***Tìm hiểu về Blockchain***

1. *Tổng quan*

## 1. ****Blockchain là gì?****

***Blockchain*** hay ***cuốn sổ cái*** (dịch ra tiếng việt là chuỗi khối), tên ban đầu của nó là **block chain,**là một hệ thống cơ sở dữ liệu chứa thông tin, được dùng để lưu trữ thông tin trong các khối thông tin được liên kết với nhau, và được quản lý bởi tất cả mọi người tham gia hệ thống, thay vì một bên thứ 3 riêng lẻ như nhà nước hay ngân hàng trung ương; đồng thời cho phép truyền tải dữ liệu một cách an toàn bằng một hệ thống mã hóa phức tạp, và được mở rộng theo thời gian2.Ý tưởng ra đời của công nghệ Blockchain



***Blockchain*** được tạo ra để chống lại sự thay đổi dữ liệu trong hệ thống, đồng thời **công nghệ blockchain (Blockchain technology)** cũng có một tính năng rất đặc biệt đó là việc truyền tải dữ liệu không đòi hỏi một trung gian nào để xác nhận thông tin. Bởi vì trong hệ thống Blockchain tồn tại rất nhiều nút hoạt động độc lập có khả năng xác thực các thông tin trong hệ thống mà không đòi hỏi “dấu hiệu của niềm tin”.  
Thông tin khi được nhập vào trong **chuỗi khối blockchain** thì sẽ không thể thay đổi và chỉ được bổ sung thêm khi có sự chấp thuận của tất cả mọi người trong hệ thống. Đây là một hệ thống đảm bảo sự an toàn rất cao cho các dữ liệu trước các nguy cơ bị đánh cắp, nhất là các dữ liệu nhạy cảm như tài khoản ngân hàng online, tài khoản thẻ thanh toán… Ngay cả khi nếu một phần của hệ thống blockchain bị tấn công, thì các phần khác không bị ảnh hưởng và vẫn tiếp tục hoạt động để bảo vệ thông tin.

***Blockchain*** được các chuyên gia trên thế giới ví như một cuốn sổ kế toán chính (hay còn gọi là cuốn sổ cái) của một công ty, nơi mà mọi hoạt động liên quan đến tiền của công ty được giám sát rất chặt chẽ. Trong trường hợp này Blockchain là một cuốn sổ cái hoạt động trong lĩnh vực công nghệ, và dữ liệu được lưu trữ là các dữ liệu số.

## 2. ****Đặc điểm chính của công nghệ Blockchain****

***Công nghệ Blockchain (Blockchain technology)*** đóng vai trò giống như một cuốn sổ cái ghi lại tất cả các giao dịch xảy ra trong hệ thống. Các đặc điểm chính của blockchain có thể kể đến như:

* ***Không thể làm giả, không thể phá hủy các chuỗi blockchain*** : Các chuỗi Blockchian gần như không thể bị phá hủy được, và theo lý thuyết thì chỉ có máy tính lượng tử mới có thể can thiệp vào và giải mã chuỗi blockchain và nó chỉ bị phá hủy hoàn toàn khi không còn internet trên toàn cầu
* ***Bất biến :*** Dữ liệu trong blockchan gần như không thể sửa đổi được (chỉ có thể sửa đổi được bởi chính người đã tạo ra nó, nhưng phải được sự đồng thuận của các nút trên mạng) và các dữ liệu đó sẽ lưu giữ mãi mãi
* ***Bảo mật Dữ liệu :*** Các thông tin, dữ liệu trong các chuỗi blockchain được phân tán và an toàn tuyệt đối chỉ có người nắm giữ private key mới có quyền truy xuất dữ liệu đó
* **Minh bạch :** Ai cũng có thể theo dõi được đường đi của dữ liệu trong blockchain từ địa chỉ này tới địa chỉ khác và có thể thống kê toàn bộ lịch sử trên địa chỉ đó.
* [***Hợp đồng thông minh***](https://blogtienao.com/smart-contract-hop-dong-thong-minh-la-gi/)**:** là các kỹ thuật số được nhúng bởi một đoạn code if-this-then-that (IFTTT) trong hệ thống, cho phép chúng tự thực thi mà không cần bên thứ ba. Blockchain không cần bên thứ ba tham gia vào hệ thống, và nó bảo đảm rằng tất cả các bên tham gia đều biết được chi tiết hợp đồng và các điều khoản sẽ được tự động thực hiện một khi các điều kiện được bảo đảm.

## 3. ****Blockchain được phân loại như thế nào?****

***Trong hệ thống Blockchain chia thành 3 loại chính gồm:***

* ***Public :*** Đây là hệ thống blockchain mà bất kỳ ai cũng có quyền đọc và ghi dữ liệu trên Blockchain được. Quá trình xác thực giao dịch trên Blockchain này đòi hỏi phải có hàng nghìn hay thậm chí là hàng vạn nút tham gia. Do đó để tấn công vào hệ thống Blockchain này là điều bất khả thi vì chi phí rất cao. Ví dụ về public blockchain: [**Bitcoin**](https://blogtienao.com/bitcoin/), [**Ethereum**](https://blogtienao.com/ethereum/)…
* ***Private :***Đây là hệ thống blockchain cho phép người dùng chỉ được quyền đọc dữ liệu, không có quyền ghi vì điều này thuộc về một bên thứ ba tuyệt đối tin cậy. Bên thứ ba này có thể hoặc không cho phép người dùng đọc dữ liệu trong một số trường hợp. Bên thứ ba toàn quyền quyết định mọi thay đổi trên Blockchain. Vì đây là một Private Blockchain, cho nên thời gian xác nhận giao dịch khá nhanh vì chỉ cần một lượng nhỏ thiết bị tham gia xác thực giao dịch. Ví dụ: Ripple là một dạng Private Blockchain, hệ thống này cho phép 20% các nút là gian dối và chỉ cần 80% còn lại hoạt động ổn định là được.
* ***Permissioned :*** Hay còn gọi là Consortium, là một dạng của Private Blockchain nhưng bổ sung thêm một số tính năng nhất định, kết hợp giữa “niềm tin” khi tham gia vào Public và “niềm tin tuyệt đối” khi tham gia vào Private. Ví dụ: Các ngân hàng hay tổ chức tài chính liên doanh sẽ sử dụng Blockchain cho riêng mình.

## 4. ****Các phiên bản chính của Blockchain****

***Hiện tại thì công nghệ blockchain có 3 phiên bản chính gồm:***

* ***Blockchain 1.0 – Tiền tệ và Thanh toán :*** Là phiên bản sơ khai và đầu tiên của blockchain, ưng dụng chính của phiên bản này là các công việc liên quan đến tiền mã hoá: bao gồm việc chuyển đổi tiền tệ, kiều hối và tạo lập hệ thống thanh toán kỹ thuật số. Đây cũng là lĩnh vực quen thuộc với rất nhiều ngườt nhất, đôi khi khá nhiều người lầm tưởng Bitcoin và Blockchain là một.
* ***Blockchain 2.0 – Tài chính và Thị trường :*** Đây là phiên bản thứ 2 của blockchain, ứng dụng của nó là xử lý tài chính và ngân hàng: mở rộng quy mô của Blockchain, đưa blockchain tích hợp vào các ứng dụng tài chính và thị trường. Các tài sản bao gồm cổ phiếu, chi phiếu, nợ, quyền sở hữu và bất kỳ điều gì có liên quan đến thỏa thuận hay hợp đồng.
* ***Blockchain 3.0 – Thiết kế và Giám sát hoạt động :*** Hiện tại đây đang là phiên bản cao nhất của blockchain, với phiên bản này, công nghệ Blockchain sẽ vượt khỏi biên giới chỉ phục vụ cho lĩnh vực tài chính, và đi vào các lĩnh vực khác như giáo dục, chính phủ, y tế và nghệ thuật…

## 5. ****Các cơ chế đồng thuận trong Blockchain****

Cơ chế đồng thuận trong ***Blockchain*** có thể hiểu như cách thức mà mọi người quản lý trong hệ thống blockchain có thể đồng ý cho một giao dịch xảy ra trong hệ thống. Dưới đây là các loại cơ chế đồng thuận phổ biến trong blockchain:

* [***Proof of Work***](https://blogtienao.com/proof-of-work-pow-va-proof-of-stake-pos-la-gi/)***(Bằng chứng Công việc)****:* Đây là cơ chế đồng thuận phổ biến nhất, được dùng trong Bitcoin, Ethereum, [**Litecoin**](https://blogtienao.com/litecoin-la-gi/), [**Dogecoin**](https://blogtienao.com/dogecoin-la-gi/)và hầu hết các loại tiền mã hoá. Đây là cơ chế đồng thuận tiêu tốn khá nhiều điện năng.
* [***Proof of Stake***](https://blogtienao.com/proof-of-work-pow-va-proof-of-stake-pos-la-gi/)***(Bằng chứng Cổ phần):*** Đây là cơ chế đồng thuận phổ biến trong Decred, Peercoin và trong tương lai là Ethereum và nhiều loại tiền mã hoá khác. Cơ chế đồng thuận này phân cấp hơn, tiêu hao ít năng lượng và không dễ gì bị đe doạ.
* ***Delegated Proof-of-Stake (Uỷ quyền Cổ phần):*** Đây là cơ chế đồng thuận phổ biến trong [**Steemit**](https://blogtienao.com/steem-la-gi/), [**EOS**](https://blogtienao.com/eos-la-gi/), [**BitShares**](https://blogtienao.com/bitshares-la-gi/). Cơ chế đồng thuận này có chi phí giao dịch rẻ; có khả năng mở rộng; hiệu suất năng lượng cao. Tuy nhiên vẫn một phần hơi hướng tập trung vì thuật toán này lựa chọn người đáng tin cậy để uỷ quyền.
* ***Proof of Authority (Bằng chứng Uỷ nhiệm):*** Đây là cơ chế đồng thuận phổ biến thường thấy trong [**POA.Network**](https://blogtienao.com/poa-network-la-gi/), Ethereum Kovan testnet. Cơ chế đồng thuận này có hiệu suất cao, có khả năng mở rộng tốt.
* ***Proof-of-Weight (Bằng chứng Khối lượng /Càng lớn càng tốt):*** Đây là cơ chế đồng thuận phổ biến trong Algorand, Filecoin. Cơ chế đồng thuận này có thể tuỳ chỉnh và khả năng mở rộng tốt. Tuy nhiên quá trình thúc đẩy việc phát triển sẽ là một thử thách lớn.
* ***Byzantine Fault Tolerance (Đồng thuận chống gian lận /Tướng Byzantine bao vây Blockchain):*** Đây là cơ chế đồng thuận phổ biến trong Hyperledger, Stellar, Dispatch, và [**Ripple**](https://blogtienao.com/ripple-la-gi/). Cơ chế đồng thuận này có năng suất cao; chi phí thấp; có khả năng mở rộng. Tuy nhiên vẫn chưa thể tin tưởng hoàn toàn. Thuật toán này có 2 phiên bản là:
  + Practical Byzantine Fault Tolerance (Đồng thuận chống gian lận / Tướng Byzantine bao vây Blockchain trong thực tế)
  + Federated Byzantine Agreement (Liên minh Byzantine cùng đồng thuận)
* ***Directed Acyclic Graphs (Thuật toán tô pô):*** Đây là cơ chế đồng thuận thường thấy trong Iota (công nghệ Tangle), Hashgraph, Raiblocks/Nano (công nghệ Block-lattice), là một đối thủ của Blockchain.

## 6. ****Công nghệ Blockchain hoạt động như thế nào?****

***Công nghệ blockchain*** có lẽ là phát minh tốt nhất từ chính Internet. Nó cho phép trao đổi giá trị mà không cần sự tin tưởng hoặc chứng cứ làm tin. Hãy tưởng tượng bạn và tôi đặt cược 50$ cho thời tiết ngày mai ở San Francisco. Tôi đặt cược trời sẽ nắng, bạn cược là mưa. Hôm nay chúng ta có ba tùy chọn để quản lý giao dịch này:

* ***Chúng ta có thể tin tưởng lẫn nhau***. Mưa hoặc nắng, người thua sẽ trả 50 đô la cho người chiến thắng. Nếu chúng ta là bạn, đây có thể là một cách hay để đặt cược. Tuy nhiên, dù là bạn bè hay người lạ thì vẫn không thể dễ dàng trả tiền cho người kia.
* ***Chúng ta có thể biến tiền cược thành một hợp đồng****.* Với một hợp đồng tại chỗ, cả hai bên sẽ dễ phải trả tiền hơn, tuy nhiên, nếu một trong hai người quyết định không trả, người chiến thắng sẽ phải trả thêm tiền để trang trải chi phí pháp lý và bản án có thể mất một thời gian dài. Đặc biệt với một lượng tiền mặt nhỏ, điều này dường như không phải là cách tối ưu để quản lý giao dịch.
* ***Chúng ta có thể nhờ đến một bên thứ ba trung lập***. Mỗi người trong chúng ta đưa 50 đô la cho một người thứ ba, cô ấy sẽ đưa tổng số tiền cho người chiến thắng. Nhưng, cô ấy cũng có thể bỏ trốn với tất cả số tiền. Vì vậy, chúng ta sẽ chọn một trong hai lựa chọn đầu tiên: tin tưởng hoặc hợp đồng.

Cả sự tin tưởng và hợp đồng đều không phải là giải pháp tối ưu. Chúng ta không thể tin tưởng vào người lạ và thực thi hợp đồng đòi hỏi thời gian và tiền bạc. ***Công nghệ blockchain*** là thú vị vì nó cung cấp cho chúng ta lựa chọn thứ ba, an toàn, nhanh chóng và rẻ tiền.

***Blockchain*** cho phép viết một vài dòng code, chương trình chạy trên blockchain, mà cả hai chúng ta gửi 50 đô la vào đó. Chương trình này sẽ giữ 100 đô la an toàn và kiểm tra thời tiết ngày mai một cách tự động trên nhiều nguồn dữ liệu. Nắng hoặc mưa, nó sẽ tự động chuyển toàn bộ số tiền cho người chiến thắng. Mỗi bên có thể kiểm tra hợp đồng logic, và vì nó đang chạy trên blockchain nên nó không thể thay đổi hoặc ngừng lại. Nỗ lực này có thể là quá cao đối với một giao dịch 50 đô la, nhưng hãy tưởng tượng khi bán nhà hoặc công ty.

Mục tiêu của phần này là để giải thích cách blockchain hoạt động mà không thảo luận về các chi tiết kỹ thuật sâu, nhưng đủ để bạn có một ý tưởng chung về logic và cơ chế cơ bản.

## 7. Tương lai của công nghệ Blockchain

- Giống như khi máy tính cá nhân hoặc Internet mới ra đời, công nghệ blockchain xuất hiện cũng sẽ thay đổi cách mà chúng ta hiểu biết và nhìn nhận xã hội.

- [*Hợp đồng Thông minh*](https://cafebitcoin.info/huong-dan/smart-contract-la-gi/) là tiềm năng lớn nhất của công nghệ blockchain trong thực tiễn: nội dung trong hợp đồng và các giao dịch sẽ không bị tiết lộ với bên thứ ba, nhưng mọi thứ vẫn là minh bạch và an toàn.

- Thông tin trong Blockchain rất khó bị làm giả, cho dù bị làm giả thì vẫn sẽ để lại dấu vết. Mọi thay đổi cần phải nhận được sự đồng thuận của tất cả các nút tham gia trong hệ thống. Hệ thống rất khó bị phá vỡ, bởi vì ngay cả khi một phần mạng lưới bị “đơ” thì các nút khác vẫn sẽ tiếp tục hoạt động để bảo vệ thông tin.

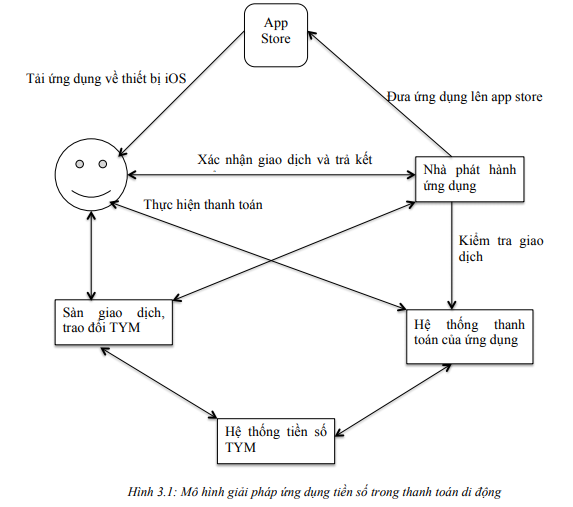
- Công nghệ Blockchain mở ra một xu hướng mới cho các lĩnh vực như: tài chính ngân hàng, logistics, điện tử viễn thông, kế toán kiểm toán…

- Ngoài ra, công nghệ Blockchain còn là nền tảng của [***Internet vạn vật (IoT)***](https://cafebitcoin.info/huong-dan/internet-van-vat/)*.* Các thiết bị điện tử có thể giao tiếp một cách an toàn và minh bạch, những nỗ lực bất chính trên môi trường Internet sẽ không thực hiện được, và còn nhiều điều nữa…

- Hiện nay có rất nhiều công ty và tập đoàn lớn đang xây dựng mạng lưới của riêng mình bằng công nghệ blockchain. Vì thế chúng ta sẽ sớm thấy điều này có thể tạo ra một làn sóng cho tương lai.

1. *Ứng dụng của Blockchain :*

### ***Ứng dụng Trong Thanh toán di dộng***



***Ứng dụng mua bán sách điện tử gồm các bước sau:***

1) Nhà phát hành đưa ứng dụng lên App Store.

2) Người dùng tải ứng dụng về từ App Store.

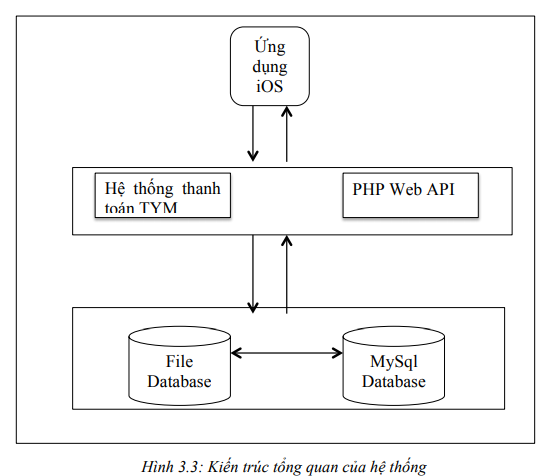
3) Khi muốn mua sách điện tử, người dùng thanh toán trực tiếp TYM vào ví của nhà phát hành ứng dụng thông qua hệ thống thanh toán. Giao thức thanh toán P2P giúp cho nhà phát hành có thể nhận tiền ngay sau đó.

4) Người dùng sau khi thanh toán, yêu cần nhà phát hành kiểm tra thông tin giao dịch và trả về sách điện tử mà người dùng đã mua. Hệ thống tiền số TYM Nhà phát hành ứng dụng App Store Hệ thống thanh toán của ứng dụng Sàn giao dịch, trao đổi TYM Đưa ứng dụng lên app store Tải ứng dụng về thiết bị iOS Thực hiện thanh toán Kiểm tra giao dịch Xác nhận giao dịch và trả kết quả 34 .

5) Nhà phát hành cần gọi sang hệ thống thanh toán để kiểm tra giao dịch là hợp lệ và trả về dữ liệu tương ứng cho người dùng. Để có được tiền số TYM, người dùng cần thực hiện giao dịch mua bán, trao đổi (exchange) thông qua một sàn giao dịch TYM. Nhà phát hành sau khi bán được sách cho người dùng cũng có thể lên sàn giao dịch này để thực hiện mua bán, chuyển đổi sang các đơn vị tiền tệ khác như USD, BTC, ETH,..

***Xây dựng hệ thống tiền số và ứng dụng mua bán sách điện tử***

* ***Kiến trúc hệ thống :***



***Hệ thống được xây dựng dựa trên ba thành phần chính***

***• Ứng dụng iOS:*** Hiển thị giao diện, cho phép người dùng mua bán sách điện tử.

***• PHP Web API:*** Cung cấp các API thực hiện các chức năng đặc trưng của ứng dụng như đăng nhập, đăng xuất, lấy danh sách các sách đang bán, sách đã mua,...

***• Hệ thống tiền số TYM:*** Lưu trữ các giao dịch, cung cấp các API để ứng dụng iOS có thể thực hiện giao dịch và kiểm tra giao dịch.

***• Hệ thống thanh toán TYM PHP Web API File Database MySql Database*** Ứng ***dụng iOS 36*** Tương tự như các đồng tiền số hiện tại, hệ thống sẽ lưu trữ dữ liệu của Blockchain vào file database nhằm mục đích dễ dàng triển khai trên nhiều nút. Các nút khi cài đặt cần lưu trữ dữ liệu vào file, giúp cho hệ thống dễ dàng cài đặt và triển khai trên nhiều thiết bị khác nhau.

***• Cơ sở dữ liệu MySql*** được dùng để lưu trữ thông tin của người dùng, thông tin sách, và các dữ liệu khác đặc thù của ứng dụng.

***• Dữ liệu trong các API của hệ thống được trả về dưới định dạng JSON.*** Trong phạm vi của luận văn, việc cài đặt hệ thống tiền số TYM sử dụng công nghệ blockchain sẽ được trình bày chi tiết, cách cài đặt Web API cũng như ứng dụng iOS sẽ không được mô tả cụ thể

* ***Đặc tả chức năng :***

***Hệ thống tiền số TYM cung cấp API với các chức năng sau:***

• API thực hiện giao dịch chuyển tiền từ ví A sang ví B.

• API thực hiện kiểm tra giao dịch có hợp lệ hay không.

• API kiểm tra giá trị TYM có thể chi tiêu của ví (balance).

• API hiển thị toàn bộ các block trong Blockchain.

***Các chức năng của ứng dụng mua sách điện tử:***

• Người bán chính là nhà phát hành ứng dụng, người bán sử dụng một hệ thống giao diện web để thao tác với cơ sở dữ liệu, thêm hoặc xóa sách, chỉnh sửa nội dung sách.

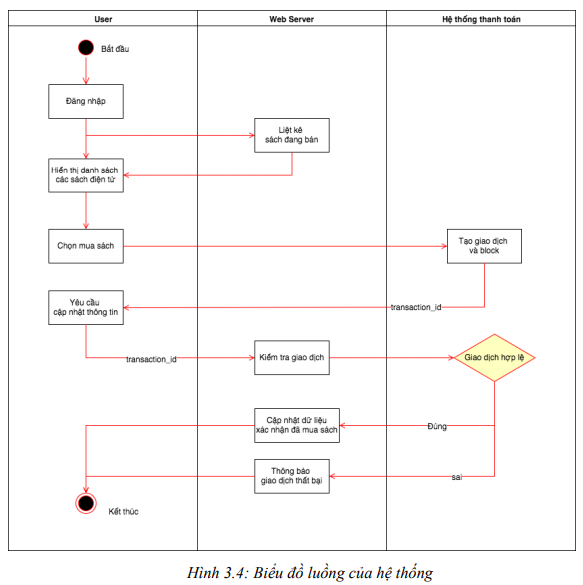
• Người mua sau khi đăng nhập vào ứng dụng, ứng dụng sẽ thực hiện gọi một số API cần thiết của PHP Web API để thực hiện lấy danh sách các sách điện tử đang bán, các sách bán chạy, sách nổi bật,...

• Người dùng chọn mua sách, sau khi xác nhận hệ thống sẽ kiểm tra xem số dư trong ví có đủ hay không, nếu đủ số dư sẽ gọi tới API của hệ thống thanh toán để thực hiện giao dịch, API sẽ trả về mã giao dịch.

• Ứng dụng iOS dùng mã giao dịch nhận được gọi PHP Web API để thực hiện cập nhật thông tin giao dịch đã thanh toán.

• PHP Web API gọi API của hệ thống thanh toán để xác nhận lại giao dịch, và tiến hành cập nhật cơ sở dữ liệu, lưu trạng thái của người dùng đã mua cuốn sách mà người dùng chọn.

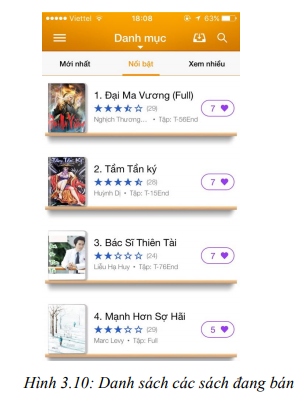
***Các bước thực hiện được mô tả chi tiết như hình 3.4 bên dưới***



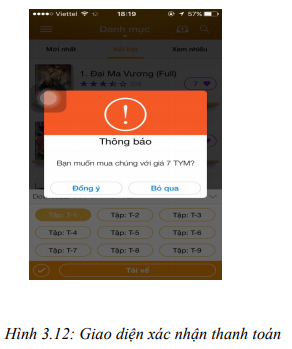
* ***Kết quả thử nghiệm***

Dưới đây là một số màn hình của ứng dụng IOS đã được xây dựng

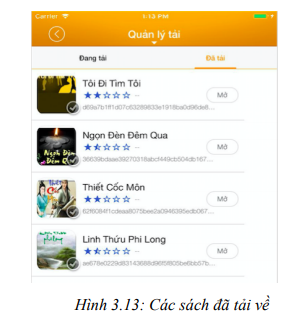
***+ Khi mới truy cập vào màn hình sẽ hiển thị danh sách các sản phẩm***



***+ Khi chọn mua một cuốn sách tại danh sách các sách đang bán, người dùng sẽ được hỏi có xác nhận mua sách hay không***



***+ Danh sách các sách đã tải về***



*TÀI LIỆU THAM KHẢO*

*Tiếng Việt*

[1] Trịnh Nhật Tiến, Giáo trình An Toàn Dữ Liệu, Hà Nội, 2008, tr.21-46

*Tiếng Anh*

[2] Satoshi Nakamoto, "Bitcoin: A Peer-to-Peer Electronic Cash System," <https://bitcoin.org/bitcoin.pdf>

[3] Don Tapscott and Alex Tapscott, "Blockchain Revolution: How the Technology Behind Bitcoin Is Changing Money, Business and the World," <http://blockchain-revolution.com/>

[4] Bitcoin project, “Bitcoin – open source P2P money,” 2017.

[5] Wang, L. Feng, H. Zhang, C. Lyu, L. Wang and Y. You, "Human Resource Information Management Model based on Blockchain Technology," 2017 IEEE Symposium on Service-Oriented System Engineering (SOSE), San Francisco, CA, 2017, pp. 168-173.

[6] Z. Zheng, S. Xie, H. Dai, X. Chen and H. Wang, "An Overview of Blockchain Technology: Architecture, Consensus, and Future Trends," 2017 IEEE International Congress on Big Data (BigData Congress), Honolulu, HI, 2017, pp. 557-564.

[7] M. E. Peck and S. K. Moore, "The blossoming of the blockchain," in IEEE Spectrum, vol. 54, no. 10, pp. 24-25, October 2017.

[8] T. Lundqvist, A. de Blanche and H. R. H. Andersson, "Thing-to-thing electricity micro payments using blockchain technology," 2017 Global Internet of Things Summit (GIoTS), Geneva, 2017, pp. 1-6.

[9] J. Sidhu, "Syscoin: A Peer-to-Peer Electronic Cash System with Blockchain-Based Services for E-Business," 2017 26th International Conference on Computer Communication and Networks (ICCCN), Vancouver, BC, 2017, pp. 1-6.

[10] Patrick D. Gallagher, "Digital Signature Standard (DSS)," in FIPS PUB 186-4, pp. 26-30, July 2013.

*Các nguồn trên Internet*

[11] <https://vi.wikipedia.org/wiki/Blockchain>

[12] <https://en.bitcoin.it/wiki/Difficulty>

[13]<http://ictnews.vn/internet/chinh-sach-doc-quyen-thanh-toan-cuagoogle-va-apple-dang-bi-cheater-truc-loi-157137.ict>

[14]<https://bfsystem.org/khac-biet-giua-tien-thuat-toan-tien-ao-tien-dien-tu/>

[15]<http://www.pcworld.com.vn/articles/congnghe/congnghe/2017/03/1250627/blockchain-xu-huong-moi-trong-tuong-lai/>