CÔNG NGHỆ BLOCKCHAIN ỨNG DỤNG XÂY DỰNG SÀN ĐẤU GIÁ TRỰC TUYẾN

APPLICATION OF BLOCKCHAIN TECHNOLOGY FOR ONLINE AUCTION SYSTEM

Đặng Đức Mạnh[1,*], Nguyễn Viết Trí[2], Đặng Trọng Hợp[3]

TÓM TẮT

Đấu giá trực tuyến là một phần trong những ứng dụng chuyển đổi số, kinh tế số. Đây là một xu hướng và cũng là nhu cầu thiết yếu đối với sự phát triển của xã hội. Công nghệ Blockchain, không thể phủ nhận, là một công cụ đắc lực để hỗ trợ các giao dịch kinh tế truyền thống chuyển đổi số. Vì khả năng cho phép hoàn thành thanh toán mà không cần bất kỳ ngân hàng hay trung gian nào, Blockchain được dùng trong các dịch vụ tài chính khác nhau như tài sản kỹ thuật số, chuyển đổi hay thanh toán. Thêm vào đó, nó còn có thể áp dụng cho các lĩnh vực khác như hợp đồng thông minh, dịch vụ công cộng, Internet vạn vật, hệ thống danh tiếng và dịch vụ bảo mật. Để tận dụng những ứng dụng của blockchain để số hóa kinh tế, nhóm nghiên cứu đã xây dựng một ứng dụng với mục đích giúp mọi người có thể giao dịch các tài sản số mà không cần trung gian một cách an toàn và bảo mật

Từ khóa: *Blockchain, đấu giá, chuyển đổi số.*

ABSTRACT

Online auctions are part of digital transformation and digital economy applications. This is a trend and also an essential need for the development of society. Blockchain technology is undeniably a powerful tool to support digital transformation of traditional economic transactions. Because of its ability to allow payments to be completed without any banks or intermediaries, Blockchain is used in various financial services such as digital assets, conversion or payments. In addition, it can be applied to other areas such as smart contracts, public services, Internet of things, reputation systems, and security services. To take advantage of the applications of blockchain to digitize the economy, we built an application with the aim of making it possible for anyone to trade digital assets without intermediaries safely and securely.

Keywords**:** *Blockchain, auction, digitalize.*

[1]Lớp KTPM 03- K15, Khoa CNTT, Trường Đại học Công nghiệp Hà Nội

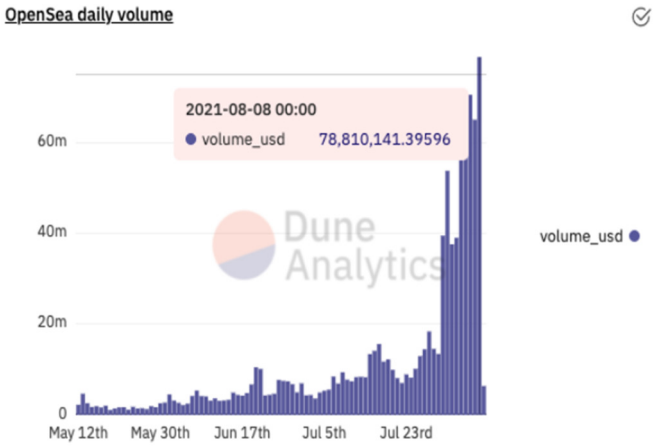
[2]Lớp CNTT 05- K13, Khoa CNTT, Trường Đại học Công nghiệp Hà Nội

[3]Khoa CNTT, Trường Đại học Công nghiệp Hà Nội

[*]Email: leo.m19981998@gmail.com

1. GIỚI THIỆU

Blockchain - Công nghệ chuỗi khối - có thể được xem như một cuốn sổ cái công khai, chống giả mạo và tất cả các giao dịch được lưu trữ trong một chuỗi các khối. Chuỗi này liên tục được phát triển khi các khối mới được thêm vào [1]. Với hàm mật mã đối xứng và cơ chế đồng thuận phân tán đã làm cho Blockchain bảo mật, nhất quán hơn so với sổ cái truyền thống. Do sự phát triển không ngừng của xã hội, đặc biệt là nền kinh tế số. An toàn và minh bạch là vấn đề không chỉ ở riêng Việt Nam mà còn là mối quan tâm hàng đầu của toàn thế giới. Chính vì vậy mà giải pháp ứng dụng blockchain vào những giao dịch đấu giá online đang rất được quan tâm vì nó mang lại sự minh bạch trong thông tin giao dịch cũng như là khả năng phân tán nhằm hạn chế rủi ro xảy ra tại một địa điểm. Đã có nhiều nền tảng sử dụng Blockchain để thực hiện những giao dịch tài sản trên mạng, nổi bật nhất là OpenSea. Như vậy, việc áp dụng blockchain vào đấu giá trực tuyến là hoàn toàn khả thi. Để thấy rõ tầm quan trọng và độ phổ biến của giao dịch đấu giá, trao đổi tài sản số, ta có thể tham khảo hình 1 về khối lượng giao dịch hàng ngày của OpenSea.



Hình 1. Khối lượng giao dịch hàng ngày của OpenSea

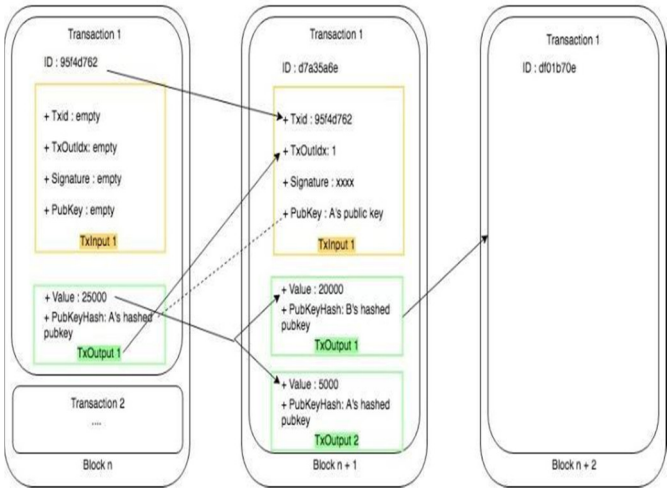
Phần tiếp theo của bài báo có cấu trúc như sau: Phần 2 sẽ giới thiệu phương pháp nghiên cứu và các công nghệ xây dựng ứng dụng. Trong phần 3, chúng tôi sẽ trình bày một số kết quả thực nghiệm cũng như hệ thống demo đã xây dựng được và cuối cùng phần 4 được dành để đưa ra một số kết luận.

2. BLOCKCHAIN VÀ CÁC GIAO THỨC ĐỒNG THUẬN

2.1. Nghiên cứu công nghệ blockchain

Có rất nhiều kỹ thuật và giao thức được áp dụng trong công nghệ blockchain. Trong giới hạn của bài báo, chúng

tôi muốn đưa ra những chủ đề quan trọng của blockchain, như hàm băm, chữ ký số và các giao thức đồng thuận tiêu biểu [2].



Hình 2. Chi tiết giao dịch có sử dụng hàm băm và chữ ký số

Hàm băm là ánh xạ một chiều chuỗi nhị phân có độ dài tùy ý thành một chuỗi nhị phân có độ dài cố định.

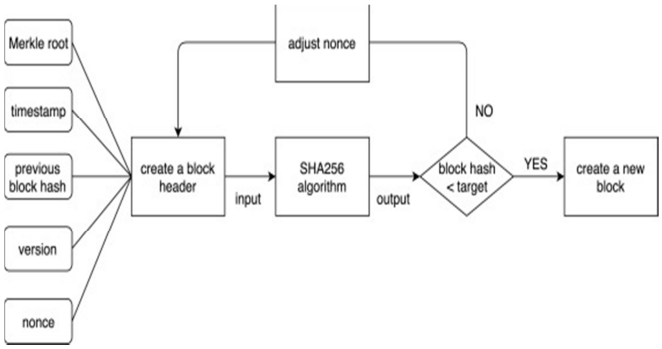
Chữ ký số xử lý vấn đề xác thực và chống chối bỏ trong mật mã học. Nói cách khác, để đảm bảo cho một người/thiết bị đã gửi một bản tin, nó cần được ký điện tử cũng giống như những bức thư tay được niêm phong và được ký bằng tay bởi chính người gửi. Chữ ký số là một phương pháp ký dữ liệu điện tử, nó đảm bảo tính định danh hơn so với chữ ký trên thư viết tay. Nó xác thực bản tin được gửi đi, đảm bảo rằng người gửi không thể chối bỏ được hành vi gửi đi của mình và danh tính của người gửi.

Có hai loại thuật toán chữ ký số: một loại sử dụng nội dung bản tin như đầu vào cho thuật toán xác minh, một loại nội dung bản tin sẽ được khôi phục từ chữ ký của nó. Loại thứ nhất thường được áp dụng rộng rãi hơn, dựa vào các thuật toán băm nên tránh được các tấn công giả mạo. Loại thứ hai không cần thông tin về nội dung bản tin để xác minh. Phương pháp này phù hợp hơn khi gửi nội dung bản tin ngắn bởi vì nội dung bản tin có thể khôi phục được từ chữ ký của nó.

Căn bản nhất của công nghệ blockchain đó là khái niệm về cây Merkle được đặt theo tên của nhà khoa học Ralph C.Merkle người đã đưa ra khái niệm về nó năm 1979 (Merkle, 1988). Đó là một cấu trúc dữ liệu được định nghĩa như sau: tất cả các node không phải là node lá thì mang giá trị băm của những node con của nó và node lá thì không có bất kỳ node con nào.

2.2. Các giao thức đồng thuận tiêu biểu

Bitcoin hay các ứng dụng khác của công nghệ blockchain được sử dụng để chuyển giá trị trong môi trường không tin tưởng, vì vậy cần một cách xác minh các giao dịch được thực hiện là đúng và đó là các thuật toán đồng thuận. Mục tiêu của thuật toán đồng thuận là đảm bảo tồn tại duy nhất 1 lịch sử giao dịch và lịch sử giao dịch đó không chứa các giao dịch không hợp lệ hoặc các giao dịch có mâu thuẫn. Ví dụ: không cho phép một tài khoản có thể tiêu dùng quá số lượng đang có trong tài khoản của mình hoặc tiêu dùng 2 lần.



Hình 3. Giao thức đồng thuận

Bitcoin xử lý vấn đề đồng thuận bằng cách với mỗi block mới sẽ có 1 target đảm bảo giá trị băm của block trước nó, block hiện tại và một giá trị nonce phải nhỏ hơn hoặc bằng giá trị target này. Quá trình này được gọi là proof-of-work (PoW). Mục tiêu là không tập trung quá nhiều quyền lực cho một cá nhân hay tổ chức nào vì thế cần phải lựa chọn một loại tài nguyên hạn chế nào đó để bầu chọn cho tính xác thực của một block. Với PoW, tài nguyên đó chính là sức mạnh tính toán của máy tính. Nhưng sức mạnh tính toán thì ngày càng sẵn có và rẻ hơn định luật Moore và công nghệ điện toán đám mây, độ khó của hàm băm đã được quy định dựa vào tần suất mà block trước đó được tìm ra [3]. Tuy nhiên, PoW là một sự lãng phí năng lực tính toán và năng lượng vô cùng lớn. Có những thợ đào chỉ đào Bitcoin vào mùa đông và sử dụng nhiệt lượng tỏa ra để sưởi ấm. Các thợ đào tập trung tài nguyên lại với nhau thành những nông trại đào bitcoin khổng lồ để tăng hiệu quả, điều này dẫn tới việc tập trung hóa trong mạng phân tán. Tốc độ trong mạng Bitcoin là cứ sau 10 phút thì sinh ra 1 block mới và block size chỉ khoảng 1 MB. Sự tiêu tốn năng lượng và thông lượng là 2 nguyên nhân chính dẫn tới sự ra đời của các thuật toán đồng thuận khác để thay thế proof-of-work. Đó là Proof - of - Stake (PoS), đây là thuật toán không sử dụng sức mạnh tính toán mà sử dụng chính quyền sử hữu các token của blockchain để chiếm ưu thế tạo ra block mới. Blockchain theo dõi một nhóm các validators (bất kỳ ai giữ token đều có thể trở thành 1 validator bằng cách gửi 1 loại giao dịch đặc biệt để khóa token của họ như 1 khoản đặt cọc). Tất cả các validator có thể tham gia vào quá trình tạo và chấp nhận block mới được thực hiện thông qua thuật toán động thuận. Có 2 loại thuật toán đồng thuận: chain-based proof of stake (CBPoS) và BFT - style proof of stake (BFTPoS). Với CBPoS, sau một khoảng thời gian nhất đinh thuật toán sẽ chọn ngẫu nhiên ra một validator và gán cho validator này quyền tạo ra block mới, và block này phải trỏ tới block cuối cùng của chuỗi. Với BFTPoS, các validators sẽ được gán ngẫu nhiên quyền để xuất các block nhưng việc chấp nhận phải thông qua một quá trình nhiều vòng nơi mà mỗi validator "bỏ phiếu" cho một số block nào đó trong mỗi vòng cho tới khi kết thúc của quá trình tất cả những

validators trung thực nhất và đang online sẽ quyết định xem có hay không bất kỳ block nào được thêm vào chuỗi.

3. KẾT QUẢ THỰC NGHIỆM

Sau khi nghiên cứu cơ bản công nghệ blockchain, chúng tôi bắt đầu xây dựng thử nghiệm ứng dụng đấu giá trực tuyến có tên gọi OpenAuction. Ứng dụng được triển khai theo mô hình sau:

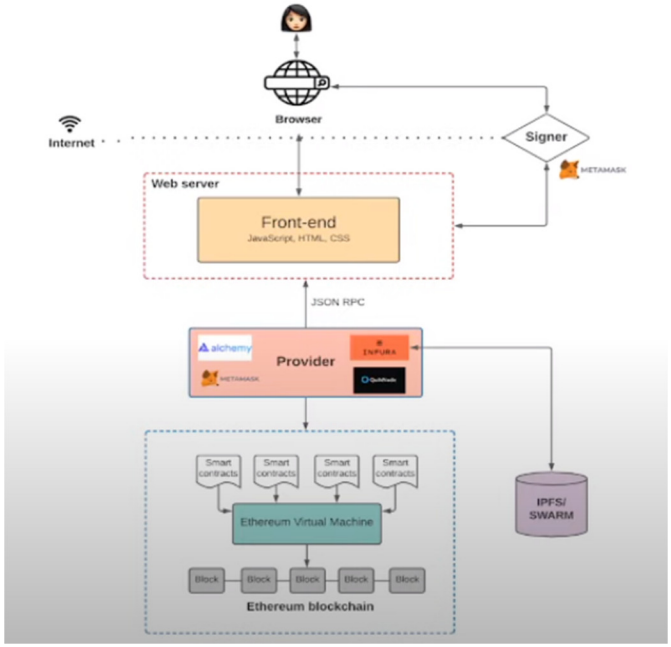
1. Người dùng đăng ký một ví mềm qua một provider(trong ứng dụng OpenAuction sử dụng provider Metamask)

2. Front-end sẽ kiểm tra kết nối đến provider và mạng blockchain, sau đó sẽ hiển thị các vật phẩm đang được đấu giá

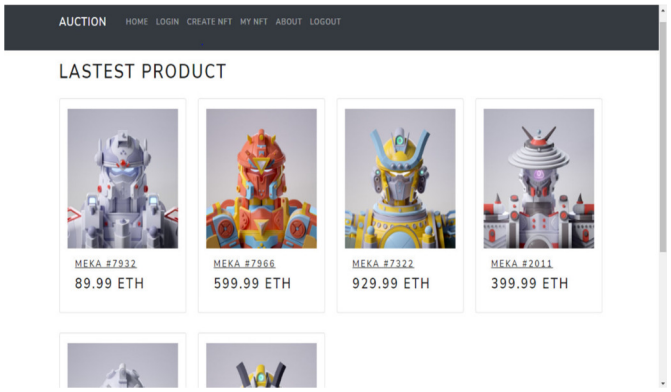
3. Sản phẩm được đấu giá là có thể là các tài sản số NFT, tranh nghệ thuật được lưu trên IPFS

4. Người dùng chọn một sản phẩm để đặt giá

5. Sau một khoảng thời gian, nếu không có Bid mới, người dùng đặt giá cuối cùng có thể thực hiện thanh toán



Hình 4. Mô hình ứng dụng



Hình 5. Màn hình chính sau khi cài đặt ứng dụng

4. KẾT LUẬN

Qua quá trình nghiên cứu, nhóm chúng tôi đã tìm hiểu được một số kiến thức cơ bản của blockchain cũng như bắt đầu thử nghiệm xây dựng một ứng dụng Decentralized app [4]. Kết quả nghiên cứu cho thấy blockchain là một công nghệ bảo mật cao, ứng dụng được vào nhiều khía cạnh trong thực tế. Hiện nay trên thế giới cũng như ở Việt Nam, số hóa kinh tế đang là xu hướng hàng đầu, vì vậy công nghệ blockchain là một thứ thiết yếu mà mỗi sinh viên hay một kỹ sư lập trình cũng nên bắt đầu tìm hiểu và phát triển.

TÀI LIỆU THAM KHẢO

[1]. Pontem.network, 2021. *A guide to blockchain Auction.*

[2]. Andreas M. Antonopoulos, Gavin Wood. *Mastering Ethereum is licensed under a Creative Commons Attribution-ShareAlike 4.0 International License.* Based on a work, https://github.com/ethereumbook/ethereumbook.

[3]. Vitalik Buterin, 2022. *Ethereum Whitepaper* Ethereum. Archived from the original on 4 August. Retrieved 6 August.

[4]. Roberts, Jeff, 2019. *Ethereum, Bitcoin's closest rival, faces its moment of truth.* Fortune. Fortune Media IP Limited. Archived from the original on 4 May 2021. Retrieved 5 August 2021.