

ĐẠI HỌC QUỐC GIA THÀNH PHỐ HỒ CHÍ MINH  
TRƯỜNG ĐẠI HỌC CÔNG NGHỆ THÔNG TIN  
KHOA HỆ THÔNG THÔNG TIN



BÁO CÁO ĐỒ ÁN

Đề tài  
**ỨNG DỤNG CÔNG NGHỆ  
BLOCKCHAIN TRONG TRUY XUẤT  
NGUỒN GỐC GIÀY**

Lớp: Hoạch định nguồn lực doanh nghiệp - IS336.N11.HTCL

Giảng viên hướng dẫn: ThS. Đỗ Duy Thanh

Sinh viên thực hiện

Trần Trọng Nghĩa	20521657
Phan Công Thành	20521923
Phạm Phú Tuấn	20522125

Thành phố Hồ Chí Minh, ngày 14 tháng 1 năm 2023

## MỤC LỤC

<b>PHẦN A: CƠ SỞ LÝ THUYẾT .....</b>	<b>3</b>
1. BLOCKCHAIN .....	3
1.1 Định nghĩa Blockchain .....	3
1.2 Ưu điểm của Blockchain .....	3
1.3 Cách hoạt động của Blockchain .....	4
1.4 Cơ chế đồng thuận của Blockchain .....	7
1.5 Ứng dụng của Blockchain .....	8
1.6 Nguyên lý mã hóa của Blockchain .....	10
2. ETHEREUM .....	11
2.1 Định nghĩa Ethereum.....	11
2.2 Kiến trúc của Ethereum: .....	11
3. SMART CONTRACT .....	14
3.1 Định nghĩa Smart Contract.....	14
3.2 Sự khác nhau giữa Hợp đồng thông minh (Smart contract) và Hợp đồng truyền thống.....	15
3.3 Cách hoạt động của Smart Contract .....	16
3.4 Ưu điểm và hạn chế của Smart Contract .....	17
<b>PHẦN B: ỨNG DỤNG .....</b>	<b>24</b>
4. ỨNG DỤNG BLOCKCHAIN TRONG TRUY XUẤT NGUỒN GỐC GIÀY ....	24
4.1 Vấn đề.....	24
4.2 Giải pháp .....	25
<b>PHẦN C: TÀI LIỆU THAM KHẢO .....</b>	<b>27</b>

# **PHẦN A: CƠ SỞ LÝ THUYẾT**

## **1. BLOCKCHAIN**

### **1.1 Định nghĩa Blockchain**

Blockchain (tiếng Việt dịch là Chuỗi khối) là một cơ sở dữ liệu (CSDL) phân cấp lưu trữ thông tin trong các khối thông tin (block) được liên kết với nhau bằng mã hóa và mở rộng theo thời gian. Mỗi khối thông tin đều chứa thông tin về thời gian khởi tạo và được liên kết tới khối trước đó, kèm một mã thời gian và dữ liệu giao dịch. Blockchain được thiết kế để chống lại việc thay đổi của dữ liệu: Một khi dữ liệu đã được mạng lưới chấp nhận thì sẽ không có cách nào thay đổi được nó [3].

Hay theo AWS: “Công nghệ Blockchain là một cơ chế cơ sở dữ liệu tiên tiến cho phép chia sẻ thông tin minh bạch trong một mạng lưới kinh doanh. Cơ sở dữ liệu chuỗi khối lưu trữ dữ liệu trong các khối được liên kết với nhau trong một chuỗi. Dữ liệu có sự nhất quán theo trình tự thời gian vì bạn không thể xóa hoặc sửa đổi chuỗi mà không có sự đồng thuận từ mạng lưới. Do đó, bạn có thể sử dụng công nghệ chuỗi khối để tạo một số cái không thể chỉnh sửa hay biến đổi để theo dõi các đơn đặt hàng, khoản thanh toán, tài khoản và những giao dịch khác. Hệ thống có những cơ chế tích hợp để ngăn chặn các mục nhập giao dịch trái phép và tạo ra sự nhất quán trong chế độ xem chung của các giao dịch này.” [2]

Vậy, Công nghệ chuỗi khối là một số cái phân tán, cho phép ghi dữ liệu vĩnh viễn và không thay đổi với giá trị cung cấp tính minh bạch hoàn toàn và tính bất biến của các bản ghi hoặc khôi. Các khôi được liên kết với nhau để tạo thành một chuỗi các khôi, tức là một chuỗi khôi

### **1.2 Ưu điểm của Blockchain**

Công nghệ chuỗi khối mang lại nhiều lợi ích cho việc quản lý giao dịch tài sản. Dưới đây, chúng tôi liệt kê một vài lợi ích trong số đó:

Bảo mật nâng cao

Hệ thống chuỗi khối cung cấp mức độ bảo mật và sự tin cậy cao mà các giao dịch kỹ thuật số hiện đại yêu cầu. Luôn tồn tại nỗi sợ rằng ai đó sẽ thao túng phần mềm cơ sở để tạo ra tiền giả cho bản thân họ. Nhưng chuỗi khối sử dụng 3 nguyên tắc mật mã, phi tập trung và đồng thuận để tạo ra một hệ thống phần mềm cơ sở có độ bảo mật cao, gần như không thể bị làm giả. Không có một điểm lỗi làm chết cả hệ thống và một người dùng sẽ không thể thay đổi các bản ghi giao dịch.

#### Cải thiện hiệu quả

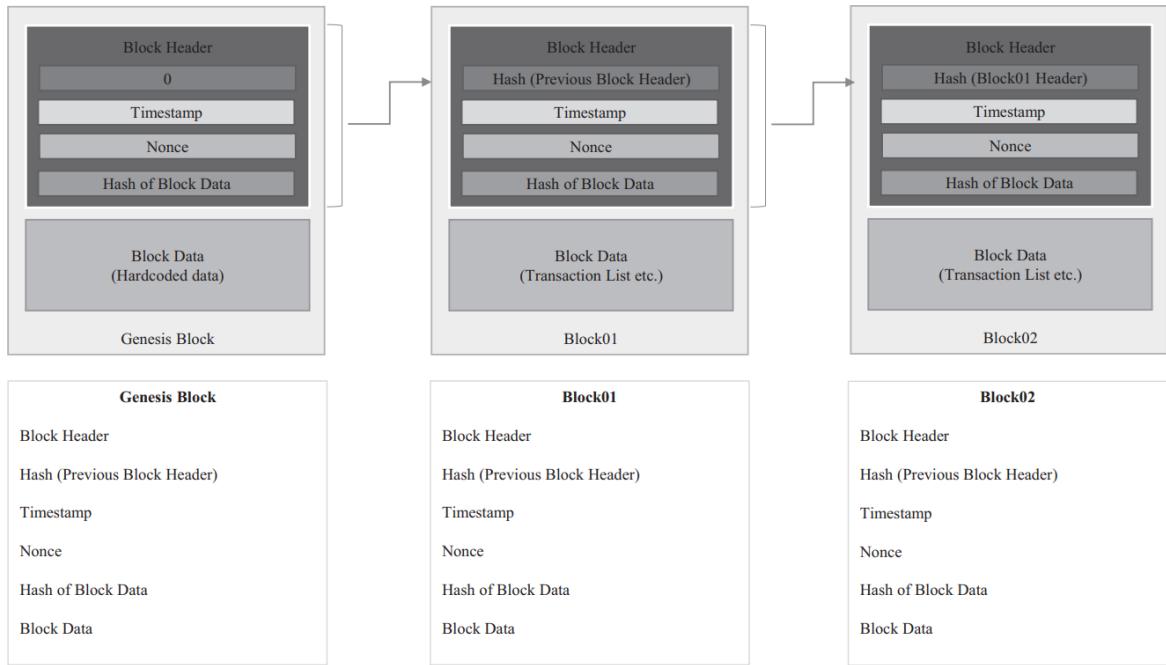
Các giao dịch giữa doanh nghiệp với nhau có thể tồn rất nhiều thời gian và tạo ra tắc nghẽn trong hoạt động, đặc biệt là khi có sự tham gia của các cơ quan quản lý và quản lý bên thứ ba. Tính minh bạch và các hợp đồng thông minh trong chuỗi khối làm cho các giao dịch kinh doanh như vậy nhanh hơn và hiệu quả hơn.

#### Kiểm tra nhanh hơn

Doanh nghiệp phải có khả năng tạo, trao đổi, lưu trữ và xây dựng lại các giao dịch điện tử một cách an toàn theo cách thức có thể kiểm tra được. Các bản ghi trong chuỗi khối là bất biến theo thời gian, có nghĩa là tất cả các bản ghi luôn được sắp xếp theo thời gian. Tính minh bạch của dữ liệu này giúp cho việc xử lý kiểm tra nhanh hơn hẳn.

### 1.3 Cách hoạt động của Blockchain

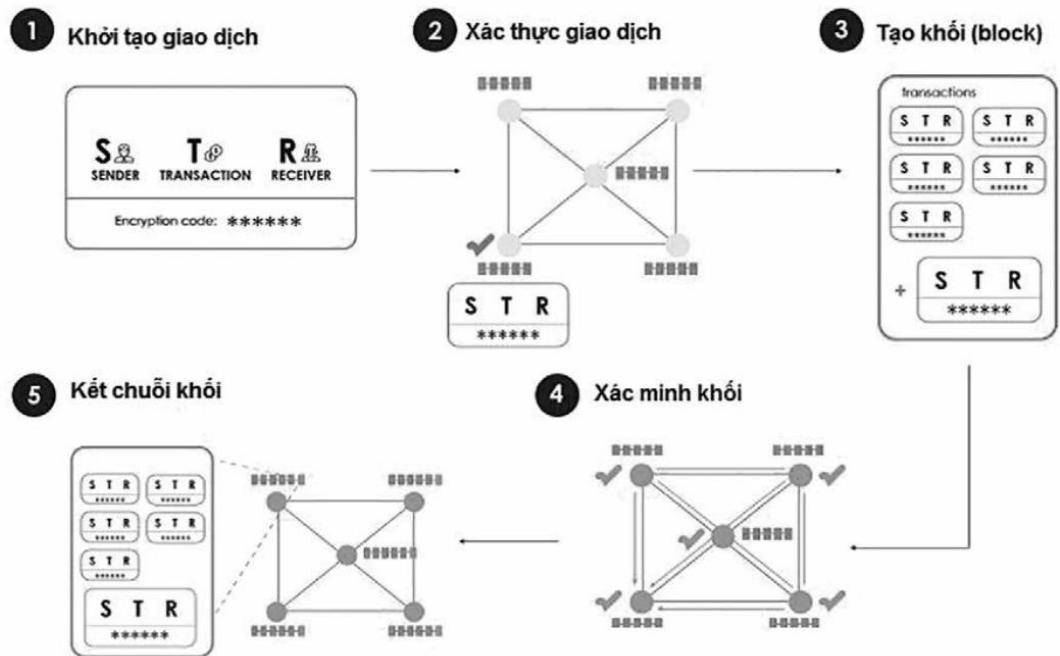
Dưới đây là cách các khối được liên kết với nhau [5]



1. Các khối được liên kết với nhau thông qua việc mỗi khối chứa một hàm băm của phần Header của khối trước đó.
2. Nếu một khối đã được tạo ra trước đó bị thay đổi, nó sẽ có một hàm băm khác.
3. Điều này đến lượt nó sẽ khiến tất cả các khối tiếp theo cũng có các hàm băm khác nhau vì chúng bao gồm hàm băm của khối trước đó.
4. Điều này giúp dễ dàng phát hiện và từ chối các khối đã thay đổi.
5. Điều này cho phép tạo một chuỗi các khối được kết nối, tức là chuỗi khối.

\* Băm là phương pháp áp dụng hàm băm cho dữ liệu, tính toán đầu ra duy nhất (được gọi là digest) cho đầu vào có kích thước bất kỳ (ví dụ: tệp, văn bản hoặc hình ảnh).

Về khái quát, có thể hình dung quy trình cơ bản của công nghệ Blockchain như trong Hình, bao gồm các bước[3]:



- (1) Khởi tạo giao dịch/Gửi yêu cầu: Người dùng gửi đi/tạo ra một giao dịch và chuyển nó lên mạng (thông điệp giao dịch bao gồm chi tiết địa chỉ công khai của Người nhận, giá trị của giao dịch và chữ ký số để chứng minh tính xác thực của giao dịch);
- (2) Xác thực giao dịch: Các nút mạng (máy tính/người dùng) nhận thông điệp; xác thực tính đúng đắn của thông điệp bằng cách giải mã chữ ký số. Giao dịch đã qua bước xác thực được đặt vào vùng chứa của các giao dịch chờ.
- (3) Tạo khối: Các giao dịch chờ này được đưa vào cùng với nhau trong một phiên bản cập nhật của sổ cái, được gọi là khối (block) bởi một trong những nút trong mạng. Tại một thời điểm xác định, nút mạng sẽ gửi khối này vào mạng để xác minh.
- (4) Xác minh khối: Những nút xác minh của mạng nhận được khối gửi đến cần xác minh và thực hiện việc xác minh thông qua một quy trình lặp mà yêu cầu tính đồng thuận của đa số trên mạng.
- (5) Kết chuỗi khối: Nếu tất cả các giao dịch được xác minh, khối mới được xâu chuỗi vào blockchain và trạng thái hiện thời của sổ cái được phát gửi (broadcast) vào mạng.

## 1.4 Cơ chế đồng thuận của Blockchain

Về cơ bản, Blockchain là cơ sở dữ liệu phân tán được thiết kế để lưu trữ, giao tiếp cũng như giao dịch mà không cần phải thông qua một cá nhân hoặc tổ chức. Phần lớn các Blockchain được xây dựng trên sự chia sẻ thông qua một mạng lưới các nút riêng lẻ phân tán hoạt động để cung cấp các giao dịch diễn ra trên mạng. Vì vậy mà Blockchain cần phải có một cơ chế để đảm bảo các nút đó được đồng bộ hóa, thống nhất với nhau để xem xét giao dịch, thay đổi nào là hợp pháp và được thêm vào Blockchain.

- Cơ chế đồng thuận là một cơ chế chịu lỗi được sử dụng trong các hệ thống máy tính và chuỗi khối để đạt được thỏa thuận mong muốn về một giá trị dữ liệu hoặc một trạng thái duy nhất của mạng giữa các qui trình phân bổ hoặc hệ thống đa tác nhân. Nó rất hữu ích trong việc lưu trữ hồ sơ so với các cơ chế khác. Sau đây là các loại cơ chế đồng thuận phổ biến:

- Proof of Work (Bằng chứng Công việc): Phổ biến trong Bitcoin, Ethereum, Litecoin,

Dogecoin và hầu hết các loại tiền mã hoá. Tiêu tốn khá nhiều năng lượng điện.

- Proof of Stake (Bằng chứng Cỗ phần): Phổ biến trong Decred, Peercoin và trong tương lai là Ethereum và nhiều loại tiền mã hoá khác. Phân cấp hơn, tiêu hao ít năng lượng và không dễ bị đe doạ.

- Delegated Proof-of-Stake (Uỷ quyền Cỗ phần): Phổ biến trong Steemit, EOS, BitShares. Chi phí giao dịch rẻ; có khả năng mở rộng; hiệu suất năng lượng cao.

Tuy

nhiên vẫn một phần hơi hướng tập trung vì thuật toán này lựa chọn người đáng tin cậy

để uỷ quyền.

- Proof of Authority (Bằng chứng Uỷ nhiệm): Đây là mô hình tập trung thường thấy trong POA.Network, Ethereum Kovan testnet. Hiệu suất cao, có khả năng mở rộng tốt.

- Proof-of-Weight (Bằng chứng Khối lượng / Càng lớn càng tốt): Phổ biến trong Algorand, Filecoin. Có thể tuỳ chỉnh và khả năng mở rộng tốt. Tuy nhiên quá trình thúc đẩy việc phát triển sẽ là một thử thách lớn.

- Byzantine Fault Tolerance (Đồng thuận chống gian lận / Tướng Byzantine bao vây

Blockchain): Phổ biến trong Hyperledger, Stellar, Dispatch, và Ripple. Năng suất cao;

chi phí thấp; có khả năng mở rộng. Tuy nhiên vẫn chưa thể tin tưởng hoàn toàn.

Thuật

toán này có 2 phiên bản là:

+ Practical Byzantine Fault Tolerance (Đồng thuận chống gian lận / Tướng

Byzantine bao vây Blockchain trong thực tế)

+ Federated Byzantine Agreement (Liên minh Byzantine cùng đồng thuận)

- Directed Acyclic Graphs (Thuật toán tô pô): Thường thấy trong Iota (công nghệ Tangle), Hashgraph, Raiblocks/Nano (công nghệ Block-lattice), là một đối thủ của Blockchain.

## 1.5 Ứng dụng của Blockchain

Công nghệ Blockchain có thể thay đổi nhiều hệ thống mà bạn gặp phải trong cuộc sống hàng ngày. Dưới đây là một số ví dụ thực tế [4]

### - Hợp đồng thông minh Smart Contract

Mọi ngành công nghiệp đều phụ thuộc nhiều vào hợp đồng. Chẳng hạn như các tổ chức tài chính, ngành bảo hiểm, lĩnh vực bất động sản, xây dựng, giải trí và pháp luật, sẽ đều có thể tận dụng công nghệ Blockchain cho việc cập nhật, quản lý, theo dõi và bảo mật các hợp đồng. Hợp đồng thông minh – những hợp đồng được nhúng với các câu lệnh if/then và được thực hiện mà không có sự tham gia của một bên trung gian nào – cũng sử dụng công nghệ Blockchain.

### - Xử lý thanh toán và tiền tệ

Ngay cả khi bạn không sử dụng Bitcoin – đồng tiền kỹ thuật số nổi tiếng sử dụng công nghệ Blockchain làm nền tảng, ảnh hưởng của Blockchain cũng không chỉ dừng lại ở đó.

Blockchain có khả năng tạo nên một cuộc cách mạng lớn trong hệ thống các công ty xử lý thanh toán. Nó có thể loại bỏ sự cần thiết phải có bên trung gian thứ 3, vốn rất phổ biến trong quy trình thanh toán hiện nay.

### - Quản lý chuỗi cung ứng

Bất cứ khi nào một tài sản nào đó thay đổi chủ sở hữu hoặc trạng thái tài sản, Blockchain sẽ là một sự lựa chọn lý tưởng để quản lý quá trình đó. Đó là lý do tại sao một số chuyên gia tin rằng Blockchain có thể trở thành “hệ thống vận hành chuỗi cung ứng”. Nó đã được Walmart và Trung tâm an toàn thực phẩm ở Bắc Kinh sử dụng để theo dõi chi tiết nguồn gốc trang trại, số lô, dữ liệu chế biến và nhà máy, ngày hết hạn, nhiệt độ lưu trữ và chi tiết vận chuyển đối với thịt lợn. Blockchain cho phép cập nhật trạng thái ngay lập tức và tăng tính bảo mật và tính minh bạch của chuỗi cung ứng. Nó cung cấp cho bất kỳ ngành nào cần theo dõi chuỗi cung ứng — cuối cùng là hầu hết các ngành — một hệ thống theo dõi tức thì, chính xác và không thể phủ nhận.

#### **- Bảo vệ tài sản**

Ngay cả khi bạn là nhạc sĩ, bạn muốn đảm bảo rằng bạn sẽ nhận được tiền bản quyền khi nhạc của mình được phát, hay chỉ đơn giản là khẳng định quyền sở hữu tài sản, công nghệ Blockchain có thể giúp bạn bảo vệ tài sản của mình bằng cách tạo hồ sơ không thể chối cãi về quyền sở hữu trong thời gian thực. Đó chính xác là dịch vụ mà Everledger — một công ty startup toàn cầu — nhắm đến, với việc sử dụng Blockchain và các hợp đồng thông minh. Cụ thể, được tạo ra để cải thiện các biện pháp chống hàng giả đối với dược phẩm, đồ xa xỉ, kim cương và đồ điện tử, BlockVerify cho phép các công ty đăng ký sản phẩm của riêng mình và tạo ra sự minh bạch cho chuỗi cung ứng.

#### **- Nhận dạng, hệ thống hồ sơ cá nhân và mật khẩu**

Chính phủ quản lý một lượng lớn dữ liệu cá nhân từ hồ sơ sinh/tử đến giấy chứng nhận kết hôn, hộ chiếu và dữ liệu điều tra dân số. Công nghệ Blockchain cung cấp một giải pháp hợp lý để quản lý tất cả một cách an toàn. Nhận dạng cá nhân là những gì mà Onename, một công ty startup Blockchain, muốn quản lý. Ngoài việc cung cấp dịch vụ để đăng ký và quản lý Blockchain ID, công ty còn cung cấp sản phẩm có tên Passcard mà họ dự định sẽ là khóa kỹ thuật số thay thế tất cả mật khẩu và ID cần thiết cho cá nhân, kể cả giấy phép lái xe. ShoCard là một hệ thống quản lý nhận dạng khác được sử dụng ngày nay, giúp các cá nhân và doanh nghiệp nhanh chóng xác nhận danh tính. Có nhiều trường hợp sử dụng thực tế khác cho công nghệ Blockchain cho cuộc sống hàng ngày và hoạt động kinh doanh của chúng ta.

## 1.6 Nguyên lý mã hóa của Blockchain

Để có thể thực hiện các giao dịch trên blockchain, bạn cần một ví tiền điện tử, đây là một chương trình phần mềm sẽ cho phép bạn lưu trữ và trao đổi các đồng Bitcoin của bạn. Vì chỉ có bạn mới có thể chi tiêu các đồng Bitcoin của mình do vậy mỗi chiếc ví tiền điện tử này được bảo vệ bằng một phương pháp mã hóa đặc biệt sử dụng một cặp khóa bảo mật duy nhất: khóa riêng tư (private key) và khóa công khai (public key). [4]

Nếu một thông điệp được mã hóa bằng một khóa công khai cụ thể thì chỉ chủ sở hữu của khóa riêng tư là một cặp với khóa công khai này mới có thể giải mã và đọc nội dung thông điệp. Khi Thành muốn gửi Bitcoin, anh ta cần phát một thông điệp được mã hóa bằng khóa riêng của ví điện tử của mình, vì thế anh ta chỉ có thể dùng Bitcoin mà anh ta sở hữu vì Thành là người duy nhất biết khóa riêng tư của anh cần thiết để mở ví điện tử của mình. Mỗi nút trong mạng có thể kiểm tra chéo các yêu cầu giao dịch được gửi từ Thành là chính xác hay không bằng cách giải mã thông điệp yêu cầu giao dịch bằng khóa công khai của Thành.

Khi mã hóa một yêu cầu giao dịch bằng khóa riêng tư từ ví của bạn tức là bạn đang tạo ra một chữ ký điện tử được các máy tính trong mạng lưới blockchain sử dụng để kiểm tra chủ thẻ gửi và tính xác thực của giao dịch. Chữ ký này là một chuỗi văn bản và nó là kết quả của việc kết hợp yêu cầu giao dịch và khóa riêng tư của bạn.



Nếu bạn thay đổi một ký tự đơn trong thông điệp yêu cầu giao dịch này thì chữ ký điện tử sẽ thay đổi theo vì vậy không có kẻ tấn công tiềm tàng nào có thể thay đổi yêu cầu giao dịch của bạn hoặc thay đổi số lượng Bitcoin mà bạn đang gửi.

## **2. ETHEREUM**

### **2.1 Định nghĩa Ethereum**

Ethereum là một nền tảng công nghệ blockchain mã nguồn mở, công khai và phân quyền mà cho phép chạy các ứng dụng phi tập trung (Dapp) trên nền tảng của mình. Mạng lưới Blockchain của Ethereum là hệ thống siêu máy (server) với hàng trăm nghìn thiết bị được kết nối trên toàn cầu hoạt động để duy trì trạng thái điện toán của nó. [10]

Hoặc theo Wiki [9]: Ethereum (ETH) là một nền tảng điện toán có tính chất phân tán, công cộng, mã nguồn mở dựa trên công nghệ Blockchain. Nó có tính năng hợp đồng thông minh (kịch bản), tạo thuận lợi cho các thỏa thuận hợp đồng trực tuyến. Nền tảng này bao gồm một máy ảo hoàn toàn Turing - Ethereum Virtual Machine (EVM), có thể thực thi các kịch bản bằng cách sử dụng một mạng lưới máy tính Ethereum. Ethereum cũng cung cấp một loại tiền mã hóa gọi là "Ether", có thể được chuyển giữa các tài khoản và được sử dụng để trả công cho các thợ đào giúp thực hiện việc tính toán. "Gas" là một cơ chế giá giao dịch nội bộ, được sử dụng để giảm thiểu giao dịch rác (spam) và phân bổ các nguồn lực trên mạng lưới.

### **2.2 Kiến trúc của Ethereum:**

#### **a) Tài khoản Ethereum:**

Mỗi tài khoản Ethereum được đại diện bởi 20 ký tự. Các thông số sau được lưu trong dữ liệu trạng thái (state) của Ethereum cho mỗi tài khoản:

- Số nonce, để đảm bảo mỗi giao dịch chỉ được xử lý một lần.
- Số dư tài khoản
- Mã nguồn hợp đồng (nếu có)
- Phần lưu trữ của tài khoản (mặc định là trống)

Các giao dịch giữa các tài khoản được trả tiền bằng Ether. Có hai loại tài khoản: Tài khoản ngoại vi được quản lý bởi khóa riêng tư, và tài khoản hợp đồng được quản lý bởi mã hợp đồng. Tài khoản ngoại vi không chứa mã hợp đồng, có thể gửi thông điệp đi bằng cách tạo và ký kết một giao dịch, giống như tài khoản Bitcoin. Về phía tài khoản hợp đồng, mỗi khi nó nhận được 1 thông điệp, mã hợp đồng sẽ chạy và cho phép đọc và

ghi vào phần lưu trữ của nó, kèm theo việc gửi thông điệp đi và tạo ra hợp đồng khác lần lượt.

Lưu ý rằng "hợp đồng" trong Ethereum không phải là một cái gì đó phải "hoàn thành" hoặc "tuân thủ". Thay vào đó, nó giống như các "thực thể tự trị" sống bên trong môi trường Ethereum, luôn thực hiện một đoạn mã cụ thể khi được tác động bởi một thông điệp hoặc giao dịch, và có quyền kiểm soát trực tiếp Ether và dữ liệu trong phần lưu trữ của nó. [6]

### b) Giao dịch và thông điệp

Thuật ngữ "giao dịch" được sử dụng để chỉ tới gói dữ liệu mà bao gồm thông điệp. Một giao dịch bao gồm:

- Tài khoản nhận thông điệp
- Chữ ký tài khoản gửi
- Số Ether chuyển đi
- Trường dữ liệu tùy chọn
- Giá trị STARTGAS, đại diện cho số lượng tối đa các bước tính toán thực hiện giao dịch được phép thực hiện
- Giá trị GASPRICE, đại diện cho khoản phí mà người gửi trả cho mỗi bước tính toán

Ba trường dữ liệu đầu tiên là các trường tiêu chuẩn trong các loại tiền mã hóa. Trường dữ liệu không có chức năng theo mặc định, nhưng EVM có mã opcode mà hợp đồng có thể truy cập vào dữ liệu. Ví dụ: Nếu một hợp đồng đang hoạt động như là một dịch vụ đăng ký tên miền trên blockchain, thì nó có thể nhận dữ liệu được truyền cho nó như là có chứa hai trường: Trường đầu tiên là tên miền đăng ký, trường thứ hai là địa chỉ IP để đăng ký với tên miền đó. Hợp đồng sẽ đọc các giá trị này từ dữ liệu thông điệp và đưa chúng vào lưu trữ một cách hợp lý.

Các trường STARTGAS và GASPRICE rất quan trọng để chống tấn công từ chối dịch vụ. Để ngăn chặn các vòng vô hạn hoặc các lăng phí điện toán khác trong mã, mỗi giao dịch được yêu cầu để đặt một giới hạn số bước tính toán của việc thực thi mã nó có thể sử dụng. Đơn vị cơ bản của tính toán là "gas". Thông thường, một bước tính toán

tốn 1 gas, nhưng một số mã tốn nhiều tiền hơn vì chúng cần nhiều tính toán hơn, hoặc tăng lượng dữ liệu phải lưu giữ vào dữ liệu state. Ngoài ra, có một khoản phí là 5 gas cho mỗi byte trong dữ liệu giao dịch. Mục đích của hệ thống phí là yêu cầu một kẻ tấn công phải trả một cách tương xứng cho mọi nguồn lực mà họ tiêu thụ, bao gồm tính toán, băng thông và lưu trữ.

### c) Thông điệp

Một hợp đồng có khả năng gửi "thông điệp" đến các hợp đồng khác. Thông điệp là các đối tượng ảo không bao giờ được serialize và chỉ tồn tại trong môi trường thực thi Ethereum. Một thông điệp chứa:

- Tài khoản gửi tin nhắn (addr)
- Tài khoản nhận tin nhắn
- Số lượng Ether để truyền tải cùng với thông điệp
- Trường dữ liệu tùy chọn
- Giá trị STARTGAS

### d) Blockchain và Khai thác

Blockchain của Ethereum có nhiều điểm tương tự như của Bitcoin, tuy nhiên có một số khác biệt sau: Khối Ethereum chứa một bản sao của cả danh sách giao dịch và trạng thái gần nhất. Bên cạnh đó, số khối và độ khó cũng được lưu trữ trong khối. Thuật toán xác nhận khối cơ bản trong Ethereum như sau:

- Kiểm tra tham chiếu khối trước đó tồn tại và hợp lệ.
- Kiểm tra dấu thời gian của khối lớn hơn dấu thời gian của khối được tham chiếu trước và nhỏ hơn 15 phút trong tương lai.
- Kiểm tra số khối, độ khó, gốc giao dịch, uncle gốc và giới hạn gas là hợp lệ.
- Kiểm tra xem chứng minh công việc trên khối là hợp lệ.
- Đặt S[0] là trạng thái cuối ở khối trước đó.
- Đặt TX là danh sách giao dịch của khối, với n giao dịch. Đối với tất cả i từ 0...n-1, đặt S[i+1] = APPLY(S[i],TX[i]). Nếu bất kỳ ứng dụng nào trả về lỗi hoặc nếu tổng

lượng khí tiêu thụ trong khối cho đến thời điểm này vượt quá GASLIMIT, trả lại lỗi.  
(APPLY là một hàm thay đổi trạng thái S khi có giao dịch).

- Đặt S\_FINAL là S[n], nhưng thêm phần thưởng cho thợ mỏ.

- Kiểm tra xem gốc cây Merkle của trạng thái S\_FINAL bằng với gốc trạng thái cuối cùng được cung cấp trong tiêu đề khối. Nếu có, khối này là hợp lệ; Nếu không, nó không hợp lệ.

Cách tiếp cận có thể có vẻ không hiệu quả ở cái nhìn đầu tiên, bởi vì nó cần phải lưu trữ toàn bộ trạng thái với mỗi khối, nhưng hiệu quả thực tế là ngang với Bitcoin. Lý do là trạng thái được lưu trữ trong cấu trúc cây, và sau mỗi khối chỉ cần một phần nhỏ của cây phải thay đổi. Do đó, nói chung, giữa hai khối liền kề, phần lớn cây phải giống nhau, và do đó dữ liệu có thể được lưu trữ một lần và được tham chiếu hai lần bằng cách sử dụng các con trỏ (ví dụ: hash các cây con). Một loại cây đặc biệt được gọi là "cây Patricia" được sử dụng để thực hiện việc này, bao gồm sửa đổi khái niệm cây Merkle cho phép chèn và xóa các nút một cách hiệu quả. Ngoài ra, vì tất cả các thông tin trạng thái là một phần của khối cuối cùng nên không cần lưu trữ toàn bộ lịch sử blockchain đối với các nút không có khả năng lưu trữ nhiều.

### 3. SMART CONTRACT

#### 3.1 Định nghĩa Smart Contract

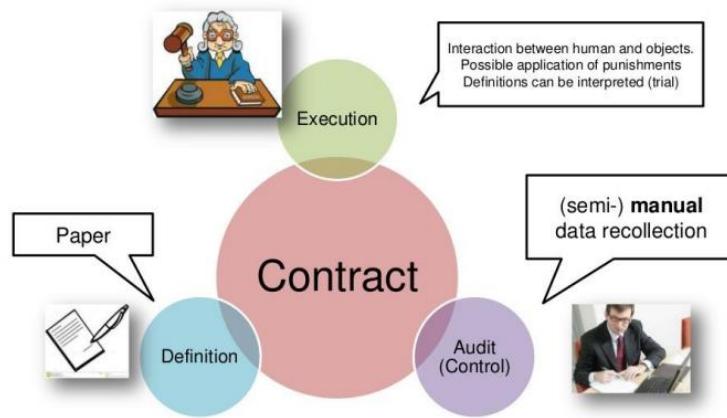
Hợp đồng thông minh Smart Contract là một tập lệnh được neo trên chuỗi khối hoặc cơ sở hạ tầng phân tán tương tự. Ngay khi nó được kích hoạt bởi một giao dịch chuỗi khối và được xác thực trên mạng, các hành động được xác định trước sẽ được thực thi. Vì các điều kiện của hợp đồng thông minh được lưu trữ minh bạch trên chuỗi khối nên nó sẽ luôn hoạt động theo ý định của tất cả các bên, điều này có thể làm giảm các vấn đề về lòng tin giữa các bên liên quan. Hợp đồng thông minh là tập lệnh phần mềm, giống như tập lệnh chạy trên các ứng dụng không phải blockchain[11]. Hay ngắn gọn lại, “Hợp đồng thông minh” là một thuật ngữ được sử dụng để mô tả những dòng code tin học giúp tự động thực thi tất cả hoặc một phần của thỏa thuận và được lưu trữ trên nền tảng dựa trên công nghệ chuỗi khối[13].

Hợp đồng thông minh là một tập hợp các lời hứa, được chỉ định ở dạng kỹ thuật số, bao gồm các giao thức trong đó các bên thực hiện những lời hứa này : “Hợp đồng thông

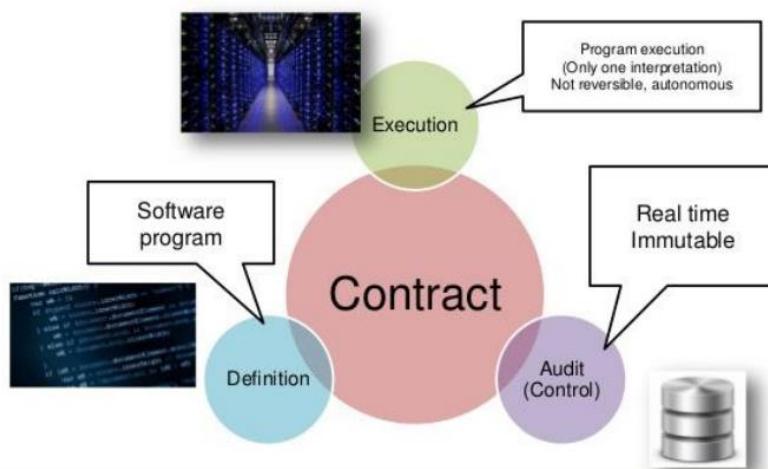
minh sử dụng công nghệ chuỗi khối có thể cho phép một hệ thống giao dịch kỹ thuật số giữa những người dùng mạng trong cơ sở dữ liệu phi tập trung”[14].

### 3.2 Sự khác nhau giữa Hợp đồng thông minh (Smart contract) và Hợp đồng truyền thống

Chúng ta cùng xét 2 hình ảnh dưới để thấy sự khác nhau giữa hai hợp đồng truyền thống và hợp đồng thông minh [14].



Đối với hợp đồng truyền thông thường, hợp đồng sẽ được định nghĩa trên giấy tờ. Sự kiểm tra, kiểm soát sẽ được thực hiện bằng việc thu thập dữ liệu thủ công và sẽ được thực thi bởi con người, có áp dụng các hình phạt và định nghĩa có thể được giải thích.

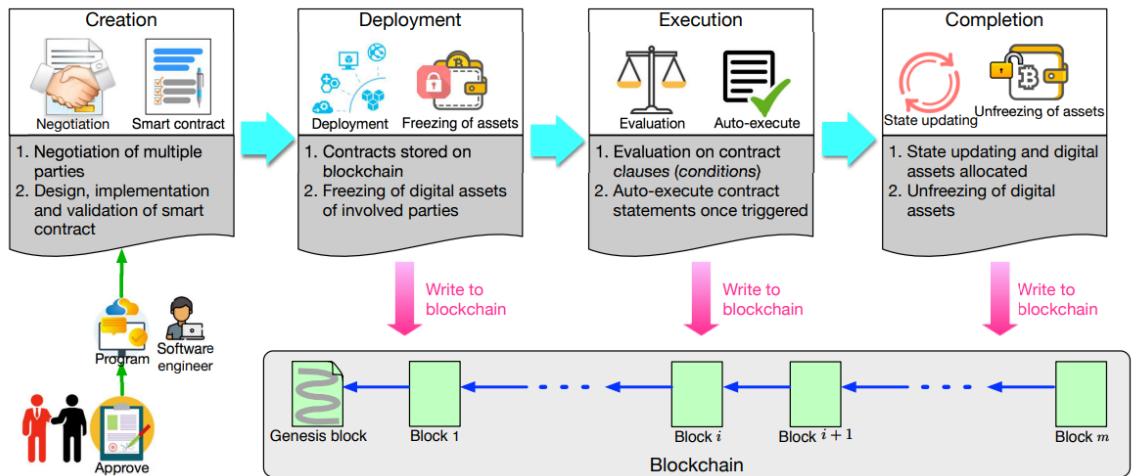


Ngược lại, đối với hợp đồng thông minh Smart Contract thì hợp đồng lúc này sẽ được định nghĩa bởi các chương trình phần mềm hay được hiểu là qua code. Sự kiểm

tra, kiểm soát sẽ được thực hiện thông qua thời gian thực bất biến. Cuối cùng việc thực thi sẽ do chương trình chạy, chỉ có thể được định nghĩa một lần và không thể đảo ngược.

### 3.3 Cách hoạt động của Smart Contract

Để hiểu rõ về cách hoạt động của Hợp đồng thông minh, ta sẽ xem sơ đồ vòng đời của nó gồm 4 giai đoạn: [15]



**1) Tạo hợp đồng thông minh.** Một số bên tham gia đàm phán trước tiên về nghĩa vụ, quyền và những điều cấm trong hợp đồng. Sau nhiều vòng thảo luận và đàm phán, một thỏa thuận có thể đạt được. Luật sư hoặc cố vấn sẽ giúp các bên soạn thảo một thỏa thuận hợp đồng ban đầu. Sau đó, các kỹ sư phần mềm chuyển đổi thỏa thuận này được viết bằng ngôn ngữ tự nhiên thành một hợp đồng thông minh được viết bằng ngôn ngữ máy tính bao gồm ngôn ngữ khai báo và ngôn ngữ quy tắc dựa trên logic. Tương tự như sự phát triển của phần mềm máy tính, quy trình chuyển đổi hợp đồng thông minh bao gồm thiết kế, triển khai và xác nhận (nghĩa là thử nghiệm). Điều đáng nói là việc tạo ra các hợp đồng thông minh là một quá trình lặp đi lặp lại liên quan đến nhiều vòng đàm phán và lặp đi lặp lại. Trong khi đó, nó cũng liên quan đến nhiều bên, chẳng hạn như các bên liên quan, luật sư và kỹ sư phần mềm.

**2) Triển khai hợp đồng thông minh.** Sau đó, các hợp đồng thông minh đã được xác thực có thể được triển khai cho các nền tảng trên các chuỗi khối. Các hợp đồng được lưu trữ trên chuỗi khối không thể sửa đổi do tính bất biến của chuỗi khối. Bất kỳ sự sửa đổi nào cũng yêu cầu tạo ra một hợp đồng mới. Sau khi hợp đồng thông minh được triển khai trên chuỗi khối, tất cả các bên có thể truy cập hợp đồng thông qua chuỗi khối. Hơn

nữa, tài sản kỹ thuật số của cả hai bên tham gia trong hợp đồng thông minh bị khóa thông qua việc đóng băng các ví kỹ thuật số tương ứng. Ví dụ: các giao dịch chuyển tiền xu (đến hoặc đi) trên các ví liên quan đến hợp đồng đều bị chặn. Khi đó, các bên có thể được xác định bằng ví kỹ thuật số của họ.

**3) Thực hiện hợp đồng thông minh.** Sau khi triển khai hợp đồng thông minh, các điều khoản hợp đồng đã được theo dõi và đánh giá. Sau khi đạt được các điều kiện hợp đồng (ví dụ: tiếp nhận sản phẩm), các quy trình (hoặc chức năng) hợp đồng sẽ tự động được thực hiện. Điều đáng chú ý là một hợp đồng thông minh bao gồm một số câu lệnh khai báo với các kết nối logic. Khi một điều kiện được kích hoạt, câu lệnh tương ứng sẽ được thực thi tự động, do đó, một giao dịch được thực hiện và xác thực bởi những người khai thác trong chuỗi khối. Các giao dịch đã cam kết và trạng thái cập nhật đã được lưu trữ trên các chuỗi khối sau đó.

**4) Hoàn thành hợp đồng thông minh.** Sau khi hợp đồng thông minh được thực hiện, các trạng thái mới của tất cả các bên liên quan sẽ được cập nhật. Theo đó, các giao dịch trong quá trình thực hiện hợp đồng thông minh cũng như trạng thái cập nhật được lưu trữ trong chuỗi khối. Trong khi đó, các tài sản kỹ thuật số đã được chuyển từ bên này sang bên khác (ví dụ: chuyển tiền từ người mua sang nhà cung cấp). Do đó, tài sản kỹ thuật số của các bên liên quan đã được mở khóa. Hợp đồng thông minh sau đó đã hoàn thành toàn bộ vòng đời. Điều đáng nói là trong quá trình triển khai, thực hiện và hoàn thành hợp đồng thông minh, một chuỗi giao dịch đã được thực hiện (mỗi giao dịch tương ứng với một tuyên bố trong hợp đồng thông minh) và được lưu trữ trong chuỗi khối. Do đó, cả ba giai đoạn này đều cần ghi dữ liệu vào chuỗi khối như trong Hình.

### **3.4 Ưu điểm và hạn chế của Smart Contract**

#### **a) Ưu điểm**

Smart Contract có rất nhiều ưu điểm, và trong đó đây là 5 ưu điểm chính [12]:

##### **- Độ chính xác:**

Một trong những lợi thế mà các tổ chức kinh doanh sẽ được hưởng lợi từ việc thực hiện các hợp đồng thông minh là độ chính xác. Như đã giải thích trong quy trình thiết lập hợp đồng thông minh, tất cả thông tin liên quan đến hợp đồng được thể hiện ở định

dạng có điều kiện, sử dụng câu lệnh if-then. Chẳng hạn, khi đặt mua một gói dịch vụ cụ thể nếu khách hàng x thanh toán x đơn vị y thì ngay lập tức ghi có số tiền cho người nhận đồng thời mở gói dịch vụ cho khách hàng x. Vì phần lớn các hợp đồng đòi hỏi phải trao đổi tiền mặt. Sau đó, các hợp đồng thông minh có thể được đồng bộ hóa với các loại tiền điện tử như Etherium, Lite Coin hoặc bitcoin, trong số những loại khác, một khía cạnh sẽ nâng cao hơn nữa tính mạnh mẽ, chính xác và hiệu suất của toàn bộ hệ thống. Sự thể hiện của tất cả các điều khoản và điều kiện trong một hợp đồng thông minh phải rõ ràng và chính xác. Về cơ bản, đây là một yêu cầu quan trọng vì lỗi giao dịch có thể bắt nguồn từ bất kỳ thiếu sót nào. Do đó, triển lâm tự động hóa trong hợp đồng thông minh tránh được phần lớn các vấn đề được tìm thấy trong hợp đồng truyền thống

#### **- Giao tiếp rõ ràng và minh bạch**

Hầu như, các điều khoản và điều kiện của các điều khoản và điều kiện hợp đồng trở nên rõ ràng đối với những người dùng mạng khác nhau của chuỗi khối cụ thể. Do đó, một khi hợp đồng được thiết lập, những thay đổi không thể dễ dàng thực hiện. Mỗi giao dịch của một trong hai bên trong hợp đồng được theo dõi và kiểm soát bởi các nút mạng khác trong chuỗi khôi. Kết quả là, tính minh bạch được thúc đẩy và các vấn đề gian lận được loại bỏ. Trong thời kỳ hiện đại, nhiều trường hợp đã được báo cáo, theo đó tổ chức bị buộc tội lừa dối khách hàng và không cung cấp cho họ giá trị đồng tiền của họ. Như đã nói ở trên, mỗi lần bán hàng hóa hoặc dịch vụ của một tổ chức đều dẫn đến một hợp đồng có thể có hoặc không có hiệu lực pháp lý. Tuy nhiên, trong nhiều trường hợp, một hoặc nhiều bên trong hợp đồng có thể vi phạm các điều khoản và điều kiện của hợp đồng. Trong trường hợp bán hàng, một tổ chức có thể tính phí quá cao cho khách hàng hoặc có thể rút ngắn thời gian của gói dịch vụ đã thỏa thuận mà không cần thông báo cho khách hàng. Việc thực hiện các hợp đồng thông minh đưa mọi chi tiết của hợp đồng ra ánh sáng. Không giống như trong hợp đồng truyền thống, nơi tổ chức sẽ phải sử dụng khung pháp lý làm trung gian, trong thế giới ảo, tất cả những gì cần thiết là các nút khác trong mạng, những người được giao nhiệm vụ đảm bảo rằng mỗi giao dịch liên quan đến hợp đồng là chính xác và hợp lệ.

#### **- Tốc độ và hiệu quả**

Về cơ bản, các hợp đồng thông minh không dựa vào sự can thiệp của con người và việc triển khai chúng được hướng dẫn và giám sát bởi các nút khác trong mạng chuỗi khối. Do đó, một khi hợp đồng được kích hoạt, hợp đồng theo kịch bản sẽ tự thực hiện. Điều này thường đạt được thông qua việc sử dụng các sự kiện kích hoạt khi viết kịch bản liên hệ. Chẳng hạn, sự kiện kích hoạt có thể là ngày, giờ hoặc thậm chí là hoạt động do một bên trong hợp đồng khởi xướng, chẳng hạn như chuyển một số đơn vị tiền điện tử nhất định từ ví của khách hàng sang ví của công ty. Khi một sự kiện kích hoạt xảy ra, hợp đồng sẽ bắt đầu tự thực hiện. Chẳng hạn, đối với các tổ chức dựa trên đăng ký trực tuyến, sau khi nhận được một đơn vị tiền điện tử cụ thể, thì đăng ký cho khách hàng sẽ được tự động gia hạn.

Không giống như trong các hợp đồng truyền thống kém hiệu quả hơn và yêu cầu một số hình thức xác minh của con người, ở đây, việc xác minh xem số tiền chính xác đã được thanh toán hay chưa và liệu tiêu mục, dịch vụ và các khía cạnh liên quan có được cung cấp cho số hay không được xác định bởi các nút trong mạng blockchain. Như vậy, không còn sự phụ thuộc vào hệ thống đã phát triển của tổ chức để xác định hợp đồng với khách hàng. Tổ chức này cũng không có quyền chủ quyền đối với các giao dịch cũng như đối với thỏa thuận hợp đồng với các đối tác. Mỗi hợp đồng được nhắm mục tiêu như một thực thể riêng biệt và mỗi giao dịch, bất kể nguồn gốc của nó, đều được xác thực trước tiên. Hơn nữa, điều này dẫn đến một cách thực hiện hợp đồng nhanh chóng, linh hoạt và mạnh mẽ

### **- Bảo mật**

Hợp đồng thông minh có một trong những biện pháp bảo mật cao nhất. Các hợp đồng thông minh được thực hiện thông qua công nghệ chuỗi khối đòi hỏi phải sử dụng mạng phi tập trung được tạo bởi các bên không tin cậy. Thực tế là các bên trong mạng không tin tưởng khiến họ phải kiểm tra lẫn nhau để đảm bảo mỗi giao dịch được thực hiện hiệu quả và có một thế giới quan thống nhất về trạng thái của tất cả các giao dịch. Một lần nữa, công nghệ chuỗi khối được thực hiện thông qua các kỹ thuật mật mã. Công nghệ này yêu cầu mã hóa dữ liệu cao và sử dụng cả khóa riêng và khóa chung để đọc các giao dịch trong mỗi chuỗi khối, cũng như thực hiện bất kỳ giao dịch nào. Thực tế là trước khi bất kỳ nút nào thực hiện giao dịch, giao dịch trước tiên phải được xác thực bởi tất cả các nút trên mạng chuỗi khối giúp tăng cường tính bảo mật của công nghệ thông minh.

Việc sử dụng các kỹ thuật mã hóa có thể tăng cường đáng kể tính bảo mật của liên lạc và trao đổi dữ liệu . Do đó, bất kỳ hợp đồng nào được thực hiện theo cách mã hóa đều tăng cường tính bảo mật của giao dịch và ngăn chặn mọi hoạt động độc hại có thể được lan truyền để thay đổi trình tự thực hiện hoặc thực hiện các giao dịch không hợp lệ.

#### **- Giảm chi phí**

Về cơ bản, các nhà quản lý kinh doanh hàng đầu được giao trách nhiệm đưa ra các chiến lược và cách giảm chi phí trong một tổ chức. Mục đích chính của việc thành lập doanh nghiệp kinh doanh là để tạo ra lợi nhuận; do đó, tất cả các hoạt động trong một tổ chức phải được hiểu theo cách thúc đẩy việc đạt được các mục tiêu của công ty, cũng như tối đa hóa lợi ích của các cổ đông. Trong thế giới gần đây đã chứng kiến một cuộc cách mạng công nghệ rộng lớn, sự thành công của các doanh nghiệp kinh doanh phụ thuộc vào khả năng theo kịp các công nghệ thịnh hành và áp dụng các biện pháp đảm bảo cũng như kỹ thuật giúp tăng năng suất và hiệu suất của nhân viên.

Việc triển khai các hợp đồng thông minh qua công nghệ chuỗi khối giúp cắt giảm nhu cầu về người trung gian, chẳng hạn như nhân viên pháp lý. Điều này hỗ trợ trong việc giảm chi phí tổ chức tổng thể và tối đa hóa tỷ suất lợi nhuận của một tổ chức. Trong trường hợp các tập đoàn đa quốc gia giải quyết một số lượng lớn hợp đồng hàng ngày hoặc hàng tuần, việc triển khai các liên hệ thông minh với các đối tác kinh doanh và khách hàng của mình có thể hỗ trợ rất nhiều trong việc giảm các chi phí khác nhau phát sinh trong các hình thức hợp đồng truyền thống. Các hợp đồng có thể tăng cường hơn nữa hiệu quả của tổ chức, đây là một thành phần quan trọng cho sự thành công của tổ chức và tăng hiệu suất. Tuy nhiên, điều quan trọng cần lưu ý là mặc dù các khía cạnh bảo mật, giảm chi phí và hiệu quả liên quan đến hợp đồng thông minh, nhưng hợp đồng thông minh không phải lúc nào cũng hoàn hảo, và do đó có thể có sai sót. Chẳng hạn, chất lượng và việc thực hiện hợp đồng phụ thuộc nhiều vào đầu vào, về cơ bản là phiên bản được mã hóa của hợp đồng. Do đó, nếu có sai sót trong việc thiết lập hợp đồng thông minh, những sai sót đó có thể gây ra các tác động bất lợi cũng như chất lượng kém của đầu ra được tạo ra.

#### **b) Hạn chế**

Mặc dù có nhiều ưu điểm khác nhau từ việc triển khai hợp đồng thông minh, nhưng điều quan trọng cần lưu ý là hợp đồng thông minh cũng còn có nhiều hạn chế, nhược điểm của hợp đồng thông minh hạn chế việc ứng dụng chúng trong các tình huống thực tế khác nhau. [12]

### - Tính bất biến

Về cơ bản, vì các hợp đồng thông minh được viết dưới dạng một đoạn mã nên sau khi được thiết lập, các liên hệ không thể dễ dàng sửa đổi. Trong các hợp đồng truyền thống, việc sửa đổi các điều khoản và điều kiện thường được sử dụng, đặc biệt là trong các hợp đồng dài hạn mà việc thực hiện phụ thuộc vào động lực thực tế và các điều kiện liên tục thay đổi. Do tính cứng nhắc thể hiện trong các hợp đồng thông minh sau khi được thiết lập, điều này dẫn đến một loạt các vấn đề thực tế liên quan đến việc dễ dàng sửa đổi các điều khoản hợp đồng tùy thuộc vào các tình huống khác nhau.

Các hợp đồng thông thường có các điều khoản cho phép hủy bỏ, nhúng và sửa đổi hợp đồng. Việc thực hiện các hợp đồng thông minh. Ở một mức độ lớn hơn, làm cho nó thực sự không thể đạt được các mục tiêu tương tự. Tuy nhiên, các hành động khác nhau có thể được thực hiện để bao gồm các khía cạnh sửa đổi và hủy bỏ hợp đồng. Ví dụ, một lối thoát hiểm có thể được bao gồm trong hợp đồng được mã hóa. Cửa thoát hiểm có thể được sử dụng để cho phép sửa đổi các điều khoản của hợp đồng, nhằm phục vụ cho các hợp đồng thực tế được đặc trưng bởi tính năng động rộng lớn. Tuy nhiên, việc triển khai như vậy trong các thỏa thuận thông minh có thể làm tổn hại đến bộ máy bảo mật và do đó có thể yêu cầu thắt chặt hơn nữa các biện pháp kiểm soát giao dịch để đảm bảo rằng lối thoát không được sử dụng để bắt đầu giao dịch không hợp lệ hoặc các giao dịch nhằm mục đích thao túng trái phép hồ sơ. do sự phức tạp của hợp đồng thông minh và công nghệ chuỗi khối nói chung, đảm bảo rằng quyền phù hợp được cấp cho đúng nút và tất cả các nút có thể giám sát việc sửa đổi của hợp đồng có thể khá phức tạp nhưng cần thiết.

### - Bí mật hợp đồng

Hầu hết, công nghệ chuỗi khối đòi hỏi phải chia sẻ hợp đồng thông minh trên tất cả các nút trong mạng chuỗi khối, vì tất cả giao dịch được ghi lại trên sổ cái chung bằng cách sử dụng các quyền được mã hóa trong mỗi nút. Về cơ bản, công nghệ chuỗi khối đòi hỏi phải sử dụng tính ẩn danh, theo đó tất cả những người tham gia trong mạng chuỗi khối đều ẩn danh và được bảo mật. Tuy nhiên, không có bảo đảm cho việc thực hiện

hợp đồng. Điều này là do mặc dù các nút ẩn danh trong hoạt động của chúng, nhưng số cái được duy trì ở chế độ công khai và do đó, các giao dịch có thể nhìn thấy được và không có sự bảo mật nào như vậy. Buterin giải thích rằng đây là một lĩnh vực cần được tập trung vì mặc dù các nút là ẩn danh, nhưng việc duy trì số cái công khai trong môi trường phân tán dẫn đến mất quyền riêng tư.

Mặc dù bản chất của các hợp đồng thông minh là duy trì một số cái công khai hiển thị cho tất cả các bên trong mạng và để theo dõi tính hợp lệ và chính xác của các loại thuế, nhưng cũng cần phải phát triển một giao thức, có thể hỗ trợ xác minh các giao dịch mà không nhất thiết phải đọc nội dung của giao dịch. Điều này là do mặc dù những người tham gia và nguồn gốc của giao dịch có thể được ẩn danh, nhưng nội dung thì không; và trên thực tế, mỗi nút có thể đọc và truy cập nội dung giao dịch. Điều quan trọng là phải phát triển các biện pháp để hạn chế các vấn đề về quyền riêng tư này vì bảo mật không chỉ liên quan đến ẩn danh và mã hóa, mà còn đòi hỏi phải đảm bảo nội dung của giao dịch được bảo vệ khỏi sự truy cập của các bên khác. Như vậy, khía cạnh này của hợp đồng thông minh vẫn chưa được giải quyết đầy đủ. Trên mạng blockchain tăng cường bảo mật của công nghệ thông minh. Mã hóa dữ liệu và đặc biệt, việc sử dụng các kỹ thuật mật mã có thể tăng cường đáng kể tính bảo mật của truyền thông và trao đổi dữ liệu. Do đó, bất kỳ hợp đồng nào được thực hiện theo cách mã hóa đều tăng cường tính bảo mật của giao dịch và ngăn chặn mọi hoạt động độc hại có thể được lan truyền để thay đổi trình tự thực hiện hoặc thực hiện các giao dịch không hợp lệ.

### **- Vấn đề pháp lý và khả năng thực thi**

Theo truyền thống, việc thiết lập một hợp đồng có hiệu lực bao gồm nhiều cấu trúc khác nhau, khiến nó có hiệu lực pháp lý. Các đặc điểm chính của hợp đồng có hiệu lực pháp lý là: đề nghị của một bên hoặc các bên, sự chấp nhận của bên hoặc các bên kia, một lời hứa, sự cân nhắc và năng lực pháp lý lẫn nhau và trong một số hợp đồng, một văn bản. Mặc dù các yếu tố này của hợp đồng rất quan trọng, nhưng một số yếu tố này không áp dụng được cho hợp đồng thông minh.

Ví dụ: lĩnh vực tài chính thể hiện các quy định rộng lớn của chính phủ và các quyền và giấy phép cụ thể được yêu cầu đối với một biểu mẫu để tham gia vào các giao dịch thực hiện số cái chung. Tuy nhiên, bất chấp việc cấp phép và phê duyệt liên quan, tính thực thi pháp lý của hợp đồng thông minh vẫn chưa được thiết lập và đồng bộ hóa với luật hợp đồng cũng như các luật khác quy định các giao dịch tài chính. Tất cả các yếu

tố của hợp đồng khía cạnh được thể hiện dưới dạng các đoạn mã và các yếu tố nói trên của hợp đồng hợp lệ có thể không nhất thiết phải nhận dạng được. Do đó, điều này đòi hỏi phải dịch khung pháp lý điều chỉnh các hợp đồng thành logic phần mềm để đảm bảo rằng bên cạnh hợp đồng thông minh có thể tự thực hiện, chúng cũng tuân thủ các quy định pháp lý của hợp đồng chính thức. Hơn nữa, sự trêu ngươi như vậy nên tính đến quan điểm của nhà phát triển chuỗi khối, quan điểm của cấp dưới và quan điểm của các bên giao dịch. Một khía cạnh như vậy sẽ hỗ trợ trong việc thực thi tính hợp pháp và hiệu lực của hợp đồng. Tuy nhiên, hiện tại, các tổ chức đã triển khai hợp đồng thông minh thông qua công nghệ chuỗi khối phải liên tục đấu tranh với khía cạnh hiệu lực và khả năng thực thi của hợp đồng. Tuy nhiên, Vukolić biểu thị rằng mặt trái của hợp đồng thông minh là việc vi phạm hợp đồng rất hiếm khi xảy ra, vì việc thực hiện hợp đồng phụ thuộc vào các điều kiện được xác định trước, điều này cũng được kích hoạt bởi một sự kiện mà cả hai nút trong mạng đều không có quyền kiểm soát.

## **PHẦN B: ÚNG DỤNG**

### **4. ÚNG DỤNG BLOCKCHAIN TRONG TRUY XUẤT NGUỒN GỐC GIÀY**

#### **4.1 Vấn đề**

Thống kê của Bộ Công Thương cho thấy, doanh thu thương mại điện tử (TMĐT) Việt Nam năm 2021 đạt 13,7 tỷ USD, tăng 16% so với năm 2020. Việt Nam thuộc nhóm 3 quốc gia có tốc độ tăng trưởng thị phần bán lẻ trực tuyến cao nhất khu vực Đông Nam Á. Dự báo, tốc độ tăng trưởng của TMĐT Việt Nam năm 2022 có thể ở mức cao nhất từ trước tới nay nhờ kiểm soát tốt đại dịch COVID-19. [6]

Bên cạnh sự phát triển vượt bậc của TMĐT tại Việt Nam thì tình trạng hàng giả, hàng nhái, hàng kém chất lượng được bán tràn lan trên mạng internet, trên các nền tảng giao dịch trực tuyến đang là những tiêu cực của thị trường.

Qua một số khảo sát cho thấy, hiện nay hàng giả, hàng nhái, hàng kém chất lượng có mặt ở rất nhiều phân khúc của thị trường, từ các “mẹt” hàng tạp hóa trên các phiên chợ vùng sâu, vùng xa đến hè phố các đô thị, thậm chí len lỏi, trà trộn vào cả những siêu thị cao cấp ở những đô thị lớn như Hà Nội, thành phố Hồ Chí Minh nhằm “thử thách” mức độ sành sỏi của khách hàng.

Hàng giả, hàng nhái, hàng kém chất lượng có những biểu hiện như đa dạng về mẫu mã, “linh động” về giá cả và đặc biệt nguy hiểm hơn là còn phong phú cả về chủng loại. Sự nguy hiểm thể hiện ở chỗ, bên cạnh việc gây thiệt hại về kinh tế cho “khô chủ”, nó còn gây ảnh hưởng nghiêm trọng đến sức khỏe của người tiêu dùng. Điển hình là đồ ăn, đồ uống, thuốc chữa bệnh...giả, kém chất lượng khiến bệnh tật thi nhau “nảy nở”, phát triển trong cơ thể những “thượng đế” nhẹ dạ, kém hiểu biết và ham rẻ.

Hầu hết các hãng có uy tín, có thương hiệu, được người tiêu dùng ưa chuộng đều có nguy cơ bị làm giả, làm nhái hàng hóa. Xét về góc độ kinh tế, hàng giả, hàng nhái gây ảnh hưởng rất lớn đến lợi nhuận của những doanh nghiệp sản xuất., kinh doanh chân chính. Tác động tiêu cực đầu tiên là hành vi nêu trên làm mất uy tín của những doanh nghiệp có sản phẩm bị làm giả, khiến người tiêu dùng hiểu lầm, dẫn đến việc quay lưng lại với sản phẩm. Mặt khác, vì có lợi thế về giá cả so với hàng “xịn” mà hàng giả,

hàng nhái khiến những mặt hàng chính hãng, có nguồn gốc xuất xứ rõ ràng lâm vào tình trạng ế ảm, suy giảm doanh thu. [7].

Một trong những mặt hàng làm giả nhiều đó là các mặt hàng về thời trang mà cụ thể hơn là giày. Những đôi giày được các thương hiệu nổi tiếng bán với giá rất cao, giá có thể lên tới vài triệu cho đến hơn chục triệu. Nhưng khi được làm giả thì giả chỉ khoảng vài trăm. Điều này sẽ khiến doanh thu của các thương hiệu này giảm mạnh vì số lượng giày nhái đang ngày càng gia tăng. Người tiêu dùng khi mua một đôi giày về thì việc xác minh xem đôi giày này có phải chính hãng không rất là khó khăn. Họ phải lên mạng xem cách so sánh, tìm hiểu về các bộ phận của giày để phân biệt hay kiểm tra mã số trên giày nhưng cũng không thể chắc chắn được vì thủ đoạn làm nhái hiện nay là vô cùng tiên tiến và tinh vi.

## 4.2 Giải pháp

Giải pháp của nhóm sẽ là tạo một ứng dụng có thể truy xuất nguồn gốc của giày, từ các công đoạn tạo đơn, sản xuất cho đến xuất kho nhằm giúp cho khách hàng có cái nhìn rõ nhất về xuất sứ của chiếc giày, từ đó khiến khách hàng yên tâm hơn về sản phẩm.

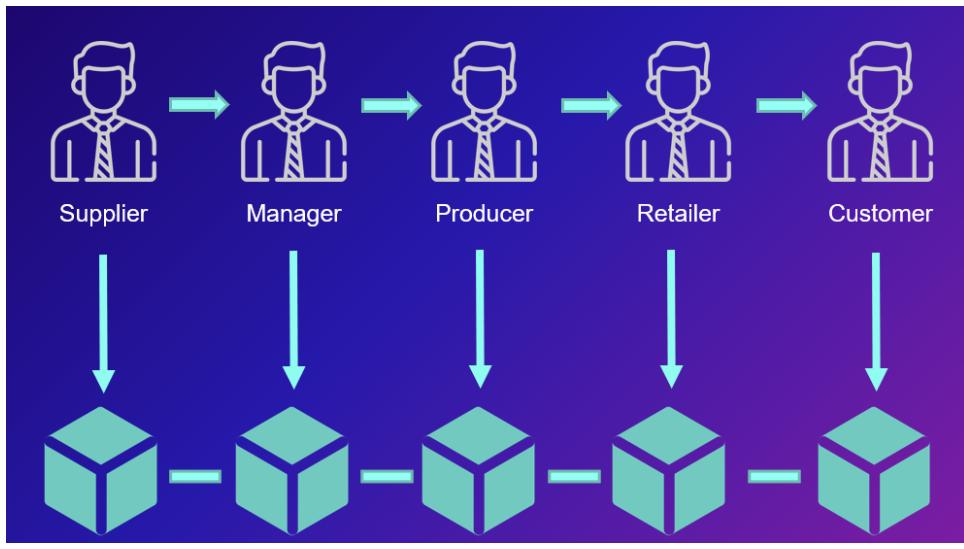
Bằng việc sử dụng việc truy xuất nguồn gốc bằng blockchain thì khách hàng có thể dễ dàng truy xuất ở ngay trên web của mình và có thể thấy rõ thông tin một cách minh bạch vì những dữ liệu này là những dữ liệu không thể thay đổi.

### a) Các bên tham gia

- Manager : Quản lý

- Supplier: Nhà cung cấp
- Producer: Nhà sản xuất
- Retailer: Người bán lẻ
- Customer: Khách hàng

### b) Các giai đoạn



- Giai đoạn 1: Nhập nguyên vật liệu từ Supplier. Lúc này Supplier phải nhận thông tin và xác nhận đồng ý và chuyển hàng tới mình, từ đó mình nhận hàng và chuyển vào kho.
- Giai đoạn 2: Tạo lệnh sản xuất cho Producer. Producer nhận lệnh, kiểm tra hàng trong kho và tiến hành sản xuất. Sau khi sản xuất xong thì để sản phẩm trong kho.
- Giai đoạn 3: Retailer tạo đơn hàng. Lúc này Manager sẽ duyệt đơn hàng và bắt đầu xuất hàng cho Retailer.

### c) Demo sản phẩm

Material ID	Material Name	Quantity	Unit
None			

Name	Quantity	Unit
Vải	100	mét
đa	20	métr

- Link demo sản phẩm: <https://www.youtube.com/watch?v=22lz2o4oJoY>
- Link source code:

## PHẦN C: TÀI LIỆU THAM KHẢO

- [1] *Blockchain White Paper National Archives and Records Administration.* (2019).
- [2] *Công nghệ chuỗi khói là gì? - Giải thích về Công nghệ chuỗi khói - AWS.* (n.d.). Retrieved January 14, 2023, from <https://aws.amazon.com/vi/what-is/blockchain/>
- [3] *NGHIÊN CỨU-TRAO ĐỔI ThS Cao Minh Kiểm.* (n.d.). Retrieved January 14, 2023, from [https://repository.vnu.edu.vn/bitstream/VNU\\_123/117328/1/40275-Article%20Text-133578-1-10-20190823.pdf](https://repository.vnu.edu.vn/bitstream/VNU_123/117328/1/40275-Article%20Text-133578-1-10-20190823.pdf)
- [4] *Công Nghệ Blockchain - Thư Viện PDF.* (n.d.). Retrieved January 14, 2023, from <https://thuvienpdf.com/cong-nghe-blockchain>
- [5] Sharma, K. (n.d.). *Blockchain; A Hype or a Hoax?*
- [6] *Ethereum Whitepaper / ethereum.org.* (n.d.). Retrieved January 14, 2023, from <https://ethereum.org/en/whitepaper/>
- [7] *For Professional clients only.* (n.d.). Retrieved January 14, 2023, from <https://ethereum.org/en/what-is-ethereum>
- [8] *Ethereum Là Gì Và Hoạt Động Như Thế Nào? | Bybit Learn.* (n.d.). Retrieved January 14, 2023, from <https://learn.bybit.com/vi/altcoins/what-is-ethereum-and-how-does-it-work/>
- [9] *Ethereum – Wikipedia tiếng Việt.* (n.d.). Retrieved January 14, 2023, from <https://vi.wikipedia.org/wiki/Ethereum>
- [10] *Ethereum là gì? Ethereum 2.0 là gì? Tương lai khi The Merge tích hợp.* (n.d.). Retrieved January 14, 2023, from <https://coin68.com/ethereum-la-gi/>
- [11] *(PDF) Smart Contracts on the Blockchain - A Bibliometric Analysis and Review.* (n.d.). Retrieved January 14, 2023, from [https://www.researchgate.net/publication/340646200\\_Smart\\_Contracts\\_on\\_the\\_Blockchain\\_-\\_A\\_Bibliometric\\_Analysis\\_and\\_Review](https://www.researchgate.net/publication/340646200_Smart_Contracts_on_the_Blockchain_-_A_Bibliometric_Analysis_and_Review)
- [12] *(PDF) Smart Contracts Implementation, Applications, Benefits, and Limitations.* (n.d.). Retrieved January 14, 2023, from [https://www.researchgate.net/publication/336369143\\_Smart\\_Contracts\\_Implementation\\_Applications\\_Benefits\\_and\\_Limitations](https://www.researchgate.net/publication/336369143_Smart_Contracts_Implementation_Applications_Benefits_and_Limitations)
- [13] Chicago, B., Los, H., New, A., Palo, Y., São, A., Washington, P. T., Wilmington, D. C., Beijing, A. P., Kong, H., Shanghai, S., Tokyo, S., Brussels, E., London, F., & Paris, M. M. (n.d.). *An Introduction to Smart Contracts and Their*

*Potential and Inherent Limitations Skadden, Arps, Slate, Meagher & Flom LLP and Affiliates.*

[14] Philippe, D. (n.d.). *BLOCKCHAIN AND SMART CONTRACT: LEX CRYPTOGRAPHIA ?* Retrieved January 14, 2023, from [https://www.eublockchainforum.eu/sites/default/files/reports/20180727\\_report\\_innovation\\_in\\_europe\\_1](https://www.eublockchainforum.eu/sites/default/files/reports/20180727_report_innovation_in_europe_1)

[15] Zheng, Z., Xie, S., Dai, H.-N., Chen, W., Chen, X., Weng, J., & Imran, M. (n.d.). *An Overview on Smart Contracts: Challenges, Advances and Platforms.*

[16] *Vấn nạn hàng giả, hàng nhái trên internet.* (n.d.). Retrieved January 14, 2023, from <https://baochinhphu.vn/van-nan-hang-gia-hang-nhai-tren-internet-102220607173803913.htm>

[17] *VÂN NAN HÀNG GIẢ, HÀNG NHÁI, HÀNG KÉM CHẤT LƯỢNG VÀ MỘT SỐ GIẢI PHÁP - VNPTCheck.* (n.d.). Retrieved January 14, 2023, from <http://vnptcheck.vn/news/details/36-vn-nan-hang-gi-hang-nhai-hang-kem-cht-lung>