể dựa trên nhiều tiêu chí như việc nắm giữ một lượng token nhất định, đã đăng ký trước, hoặc thỏa mãn các điều kiện khác. Quan trọng hơn, nó đảm bảo rằng chỉ những người đủ điều kiện mới có thể thực hiện giao dịch bỏ phiếu.
* **Mỗi ví chỉ được phép vote một lần:** Để chống lại việc bỏ phiếu lặp lại và đảm bảo tính công bằng, Smart Contract sẽ bao gồm một cơ chế kiểm tra chặt chẽ. Khi một ví gửi phiếu bầu, Smart Contract sẽ ghi lại địa chỉ ví đó và đánh dấu rằng nó đã bỏ phiếu. Nếu cùng một địa chỉ ví cố gắng bỏ phiếu lần thứ hai cho cùng một cuộc biểu quyết, giao dịch đó sẽ bị Smart Contract từ chối. Điều này dựa trên nguyên lý rằng mỗi địa chỉ ví là duy nhất và có thể được xác định công khai trên blockchain, tạo ra một sự ràng buộc hiệu quả.
* **Toàn bộ dữ liệu vote được ghi lại trên Blockchain và không thể thay đổi:** Đây là đặc tính cốt lõi mang lại sự tin cậy tuyệt đối cho hệ thống. Mọi giao dịch liên quan đến việc bỏ phiếu, từ khi phiếu bầu được gửi đi cho đến khi nó được Smart Contract xác nhận và ghi nhận, đều được ghi lại vĩnh viễn trên blockchain dưới dạng các khối dữ liệu. Nhờ vào tính chất **bất biến (immutability)** của blockchain, một khi dữ liệu đã được ghi vào một khối và khối đó đã được thêm vào chuỗi, nó **không thể bị thay đổi, xóa bỏ hay giả mạo** bởi bất kỳ ai, kể cả người tạo ra hệ thống. Điều này đảm bảo rằng kết quả biểu quyết là không thể bị can thiệp sau khi đã được xác nhận.

### 2.3.2. Lợi ích của biểu quyết trên nền tảng Blockchain

Việc ứng dụng Blockchain vào hệ thống biểu quyết mang lại nhiều lợi ích vượt trội so với các phương pháp truyền thống, giải quyết các vấn đề cố hữu về niềm tin, bảo mật và hiệu quả:

* **Minh bạch:** Blockchain cung cấp một mức độ minh bạch chưa từng có. Toàn bộ quá trình biểu quyết, từ việc thiết lập các lựa chọn, thời gian biểu quyết, đến từng phiếu bầu được gửi đi và tổng kết quả, đều **được ghi công khai và vĩnh viễn trên sổ cái phân tán**. Bất kỳ ai cũng có thể dễ dàng **kiểm tra và xác minh dữ liệu biểu quyết** thông qua các công cụ khám phá blockchain (blockchain explorer). Điều này loại bỏ mọi nghi ngờ về tính chính xác của kết quả, xây dựng niềm tin vững chắc trong cộng đồng người tham gia. Không có "hộp đen" nào giấu diếm thông tin, mọi thứ đều rõ ràng như pha lê.
* **Không thể gian lận:** Đây là một trong những lợi ích quan trọng nhất. Nhờ vào tính chất **bất biến và mã hóa mạnh mẽ** của Blockchain, **không ai, dù là người quản trị hệ thống, người tham gia hay thậm chí là một bên thứ ba độc hại, có thể sửa đổi phiếu bầu đã được ghi nhận hoặc thêm vào các phiếu bầu trái phép** sau khi chúng đã được đưa vào chuỗi. Mọi nỗ lực giả mạo sẽ ngay lập tức bị phát hiện do tính chất liên kết mật mã giữa các khối. Điều này cung cấp một hàng rào bảo mật cực kỳ vững chắc chống lại các hành vi gian lận bầu cử, vốn là nỗi lo thường trực trong các hệ thống truyền thống.
* **Tự động hóa:** Smart Contract đóng vai trò như một bộ máy xử lý tự động và không ngừng nghỉ. Toàn bộ **logic của quá trình biểu quyết – từ việc kiểm tra quyền bỏ phiếu, ghi nhận phiếu, đến tổng kết kết quả – đều được mã hóa và thực thi tự động bởi Smart Contract** mà không cần sự can thiệp của bất kỳ bên thứ ba hay nhân lực nào. Điều này loại bỏ hoàn toàn sự cần thiết của các bên trung gian tin cậy, vốn có thể là nguồn gốc của sai sót, thiên vị hoặc tham nhũng. Việc tự động hóa giúp giảm thiểu chi phí vận hành, tăng tốc độ xử lý và đảm bảo rằng các quy tắc biểu quyết được áp dụng một cách nhất quán và công bằng tuyệt đối.

# CHƯƠNG III: THỰC HIỆN VÀ TRIỂN KHAI

## 3.1. Mục đích xây dựng giao diện

Giao diện web là cầu nối giữa người dùng và hệ thống blockchain. Trong hệ thống biểu quyết điện tử, việc minh bạch hóa quá trình và kết quả bầu chọn là yếu tố cực kỳ quan trọng nhằm tạo niềm tin và đảm bảo tính công bằng. Giao diện được xây dựng nhằm phục vụ mục đích:

* Giúp người dùng dễ dàng truy xuất kết quả bầu chọn trên chuỗi khối.
* Thể hiện thông tin ứng viên và số phiếu một cách trực quan.
* Kết nối với ví điện tử (MetaMask) để tương tác với hợp đồng thông minh.
* Tăng cường trải nghiệm người dùng thông qua thiết kế đơn giản, rõ ràng.

## 3.2. Cấu trúc giao diện

Giao diện được xây dựng bằng các công nghệ web cơ bản:

* **HTML**: Khung hiển thị các thành phần (nút, bảng, tiêu đề).
* **CSS**: Tùy chỉnh kiểu hiển thị, tạo giao diện hiện đại, dễ nhìn.
* **JavaScript + Ethers.js**: Xử lý kết nối blockchain và tương tác với smart contract.

**CODE GIAO DIỆN**:

<!DOCTYPE html>

<html lang="en">

<head>

<meta charset="UTF-8">

<title>Kết quả bầu chọn</title>

<style>

body { font-family: sans-serif; padding: 20px; background: #f4f4f4; }

button { padding: 10px 20px; margin-bottom: 20px; }

table { width: 100%; border-collapse: collapse; background: white; }

th, td { border: 1px solid #ccc; padding: 10px; text-align: center; }

th { background: #e0e0e0; }

</style>

</head>

<body>

<h2>📊 KẾT QUẢ BẦU CHỌN TRỰC TIẾP TRÊN BLOCKCHAIN</h2>

<button onclick="connectAndLoad()">🔌 Kết nối & Xem kết quả</button>

<p id="status"></p>

<table id="resultsTable" style="display: none;">

<thead>

<tr><th>STT</th><th>Tên Ứng viên</th><th>Số phiếu</th></tr>

</thead>

<tbody id="resultsBody"></tbody>

</table>

<script src="https://cdn.jsdelivr.net/npm/ethers@5.7.2/dist/ethers.min.js"></script>

<script>

const contractAddress = "PASTE\_YOUR\_CONTRACT\_ADDRESS\_HERE"; // Dán địa chỉ ở đây

const abi = [ // Dán ABI của bạn ở đây (nếu là getCandidates thì dùng đoạn này)

{

"inputs": [],

"name": "getCandidates",

"outputs": [

{

"components": [

{ "internalType": "string", "name": "name", "type": "string" },

{ "internalType": "uint256", "name": "voteCount", "type": "uint256" }

],

"internalType": "struct VotingSystem.Candidate[]",

"name": "",

"type": "tuple[]"

}

],

"stateMutability": "view",

"type": "function"

}

];

async function connectAndLoad() {

try {

if (!window.ethereum) {

alert("Bạn cần cài MetaMask để sử dụng.");

return;

}

document.getElementById("status").innerText = "⏳ Đang kết nối...";

const provider = new ethers.providers.Web3Provider(window.ethereum);

await provider.send("eth\_requestAccounts", []);

const signer = provider.getSigner();

const contract = new ethers.Contract(contractAddress, abi, signer);

const candidates = await contract.getCandidates();

const tbody = document.getElementById("resultsBody");

tbody.innerHTML = "";

candidates.forEach((c, i) => {

const row = `<tr><td>${i + 1}</td><td>${c.name}</td><td>${c.voteCount}</td></tr>`;

tbody.innerHTML += row;

});

document.getElementById("resultsTable").style.display = "table";

document.getElementById("status").innerText = "✅ Dữ liệu đã được tải!";

} catch (err) {

document.getElementById("status").innerText = "❌ Lỗi: " + err.message;

console.error(err);

}

}

</script>

</body>

</html>

# Ngôn ngữ Solidity:

// SPDX-License-Identifier: MIT

pragma solidity ^0.8.0;

contract VotingSystem {

struct Candidate {

string name;

uint voteCount;

}

mapping(address => bool) public hasVoted;

Candidate[] public candidates;

constructor(string[] memory candidateNames) {

for (uint i = 0; i < candidateNames.length; i++) {

candidates.push(Candidate(candidateNames[i], 0));

}

}

function vote(uint candidateIndex) public {

require(!hasVoted[msg.sender], "Already voted!");

hasVoted[msg.sender] = true;

candidates[candidateIndex].voteCount++;

}

function getCandidates() public view returns (Candidate[] memory) {

return candidates;

}

}

**TÀI LIỆU THAM KHẢO**

1. TS. Trần Đăng Công – Bài giảng môn học Blockchain, Trường Đại học Đại Nam, Học kỳ II năm học 2024–2025.
2. Wood, G. (2014). Ethereum: A Secure Decentralised Generalised Transaction Ledger. Ethereum Project Yellow Paper.
3. Buterin, V. (2014). A Next-Generation Smart Contract and Decentralized Application Platform. [Online]. Available: https://ethereum.org/en/whitepaper/
4. Ethereum Foundation. (2023). Solidity Documentation. [Online]. Available: https://docs.soliditylang.org
5. Ethers.js Documentation. (2023). [Online]. Available: https://docs.ethers.org
6. MetaMask Documentation. (2023). [Online]. Available: https://docs.metamask.io
7. OpenZeppelin. (2023). OpenZeppelin Contracts. [Online]. Available: https://docs.openzeppelin.com/contracts
8. Nakamoto, S. (2008). Bitcoin: A Peer-to-Peer Electronic Cash System. [Online]. Available: https://bitcoin.org/bitcoin.pdfMozilla Developer Network. (2023). JavaScript Date and Time. [Online]. Available: <https://developer.mozilla.org>
9. Stack Overflow Community. (2023). Various Discussions on Solidity Time Management and Smart Contract Deployment. [Online]. Available: <https://stackoverflow.com>