

HỌC VIỆN CÔNG NGHỆ BƯU CHÍNH VIỄN THÔNG



BÁO CÁO BÀI TẬP LỚN
THỰC TẬP CƠ SỞ
ĐỀ TÀI:
Web3 Crowdfunding

Giảng viên hướng dẫn : Kim Ngọc Bách

Họ và tên sinh viên : Lê Đức Thiện

Mã sinh viên : B22DCCN823

HỌC KỲ 2 2024-2025

LỜI CẢM ƠN

Em xin chân thành cảm ơn thầy **Kim Ngọc Bách** – người đã tận tình hướng dẫn và định hướng quý báu trong suốt thời gian qua. Thầy đã cho tự do lựa chọn đề tài, nên em có thể thử sức với một công nghệ mới mà chưa từng biết trước đây. Vì vậy, trong thời gian 3 tháng nghiên cứu và học tập em đã học được rất nhiều kiến thức và kỹ năng mới.

Em kính chúc thầy luôn mạnh khỏe, hạnh phúc và tiếp tục thành công trong sự nghiệp giảng dạy và nghiên cứu ạ!

MỤC LỤC

LỜI CẢM ƠN.....	2
PHẦN 1: MỞ ĐẦU	5
1.1 Lý do chọn đề tài	5
1.2. Nội dung nghiên cứu	6
1.3. Ý nghĩa học tập và thực tiễn	7
PHẦN 2: CƠ SỞ LÝ THUYẾT	9
2.1. Tổng quan về Blockchain	9
2.1.1. Khái niệm về Blockchain.....	9
2.1.2. Cấu trúc của một khối (Block) và chuỗi khối (Blockchain).....	10
2.1.3. Cơ chế đồng thuận (Consensus Mechanism)	11
2.1.4. Ưu điểm của Blockchain.....	12
2.2. Hợp đồng thông minh (Smart Contracts)	13
2.2.1. Định nghĩa và cách hoạt động.....	13
2.2.2. Vai trò trong hệ thống Web3	14
2.2.3. So sánh với hợp đồng truyền thống.....	15
2.2.4. Công cụ và nền tảng phát triển.....	16
2.2.5. Hạn chế và thách thức	16
2.3. Web3 là gì?	17
2.3.1. Định nghĩa Web3.....	17
2.3.2. Đặc điểm nổi bật của Web3	18
2.3.3. Thành phần chính trong hệ sinh thái Web3.....	19
2.3.4. Lợi ích của Web3 trong Crowdfunding.....	19
2.3.5. Thách thức của Web3.....	20
2.4. Mô hình ứng dụng Web3 trong Crowdfunding	20
2.4.1. Khái niệm về Crowdfunding.....	20
2.4.2. Hạn chế của Crowdfunding truyền thống	21

2.4.3. Giải pháp Web3 cho Crowdfunding	21
2.4.4. Sơ đồ mô hình hệ thống Web3 Crowdfunding.....	22
2.4.5. Ưu điểm của Web3 Crowdfunding	22
2.4.6. Hạn chế và thách thức	23
PHẦN 3: PHÂN TÍCH VÀ TRIỂN KHAI HỆ THỐNG	24
3.1. Kiến trúc tổng quan hệ thống	24
3.2. Tính năng chính của hệ thống	25
3.3. Quy trình hoạt động của chiến dịch.....	29
3.4. Công nghệ sử dụng.....	30
3.5. Kết quả kiểm thử.....	31
3.5.1. Các kịch bản kiểm thử.....	31
3.5.2. Tổng hợp kết quả kiểm thử.....	36
3.5.3. Nhận xét về hiệu suất.....	37
3.6. Thiết kế giao diện người dùng (UI/UX)	38
3.6.1. Các thành phần giao diện chính	38
3.6.2. Hạn chế và đề xuất cải tiến	42
TÀI LIỆU THAM KHẢO	43

PHẦN 1: MỞ ĐẦU

1.1 Lý do chọn đề tài

Trong thời đại công nghệ số phát triển mạnh mẽ, các mô hình gọi vốn cộng đồng (crowdfunding) đã và đang đóng vai trò quan trọng trong việc hỗ trợ các cá nhân, tổ chức và startup hiện thực hóa những ý tưởng sáng tạo. Tuy nhiên, các nền tảng crowdfunding truyền thống hiện nay vẫn tồn tại nhiều hạn chế như thiếu minh bạch, phụ thuộc vào bên thứ ba trung gian, chi phí giao dịch cao, rủi ro gian lận và giới hạn tiếp cận người dùng toàn cầu. Những yếu tố này đã đặt ra nhu cầu cần một giải pháp đổi mới, minh bạch và hiệu quả hơn.

Sự ra đời của công nghệ Blockchain và sự phát triển của Web3 đã mở ra cơ hội để tái định hình cách thức thực hiện các chiến dịch gọi vốn cộng đồng. Web3 không chỉ mang đến một môi trường phi tập trung (decentralized) mà còn đảm bảo tính minh bạch, không thể thay đổi dữ liệu (immutability) và tính bảo mật cao nhờ các hợp đồng thông minh (smart contracts). Với những ưu điểm đó, mô hình **Web3 Crowdfunding** – tức gọi vốn cộng đồng dựa trên nền tảng Blockchain – đang nổi lên như một xu hướng tất yếu và hứa hẹn sẽ thay thế các nền tảng truyền thống trong tương lai gần.

Từ góc độ sinh viên ngành Công nghệ Thông tin, việc nghiên cứu và triển khai một dự án ứng dụng công nghệ Blockchain vào mô hình gọi vốn cộng đồng là một cơ hội quý giá để tìm hiểu sâu hơn về những công nghệ tiên tiến như hợp đồng thông minh (smart contract), mạng Ethereum, ví phi tập trung (crypto wallets). Đây không chỉ là một đề tài giàu tính thời sự mà còn mang tính thực tiễn cao, phù hợp với định hướng phát triển công nghệ hiện đại trên thế giới và cả tại Việt Nam.

Chính vì những lý do trên, em đã lựa chọn đề tài **“Web3 Crowdfunding”** để làm bài tập lớn. Thông qua đề tài này, em mong muốn được áp dụng lý thuyết vào thực tiễn, tiếp cận với công nghệ mới và góp phần hiểu rõ hơn tiềm năng ứng dụng của Blockchain trong đời sống hiện đại.

1.2. Nội dung nghiên cứu

Đề tài hướng tới việc xây dựng một hệ thống gọi vốn cộng đồng sử dụng công nghệ Web3, dựa trên nền tảng Blockchain. Nội dung nghiên cứu chính được chia thành các phần như sau:

- Tìm hiểu tổng quan về mô hình Crowdfunding và các nền tảng truyền thống hiện nay như Kickstarter, GoFundMe, IndieGoGo... Đồng thời, phân tích những ưu điểm và hạn chế của các nền tảng này.
- Nghiên cứu công nghệ Blockchain và Web3, tập trung vào các khái niệm cốt lõi như:
 - Hợp đồng thông minh (Smart Contracts)
 - Giao dịch phi tập trung
 - Mạng thử nghiệm Ethereum (Sepolia...)
 - Ví phi tập trung như MetaMask
- Phân tích, thiết kế và triển khai hệ thống Web3 Crowdfunding, trong đó bao gồm:
 - Giao diện người dùng (UI/UX) thân thiện, được xây dựng bằng các công nghệ như React.js, TailwindCSS.
 - Hợp đồng thông minh được viết bằng Solidity, triển khai và kiểm thử trên mạng thử nghiệm.
 - Kết nối giao diện Web2 với hợp đồng Web3 thông qua thư viện ethers.js hoặc web3.js.

- Chức năng chính bao gồm: tạo dự án gọi vốn, đóng góp vào dự án, theo dõi tiến độ gây quỹ, rút vốn sau khi thành công, hoàn tiền nếu không đạt mục tiêu...
- Kiểm thử và đánh giá hệ thống, so sánh ưu nhược điểm giữa mô hình Web3 với mô hình truyền thống, từ đó rút ra nhận định về tính khả thi của giải pháp.

Toàn bộ quá trình phát triển sản phẩm đều tuân thủ nguyên tắc minh bạch, bảo mật và đảm bảo tính dễ sử dụng cho người dùng phổ thông. Bên cạnh đó, em cũng sẽ khảo sát các rào cản hiện tại của Web3 đối với người dùng không chuyên và đề xuất hướng cải tiến để nâng cao trải nghiệm người dùng.

1.3. Ý nghĩa học tập và thực tiễn

Đề tài "Web3 Crowdfunding" không chỉ có ý nghĩa trong phạm vi học thuật mà còn mang lại nhiều giá trị thực tiễn, cụ thể như sau:

- **Về mặt kiến thức chuyên môn**, đề tài giúp sinh viên tiếp cận và hiểu sâu hơn về các công nghệ cốt lõi của Blockchain và Web3 như: hợp đồng thông minh, cơ chế phân quyền, quản lý tài sản số và ứng dụng thực tế của các mô hình phi tập trung. Đây là nền tảng vững chắc cho các nghiên cứu và dự án cao cấp hơn trong tương lai.
- **Về kỹ năng thực hành**, sinh viên được rèn luyện khả năng phân tích, thiết kế hệ thống, viết và triển khai hợp đồng thông minh, phát triển frontend/backend, quản lý dự án, kỹ năng kiểm thử và trình bày sản phẩm. Qua đó, nâng cao năng lực làm việc và khả năng tư duy giải quyết vấn đề thực tế.
- **Về mặt ứng dụng thực tiễn**, hệ thống có thể được mở rộng và áp dụng trong các lĩnh vực như từ thiện, phát triển cộng đồng, hỗ trợ startup gọi vốn, hay thậm chí là vận hành mô hình DAO để cộng đồng cùng quản lý và ra quyết

định. Trong bối cảnh chuyển đổi số đang diễn ra mạnh mẽ, những mô hình dựa trên Blockchain sẽ ngày càng phát huy vai trò quan trọng.

- **Về mặt định hướng nghề nghiệp**, việc làm chủ được công nghệ Web3 và Blockchain giúp sinh viên có nhiều lợi thế khi tham gia vào thị trường lao động, nhất là trong các lĩnh vực đang phát triển như fintech, DeFi (tài chính phi tập trung), NFT, và các hệ thống tài sản số.

Qua việc thực hiện đề tài này, em không chỉ mong muốn xây dựng một sản phẩm hoàn chỉnh mà còn xem đây là một bước đi vững chắc để tiếp cận với xu hướng công nghệ tương lai. Đồng thời, đây cũng là dịp để nâng cao tinh thần nghiên cứu khoa học, chủ động tiếp cận cái mới, góp phần tích cực vào quá trình học tập và phát triển bản thân.

Ý nghĩa học tập của đề tài nằm ở việc giúp sinh viên củng cố kiến thức về công nghệ blockchain và Web3, nâng cao tư duy hệ thống, cũng như chuẩn bị nền tảng cho việc nghiên cứu và triển khai các dự án công nghệ trong tương lai.

PHẦN 2: CƠ SỞ LÝ THUYẾT

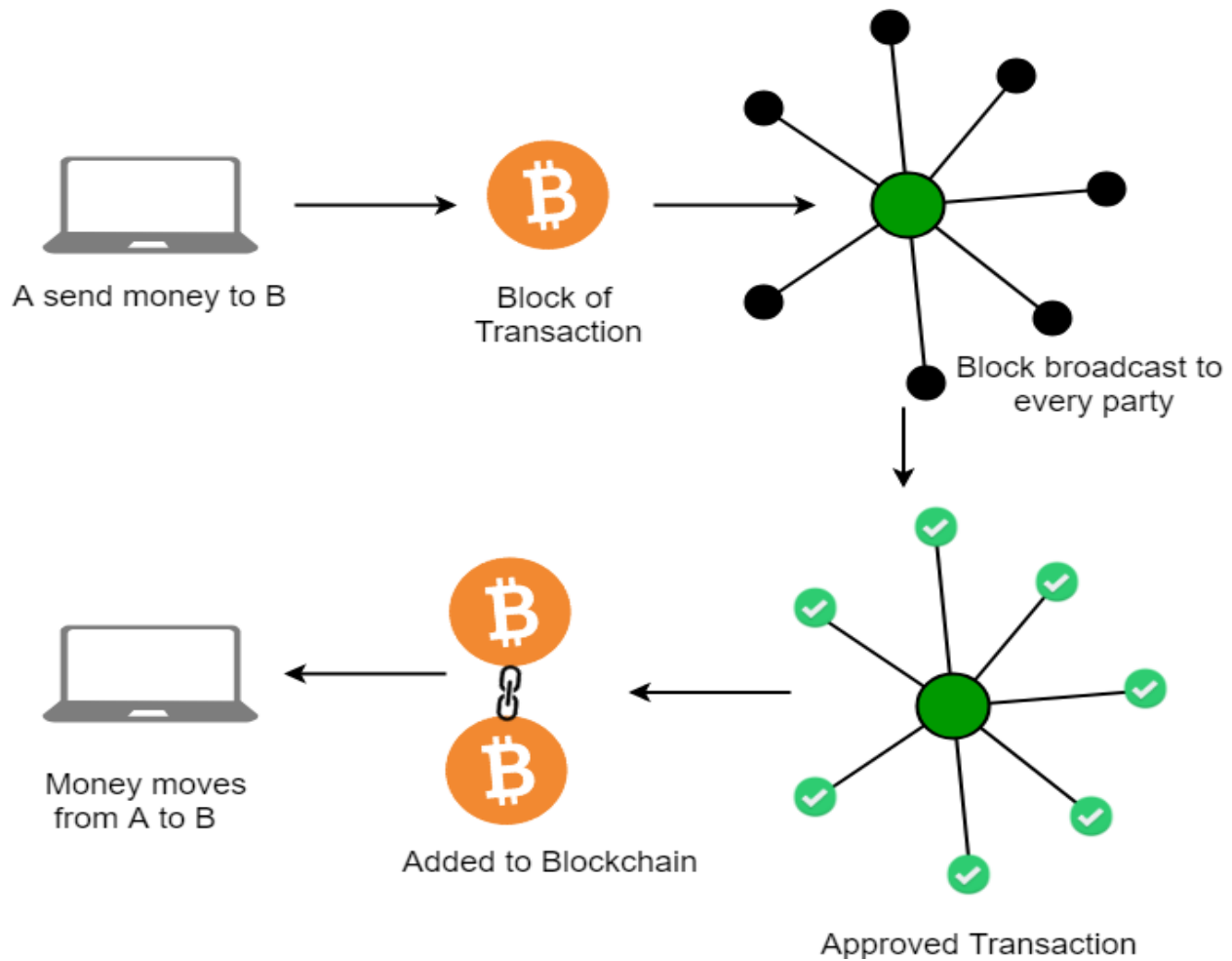
2.1. Tổng quan về Blockchain

2.1.1. Khái niệm về Blockchain

Blockchain (chuỗi khối) là một công nghệ lưu trữ và truyền tải dữ liệu dạng khối (block), trong đó các khối dữ liệu được liên kết với nhau theo thứ tự thời gian và được bảo mật bằng các kỹ thuật mã hóa. Mỗi khối chứa thông tin về các giao dịch, một mã băm (hash) của chính nó và mã băm của khối trước đó, tạo nên một chuỗi liên tục.

Đặc điểm nổi bật của Blockchain là tính **phi tập trung**: không có máy chủ trung tâm quản lý, mà toàn bộ dữ liệu được ghi lại, xác nhận và đồng bộ trên nhiều nút (node) trong mạng lưới. Nhờ vậy, Blockchain mang lại tính minh bạch, không thể sửa đổi và khả năng hoạt động mà không cần sự tin tưởng vào bên trung gian.

Ban đầu được biết đến rộng rãi thông qua ứng dụng tiền điện tử Bitcoin, ngày nay Blockchain đã được ứng dụng trong nhiều lĩnh vực như tài chính, chuỗi cung ứng, y tế, bất động sản, và đặc biệt là các hệ thống Web3 như nền tảng gọi vốn cộng đồng (crowdfunding).



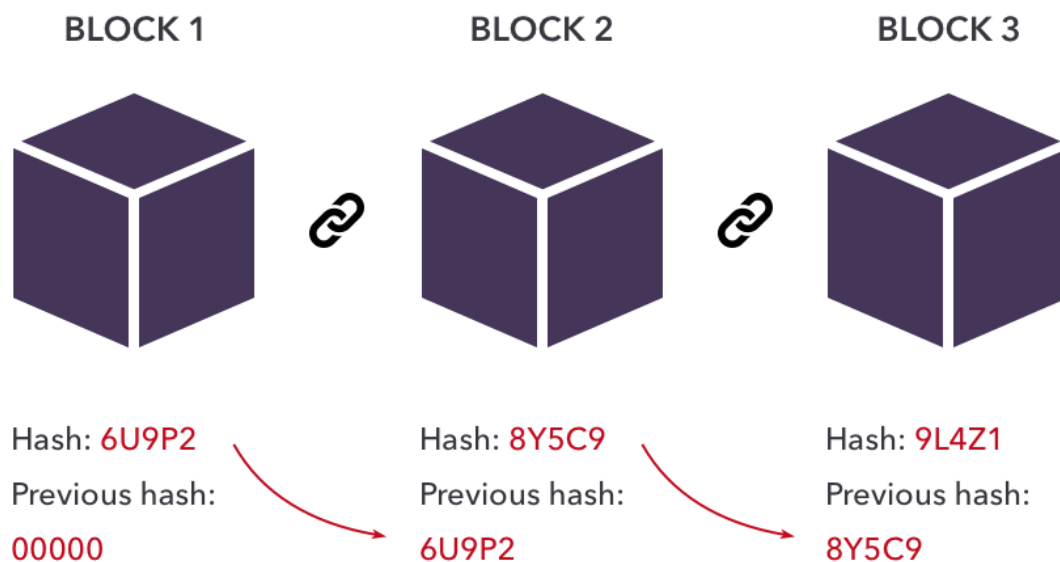
Hình 1: Mô hình hoạt động của Bitcoin

2.1.2. Cấu trúc của một khối (Block) và chuỗi khối (Blockchain)

Mỗi **khối (block)** trong chuỗi Blockchain thường bao gồm 3 thành phần chính:

- **Dữ liệu (Data):** Đây là nội dung chính của khối, thường là các giao dịch hoặc thông tin liên quan đến các sự kiện cụ thể.
- **Mã băm của khối hiện tại (Current Hash):** Là giá trị duy nhất được tạo ra bằng thuật toán mã hóa (thường là SHA-256), đại diện cho toàn bộ nội dung của khối.

- **Mã băm của khối trước (Previous Hash):** Giúp liên kết khối hiện tại với khối trước đó, tạo thành chuỗi liên tục. Bất kỳ thay đổi nào trong khối trước sẽ làm thay đổi toàn bộ chuỗi sau nó.



Hình 2: Cấu trúc khối của Blockchain

Blockchain là tập hợp các khối được nối với nhau theo trình tự thời gian, trong đó mỗi khối đều chứa mã băm của khối trước. Chính mối liên kết này khiến cho việc thay đổi dữ liệu trở nên cực kỳ khó khăn nếu không có sự đồng thuận từ phần lớn các nút trong mạng.

2.1.3. Cơ chế đồng thuận (Consensus Mechanism)

Trong môi trường phi tập trung, các nút trong mạng cần một cách để đồng ý với nhau về trạng thái của hệ thống. Cơ chế đồng thuận là giải pháp đảm bảo rằng tất cả các nút trong mạng Blockchain đều ghi nhận và xác thực thông tin một cách thống nhất.

Một số cơ chế đồng thuận phổ biến:

- **Proof of Work (PoW):**
 - Được sử dụng trong Bitcoin.
 - Yêu cầu các nút giải các bài toán tính toán phức tạp để tạo ra khối mới.
 - Ưu điểm: bảo mật cao, khó tấn công.
 - Nhược điểm: tiêu tốn nhiều năng lượng.
- **Proof of Stake (PoS):**
 - Được sử dụng trong Ethereum 2.0 và nhiều mạng khác.
 - Các nút không cần giải bài toán mà phải đặt cọc (stake) tài sản để có quyền xác thực khối.
 - Ưu điểm: tiết kiệm năng lượng, hiệu quả hơn PoW.
 - Có nhiều biến thể như Delegated PoS (DPoS), Leased PoS (LPoS), v.v.
- **Các cơ chế khác:** Practical Byzantine Fault Tolerance (PBFT), Proof of Authority (PoA), Proof of History (PoH)...

Việc lựa chọn cơ chế đồng thuận phù hợp ảnh hưởng trực tiếp đến khả năng mở rộng, hiệu suất và tính bảo mật của mạng Blockchain.

2.1.4. Ưu điểm của Blockchain

Blockchain sở hữu nhiều ưu điểm vượt trội so với các hệ thống truyền thống:

- **Tính minh bạch (Transparency):** Mọi giao dịch đều được ghi lại và công khai trên mạng lưới, bất kỳ ai cũng có thể kiểm tra và xác minh.
- **Không thể sửa đổi (Immutability):** Khi dữ liệu đã được ghi vào một khối và khối đó được thêm vào chuỗi, gần như không thể thay đổi thông tin đó nếu không có sự đồng thuận từ phần lớn mạng lưới.
- **Phi tập trung (Decentralization):** Không có một tổ chức hay cá nhân nào kiểm soát toàn bộ hệ thống, loại bỏ sự phụ thuộc vào bên trung gian.

- **Tăng cường bảo mật (Security):** Mã hóa và cấu trúc liên kết giữa các khối giúp ngăn chặn các hành vi giả mạo hoặc tấn công.
- **Tự động hóa (Automation):** Khi kết hợp với hợp đồng thông minh, các quy trình có thể được thực hiện tự động mà không cần sự can thiệp thủ công.

2.2. Hợp đồng thông minh (Smart Contracts)

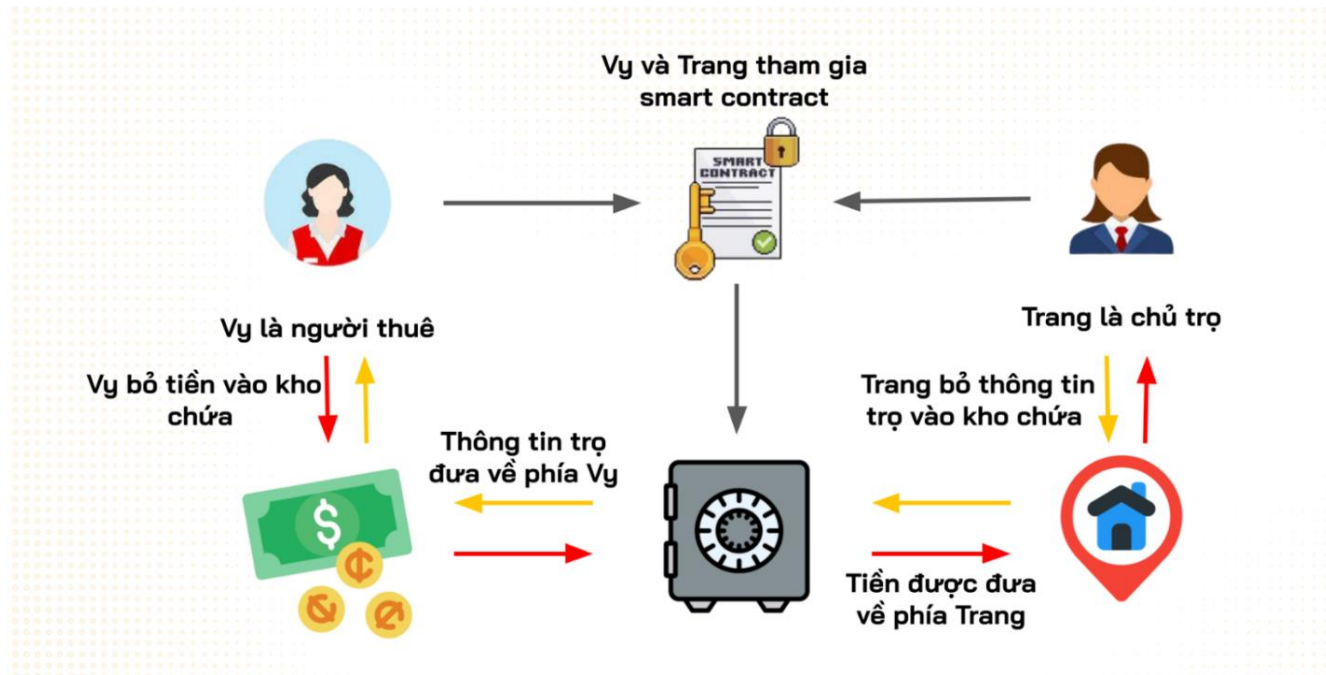
2.2.1. Định nghĩa và cách hoạt động

Hợp đồng thông minh (Smart Contract) là một đoạn mã được triển khai trên nền tảng blockchain, có khả năng tự động thực hiện các điều khoản đã lập trình sẵn khi các điều kiện được thỏa mãn. Nói cách khác, smart contract là “hợp đồng số” chạy trên blockchain, hoạt động mà không cần đến sự can thiệp của bên trung gian hay cơ quan quản lý.

Smart contract được tạo ra bằng ngôn ngữ lập trình chuyên biệt (phổ biến nhất là **Solidity** trên Ethereum), sau đó được triển khai lên blockchain thông qua một giao dịch. Sau khi triển khai, mã của smart contract là bất biến và có thể được gọi bởi người dùng hoặc các ứng dụng phi tập trung (dApps).

Ví dụ đơn giản về Smart Contract:

Một hợp đồng thông minh có thể quy định rằng: “Trong quá trình thuê trọ giữa Vy và Trang, cả hai bên tham gia vào một hợp đồng thông minh, đóng vai trò là trung gian tự động và minh bạch. Trang cung cấp thông tin trọ vào kho chứa của hợp đồng, còn Vy nạp tiền thuê vào đó. Smart contract giữ cả tiền và thông tin cho đến khi điều kiện được đáp ứng. Khi đúng điều kiện như thời gian thuê bắt đầu, hợp đồng tự động giải phóng tiền cho Trang và gửi thông tin trọ cho Vy, đảm bảo an toàn, không cần bên thứ ba.” Quy tắc này sẽ được mã hóa thành code, không thể thay đổi, và tự động thực hiện mà không cần người giám sát.



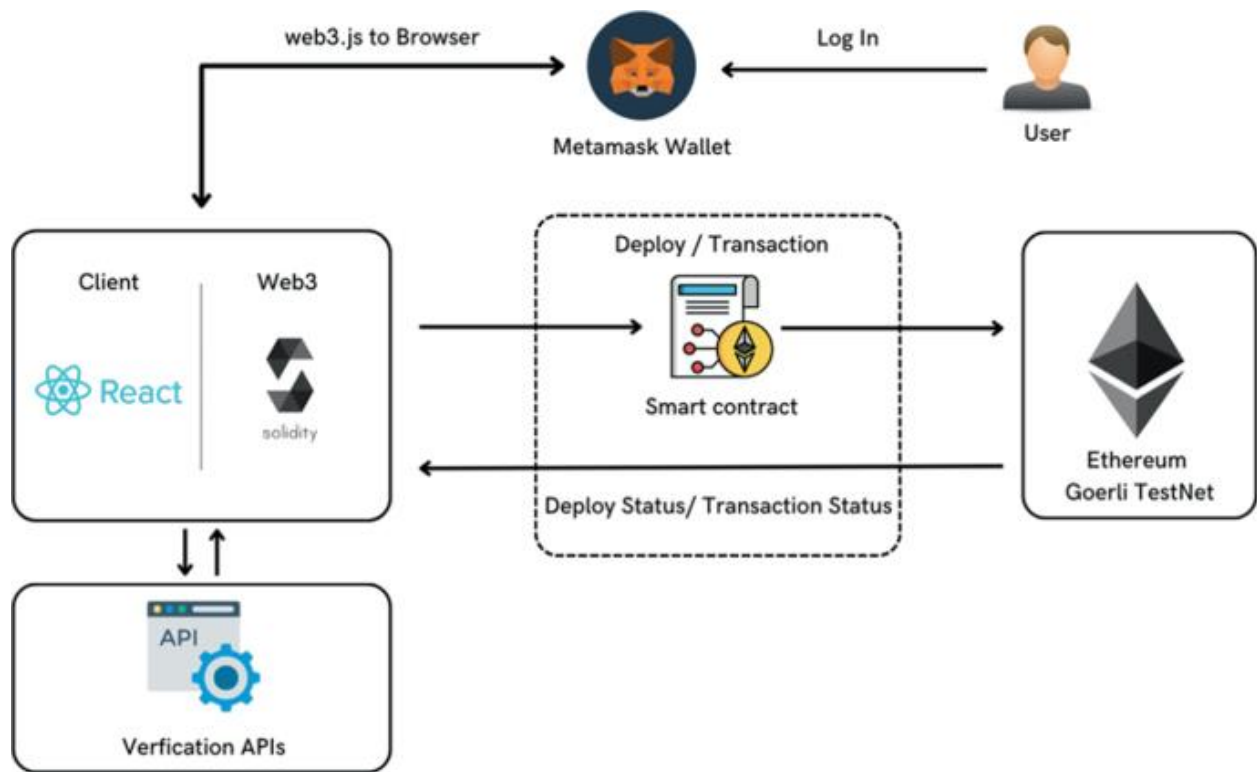
Hình 3: Ứng dụng Smart Contract trong thuê nhà

2.2.2. Vai trò trong hệ thống Web3

Smart contract đóng vai trò **cốt lõi** trong các ứng dụng Web3. Trong bối cảnh của một nền tảng gọi vốn cộng đồng (Web3 Crowdfunding), hợp đồng thông minh có thể đảm nhiệm những chức năng sau:

- **Tạo chiến dịch kêu gọi vốn** với các thông tin: tên dự án, mục tiêu vốn, thời hạn.
- **Tự động thu nhận đóng góp (donations)** từ người dùng, ghi nhận số tiền và địa chỉ ví tương ứng.
- **Phân phối vốn** hoặc **hoàn trả** nếu dự án không đạt được mục tiêu tài chính trong thời hạn.
- **Theo dõi tiến độ** và kích hoạt các đợt giải ngân vốn theo giai đoạn.

Nhờ tính minh bạch và bất biến của smart contract, người dùng có thể hoàn toàn tin tưởng rằng quy trình gây quỹ được thực hiện công bằng và đúng theo cam kết.



Hình 4: Mô hình hoạt động của hệ thống Web3

2.2.3. So sánh với hợp đồng truyền thống

Tiêu chí	Hợp đồng truyền thống	Hợp đồng thông minh
Hình thức	Văn bản giấy hoặc điện tử	Mã lập trình chạy trên blockchain
Bên trung gian	Cần (luật sư, ngân hàng, chính phủ)	Không cần
Thực thi	Bằng pháp luật, có thể mất thời gian	Tự động, nhanh chóng khi đủ điều kiện

Chi phí	Có thể cao (phí luật sư, công chứng)	Thấp hơn nhiều
Tính minh bạch	Khó kiểm tra nếu không có quyền truy cập	Công khai trên blockchain
Tính bất biến	Có thể sửa đổi hoặc giả mạo	Không thể sửa đổi sau khi triển khai

Bảng 1: So sánh giữa hợp đồng thông minh và hợp đồng truyền thống

2.2.4. Công cụ và nền tảng phát triển

Hiện nay, có nhiều công cụ hỗ trợ lập trình và triển khai smart contract, phổ biến nhất là trên nền tảng Ethereum. Một số công cụ tiêu biểu gồm:

- **Ngôn ngữ lập trình Solidity:** Ngôn ngữ phổ biến nhất để viết hợp đồng thông minh trên Ethereum.
- **Remix IDE:** Môi trường lập trình trực tuyến hỗ trợ viết, biên dịch và thử nghiệm smart contract.
- **Hardhat / Truffle:** Framework mạnh mẽ dùng để phát triển, kiểm thử, triển khai và quản lý smart contract.
- **MetaMask:** Ví phi tập trung dùng để tương tác với các dApp và smart contract.
- **Sepolia Testnet / Goerli Testnet:** Mạng thử nghiệm miễn phí cho lập trình viên kiểm thử hợp đồng mà không cần sử dụng ETH thật.

2.2.5. Hạn chế và thách thức

Dù sở hữu nhiều ưu điểm, hợp đồng thông minh vẫn còn tồn tại một số thách thức:

- **Không thể chỉnh sửa:** Nếu mã hợp đồng có lỗi, không thể sửa đổi, phải triển khai lại hợp đồng mới.

- **Bảo mật:** Các lỗ hổng bảo mật có thể bị khai thác, gây thiệt hại lớn (như vụ DAO Hack 2016).
- **Khó tiếp cận với người không chuyên:** Người dùng phổ thông cần có giao diện thân thiện để tương tác với hợp đồng.
- **Vấn đề pháp lý:** Nhiều quốc gia chưa có khung pháp lý rõ ràng về tính ràng buộc của hợp đồng thông minh.

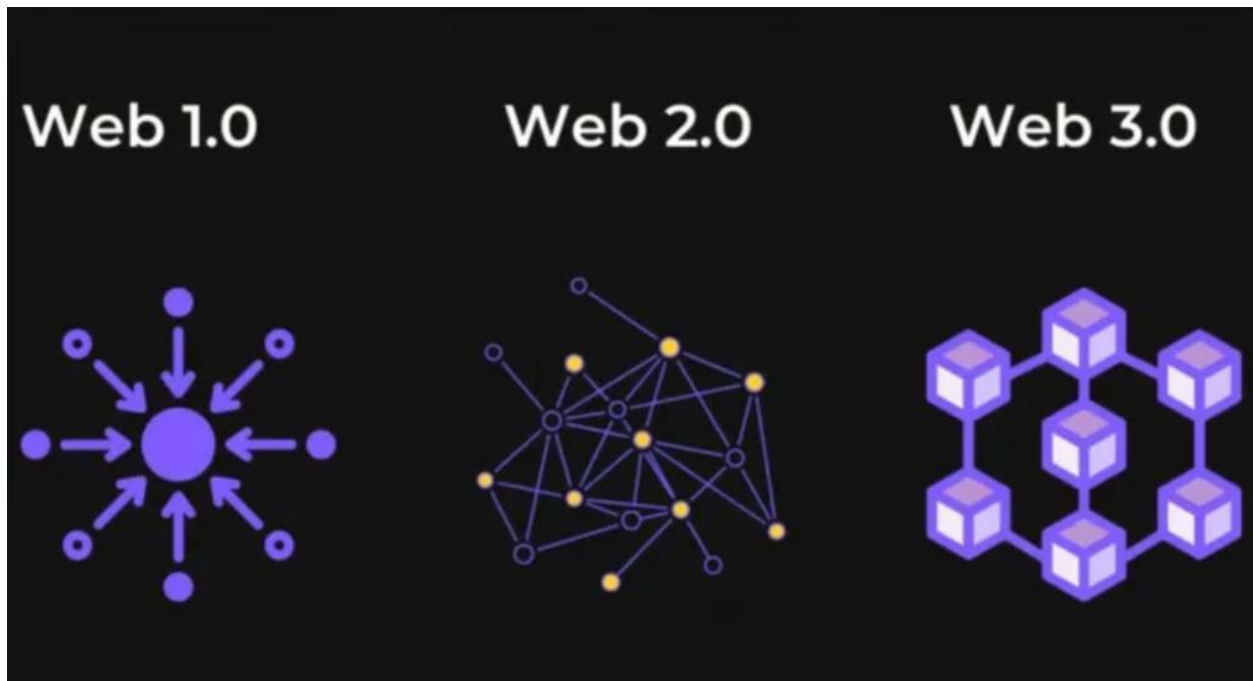
2.3. Web3 là gì?

2.3.1. Định nghĩa Web3

Web3 (Web 3.0) là thế hệ tiếp theo của Internet, nơi dữ liệu và quyền kiểm soát không còn tập trung vào các công ty công nghệ lớn (Big Tech) mà được phân phối và kiểm soát bởi người dùng thông qua các công nghệ như **Blockchain**, **hợp đồng thông minh** và **tài sản kỹ thuật số**. Web3 cho phép tạo ra các ứng dụng phi tập trung (**dApps**) mà người dùng có thể tương tác một cách tự chủ, minh bạch và bảo mật mà không cần đến bên trung gian.

Nếu ta xem sự phát triển của web theo từng giai đoạn:

- **Web 1.0:** Web tĩnh – người dùng chỉ đọc nội dung (read-only).
- **Web 2.0:** Web tương tác – người dùng vừa đọc vừa tạo nội dung (read-write), nhưng dữ liệu do các nền tảng trung gian kiểm soát (Facebook, Google...).
- **Web 3.0:** Web phi tập trung – người dùng đọc, viết và sở hữu dữ liệu (read-write-own) nhờ vào các công nghệ Blockchain.



Hình 5: Mô hình hoạt động của website trong 3 thời kỳ 1.0, 2.0 và tương lai là 3.0

2.3.2. Đặc điểm nổi bật của Web3

- **Phi tập trung (Decentralized):** Không có máy chủ trung tâm, dữ liệu và quyền kiểm soát được phân phối qua nhiều nút mạng (nodes).
- **Sở hữu dữ liệu cá nhân:** Người dùng có thể kiểm soát ví (wallet), tài sản kỹ thuật số và dữ liệu cá nhân mà không phụ thuộc vào các công ty trung gian.
- **Tương tác ngang hàng (Peer-to-Peer):** Giao dịch trực tiếp giữa người dùng mà không cần trung gian như ngân hàng, sàn thương mại điện tử...
- **Minh bạch:** Mọi hoạt động của ứng dụng đều có thể được kiểm chứng công khai trên blockchain.
- **Tích hợp tài sản kỹ thuật số:** Ví dụ: token, NFT (non-fungible token), stablecoin, đóng vai trò như phần thưởng, phương tiện thanh toán hoặc quyền biểu quyết.

- **Tự động hóa với Smart Contracts:** Giao dịch và logic kinh doanh được tự động hóa qua các hợp đồng thông minh.

2.3.3. Thành phần chính trong hệ sinh thái Web3

- **Blockchain:** Nền tảng cơ sở dữ liệu phi tập trung, lưu trữ giao dịch và smart contract.
- **Smart Contracts:** Tự động hóa logic ứng dụng và giao dịch.
- **Wallet (Ví phi tập trung):** Dùng để lưu trữ tài sản và nhận dạng người dùng (VD: MetaMask, Trust Wallet).
- **Token & NFT:** Tài sản kỹ thuật số đại diện cho giá trị, quyền sở hữu hoặc quyền truy cập.
- **DApps:** Ứng dụng phi tập trung hoạt động trên blockchain, như Uniswap, OpenSea, hoặc nền tảng gọi vốn cộng đồng Web3.

2.3.4. Lợi ích của Web3 trong Crowdfunding

Web3 đặc biệt phù hợp với các nền tảng gọi vốn cộng đồng vì các lý do sau:

Lợi ích	Mô tả
Minh bạch	Mọi dòng tiền đóng góp và phân phối đều được ghi lại công khai trên blockchain.
Tin cậy và không cần trung gian	Người dùng đóng góp trực tiếp vào smart contract, không qua ngân hàng hay đơn vị quản lý.
Chi phí thấp hơn	Không mất phí cho trung gian tài chính hoặc nền tảng lưu trữ dữ liệu.
Khả năng tự động hoàn trả	Nếu không đạt mục tiêu, hệ thống có thể tự động hoàn lại tiền cho người ủng hộ.

Phân quyền và biểu quyết	Người đóng góp có thể sở hữu token để tham gia quyết định hướng phát triển dự án.
Minh bạch	Mọi dòng tiền đóng góp và phân phối đều được ghi lại công khai trên blockchain.

Bảng 2: Lợi ích của Web3 trong Crowdfunding

2.3.5. Thách thức của Web3

Mặc dù đầy tiềm năng, Web3 vẫn đối mặt với nhiều thách thức:

- **Khả năng mở rộng:** Hiệu suất và tốc độ xử lý còn hạn chế so với hệ thống tập trung.
- **Trải nghiệm người dùng chưa thân thiện:** Người mới khó tiếp cận vì cần hiểu ví điện tử, seed phrase, gas fee,...
- **Rủi ro bảo mật:** Người dùng tự giữ ví, nếu mất private key sẽ mất quyền truy cập tài sản vĩnh viễn.
- **Thiếu khung pháp lý rõ ràng:** Nhiều quốc gia vẫn đang trong giai đoạn hoàn thiện chính sách về blockchain và tài sản số.

2.4. Mô hình ứng dụng Web3 trong Crowdfunding

2.4.1. Khái niệm về Crowdfunding

Crowdfunding (gọi vốn cộng đồng) là hình thức huy động vốn từ nhiều cá nhân thông qua các nền tảng trực tuyến, thay vì chỉ dựa vào nhà đầu tư lớn hoặc tổ chức tài chính. Những người tham gia có thể đóng góp số tiền nhỏ để hỗ trợ một dự án, sản phẩm hoặc sáng kiến mà họ tin tưởng.

Các mô hình crowdfunding phổ biến gồm:

- **Donation-based:** Người đóng góp không mong muốn lợi ích tài chính.

- **Reward-based:** Người đóng góp nhận phần thưởng (ví dụ: sản phẩm).
- **Equity-based:** Người đóng góp nhận cổ phần hoặc quyền sở hữu.
- **Debt-based:** Người đóng góp cho vay với kỳ vọng được hoàn trả.

2.4.2. Hạn chế của Crowdfunding truyền thống

Vấn đề	Mô tả
Thiếu minh bạch	Người dùng không thể theo dõi chính xác dòng tiền sau khi đóng góp.
Phụ thuộc bên trung gian	Các nền tảng như Kickstarter, GoFundMe thu phí cao và kiểm soát dòng vốn.
Thiếu niềm tin	Dự án có thể thất bại hoặc không thực hiện đúng cam kết sau khi nhận vốn.
Khó tiếp cận toàn cầu	Giới hạn về khu vực địa lý, pháp lý, và phương thức thanh toán.
Thiếu minh bạch	Người dùng không thể theo dõi chính xác dòng tiền sau khi đóng góp.
Phụ thuộc bên trung gian	Các nền tảng như Kickstarter, GoFundMe thu phí cao và kiểm soát dòng vốn.

Bảng 3: Hạn chế của Crowdfunding truyền thống

2.4.3. Giải pháp Web3 cho Crowdfunding

Ứng dụng Web3 vào Crowdfunding giúp loại bỏ nhiều điểm yếu trên bằng cách sử dụng các thành phần chính:

- **Smart Contract:** Là trung tâm của nền tảng, tự động hóa mọi quy trình: tạo dự án, nhận đóng góp, kiểm tra điều kiện và giải ngân.

- **Ví phi tập trung (Wallet):** Người dùng sử dụng ví như MetaMask để kết nối, đóng góp, và nhận token.
- **Blockchain:** Lưu trữ công khai và bất biến toàn bộ thông tin giao dịch, giúp tăng tính minh bạch.
- **Token hóa:** Có thể sử dụng token như phần thưởng, quyền biểu quyết, hoặc cổ phần ảo.

2.4.4. Sơ đồ mô hình hệ thống Web3 Crowdfunding

Dưới đây là mô hình minh họa quy trình hoạt động cơ bản:

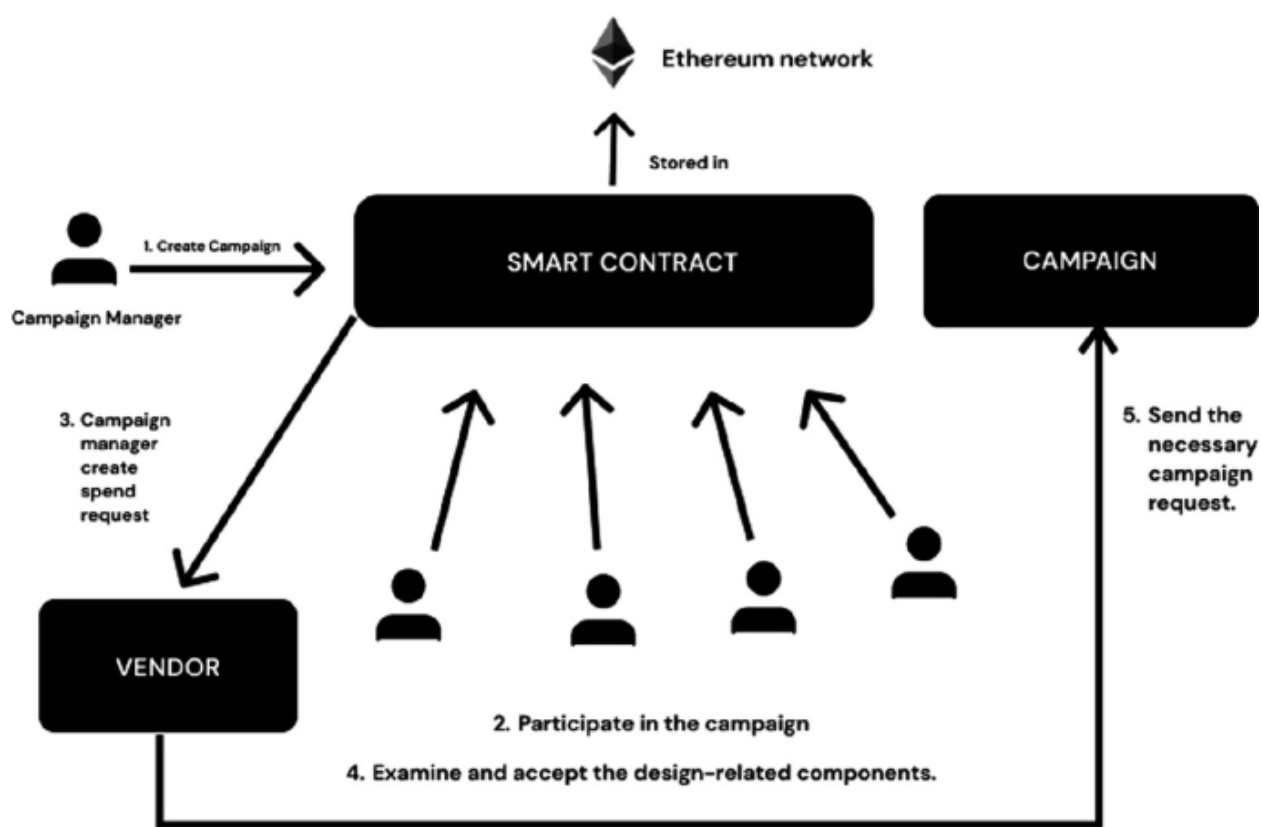


FIG. Flow of Ether in proposed blockchain model

Hình 6: Mô hình hoạt động của hệ thống Web3 Crowdfunding

2.4.5. Ưu điểm của Web3 Crowdfunding

- Minh bạch: Mọi khoản đóng góp và chi tiêu đều có thể kiểm chứng.
- Không cần tin tưởng (trustless): Hợp đồng thông minh đảm bảo thực thi đúng cam kết.

- Chi phí thấp: Không mất phí trung gian lớn.
- Tự động hóa: Giải ngân, phân phối token, hoặc hoàn tiền diễn ra hoàn toàn tự động.
- Khả năng mở rộng toàn cầu: Không bị giới hạn bởi biên giới địa lý.

2.4.6. Hạn chế và thách thức

- Đòi hỏi kiến thức kỹ thuật: Cả người tạo chiến dịch và người dùng cần hiểu về ví, blockchain, gas fee,...
- Khó khôi phục nếu mất quyền truy cập ví.
- Rủi ro bảo mật nếu hợp đồng thông minh có lỗi.
- Chưa có khung pháp lý rõ ràng tại nhiều quốc gia.

PHẦN 3: PHÂN TÍCH VÀ TRIỂN KHAI HỆ THỐNG

3.1. Kiến trúc tổng quan hệ thống

Hệ thống crowdfunding Web3 là một nền tảng phi tập trung (decentralized) được xây dựng trên blockchain Ethereum. Các thành phần chính của hệ thống bao gồm:

- **Chủ dự án (Project Creator):** Cá nhân hoặc tổ chức tạo chiến dịch gây quỹ. Họ nhập thông tin chiến dịch (tiêu đề, mô tả, mục tiêu tài trợ, thời hạn) thông qua giao diện người dùng (React.js). Sau đó, thông tin được gửi đến blockchain để triển khai một hợp đồng thông minh (smart contract) quản lý chiến dịch.
- **Người ủng hộ (Backer):** Người dùng đóng góp ETH (hoặc các token khác nếu hệ thống mở rộng) để hỗ trợ chiến dịch. Họ sử dụng ví Web3 (như MetaMask) để tương tác trực tiếp với smart contract.
- **Smart Contract:** Lớp logic cốt lõi của hệ thống, được viết bằng Solidity và triển khai trên Ethereum (testnet Sepolia cho thử nghiệm). Smart contract quản lý các quy tắc gây quỹ, bao gồm: nhận ETH từ người ủng hộ, kiểm tra mục tiêu tài trợ, xử lý rút tiền hoặc hoàn tiền, và đảm bảo tính minh bạch của mọi giao dịch.
- **Ví Web3 (MetaMask):** Cầu nối giữa người dùng và blockchain. MetaMask cho phép người dùng xác thực danh tính, ký giao dịch, và gửi ETH trực tiếp đến smart contract.
- **Blockchain Ethereum:** Nền tảng lưu trữ tất cả giao dịch và trạng thái của smart contract. Trong môi trường thử nghiệm, testnet Sepolia được sử dụng để giảm chi phí (không cần ETH thực). Mọi giao dịch được ghi nhận và xác minh trên blockchain, đảm bảo tính bất biến và minh bạch.

3.2. Tính năng chính của hệ thống

Hệ thống crowdfunding Web3 cung cấp các tính năng cốt lõi sau:

1. Tạo chiến dịch huy động vốn:

- Chủ dự án thiết lập chiến dịch thông qua giao diện người dùng, bao gồm: tiêu đề, mô tả, mục tiêu tài trợ (số ETH cần huy động), thời hạn chiến dịch (ví dụ: 30 ngày), và địa chỉ ví nhận tiền nếu đạt mục tiêu.
- Thông tin được gửi đến smart contract, tạo một instance độc lập cho mỗi chiến dịch.

```
// Create a new campaign
function createCampaign(address _owner, memory _title, memory
_description, _target, uint256 _deadline, string memory _image )
public returns (uint256) {
    require(_owner != address(0), "Invalid owner address.");
    require(bytes(_title).length > 0, "Title cannot be empty.");
    require(bytes(_description).length > 0, "Description cannot be
empty.");
    require(_target > 0, "Target must be greater than 0.");
    require(_deadline > block.timestamp, "The deadline should be a
date in the future.");

    Campaign storage campaign = campaigns[numberOfCampaigns];
    campaign.owner = _owner;
    campaign.title = _title;
    campaign.description = _description;
    campaign.target = _target;
    campaign.deadline = _deadline;
    campaign.amountCollected = 0;
    campaign.image = _image;

    numberOfCampaigns++;
    emit CampaignCreated(numberOfCampaigns - 1, _owner, _title,
_target, _deadline);
    return numberOfCampaigns - 1;
}
```

Hình 7: Cài đặt hàm `createCampaign()` trong Contract

2. Đóng góp ETH:

- Người ủng hộ sử dụng ví MetaMask để gửi ETH trực tiếp đến địa chỉ smart contract của chiến dịch.
- Giao dịch được ghi nhận trên blockchain, đảm bảo không thể can thiệp hoặc gian lận.

```
// Donate to a campaign
function donateToCampaign(uint256 _id) public payable
validCampaign(_id) {
    Campaign storage campaign = campaigns[_id];
    require(block.timestamp < campaign.deadline, "Campaign has
ended.");
    require(msg.value > 0, "Donation amount must be greater than
0.");


    campaign.donators.push(msg.sender);
    campaign.donations.push(msg.value);
    campaign.amountCollected += msg.value;

    emit DonationReceived(_id, msg.sender, msg.value);
}
```

Hình 8: Cài đặt hàm donateToCampaign() trong Contract

3. Theo dõi số tiền huy động:

- Giao diện frontend (React.js) truy vấn trạng thái của smart contract để hiển thị số ETH đã huy động theo thời gian thực.
- Người dùng có thể xem tiến độ (tỷ lệ phần trăm đạt được so với mục tiêu) và thời gian còn lại của chiến dịch.



**MAFIA/CRIME
SYNDICATE ROMANCE**


-0
Days Left

0.0
Raised of 0.1

2
Total Backers

Withdra...
Status

CREATOR



0xe5b21206bAaFa4e99a6073ba1C2832aA7DacA61E
7 campaigns

FUND

Fund the campaign

The campaign has been withdrawn. You cannot donate to the campaign.

Fund

STORY

Hey, it's Summer. This series changed my life. Not in a slow, gradual way—but in a “write-through-the-night, fall-hard-for-an-unhinged- crime-boss, holy-sh*t-this-book-just-hit-the-top-50-on-Kindle” kind of way. When I wrote Make Me, I wasn’t planning to launch a series. I wasn’t planning to fall completely obsessed with the Fox brothers and the women strong enough to stand toe-to-toe with them. But the second I started writing Cash Fox, everything changed—and you all showed up in a massive way to support this story. You gave me the freedom to become a full-time author. And when I asked what series you wanted in collector’s editions, the answer was overwhelming: Fox Family.

DONATORS

1. 0xe5b21206bAaFa4e99a6073ba1C2832aA7DacA61E	0.05
2. 0xD557cC1262eF876D26E9A5a17Bd3593Fae2e8Fc3	0.150000000000000002

Hình 9: Chi tiết của một chiến dịch đang hoạt động

4. Rút tiền khi đạt mục tiêu:

- Nếu tổng số ETH huy động đạt hoặc vượt mục tiêu trong thời hạn, chủ dự án có thể gọi hàm **withdraw()** trong smart contract để chuyển toàn bộ số ETH về ví của mình.
- Smart contract kiểm tra các điều kiện (mục tiêu đạt được, thời hạn chưa hết) trước khi cho phép rút.

```
// Withdraw funds (only by campaign owner)
function withdrawFunds(uint256 _id) public onlyOwner(_id)
validCampaign(_id) nonReentrant {
    Campaign storage campaign = campaigns[_id];
    require(block.timestamp >= campaign.deadline, "Campaign is
still ongoing.");
    require(campaign.amountCollected >= campaign.target,
"Campaign did not reach target.");
    require(address(this).balance >= campaign.amountCollected,
"Insufficient contract balance.");

    uint256 amount = campaign.amountCollected;
    campaign.amountCollected = 0;

    (bool sent,) = payable(campaign.owner).call{value:
amount}("");
    require(sent, "Failed to withdraw funds.");
    emit FundsWithdrawn(_id, campaign.owner, amount);
}
```

Hình 10: Cài đặt hàm *withdrawFunds()* trong *Contract*.

5. Hoàn tiền nếu thất bại:

- Nếu chiến dịch không đạt mục tiêu trong thời hạn, người ủng hộ có thể gọi hàm **refund()** để nhận lại số ETH đã đóng góp.
- Quá trình hoàn tiền được tự động hóa thông qua smart contract, đảm bảo công bằng và minh bạch.

```

// Refund donators if campaign fails
function refundDonators(uint256 _id) public validCampaign(_id)
nonReentrant {
    Campaign storage campaign = campaigns[_id];
    require(block.timestamp > campaign.deadline, "Campaign is
still ongoing.");
    require(campaign.amountCollected < campaign.target,
"Campaign reached its target.");
    require(address(this).balance >= campaign.amountCollected,
"Insufficient contract balance.");

    for (uint256 i = 0; i < campaign.donators.length; i++) {
        address donator = campaign.donators[i];
        uint256 amount = campaign.donations[i];
        if (amount > 0) {
            campaign.donations[i] = 0;
            (bool sent,) = payable(donator).call{value:
amount}("");
            require(sent, "Failed to refund donator.");
            emit FundsRefunded(_id, donator, amount);
        }
    }
    campaign.amountCollected = 0;
}

```

Hình 11: Cài đặt hàm `refundDonators()` trong Contract.

3.3. Quy trình hoạt động của chiến dịch

Quy trình hoạt động của hệ thống có thể được mô tả chi tiết qua các bước sau:

1. Tạo chiến dịch:

- Chủ dự án truy cập giao diện người dùng (React.js) và nhập thông tin chiến dịch (tiêu đề, mô tả, mục tiêu ETH, thời hạn).
- Giao diện gửi thông tin đến smart contract thông qua thư viện Ethers.js.
- Smart contract được triển khai trên testnet Sepolia, tạo một instance mới cho chiến dịch. Địa chỉ smart contract được lưu trữ để người ủng hộ tương tác.

2. Góp vốn:

- Người ủng hộ kết nối ví MetaMask với giao diện frontend.
- Họ chọn số ETH muốn đóng góp và gọi hàm **donateToCampaign()** trong smart contract.
- Giao dịch được ký bởi MetaMask và gửi đến blockchain. Smart contract ghi nhận đóng góp và cập nhật tổng số ETH đã huy động.

3. Theo dõi chiến dịch:

- Giao diện frontend truy vấn backend để lấy thông tin về số tiền đã huy động và thời gian còn lại.
- Thông tin được hiển thị dưới dạng các tập dữ liệu.

4. Kết thúc chiến dịch:

- **Nếu đạt mục tiêu:** Chủ dự án gọi hàm **withdraw()** để chuyển ETH về ví của mình. Smart contract kiểm tra điều kiện (mục tiêu đạt được, thời hạn chưa hết) trước khi thực hiện.
- **Nếu không đạt mục tiêu:** Người ủng hộ gọi hàm **refund()** để nhận lại ETH. Smart contract tự động hoàn tiền mà không cần trung gian.

3.4. Công nghệ sử dụng

Hệ thống sử dụng các công nghệ và công cụ sau:

Thành phần	Công nghệ sử dụng
Blockchain	Ethereum (Sepolia Testnet cho môi trường thử nghiệm)
Smart Contract	Solidity (viết hợp đồng thông minh)
Frontend (UI)	React.js + Tailwind CSS (giao diện người dùng)
Ví Web3	MetaMask (kết nối người dùng với blockchain)

Backend	Node.js (quản lý API, xử lý dữ liệu phụ trợ)
Triển khai hợp đồng	ThirdWeb (triển khai và kiểm tra hợp đồng)
Xác minh giao dịch	Etherscan Sepolia (theo dõi giao dịch trên blockchain)

Bảng 4: Các công nghệ sử dụng trong hệ thống Web3 Crowdfunding

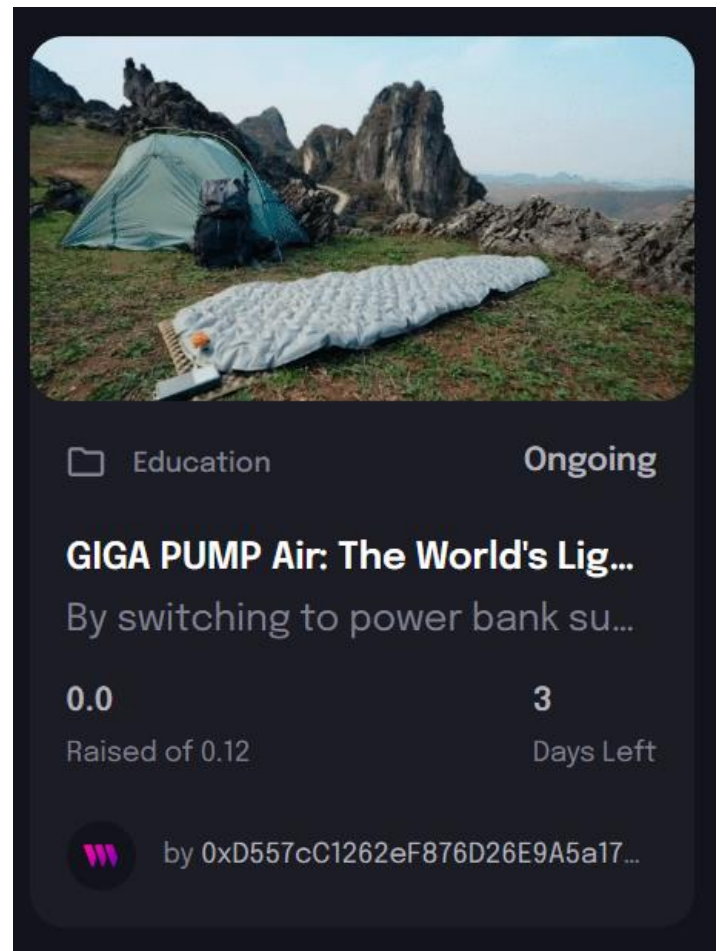
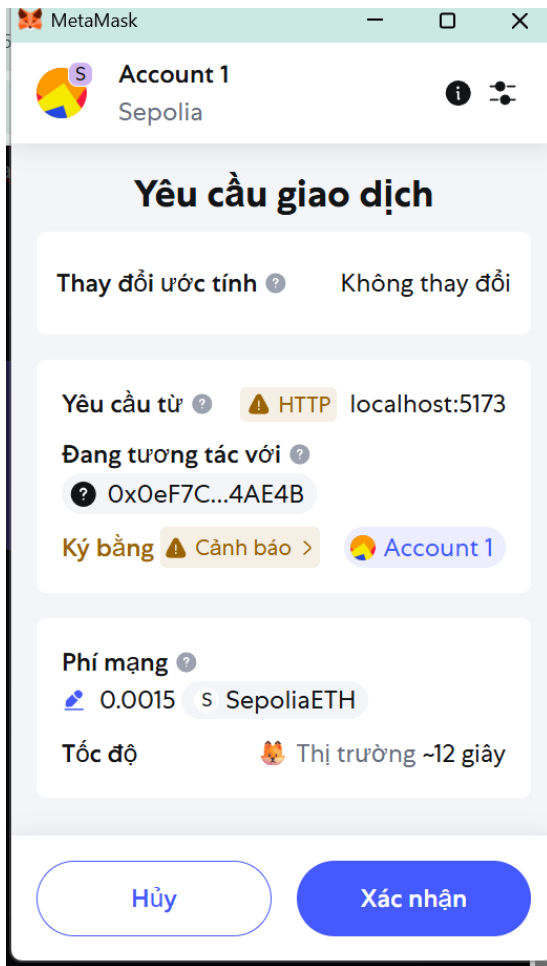
3.5. Kết quả kiểm thử

Để đánh giá tính khả thi và hiệu suất của hệ thống Web3 Crowdfunding, quá trình kiểm thử đã được thực hiện trên mạng thử nghiệm Sepolia Testnet. Các kịch bản kiểm thử được thiết kế để kiểm tra các tính năng chính của hệ thống, bao gồm: tạo chiến dịch, đóng góp ETH, theo dõi tiến độ, rút tiền khi đạt mục tiêu, và hoàn tiền khi thất bại. Dưới đây là mô tả chi tiết về các kịch bản kiểm thử và kết quả thu được.

3.5.1. Các kịch bản kiểm thử

1. Kịch bản 1: Tạo chiến dịch

- **Mô tả:** Một chủ dự án sử dụng giao diện frontend để tạo một chiến dịch với các thông tin: tiêu đề ("GIGA PUMP Air: The World's Lightest 2-in-1 Air Pump Only 1oz."), mô tả, mục tiêu 0.12 ETH, thời hạn 3 ngày.
- **Thực hiện:** Giao diện gửi thông tin đến smart contract thông qua hàm `createCampaign()`. MetaMask được sử dụng để ký giao dịch triển khai hợp đồng.



Hình 12 + 13: Minh họa khi tạo một chiến dịch mới

○ Kết quả:

- Chiến dịch được tạo thành công, với địa chỉ smart contract được ghi nhận trên Sepolia Testnet.
- Thời gian xử lý: ~8 giây.
- Chi phí gas: ~0.0015 ETH.
- Giao dịch được xác minh trên Etherscan Sepolia.

2. Kịch bản 2: Đóng góp ETH

- **Mô tả:** Người ủng hộ sử dụng ví MetaMask để đóng góp 0.09 ETH vào chiến dịch đã tạo.

- **Thực hiện:** Người ủng hộ gọi hàm `donateToCampaign()` thông qua giao diện. Mỗi giao dịch được ký bởi MetaMask và gửi đến blockchain.
- **Kết quả:**
 - 0.09 ETH được ghi nhận vào smart contract.
 - Thời gian xử lý trung bình mỗi giao dịch: ~6 giây.
 - Chi phí gas trung bình: ~ 0.0002 ETH
 - Tất cả giao dịch đều được xác minh thành công trên Etherscan Sepolia.

TRANSACTION ACTION

Call

Donate To Campaign

Function by 0xe5b21206...A7DacA61E on 0x0eF7C424...aa674AE4B

[This is a Sepolia Testnet transaction only]

Transaction Hash:	0xaaada01c7b52787cba6376c91490592d3de1c8fb4adb590c96db1c94cedfd88e
Status:	Success
Block:	8429250 2 Block Confirmations
Timestamp:	21 secs ago (May-29-2025 03:28:12 AM UTC)
From:	0xe5b21206bAaFa4e99a6073ba1C2832aA7DacA61E
To:	0x0eF7C424968D9e4EDA796E293D80f4Daa674AE4B
Value:	0.09 ETH
Transaction Fee:	0.000207561002629106 ETH
Gas Price:	1.500000019 Gwei (0.000000001500000019 ETH)

Hình 14: Kết quả giao dịch được ghi nhận trên Etherscan Sepolia.


3. Kịch bản 3: Theo dõi tiến độ chiến dịch

- **Mô tả:** Giao diện frontend truy vấn trạng thái smart contract để hiển thị số ETH đã huy động và thời gian còn lại.

- **Thực hiện:** Sử dụng thư viện Ethers.js để gọi hàm đọc dữ liệu từ smart contract (không tốn phí gas vì là truy vấn off-chain).
- **Kết quả:**
 - Giao diện hiển thị chính xác: 0.09 ETH đã huy động (75% mục tiêu), thời gian còn lại 3 ngày.
 - Thời gian phản hồi: <1 giây.
 - Không phát sinh lỗi trong quá trình truy vấn.

4. Kịch bản 4: Rút tiền khi đạt mục tiêu

- **Mô tả:** Một chiến dịch khác sau khi đạt mục tiêu, chủ dự án gọi hàm withdraw() để rút tiền.
- **Thực hiện:** Hàm withdraw() kiểm tra điều kiện (mục tiêu đạt được, thời hạn đã hết) và chuyển số ETH về ví của chủ dự án.
- **Kết quả:**
 - Rút tiền thành công, số dư smart contract về 0 ETH.
 - Thời gian xử lý: ~6 giây.
 - Chi phí gas: ~0.00025 ETH.
 - Giao dịch được xác minh trên Etherscan Sepolia.



TRANSACTION ACTION

Call

Withdraw Funds

Function by [0xe5b21206...A7DacA61E](#) on [0x0eF7C424...aa674AE4B](#)

[This is a Sepolia Testnet transaction only]

Transaction Hash:

0x0bcbc210dd425248a84512044faa327ff68cf2c80b0618b3fb9254fd894c22a7

Status:

Success

Block:

8423436 5853 Block Confirmations

Timestamp:

19 hrs ago (May-28-2025 08:03:00 AM UTC)

From:

[0xe5b21206bAaFa4e99a6073ba1C2832aA7DacA61E](#)

To:

[0x0eF7C424968D9e4EDA796E293D80f4Daa674AE4B](#)

Internal Transactions:

All Transfers

Net Transfers

Transfer 0.2 ETH From [0x0eF7C424...aa674AE4B](#) To [0xe5b21206...A7DacA61E](#)

Value:

0 ETH

Transaction Fee:

0.000063401558869856 ETH

Gas Price:

1.513922464 Gwei (0.000000001513922464 ETH)

Hình 14: Kết quả giao dịch được ghi nhận trên Etherscan Sepolia.

5. Kịch bản 5: Hoàn tiền khi thất bại

- Mô tả:** Trong một chiến dịch khác với mục tiêu 10 ETH, chỉ huy động được 3 ETH sau khi hết thời hạn. Người ủng hộ gọi hàm refund() để nhận lại tiền.
- Thực hiện:** Hàm refund() kiểm tra điều kiện (thời hạn đã hết, mục tiêu không đạt) và hoàn tiền tương ứng cho mỗi người ủng hộ.
- Kết quả:**
 - Tất cả người ủng hộ nhận lại đúng số ETH đã đóng góp (3 ETH tổng cộng).
 - Thời gian xử lý trung bình mỗi giao dịch hoàn tiền: ~5 giây.
 - Chi phí gas trung bình: ~0.0002 ETH

- Giao dịch được xác minh trên Etherscan Sepolia.

TRANSACTION ACTION

[Call](#)
[Refund Donators](#)
Function by [0xe5b21206...A7DacA61E](#) on [0xdbad2D05...06B785146](#)

[This is a Sepolia **Testnet** transaction only]

Transaction Hash:

0x50ec929d4efac329ec50006387d7f1cb40268d0701a519713286d09935335596

Status:

Success

Block:

8266506 162802 Block Confirmations

Timestamp:

22 days ago (May-06-2025 07:21:48 AM UTC)

From:

0xe5b21206bAaFa4e99a6073ba1C2832aA7DacA61E

To:

0xdbad2D052b040Dc0D3F35CC54Ef09Ef06B785146

Internal Transactions:

All Transfers

Net Transfers

Transfer 0.005 ETH From 0xdbad2D05...06B785146 To 0xe5b21206...A7DacA61E

Value:

0 ETH

Transaction Fee:

0.00396936597453227 ETH

Gas Price:

84.021971435 Gwei (0.000000084021971435 ETH)

Hình 15: Kết quả giao dịch được ghi nhận trên Etherscan Sepolia.

3.5.2. Tổng hợp kết quả kiểm thử

Kịch bản	Thành công	Thời gian xử lý (giây)	Chi phí gas (ETH)	Ghi chú
Tạo chiến dịch	Có	~8	~0.001	Giao dịch ổn định, không lỗi.
Đóng góp ETH	Có	~6	~0.0002	Hỗ trợ nhiều giao dịch đồng thời, không xảy ra xung đột.
Theo dõi tiến độ	Có	<1	0 (off-chain)	Giao diện phản hồi nhanh, dữ liệu chính xác.

Rút tiền khi đạt mục tiêu	Có	~5	~0.00025	Quy trình rút tiền minh bạch, đúng địa chỉ ví.
Hoàn tiền khi thất bại	Có	~5	~0.0002	Hoàn tiền tự động, đảm bảo công bằng cho người ủng hộ.
Tạo chiến dịch	Có	~8	~0.001	Giao dịch ổn định, không lỗi.

Bảng 5: Tổng hợp kết quả kiểm thử hệ thống Web3 Crowdfunding

3.5.3. Nhận xét về hiệu suất

- **Hiệu suất giao dịch:** Thời gian xử lý giao dịch trên Sepolia Testnet dao động từ 5-7 giây, phù hợp với đặc điểm của mạng Ethereum. Tuy nhiên, trên mainnet Ethereum, thời gian này có thể tăng do tắc nghẽn mạng hoặc chi phí gas cao hơn.
- **Chi phí gas:** Chi phí gas trung bình (~0.0002-0.0003 ETH) là hợp lý trong môi trường thử nghiệm. Trong thực tế, chi phí này có thể tăng đáng kể, đòi hỏi tối ưu hóa mã Solidity để giảm gas .
- **Tính ổn định:** Hệ thống hoạt động ổn định, không ghi nhận lỗi trong các kịch bản kiểm thử.
- **Trải nghiệm người dùng:** Giao diện frontend (React.js + Tailwind CSS) phản hồi nhanh, hiển thị dữ liệu theo thời gian thực. Tuy nhiên, người dùng mới có thể gặp khó khăn trong việc cài đặt và sử dụng ví MetaMask, đòi hỏi hướng dẫn chi tiết hơn.

3.5.4. Hạn chế và đề xuất cải tiến

- **Hạn chế:**

- Chi phí gas có thể trở thành rào cản khi triển khai trên Ethereum mainnet, đặc biệt với các giao dịch phức tạp như rút tiền hoặc hoàn tiền.
- Người dùng không quen với ví Web3 (như MetaMask) có thể gặp khó khăn trong việc tham gia chiến dịch.

- **Đề xuất cải tiến:**

- Tối ưu hóa smart contract để giảm chi phí gas.
- Cung cấp hướng dẫn sử dụng chi tiết hoặc tích hợp chatbot hỗ trợ trong giao diện để hướng dẫn người dùng mới.
- Thêm các tính năng bảo mật như kiểm tra danh tính chủ dự án hoặc cơ chế cảnh báo khi phát hiện giao dịch bất thường.

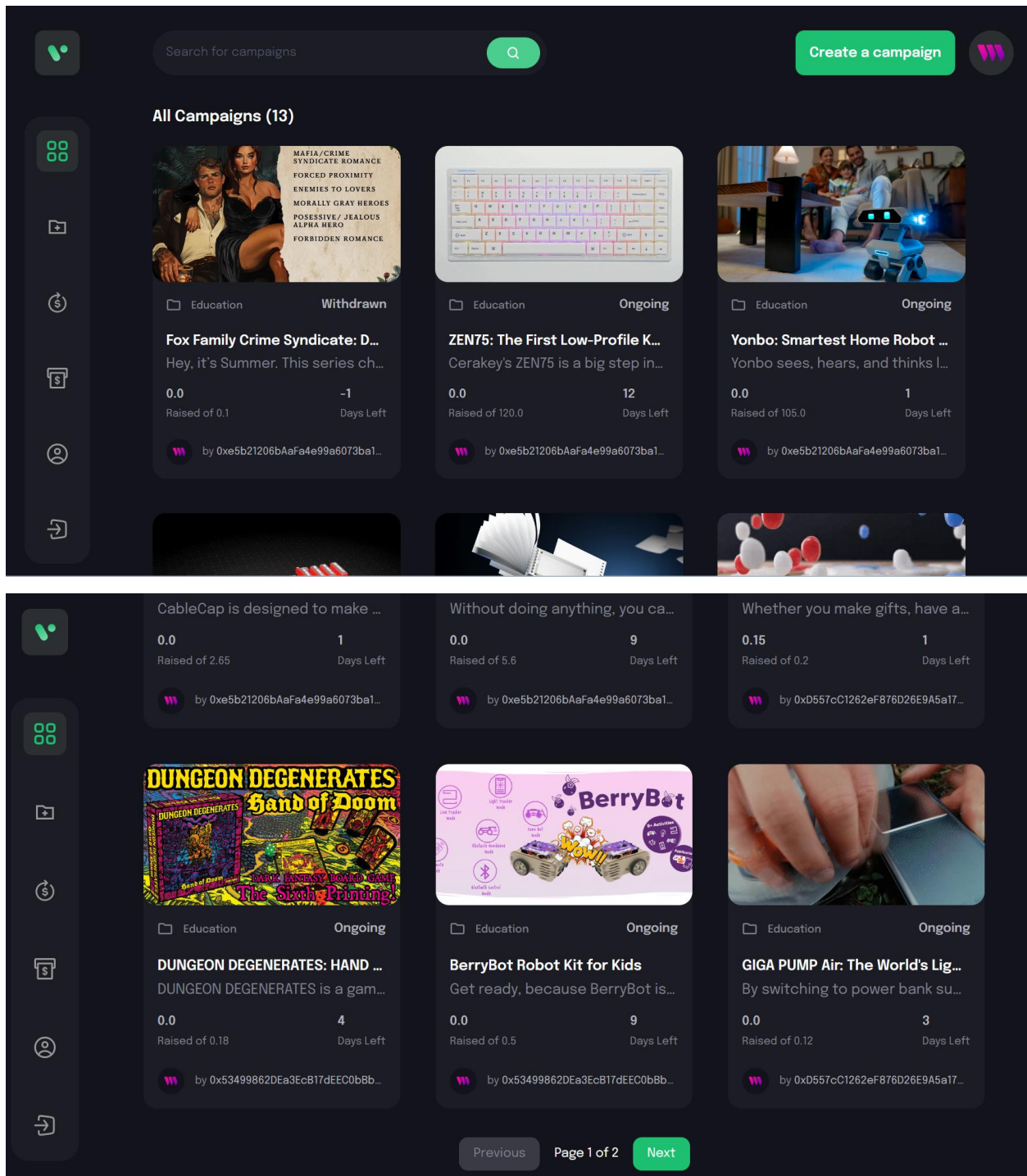
3.6. Thiết kế giao diện người dùng (UI/UX)

Giao diện được phát triển bằng **React.js** kết hợp với **Tailwind CSS**, tập trung vào tính trực quan, đơn giản và khả năng tương tác với blockchain một cách liền mạch.

3.6.1. Các thành phần giao diện chính

1. Trang chủ (Dashboard), trang rút tiền và hoàn tiền:

Mô tả: Trang chủ, trang rút tiền và hoàn tiền sử dụng chung 1 giao diện hiển thị danh sách các chiến dịch, với các thông tin tóm tắt như tiêu đề, mục tiêu huy động, số ETH đã đạt, và thời gian còn lại. Người dùng có thể tìm kiếm chiến dịch bằng thanh tìm kiếm.



Hình 16: Giao diện trang chủ

2. Trang chi tiết chiến dịch:

Mô tả: Trang này cung cấp thông tin chi tiết về một chiến dịch, bao gồm mô tả dự án, mục tiêu tài trợ, số ETH đã huy động, danh sách người ủng hộ (địa chỉ ví ẩn danh), và thời gian còn lại.

The screenshot shows a campaign detail page with a dark background. At the top, there is a search bar with the text "Search for campaigns" and a magnifying glass icon. To the right is a green button labeled "Create a campaign" and a user profile icon. The main content area features a large image of a globe. To the right of the image, there are four statistics: "1 Days Left", "0.15 Raised of 0.2", "2 Total Backers", and "Ongoing Status". Below the image, there are three sections: "CREATOR" showing a profile icon and address "0xD557cC1262eF876D26E9A5a17Bd3593Fae2e8Fc3" with "3 campaigns"; "STORY" with a paragraph about UV printing; and "DONATORS" with a list of two donors and their contribution amounts. On the right side, there is a "REFUND" section with a button labeled "Refund your donation" and a message stating "The campaign is still ongoing. You cannot refund yet." with a "Refund" button below it.

Search for campaigns

Create a campaign

1 Days Left

0.15 Raised of 0.2

2 Total Backers

Ongoing Status

CREATOR

0xD557cC1262eF876D26E9A5a17Bd3593Fae2e8Fc3
3 campaigns

STORY

Whether you make gifts, have a side hustle, or create simply for the joy it brings, it's always important to show your true colors. But traditional DIY printing solutions can limit even the most vivid of visions to a tiny handful of hues. UV printing transcends those boundaries, offering the full spectrum of vibrant colors and intricate details.

DONATORS

1. 0xe5b21206bAaFa4e99a6073ba1C2832aA7DacA61E	0.05
2. 0xD557cC1262eF876D26E9A5a17Bd3593Fae2e8Fc3	0.1

REFUND

Refund your donation

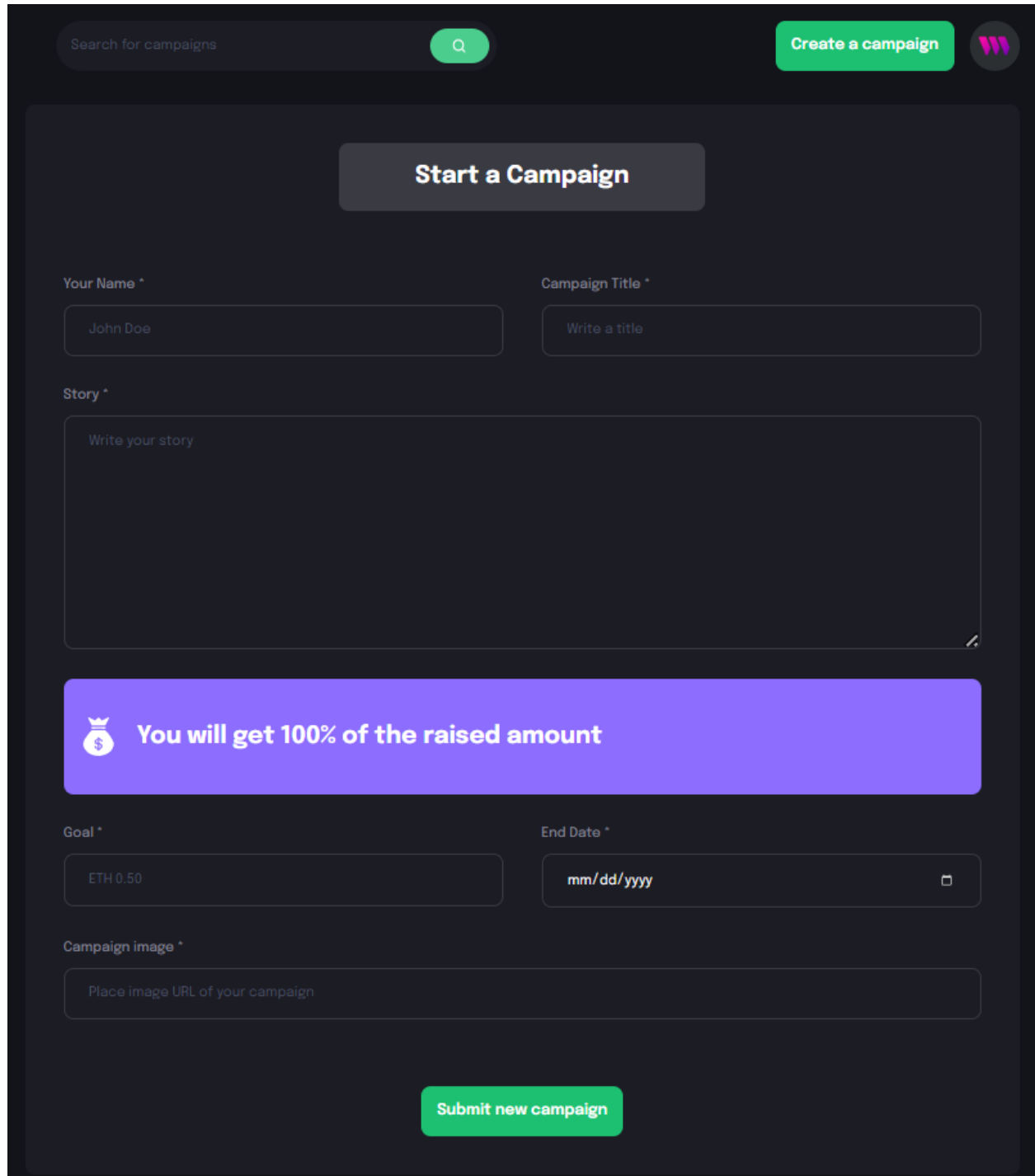
The campaign is still ongoing. You cannot refund yet.

Refund

Hình 17: Giao diện trang chi tiết chiến dịch

3. Trang tạo chiến dịch:

- **Mô tả:** Chủ dự án nhập thông tin chiến dịch (tiêu đề, mô tả, mục tiêu ETH, thời hạn) thông qua biểu mẫu (form) trực quan.



The screenshot displays a web interface for creating a campaign. At the top, there is a search bar labeled 'Search for campaigns' and a green button labeled 'Create a campaign'. Below this is a large button labeled 'Start a Campaign'. The form consists of several fields: 'Your Name *' with the placeholder 'John Doe', 'Campaign Title *' with the placeholder 'Write a title', and 'Story *' with a large text area and the placeholder 'Write your story'. A prominent purple banner with a money bag icon and the text 'You will get 100% of the raised amount' is positioned below the story field. Further down are 'Goal *' with the placeholder 'ETH 0.50' and 'End Date *' with the placeholder 'mm/dd/yyyy'. Below these is 'Campaign image *' with the placeholder 'Place image URL of your campaign'. At the bottom is a green button labeled 'Submit new campaign'.

Hình 18: Giao diện trang tạo chiến dịch

3.6.2. Hạn chế và đề xuất cải tiến

- **Hạn chế:**

- Người dùng mới có thể gặp khó khăn trong việc cài đặt và sử dụng MetaMask, đặc biệt nếu chưa quen với khái niệm ví Web3 hoặc private key.
- Giao diện chưa tích hợp các tính năng nâng cao như bình luận trực tiếp hoặc nhắn tin giữa chủ dự án và người ủng hộ.

- **Đề xuất cải tiến:**

- Tích hợp video hướng dẫn ngắn (dưới 1 phút) hoặc chatbot hỗ trợ để giải đáp thắc mắc về MetaMask và blockchain.
- Thêm tính năng bình luận hoặc diễn đàn để tăng tương tác giữa người dùng và chủ dự án.

TÀI LIỆU THAM KHẢO

1. Ethereum Foundation. (n.d.). **What is Ethereum?**
2. Ethereum Foundation. (n.d.). **Smart Contracts**
3. Moralis Blog. (2022). **How to Build a Web3 Crowdfunding DApp**
4. Alchemy. (2023). **What is a DApp?**
5. Thirdweb Docs. (n.d.). **How to Build a Crowdfunding App**
6. Chainlink Blog. (2021). **How Smart Contracts Work**
7. ConsenSys. (n.d.). **A Developer's Guide to Ethereum**
8. Binance Academy. (n.d.). **What is Web 3.0?**
9. OpenZeppelin Docs. (n.d.). **Smart Contract Security Best Practices**
10. IBM Blockchain. (n.d.). **How smart contracts work**
11. Vitalik Buterin. (2020). **The Meaning of Decentralization**
12. World Economic Forum. (2021). *Decentralized Finance (DeFi): Policy-Maker Toolkit.*