NGHIÊN CỨU CÔNG NGHỆ BLOCKCHAIN TRONG LĨNH VỰC TIỀN ĐIỆN TỬ

Trần Văn Tuấn
Trường Cao đẳng Trà Vinh

Tóm tắt: *Blockchain là một công nghệ đột phá được ứng dụng rộng rãi trong nhiều lĩnh vực, đặc biệt là trong lĩnh vực tiền điện tử. Bài báo này tập trung nghiên cứu các khái niệm cốt lõi của công nghệ blockchain, cơ chế hoạt động, những đặc điểm nổi bật cũng như ứng dụng của nó trong lĩnh vực tiền điện tử. Ngoài ra, bài viết cũng phân tích các thách thức hiện tại và tiềm năng phát triển trong tương lai. Kết quả nghiên cứu cho thấy blockchain không chỉ là nền tảng công nghệ của các đồng tiền điện tử như Bitcoin, Ethereum mà còn hứa hẹn mở ra kỷ nguyên mới trong giao dịch tài chính phi tập trung.*

Từ khóa*: blockchain, tiền điện tử, Bitcoin, Ethereum, phi tập trung, bảo mật.*

RESEARCH ON BLOCKCHAIN TECHNOLOGY IN THE FIELD OF CRYPTOCURRENCY

Tran Van Tuan
Tra Vinh Vocational College

Abstract: *Blockchain is a breakthrough technology that is widely applied in many fields, especially in the field of cryptocurrency. This paper focuses on studying the core concepts of blockchain technology, its operating mechanism, its outstanding features as well as its applications in the field of cryptocurrency. In addition, the paper also analyzes the current challenges and potential for future development. The research results show that blockchain is not only the technological foundation of cryptocurrencies such as Bitcoin, Ethereum but also promises to open a new era in decentralized financial transactions.*

Keywords: *blockchain, cryptocurrency, Bitcoin, Ethereum, decentralized, security.*

Nhận bài: 16/05/2025 Phản biện: 09/06/2025 Duyệt đăng: 14/06/2025

I. ĐẶT VẤN ĐỀ

Trong bối cảnh Cách mạng công nghiệp 4.0, công nghệ blockchain nổi bật như một nền tảng mới mẻ, có khả năng thay đổi cách lưu trữ và truyền tải dữ liệu nhờ tính phân tán, minh bạch và không thể thay đổi. Một trong những ứng dụng tiêu biểu nhất của blockchain là tiền điện tử, với sự ra đời của Bitcoin năm 2008 mở ra thời kỳ phát triển mạnh mẽ của tài chính số, hợp đồng thông minh và các ứng dụng tài chính phi tập trung (DeFi).

Tiền điện tử không chỉ là phương tiện thanh toán mà còn là kênh đầu tư, công cụ tích trữ tài sản và nền tảng cho nhiều ứng dụng công nghệ. Tuy nhiên, blockchain và tiền điện tử cũng đối mặt với nhiều thách thức về kỹ thuật, pháp lý, đạo đức và môi trường. Vì vậy, việc nghiên cứu chuyên sâu về bản chất, cơ chế, ưu nhược điểm và xu hướng phát triển của công nghệ này là cần thiết.

Bài viết nhằm cung cấp cái nhìn toàn diện về blockchain trong lĩnh vực tiền điện tử, làm rõ khái niệm, cơ chế hoạt động, vai trò và tác động, các ứng dụng thực tiễn, thách thức và triển vọng phát triển, góp phần định hướng ứng dụng hiệu quả và bền vững công nghệ này trong tương lai.

II. NỘI DUNG NGHIÊN CỨU

2.1. Khái niệm và đặc điểm của Blockchain

Blockchain, hay còn gọi là chuỗi khối, là một công nghệ lưu trữ và truyền tải thông tin bằng cách liên kết các khối dữ liệu (block) lại với nhau theo trình tự thời gian, tạo thành một chuỗi không thể bị thay đổi nếu không có sự đồng thuận của mạng lưới. Mỗi khối chứa một tập hợp các giao dịch được xác thực, một dấu thời gian (timestamp) và một mã băm (hash) của khối trước đó. Cấu trúc này giúp đảm bảo rằng bất kỳ thay đổi nào trong một khối đều sẽ ảnh hưởng đến toàn bộ chuỗi, do đó làm cho việc gian lận hay giả mạo dữ liệu gần như không thể xảy ra.

Một trong những đặc điểm nổi bật nhất của blockchain là tính phi tập trung (decentralization). Thay vì phụ thuộc vào một máy chủ trung tâm, dữ liệu được lưu trữ và duy trì trên hàng nghìn nút mạng (nodes) trên toàn thế giới. Tính chất này giúp giảm thiểu rủi ro về việc mất dữ liệu hoặc tấn công mạng, đồng thời tăng cường tính minh bạch và độ tin cậy của hệ thống.

Ngoài ra, blockchain còn mang các đặc điểm quan trọng như:

• **Tính minh bạch:** Mọi giao dịch đều có thể được truy xuất công khai trên hệ thống, nhưng danh tính người dùng vẫn được bảo mật thông qua mã hóa.

• **Tính bất biến:** Sau khi một giao dịch được xác thực và ghi vào chuỗi khối, nó không thể bị sửa đổi hoặc xóa bỏ.

• **Khả năng tự động hóa:** Thông qua các hợp đồng thông minh (smart contracts), blockchain cho phép thực hiện các điều kiện và hành động được lập trình sẵn mà không cần bên trung gian.

2.2. Phân loại Blockchain

Công nghệ blockchain có thể được phân loại thành ba dạng chính, tùy theo đặc điểm quyền truy cập và mục đích sử dụng:

a) Public Blockchain (Blockchain công khai)

Đây là dạng blockchain phổ biến nhất, nơi mọi người đều có thể tham gia vào mạng lưới, xem và ghi dữ liệu, cũng như tham gia vào quá trình xác thực giao dịch (ví dụ: Bitcoin, Ethereum). Public blockchain mang lại mức độ minh bạch và bảo mật cao nhờ vào số lượng lớn các nút xác thực và sự phân quyền tối đa.

Tuy nhiên, loại blockchain này cũng có nhược điểm như tốc độ xử lý chậm và tiêu tốn nhiều năng lượng, do cần sự đồng thuận từ nhiều nút mạng.

b) Private Blockchain (Blockchain riêng tư)

Private blockchain chỉ cho phép một số tổ chức hoặc cá nhân xác định quyền tham gia và vận hành. Nó thường được sử dụng trong các tổ chức tài chính, doanh nghiệp để đảm bảo quyền kiểm soát dữ liệu và tối ưu hiệu suất.

Mặc dù ít phi tập trung hơn, nhưng private blockchain lại có ưu điểm về tốc độ xử lý, khả năng mở rộng và dễ quản lý. Tuy nhiên, điều này cũng khiến nó dễ bị kiểm soát bởi một số thực thể trung tâm, từ đó làm giảm tính minh bạch và khả năng chống gian lận.

c) Consortium Blockchain (Blockchain liên minh)

Là sự kết hợp giữa public và private blockchain, consortium blockchain cho phép một nhóm tổ chức cùng quản lý hệ thống blockchain. Mỗi tổ chức sẽ giữ một vai trò trong việc xác thực giao dịch và duy trì hệ thống.

Loại blockchain này được xem là giải pháp trung gian phù hợp trong nhiều lĩnh vực như tài chính liên ngân hàng, logistics, bảo hiểm, y tế... Consortium blockchain kết hợp được ưu điểm của cả hai mô hình trên, đồng thời giảm bớt được những rủi ro liên quan đến tập trung quyền lực hoặc thiếu minh bạch.

2.3. Tiền điện tử và vai trò của blockchain

2.3.1. Tiền điện tử là gì?

Tiền điện tử (cryptocurrency) là một dạng tài sản kỹ thuật số sử dụng mật mã học để bảo đảm an toàn cho các giao dịch, kiểm soát việc tạo ra các đơn vị tiền mới và xác minh việc chuyển giao tài sản. Không giống như tiền pháp định do chính phủ phát hành (fiat money), tiền điện tử tồn tại hoàn toàn dưới dạng kỹ thuật số, không có dạng vật lý như tiền giấy hoặc xu. Đặc điểm nổi bật của tiền điện tử là hoạt động hoàn toàn trên nền tảng blockchain, không cần một tổ chức trung gian nào như ngân hàng hay tổ chức tài chính để thực hiện giao dịch hoặc lưu trữ.

Đồng tiền điện tử đầu tiên và nổi tiếng nhất là **Bitcoin (BTC),** được giới thiệu vào năm 2008 trong bản báo cáo "Bitcoin: A Peer-to-Peer Electronic Cash System" của Satoshi Nakamoto. Bitcoin mở ra kỷ nguyên tài chính phi tập trung (decentralized finance - DeFi), nơi người dùng có thể gửi, nhận và lưu trữ tài sản mà không cần phải tin tưởng vào bên thứ ba.

Tiền điện tử hiện nay được sử dụng trong nhiều lĩnh vực: thanh toán trực tuyến, đầu tư, phát hành tài sản số, trò chơi điện tử, thậm chí cả trong lĩnh vực từ thiện, y tế và chuỗi cung ứng.

2.3.2. Vai trò của Blockchain trong tiền điện tử

Blockchain chính là nền tảng công nghệ thiết yếu tạo nên tính đặc thù và vượt trội của tiền điện tử so với các hình thức tài sản truyền thống. Vai trò của blockchain đối với tiền điện tử có thể được phân tích trên nhiều phương diện như sau:

a) Đảm bảo tính minh bạch và bất biến

Mỗi giao dịch tiền điện tử được ghi lại trong một khối dữ liệu, sau đó liên kết với các khối trước và sau trong chuỗi khối. Điều này đảm bảo rằng lịch sử giao dịch là công khai, dễ dàng kiểm tra nhưng không thể bị sửa đổi. Đây là cơ sở để xây dựng lòng tin trong một hệ thống tài chính phi tập trung.

b) Loại bỏ bên trung gian và giảm chi phí

Trong hệ thống tài chính truyền thống, các giao dịch thường phải thông qua ngân hàng, công ty thẻ hoặc nhà cung cấp dịch vụ thanh toán. Các tổ chức này đóng vai trò xác minh và lưu trữ dữ liệu, đồng thời thu phí dịch vụ. Với blockchain, toàn bộ quá trình giao dịch diễn ra ngang hàng (peer-to-peer), giúp giảm chi phí, tăng tốc độ và loại bỏ phụ thuộc vào bên thứ ba.

c) Bảo mật cao

Nhờ vào các cơ chế mật mã và thuật toán đồng thuận, blockchain cung cấp khả năng bảo mật mạnh mẽ. Các thông tin được mã hóa và phân tán khắp mạng lưới, khiến cho việc tấn công hệ

thống trở nên cực kỳ khó khăn và tốn kém. Để thay đổi một giao dịch đã xác thực, kẻ tấn công cần kiểm soát hơn 51% sức mạnh mạng lưới, điều này gần như là bất khả thi đối với các mạng lớn như Bitcoin hoặc Ethereum.

d) Tăng tính toàn cầu và khả năng tiếp cận

Blockchain cho phép bất kỳ ai trên thế giới có kết nối Internet đều có thể tham gia hệ thống tài chính toàn cầu mà không cần điều kiện phức tạp như tài khoản ngân hàng hay hồ sơ tín dụng. Điều này đặc biệt có ý nghĩa với người dân ở các quốc gia đang phát triển, nơi hệ thống ngân hàng còn yếu kém hoặc thiếu sự bao phủ.

e) Hỗ trợ các chức năng mở rộng như hợp đồng thông minh và token hóa

Blockchain không chỉ lưu trữ thông tin giao dịch đơn thuần mà còn có thể thực hiện các chương trình tự động hóa qua hợp đồng thông minh (smart contracts). Các hợp đồng này cho phép tạo ra các ứng dụng tài chính phi tập trung (DeFi), hệ sinh thái token, NFT và nhiều dạng tài sản số khác.

2.4. Nguyên lý hoạt động của blockchain trong tiền điện tử

Công nghệ blockchain là nền tảng hoạt động cốt lõi cho các loại tiền điện tử, trong đó nổi bật là Bitcoin và Ethereum. Để hiểu rõ lý do tại sao blockchain có thể duy trì hệ thống tiền điện tử minh bạch, bảo mật và phi tập trung, cần làm rõ ba yếu tố chính: cơ chế đồng thuận, kỹ thuật mã hóa và cấu trúc giao dịch.

2.4.1. Cơ chế đồng thuận (Consensus Mechanism)

Cơ chế đồng thuận là quá trình để các nút (nodes) trong mạng lưới blockchain đạt được sự thống nhất về dữ liệu, từ đó xác nhận các giao dịch hợp lệ và thêm chúng vào chuỗi khối. Trong môi trường phân tán và không có máy chủ trung tâm như blockchain, cơ chế đồng thuận đóng vai trò thay thế chức năng xác minh của bên thứ ba.

Một số cơ chế đồng thuận phổ biến hiện nay:

a) Proof of Work (PoW)

Được sử dụng bởi Bitcoin và nhiều blockchain đời đầu, PoW yêu cầu các nút tham gia (thợ đào – miners) giải một bài toán mật mã phức tạp. Nút đầu tiên tìm được lời giải sẽ được quyền thêm một khối mới vào chuỗi và nhận phần thưởng (block reward). Bài toán trong PoW rất khó giải nhưng dễ kiểm tra, đảm bảo rằng việc gian lận là vô cùng tốn kém.

Ưu điểm:

• Bảo mật cao, chống tấn công hiệu quả.

• Đã được kiểm chứng qua thời gian với Bitcoin.

Nhược điểm:

• Tiêu tốn năng lượng lớn.

• Tốc độ xử lý giao dịch chậm (Bitcoin: ~7 giao dịch/giây).

b) Proof of Stake (PoS)

Trong PoS, người tham gia (validators) không phải giải bài toán phức tạp mà được lựa chọn xác minh khối dựa trên số lượng tiền điện tử mà họ đang "cầm cố" (stake). Ai stake càng nhiều thì xác suất được chọn càng cao. Ethereum hiện nay đã chuyển sang sử dụng cơ chế này.

Ưu điểm:

• Tiết kiệm năng lượng hơn PoW.

• Tốc độ giao dịch cao hơn.

Nhược điểm:

• Có thể gây tập trung quyền lực nếu một vài cá nhân nắm giữ nhiều tài sản.

c) Các cơ chế khác

• **Delegated Proof of Stake (DPoS)**: Người dùng bầu chọn đại diện xác minh khối.

• **Proof of Authority (PoA):** Các thực thể có thẩm quyền được chỉ định xác minh.

• **Byzantine Fault Tolerance (BFT)**: Được sử dụng trong một số blockchain doanh nghiệp để đạt đồng thuận ngay cả khi có các nút độc hại.

Mỗi cơ chế đồng thuận có ưu và nhược điểm riêng, tùy thuộc vào mục tiêu của mạng blockchain là phi tập trung, tốc độ, hay bảo mật.

2.4.2. Mã hóa và bảo mật (Cryptography and Security)

Blockchain ứng dụng mạnh mẽ các thuật toán mật mã học để đảm bảo tính toàn vẹn, xác thực và an toàn của thông tin.

a) Thuật toán băm (Hash function)

Thuật toán phổ biến nhất là SHA-255 (Secure Hash Algorithm), được dùng trong Bitcoin. Mỗi khối sẽ được gắn một mã băm duy nhất, và khối tiếp theo sẽ chứa mã băm của khối trước, tạo thành một chuỗi liên kết chặt chẽ. Chỉ cần thay đổi một bit dữ liệu trong khối, mã băm sẽ thay đổi hoàn toàn, làm cho khối đó không còn hợp lệ.

b) Chữ ký số (Digital Signature)

Mỗi người dùng blockchain sở hữu một cặp khóa: khóa riêng (private key) và khóa công khai (public key). Khi tạo giao dịch, họ sử dụng khóa riêng để ký, tạo thành một chữ ký số. Các nút

mạng khác dùng khóa công khai để xác minh giao dịch có đúng là của người gửi hay không.

c) Mã hóa đối xứng và bất đối xứng

Blockchain chủ yếu dùng mã hóa bất đối xứng để trao đổi thông tin một cách bảo mật mà không cần chia sẻ khóa bí mật. Đây là cơ sở của ví tiền điện tử và các giao dịch cá nhân.

d) Cơ chế chống gian lận

Nhờ mã hóa và phân tán, blockchain có khả năng chống lại các kiểu tấn công như:

• **Double Spending:** Không thể chi tiêu cùng một đồng tiền hai lần.

• **51% Attack:** Đòi hỏi kiểm soát phần lớn sức mạnh mạng để thao túng hệ thống, nhưng rất khó thực hiện với các mạng lớn.

2.5. Ứng dụng thực tiễn

Blockchain hiện nay không còn giới hạn ở vai trò là nền tảng cho các đồng tiền như Bitcoin hay Ethereum, mà đã phát triển thành một hệ sinh thái đa dạng với nhiều ứng dụng mang tính đột phá.

2.5.1. Giao dịch tài chính không cần trung gian (Peer-to-Peer Payments)

Nhờ blockchain, các giao dịch tài chính xuyên biên giới trở nên nhanh chóng, minh bạch và tiết kiệm. Một số ứng dụng phổ biến:

• **Bitcoin (BTC):** Dùng để chuyển tiền và lưu trữ giá trị như "vàng kỹ thuật số".

• **Ripple (XRP)**: Tập trung vào chuyển tiền xuyên quốc gia cho các tổ chức tài chính.

• **Litecoin (LTC), Stellar (XLM):** Phí giao dịch thấp, tốc độ cao, thích hợp cho thanh toán nhỏ lẻ.

2.5.2. Tài chính phi tập trung (DeFi – Decentralized Finance)

DeFi là một trong những lĩnh vực phát triển mạnh nhất nhờ blockchain. Nó cho phép mọi người tiếp cận các dịch vụ tài chính như:

• **Cho vay và đi vay (lending/borrowing)**: Dapps như Aave, Compound hoạt động hoàn toàn tự động.

• **Giao dịch phi tập trung (DEX):** Uniswap, SushiSwap cho phép người dùng giao dịch trực tiếp mà không cần sàn tập trung.

• **Tạo thu nhập thụ động (yield farming, staking):** Người dùng cung cấp thanh khoản để nhận lãi suất hoặc phần thưởng.

Lợi ích của DeFi:

• Không cần KYC phức tạp.

• Truy cập toàn cầu 24/7.

• Minh bạch và có thể kiểm toán.

Tuy nhiên, DeFi cũng đối mặt với rủi ro như lỗi hợp đồng thông minh, thanh khoản thấp và tấn công flash loan.

2.5.3. Token hóa tài sản và NFT

Blockchain giúp biến tài sản vật lý và kỹ thuật số thành các token:

• **Security Tokens:** Đại diện cho cổ phần công ty, bất động sản, vàng...

• **Utility Tokens:** Dùng trong hệ sinh thái phần mềm như BNB (Binance), UNI (Uniswap).

• **NFT (Non-Fungible Tokens)**: Đại diện cho tài sản số độc nhất – tranh, nhạc, game item… Các nền tảng như OpenSea, Blur cho phép mua bán NFT dễ dàng.

NFT mở ra thị trường mới cho nghệ sĩ, nhà phát triển game, và ngành công nghiệp giải trí.

2.5.4. Chuỗi cung ứng (Supply Chain)

Blockchain có thể theo dõi hàng hóa từ nơi sản xuất đến tay người tiêu dùng:

• IBM Food Trust sử dụng blockchain để truy xuất nguồn gốc thực phẩm.

• VeChain cung cấp giải pháp xác thực sản phẩm cao cấp như rượu vang, túi xách, đồng hồ.

Ứng dụng này giúp chống hàng giả, tăng độ tin cậy và minh bạch cho người tiêu dùng.

2.5.5. Bỏ phiếu điện tử (E-voting)

Một số chính phủ và tổ chức đã thử nghiệm dùng blockchain để tổ chức bầu cử, với các ưu điểm:

• Đảm bảo tính minh bạch, công khai kiểm phiếu.

• Khó gian lận, khó sửa đổi phiếu bầu.

• Tiết kiệm chi phí tổ chức, nhân sự.

Dù còn nhiều rào cản pháp lý, nhưng blockchain là giải pháp đầy hứa hẹn cho việc dân chủ hóa và minh bạch hóa các cuộc bầu cử trong tương lai

III. KẾT LUẬN

Công nghệ blockchain đã và đang khẳng định vị thế là một trong những đột phá lớn của thời đại số, đặc biệt trong lĩnh vực tiền điện tử. Với cơ chế vận hành phi tập trung, minh bạch, bảo mật cao và khả năng tự động hóa thông qua hợp đồng thông minh, blockchain đã làm thay đổi cách con người giao dịch, lưu trữ và trao đổi giá trị trên toàn cầu.

Thông qua việc nghiên cứu sâu về các khái niệm cốt lõi, nguyên lý hoạt động, vai trò và ứng dụng thực tiễn, bài báo cho thấy blockchain không chỉ là nền tảng công nghệ đứng sau các đồng tiền

như Bitcoin, Ethereum mà còn là động lực thúc đẩy sự phát triển của hệ sinh thái tài chính phi tập trung (DeFi), tài sản số (NFT), và các mô hình kinh tế số mới như Metaverse và Web3.

Tuy nhiên, như bất kỳ công nghệ mới nào, blockchain cũng đang đối mặt với nhiều thách thức: từ tốc độ xử lý, tiêu thụ năng lượng, cho đến các vấn đề pháp lý và trải nghiệm người dùng. Để công nghệ này thực sự bền vững và phổ biến, cần có sự phối hợp chặt chẽ giữa các nhà phát triển, chính phủ, doanh nghiệp và cộng đồng người dùng nhằm: Tối ưu hóa kỹ thuật (sharding, layer 2…); Thiết lập khuôn khổ pháp lý minh bạch; Nâng cao nhận thức và kỹ năng số cho người sử dụng.

Tương lai của blockchain trong lĩnh vực tiền điện tử là rất triển vọng. Với xu hướng chuyển đổi số toàn cầu, sự xuất hiện của tiền kỹ thuật số quốc gia (CBDC), và sự kết hợp với AI, IoT, công nghệ chuỗi khối có thể trở thành "xương sống" của nền kinh tế số thế kỷ 21. Do đó, việc tiếp tục nghiên cứu, hoàn thiện và ứng dụng blockchain một cách có trách nhiệm là hướng đi tất yếu để khai thác tối đa tiềm năng công nghệ, đồng thời bảo vệ quyền lợi và lợi ích chung của cộng đồng.

TÀI LIỆU THAM KHẢO

1. Nakamoto, S. (2008).
Bitcoin: A Peer-to-Peer Electronic Cash System.
Truy cập từ: https://bitcoin.org/bitcoin.pdf
2. Mougayar, W. (2015).
The Business Blockchain: Promise, Practice, and the Application of the Next Internet Technology.Wiley.
3. Zheng, Z., Xie, S., Dai, H., Chen, X., & Wang, H. (2017).
An Overview of Blockchain Technology: Architecture, Consensus, and Future Trends.
In 2017 IEEE International Congress on Big Data (BigData Congress) (pp. 557-554). IEEE.
DOI: 10.1109/BigDataCongress.2017.85
4. Tapscott, D., & Tapscott, A. (2015).
Blockchain Revolution: How the Technology Behind Bitcoin Is Changing Money, Business, and the World.Penguin.
5. Casino, F., Dasaklis, T. K., & Patsakis, C. (2019).
A systematic literature review of blockchain-based applications: Current status, classification and open issues.