**ĐẠI HỌC QUỐC GIA TP. HỒ CHÍ MINH**

**TRƯỜNG ĐẠI HỌC CÔNG NGHỆ THÔNG TIN**

**LỚP IT009.K17**



**ĐỒ ÁN GIỚI THIỆU NGÀNH**

**ĐỀ TÀI: CÔNG NGHỆ BLOCKCHAIN VÀ ỨNG DỤNG**

**NHÓM THỰC HIỆN: B7**

**GIẢNG VIÊN HƯỚNG DẪN**

**CÔ: NGUYỄN THỊ ANH THƯ**

**TP. HỒ CHÍ MINH, 2019**

**MỤC LỤC**

[Chương 1. TÌM HIỂU CHUNG 3](#_Toc22498012)

[1. Khái niệm 3](#_Toc22498013)

[2. Cách hoạt động 3](#_Toc22498014)

[3. Đặc trưng 3](#_Toc22498015)

[Chương 2. LỊCH SỬ HÌNH THÀNH 5](#_Toc22498016)

[1. Những bước đầu hình thành 5](#_Toc22498017)

[2. Blockchain 1.0: Giao dịch điện tử – Sự xuất hiện của Bitcoin 5](#_Toc22498018)

[3. Blockchain 2.0: Hợp đồng thông minh – Ethereum 6](#_Toc22498019)

[4. Blockchain 3.0: Các ứng dụng khác – Tương lai của Blockchain 6](#_Toc22498020)

[4.1 Vai trò của Blockchain trong lĩnh vực kinh tế 7](#_Toc22498021)

[4.2 Vai trò của Blockchain trong lĩnh vực xã hội 7](#_Toc22498022)

[Chương 3. BITCOIN 9](#_Toc22498023)

[1. Khái niệm 9](#_Toc22498024)

[2. Cách hoạt động 9](#_Toc22498025)

[3. Đào Bitcoin 9](#_Toc22498026)

[4. Ưu điểm 10](#_Toc22498027)

[5. Nhược điểm 10](#_Toc22498028)

[KẾT LUẬN 11](#_Toc22498029)

[BẢNG PHÂN CÔNG CÔNG VIỆC 12](#_Toc22498030)

[TÀI LIỆU THAM KHẢO 13](#_Toc22498031)

# TÌM HIỂU CHUNG

## Khái niệm

* ***Chuỗi khối (Blockchain):*** là một cơ sở dữ liệu phân tán lưu trữ thông tin trong các khối thông tin được liên kết với nhau bằng mã hóa và mở rộng theo thời gian. Mỗi khối (block) là một đơn vị chứa dữ liệu, dữ liệu sau khi được đóng gói trong một khối sẽ được mã hóa và không thể thay đổi. Các khối sau khi được tạo ra sẽ được liên kết lại với nhau thành một chuỗi (chain). Trong mỗi khối, tồn tại mã băm định danh chính khối đó và mã băm định danh khối trước nó, từ đó hình thành liên kết.

## Cách hoạt động

* Người dùng tạo một giao dịch (transaction) và gắn kết nó với một khóa bảo mật (private key). Một ‘transaction’ bao gồm một chuỗi dữ liệu, thông thường là nó là một cấu trúc dữ liệu thể hiện các giao dịch (tài chính, vật chất, …) giữa các người dùng trong mạng lưới.
* Một ‘transaction’ sẽ được truyền tới những người dùng khác thông qua giao thức Gossip (Gossip protocol) tới các thành viên khác để xác thực độ đáng tin cậy của giao dịch.
* Sau bước xác thực, nó được chuyển vào một khối (dữ liệu) và gắn kết vào mạng lưới blockchain cùng với những block khác bằng hàm hash. Mỗi khi một block mới được tạo, nó sẽ gắn hàm hash với các block trước đó. Nếu dữ liệu trong một block bị xâm phạm thì hàm hash của nó sẽ thay đổi, tức là nó sẽ không khớp với các khối khác nữa. Những ‘transaction’ sẽ được tái xác nhận mỗi khi có một block mới được gắn vào.

## Đặc trưng

* ***Sổ cái phân tán (Distributed Ledger):***
* *Sổ cái*: là cơ sở dữ liệu lưu lại các hoạt động diễn ra trên mạng lưới.
* *Sổ cái phân tán*: là mô hình phân tán “sổ cái” đến tất cả các cá thể trong hệ thống, mỗi cá thể lưu trữ một bản sao của sổ cái.
* ***Cơ chế đồng thuận phi tập trung (Decentralized Consensus):*** là một tập hợp các nguyên tắc và kỹ thuật cho phép các cá thể trên hệ thống phân tán đạt được thỏa thuận về tài liệu hoặc cơ sở dữ liệu dùng chung. Cơ chế đồng thuận phi tập trung sẽ giúp hệ thống ra quyết định dựa trên sự đồng thuận của nhóm đa số.
* ***Tính bất biến (Immutability):*** Nhờ vào lý thuyết mật mã và hàm băm, một khi block được thêm vào chuỗi thì dữ liệu trong block sẽ rất khó có thể bị thay đổi. Có 2 mối đe dọa cho tính bất biến trong Blockchain: cuộc tấn công 51% và máy tính lượng tử. Thực tế chỉ ra rằng việc chiếm tới hơn 50% các node trong mạng lưới là một điều rất khó để thực hiện. Đối với vấn đề điện toán lượng tử, các chuyên gia đang đề xuất việc ứng dụng công nghệ mật mã lượng tử vào Blockchain. Trong tương lai, kiến trúc Blockchain tạo nên từ các thành phần lượng tử sẽ trở nên an toàn hơn cho việc lưu trữ dữ liệu.

# LỊCH SỬ HÌNH THÀNH

## Những bước đầu hình thành

* Năm 1991, các nhà nghiên cứu Stuart Haber và W. Scott Stornetta giới thiệu một giải pháp thực tế về mặt tính toán để đánh dấu thời gian (time stamp) các văn bản số để chúng không bị đề lùi ngày về trước hoặc can thiệp vào.
* Hệ thống sử dụng một chuỗi gồm các khối được bảo mật bằng mật mã để lưu trữ các văn bản được đánh dấu thời gian.
* Năm 1992, các cây Merkle đã được tích hợp vào thiết giúp tăng cường tính hiệu quả bằng cách cho phép một khối có thể tập hợp một vài văn bản.
* Năm 1997, Adam Back đề xuất một hệ thống hạn chế thư quảng cáo cùng với phương thức tấn công từ chối dịch vụ bằng cách sử dụng một thuật toán “Bằng chứng xử lý”, được biết đến với tên là Hashcash.
* Năm 2004, nhà khoa học máy tính và người theo chủ nghĩa mật mã Hal Finney đưa ra một hệ thống gọi là RPoW, Proof Of Work Tái sử dụng. Hệ thống hoạt động bằng cách nhận một Hashcash không thể thay đổi hoặc không thể thay thế dựa trên token proof of work, và đổi lại đã tạo ra một token đã được ký RSA mà sau đó có thể được trao đổi trực tiếp từ người này sang người khác.

## Blockchain 1.0: Giao dịch điện tử – Sự xuất hiện của Bitcoin

* Năm 2008, cuốn sách trắng (whitepaper) giới thiệu về hệ thống tiền mặt điện tử mạng ngang hàng, phi tập trung – tên là Bitcoin – đã được đăng trên danh sách nhận thư về mật mã học bởi một người hoặc tổ chức lấy biệt danh là Satoshi Nakamoto.
* Dựa trên thuật toán Proof of work Hashcash, nhưng thay vì sử dụng một hàm tính toán dựa trên phần cứng như RPoW, tính năng chống chi tiêu hai lần trong Bitcoin được cung cấp bởi một giao thức mạng ngang hàng để theo dõi và xác thực các giao dịch. Nói ngắn gọn, các thợ đào “đào” Bitcoin để nhận phần thưởng bằng cách sử dụng cơ chế proof-of-work và sau đó xác minh bằng các node phi tập trung trong mạng.
* Mặc cho một số thành quả nổi bật trong thời gian đầu phát triển, Bitcoin vẫn chưa phải là hệ thống tận dụng tối đa những lợi ích mà nền tảng Blockchain mang lại. Điều này dẫn tới một giai đoạn mới của công nghệ Blockchain.

## Blockchain 2.0: Hợp đồng thông minh – Ethereum

* Năm 2013, Vitalik Buterin, nhà lập trình và nhà đồng sáng lập của Bitcoin Magazine bắt đầu phát triển một nền tảng tính toán phân tán dựa trên blockchain mới, Ethereum, với một chức năng mật mã mới được gọi là hợp đồng thông minh (smart contract).
* Là những bản hợp đồng số được viết bằng code trên nền tảng blockchain, có thể vận hành tự động và cho phép các bên tham gia trao đổi tài sản ảo, dịch vụ, cổ phiếu, ... một cách minh bạch mà không cần đến người hay dịch vụ trung gian làm chứng.
* Smart contract vượt trội hơn Bitcoin ở chỗ nó không chỉ là một hình thức giao dịch tiền tệ thuần túy nữa mà còn hỗ trợ trao đổi những hợp đồng, tài sản, dịch vụ (thanh toán, vay nợ, bảo hiểm, pháp lý, …).
* Hợp đồng thông minh là các chương trình hoặc tệp lệnh được triển khai và thực thi trên blockchain Ethereum, chúng có thể được sử dụng, ví dụ, để thực hiện một giao dịch khi các điều kiện được thỏa mãn.
* Hợp đồng thông minh có thể được sử dụng trong tất cả các dịch vụ như bảo hiểm, thanh toán, vay nợ, pháp lý,…
* Tiền điện tử của Ethereum được gọi là Ether; nó có thể được chuyển giữa các tài khoản và được sử dụng để trả phí cho công suất tính toán được sử dụng khi thực thi các hợp đồng thông minh.

## Blockchain 3.0: Các ứng dụng khác – Tương lai của Blockchain

* Sự phát triển của Blockchain không dừng lại tại đây. Những năm gần đây, vô số những dự án đã được triển khai và đã gặt hái được nhiều thành quả từ khả năng tiềm tàng mà Blockchain đem lại. Ngoài ra, một số dự án mới đã được thực hiện để có thể bổ khuyết cho những thiếu sót của Bitcoin và Ethereum nhằm có thể thích ứng được với những thành quả mới mà Blockchain đem lại.
* Nhờ trên nền tảng blockchain Ethereum, các DApp (ứng dụng phi tập trung) đã được viết ra và đã có hàng trăm DApp bao gồm các nền tảng mạng truyền thông xã hội, các ứng dụng chơi bạc, và các sàn giao dịch tài chính.
* Blockchain tham gia vào gần như tất cả các lĩnh vực của xã hội như quân sự, kinh tế, xã hội,…, giúp con người thực hiện được những nhu cầu của bản thân tốt hơn trong thời kì công nghệ 4.0 này.

### Vai trò của Blockchain trong lĩnh vực kinh tế

* Các công ty công nghệ lớn như Facebook, Twitter, Airbnb và Uber dùng blockchain trong hệ thống để bảo vệ dữ liệu của người dùng khỏi bị rò rỉ hoặc tấn công. Nếu như dữ liệu người dùng bị rò rỉ hay tấn công, các công ty sẽ mất đi một nguồn lợi to lớn, đồng thời thông tin cá nhân của khách hàng sẽ bị đe dọa. Mặt khác, Blockchain còn giúp doanh nghiệp giảm thiểu các chi phí. Theo một báo cáo của Accenture, việc ứng dụng Blockchain có thể cắt giảm 30% chi phí doanh nghiệp chi ra cho các middle (bộ phận Quản lý rủi ro) và back office (bộ phận Hỗ trợ), dựa trên thống kê từ dữ liệu của 8 đến 10 ngân hàng lớn nhất thế giới.

### Vai trò của Blockchain trong lĩnh vực xã hội

* Blockchain khắc phục tình trạng lạm phát hiện nay bằng cách cho phép một mạng trao đổi giá trị toàn cầu không bị ràng buộc với bất kỳ chính phủ hoặc lượng tài nguyên nào mà một quốc gia có.
* Do tính chất ngang hàng của Blockchain, các tổ chức phi lợi nhuận có thể được hưởng lợi từ việc gây quỹ trực tiếp và theo dõi chi tiêu minh bạch hơn, đảm bảo các nhà tài trợ rằng tiền của họ đi vào mục đích của nó.
* Ngoài ra Blockchain còn có thể áp dụng vào rất nhiều lĩnh vực khác như: y tế, giáo dục, bầu cử, thương mại điện tử, …

#### MedicalChain

* Công ty trong lĩnh vực chăm sóc sức khỏe đầu tiên sử dụng công nghệ blockchain để tạo thuận lợi trong việc lưu trữ và sử dụng hồ sơ y tế điện tử để cung cấp trải nghiệm y học từ xa (telemedicine) hoàn chỉnh. Họ là các bác sĩ thực tế trong hệ thống chăm sóc sức khỏe của Anh và muốn thay đổi hệ thống này từ bên trong.

#### OriginTrail

* OriginTrail là một nền tảng blockchain cho phép người tiêu dùng biết hàng hóa thực phẩm mà họ mua đến từ đâu và cách chúng được sản xuất. OriginTrail mang lại sự chia sẻ dữ liệu đáng tin cậy cho chuỗi cung ứng toàn cầu bằng cách sử dụng công nghệ blockchain.

# BITCOIN

## Khái niệm

* Bitcoin là một loại tiền tệ kỹ thuật số được mã hóa xuất hiện vào năm 2008. Nó có thể được trao đổi, giao dịch trực tiếp bằng các thiết bị có kết nối Internet mà không cần thông qua một tổ chức tài chính trung gian nào, không có ai quản lý, các giao dịch hoàn toàn được thực hiện ngay lập tức và ẩn danh.
* Hiện tại càng có nhiều người hướng đến Bitcoin vì nó không bị điều khiển bởi chính phủ hay ngân hàng nào. Mặt khác, sự chi tiêu của họ trên Bitcoin là ẩn danh. Mặc dù tất cả các chi tiêu đều được ghi nhận trên hệ thống, nhưng mọi người sẽ không biết số tài khoản nào đã chi tiêu trừ khi bạn nói cho họ.

## Cách hoạt động

* Mỗi đồng tiền bitcoin về cơ bản là 1 loại tệp máy tính được lưu trữ trong ứng dụng trên điện thoại hoặc máy tính gọi là “ví điện tử”.
* Mọi người có thể gửi đồng tiền Bitcoin tới ví điện tử của bạn, hoặc bạn cũng có thể gửi đồng Bitcoin tới những người khác.
* Mọi giao dịch sẽ được ghi nhận trên 1 danh sách công khai gọi là Blockchain. Điều này có thể giúp theo dõi lịch sử của Bitcoin để ngăn mọi người tiêu tiền không phải của họ, tạo bản sao hoặc hoàn tác giao dịch.

## Đào Bitcoin

* Đào Bitcoin (Bitcoin Mining): Chúng ta có thể kiếm Bitcoin bằng cách dùng những máy tính mạnh mẽ để giúp xác thực các giao dịch. Bằng việc giải những bài toán phức tạp liên quan tới xác thực (verification), độ bảo mật của mạng lưới Bitcoin sẽ được nâng cao, từ đó gia tăng độ tin cậy, đảm bảo tính an ninh cho những thông tin giao dịch bằng Bitcoin sau này.
* Các Bitcoin được đào bằng những con chip chuyên dụng do các công ty Bitcoin Mining sản xuất.
* Bitcoin Mining là một phần rất quan trọng và không thể thiếu đối với mạng lưới bitcoin vì nó duy trì tính công bằng, song song đó cũng giữ cho việc giao dịch bằng bitcoin diễn ra được ổn định, an toàn và bảo mật.

## Ưu điểm

* **Bitcoin thuận tiện trong giao dịch:** Các giao dịch Bitcoin có thể được thực hiện mọi lúc mọi nơi, với số lượng không giới hạn.
* **Có tính bảo mật và an toàn cao:** Bitcoin được giao dịch với độ bảo mật và an toàn cao. Các thông tin giao dịch cũng như danh tính người dùng sẽ không hiển thị ở bất cứ đâu để tránh hacker xâm nhập và chiếm thông tin.
* **Có tiềm năng thương mại điện tử:** Hiện nay đã có rất nhiều doanh nghiệp, công ty, cửa hàng, cho phép sử dụng Bitcoin để thanh toán hóa đơn. Mọi giao dịch Bitcoin không thể hoàn trả hay đảo ngược lại, nên mọi tình trạng gian lận đều vô ích với Bitcoin.

## Nhược điểm

* **Giá Bitcoin thường biến động:** Tỷ giá Bitcoin sẽ biến động theo thời gian thực, có lúc tăng nhưng cũng có lúc giảm. Vì vậy, người dùng cần có đủ kinh nghiệm để có thể theo dõi và phán đoán hợp lý.
* **Dễ thu hút hacker:** Việc Bitcoin được giao dịch không kiểm soát và hấp dẫn như một mỏ vàng nên cũng thu hút hacker tìm đến. Chính vì vậy, người dùng tuyệt đối tránh xảy ra sai sót trong việc bảo mật tài khoản bitcoin của mình.
* **Khó sử dụng:** Việc tham gia đầu tư vào Bitcoin đòi hỏi người người chơi phải phải biết cách chơi tiền ảo Bitcoin, có kinh nghiệm cũng như thông tin về các bước giao dịch trong quá trình đầu tư. Nếu không nắm chắc quy luật, chắc chắn rủi ro của bạn sẽ rất lớn.

# KẾT LUẬN

* Tóm lại, Blockchain là một hệ thống cho phép người dùng lưu trữ trao đổi dữ liệu một cách trực tiếp mà không cần bên thứ ba. Với các đặc trưng cơ bản như: Sổ cái phân tán, cơ chếS đồng thuận phi tập trung và tính bất biến, cùng với ưu điểm vượt trội (an toàn, bảo mật), Blockchain là một nền tảng vững chắc cho cho những ứng dụng mang tính cách mạng trong nhiều lĩnh vực như: tiền tệ, y tế, giáo dục, logistics,… Tuy độ phủ sóng của Blockchain vẫn còn thấp, tập trung ở nhiều công ty lớn. Chúng ta có thể tự tin rằng công nghệ tiên tiến này sẽ còn vươn lên mạnh mẽ và tác động lên mọi mặt cuộc sống trong tương lai không xa.

# BẢNG PHÂN CÔNG CÔNG VIỆC

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| STT | MSSV | Họ tên | Nhiệm vụ | Đánh giá chung |
| 1 | 19520071 | Nguyễn Thị Bảo Hân | - Tìm kiếm nội dung Bitcoin  - Thuyết trình | **Tốt** |
| 2 | 19520860 | Nguyễn Hoàng Thiên Phước | - Tìm kiếm Khái niệm và Lịch sử Blockchain | **Tốt** |
| 3 | 19521001 | Bùi Anh Thuận | - Tìm kiếm Vai trò của Blockchain  - Thiết kế file word | **Tốt** |
| 4 | 19521272 | Lưu Đức Cảnh | - Thuyết trình  - Nhận xét chung | **Tốt** |
| 5 | 19521306 | Nguyễn Quang Đại | - Làm file powerpoint  - Thuyết trình | **Tốt** |
| 6 | 19520593 | Dương Nguyễn Hoàng Huy | - Thiết kế file word | **Chưa đạt** |

# TÀI LIỆU THAM KHẢO

|  |  |
| --- | --- |
| [1] | #Rất-đơn-giản, “Giải thích công nghệ BLOCKCHAIN rất dễ hiểu,” 14 8 2018. [Trực tuyến]. Available: https://www.youtube.com/watch?v=auMA7jIHYvQ. [Đã truy cập 14 9 2019]. |
| [2] | B. Academy, “Lịch sử Blockchain (Chuỗi khối),” 7 10 2019. [Trực tuyến]. Available: https://www.binance.vision/vi/blockchain/history-of-blockchain. [Đã truy cập 14 9 2019]. |
| [3] | B. V. News, “https://www.binance.vision/vi/blockchain/history-of-blockchain,” 1 10 2019. [Trực tuyến]. Available: https://bitcoinvietnamnews.com/blockchain-la-gi. [Đã truy cập 14 9 2019]. |
| [4] | W. t. Việt, “Blockchain,” 7 10 2019. [Trực tuyến]. Available: https://vi.wikipedia.org/wiki/Blockchain. [Đã truy cập 16 9 2019]. |
| [5] | A. Brownworth, “How Blockchain works,” [Trực tuyến]. Available: http://blockchain.mit.edu/how-blockchain-works. [Đã truy cập 9 22 2019]. |
| [6] | D. Nam, “The Importance and Impact of Blockchain Technology and Decentralization,” 27 8 2017. [Trực tuyến]. Available: https://medium.com/@damonnam/the-importance-and-impact-of-blockchain-technology-and-decentralization-27c0de972233. [Đã truy cập 22 9 2019]. |
| [7] | I. f. t. F. (IFTF), “Understand the Blockchain in Two Minutes,” 18 4 2016. [Trực tuyến]. Available: https://www.youtube.com/watch?v=r43LhSUUGTQ. [Đã truy cập 16 9 2019]. |
| [8] | L. Fortney, “Blockchain Explained,” 25 6 2019. [Trực tuyến]. Available: https://www.investopedia.com/terms/b/blockchain.asp#how-blockchain-works. [Đã truy cập 22 9 2019]. |
| [9] | L. Fortney, “Bitcoin Mining, Explained,” 25 6 2019. [Trực tuyến]. Available: https://www.investopedia.com/terms/b/bitcoin-mining.asp. [Đã truy cập 22 9 2019]. |
| [10] | M. Murray, “Blockchain explained,” 15 6 2018. [Trực tuyến]. Available: http://graphics.reuters.com/TECHNOLOGY-BLOCKCHAIN/010070P11GN/index.html. [Đã truy cập 23 9 2019]. |
| [11] | M. Noor, “A Very Brief History Of Blockchain Technology | Blockchain History 2019,” 21 1 2019. [Trực tuyến]. Available: https://medium.com/@muhammadnoor/a-very-brief-history-of-blockchain-technology-blockchain-history-2019-3c9f9857e085. [Đã truy cập 22 9 2019]. |
| [12] | P. Dash, “Crypto Thoughts — Does it matter who came first Blockchain or Bitcoin?,” 20 2 2018. [Trực tuyến]. Available: https://medium.com/crypt-bytes-tech/crypto-thoughts-does-it-matter-who-came-first-blockchain-or-bitcoin-fcdc0268f8f9. [Đã truy cập 22 9 2019]. |
| [13] | Victor, “WHY IS BLOCKCHAIN TECHNOLOGY IMPORTANT?,” 8 31 2018. [Trực tuyến]. Available: https://crushcrypto.com/why-is-blockchain-important/. [Đã truy cập 22 9 2019]. |