DOC- BLOCK: Một hệ thống xác thực dựa trên blockchain cho tài liệu số

**Tóm tắt**

Với tốc độ phát triển nhanh chóng trong lĩnh vực công nghệ thông tin và khả năng tiếp cận dễ dàng với các công cụ văn phòng tiên tiến và giá rẻ trên thị trường, việc làm giả các tài liệu quan trọng đã trở thành một vấn đề đáng lo ngại. Vì vậy, xác minh và xác thực các tài liệu quan trọng khác nhau như tài liệu ngân hang, tài liệu chính phủ, chứng chỉ giáo dục, vvv.. ngày càng tăng. Tuy nhiên, nhiều thách thức và quá trình kiểm tra thiếu hiệu quả những tài liệu phức tạp và mất nhiều thời gian khiến ta tiến hành nghiên cứu này. Trong tài liệu này, chúng tôi đưa ra một chương trình ứng dụng web cho xác thực tài liệu số sử dụng nền tảng công nghệ blockchain Ethereum và công nghệ lưu trữ đám mây P2P để tăng cường kiểm tra xử lý bằng cách làm nó công khai, minh bạch và dễ kiểm tra hơn. Các mô hình đề xuất bao gồm một số phương pháp như khóa mã hóa pulic/private, lưu trữ online, chữ ký số, mã hash, mạng peer to peer và bằng chứng công việc, những cái này làm cho việc xác minh tài liệu nhanh hơn và thuận tiện hơn chỉ với một cú nhập chuột. Hơn nữa, các giá trị băm cũng được gán cho các tài liệu riêng lẻ. Mô hình để xuất đáp ứng các tiêu chí cho một hệ thống xác minh tài liệu kỹ thuật số bằng cách giảm bớt những lổ hổng và khó khan trong các phương pháp truyền thống trong xác minh tài liệu.

I.Giới thiệu

Sự phát triển nhanh chóng của chia sẻ và trao đổi thông tin đã làm cho ngày càng nhiều công ty và cá nhân sử dụng tài liệu số. Hơn nữa sự nặng nề và mất thời gian của việc sử dụng và xác nhận tài liệu truyền thống là động lực thúc đẩy người ta sử dụng modern này để in ấn và xác thực tài liệu quan trọng. Mặc dù tài liệu số rõ ràng thuận tiện sử dụng, nhưng việc chứng minh xác thực những tài liệu này là vấn đề đáng quan tâm. Do cuộc cách mạng công nghệ và sự dễ dàng tiếp cận với các thiết bị tiên tiến và rẻ tiền, việc giả mạo các tài liệu quan trọng trở nên khá dễ dàng và khiến cho việc xác thực tài liệu trở thành một công việc khá khó khă. Hệ lụy nảy sinh từ vấn nạn làm giả giấy tờ đang gây ra những tác động nghiêm trọng, đáng báo động và cần được khẩn trương xem xét. Do đó, một hệ thống xác nhận tính xác thực của các tài liệu quan trọng sẽ rất có lợi cho người dùng để duy trì các tài liệu kỹ thuật số của họ. Có một mô hình mã nguồn mở, bất biến và đồng thuận có sẵn được gọi là blockchain để giải quyết vấn đề này.

Công nghệ blockchain là một phát minh gần đây nhằm tăng cường

quá trình xác minh tài liệu và vướng mắc nhiệm vụ giảm gian lận và sử dụng sai tài liệu. Blockchain chỉ đơn giản là đề cập đến một cơ sở dữ liệu phân tán lưu trữ theo thứ tự thời gian nhiều khối được xâu chuỗi lại với nhau với mỗi gói dữ liệu hoặc khối lưu trữ tài liệu theo cách khiến không thay đổi các tài liệu này. Blockchain là một công nghệ tiên tiến có thể đóng nhiều vai trò quan trọng trong lĩnh vực bảo mật. Blockchain đảm bảo sự tin cậy, toàn vẹn, đồng thuận, tự chủ và an toàn. Nhờ vào phương pháp lưu trữ và xác thực các giao dịch hoàn toàn đáng tin cậy, minh bạch và an toàn , chúng tôi sử dụng nó trong công việc của chúng tôi để xác thực các tài liệu kỹ thuật số quan trọng

Hiện tại, quy trình xác minh tài liệu bao gồm diễn giải của con người và quan sát của bên thứ ba. Và như chúng ta đã biết, đó là một quá trình rất dài và luôn có  
khả năng xảy ra sai sót và thiếu trung thực. Vì vậy, phương pháp xác minh hiện tại có vẻ không đáng tin cậy và hiệu quả. Một số loại nghiên cứu đã nêu, có rất nhiều tài liệu và chứng chỉ giả mạo bao quanh ngành công nghiệp toàn cầu. Và  
nó có thể ảnh hưởng như thế nào đến nền kinh tế và sự phát triển của xã hội. Nhưng công nghệ blockchain có thể loại bỏ những khó khăn này và cải thiện bảo mật bằng cách duy trì tính toàn vẹn. Trong công việc của mình, chúng tôi đã xây dựng một ứng dụng web phi tập trung để tránh mất thời gian không cần thiết để thực hiện quy trình xác minh truyền thống một cách nhanh chóng và an toàn hơn bất kể thời gian và địa điểm chỉ với một cú nhấp chuột bằng cách sử dụng khái niệm cơ bản của công nghệ chuỗi khối Ethereum. Ứng dụng web của chúng tôi phục vụ ba mục đích chủ yếu:  
1. Lưu trữ Tài liệu Chính  
2. Xác minh bất kỳ Tài liệu nhất định nào  
3. Tải xuống bất kỳ Tài liệu cụ thể nào  
Trong quy trình đầu tiên, người dùng có thể tải lên bất kỳ tài liệu nào bằng cách sử dụng hệ thống của chúng tôi. Và tất cả các tài liệu được tải lên sẽ được lưu trữ trực tiếp vào blockchain. Sau đó, chúng tôi sẽ xác minh bất kỳ tài liệu nhất định nào để tìm xem nó là tài liệu gốc hay bị hỏng. Để xác minh tài liệu kỹ thuật số, chúng tôi cần tài liệu chính và khớp với nó với cái đã cho. Ở đây chúng tôi đã sử dụng cơ chế băm SHA-256 để mã hóa và giải mã mọi tài liệu. Hơn nữa, chúng tôi cũng đã sử dụng các hợp đồng thông minh ở phần phụ trợ liên kết với blockchain và lưu trữ giá trị băm được mã hóa của các tài liệu riêng lẻ sẽ được kiểm tra chéo so với tài liệu. Vì vậy, bất kỳ thay đổi nào trong tài liệu thực tế cũng sẽ thay đổi hàm băm tương ứng. Nếu ai đó cố gắng thao túng một tài liệu thì tài liệu đó sẽ không bao giờ vượt qua được bài kiểm tra xác minh . Như vậy, chúng ta có thể thoát khỏi vấn đề tài liệu giả mạo. Quan trọng hơn, nếu bất kỳ tổ chức nào cần tải xuống bất kỳ  
tài liệu nào cho mục đích của họ, họ có thể dễ dàng tải xuống bằng cách sử dụng mã băm IPFS được cung cấp bởi hệ thống của chúng tôi.

II. Các công việc liên quan

Trong những năm gần đây, blockchain trở thành một công cụ phổ biến trong công nghiệp. Một vài khảo sát và nghiên cứu được thực hiện để triển khai blockchain trong các lĩnh vực khác nhau. Trong phần này sẽ giới thiệu về một số công trình có sắn liên quan đến blockchain.

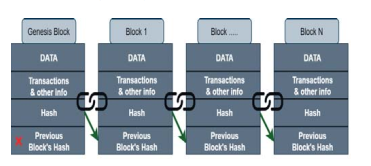
Trong phần này mô tả cách chúng ta triển khai blockchain trong các lĩnh vực khác nhau và dóng góp của nó cho công nghiệp tương lai. Khi blockchain đang trở nên phổ biến trên thế giới vì bản chất phân tán và phi tập trung của nó. Tác giả đã thực hiện một cuộc khảo sát toàn diện về quản lý danh tính dựa trên blockchain và hệ thống lưu trữ dữ liệu cá nhân. Họ đã thảo luận về khái niệm nhận dạng tự chủ(SSI) cho người dùng, đó là quyền kiểm soát quyền sở hữu dữ liệu. Cuộc khảo sát này là một hệ thống quản lý dữ liệu người dùng làm trung tâm loại bỏ hệ thống tập trung bằng cách sử dụng blockchain. Nghiên cứu về việc sử dụng blockchain trong sở hữu trí tuệ mô tả tổng quan kỹ thuật về blockchain Ethereum và hợp đồng thông minh.

Những tác giả đã đề xuất một mô hình xác minh tính toàn vẹn dữ liệu bằng phương pháp blockchain. Họ mô tả những sai sót trong hệ thống xác thực dựa trên cloud thông thường bao gồm chủ sở hữu bên thứ ba và tạo nền tảng P2P bằng ccasch sử dụng cấu trúc cây Markle dựa trên blockchain, nơi người dùng có thể đảm bảo tính toàn vẹn dữ liệu. Để xác minh các tác giả sử dụng phương pháp chọn mẫu ngẫu nhiên. Teymourlouei và cộng sự đã đề xuất một mô hình xác thực người dùng bằng cách sử dụng blockchain được bảo mật hơn so với hệ thống xác thực dựa trên email và mật khẩu truyền thống. Các tác giả đã mô tả những lợi thế của việc sử dụng khóa riêng và khóa công khai cho xác minh tài liệu. Họ cũng thảo luận về khả năng sử dụng rộng rãi của blockchain trong IoT và theo dõi dữ liệu, quản lý chuỗi cung ứng, đăng ký và bảo vệ tài sản. Họ đề xuất một phương pháp cho các hệ thống báo cáo tín dụng an toàn trong các lĩnh vực tài chính sử dụng công nghệ blockchain để xây dựng lòng tin giữa người dùng vì blockchain cung cấp một mô hình bảo mật mạnh nhất.

Mô hình đề xuất của họ bao gồm xác thực đa chiều để chuyển tín dụng bằng cách sử dụng blockchain, smart contract và hàm băm. Arjomandi đã đề xuất một phương pháp xác minh tài liệu sử dụng nhận dạng tần số cô tuyến không chíp (RFID). Mô hình của họ quét tài liệu bằng RFID không chip và lưu trữ các mẫu tần số tiêng lẻ trong bộ nhớ đám mây. Nhưng mô hình này dựa trên một cơ quan quyền lực tập trung. Musarella đề xuất mã hóa dựa trên nhận dạng kỹ thuật số sử dụng blockchain Ethereum bằng cách sử dụng các smart contract. Lkmal đề xuất một mô hình xác minh tài liệu bằng cách sử dụng digital signature. Họ chuyển bất cứ tài liệu nào cần chuyển thành tệp JSON có thể đọc được bằng máy và gửi nó đến trình xác thực. Trình xác thực xác minh và thêm chữ ký điện tử vào tài liệu. Họ cũng cung cấp một tính năng khác để kiểm tra chúng và cho điểm dựa trên trên tính xác thực. Tuy nhiên điều này liên quan đến những người của bên thứ ba khiến hệ thống này dễ bị tin tặc tấn công. HamithaNasin đã thảo luận về các nhóm ý tưởng khác nhau để sử dụng blockchain và cung cấp một cuộc khảo sát chi tiết về sử dụng blockchain để xác minh mức độ trong Ethereum Smart contract. Họ cũng mô tả quy trình khai thác của blockchain và các thuật toán khai thác khác, ví dụ: bằng chứng công việc, bằng chứng về cổ phần và bằng chứng về tầm quan trọng. Ghazali đã mô tả tầm quan trọng của chứng chỉ tốt nghiệp nó có thể làm giả dễ dàng. Họ đã đề xuất một mô hình lý thuyết để xác minh các chứng chỉ bằng cách sử dụng công nghệ blockchain. Mô hình của họ bao gồm mã hóa với khóa riêng tư và công khai và chữ ký điện tử với dấu thời gian để chứng minh kỹ thuật số. Shah đx mô tả một hệ thống cấp giấy khai sinh và xác minh giấy khai sinh bằng cách sử dụng blockchain. Mô hình để xuất của họ sử dụng khóa RSA và AES để đăng ký người dùng, đăng nhập và truy xuất dữ liệu và xác minh giấy khai sinh, hệ thống xác minh dựa trên mã pin làm cho hệ thống của họ minh bạch và an toàn hơn.

II. Kiến trúc và triển khai

1. Blockchain

Blockchain là công nghệ tiên tiến tiện lợi và an toàn hơn hệ thống lưu trữ tập trung hiện nay. Nó là một mạng lưu trũ dựa trên giao dịch. Trong công nghệ blockchain, tất cả thông tin được lưu trữ bằng cách pho tập trung bằng cách tạo ra một mạng lưới phân tán. Một mạng blockchain bao gòm nhiều máy tính cá nhân nơi mà mỗi máy tính làm việc như một cơ sở dữ liệu riêng lẻ kết nối với các máy tính khác trong mạng. Nếu chúng ta giả định các máy tính được kết nối như một nút thì blockchain là một mạng của nút được kết nối bởi giao thức ngang hàng Peer to Peer (P2P). Bất kỳ nút nào trong mạng không thể thao tác dữ liệu một cách thủ công vì tất cả các nút khác có quyền truy cập thực tế bào dữ liệu thực tế. Hơn nữa mỗi nút hoặc mỗi khối được mã hóa bằng thuật toán băm cực kì an toàn. Mỗi khối cũng lưu trữ hàm băm của khối trước đó làm cho chúng kết nối với nhau giống như một chuỗi các khối trong mạng. Bất kĩ sự thay đổi nào trong một khối sẽ tự động thay đổi mã băm của các khối sau đó khiến toàn bộ giao dịch không hợp lệ. Dữ liệu được lưu trữ trong mạng blockchain là bất biến. 

Hình 1. Cấu trúc blockchain

Một khối có thể chứa:

1. Giá trị băm của nó
2. Giá trị băm của khối trước đó
3. Bất kỳ loại dữ liệu hoặc giao dịch đã xảy ra trong khối trong suốt quá trình

Chúng ta có thể hình dung cấu trúc này trong hình 1, nơi khối đầu tiên được gọi là khối gốc và nó không có giá trị băm của khối trước đó. Bất kỳ giao dịch nào trên khối đều được xác minh bởi hàng nghìn, hàng triệu máy tính được phân phối xung quanh hệ thống. Khi khối đó được xác minh bởi các nút khác nó có thể được thêm vào mạng

1. Ethereum

Ethereum là một mạng dựa trên blockchain được tạo ra để quản lý cơ sở hạ tầng hệ thống máy tính của mạng blockchain. Nó là một nền tảng mã nguồn mở có nhiều chức năng bao gồm smart contract, etherm, vv.. Smart contract là một mã lập trình được triển khai trong mạng blockchain, thực thi khi một sự kiện nhất định xảy ra trong bất kỳ khối nào. Smart contract có thể tự thực thi, phân phối và chia sẻ trên mạng blockchain. Ether là một loại tiền điện tử dành cho các ứng dụng dựa trên ethereum. Tiền điện tử là tiền kỹ thuật số để giao dịch trong giao dịch kỹ thuật số. Ether hoạt động như một khoản phí giao dịch để được trả tiền cho bất kỹ sự kiện nào. Vì vậy Ethereum cung cấp một nền tảng cho các nhà phát triển để tạo bất kỳ ứng dụng phi tập trung nào trong mạng blockchain.

1. Solidity

Solidity là ngôn ngữ bậc cao để triển khai smart contract trên các mạng bkockchain khác nhau như Ethereum. Solidity cũng là ngôn ngữ hướng đối tượng. Nó lấy cảm hứng từ các đặc tính của các ngôn ngữ khác như C++, Python và JavaCript. Solidity được thiết kế để chạy triển khai các smart contract trong máy ảo Ethereum (EVM). Smart contract được nhúng với logic doanh nghiệp và logic điện toán sử dụng bởi ngôn ngữ solidity. Do solidity hỗ trợ các tính năng để viết smart contract, nên nó khá là thuận tiện khi viết smart contract bằng solidity.

1. Infura

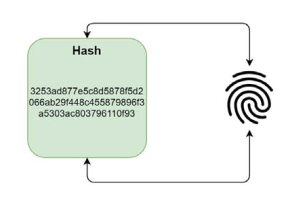
Trong hệ thống đề xuất để chạy máy tính người dùng như một node Ethereum Infura được sử dụng. Nói chung để tương tác với mạng blockchain Ethereum người dùng luôn cần tạo một ví Ethereum trước. Không có ví, người dùng không thể giao dịch hoặc trả phí cho mỗi giao dịch hay nói cách khác không thể sử dụng tiền điện tử Ether. Infura là một máy chủ cụm node Ethereum giúp người dùng tương tác với các ứng dụng Ethereum phi tạp trung để set up các ví Ethereum của chúng ta.

1. Hệ thống file InterPlanetary

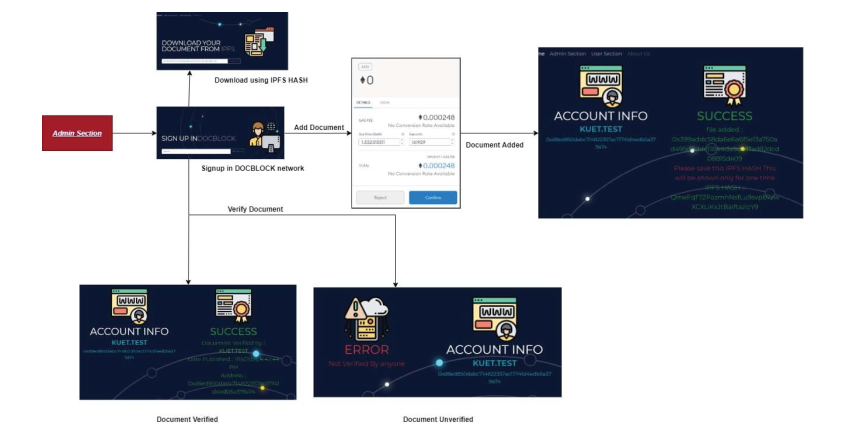
Hệ thống file InterPlanetary (IDFS) có thể hiểu là giao thức lưu trữ dữ liệu phân phối và vận chuyển ngang hàng peer to peer (P2P). IPFS sử dụng hệ thống định vị địa chỉ dựa trên nội dung để định vị độc lập từng file liên kết tất cả các máy tính trên toàn cầu. Sử dụng IPFS trong hệ thống đề xuất của chúng ta sẽ kích hoạt một tính năng mới cho người dùng theo cách tương tự như BitTorrent. VÌ vậy, người dùng có thể nhận được nội dung từ bất kỳ nút nào có nội dung được yêu cầu và cũng có thể lưu trữ bất kỳ nội dung nào cho những người dùng khác trong mạng. Trong hệ thống IPFS, một số lượng tổng dữ liệu được thực hiện bởi một nhà khai thác người dùng nhất định, cung cấp hệ thống lưu trữ và phân phối tên linh hoạt. Bất cứ người dùng mạng nào có thể lưu trữ tệp dữ liệu hoặc thông tin khác bằng cách sử dụng địa chỉ nội dung duy nhất của nó, sau đó những người dùng mạng khác có thể xác định, yêu cầu hoặc truy cập thong tin đó từ bất kỳ máy tính cá nhân nào có nó.

1. Hàm băm SHA-256

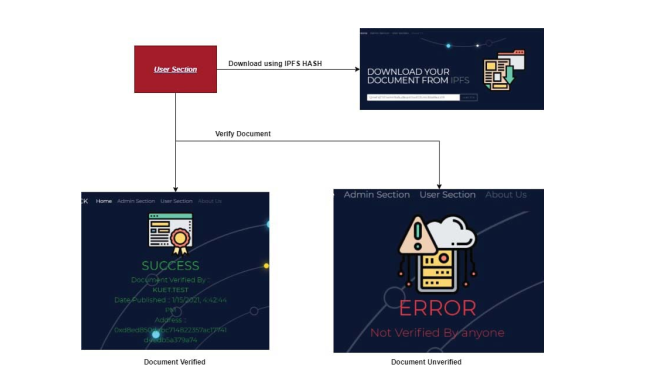
Như chúng ta có thể thấy ở hình 2, giá trị băm có thể hiểu như vân tay của con người cái mà duy nhất cho mỗi đầu vào.



Lưu file gốc trong cơ sở dữ liệu sẽ mất một số lượng lớn không gian lưu trữ. Vì vậy chúng ta cần một cách duy nhất để ánh xạ các file và các tài liệu có kích thươc nhỏ hơn kích thước ban đầu. Chúng ta sẽ sử dụng một hàm băm để có được công việc này. Mã hóa hàm băm có thể được định nghĩa là một hàm toán học phức tạp mà từ một đầu vào có chiều dài và kích thước không cố định tạo ra một đầu ra có chiều dài kích thước cố định. Hash luôn hoạt động như hàm một chiều. Vì vậy từ đầu ra không thể suy ra được đầu vào của hàm băm. Hàm băm thường được sử dụng cho chữ ký số và mật mã. Ví dụ: bảo mật mật khẩu, xác minh tin nhắn, lấy khóa, tạo số giả ngẫu nhiên và các blockchain. Chủ yếu băm đảm bảo tính bảo mật cao nhất của bất kỳ nội dung tài liệu nào. Một số hàm băm: MD5, SHA-1, SHA-256. Trong mô hình đề xuất chúng tôi sử dụng thuật toán SHA-256. SHA-256 có thể che giấu dữ liệu đầu vào lớn hơn kích thước cố định.



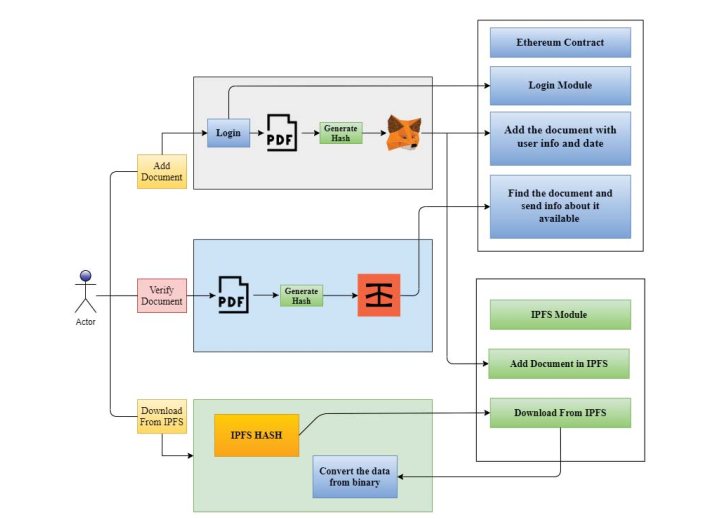
Hình 3. Admin-section Workflow



Hình 4. User-Section Workflow

IV. Framework đề xuất

Khái niệm chính đằng sau dự án này là xây dựng một nền tảng đóng vai trò quan trọng trong việc xác minh xác thực của các file quan trọng, hợp đồng, giấy xác nhận và tài liệu đất đai, tài sản một cách chính xác và nhanh chóng hơn. Chúng tôi đã sử dụng các phương pháp nổi tiếng và an toàn để xây dựng hệ thống. CHúng tôi đã sử dụng blockchain Ethereum để phát triển hệ thống này. SHA-256 được sử dụng cùng với blockchain. Nó là một thuật toán mã hóa một chiều và chống dịch ngược để mã hóa dữ liệu.



Hình 5 Tiến trình hệ thống đề xuất DOC-BLOCK

Toàn bộ quy trình rất an toàn mà không ai có thể làm hại bất kỳ tài liệu nào. Vì vậy dự án này tập trung mạnh mẽ vào việc phòng thủ vững chắc trước bất kỳ cuộc tấn công mạng nào. Người dùng không bao giờ cần phải nghĩ đến việc các file của họ bị mất hoặc xâm phạm, bởi vì họ có thể truy cập hồ sơ của mình một cách thuận tiện bất cứ khi nào họ muốn. Mặc dù có nhiều công nghệ tiên tiến trong back-end bằng HTML và JavaCript. Giao diện người dùng của web được thiết kế theo cách thủ công, giữ mối quan tâm về tính thân thiện với người dùng. Đối với bất kỳ công việc chuyên môn hay điều gì đó, trang web này có thể được điều hành bởi một người mới làm quen, người không có nhiều hiểu biết về Ethereum hay blockchain. Trang web không có nhiều nội dung hoặc có bất kỳ thông tin vô ích hoặc hành vi không mong muốn nào. Nó rất đơn giản và tốt để sử dụng cho bất kỳ ai. Việc triển khai của chúng tôi được thực hiên trong Heroku. Trong hệ thống đã phát triển có hai phần (người dùng và quản trị viên) được hiển thị trong hình 3 và hình 4.

Hệ thống có 3 tính năng quan trọng là: upload, xác nhận và dowload. Toàn bộ quá trình back-end được thể hiện trong hình 5. Để duy trì khả năng sử dụng cho mọi tình huống, chủ yếu có hai phần riêng biệt, một phần dành cho tổ chức và phần còn lại cho mục đích chung. Phần quản trị đề cập đến bất ký tỏ chức hoặc cơ quan nào. Đôi hi một tổ chức hoặc một cơ quan cần phải kiểm tra cẩn thận bất kỳ tài liệu nào được gửi cho họ trước khi kết thúc giao dịch nếu không họ sẽ không bao giờ chắc chắn về tính xác thực của tài liệu đó. Đối với bất kỳ mục đích của tổ chức nào, tổ chức cần phải cài đặt Metamask để tài liệu đã được xác minh trong chuỗi khối. Sau mỗi lần tải lên, hàm băm của file được đính kèm với khóa công khai của tổ chức và thời gian thêm tài liệu được sử dụng để xác minh thêm tính xác thực của tài liệu. Tổ chức cũng sẽ nhận được một hash IPFS, chỉ họ mới có thể xem và chia sẻ với một người dùng cụ thể để tải xuống thêm tài liệu. Phần trên cùng của hình 5 của hình quy trình làm việc hiển thị quá trình thêm file/ tài liệu vào mạng Ethereum. Nếu cùng một tệp được thêm nhiều lần, chỉ người dùng đầu tiên đã thêm nó, kết quả sẽ được hiển thị. Ví dụ: chúng tôi đã thêm một file và nó có thể được tải xuống từ dowload tài liệu từ bất cứ phần nào bằng IPFS hash này: *QmbfhzU8akbENKJwp3c8eW2vw19fLb8vUYzfjtHKeUsBbN*

File này được thêm vào ngày 13/1/2021 lúc 7:50:29 PM. Chi phí để thêm tài liệu tới hợp đồng là 0,04787 USD. Vì vậy khi một tổ chức upload bất cứ tài liệu nào lên hệ thống của nhà phát triển, hệ thống sẽ thêm tài liệu vào blockchain và cung cấp những thông tin khác về việc thêm tài liệu trên màn hình. Ví dụ như tên người tải lên và địa chỉ, thời gian, mã IPFS cho file cụ thể đó được cung cấp để xác minh thêm. Và nếu tài liệu bị hỏng bằng cách nào đó, cơ quan có thẩm quyền sẽ biết về nó do sự thay đổi của giá trị hàm băm của tài liệu. Một lưu ý khác đối với mục đích chung, bất kỳ người dùng/ người xác minh nào cũng có thể xác minh tài liệu đã cho hoặc tải xuống tài liệu có hàm băm IPFS mà không cần bất kỳ quyền truy cập nào vào Ethereum/ IPFS, được xử lý trên máy chủ để tăng khả năng sử dụng. File SHA256 bằm của chúng tôi là: *3253ad877e5c8d5878f5d2066ab29f448c455879896f3a5303ac  
803796110f93*

Nó là một phương pháp băm và chúng tôi không thể lấy tệp chính từ hàm băm này. Sau đó chung tôi thực hiện một chỉnh sửa đơn giản trong tài liệu này và cố gằng xác minh nó. Như mong đợi ngay cả một thay đổi nhỏ băm đã được thay đổi và tệp này không được xác minh. Các xác xuất va chạm của hàm băm là P ≈ 1 2 (n / 2128) 2  
trong đó n là chiều dài của các hash là 256 chiều dài,  
khả năng va chạm thực sự thấp mà chúng ta không cần phải thêm  
một phương pháp băm kép hoặc phương pháp băm 512-bit để làm cho nó  
an toàn hơn.

Nếu cần bất kỳ bản sao chính hãng nào của file/ tài liệu cho bất kỳ truy vấn nào, người dùng hệ thống của chúng tôi sẽ có thể thực hiện điều đó trong giây lát. Sau khi thêm một tài liệu, người dùng sẽ được cấp một mã băm IPFS, nó được cấp một lần và người dùng cần lưu nó ở đâu đó để sử dụng thêm. Chúng tôi đã không lưu trữ mã băm IPFS trong hợp đồng thông minh để làm cho hệ thống riêng tư hơn. Khi 1 người dùng cung cấp hàm băm IPFS vào hệ thống của chúng tôi, nó sẽ tìm kiếm file tương ứng khớp với hàm băm này và gửi lại file gốc được chuyển đổi từ mã nhị phân. Phần dưới cùng trong hình 5 của quy trinh làm việc cho thấy quá trình này. VÌ IPFS tự động xóa ít file tải xuống hơn overtime, file này có thể không truy cập được.

Đối với bất kỳ người dùng cá nhân hoặc tổ chức, hoặc cơ quan nào chúng tôi có thể tháy rằng bằng cách làm theo mô hình đề xuất của chúng tôi, chúng tôi có thể dễ dàng xác minh bất kỳ tài liệu nào và chắc chắn về tính xác thực của tài liệu và cũng có thể tải xuống tệp gốc để kiểm tra thêm để tìm bất kỳ tài liệu giả mạo nào. Và quá trình thực hiện toàn bộ điều này rất đơn giản và dễ dàng. Vì vậy, không có khả năng xảy ra bất kỳ lỗi không mong muốn nào. Bất kỳ người dùng nào có ít kiến thức về blockchai, Ethereum sẽ không bao giờ gặp bất cứ vấn đề nào khi sử dụng hệ thống này.