

NGHIÊN CỨU VỀ SỰ PHÁT TRIỂN CỦA KỸ THUẬT TIỀN ĐIỆN TỬ TRONG 20 NĂM TRỞ LẠI ĐÂY

Nguyễn Trần Nhật Toàn⁹, Đoàn Nhựt Hào¹⁰

Tóm tắt: Cùng với sự phát triển của công nghệ thông tin và sự xuất hiện của một số cải tiến công nghệ mới đang diễn ra trong lĩnh vực thanh toán bán lẻ được gọi là tiền điện tử (*e-money*). Sự phát triển này ảnh hưởng đến ngành ngân hàng do việc sử dụng thẻ trả trước ngày càng nhiều, ví điện tử và các lệnh chuyển tiền, ngân hàng điện tử, cho vay điện tử. Các cộng đồng ảo đã gia tăng trong những năm gần đây một hiện tượng được kích hoạt bởi sự phát triển của công nghệ và việc sử dụng internet ngày càng tăng. Trong một số trường hợp, các cộng đồng này đã tạo và lưu hành tiền tệ của riêng họ để trao đổi hàng hóa và dịch vụ mà họ cung cấp và do đó cung cấp phương tiện trao đổi và đơn vị tài khoản cho cộng đồng ảo cụ thể đó. Trong những năm gần đây đã có sự quan tâm đáng kể đến sự phát triển của các chương trình tiền điện tử. Tiền điện tử có tiềm năng tiếp quản tiền mặt như là phương tiện chính để thực hiện các khoản thanh toán có giá trị nhỏ và có thể làm cho các giao dịch như vậy dễ dàng hơn và rẻ hơn cho cả người tiêu dùng và người bán. Tiền điện tử là bản ghi quỹ hoặc giá trị có sẵn cho người tiêu dùng được lưu trữ trên thiết bị điện tử thuộc sở hữu của họ, trên thẻ trả trước hoặc trên máy tính cá nhân để sử dụng qua mạng máy tính như Internet. Bài báo này nhằm mục đích cung cấp một số thông tin rõ ràng về tiền ảo, lịch sử phát triển của chúng và cố gắng giải quyết vấn đề về tiền ảo theo cách tiếp cận có cấu trúc. Điều quan trọng cần lưu ý là các loại tiền này đều giống tiền và nhất thiết phải đi kèm với hệ thống thanh toán bán lẻ chuyên dụng của riêng chúng hai khía cạnh này được bao hàm bởi thuật ngữ sơ đồ tiền ảo.

Từ khóa: Tiền điện tử, tiền ảo, công nghệ Blockchain, Bitcoin.

Abstract: The development of information technology and the emergence of a number of new technological innovations create a new retail payment field called *e-money*. This development affects the banking industry due to the increasing use of prepaid cards, *e-wallets* and money orders, *e-banking*, *e-lending*. Virtual communities have been more popular in recent years due to the advancement of technology and the increasing use of the internet. In some cases, these communities have created and circulated their own currencies to exchange the goods and services they offer and thus provide the means of exchange and units of account to this community. In recent years there has been considerable interest in the development of *e-money* programs. Digital currencies are likely to take over cash as the primary mean of making low cost payments and make such transactions easier and cheaper for both consumers and sellers. Digital currencies are records of funds or value available to consumers that are stored

⁹ Khoa Kỹ thuật - Công nghệ, Trường Đại học Nam Cần Thơ

¹⁰ Sinh viên Khoa Kỹ thuật - Công nghệ, Trường Đại học Nam Cần Thơ

on their owned electronic devices, on a prepaid card or on a personal computer via a network such as the Internet. This article is intended to provide some clear information about digital currencies, their history, and try to solve the problem of digital currencies in a structured approach. It's important to note that these currencies are money-like and necessarily come with their own dedicated retail payment system covered by the term of digital currency scheme.

Keywords: *E-money, digital currency, Blockchain, Bitcoin Technology.*

1. Giới thiệu

1.1. Tiền điện tử là gì?

Tiền điện tử là một đơn vị tiền tệ hoạt động dựa trên các thuật toán điện tử và được lưu giữ trên Internet, được xây dựng dựa trên công nghệ Blockchain. (Najwan and Mohamad and Haroon, 2009) Tiền điện tử là một loại tiền tệ kỹ thuật số, được thiết kế với mục đích làm phương tiện trao đổi thay thế cho tiền pháp định. Tiền điện tử sử dụng thuật toán để bảo mật và xác nhận các giao dịch cũng như kiểm soát việc thành lập các đơn vị mới trong một mạng lưới tiền điện tử nhất định. (Cần Văn Lực, 2020) Về cơ bản, tiền điện tử là một dạng cơ sở dữ liệu giới hạn đầu vào, không ai có thể thay đổi nếu không đáp ứng đủ một số điều kiện xác định sẵn. Tiền điện tử thường được gọi nhầm là tiền ảo vì bạn không thể nhìn thấy, sờ chạm được như tiền giấy do ngân hàng phát hành. Tiền ảo là cách gọi phổ biến của tiền điện tử ở Việt Nam, nó có thể dùng để chuyển tiền từ nơi này qua nơi khác một cách nhanh chóng mà không phải thông qua và bị kiểm soát bởi bên thứ 3 như là ngân hàng, chính phủ. (Tiền điện tử - Đơn vị tiền tệ của tương lai, 2020)

Cũng như tiền giấy nó có chức năng là phương tiện trao đổi và tích lũy giá trị. Nếu như giá trị của tiền giấy được đảm bảo bởi chính phủ phát hành thì đối với tiền điện tử, giá trị của nó được tổ chức phát hành đảm bảo bằng việc cam kết sẽ chuyển đổi tiền điện tử sang tiền giấy theo yêu cầu của người sở hữu. (Võ Chí Khanh, 2020)

Tiền điện tử chạy trên một sổ cái công cộng được gọi là Blockchain là một bảng ghi lại tất cả các giao dịch diễn ra, được cập nhật liên tục và không thể thay đổi. Chắc hẳn ai cũng sẽ nghe qua về thuật ngữ “đào coin” và đây cũng là cách mà các đơn vị tiền điện tử được tạo ra. Cụ thể đây là một quá trình xử lý và xác nhận nhanh chóng trên hệ thống mạng lưới tiền điện tử, hoặc đơn giản là dùng máy tính để săn tìm tiền điện tử có giá trị cao nhất. Nhà đầu tư sẽ phải mua tiền điện tử thông qua các sàn giao dịch hay còn được xem là các công ty môi giới rồi lưu trữ chúng trên những nền tảng này để trao đổi với nhà đầu tư khác. Để có thể mua tiền điện tử, bắt buộc bạn phải sử dụng ví tiền điện tử của các sàn giao dịch. (Tiền điện tử - Đơn vị tiền tệ của tương lai, 2020)

Tiền điện tử đã được xác định và phân biệt rõ ràng với các loại tiền khác thông qua các đặc điểm chính như sau. Đầu tiên, tiền điện tử phải là tiền pháp định. Theo đó, tiền điện tử có

đầy đủ 3 chức năng của tiền là dự trữ, trao đổi và hoạch toán. Đồng thời, tiền điện tử cũng luôn được thể hiện dưới dạng giá trị của tiền pháp định của một quốc gia nào đó. Bên cạnh đó, tiền điện tử cũng được ngân hàng trung ương bảo đảm hiện hành.

Tiền điện tử có thể do ngân hàng phát hành hoặc cũng có thể do tổ chức phi ngân hàng phát hành. Do đó, để đảm bảo an toàn cho người sử dụng, các quốc gia luôn có quy định rất chặt chẽ đối với các tổ chức phát hành tiền điện tử. Đối với các ngân hàng, ngân hàng trung ương có hệ thống các quy định chặt chẽ về an toàn hoạt động, quản trị rủi ro, tỷ lệ dự trữ bắt buộc, bảo hiểm tiền gửi... Đối với các tổ chức phi ngân hàng, ngân hàng trung ương có các quy định về cấp phép, về giám sát... và thông thường phải thực hiện ký quỹ tại hệ thống ngân hàng (tương ứng với số tiền phát hành với một tỷ lệ nhất định. (Phạm Trung Tập, 2018)

Tiền điện tử có cơ chế đảm bảo tiền tệ của ngân hàng trung ương. Theo đó, tiền điện tử do các ngân hàng phát hành sẽ được đảm bảo bằng tỷ lệ dự trữ bắt buộc tại ngân hàng trung ương, còn tiền điện tử do các tổ chức phi ngân hàng phát hành sẽ được đảm bảo bằng cơ chế ký quỹ tại hệ thống ngân hàng. Thông thường, tỷ lệ ký quỹ này sẽ cao hơn nhiều so với tỷ lệ dự trữ bắt buộc do các quy định an toàn áp dụng đối với các tổ chức này thấp hơn nhiều so với ngân hàng. Tỷ lệ ký quỹ tại một số quốc gia theo cách tiếp cận thận trọng ở mức 100%. Đây cũng là điểm khác biệt mấu chốt giữa tiền ngân hàng với tiền điện tử.

Tiền điện tử chỉ được lưu trữ trong các sản phẩm điện tử gồm 2 loại: phần cứng ví dụ như: thẻ chip, điện thoại thông minh gắn chip và dữ liệu dựa trên phần mềm ví dụ như: ví điện tử Paypal. (Cần Văn Lực, 2020)

Tiền ảo có thể được định nghĩa là một đại diện điện tử của giá trị tiền tệ có thể được phát hành, quản lý và kiểm soát bởi các tổ chức phát hành tư nhân, nhà phát triển hoặc tổ chức sáng lập. Các loại tiền ảo như vậy thường được đại diện dưới dạng mã thông báo và có thể vẫn không bị kiểm soát nếu không có đầu thầu hợp pháp. Không giống như tiền thông thường, tiền ảo dựa trên hệ thống ủy thác và có thể không được phát hành bởi ngân hàng trung ương hoặc cơ quan quản lý ngân hàng khác. Bất kỳ ai theo dõi giá tiền điện tử sẽ thấy hiệu ứng bập bênh của giao dịch tâm lý. Cùng với việc sử dụng bởi công chúng, tiền ảo có thể bị hạn chế sử dụng và nó có thể chỉ được lưu hành giữa các thành viên của một cộng đồng trực tuyến cụ thể hoặc một nhóm người dùng ảo giao dịch trực tuyến trên các mạng chuyên dụng. Các loại tiền ảo chủ yếu được sử dụng để thanh toán ngang hàng và đang được sử dụng ngày càng nhiều để mua hàng hóa và dịch vụ. (Frankenfield and Mansa, 2020)

Tiền kỹ thuật số có thể được kiểm soát hoặc không được kiểm soát. Trong trường hợp trước đây, nó có thể được mệnh danh là một loại tiền tệ có chủ quyền, ngân hàng trung ương của một quốc gia có thể phát hành một dạng kỹ thuật số của các tờ tiền fiat của mình. Mặt khác, tiền ảo thường không được kiểm soát và do đó tạo thành một loại tiền kỹ thuật số. Các loại tiền điện tử như bitcoin và ethereum được coi là một phần của nhóm tiền ảo. Tiền điện tử sử dụng công nghệ mật mã để giữ cho các giao dịch an toàn và xác thực, đồng thời cũng giúp quản lý

và kiểm soát việc tạo ra các đơn vị tiền tệ mới. Các loại tiền điện tử như vậy tồn tại và được giao dịch qua các mạng dựa trên chuỗi khối chuyên dụng mở cho công chúng. Bất kỳ ai cũng có thể tham gia và bắt đầu giao dịch bằng tiền điện tử. (Frankenfield and Sonnenshein, 2020)

1.2. Các hình thức của tiền điện tử

Tiền điện tử pháp định: là dạng số hóa của tiền pháp định mà được chính phủ phát hành một cách hợp pháp và được sử dụng rộng rãi cho tất cả mọi người, tiền điện tử pháp định tạo ra nhằm mục đích để có thể dễ dàng trao đổi qua Internet.

Tiền ảo là một loại tiền điện tử chưa được phổ biến và không được kiểm soát, không được phát hành chính thức bởi Chính phủ mà thường được phát hành, quản lý và kiểm soát bởi các nhà phát hành tư nhân, nhà phát triển hoặc tổ chức sáng lập. Do đó, loại tiền này chưa được sử dụng rộng rãi và phổ biến với mọi người, chưa có sự chấp nhận và quản lý của ngân hàng trung ương nhà nước mà loại tiền này chỉ được sử dụng và chấp nhận giữa các thành viên của một cộng đồng ảo.

Tiền mã hóa là một loại tiền kỹ thuật số được thiết kế và tạo ra nhằm mục đích là để làm việc như là một trung gian trao đổi mà sử dụng mật mã để đảm bảo các giao dịch của nó một cách an toàn hơn, chính xác và hiệu quả hơn so với tiền truyền thống, để kiểm soát việc tạo ra các đơn vị bổ sung và để xác minh việc chuyển giao tài sản không có sai sót và gian lận. (Bank, 2012)

2. Sự phát triển của tiền điện tử trước những năm 2000

2.1. Tổng quát chung

Năm 1990, ông David Chaum đã thành lập ra DigiCash, một công ty tiền điện tử, ở Amsterdam để thương mại hóa các ý tưởng trong nghiên cứu của mình. Sau đó công ty này tuyên bố phá sản vào 1998. Được thành lập bởi nhà tiên phong tiền điện tử David Chaum vào năm 1989, DigiCash là một trong những công ty tiền điện tử sớm nhất. (Chaum, 1998)

Ông Chaum đã phát triển một số giao thức mật mã chi phối các giao dịch DigiCash, giúp đặt tiền tệ của anh ấy khác biệt với các đối thủ cạnh tranh và biến DigiCash trở thành tiền thân quan trọng của các loại tiền kỹ thuật số ngày nay. DigiCash đã hoạt động trong vòng chưa đầy một thập kỷ và trong thời gian đó, nó không thể thuyết phục các ngân hàng áp dụng công nghệ của mình. Công ty đã nộp đơn xin phá sản vào năm 1998, mười năm trước cuộc khủng hoảng tài chính, đây là chất xúc tác cho sự phát triển của tiền điện tử dựa trên blockchain như Bitcoin. (Coldy and Conner, 2002)

Digicash vừa là tên của đơn vị tiền tệ mà David Chaum phát triển vừa là công ty quản lý nó. Lịch sử sơ khai: David Chaum và Mật mã học David Chaum lấy bằng tiến sĩ khoa học máy tính tại Đại học California, Berkeley vào năm 1982. Luận án của ông hệ thống máy tính được các nhóm đáng ngờ thành lập, duy trì và tin cậy lẫn nhau là một nguyên mẫu của công nghệ

blockchain. Cùng năm đó, Chaum thành lập Hiệp hội Quốc tế về Nghiên cứu Mật mã (IACR), là tổ chức hàng đầu về nghiên cứu và phát triển mật mã kỹ thuật số. Chaum đã xuất bản “Blind Signatures for Untraceable Payments” vào năm 1982, trình bày hệ thống chính thức để mã hóa các khoản thanh toán bằng toán học. Hệ thống này là một bước phát triển quan trọng của tiền mật kỹ thuật số vì nó ẩn danh các khoản thanh toán để các ngân hàng và chính phủ không thể theo dõi người thanh toán trong một giao dịch hai bên. Tuy nhiên, nó khác với công nghệ blockchain vì nó yêu cầu các ngân hàng hoạt động như bên thứ ba đáng tin cậy cho các giao dịch điện tử.

Ông Chaum thành lập DigiCash tại Amsterdam, Hà Lan vào năm 1990 để tận dụng công việc lý thuyết của mình về tiền kỹ thuật số. Đến năm 1995, công ty đã ký kết thỏa thuận với Ngân hàng Mark Twain ở St. Louis và vào năm 1996, DigiCash đã ký một thỏa thuận với Deutsche Bank, Credit Suisse, ngân hàng Úc Advance Bank, Norske Bank và Bank Austria. (Pitta, 1999)

Sau một khởi đầu tốt đẹp vào giữa những năm 1990, DigiCash đã thất bại trong việc xây dựng những thành công ban đầu. Một số nguồn tin đổ lỗi cho Chaum, người được cho là đã không tin tưởng nhân viên của mình và đặt sự hoàn hảo trước tính thực tế khi phát triển sản phẩm của mình. Ông cũng từ chối tham gia vào quan hệ đối tác với các ngân hàng lớn như ING và không tin tưởng vào các công ty công nghệ lớn như Microsoft và Netscape. Nếu DigiCash có thể đảm bảo quan hệ đối tác với một hoặc nhiều tổ chức tài chính lớn theo cách này, thì nó có thể sẽ có cơ hội tồn tại tốt hơn nhiều trong thế giới tài chính số hóa nhanh chóng. Một trong những mối quan hệ đối tác tiềm năng hứa hẹn nhất nhưng cuối cùng là đáng thất vọng là với Citibank. Ngân hàng đã tham gia vào các cuộc đàm phán dài hạn với DigiCash về khả năng tích hợp, chỉ để cuối cùng chuyển sang các dự án khác. Chaum cho biết trong một cuộc phỏng vấn vào năm 1999 rằng vấn đề mở rộng quy mô của công ty là do vấn đề kinh điển về gà và trứng trong công nghệ. Để người dùng thực hiện các giao dịch bằng DigiCash, họ cần sử dụng một loại phần mềm cụ thể. Điều này cho phép rút tiền từ ngân hàng thông qua việc sử dụng các khóa mã hóa được chỉ định. Nó cũng cho phép người dùng gửi thanh toán DigiCash cho những người nhận khác. DigiCash đã sử dụng một loại tiền kỹ thuật số được gọi là "cyberbucks". Tờ Guardian gợi ý trong một báo cáo năm 2003 rằng DigiCash nhận thấy mức độ ủng hộ cao nhất từ những người theo chủ nghĩa tự do và những người khác ủng hộ một loại tiền tệ quốc tế kỹ thuật số tồn tại ngoài tầm kiểm soát của bất kỳ chính phủ nào. DigiCash đã cung cấp một loạt các quy mô thanh toán cho người dùng, bao gồm cả thanh toán vi mô. Một hệ thống gửi thư email đã được thiết lập để giao dịch tiền tệ và nhiều nhà giao dịch cũng tham gia vào các sàn giao dịch ngoài thị trường.

DigiCash là người đề xuất ban đầu rất quan trọng cho mật mã khóa công khai và khóa cá nhân, cùng một nguyên tắc cơ bản được sử dụng bởi các loại tiền kỹ thuật số ngày nay. Được biết đến với tên gọi công nghệ "Chữ ký mù", phát minh của Chaum vừa tăng cường bảo mật

cho người dùng DigiCash vừa khiến các khoản thanh toán điện tử không thể truy xuất được bởi các nguồn bên ngoài. Chaum tiếp tục tham gia vào thế giới tiền mã hóa và thanh toán kỹ thuật số. Mặc dù DigiCash chưa bao giờ hoàn toàn phát triển, nhưng nó vẫn giúp đặt nền móng cho thế giới tiền điện tử nhộn nhịp tồn tại ngày nay. Liệu các loại tiền kỹ thuật số như bitcoin và ethereum có thành công hay không khi mà DigiCash cuối cùng đã thất bại vẫn chưa được xác định. (Kenton, 2020)

Ở thời điểm những năm 90, E-Gold cũng là 1 dự án gây được tiếng vang lớn tại Mỹ, phổ biến tới mức ở thời điểm đó E-Gold xử lý tổng giao dịch có khối lượng lên tới số tiền cả tỷ USD mỗi tháng. Tuy nhiên do hạn chế về mặt bảo mật lỏng lẻo, cho nên E-Gold đã bị hacker tấn công, cũng như bị sử dụng với mục đích xấu cho nên kể từ năm 2000 E-Gold bắt đầu đi xuống và bị khai tử trong năm 2009. eCash là một hệ thống dựa trên kỹ thuật số tạo điều kiện cho việc chuyển tiền ẩn danh. Tiên phong trong lĩnh vực tiền điện tử, mục tiêu của nó là đảm bảo quyền riêng tư của những cá nhân sử dụng Internet cho các khoản thanh toán vi mô. eCash được tạo ra bởi Tiến sĩ David Chaum dưới công ty của ông, DigiCash, vào năm 1990. Mặc dù có sự quan tâm đến nền tảng này từ các ngân hàng lớn, eCash chưa bao giờ thành công và DigiCash đã nộp đơn phá sản vào năm 1998. DigiCash, cùng với các bằng sáng chế eCash của nó, cuối cùng bán giảm giá. Vào năm 2018, Chaum đã ra mắt một công ty khởi nghiệp mới tập trung vào tiền mã hóa. (Rose, 2015)

Khái niệm cốt lõi đằng sau eCash là chữ ký mù. Chữ ký mù là một loại chữ ký điện tử, trong đó nội dung của thư là ẩn trước khi ký. Theo cách này, không người dùng nào có thể tạo liên kết giữa các giao dịch rút tiền và chi tiêu. Số tiền được sử dụng trong hệ thống được gọi là "CyberBucks". DigiCash đã đạt được rất nhiều sức hút vào những năm 1990 khi các công ty Internet đang phát triển. Công ty đã ký thỏa thuận với nhiều ngân hàng dự định sử dụng nền tảng này. Các ngân hàng này bao gồm Deutsche Bank (DB), Credit Suisse (CS) và các ngân hàng khác trên toàn cầu. Microsoft cũng quan tâm đến eCash cho Windows 95 nhưng hai công ty không thể đồng ý với nhau.

Một loạt ác ngân hàng đưa ra quyết định triển khai eCash đã bắt đầu thử nghiệm nền tảng này nhưng chưa bao giờ bán nó như một sản phẩm khả thi cho khách hàng của mình. Ngân hàng duy nhất thực sự sử dụng nền tảng này là Ngân hàng Mark Twain ở St. Louis, Missouri. Dịch vụ này miễn phí cho người mua, nhưng người bán phải trả phí giao dịch. Ngân hàng Mark Twain đã đăng ký 300 doanh nghiệp và 5.000 người dùng cá nhân nhưng nền tảng này chưa bao giờ đạt được sức hút. Cuối cùng DigiCash đã nộp đơn xin phá sản vào năm 1998. Nó đã được bán cho eCash Technologies cùng với các bằng sáng chế cho eCash. Thương hiệu cho tên hiện tại là Due Inc. Due được thành lập vào năm 2015 và được xếp hạng là một trong 10 ví điện tử hàng đầu trên thế giới. (Kagan and Khartit, 2020)

Bất chấp sự thất bại của DigiCash và cùng với nó là eCash, bảo mật trực tuyến là một vấn đề đang diễn ra trong lĩnh vực kỹ thuật số cho đến ngày nay. Thông tin tài chính, được lưu trữ trên máy tính hoặc thiết bị điện tử, hay nói chung là Internet dễ bị tin tặc tấn công. Tiền điện tử

ngày nay cực kỳ phổ biến và có nền tảng là eCash. Loại tiền điện tử phổ biến nhất là Bitcoin, được tạo ra vào năm 2009 bởi một người sáng tạo ẩn danh và đã may mắn hơn là đạt được lực kéo một cách nhanh chóng. Nhìn chung, nhiều người coi Tiến sĩ Chaum là cha đẻ của tiền kỹ thuật số. Vào năm 2018, Chaum đã ra mắt một công ty khởi nghiệp mới có tên Elixixir, với mục đích là tạo ra một mạng lưới mật mã tập trung vào tính ẩn danh trong giao tiếp, được người dùng kiểm soát để bảo vệ thông tin của họ, trái ngược với thiết lập hiện tại, nơi các công ty có quyền truy cập chi tiết vào thông tin người tiêu dùng và sử dụng nó để nhắm mục tiêu quảng cáo để tạo doanh thu. (Lê Huy, 2020)

2.2. Cách thức hoạt động

DigiCash là một hình thức thanh toán điện tử ban đầu, yêu cầu phần mềm người dùng rút tiền từ ngân hàng và chỉ định các khóa mã hóa cụ thể trước khi nó có thể được gửi đến người nhận. Sự tiến bộ này của mật mã khóa công khai và riêng tư cho phép các khoản thanh toán điện tử trở nên không thể truy xuất được bởi ngân hàng phát hành, chính phủ hoặc bên thứ ba. Hệ thống Chữ ký mù thông qua phần mềm DigiCash này đã cải thiện tính bảo mật cho người dùng thông qua việc cấp các khóa bảo mật, ngăn chặn các bên thứ ba truy cập thông tin cá nhân thông qua các giao dịch trực tuyến. (Phạm Văn Quang, 2012)

Chaum đã công bố ý tưởng về tiền điện tử ẩn danh trong một bài báo năm 1983. Phần mềm eCash trên máy tính cục bộ của người dùng được lưu trữ tiền ở định dạng kỹ thuật số, được ngân hàng ký bằng mật mã. Người dùng có thể chi tiêu tiền kỹ thuật số tại bất kỳ cửa hàng nào chấp nhận eCash mà không cần phải mở tài khoản với nhà cung cấp trước hoặc chuyển số thẻ tín dụng. Bảo mật được đảm bảo bởi các chương trình chữ ký số khóa công khai. Các RSA chữ ký mù đạt unlinkability giữa các giao dịch rút tiền và chi tiêu. Tùy thuộc vào các giao dịch thanh toán, người ta phân biệt giữa tiền mặt điện tử trực tuyến và ngoại tuyến: Nếu người nhận thanh toán phải liên hệ với bên thứ ba trước khi chấp nhận thanh toán, hệ thống được gọi là hệ thống trực tuyến. Năm 1990, Chaum cùng với Moni Naor đề xuất hệ thống tiền điện tử ngoại tuyến đầu tiên, cũng dựa trên chữ ký mù. (Satoshi, 2019)

2.3. Kỹ thuật Blind Signature trên DigiCash và eCash

Blind Signature (chữ ký mù) đã giới thiệu bởi David Chaum, là một dạng của chữ ký điện tử trong đó nội dung của một thông điệp được ngụy trang trước khi nó được ký kết. Chữ ký mù kết quả có thể được xác minh công khai dựa trên thông điệp ban đầu, không bị ràng buộc theo cách của một chữ ký điện tử thông thường. Chữ ký mù thường được sử dụng trong các giao thức liên quan đến quyền riêng tư trong đó người ký và tác giả thư là các bên khác nhau. (Hoàn Ngọc Thanh, 2018)

Chữ ký mù cũng có thể được sử dụng để cung cấp tính không liên kết, điều này ngăn người ký liên kết thông điệp bị mù mà họ ký với một phiên bản không bị che sau này mà nó có thể được gọi để xác minh. Trong trường hợp này, phản hồi của người ký trước tiên là không bị che trước khi xác minh theo cách mà chữ ký vẫn có giá trị đối với thông điệp không bị che.

Điều này có thể hữu ích trong các chương trình yêu cầu ẩn danh. Các lược đồ chữ ký mù có thể được thực hiện bằng cách sử dụng một số lược đồ ký khóa công khai chung, ví dụ như RSA và DSA. (Floyd and Mansa, 2020) Để thực hiện một chữ ký như vậy, đầu tiên thông điệp được làm mù, thường bằng cách kết hợp nó theo một cách nào đó với một yếu tố làm mờ ngẫu nhiên. Thông điệp bị che khuất được chuyển cho người ký, người này sau đó sẽ ký bằng thuật toán ký chuẩn. Thông báo kết quả, cùng với yếu tố làm mờ, có thể được xác minh sau đó dựa trên khóa công khai của người ký. Trong một số chương trình chữ ký mù, chẳng hạn như RSA, thậm chí có thể loại bỏ yếu tố gây mù khỏi chữ ký trước khi nó được xác minh. Trong các lược đồ này, đầu ra cuối cùng thông điệp hoặc chữ ký của lược đồ chữ ký mù giống với đầu ra của giao thức ký thông thường. (Moldovyan, 2011)

3. Sự phát triển của tiền điện tử từ năm 2000 đến nay

3.1. Tổng quát chung

Năm 2008, một lập trình viên hoặc một nhóm lập trình viên sử dụng tên Satoshi Nakamoto đã xuất bản một bài báo mô tả các loại tiền điện tử và năm sau đã ra mắt Bitcoin - loại tiền điện tử mà sau này được chấp nhận và sử dụng rộng rãi nhất. Tháng 11-2008, cái tên Satoshi Nakamoto lần đầu tiên xuất hiện trên Internet, trong một bài viết với tựa đề "Bitcoin: Hệ thống tiền mặt điện tử vi tính ngang hàng (peer-to-peer)". Bài viết mô tả phương thức sử dụng hệ thống máy vi tính ngang hàng để tạo ra một hệ thống các giao dịch điện tử "không cần phụ thuộc vào sự tin nhiệm". Và đến ngày 3-1-2009, Satoshi Nakamoto đã biến ý tưởng này thành hiện thực khi ông ta (hay bà ta hoặc họ) nhấn nút trên máy vi tính và tạo ra đồng tiền ảo bitcoin. (Hoàng Trung và Nguyễn Văn Cẩm, 2013)

Ngày 18 tháng 8 năm 2008: Tên miền bitcoin.org được đăng ký. Ngày nay tên miền được thay đổi thành là "Who is Guard Protected", nghĩa là danh tính của người đã đăng ký miền này không phải là thông tin công khai. Ngày 31 tháng 10 năm 2008: Một người hoặc một nhóm sử dụng tên Satoshi Nakamoto đưa ra thông báo trên danh sách Gửi thư mật mã tại metzdowd.com. Tiền này đang làm việc trên một hệ thống tiền điện tử mới hoàn toàn ngang hàng, không có bên thứ ba đáng tin cậy. Sách trắng nổi tiếng hiện nay được xuất bản trên bitcoin.org, có tựa đề "Bitcoin: Hệ thống tiền mặt điện tử ngang hàng", sẽ trở thành tương lai về cách Bitcoin hoạt động ngày nay. (Rose, 2015). Ngày 8 tháng 1 năm 2009: Phiên bản đầu tiên của phần mềm Bitcoin được công bố trên danh sách gửi thư bằng mật mã. Ngày 9 tháng 1 năm 2009: Khối 1 được khai thác và quá trình khai thác Bitcoin bắt đầu một cách nghiêm túc. (Mahmoud and Lescisin and Aitaei, 2019)

Ngày 5 tháng 10 năm 2009, lần đầu tiên giá trị của Bitcoin được ấn định trên sàn giao dịch, khởi điểm ở mức 1 đô la Mỹ tương đương 1 309,03 Bitcoin (hoặc 1 Bitcoin = 0,00076 USD). Giá trị này được tính bởi chi phí tiền điện của một máy tính hao tổn khi đào ra Bitcoin và Bitcoin chỉ có số lượng hữu hạn chỉ có 21 triệu coin trên toàn thế giới được tạo ra. (Bonneau and Miller and Clark and Kroll and Filten, 2010)

Những người quan tâm đến sự phát triển của Bitcoin đã mất dần dần liên lạc với người tạo ra BTC là Satoshi từ giữa năm 2010, sau khi ông đưa cho ông Gavin Andresen khóa bảo động khi mạng lưới Bitcoin bị tấn công. Khóa này có thể dùng để bảo động tới toàn mạng lưới ngừng lưu lại giao dịch. Khóa bảo động này sau đó được hủy bỏ để tăng tính phân tán của hệ thống Bitcoin. Cho tới nay, danh tính chính xác của Satoshi Nakamoto vẫn còn là ẩn số chưa thể xác định chính xác được. (Rodriguez, 2014)

Bitcoin là một tập hợp các máy tính hoặc các nút, tất cả đều chạy mã của Bitcoin và lưu trữ chuỗi khối của nó. Một blockchain có thể được coi là một tập hợp các khối. Trong mỗi khối là một tập hợp các giao dịch. Bởi vì tất cả các máy tính chạy chuỗi khối này có cùng danh sách các khối và giao dịch và có thể thấy rõ ràng các khối mới này được lấp đầy bằng các giao dịch Bitcoin mới, nên không ai có thể gian lận hệ thống. Bất kỳ ai, cho dù họ có chạy "nút" Bitcoin hay không, đều có thể thấy các giao dịch này diễn ra trực tiếp. Để thực hiện được hành vi bất chính, một kẻ xấu sẽ cần vận hành 51% sức mạnh tính toán tạo nên Bitcoin. Bitcoin có khoảng 47.000 nút tính đến tháng 5 năm 2020 và con số này đang tăng lên, khiến một cuộc tấn công như vậy rất khó xảy ra. (Trần Việt, 2010)

Bitcoin là một loại cryptocurrency. Số dư của mã thông báo Bitcoin được lưu giữ bằng cách sử dụng "khóa" công khai và riêng tư, là những chuỗi dài gồm số và chữ cái được liên kết thông qua mã hóa toán học, thuật toán đã được sử dụng để tạo chúng. Khóa công khai có thể so sánh với số tài khoản ngân hàng đóng vai trò là địa chỉ được công bố với thế giới và những người khác có thể gửi bitcoin. Khóa riêng tư có thể so sánh với mã PIN ATM được coi là bí mật được bảo vệ và chỉ được sử dụng để cho phép truyền Bitcoin. Không nên nhầm lẫn các khóa Bitcoin với ví Bitcoin, đây là một thiết bị vật lý hoặc kỹ thuật số tạo điều kiện thuận lợi cho việc giao dịch Bitcoin và cho phép người dùng theo dõi quyền sở hữu của tiền xu. Thuật ngữ "ví" hơi gây hiểu nhầm, vì bản chất phi tập trung của Bitcoin có nghĩa là nó không bao giờ được lưu trữ "trong" ví, mà là một cách phi tập trung trên một blockchain. Ghi chú phong cách theo Tổ chức Bitcoin chính thức, từ "Bitcoin" được viết hoa trong ngữ cảnh đề cập đến thực thể hoặc khái niệm, trong khi bitcoin được viết bằng chữ thường khi đề cập đến một số lượng tiền tệ hoặc chính các đơn vị. Dạng số nhiều có thể là "bitcoins". Bitcoin cũng thường được viết tắt là "BTC". (Academy, 2020)

Trọng tâm của sự hấp dẫn và chức năng của Bitcoin và các loại tiền điện tử khác là công nghệ blockchain, được sử dụng để lưu giữ một sổ cái trực tuyến của tất cả các giao dịch đã từng được thực hiện, do đó cung cấp một cấu trúc dữ liệu cho sổ cái này khá an toàn và được chia sẻ và đồng ý dựa trên toàn bộ mạng của từng nút hoặc máy tính duy trì một bản sao của sổ cái. (Võ Khánh Nam, 2020) Mỗi khối mới được tạo phải được xác minh bởi từng nút trước khi được xác nhận, khiến cho việc giả mạo lịch sử giao dịch gần như không thể. Nhiều chuyên gia nhận thấy công nghệ blockchain có tiềm năng sử dụng nghiêm túc như bỏ phiếu trực tuyến và huy động vốn từ cộng đồng, và các tổ chức tài chính lớn như JPMorgan Chase (JPM) nhận thấy tiềm năng giảm chi phí giao dịch bằng cách hợp lý hóa quá trình thanh toán. Tuy nhiên, vì tiền

điện tử là ảo và không được lưu trữ trên cơ sở dữ liệu trung tâm, số dư tiền điện tử kỹ thuật số có thể bị xóa do mất hoặc phá hủy ổ cứng nếu bản sao dự phòng của khóa cá nhân không tồn tại. Đồng thời, không có cơ quan trung ương, chính phủ hoặc công ty nào có quyền truy cập vào quỹ của bạn hoặc thông tin cá nhân của bạn. (Hajdarbegovic, 2014)

Vì giá thị trường cho tiền điện tử dựa trên cung và cầu, tỷ lệ mà một loại tiền điện tử có thể được trao đổi sang một loại tiền tệ khác có thể dao động rộng rãi, vì thiết kế của nhiều loại tiền điện tử đảm bảo mức độ khan hiếm cao. Bitcoin đã trải qua một số đợt tăng giá và sụt giảm nhanh chóng về giá trị, leo lên mức 19 000 đô la cho mỗi Bitcoin vào tháng 12 năm 2017 trước khi giảm xuống khoảng 7 000 đô la trong những tháng tiếp theo. (Phạm Văn Vũ, 2018) Do đó, tiền điện tử được một số nhà kinh tế coi là một một ngắn hạn hoặc bong bóng đầu cơ. Có lo ngại rằng tiền điện tử như Bitcoin không bắt nguồn từ bất kỳ hàng hóa vật chất nào. Tuy nhiên, một số nghiên cứu đã xác định rằng chi phí sản xuất Bitcoin, đòi hỏi một lượng năng lượng ngày càng lớn, có liên quan trực tiếp đến giá thị trường của nó. Các blockchains tiền điện tử có độ bảo mật cao, nhưng các khía cạnh khác của hệ sinh thái tiền điện tử, bao gồm các sàn giao dịch và ví, không tránh khỏi các mối đe dọa bị hack. (Lee, 2020) Trong lịch sử 10 năm của Bitcoin, một số sàn giao dịch trực tuyến đã là đối tượng của các vụ hack và trộm cắp, đôi khi số "coin" trị giá hàng triệu đô la bị đánh cắp. Tuy nhiên, nhiều nhà quan sát nhận thấy những lợi thế tiềm năng trong tiền điện tử, như khả năng bảo toàn giá trị chống lại lạm phát và tạo điều kiện trao đổi trong khi dễ vận chuyển và phân chia hơn kim loại quý và tồn tại bên ngoài ảnh hưởng của các ngân hàng trung ương và chính phủ. (Trần Tun, 2009)

3.2. Cách thức hoạt động của Bitcoin

Bitcoin là một trong những loại tiền kỹ thuật số đầu tiên sử dụng công nghệ peer-to-peer để tạo điều kiện thanh toán tức thì. Các cá nhân và công ty độc lập sở hữu sức mạnh tính toán chi phối và tham gia vào mạng Bitcoin, bao gồm các nút hoặc thợ đào. "Thợ mỏ" hoặc những người xử lý các giao dịch trên blockchain, được thúc đẩy bởi phần thưởng việc phát hành bitcoin mới và phí giao dịch được trả bằng bitcoin. Những người khai thác này có thể được coi là cơ quan phân quyền thực thi uy tín của mạng Bitcoin. (Ramza, 2012) Bitcoin mới đang được phát hành cho các thợ đào với tốc độ cố định, nhưng giảm theo định kỳ, như vậy tổng nguồn cung bitcoin đạt 21 triệu. Tính đến tháng 7 năm 2020, có khoảng 3 triệu bitcoin vẫn chưa được khai thác. Theo cách này, Bitcoin và bất kỳ loại tiền điện tử nào được tạo ra thông qua một quy trình tương tự hoạt động khác với tiền tệ fiat; trong các hệ thống ngân hàng tập trung, tiền tệ được phát hành với tỷ lệ phù hợp với sự tăng trưởng của hàng hóa nhằm cố gắng duy trì sự ổn định giá cả, trong khi một hệ thống phi tập trung như Bitcoin đặt tỷ lệ phát hành trước thời hạn và theo một thuật toán. (Xuyên Mai, 2020)

Khai thác bitcoin là quá trình bitcoin được phát hành vào lưu thông. Nói chung, khai thác đòi hỏi phải giải các câu đố khó về mặt tính toán để khám phá ra một khối mới, khối này được thêm vào blockchain. Trong việc đóng góp vào chuỗi khối, việc khai thác sẽ bổ sung và xác

minh các bản ghi giao dịch trên toàn mạng. Để thêm các khối vào blockchain, các thợ đào sẽ nhận được phần thưởng dưới dạng một vài bitcoin; phần thưởng giảm một nửa sau mỗi 210.000 khối. Phần thưởng khối là 50 bitcoin mới vào năm 2009 và hiện là 12,5. Vào ngày 11 tháng 5 năm 2020, đợt giảm một nửa thứ ba đã xảy ra, đưa phần thưởng cho mỗi lần phát hiện khối xuống còn 6,25 bitcoin. (Trần Minh, 2020)

Nhiều loại phần cứng có thể được sử dụng để khai thác bitcoin nhưng một số mang lại phần thưởng cao hơn những phần cứng khác. Một số chip máy tính nhất định được gọi là mạch tích hợp dành riêng cho ứng dụng (ASIC) và các bộ xử lý nâng cao hơn như Bộ xử lý đồ họa (GPU) có thể đạt được nhiều phần thưởng hơn. Những bộ xử lý khai thác phức tạp này được gọi là giàn khai thác. Một bitcoin có thể chia hết cho tám chữ số thập phân 100 phần triệu của một bitcoin và đơn vị nhỏ nhất này được gọi là Satoshi. Nếu cần thiết và nếu các thợ đào tham gia chấp nhận thay đổi, Bitcoin cuối cùng có thể được chia thành nhiều chữ số thập phân hơn. (Nguyễn Công Đạt, 2021)

3.3. Ưu điểm

Phí giao dịch thấp: Với đồng tiền điện tử được sử dụng phổ biến hiện nay là đồng Bitcoin, thì giao dịch của nó hiện nay là không có phí hoặc là mức phí giao dịch rất nhỏ. Để khắc phục tình trạng này cần hỗ trợ quá trình giải quyết nhanh chóng các giao dịch, chuyển đổi Bitcoin và gửi tiền trực tiếp vào tài khoản ngân hàng. (Trần Thị Kim Chi và Trần Thúy Kim Thành, 2020)

Giá trị cao vì sự khan hiếm đa phần các đồng tiền ảo, ví dụ như Bitcoin đều chỉ có số lượng nhất định, với tổng nguồn cung được quy định. Vì thế mà BTC hiện nay là 1 loại tiền có giá trị rất cao và phá vỡ sự độc quyền ngoại tệ của chính phủ tiền kỹ thuật số là 1 phương tiện thanh toán giao dịch thuận tiện, và không thuộc sự chi phối của ngân hàng hay chính phủ. Vì thế chúng ta sẽ giảm bớt sự phụ thuộc của những chính sách tiền tệ quốc gia. (Đào Tín, 2020)

Quyền tự chủ của người dùng: Điểm thu hút chính của bitcoin đối với nhiều người dùng và thực sự là một trong những nguyên lý trung tâm của tiền điện tử nói chung là quyền tự chủ. Tiền tệ kỹ thuật số cho phép người dùng tự chủ nhiều hơn đối với tiền của họ hơn so với tiền tệ fiat, ít nhất là trên lý thuyết. Người dùng có thể kiểm soát cách họ tiêu tiền mà không cần giao dịch với cơ quan trung gian như ngân hàng hoặc chính phủ. (Brock, 2017)

Ít rủi ro hơn cho người sử dụng: Các giao dịch tiền điện tử được xác minh là an toàn, không thể đảo ngược và đặc biệt là nó không chứa thông tin nhạy cảm của khách hàng. Do chắc chắn sẽ nhận được tiền, nên các doanh nghiệp không cần phải lo ngại về tình trạng gian lận, không cần phải biết quá nhiều thông tin về khách hàng và đặc biệt là không cần phải dựa vào bên thứ 3 để thực hiện giao dịch mua bán như thẻ tín dụng. (Fatas and Mauro, 2019)

Loại bỏ phí ngân hàng: Mặc dù nó được coi là tiêu chuẩn trong số các sàn giao dịch tiền điện tử để tính phí cái gọi là nhà sản xuất và người nhận, cũng như phí gửi và rút tiền không thường xuyên, người dùng bitcoin không phải chịu các khoản phí ngân hàng truyền thống liên

quan đến tiền tệ fiat. Điều này có nghĩa là không có phí duy trì tài khoản hoặc số dư tối thiểu, không có phí thấu chi và không có phí gửi trả lại, trong số nhiều khoản phí khác. (Divi, 2020)

Thuận tiện trong giao dịch, tự do thanh toán: Với đồng tiền điện tử thì mọi người có thể gửi và nhận tiền ngay lập tức và có thể gửi tùy ý với số lượng không giới hạn.

Thanh toán di động: Giống như với nhiều hệ thống thanh toán trực tuyến, người dùng bitcoin có thể thanh toán tiền của họ ở bất kỳ đâu họ có thể truy cập Internet. Điều này có nghĩa là người mua không bao giờ phải đi đến ngân hàng hoặc cửa hàng để mua một sản phẩm. Tuy nhiên, không giống như thanh toán trực tuyến được thực hiện bằng tài khoản ngân hàng hoặc thẻ tín dụng của Hoa Kỳ, thông tin cá nhân là không cần thiết để hoàn thành bất kỳ giao dịch nào. (Bailis and Song, 2010)

Khả năng tiếp cận: Vì người dùng có thể gửi và nhận bitcoin chỉ bằng điện thoại thông minh hoặc máy tính, nên về mặt lý thuyết, bitcoin có sẵn cho những người dùng không có quyền truy cập vào các hệ thống ngân hàng truyền thống, thẻ tín dụng và các phương thức thanh toán khác. (Li and Wang, 2008)

Tính minh bạch cao: Bởi sử dụng công nghệ Blockchain, nên mọi thông tin liên quan đến nguồn cung tiền điện tử đều có sẵn trên chuỗi khối cho bất cứ ai muốn xác minh và sử dụng đều có thể theo dõi. Tiền điện tử đã được mã hóa nên không có cá nhân hay tổ chức nào có thể kiểm soát hay thay đổi các giao dịch. Điều này đã làm tăng độ tin cậy, tính minh bạch cho tiền điện tử.

3.4. Nhược điểm

Mức độ chấp nhận còn thấp: Tiền điện tử ra đời sớm nhất và phổ biến nhất hiện nay là đồng Bitcoin mới chỉ có lịch sử 10 năm hình thành và phát triển, trong khi nhiều người vẫn quen với việc sử dụng đồng tiền của quốc gia, vì thế với một loại tiền tệ mới thì mức độ chấp nhận của người dùng chưa phổ biến. (Trần Thị Kim Chi và Trần Thúy Kim Thành, 2020)

Có thể bị tác động bởi hệ thống an ninh mạng: Tiền điện tử được thiết lập cũng như lưu hành chủ yếu thông qua các thiết bị điện tử, do vậy người nắm giữ tiền điện tử có thể bị mất tiền nếu ổ cứng bị lỗi, dữ liệu bị virus, các tập tin bị mất... không có cách nào khôi phục được, Rủi ro bảo mật của Bitcoin hầu hết các cá nhân sở hữu và sử dụng Bitcoin đều không có được token của họ thông qua các hoạt động khai thác. Thay vào đó, họ mua và bán Bitcoin và các loại tiền kỹ thuật số khác trên bất kỳ thị trường trực tuyến phổ biến nào được gọi là sàn giao dịch Bitcoin. Các sàn giao dịch bitcoin hoàn toàn là kỹ thuật số và cũng như với bất kỳ hệ thống ảo nào, có nguy cơ bị tin tặc, phần mềm độc hại và trục trặc hoạt động. Nếu kẻ trộm có quyền truy cập vào ổ cứng máy tính của chủ sở hữu Bitcoin và đánh cắp khóa mã hóa riêng tư của họ, hẳn có thể chuyển Bitcoin bị đánh cắp sang một tài khoản khác. Người dùng chỉ có thể ngăn chặn điều này nếu bitcoin được lưu trữ trên máy tính không được kết nối với Internet hoặc bằng cách chọn sử dụng ví giấy - in ra các khóa và địa chỉ riêng tư của Bitcoin và hoàn toàn không lưu giữ chúng

trên máy tính. Tin tặc cũng có thể nhắm mục tiêu vào các sàn giao dịch Bitcoin, giành quyền truy cập vào hàng nghìn tài khoản và ví kỹ thuật số nơi lưu trữ bitcoin. (Boukhalfa, 2019)

Rủi ro bảo hiểm một số khoản đầu tư được bảo hiểm thông qua Công ty Cổ phần Bảo vệ Nhà đầu tư Chứng khoán. Các tài khoản ngân hàng thông thường được bảo hiểm thông qua Tổng công ty Bảo hiểm Tiền gửi Liên bang (FDIC) với số tiền nhất định tùy thuộc vào khu vực tài phán. Nói chung, các sàn giao dịch Bitcoin và tài khoản Bitcoin không được bảo hiểm bởi bất kỳ loại chương trình liên bang hoặc chính phủ nào.

Có thể trở thành công cụ của hacker, tội phạm rửa tiền: Chính bởi hình thức giao dịch không được kiểm soát, cho nên tiền điện tử đã được nhiều nhóm đối tượng tội phạm nhắm đến và sử dụng như một phương thức giao dịch để rửa tiền. (Tech, 2019)

Rủi ro gian lận Bitcoin trong khi Bitcoin sử dụng mã hóa khóa cá nhân để xác minh chủ sở hữu và đăng ký giao dịch, những kẻ lừa đảo và kẻ lừa đảo có thể cố gắng bán bitcoin giả.

Rủi ro về thuế của Bitcoin vì bitcoin không đủ điều kiện để được đưa vào bất kỳ tài khoản hưu trí có lợi về thuế nào, nên không có lựa chọn hợp pháp, tốt nào để bảo vệ các khoản đầu tư khỏi bị đánh thuế. (Đoàn Bảo, 2020)

3.5. Sử dụng công nghệ Blockchain trong tiền điện tử

Với mục đích hiểu rõ về blockchain, bạn nên xem nó trong bối cảnh cách nó được Bitcoin thực hiện. Giống như một cơ sở dữ liệu, Bitcoin cần một tập hợp các máy tính để lưu trữ chuỗi khối của nó. Đối với Bitcoin, blockchain này chỉ là một loại cơ sở dữ liệu cụ thể lưu trữ mọi giao dịch Bitcoin từng được thực hiện. Trong trường hợp của Bitcoin, và không giống như hầu hết các cơ sở dữ liệu, các máy tính này không phải là tất cả dưới một mái nhà và mỗi máy tính hoặc nhóm máy tính được vận hành bởi một cá nhân hoặc một nhóm cá nhân duy nhất. Hãy tưởng tượng rằng một công ty sở hữu một máy chủ bao gồm 10.000 máy tính với cơ sở dữ liệu chứa tất cả thông tin tài khoản của khách hàng. Công ty này có một kho chứa tất cả các máy tính này dưới một mái nhà và có toàn quyền kiểm soát từng máy tính này và tất cả thông tin chứa trong chúng. Tương tự, Bitcoin bao gồm hàng nghìn máy tính, nhưng mỗi máy tính hoặc nhóm máy tính chứa blockchain của nó lại ở một vị trí địa lý khác nhau và chúng đều được vận hành bởi các cá nhân hoặc nhóm người riêng biệt. Những máy tính tạo nên mạng của Bitcoin được gọi là các nút. (Conway, 2020)

Trong mô hình này, blockchain của Bitcoin được sử dụng theo cách phi tập trung. Tuy nhiên, các blockchain riêng tư, tập trung, nơi các máy tính tạo nên mạng của nó được sở hữu và vận hành bởi một thực thể duy nhất, tồn tại. Trong một blockchain, mỗi nút có một bản ghi đầy đủ về dữ liệu đã được lưu trữ trên blockchain kể từ khi thành lập. Đối với Bitcoin, dữ liệu là toàn bộ lịch sử của tất cả các giao dịch Bitcoin. Nếu một nút có lỗi trong dữ liệu của nó, nó có thể sử dụng hàng nghìn nút khác làm điểm tham chiếu để sửa chính nó. Bằng cách này, không một nút nào trong mạng có thể thay đổi thông tin được giữ bên trong nó. Do đó, lịch sử của các giao dịch trong mỗi khối tạo nên chuỗi khối của Bitcoin là không thể thay đổi.

Nếu một người dùng giả mạo hồ sơ giao dịch của Bitcoin, tất cả các nút khác sẽ tham chiếu chéo lẫn nhau và dễ dàng xác định nút có thông tin không chính xác. Hệ thống này giúp thiết lập một thứ tự chính xác và minh bạch của các sự kiện. Đối với Bitcoin, thông tin này là danh sách các giao dịch, nhưng blockchain cũng có thể chứa nhiều thông tin khác nhau như hợp đồng pháp lý, danh tính nhà nước hoặc kho sản phẩm của công ty. Để thay đổi cách hệ thống đó hoạt động hoặc thông tin được lưu trữ bên trong nó, phần lớn sức mạnh tính toán của mạng phi tập trung sẽ cần phải đồng ý về những thay đổi đã nêu. Điều này đảm bảo rằng bất kỳ thay đổi nào xảy ra đều vì lợi ích tốt nhất của đa số. (Killer, 2019)

Mục tiêu của blockchain là cho phép thông tin kỹ thuật số được ghi lại và phân phối, nhưng không được chỉnh sửa. Công nghệ chuỗi khối lần đầu tiên được phác thảo vào năm 1991 bởi Stuart Haber và W. Scott Stornetta, hai nhà nghiên cứu muốn triển khai một hệ thống mà dấu thời gian tài liệu không thể bị giả mạo. Nhưng phải đến gần hai thập kỷ sau, với sự ra mắt của Bitcoin vào tháng 1 năm 2009, blockchain mới có ứng dụng thực tế đầu tiên.

Giao thức Bitcoin được xây dựng trên một blockchain. Trong một bài báo nghiên cứu giới thiệu về tiền tệ kỹ thuật số, người tạo ra biệt danh của Bitcoin, Satoshi Nakamoto, đã gọi nó là “một hệ thống tiền điện tử mới hoàn toàn ngang hàng, không có bên thứ ba đáng tin cậy”. Điều quan trọng cần hiểu ở đây là Bitcoin chỉ sử dụng blockchain như một phương tiện để ghi lại số cái thanh toán một cách minh bạch, nhưng về lý thuyết, blockchain có thể được sử dụng để ghi lại bất kỳ số lượng điểm dữ liệu nào. Như đã thảo luận ở trên, điều này có thể ở dạng giao dịch, phiếu bầu trong một cuộc bầu cử, kiểm kê sản phẩm, danh tính tiểu bang, giấy chứng nhận nhà, v.v. Hiện tại, có rất nhiều dự án dựa trên blockchain đang tìm cách triển khai blockchain theo những cách để giúp đỡ xã hội ngoài việc ghi lại các giao dịch. Một ví dụ điển hình là blockchain được sử dụng như một cách để bỏ phiếu trong các cuộc bầu cử dân chủ. Bản chất của tính bất biến của blockchain có nghĩa là việc bỏ phiếu gian lận sẽ trở nên khó xảy ra hơn nhiều. (Tuấn Anh, 2018)

Bằng cách trải rộng các hoạt động của mình trên một mạng máy tính, blockchain cho phép Bitcoin và các loại tiền điện tử khác hoạt động mà không cần cơ quan trung ương. Điều này không chỉ làm giảm rủi ro mà còn loại bỏ nhiều phí xử lý và giao dịch. Nó cũng có thể cung cấp cho những người ở các quốc gia có tiền tệ hoặc cơ sở hạ tầng tài chính không ổn định một loại tiền tệ ổn định hơn với nhiều ứng dụng hơn và mạng lưới cá nhân và tổ chức rộng lớn hơn mà họ có thể kinh doanh, cả trong nước và quốc tế. Sử dụng ví tiền điện tử cho tài khoản tiết kiệm hoặc làm phương tiện thanh toán đặc biệt sâu sắc đối với những người không có giấy tờ tùy thân. Một số quốc gia có thể bị chiến tranh tàn phá hoặc có chính phủ thiếu bất kỳ cơ sở hạ tầng thực sự nào để cung cấp nhận dạng. Công dân của các quốc gia như vậy có thể không có quyền truy cập vào tài khoản tiết kiệm hoặc tài khoản môi giới và do đó, không có cách nào để cất giữ của cải một cách an toàn. (Trương Phan, 2018)

3.6. Hướng phát triển tiền điện tử tại Việt Nam

Cần đẩy nhanh quá trình nghiên cứu, hoàn thiện khuôn khổ pháp lý quản lý tiền điện tử tại Việt Nam. Với sự phát triển khoa học công nghệ, đặc biệt là công nghệ thông tin, sự lan tỏa nhanh chóng của các đồng tiền điện tử ở Việt Nam đã hiện hữu và diễn biến phức tạp. Do đó, nếu không thực hiện việc kiểm soát hiệu quả đồng tiền này thì không chỉ gây nên những rủi ro đối với các nhà đầu tư, mà còn ảnh hưởng tới hệ thống tài chính, chính sách tiền tệ. Thách thức này đòi hỏi, Ngân hàng Nhà nước Việt Nam cần có những biện pháp hữu hiệu và phối hợp với Bộ Tư pháp, Bộ Tài chính, Bộ Công an để hoàn thiện khung khổ pháp lý quản lý đối với tiền điện tử.

Nên tận dụng thế mạnh của công nghệ đằng sau tiền điện tử KTS, thay vì tập trung nhiều vào việc thắt chặt loại tiền này. Công nghệ Blockchain mang lại nhiều lợi thế cho hệ thống tài chính, đặc biệt là đối với hệ thống thanh toán, do đó, công nghệ Blockchain sẽ là một nền tảng quan trọng đối với định hướng nền kinh tế không tiền mặt của Việt Nam. (Nguyễn Thị Ngọc Lan, 2020)

Cần có các chính sách nâng cao cơ sở hạ tầng công nghệ thông tin; tổ chức đào tạo, nâng cao năng lực đội ngũ chuyên gia tài chính, chuyên gia mã hóa và bảo mật; nâng cao nhận thức của người dân về bản chất của Bitcoin cũng như các loại tiền điện tử khác.

Đẩy mạnh công tác truyền thông để người dân cảnh giác khi được mời chào tham gia các hoạt động liên quan đến tiền điện tử, tiền ảo. Về vấn đề này, Bộ Công an đã từng cảnh báo người dân không nên đầu tư, nắm giữ, thực hiện các giao dịch liên quan đến tiền điện tử, tuy nhiên trong thực tế vẫn còn nhiều người đã bỏ qua những cảnh báo này. Do đó, công tác thông tin tuyên truyền, cảnh báo qua các kênh thông tin chính thức và mạng xã hội cần được đẩy mạnh, để các chủ thể kinh tế nhận rõ các dấu hiệu, hạn chế tối đa các rủi ro trong giao dịch tiền điện tử, đảm bảo sự phát triển an toàn, hiệu quả của hệ thống tài chính Việt Nam. Cần đẩy mạnh hợp tác quốc tế để tăng cường các biện pháp quản lý, giám sát đối với các giao dịch liên quan tới tiền điện tử xuyên biên giới. (Lê Thị Thanh Hà, 2019)

4. Kết luận

Trong bài báo này, đã cung cấp một bản tóm tắt về lý thuyết được sử dụng để xây dựng kiến thức về tiền điện tử nói chung và Bitcoin nói riêng. Chúng tôi đã chỉ ra cách xây dựng sổ cái phân tán hay còn gọi là blockchain này đã cho phép các nhà phát triển phần mềm tạo ra các loại tiền kỹ thuật số hoạt động mà không cần các tổ chức tài chính trung ương. Bài báo này cũng đã chỉ ra rằng phương pháp đồng thuận phân phối này có thể được sử dụng như thế nào để thực thi các quy tắc khác về tài sản kỹ thuật số. Ngoài ra, cũng đã tóm tắt công việc hiện tại và các giải pháp đề xuất giải quyết các vấn đề khác nhau xung quanh công nghệ blockchain...

Bài báo này đã xem xét các tính năng chính của tiền điện tử và các vấn đề chính sách chính phát sinh. Nó lưu ý rằng có rất nhiều vấn đề tiềm ẩn, một số vấn đề trong số đó được các ngân hàng trung ương đặc biệt quan tâm. Đồng thời, sự phát triển của tiền điện tử và các đánh giá chính sách liên quan được thảo luận trong bài báo này có khả năng không chắc chắn đáng kể, có khả năng ảnh hưởng đến bản chất và thời gian của bất kỳ phản ứng quy định nào. Việc thiết kế một khuôn khổ quy định thích hợp cho tiền điện tử liên quan đến việc cân bằng các mục tiêu khác nhau bao gồm sự ổn định và tính toàn vẹn tài chính của các tổ chức phát hành, bảo vệ người tiêu dùng và thúc đẩy cạnh tranh và đổi mới. Bài báo này lập luận rằng tiền điện tử, với tư cách là một mạng tốt, có thể trở thành một dạng tiền tệ quan trọng trong tương lai. Sự phát triển như vậy sẽ ảnh hưởng đến hiệu quả và việc thực thi chính sách tiền tệ. Nếu việc sử dụng tiền điện tử tăng lên làm hạn chế đáng kể nhu cầu dự trữ của ngân hàng trung ương, thì điều đó sẽ đòi hỏi những thay đổi trong mục tiêu hoạt động của ngân hàng trung ương và sự phối hợp chặt chẽ hơn nữa của các chính sách tài khóa và tiền tệ.

Trên những lợi ích mà tiền điện tử mang lại nhưng việc tăng cường sử dụng tiền điện tử sẽ ảnh hưởng đến kinh tế văn hóa như: hạn chế khả năng kiểm soát cung tiền của ngân hàng trung ương, tăng tốc độ vận chuyển của tiền, giảm thu nhập từ dân cư, giảm dự trữ, giảm kiểm soát tiền tệ quốc tế, thay đổi số nhân tiền. Vì thế cần hướng phát triển rõ ràng cho tiền điện tử trong tương lai như:

Giám sát hiệu quả: các tổ chức phát hành tiền điện tử phải chịu sự giám sát hiệu quả và thỏa thuận pháp lý rõ ràng và minh bạch: quyền và nghĩa vụ của những người tham gia tương ứng (khách hàng, người bán, tổ chức phát hành và nhà khai thác) trong một sơ đồ tiền điện tử phải được xác định và tiết lộ rõ ràng. Các quyền và nghĩa vụ đó phải có hiệu lực thi hành theo tất cả các khu vực pháp lý có liên quan.

Bảo mật kỹ thuật: các chương trình tiền điện tử phải duy trì các biện pháp bảo vệ đầy đủ về kỹ thuật, tổ chức và thủ tục để ngăn chặn và phát hiện các mối đe dọa đối với an ninh của chương trình, đặc biệt là mối đe dọa về tiền giả.

Bảo vệ chống lại sự lạm dụng của tội phạm: bảo vệ chống lại sự lạm dụng của tội phạm, chẳng hạn như rửa tiền, phải được tính đến khi thiết kế và triển khai các chương trình tiền điện tử.

Báo cáo thống kê tiền tệ: các chương trình tiền điện tử phải cung cấp cho ngân hàng trung ương ở mỗi quốc gia liên quan bất kỳ thông tin nào có thể được yêu cầu cho các mục đích của chính sách tiền tệ.

Yêu cầu dự trữ: khả năng phải tồn tại đối với các ngân hàng trung ương để áp đặt các yêu cầu dự trữ đối với tất cả các tổ chức phát hành tiền điện tử.

TÀI LIỆU THAM KHẢO

- [1] Najwan. A and Mohamad and Haroon 2009, *Development of Electronic Money and Its Impact on the Central Bank Role and Monetary Policy*, Hardware for Deep Learning. Communications of the ACM, 60(5), p. 48-51.
- [2] Cấn, Văn Lực 2020, *Tiền điện tử khác gì so với tiền ảo, tiền kỹ thuật số?*, truy cập 13/01/2020, <<https://thitruongtaichinhntiente.vn/tien-dien-tu-khac-gi-so-voi-tien-ao-tien-ky-thuat-so-28184.html>>.
- [3] *Tiền điện tử - Đơn vị tiền tệ của tương lai 2020*, truy cập 13/01/2020 <<https://thebank.vn/blog/15459-tien-dien-tu-don-vi-tien-te-cua-tuong-lai.html>>.
- [4] Võ, Chí Khanh 2020, *Tiền điện tử là gì? Những điều cần biết về tiền điện tử*, truy cập 13/01/2020, <<https://www.vaytaichinh.vn/kinh-nghiem/tien-dien-tu-la-gi/>>.
- [5] *Tiền điện tử - Đơn vị tiền tệ của tương lai 2020*, truy cập 13/01/2020, <<https://thebank.vn/blog/15459-tien-dien-tu-don-vi-tien-te-cua-tuong-lai.html>>.
- [6] Phạm, Trung Tập 2018, *Tiền ảo và những khía cạnh của tiền ảo*, truy cập 13/01/2020, <<https://vksndtc.gov.vn/tin-tuc/cong-tac-kiem-sat/tien-ao-va-nhung-khia-canhh-cua-tien-ao-d10-t1037.html>>.
- [7] Cấn, Văn Lực 2020, *Tiền điện tử khác gì so với tiền ảo, tiền kỹ thuật số?*, truy cập 13/01/2020, <<https://thitruongtaichinhntiente.vn/tien-dien-tu-khac-gi-so-voi-tien-ao-tien-ky-thuat-so-28184.html>>.
- [8] J. Frankenfield and J. Mansa 2020, *VirtualCurrency*, truy cập 13/01/2020, <<https://www.investopedia.com/terms/v/virtual-currency.asp>>.
- [9] J. Frankenfield and M. Sonnenshein 2020, *CryptoCurrency*, truy cập 13/01/2020, <<https://www.investopedia.com/terms/c/cryptocurrency.asp>>.
- [10] E. C. Bank 2012 *Virtual Currency Scheme*, Hardware for Deep Learning. Communications of the ACM, 60(5), p. 48-51s.
- [11] D. Chaum 1998, *Blind signature for untraceable payment*, Deep Learning. Communications of the ACM, 70(5), p. 40-55.
- [12] C. Coldy and K. Conner 2002, *Digicash files Chapter 11*, truy cập 13/01/2020, <<https://www.cnet.com/news/digicash-files-chapter-11/>>.
- [13] J. Pitta 1999, *Requiem for a Bright Idea*, truy cập 13/01/2020, <<https://www.forbes.com/forbes/1999/1101/6411390a.html?sh=7344410715f6>>.
- [14] W. Kenton 2020, *DigiCash*, truy cập 13/01/2020, <<https://www.investopedia.com/terms/d/digicash.asp>>.
- [15] C. Rose 2015, *The Evolution Of Digital Currencies: Bitcoin, A Cryptocurrency Causing A Monetary Revolution*, Hardware for Deep Learning. Communications of the ACM, 60(5), p. 48-51.
- [16] J. Kagan and K. Khartit 2020, *Personal Finance eCash*, truy cập 13/01/2020, <<https://www.investopedia.com/terms/e/ecash.asp>>.
- [17] Lê, Huy 2020, *eCash là gì? Sự trỗi dậy và sụp đổ của eCash*, truy cập 13/01/2020, <<https://vietnambiz.vn/ecash-la-gi-su-troi-day-va-sup-do-cua-ecash-20200504104449261.htm>>.

- [18] P. V. Quang 2012, *Nghiên cứu một số kỹ thuật và công nghệ để thực hiện thanh toán bằng tiền điện tử qua mạng máy tính*, Luận văn thạc sĩ, Đại học công nghệ.
- [19] Satoshi 2019, *Lịch sử tiền mã hóa*, truy cập 13/01/2020, <<https://vic.news/lich-su-tien-dien-tu/>>.
- [20] Hoàng, Ngọc Thanh 2018, *Lịch sử Blockchain và Bitcoin*, truy cập 13/01/2020, <<https://www.justpassion.net/tech/database/blockchain/lich-su-blockchain-va-bitcoin.html>>.
- [21] D. Floyd and J. Mansa 2020, *How Bitcoin Works*, truy cập 13/01/2020, <<https://www.investopedia.com/news/how-bitcoin-works/>>.
- [22] N. A. Moldovyan 2011, *Blind Signature Protocols from Digital Signature Standards*, International Journal of Network Security, Vol.13, No.1, PP.22-30, 07/2011.
- [23] C. Rose 2015, *The Evolution Of Digital Currencies: Bitcoin, A Cryptocurrency Causing A Monetary Revolution*, International Business & Economics Research Journal, 07/2015.
- [24] Hoàng, Trung và Nguyễn, Văn Cẩm 2013, *Kỳ 2: cuộc săn lùng “cha đẻ” bitcoin*, truy cập 13/01/2020, <<https://tuoitre.vn/ky-2-cuoc-san-lung-cha-de-bitcoin-587458.htm>>.
- [25] Q. H. Mahmoud and M. Lescisin and M. Aitaei 2019, *Research Challenges and Opportunities in Blockchain and Cryptocurrencies*, Internet Technology Letters, 02/2019.
- [26] J. Bonneau and A. Miller and J. Clark and J. A. Kroll and E. W. Filten 2010, *Research Perspectives and Challenges for Bitcoin and Cryptocurrencies*, International Journal of Network Security, Vol.13, No.1, PP.22-30, 07/2011.
- [27] S. Rodriguez 2014, *Dorian Satoshi Nakamoto chased by reporters, denies founding Bitcoin*, truy cập 13/01/2020, <<https://www.latimes.com/business/technology/la-fi-tn-bitcoin-founder-la-chased-20140306-story.html>>.
- [28] Trần, Việt 2010, *Blockchain là gì? Các ứng dụng liên quan đến Blockchain*, truy cập 13/01/2020, <<https://topdev.vn/blog/blockchain-la-gi/>>.
- [29] D. Academy 2020, *Blockchain là gì và nó hoạt động như thế nào?*, truy cập 13/01/2020, <<https://devera.vn/blog/our-blog-1/post/blockchain-la-gi-va-no-hoat-ong-nhu-the-nao-5>>.
- [30] Võ, Khánh Nam 2020, *Bitcoin là gì? Cách đào và đầu tư BTC như thế nào?*, truy cập 13/01/2020, <<https://vakafx.com/vi/detail/Bitcoin-la-gi-cach-dao-va-dau-tu-btc-nhu-the-nao>>.
- [31] N. Hajdarbegovic 2014, *Bitcoin Foundation to Standardise Bitcoin Symbol and Code Next Year*, truy cập 13/01/2020, <<https://www.coindesk.com/bitcoin-foundation-standardise-bitcoin-symbol-code-next-year>>.
- [32] Phạm, Văn Vũ 2018, *BitCoin Là Gì? Kiểm BitCoin Từ Đâu? Cách Mua Bán BitCoin*, truy cập 13/01/2020, <https://www.payvnn.com/bitcoin-la-gi/#Gia_Tri_Ban_Dau_Cua_BitCoin>.
- [33] T. B. Lee 2020, *When will the people who called Bitcoin a bubble admit they were wrong?*, truy cập, <<https://www.washingtonpost.com/news/theswitch/wp/2013/11/05/when-will-the-people-who-called-bitcoin-a-bubble-admit-they-were-wrong/>>.
- [34] Trần, Tun 2009, *Hệ sinh thái tiền mã hóa gồm những thành phần nào?*, truy cập 14/01/2020, <<https://vic.news/category/tien-ma-hoa-la-gi/bitcoin-la-gi/>>.
- [35] Z. Ramza 2012, *Bitcoin: What is it?*, truy cập 13/01/2020, <<https://www.khanacademy.org/economics-finance-domain/core-finance/money-and-banking/bitcoin/v/bitcoin-what-is-it>>.

- [36] Xuyên, Mai 2020, *Tiền ảo bùng nổ: "Bong bóng" Bitcoin còn dễ vỡ?*, truy cập 14/02/2020, <<https://nld.com.vn/thoi-su-quoc-te/tien-ao-bung-no-bong-bong-bitcoin-con-de-vo-2020122321192581.htm>>.
- [37] Trần. Minh 2020, *Đây là chuyện xảy ra khi những người khai thác bitcoin xâm lấn thị trấn của bạn*, truy cập 14/01/2020, <<https://www.saga.vn/day-la-chuyen-se-xay-ra-khi-nhung-nguoi-khai-thac-bitcoin-xam-chiem-thi-tran-cu~45470>>.
- [38] Nguyễn. Công Đạt 2021, *Đào Bitcoin là gì? Cách đào chúng như thế nào? 2021*, truy cập 14/01/2020, <<https://blogtienao.com/dao-bitcoin-la-gi/>>.
- [39] Trần. Thị Kim Chi và Trần Thúy Kim Thành 2020, *Kinh nghiệm quản lý tiền điện tử kỹ thuật số*, truy cập 14/01/2020, <<http://tapchitaichinh.vn/tai-chinh-quoc-te/kinh-nghiem-quan-ly-tien-dien-tu-ky-thuat-so-318148.html>>.
- [40] Đào. Tín 2020, *Cryptocurrency là gì? Lịch sử hình thành, ưu điểm và nhược điểm*, truy cập 14/01/2020, <<https://tapchicoi24h.com/cryptocurrency-la-gi/>>.
- [41] T. Brock 2017, *7 benefits of using digital currencies*, truy cập 14/01/2020, <<https://www.bizjournals.com/bizjournals/how-to/growth-strategies/2017/06/7-benefits-of-using-digital-currencies.html>>.
- [42] Fatas and B. W. D. Mauro 2019, *The benefits of a global digital currency*, truy cập 14/01/2020, <<https://voxeu.org/article/benefits-global-digital-currency>>.
- [43] G. Divi 2020, *Advantages and Disadvantages of Cryptocurrency in 2020*, truy cập 14/01/2020, <<https://www.geeksforgeeks.org/advantages-and-disadvantages-of-cryptocurrency-in-2020/>>.
- [44] P. Bailis. and H. Song 2010, *Research for Practice: Cryptocurrencies, Blockchains, and Smart Contracts*, Hardware for Deep Learning. Communications of the ACM, 60(5), p. 48-51.
- [45] X. Li and C. A. Wang 2008, *The technology and economic determinant of cryptocurrenc exchange rates: The case of Bitcoin*, Decision support system, 95, p. 49-60.
- [46] Trần. Thị Kim Chi và Trần Thúy Kim Thành 2020, *Kinh nghiệm quản lý tiền điện tử kỹ thuật số*, truy cập 14/01/2020, <<http://tapchitaichinh.vn/tai-chinh-quoc-te/kinh-nghiem-quan-ly-tien-dien-tu-ky-thuat-so-318148.html>>.
- [47] S. Boukhalifa 2019, *What are the disadvantages of cryptocurrencies?*, truy cập 14/01/2020, <<https://www.prescouter.com/2019/11/disadvantages-of-cryptocurrencies/>>.
- [48] V. Tech 2019, *Top 5 Disadvantages Of Cryptocurrency*, truy cập 14/01/2020, <<https://medium.com/the-capital/top-5-disadvantages-of-cryptocurrency-925d6679195d>>.
- [49] Đoàn. Bảo 2020, *Những Ưu Nhược Điểm Của Đồng Bitcoin*, truy cập 14/01/2020, <<https://vnpro.medium.com/nh%E1%BB%AFng-%C6%B0u-nh%C6%B0%E1%BB%A3c-%C4%91i%E1%BB%83m-c%E1%BB%A7a-%C4%91%E1%BB%93ng-bitcoin-a6d076accb92>>.
- [50] L. Conway 2020, *Blockchain Explained*, truy cập 14/01/2020, <<https://www.investopedia.com/terms/b/blockchain.asp#bitcoin-vs-blockchain>>.
- [51] F. Kiler 2019, *How Digital Currency Works*. Truy cập 14/01/2020, <<https://www.bitira.com/how-digital-currency-works/>>.

- [52] Tuấn Anh 2018, *Blockchain là gì? Ưu, nhược điểm của blockchain?*, truy cập 14/01/2020, <<https://dungdiem.vn/tin-tuc-tong-hop/blockchain-la-gi-uu-nhuoc-diem-cua-blockchain/>>.
- [53] Trương. Phan 2018, *Công nghệ blockchain là gì? Tìm hiểu về bản chất và ứng dụng Blockchain*, truy cập 14/01/2020, <<https://www.mitrade.com/vn/forex/cryptocurrency/cryptocurrency-la-gi/cong-nghe-blockchain>>.
- [54] Nguyễn. Thị Ngọc Lan 2020, *Xu hướng phát triển tiền kỹ thuật số và đề xuất chính sách ở Việt Nam*, truy cập 14/01/2020, <<http://tapchitaichinh.vn/ngan-hang/xu-huong-phat-trien-tien-ky-thuat-so-va-de-xuat-chinh-sach-o-viet-nam-330752.html>>.
- [55] Lê. Thị Thanh Hà 2019, *6 xu hướng tiền điện tử không thể bỏ qua năm 2020*, truy cập 14/01/2020, <<https://www.fiahub.com/blog/6-xu-huong-tien-dien-tu-khong-the-bo-qua-nam-2020/>>.