

TRƯỜNG ĐẠI HỌC KHOA HỌC TỰ NHIÊN
KHOA CÔNG NGHỆ THÔNG TIN

Bùi Huy Thông

QUẢN LÝ VÀ CHIA SẺ NỘI DUNG SỐ
PHI TẬP TRUNG

LUẬN VĂN THẠC SĨ KHOA HỌC MÁY TÍNH

Tp. Hồ Chí Minh, tháng MM/YYYY

TRƯỜNG ĐẠI HỌC KHOA HỌC TỰ NHIÊN
KHOA CÔNG NGHỆ THÔNG TIN

Bùi Huy Thông - 2611030

**QUẢN LÝ VÀ CHIA SẺ NỘI DUNG SỐ
PHI TẬP TRUNG**

LUẬN VĂN THẠC SĨ KHOA HỌC MÁY TÍNH

NGƯỜI HƯỚNG DẪN

PGS.TS. Nguyễn Đình Thúc

Tp. Hồ Chí Minh, tháng MM/YYYY

Lời cảm ơn

Tôi xin chân thành cảm ơn ...

Mục lục

Lời cảm ơn	i
Đề cương chi tiết	ii
Mục lục	ii
Tóm tắt	iv
1 Giới thiệu	1
2 Các công trình liên quan	2
2.0.1 Blockchain	2
2.0.2 Mã hóa bất đối xứng	4
2.0.3 Chữ kí điện tử	4
3 Phương pháp	5
3.0.1 Tạo và chuyển dữ liệu cho chủ dữ liệu	5
3.0.2 Chia sẻ dữ liệu ngang hàng	5
4 Ứng dụng và cài đặt	6
4.0.1 Web Application (cho nhà cung cấp nội dung) . . .	6
4.0.2 Mobile Application (cho người dùng)	6
Danh mục công trình của tác giả	7
Tài liệu tham khảo	8

Danh sách hình

Danh sách bảng

Chương 1

Giới thiệu

Chương 2

Các công trình liên quan

2.0.1 Blockchain

Trong những năm gần đây, với sự mở rộng và phát triển nhanh chóng của các loại tiền ảo (cryptocurrency) như Bitcoin[], Ethereum[], Zcash[], ...etc, khiến cho mức độ quan tâm đến công nghệ nền tảng của chúng, blockchain, tăng lên đáng kể. Trên thực tế, blockchain đã cho thấy công nghệ này không chỉ đóng vai trò quan trọng trong các lĩnh vực liên quan đến tài chính, mà các ứng dụng của nó đã và đang dần phổ biến rộng rãi trên nhiều lĩnh vực phi tài chính khác. Shen[] đã tổng hợp các ứng dụng của blockchain trong việc phát triển đô thị thông minh và sắp xếp chúng thành 9 danh mục, bao gồm: quản lý nhà nước(governance and citizen engagement), giáo dục, chăm sóc sức khỏe, kinh tế, giao thông vận tải, năng lượng, quản lý nước và chất thải, công trình công cộng và bảo vệ môi trường. Jaroodi[] cũng đã chỉ ra các lợi ích cũng như thách thức của việc sử dụng blockchain trong các lĩnh vực: tài chính, chăm sóc sức khỏe, các hoạt động thương mại, sản xuất, năng lượng, nông nghiệp và thực phẩm, tự động hóa, xây dựng, truyền thông và các ứng dụng giải trí.

Blockchain trong việc bảo vệ dữ liệu và thông tin cá nhân

Bảo mật thông tin cá nhân khi sử dụng internet đã và đang là một vấn đề nan giải khi các mạng xã hội liên tục thu thập thông tin người dùng, bao gồm các thông tin cá nhân, hoạt động và thói quen. Người sử dụng các mạng xã hội gặp khó khăn trong việc quản lý các loại thông tin mà nhà cung cấp dịch vụ được quyền thu thập và mục đích sử dụng các thông tin này và thường không thể rút lại các quyền truy cập đã cho phép. Zyskind[] đề xuất một ý tưởng lưu trữ các chính sách truy cập thông tin trên một Blockchain và để cho các node của Blockchain truy cập thông tin từ một bảng băm phân tán (Distributed hash table). Khi người dùng muốn cấp hoặc hủy bỏ quyền truy cập vào thông tin cá nhân, Blockchain đóng vai trò như một nhà phân phối chỉ cho phép bên thứ 3 truy cập các thông tin đã được cấp quyền. Wang[] đề xuất một mô hình kết hợp hệ thống lưu trữ phân tán (decentralize storage system), Ethereum Blockchain và kỹ thuật mã hóa dựa trên thuộc tính (attribute-based encryption). Mô hình này cho phép người dùng tìm kiếm trên các thông tin đã mã hóa dựa vào các hợp đồng thông minh (smart contract) của Ethereum. Đồng thời cũng cho phép người sở hữu thông tin phân phối các khóa bí mật cho người dùng và chia sẻ thông tin thông qua các chính sách truy cập đặc tả.

Blockchain trong các hệ thống IOT

Các hệ thống lưu trữ phân tán - (Decentralize storage systems)

Các hệ thống lưu trữ phân tán hướng đến việc chia nhỏ dữ liệu và phân phối chúng lên các node trong một mạng lưới có sẵn thay vì dồn nén tất cả dữ liệu trong một server duy nhất. Dựa vào bảng A, ta nhận thấy các hệ thống lưu trữ phân tán có một số ưu điểm so với cách lưu trữ tập trung truyền thống.

- Khi một hệ thống bị tấn công, việc phân tán dữ liệu sẽ giảm thiểu

được rủi ro về thông tin bị lộ một cách toàn vẹn.

- Ngoài ra, tính tồn tại của một hệ thống lưu trữ phân tán cũng cao hơn, khi một hoặc nhiều node bị ngắt kết nối, các node còn lại có thể được lập trình để hoạt động độc lập. Điều này tốt hơn nhiều so với việc một hệ thống lưu trữ tập trung sẽ ngừng hoạt động khi server lưu trữ bị ngắt kết nối.
- Cuối cùng, một hệ thống lưu trữ phi tập trung sẽ thân thiện hơn với người dùng thông qua việc cho phép người sử dụng dịch vụ trả phí theo dung lượng đã sử dụng thay vì phải trả trước để mua dung lượng như cách làm hiện tại của các hệ thống lưu trữ tập trung.

2.0.2 Mã hóa bất đối xứng

2.0.3 Chữ kí điện tử

Chương 3

Phương pháp

3.0.1 Tạo và chuyển dữ liệu cho chủ dữ liệu

3.0.2 Chia sẻ dữ liệu ngang hàng

Chương 4

Ứng dụng và cài đặt

4.0.1 Web Application (cho nhà cung cấp nội dung)

4.0.2 Mobile Application (cho người dùng)

Danh mục công trình của tác giả

1. Tạp chí ABC
2. Tạp chí XYZ

Tài liệu tham khảo