**ĐẠI HỌC QUỐC GIA TP. HỒ CHÍ MINH**
**TRƯỜNG ĐẠI HỌC CÔNG NGHỆ THÔNG TIN**
**KHOA MẠNG MÁY TÍNH VÀ TRUYỀN THÔNG**

**NGUYỄN THANH TÙNG - 15520983**
**LÊ HOÀNG TUẤN - 15520967**

**KHÓA LUẬN TỐT NGHIỆP**

# CẢI THIỆN TÍNH MINH BẠCH VÀ TIN CẬY CỦA ỨNG DỤNG GÂY QUỸ CỘNG ĐỒNG TỪ THIỆN ÁP DỤNG CÔNG NGHỆ BLOCKCHAIN

**GIẢNG VIÊN HƯỚNG DẪN**
**TS. PHẠM VĂN HẬU**
**ThS. PHAN THẾ DUY**

**TP. HỒ CHÍ MINH, 2019**

# DANH SÁCH HỘI ĐỒNG BẢO VỆ KHÓA LUẬN

Hội đồng chấm khóa luận tốt nghiệp, thành lập theo quyết định số .../QĐ-ĐHCNTT ...QĐ-ĐHCNTT ngày ../../.. của Hiệu trưởng Trường Đại học Công nghệ Thông tin.

1. ..... — Chủ tịch.
2. ..... — Thư ký.
3. ..... — Ủy viên.

# LỜI CẢM ƠN

Nhóm thực hiện khóa luận chân thành cảm ơn thầy ThS. Phan Thế Duy, cùng với TS. Phạm Văn Hậu đã theo sát quá trình thực hiện đề tài, đóng góp những ý kiến thiết thực và hữu ích để nhóm có thể hoàn thành đề tài khóa luận một cách hoàn chỉnh nhất.

Nhóm xin gởi lời cảm ơn đến gia đình và bạn bè đã động viên, khuyến khích nhóm hoàn thành khoá luận.

Nhóm cũng xin cảm ơn đến quý thầy cô khoa Mạng máy tính và truyền thông, trường Đại học Công nghệ Thông tin - ĐHQG TP.HCM đã giúp đỡ và hỗ trợ nhóm.

Xin chân thành cảm ơn!

TP.Hồ Chí Minh, ngày . . . tháng . . . năm . . .

Nhóm tác giả

# Mục lục

# Danh sách hình vẽ

# Danh sách bảng biểu

# Danh sách thuật ngữ

| Thuật ngữ | Diễn giải |
|---|---|
| address | địa chỉ, địa chỉ người dùng trong mạng blockchain. 16 |
| blockchain | chuỗi khối. 7, 8, 10, 11, 12, 14, 16, 18, 21 |
| crowdfunding | gây quỹ cộng đồng. 10, 11 |
| cryptocurrency | đồng tiền mã hóa. 15, 16 |
| smart contract | hợp đồng thông minh. 20 |
| transaction | giao dịch. 21, 22, 23 |

# Danh sách từ viết tắt

| Từ viết tắt | Từ đầy đủ |
|---|---|
| BCF | Binance Charity Foundation. 12 |
| IPFS | InterPlanetary File System. 20 |

# TÓM TẮT KHÓA LUẬN

Khóa luận này tập trung giải quyết các vấn đề sau: (1) vấn đề 1, (2) vấn đề 2,...

Kết quả đạt được là: (i) kết quả 1, (ii) kết quả 2,..

# Chương 1

# MỞ ĐẦU

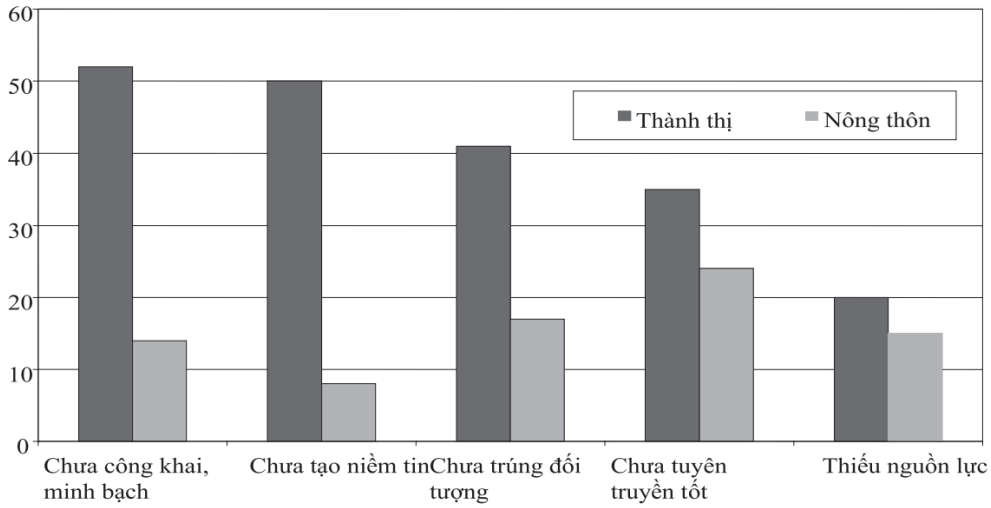
## 1.1 Vấn đề đặt ra

Hoạt động từ thiện là một hoạt động được đông đảo mọi người quan tâm, theo một kết quả của cuộc một cuộc điều tra [1] cho thấy có tới 81% người ở nước ta được khảo sát cho rằng những hoạt động tình nguyện thì họ rất quan tâm đến. Tương tự có khoảng 83% cho rằng hoạt động từ thiện đặc biệt quan trọng đối với một đất nước đang phát triển như Việt Nam.

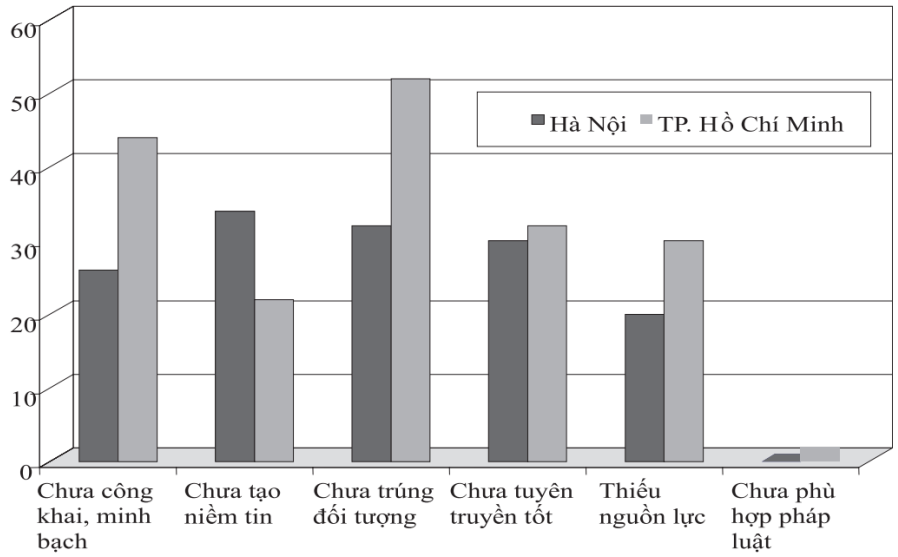
Tuy nhiên, các hoạt động từ thiện thì chưa được đông đảo người dân thực sự tin tưởng. Thật vậy, trong một cuộc khảo sát [2] có hơn 50% người dân thành thị (người dân thành thị chiếm đa số trong nguồn gây quỹ) cho rằng các hoạt động từ thiện của người dân hiện tại chưa công khai minh bạch, và đứng sau đó là các lý do được thể hiện ở hình 1.1 như: chưa tạo niềm tin, chưa trùng đối tượng, chưa tuyên truyền tốt, thiếu nguồn lực.

Đối với các hoạt động từ thiện của các doanh nghiệp, cũng trong cuộc khảo sát trên thì có tới hơn 50% người dân thành phố Hồ Chí Minh cho rằng lý do khiến họ không tin tưởng vào hoạt động từ thiện của doanh nghiệp là chưa đúng đối tượng cần được hỗ trợ. Lý do này chiếm tỉ lệ cao nhất trong các lý do được liệt kê ở hình 1.2.

Trong một bài nghiên cứu về từ thiện của tác giả Bekkers và Wiepking [3], các cá nhân sẽ đóng góp từ thiện nếu họ (i) nhận thức được nhu cầu của người cần giúp đỡ, ví dụ như biết cụ thể người cần giúp đỡ; (ii) được vận động đóng góp bởi một tổ chức đáng tin cậy; (iii) nhận thấy chi phí cho việc đóng góp (thuế) nhỏ và lợi ích khi đóng góp rõ ràng; (iv) động cơ nhân ái mạnh mẽ; (v) nhận thấy việc đóng góp từ thiện có lợi cho danh tiếng bản thân; (vi) nhận thấy lợi ích về mặt tâm lý, ví dụ như thoải mái khi đem cho; (vii) đóng góp cho những giá trị sống vì cộng đồng, và (viii) thấy rõ tính hiệu quả.




Hình 1.1: Những lý do chưa tạo được niềm tin trong hoạt động từ thiện của người dân




Hình 1.2: Những lý do chưa tạo được niềm tin trong hoạt động từ thiện của doanh nghiệp

Trong sách trắng của nền tảng Alice[1] cũng chỉ ra rằng sự minh bạch trong các hoạt động gây quỹ từ thiện ở các nước trên thế giới khiến cho lòng tin người dân sụt giảm một cách đáng kể. [4]

Do đó việc tạo ra một ứng dụng gây quỹ từ thiện theo mô hình gây quỹ cộng đồng áp dụng công nghệ blockchain là cần thiết. Ứng dụng có thể loại bỏ sự kiểm soát về mặt tài chính của các tổ chức, các giao dịch được công khai, minh bạch và đảm bảo được chiến dịch là đáng

[1] https://alice.si

tin cậy khi nó được xác minh bởi tổ chức, cơ quan chuyên trách.

## 1.2 Tính khoa học và tính mới của đề tài

### 1.2.1 Tính khoa học

Với các vấn đề đặt ra ở phần 1.1, hệ thống mà nhóm tác giả xây dựng sẽ:

- Giải quyết vấn đề công khai, minh bạch trong hoạt động gây quỹ khi xây dựng mô hình ứng dụng phi tập trung bằng công nghệ blockchain.
- Loại bỏ sự kiểm soát tài chính bởi các tổ chức, thay vào đó là ứng dụng hợp đồng thông minh trong công nghệ blockchain để phân bổ dòng tiền một cách tự động và an toàn.
- Tăng cường niềm tin ở người đóng góp quỹ khi các chiến dịch được xác minh một cách công khai trước khi đưa đến cộng đồng mà không tiết lộ các thông tin liên quan tới quyền riêng tư bằng công nghệ mã hoá.
- Tạo ra những cuộc bỏ phiếu của người đóng góp quỹ cho việc phân bổ nguồn quỹ một cách công khai, minh bạch bằng hợp đồng thông minh. Do đó tăng cường quyền hạn của người đóng góp quỹ.

### 1.2.2 Tính mới

- Xây dựng ứng dụng gây quỹ từ thiện theo mô hình gây quỹ cộng đồng.
- Ứng dụng công nghệ blockchain vào hoạt động gây quỹ từ thiện.

## 1.3 Mục tiêu

Mục tiêu khi thực hiện khóa luận này bao gồm:

- Xây dựng một ứng dụng web gây quỹ cộng đồng cho mục đích từ thiện dựa trên công nghệ Blockchain để tăng cường tính minh bạch, công khai với các chức năng cơ bản: lập hồ sơ gây quỹ, vận động gây quỹ, đóng góp tiền vào chiến dịch gây quỹ, phân phối tiền gây quỹ.
- Tạo cơ chế để ứng dụng đảm bảo các yêu cầu sau:
  - Các chiến dịch gây quỹ phải được xác minh trước khi công khai cho những người đóng góp.
  - Đảm bảo nguồn quỹ được chuyển trực tiếp từ người đóng góp tới người thụ hưởng.
  - Nguồn quỹ chỉ được phân phối theo lộ trình nếu như mục tiêu đặt ra trong hồ sơ gây quỹ được hoàn thành và được những người ủng hộ chấp nhận bằng cách bỏ phiếu.

## 1.4 Đối tượng và phạm vi nghiên cứu

Thứ nhất về mặt công nghệ, tập trung nghiên cứu nền tảng công nghệ Ethereum và hợp đồng thông minh. Các công nghệ xây dựng ứng dụng trên nền web như NodeJS, ReactJS.

Thứ hai về mặt nghiệp vụ, nghiên cứu các phương thức gây quỹ từ thiện bằng tài chính, các quy trình, giai đoạn của hoạt động gây quỹ.

# Chương 2

# TỔNG QUAN

## 2.1 Giới thiệu

Trong những năm gần đây, Blockchain được biết tới như là công nghệ để vận hành đồng tiền số Bitcoin, số lượng giao dịch và các tài khoản trong mạng Bitcoin đang càng ngày càng tăng cao. Dưới sự phát triển bùng nổ này, không khó để khiến đồng tiền điện tử Bitcoin thu hút được sự chú ý của cộng đồng. Blockchain là một cuốn sổ cái mà ở đó các dữ liệu không thể bị chỉnh sửa hoặc xoá khi đã được chấp thuận bởi các nút trong mạng. Vì đặc điểm này nên blockchain còn được biết đến như là một công nghệ giúp dữ liệu được lưu trữ toàn vẹn, tin tưởng [5]. Công nghệ blockchain này còn được áp dụng không chỉ về các lĩnh vực tài chính mà nó còn được áp dụng ở một số các lĩnh vực khác như chăm sóc sức khoẻ, sở hữu trí tuệ,...

Chính vì các đặc điểm nổi bật này của blockchain mà PwC và VeChain đã tiến hành cuộc khảo sát vào tháng 11 và tháng 12 năm 2017. Kết quả đã chi ra rằng hầu hết các doanh nghiệp của họ đang thành lập bộ phận nghiên cứu và phát triển (R&D) để đầu tư cho blockchain. Lý do mà họ (các công ty trong cuộc khảo sát đã triển khai công nghệ blockchain) chọn công nghệ này để nghiên cứu và phát triển thì có đến 50% về lý do bảo mật, các lý do còn lại như phân tán dữ liệu (26.7%), chứng thực định danh (23.3%),...

Khóa luận này tập trung vào việc áp dụng công nghệ blockchain vào hình thức Gây quỹ cộng đồng (Crowdfunding). Định nghĩa về crowdfunding được nhóm tác giả trích từ bài nghiên cứu của tác giả Lambert và Schwienbacher (2010) như sau:

> *"Crowdfunding involves an open call, essentially through the Internet, for the provision of financial resources either in form of donationor in exchange for some form of reward and/or voting rights."* [6]

Có thể hiểu định nghĩa trên theo tiếng Việt là crowdfunding giống như một lời gọi mở, thường

được thực hiện qua Internet, để cung cấp nguồn tài chính dưới hình thức tài trợ để đổi lấy phần thưởng hoặc quyền biểu quyết.

Crowdfunding là một thị trường chứa hàng tỉ đô-la, những giao dịch quốc tế đã đạt tới 34 tỷ đô-la trong năm 2015, gấp đôi năm trước [7]. Hiện nay, trên thế giới đã xuất hiện nhiều mô hình gây quỹ cộng đồng có thể kể đến như **Kickstarter**[1] và **Indiegogo**[2]. Những mô hình này cung cấp một platform để cho các chủ đầu tư có thể kêu gọi các nhà đầu tư, đầu tư vào các dự án của họ, các dự án này đa dạng, phong phú về lĩnh vực có thể kể đến như: âm nhạc, sản xuất vật liệu mới, đầu tư về giáo dục hay thậm chí là kêu gọi quỹ từ thiện.

Theo một cuộc nghiên cứu về Kickstarter bắt đầu từ năm 2008 đến tháng 7 năm 2012 của một cuộc điều tra kết quả là có 48.526 nỗ lực kêu gọi dự án với 237 triệu cam kết, và có 23.719 dự án chiếm 48.1% là kêu gọi quỹ thành công. Kickstarter cũng đã công bố phân tích tổng thể danh sách 26.017 dự án thành công và 33.098 dự án thất bại [8].

Tuy nhiên, các dự án trong Kickstarter đa phần tập trung vào mục đích lợi nhuận, thương mại cụ thể có 16% về lĩnh vực Film, 13% liên quan đến âm nhạc, 11% là về sách và 10% là các dự án về games các dự án phi lợi nhuận, gây quỹ cộng đồng chiếm tỉ lệ thấp, hầu như ít xuất hiện trên platform này [3]. Có thể thấy trên các nền tảng này, nguồn tiền được đóng góp thông qua bên thứ 3 (Visa, Mastercard, ...), bên thứ 3 này có tác dụng là nắm giữ nguồn vốn của nhà đầu tư, khi việc gây quỹ thành công, tuỳ vào cơ chế quản lý của nền tảng, nguồn vốn sẽ được xử lý và công nghệ hiện tại mà các platform này sử dụng đều đi qua cơ sở dữ liệu của chính nền tảng đó, điều này đặt ra tính toàn vẹn dữ liệu của dự án cũng như số tiền thật sự mà họ nhận được. Bên cạnh đó, các giải pháp giải quyết rủi ro về vấn đề tính sẵn sàng cao cũng như các cuộc tấn công khác nhằm chiếm đoạt tài sản của các nhà đầu tư chưa được chú ý đến. Tất cả các yếu tố bất lợi trên ta có thể thấy được rằng mô hình gây quỹ cộng đồng truyền thống chưa thật sự an toàn đối với các nhà đầu tư cũng như chủ chiến dịch và đặc biệt là nó chưa quan tâm đến các dự án gây quỹ cộng đồng, phi lợi nhuận. Bằng cách áp dụng blockchain vào mô hình gây quỹ truyền thống, ta có thể loại bỏ các yếu tố bất lợi được đề cập ở trên.

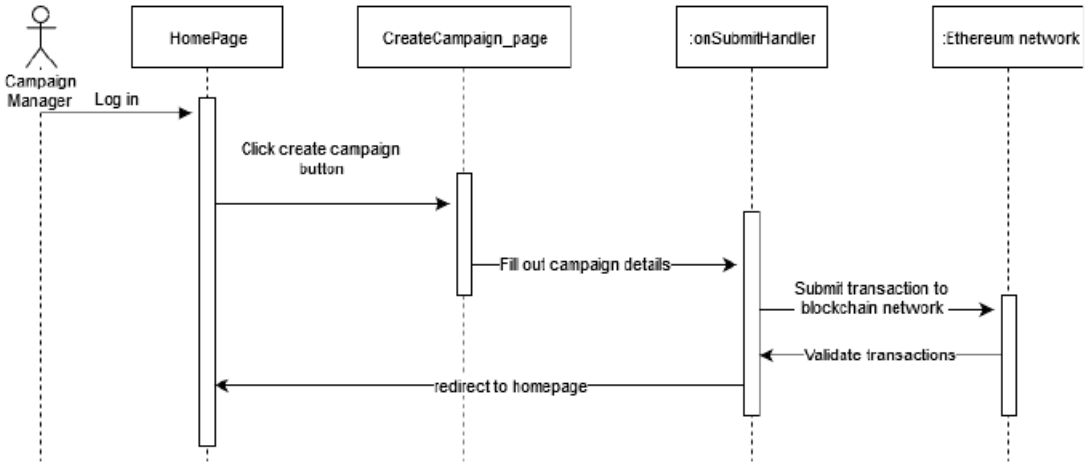
## 2.2 Các nghiên cứu liên quan

Với ý tưởng áp dụng blockchain vào các chiến dịch với mục đích phi lợi nhuận – trên thế giới đã có một chiến dịch có tên là **Usizo**[4], dự án này nhằm mục đích mua điện cho trường học ở miền nam của châu Phi bằng Bitcoin được đề xuất bởi Nir Kshetri – một giáo sư tại trường

[1] https://www.kickstarter.com
[2] https://www.indiegogo.com
[3] Nguồn: https://thehustle.co/archive/02102019d
[4] http://secret.usizo.org

đại học North Carolina, ý tưởng của chiến dịch này đó chính là áp dụng đồng tiền kỹ thuật số Bitcoin từ các nhà tài trợ để thanh toán tiền điện cho trường học, số tiền được nhận sẽ được thanh toán trực tiếp vào nguồn điện mà nhà trường đã sử dụng [9]. Theo đó, các nhà tài trợ có thể theo dõi số lượng nguồn điện mà nhà trường tiêu thụ và đồng thời tính toán nguồn tiền đóng góp của họ.

Trong một bài báo của tác giả Nazmus Saadat [10] đề xuất mô hình gây quỹ cộng đồng áp dụng hợp đồng thông minh trên nền tảng Ethereum blockchain để các hợp đồng được thực hiện hoàn toàn tự động, do đó ngăn ngừa gian lận và đảm bảo rằng các dự án có thể được phân phối trong thời gian nhất định. Hợp đồng thông minh sẽ giữ tiền của người đóng góp cho tới khi đạt được mục tiêu đặt ra. Tùy thuộc vào kết quả gây quỹ, tiền sẽ được trao cho chủ dự án hoặc trả lại an toàn cho người đóng góp. Tuy nhiên trong quy trình tạo chiến dịch ở hình 2.1, người tạo chiến dịch không được xác minh danh tính trước khi tạo chiến dịch, mà chỉ đơn thuần là đăng nhập vào một trình quản lý ví ethereum được gọi là Metamask[5]. Mà trên ví Metamask không cung cấp bất kì cơ chế nào để định danh người dùng.




Hình 2.1: Sơ đồ quy trình tạo chiến dịch trong mô hình của tác giả Nazmus Saadat

Một hệ thống khác cũng ứng dụng hợp đồng thông minh trên nền tảng Ethereum được gọi là **WeiFund**[6], tuy nhiên trong quy trình hoàn tiền cho người đóng góp khi mục tiêu gây quỹ thất bại được thực hiện một cách thủ công, tức người đóng góp phải thực hiện nhấp chuột vào một nút được gọi là "Claim Refund Owed" thì tiền mới được hoàn lại.

Một ứng dụng gây quỹ cộng đồng cho mục đích từ thiện khác được tổ chức có tên **Binance Charity Foundation (BCF)**[7] thực hiện. Tuy nhiên việc đăng kí chiến dịch trên hệ thống của

[5]https://metamask.io
[6]http://weifund.io
[7]https://www.binance.charity

BCF hoàn toàn chưa có tính mở, chưa cho phép cộng đồng đăng kí chiến dịch.

## 2.3 Kiến thức nền tảng

### 2.3.1 Công nghệ blockchain

### 2.3.2 Nền tảng Ethereum

### 2.3.3 Hợp đồng thông minh - Smart contract

# Chương 3

# PHÂN TÍCH VÀ THIẾT KẾ HỆ THỐNG

## 3.1 Giới thiệu hệ thống

Khóa luận hướng đến việc áp dụng công nghệ blockchain để giải quyết các vấn đề về tính minh bạch, công khai và tin cậy của ứng dụng gây quỹ cộng đồng theo mô hình truyền thống đã đề cập ở mục 1.1, 2.2. Nhóm tác giả sử dụng blockchain cho việc lưu trữ các thông tin về tài chính, các giao dịch của người dùng trong hệ thống nhằm hạn chế việc lưu các thông tin này trên bất kì một bên thứ ba nào. Hơn thế nữa, hệ thống sử dụng hợp đồng thông minh cho các lệnh liên quan tài chính trong hệ thống. Các lệnh này được thực hiện một cách tự động và chính xác, tránh sự can thiệp hay tác động từ yếu tố con người vào hệ thống. Với hợp đồng thông minh, nhóm tác giả cũng bổ sung các tính năng như tự động hoàn tiền khi mục tiêu gây quỹ chiến dịch không thành công; bỏ phiếu để giải ngân, tăng quyền hạn cho người đóng góp chiến dịch.

Bên cạnh đó, hệ thống của nhóm tác giả cũng sử dụng một phần dữ liệu được lưu trữ tập trung nhằm cải thiện tốc độ đọc ghi với các dữ liệu không cần độ tin cậy cao.

## 3.2 Quy trình gây quỹ cộng đồng

Đây là quy trình gây quỹ cộng đồng trong hệ thống của nhóm tác giả.

### 3.2.1 Các đối tượng trong quy trình

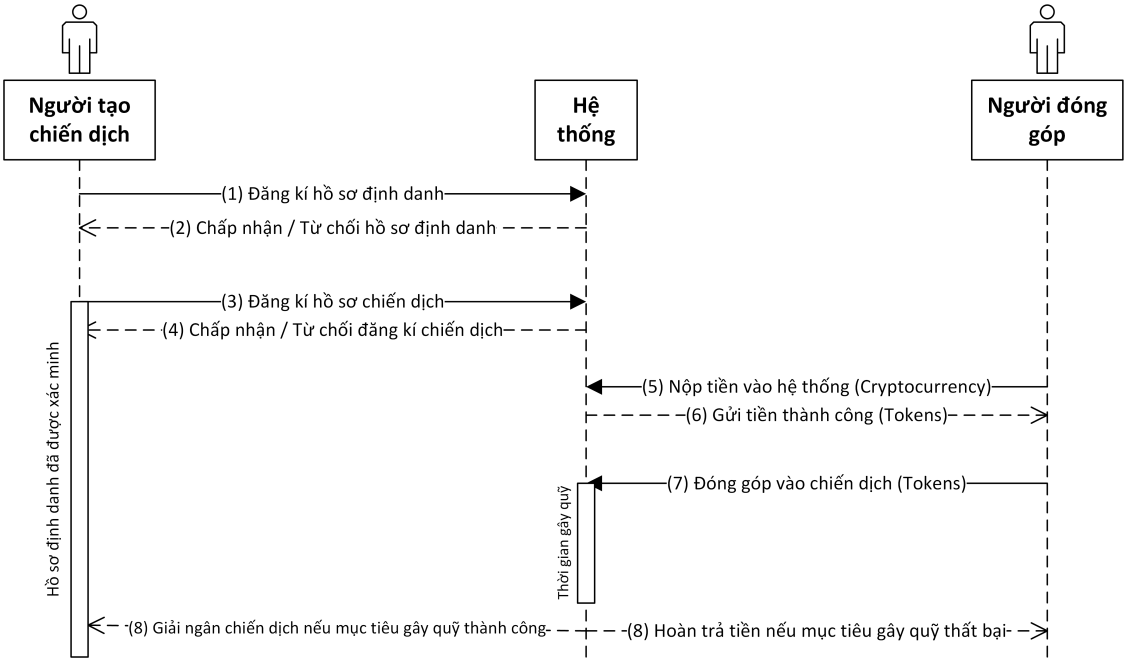
Trong quy trình gây quỹ, có các đối tượng sau:

- **Người tạo chiến dịch:** là những cá nhân / tổ chức có nhu cầu gây quỹ vì mục đích từ thiện, hướng tới cộng đồng.

- **Hệ thống:** là hệ thống gây quỹ trung gian, đứng giữa người tạo chiến dịch và người đóng góp.
- **Người đóng góp:** là người ủng hộ đóng góp tiền cho chiến dịch gây quỹ.

### 3.2.2 Sơ đồ quy trình gây quỹ

Sơ đồ quy trình gây quỹ được thể hiện ở hình 3.1.




Hình 3.1: Sơ đồ quy trình gây quỹ cộng đồng

Quy trình này được diễn giải như sau:

(1) Người tạo chiến dịch sẽ tiến hành tạo lập hồ sơ định danh bao gồm thông tin cá nhân cơ bản và thông tin chứng minh định danh.

(2) Hệ thống (nhân viên xác minh) tiến hành xác minh hồ sơ định danh và chấp nhận hay từ chối hồ sơ. Nếu hồ sơ định danh được chấp nhận thì hồ sơ đó được phép gọi lệnh tạo chiến dịch, ngược lại thì không.

(3) Người tạo chiến dịch tiếp tục tạo lập hồ sơ chiến dịch gây quỹ nếu hồ sơ định danh được chấp nhận.

(4) Hệ thống (nhân viên xác minh) tiến hành xác minh hồ sơ chiến dịch và chấp nhận hay từ chối hồ sơ. Hồ sơ được chấp nhận sẽ được công khai lên hệ thống và cho phép người đóng góp ủng hộ tiền. Ngược lại thì không.

(5) Người đóng góp muốn ủng hộ tiền cho một chiến dịch thì cần sử dụng cryptocurrency (đồng tiền mã hóa) gửi vào hệ thống (lúc này là hợp đồng thông minh) để sử dụng các

chức năng trong hệ thống.

(6) Sau khi người đóng góp gửi tiền vào hệ thống, hệ thống sẽ lưu số tiền người gửi vào dưới dạng một giá trị được gọi là token. Người đóng góp sử dụng token này trong các giao dịch nội bộ của hệ thống. Token này có thể được đổi ngược lại sang đồng cryptocurrency với giá tương ứng

(7) Người đóng góp ủng hộ tiền cho một chiến dịch (chiến dịch đã được xác minh) bằng một lượng token mà người đóng góp mong muốn và đang có.

(8) Mỗi chiến dịch sẽ có một khoảng thời gian để kêu gọi đóng góp, và một mục tiêu là số lượng token cần đạt được. Khi hết thời gian kêu gọi đóng góp, nếu chiến dịch hoàn thành mục tiêu thì sẽ tiến hành cho người tạo chiến dịch giải ngân. Ngược lại, lượng token đã đóng góp sẽ được hoàn lại cho người đóng góp.

## 3.3 Kiến trúc hệ thống

## 3.4 Các chức năng

### 3.4.1 Tổng quan các chức năng

Tổng quan các chức năng trong hệ thống được thể hiện ở hình 3.2.

### 3.4.2 Chức năng nộp tiền và rút tiền

#### 3.4.2.1 Mục tiêu

#### 3.4.2.2 Sơ đồ hoạt động

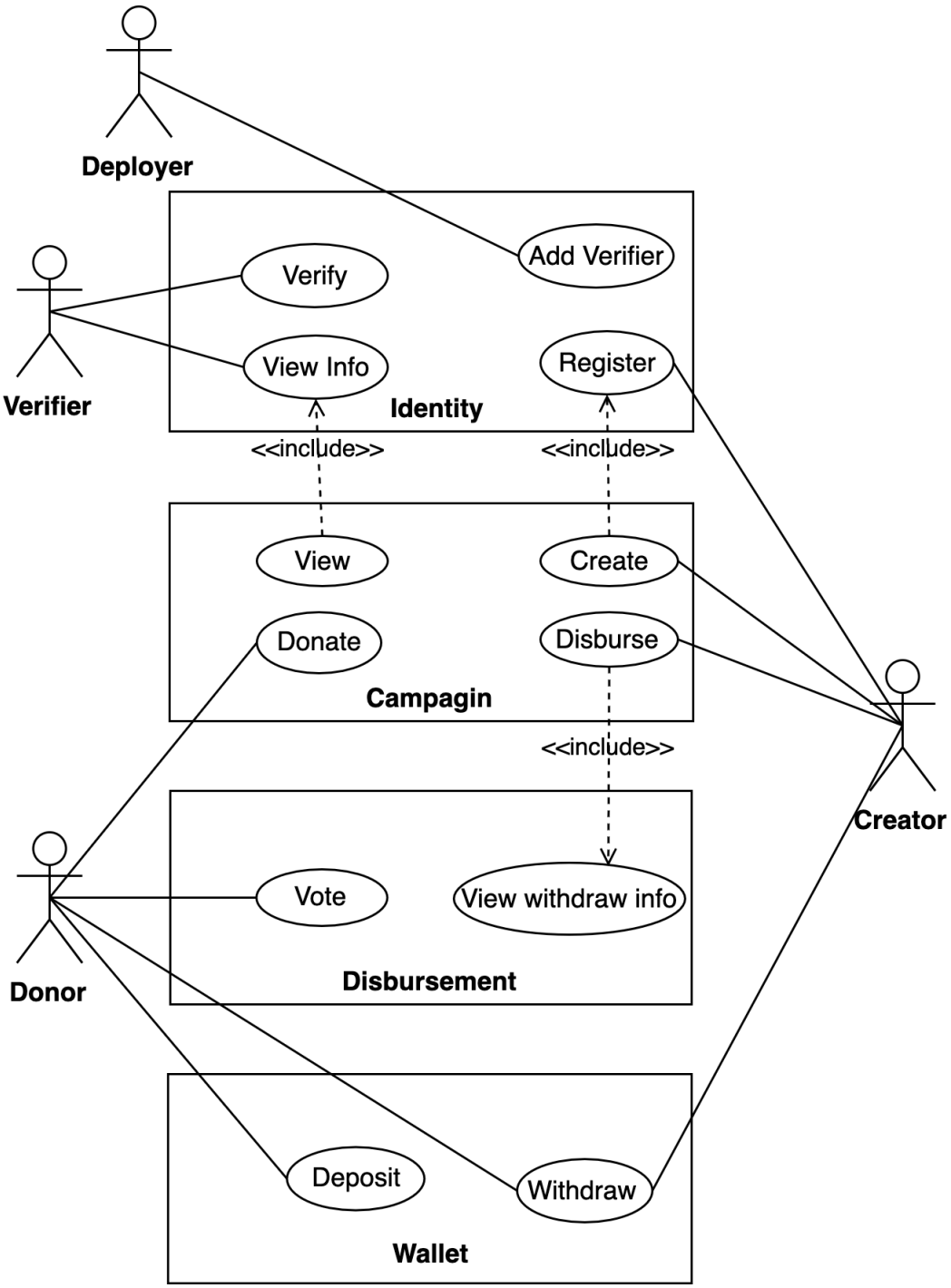
### 3.4.3 Chức năng quản lý định danh

#### 3.4.3.1 Mục tiêu

Do trong blockchain mỗi người dùng sẽ được xác định bởi các address (địa chỉ), các địa chỉ này hoàn toàn tách biệt với danh tính của người dùng, tức nó không bao gồm danh tính hay bất cứ thông tin nào như địa chỉ IP, định vị, .... Do đó có thể nói mỗi người dùng trên mạng blockchain là ẩn danh [12]. Để tăng tính tin cậy cho chiến dịch gây quỹ thì cần thiết phải gắn mỗi địa chỉ người dùng cho một hồ sơ định danh, vì vậy một địa chỉ người dùng muốn đăng kí tạo chiến dịch thì bắt buộc địa chỉ đó đã có hồ sơ định danh và hồ sơ định danh đó phải được xác minh. Việc tạo lập hồ sơ định danh chỉ bắt buộc với địa chỉ người dùng nào muốn tạo chiến dịch, còn đối với người đóng góp vào chiến dịch thì không bắt buộc.

Hồ sơ định danh có 2 loại thông tin cơ bản là:

- **Thông tin công khai:** là những thông tin cơ bản của người tạo chiến dịch như họ tên, địa chỉ, ngày sinh. Việc công khai thông tin là bắt buộc đối với người tạo chiến dịch.




Hình 3.2: Sơ đồ tổng quan các chức năng trong hệ thống

- **Thông tin cá nhân nhạy cảm**: là các thông tin cá nhân bí mật, được dùng để chứng minh cho các thông tin được công khai. Do đó cần lưu trữ thông tin cá nhân nhạy cảm một cách bí mật và toàn vẹn.

Yêu cầu về chia sẻ thông tin cá nhân giữa người dùng và người xác minh phải đảm bảo được

các yếu tố:

1. Chỉ có người dùng và người xác minh mới có thể đọc được thông tin.
2. Việc xác minh cho một hồ sơ được minh bạch. Tức biết ai là người đã xác minh cho hồ sơ, và vào thời gian nào.

#### 3.4.3.2 Cách hoạt động

Nhóm tác giả chia làm 2 tiến trình hoạt động cho chức năng này:

- Tạo lập và lưu trữ hồ sơ định danh.
- Chia sẻ thông tin hồ sơ định danh.

Các đối tượng trong chức năng định danh bao gồm:

- **Người tạo lập hồ sơ (người dùng - user):** là người tạo hồ sơ định danh, hay người tạo chiến dịch gây quỹ.
- **Người xác minh hồ sơ (verifier)**: người xác minh cho một hồ sơ định danh. Có thể là nhân viên trong hệ thống, tình nguyện viên.
- **Người vận hành hệ thống (deployer):** người quản lí danh sách các verifier. Hay người sẽ triển khai hợp đồng thông minh lên blockchain.

Cách thức tạo lập và lưu trữ hồ sơ định danh được thể hiện ở hình 3.3. Cụ thể:

- Người tạo lập hồ sơ định danh tiến hành nhập thông tin định danh.
- Người tạo lập hồ sơ nhập một chìa khóa bảo vệ hồ sơ định danh, được gọi là **SecretKey**. SecretKey được dùng cho 2 mục đích:
  (i) Làm khóa (key) cho thuật toán AES dùng để mã hóa các thông tin nhạy cảm của người dùng trước khi lưu trữ.
  (ii) SecretKey sẽ được mã hóa bằng thuật toán RSA bởi khóa công khai của verifier, sau đó chuỗi mã hóa sẽ được lưu trữ trên blockchain.

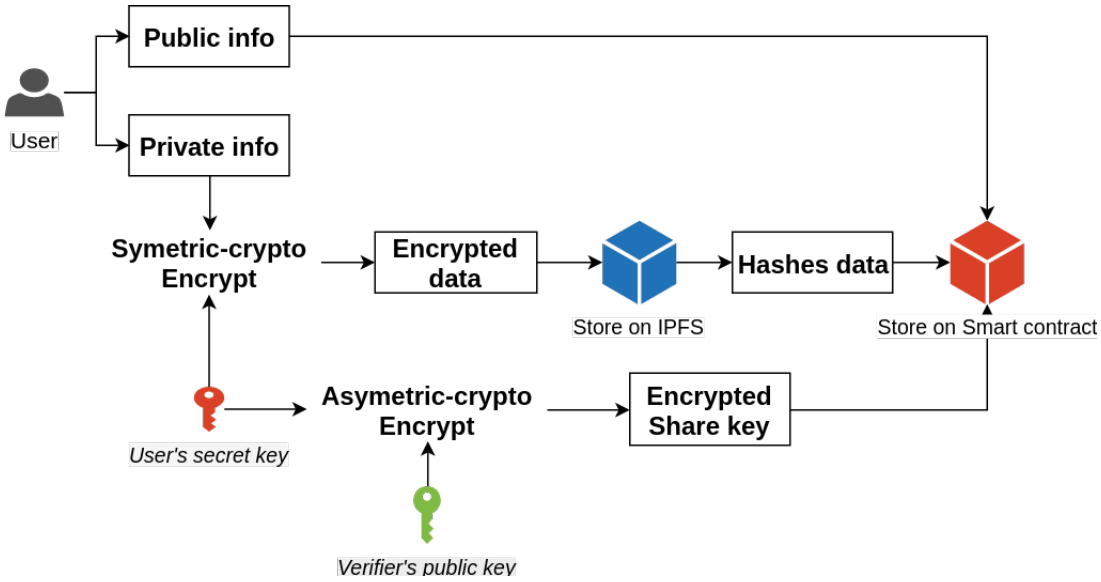
Cách thức chia sẻ hồ sơ định danh được thể hiện trong hình 3.4.

### 3.4.4 Chức năng giải ngân theo tiến độ

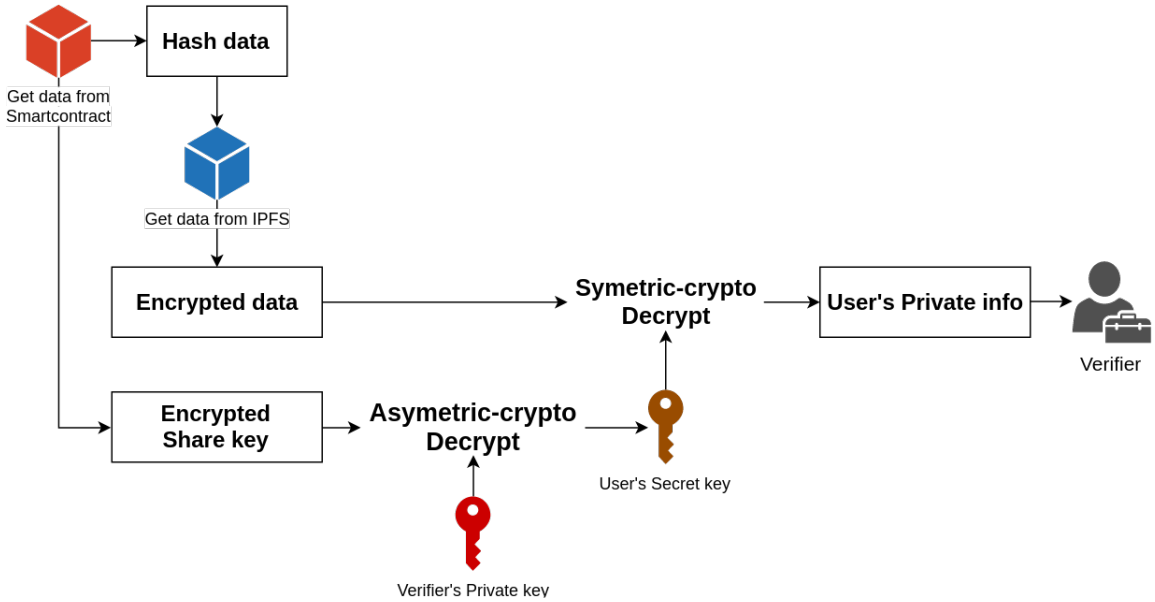
#### 3.4.4.1 Mục tiêu

#### 3.4.4.2 Sơ đồ hoạt động

## 3.5 Tổ chức dữ liệu




Hình 3.3: Sơ đồ cách thức lưu trữ hồ sơ định danh




Hình 3.4: Sơ đồ cách thức chia sẻ thông tin định danh

# Chương 4

# HIỆN THỰC VÀ ĐÁNH GIÁ HỆ THỐNG

## 4.1 Hiện thực

### 4.1.1 Môi trường hiện thực

Môi trường hiện thực bao gồm:

### 4.1.2 Các công nghệ được sử dụng

Các công nghệ được sử dụng bao gồm:

- Phần giao diện người dùng: nhóm tác giả sử dụng **ReactJS/NodeJS** kết hợp **Material UI** để tạo giao diện ứng dụng web cho người dùng.
- Phần backend được chia làm hai thành phần như sau:
  - Kiến trúc phi tập trung (decentralized): nhóm sử dụng ngôn ngữ solidity để xây dựng các smart contract kết hợp IPFS để thực hiện lưu trữ các dữ liệu phi tập trung.
  - Kiến trúc tập trung (centralized): công nghệ NodeJS kết hợp với Redis để tổ chức và tương tác với dữ liệu tập trung.

#### 4.1.2.1 Công nghệ ReactJS/NodeJS

#### 4.1.2.2 Material UI framework

#### 4.1.2.3 Cơ sở dữ liệu Redis

### 4.1.3 Các bước hiện thực

- Bước 1

- Bước 2
- Bước 3

## 4.2 Đánh giá hệ thống đã hiện thực

### 4.2.1 Đo lường tốc độ thực hiện giao dịch

Để tăng tính tin cậy cho phần đánh giá dưới đây của khóa luận, nhóm tác giả đã tham khảo mô hình đánh giá và kết quả đánh giá về hiệu suất của ethereum ở các công trình khác để làm thước đo và thực hiện tương tự với mô hình đánh giá đó.

Cụ thể, công trình của tác giả Sara Rouhani và Ralph Deters [11] đã đo được thời gian trung bình cho mỗi transaction là 104.609ms với Parity client và 198.9125ms với Geth. Tổng số transaction được gửi là 2000. Hai Ethereum private blockchain khác nhau với cùng cấu hình được thực thi bởi Parity client và Geth client được sử dụng để đo lường. Cấu hình hệ thống bao gồm 24GiB RAM và Core i7-6700 CPU. Việc gửi các transaction được thực hiện bằng ngôn ngữ NodeJS và sau đó thu thập thời gian xử lí cho việc xác nhận các transaction.

#### 4.2.1.1 Môi trường thực hiện đánh giá

Nhóm tác giả thực hiện việc đánh giá này trên cấu hình máy như sau:

- **CPU**: Intel(R) Xeon(R) CPU E5-2673 v4 @ 2.30GHz
- **RAM**: 2GB
- **OS**: Ubuntu 18.04 server x64 amd

Công cụ mà nhóm tác giả sử dụng trong phần đánh giá này là **Truffle framework**[1], đây là một bộ công cụ được sử dụng để triển khai các hợp đồng thông minh hỗ trợ ngôn ngữ Solidity.

Trong phần đánh giá thời gian này, nhóm tác giả sử dụng một mạng ethereum riêng được chạy trên mạng cục bộ nhằm loại bỏ đi thời gian chờ xác nhận giao dịch thông thường trên các mạng công khai hiện tại.

#### 4.2.1.2 Phương pháp thực hiện đánh giá

Đầu tiên nhóm tác giả thực hiện lựa chọn các hàm trong hợp đồng thông minh thường xuyên được sử dụng trong hệ thống, sau đó các hàm được chọn sẽ được hiện thực thông qua các transaction. Các transaction sẽ được xử lí và gửi đi bằng NodeJS, thời gian đo được tính từ lúc transaction được tạo ra đến lúc hoàn tất transaction đó. Với mỗi transaction, thực hiện gửi đi tuần tự 1000 lần với cùng một input cho trước. Sau đó lấy kết quả là thời gian trung bình

[1] https://www.trufflesuite.com

thực hiện cho mỗi transaction.

Các hàm được chọn và tham số đầu vào cho mỗi hàm để đo thời gian được thể hiện ở bảng 4.1.

| Contract | Hàm được chọn | Tham số đầu vào | Ghi chú |
|---|---|---|---|
| Wallet | deposit() | | value = $10^{15}$ gas |
| Campaigns | createCampaign() | 77760000,<br>1000000,<br>1,<br>[],<br>0,<br>[],<br>'8f1ef45972ebd8ef45b2410e8a0b399181fed3d929738d2eb96baf470758a97d',<br>'c2337a3217ffcf3b01398d83577a1c32235ceb4f481b8c7be00a055798e95d36' | tạo chiến dịch với số giai đoạn giải ngân $= 1$ |
| | createCampaign() | 77760000,<br>1000000,<br>3,<br>[300000, 300000, 400000]<br>2,<br>[0, 7200, 7200],<br>'8f1ef45972ebd8ef45b2410e8a0b399181fed3d929738d2eb96baf470758a97d',<br>'c2337a3217ffcf3b01398d83577a1c32235ceb4f481b8c7be00a055798e95d36' | tạo chiến dịch với số giai đoạn giải ngân $> 1$ |
| | donate() | 0,<br>1 | |

Bảng 4.1: Các hàm và tham số đầu vào được dùng để đo thời gian thực hiện giao dịch

#### 4.2.1.3 Kết quả đánh giá

Sau khi thực hiện đánh giá thời gian, nhóm tác giả đã tổng hợp kết quả như ở bảng 4.2. Theo như kết quả tổng hợp được, nhóm tác giả nhận xét rằng với dữ liệu đầu vào càng nhiều (kích thước lớn) thì thời gian xử lí càng lâu.

| Contract | Hàm được chọn | Tổng thời gian 1000 lần thực hiện (giây) | Thời gian trung bình một giao dịch (giây) | Ghi chú |
|---|---|---|---|---|
| Wallet | deposit() | 49.919 | 0.049919 | |
| Campaigns | createCampaign() | 123.9712 | 0.1239712 | tạo chiến dịch với số giai đoạn giải ngân $= 1$ |
| | createCampaign() | 288.936 | 0.288936 | tạo chiến dịch với số giai đoạn giải ngân $> 1$ |
| | donate() | 110.999 | 0.110999 | |

Bảng 4.2: Bảng kết quả đánh giá thời gian thực hiện giao dịch

### 4.2.2 Chi phí thực hiện các giao dịch trong hệ thống

#### 4.2.2.1 Môi trường thực hiện đánh giá

Nhóm tác giả thực hiện việc đo lường chi phí giao dịch trên cấu hình máy như sau:

- **CPU**: Intel(R) Xeon(R) CPU E5-2673 v4 @ 2.30GHz
- **RAM**: 2GB
- **OS**: Ubuntu 18.04 server x64 amd

Bộ công cụ **Truffle framework** kết hợp plug-in có tên là **eth-gas-reporter**[2] được sử dụng để triển khai các hợp đồng thông minh và đo lường chi phí thực hiện. Mạng ethereum riêng chạy trên máy cục bộ được sử dụng nhằm loại bỏ đi thời gian chờ xác nhận giao dịch thông thường trên các mạng công khai hiện tại.

#### 4.2.2.2 Phương pháp thực hiện đánh giá

Do chỉ có các hàm thực hiện ghi dữ liệu mới tốn chi phí thực hiện nên nhóm tác giả chọn ra các hàm có thao tác ghi dữ liệu, sau đó các hàm được chọn sẽ được hiện thực thông qua các transaction. Các transaction sẽ được xử lí và gửi đi bằng NodeJS. Sau đó thực hiện ghi lại kết quả chi phí.

Các hàm được chọn và tham số đầu vào cho mỗi hàm để đo lường chi phí được thể hiện ở bảng 4.3. Các tham số đầu vào mẫu được cho là sát với thực tế khi triển khai hệ thống (độ dài từng tham số mẫu là sát với thực tế).

#### 4.2.2.3 Kết quả chi phí cho các giao dịch trong hệ thống

Bảng tổng hợp chi phí cho các giao dịch được liệt kê ở bảng 4.4. Kết quả màn hình khi chạy chạy công cụ đo lường chi phí được thể hiện ở hình 4.1.

```
Contract: Perform cost all functions
  ✓ contract Wallet: function deposit (64512 gas)
  ✓ contract Wallet: function withdraw (46257 gas)
  ✓ contract Identity: function addVerifier (265666 gas)
  ✓ contract Identity: function changePubKey (79644 gas)
  ✓ contract Identity: function registerIdentity (430215 gas)
  ✓ contract Identity: function verify (20778 gas)
  ✓ contract Campaigns: function createCampaign (ONE-STAGE) (281589 gas)
  ✓ contract Campaigns: function createCampaign (MULTI-STAGE) (497048 gas)
  ✓ contract Campaigns: function verifyCampaign (46288 gas)
  ✓ contract Campaigns: function donate (177817 gas)
  ✓ contract Campaigns: function claimRefund (36007 gas)
  ✓ contract Campaigns: function donate (again) (48473 gas)
  ✓ contract Campaigns: function endCampaign (82927 gas)
  ✓ contract Disbursement: function vote (91003 gas)
```

Hình 4.1: Ảnh chụp màn hình kết quả đo lường chi phí giao dịch

Công cụ đo lường còn cung cấp cho chúng ta chi phí triển khai các hợp đồng thông minh, kết quả được thể hiện ở bảng 4.5.

Một số đại lượng trong bảng kết quả:

[2]https://www.npmjs.com/package/eth-gas-reporter

| Contract | Hàm | Dữ liệu đầu vào | Ghi chú |
|---|---|---|---|
| Wallet | deposit | | Thực hiện gửi vào 2000 tokens |
| | withdraw | 1000 | |
| Identity | addVerify | '0x93598a39777ED4B4Af3Ac7429d123Ca3bE9658C5',<br>'AAAAB3NzaC1yc2EAAAADAQABAAAAgQCDxbho2O3XWhktz4Hwi6/61ltfk/l<br>SCqeXLufvjr6O3wh1++MmTZT+KzcO0azsKsiFJTXL7ynC06Vp1Hp9o0BK3Q/Q<br>ZTo8jRoP3XX1LBu1CLe7OeOA5P2TO/nz2mWtuxz0b11GmRrjO8YoznizlPiolL<br>kv9hoDBvwTy0JonyJ6+w==' | |
| | changePubKey | '0x93598a39777ED4B4Af3Ac7429d123Ca3bE9658C5',<br>'MIGfMA0GCSqGSIb3DQEBAQUAA4GNADCBiQKBgQCMjs5j52lzXN6XX+nZ1js<br>yaBgzVBsA/JlWVux1zL0pw4GocvqPsZrIKwKsTeQycGdf3azjKRKwMga6g8fPF<br>HO+Ayh+6v33B1h+3ckWu81alwsM+Y9ADpcMret5qH2Mv9rDyWi+lmAYeUA<br>OOosAWfmgc6QJz+psSMtuGKOr08q+1wIDAQAB' | |
| | registerIdentity | 'KLTN',<br>'UIT-HCM, Linh Trung, Thu Duc, HCM',<br>830550240,<br>'QmarHSr9aSNaPSR6G9KFPbuLV9aEqJfTk1y9B8pdwqK4Rq',<br>'frPULs0boASMCqSq1guu+jX636wkY+fzhFSRnFQi9dQuK50yzCobUIGm5b/f7<br>oGDea/NrieB5c883EpWiQdgJlO+0B43jJLAtfSfJ/mlbGX3FUPc6LAQzxlCb5FSh<br>7+Q1E4WIUyFwLwoNdipDYFcpuXxtCsKeepjFHwGFhfupxM=',<br>'0x93598a39777ED4B4Af3Ac7429d123Ca3bE9658C5' | |
| | verify | '0x41A418C946Fd3201b7b2b30B367De35b0c54A6ce',<br>true | |
| Campaigns | createCampaign | 77760000,<br>1000000,<br>1,<br>[],<br>0,<br>[],<br>'8f1ef45972ebd8ef45b2410e8a0b399181fed3d929738d2eb96baf470758a97d',<br>'c2337a3217ffcf3b01398d83577a1c32235ceb4f481b8c7be00a055798e95d36' | tạo chiến dịch với số giai đoạn giải ngân = 1 |
| | createCampaign | 10,<br>1000,<br>3,<br>[300, 300, 400],<br>0,<br>[],<br>'8f1ef45972ebd8ef45b2410e8a0b399181fed3d929738d2eb96baf470758a97d',<br>'c2337a3217ffcf3b01398d83577a1c32235ceb4f481b8c7be00a055798e95d36' | tạo chiến dịch với số giai đoạn giải ngân >1 |
| | verifyCampaign | 1,<br>true | |
| | donate | 1,<br>1000 | |
| | claimRefund | 1,<br>200 | |
| | donate | 1,<br>200 | thực hiện donate lại cho đủ mục tiêu chiến dịch |
| | endCampaign | 1 | |
| Disbursement | vote | 1,<br>1,<br>true | |

Bảng 4.3: Các hàm và dữ liệu đầu vào được dùng để đo lường chi phí giao dịch

- **Gas** - là một đơn vị đo lường công việc tính toán của các giao dịch hoặc hợp đồng thông minh trong mạng Ethereum.
- **ETH** - là một đơn vị tiền tệ được sử dụng nội bộ trong mạng Ethereum. Tỉ lệ trao đổi giữa các đại lượng như sau: giá gas là 2 GWei/gas, và 1 ETH = $10^9$ GWei. Giá trị chuyển đổi giữa ETH và USD hiện tại được tham khảo trên **CoinMarketcap**[3] là

[3]https://coinmarketcap.com

150.08 USD/ETH (cập nhật ngày 27/11/2019)

| Contract | Hàm | Chi phí tính toán (gas) | Chi phí giao dịch (ETH) | Chi phí giao dịch (USD) |
|---|---|---|---|---|
| Wallet | deposit | 64512 | 0.000129024 | 0.02 |
| | withdraw | 46257 | 0.000092514 | 0.01 |
| Identity | addVerify | 265666 | 0.000531332 | 0.08 |
| | changePubKey | 79644 | 0.000159288 | 0.02 |
| | registerIdentity | 430215 | 0.000860430 | 0.13 |
| | verify | 20778 | 0.000041556 | 0.01 |
| Campaigns | createCampaign | 281589 | 0.000563178 | 0.08 |
| | createCampaign | 497048 | 0.000994096 | 0.15 |
| | verifyCampaign | 46288 | 0.000092576 | 0.01 |
| | donate | 177817 | 0.000355634 | 0.05 |
| | claimRefund | 36007 | 0.000072014 | 0.01 |
| | donate | 48473 | 0.000096946 | 0.01 |
| | endCampaign | 82927 | 0.000165854 | 0.02 |
| Disbursement | vote | 91003 | 0.000182006 | 0.03 |

Bảng 4.4: Kết quả đo lường chi phí giao dịch

| Contract | Chi phí (gas) | Chi phí (ETH) | Chi phí (USD) |
|---|---|---|---|
| Campaigns | 3447461 | 0.006894922 | 1.03 |
| Disbursement | 1331555 | 0.002663110 | 0.4 |
| Identity | 2401480 | 0.004802960 | 0.72 |
| Wallet | 1163284 | 0.002326568 | 0.35 |

Bảng 4.5: Kết quả đo lường chi phí triển khai các hợp đồng

### 4.2.3 Phân tích bảo mật của hợp đồng thông minh trong hệ thống

# Chương 5

# KẾT LUẬN

## 5.1 Thuận lợi

Trong khóa luận này, có những thuận lợi như sau:

## 5.2 Khó khăn

.....

## 5.3 Hướng phát triển

.....

# Tài liệu tham khảo


[1] H. P. Vu, L. Bình, H. Dũng, and P. Trà, *Nhận thức của người dân về hoạt động từ thiện và khả năng gây quỹ của các tổ chức phi chính phủ Việt Nam*. NXB Giao thông vận tải, Nov. 2015.

[2] T. tâm Nghiên cứu Châu Á – Thái Bình Dương Hà Nội & Quỹ Châu Á. (2011). Đóng góp từ thiện tại việt nam, [Online]. Available: `https://asiafoundation.org/resources/pdfs/ASIATVfinal.pdf` (visited on 08/25/2019).

[3] R. Bekkers and P. Wiepking, "A literature review of empirical studies of philanthropy: Eight mechanisms that drive charitable giving," *Nonprofit and voluntary sector quarterly*, vol. 40, no. 5, pp. 924–973, 2011.

[4] Alice. (2019). Alice whitepaper, [Online]. Available: `https://github.com/alice-si/whitepaper` (visited on 08/25/2019).

[5] J. Yli-Huumo, D. Ko, S. Choi, S. Park, and K. Smolander, "Where is current research on blockchain technology?—a systematic review," *PloS one*, vol. 11, no. 10, e0163477, 2016.

[6] P. Belleflamme, T. Lambert, and A. Schwienbacher, "Crowdfunding: An industrial organization perspective," in *Prepared for the workshop Digital Business Models: Understanding Strategies', held in Paris on June*, Citeseer, 2010, pp. 25–26.

[7] L. Hornuf and D. Cumming, *The Economics of Crowdfunding: Startups, Portals and Investor Behavior*. Taylor & Francis Limited, 2018.

[8] E. Mollick, "The dynamics of crowdfunding: An exploratory study," *Journal of business venturing*, vol. 29, no. 1, pp. 1–16, 2014.

[9] A. Goranović, M. Meisel, L. Fotiadis, S. Wilker, A. Treytl, and T. Sauter, "Blockchain applications in microgrids an overview of current projects and concepts," in *IECON 2017-43rd Annual Conference of the IEEE Industrial Electronics Society*, IEEE, 2017, pp. 6153–6158.

[10] M. N. Saadat, S. A. H. S. A. Rahman, R. M. Nassr, and M. F. Zuhiri, “Blockchain based crowdfunding systems in malaysian perspective,” in *Proceedings of the 2019 11th International Conference on Computer and Automation Engineering*, ACM, 2019, pp. 57–61.

[11] S. Rouhani and R. Deters, “Performance analysis of ethereum transactions in private blockchain,” in *2017 8th IEEE International Conference on Software Engineering and Service Science (ICSESS)*, IEEE, 2017, pp. 70–74.

[12] R. Henry, A. Herzberg, and A. Kate, “Blockchain access privacy: Challenges and directions,” *IEEE Security & Privacy*, vol. 16, no. 4, pp. 38–45, 2018.

# Phụ lục A

# Mã hợp đồng thông minh - TokenSystem

Mã được liệt kê ở đây

# Phụ lục B

# Mã hợp đồng thông minh - Campaigns

Mã được liệt kê ở đây