ĐẠI HỌC QUỐC GIA TP. HỒ CHÍ MINH
ĐẠI HỌC BÁCH KHOA
KHOA KHOA HỌC & KĨ THUẬT MÁY TÍNH

LUẬN VĂN TỐT NGHIỆP

Xây Dựng Công Cụ Hỗ Trợ Dự Đoán Giá Trị Bitcoin Bằng Máy Học

Hội đồng: Mạng và Hệ Thống Máy Tính

Người thực hiện:

Phan Sơn Tự 51204436

Giáo viên hướng dẫn:

TS. Nguyễn Đức Thái

TP. Hồ Chí Minh, ngày 22 tháng 12 năm 2016

Lời cam kết

Tôi tên Phan Sơn Tự - 51204436, hiện đang là sinh viên khoa Khoa Học và Kĩ Thuật Máy Tính, Đại học Bách Khoa TP.HCM. Tôi xin cam kết báo cáo luận văn tốt nghiệp với đề tài "Xây dựng công cụ hỗ trợ dự đoán giá trị bitcoin bằng Máy học" là công trình nghiên cứu độc lập, tự tìm hiểu của bản thân, không sao chép bất kì công trình nghiên cứu nào.

Đề tài được thực hiện cho mục đích tìm hiểu và nghiên cứu ở bậc đại học.

Tất cả những tài liệu tham khảo được ghi trong báo cáo đều được trích dẫn rõ ràng từ các nguồn đáng tin cậy và từ một số bài báo khoa học.

Tất cả số liệu trong bài báo cáo đều được thực hiện một cách trung thực, không gian dối, không sao chép từ bất kì nguồn nào.

Các công cụ hỗ trợ cho việc thực hiện giải thuật, đo đạt số liệu đều là mã nguồn mở và tập dữ liệu được cung cấp hoàn toàn công khai của chủ nhân, tổ chức sở hữu.

Hình ảnh trong bài báo cáo đều được trích dẫn nguồn gốc rõ ràng.

Lời cảm ơn

Lời đầu tiên, xin cám ơn mẹ Hoa yêu quý của tôi, người đã chăm lo cuộc sống đầy đủ cho tôi trong suốt quãng đời sinh viên, giúp tôi an tâm trong học tập, nghiên cứu. Và thật lòng, tôi không thể có ngày hôm nay nếu bên cạnh tôi không phải là mẹ.

Sau đó, tôi xin được phép gửi lời cảm ơn sâu sắc đến TS. Nguyễn Đức Thái, người thầy đã giúp đỡ tôi trong thời gian thực hiện đề tài. Không chỉ đơn thuần là một giảng viên truyền thụ kiến thức, cũng không đơn thuần là một giáo viên hướng dẫn luận văn, thầy đối với tôi còn nhiều hơn thế. Thầy là một trong số ít những người đã truyền cảm hứng cho tôi trong lĩnh vực Machine Learning và đó là còn đường tôi đang chọn. Làm việc trong một khoảng thời gian với thầy, nhờ những sự chỉ bảo, định hướng tận tình của thầy cũng như không ngại ngần đưa ra những khuyết điểm đã giúp tôi hiểu rõ bản thân và ngày càng hoàn thiện mình hơn. Thầy hết lòng vì sinh viên đó là điều tôi thán phục ở thầy.

Cuối cùng, tôi xin gửi lời cảm ơn đến những người thầy, người cô đã và đang công tác tại mái trường Đại học Bách Khoa TP. Hồ Chí Minh và đặc biệt là khoa Khoa Học và Kĩ Thuật Máy Tính, chúc thầy cô sức khỏe dồi dào, tiếp tục công tác giảng dạy đào tạo để cho ra những thế hệ kỹ sư có chuyên môn giỏi, đạo đức tốt, góp phần xây dựng một xã hội vững mạnh.

Thành phố Hồ Chí Minh, ngày 22 tháng 12 năm 2016
Phan Sơn Tự

Lời giới thiệu

"Rủi ro càng cao, lợi ích càng nhiều" đó là một trong những câu nói thường được nghe trong môi trường kinh tế và tài chính, điều này đa số đúng với các hành vi đầu tư kinh tế. Người đầu tư giỏi là người đầu tư có khả năng đoán biết rủi ro từ đó giảm thiểu rủi ro nhưng vẫn gia tăng lợi nhuận, để làm được điều này người đầu tư cần có kiến thức chuyên sâu về kinh tế và kinh nhgiệm, trong đó kinh nghiệm chiếm một vị trí rất quan trọng.

Về một lĩnh vực khác, ngành Công nghệ thông tin đang trở thành một ngành không thể thiếu đối mọi lĩnh vực, nó làm thay đổi phương thức lao động, tạo ra các giá trị hoàn toàn mới, thúc đẩy các lĩnh vực khác cực kỳ mạnh mẽ. Và Kinh tế cũng không nằm ngoài tác động đó. Cũng vì vậy mà lĩnh vực Business Intelligence được sinh ra, đây là một sản phẩm của quá trình sử dụng chất xám Công nghệ thông tin để giải quyết thông minh các vấn đề kinh tế.

Business Intelligence là một bức tranh rộng lớn, riêng trong phạm vi luận văn này, tác giả xin trình bày một đề tài cụ thể, đó là sử dụng Máy học để giải quyết bài toán giảm thiểu rủi ro trong đầu tư Bitcoin.

Mục lục

Lời cam kết **i**

Lời cảm ơn **ii**

Lời giới thiệu **iii**

Mục lục **iv**

Danh sách hình vẽ **vi**

Danh sách bảng **vii**

Danh mục chữ viết tắt **viii**

1 Giới thiệu đề tài **1**
1.1 Tính cấp thiết của đề tài 1
1.2 Đặc tả đề tài 1
1.3 Mục tiêu của đề tài 2
1.4 Phương pháp thực hiện đề tài 3
1.5 Bố cục luận văn 3

2 Những công trình liên quan **4**

3 Nền tảng lý thuyết **6**
3.1 Bitcoin 6
3.1.1 Máy chủ nhãn thời gian - Timestamp Server 6
3.1.2 Giao dịch - Transaction (trên Blockchain) 7
3.1.3 Proof-of-Work 7
3.1.4 Blockchain 7
3.1.5 Mạng - Network 8
3.1.6 Phần thưởng khích lệ 9
3.1.7 Tổ chức lưu trữ thông tin giao dịch 9
3.2 Một số khái niệm về tài chính 11
3.2.1 Phiên giao dịch và các giá trị cơ bản 11
3.2.2 Rate of Change 12

3.2.3 Stochastic Oscillator 12
3.3 Máy học 12
3.3.1 Khái niệm cơ bản 12
3.3.2 Thông số đánh giá 13
3.3.3 Mạng neural - Neural Network 14

4 Phân tích và thiết kế hệ thống 21
4.1 Xây dựng Multilayer Neural Network 21
4.1.1 Feature Selection - Dữ liệu luyện tập 21
4.1.2 Training - Học giải thuật 22
4.1.3 Validation - Đánh giá giải thuật 22
4.2 Xây dựng hệ thống - Web Application 24
4.2.1 Tổng quan hệ thống 24
4.2.2 Hệ thống Machine Learning Server 24
4.2.3 Hệ thống Backend Server 25
4.2.4 Hệ thống UI Frontend Server 26

5 Kết luận và hướng phát triển 28
5.1 Kết luận 28
5.2 Hướng phát triển 29

Tài liệu tham khảo 30

Danh sách hình vẽ

3.1 Máy chủ nhãn thời gian 6
3.2 Giao dịch 7
3.3 Blockchain 8
3.4 Cây Merkle 10
3.5 Cấu trúc tổ chức giao dịch trong một block 10
3.6 Thông số đánh giá 14
3.7 Perceptron 15
3.8 MNN 16
3.9 Ví dụ perceptron với giá trị bias 16
3.10 Đồ thị hàm sigmoid 17
3.11 Đồ thị rời rác hóa hàm sigmoid 18
3.12 Weight Notation example 19
3.13 Bias Notation example 20

4.1 System Structure 24
4.2 UI Frontend Server 1 26
4.3 UI Frontend Server 2 27
4.4 UI Frontend Server 3 27

Danh sách bảng

2.1 Bảng đánh giá - Predicting Gold Prices 4
2.2 Bảng đánh giá - Machine Learning in Stock Price Trend Forecasting 5

4.1 Bảng đánh giá 23

5.1 Bảng đánh giá hệ thống thực tế 28

Danh mục chữ viết tắt

MNN	Multilayer Neural Network
KNN	K-Nearest Neighbors
LR	Logistic Regression
SVM	Support Vector Machine
GDA	Gaussian Discriminant Analysis
QDA	Quadratic Discriminant Analysis
BTC	Bitcoin
USD	US Dollar
ROC	Rate of Change
SO	Stochastic Oscillator
RDP	Relative Difference Percentage
UI	User Interface

Chương 1

Giới thiệu đề tài

1.1 Tính cấp thiết của đề tài

Bitcoin - một hệ thống tiền mã hóa (hay tiền điện tử) được xuất hiện lần đầu tiên vào năm 2009 bởi Satoshi Nakamoto [1], với những đặc tính ưu việt hơn cả tiền tệ truyền thống hiện nay khiến cho sự tăng lên nhanh chóng về giá trị. Nhận thấy được sức mạnh của tiền mã hóa có thể sẽ là tương lai của kinh tế và chính trị nên việc hiểu rõ cũng như đầu tư vào Bitcoin là việc đáng để suy ngẫm.

Hiển nhiên, đối với nước ta Bitcoin là rất mới và việc đầu tư là hết sức rủi ro khi không có nền tảng kiến thức và kinh nghiệm đầu tư. Nhận thấy vấn đề này, bản thân đã đặt ra vấn đề "Tại sao không tạo ra một công cụ để cho nhà đầu tư có thể dựa vào như một yếu tố tham khảo tin cậy?".

Đồng thời, trong lĩnh vực công nghệ thông tin nói riêng, Máy học đang là nền tảng cho hàng loạt các sản phẩm công nghệ mang tính dự đoán thông minh, ngoài ra còn ứng dụng trong các lĩnh vực về trí thông minh nhân tạo, xử lý ngôn ngữ tự nhiên... và điều đó đang đi đúng với mục tiêu của vấn đề được đưa ra trong phạm vi luận văn này.

1.2 Đặc tả đề tài

Trên một sàn giao dịch tiền mã hóa điển hình, quá trình mua bán BTC được chia ra thành các giai đoạn thời gian và được gọi là phiên giao dịch. Một phiên giao dịch được diễn tả bởi các giá trị điển hình như sau:

- Giá mở phiên: giá bán (mua) BTC của (các) giao dịch ngay tại thời điểm mở phiên.
- Giá đóng phiên: giá bán (mua) BTC của (các) giao dịch tại thời điểm kết thúc phiên.

- Giá cao nhất: giá bán (mua) BTC cao nhất của giao dịch trong khoảng thời gian mở phiên đến kết thúc phiên.
- Giá thấp nhất: giá bán (mua) BTC thấp nhất của giao dịch trong khoảng thời gian mở phiên đến kết thúc phiên.

Thời gian của một phiên giao dịch thường được chọn là 5 phút, 30 phút, 1 tiếng, 2 tiếng, 4 tiếng hoặc 1 ngày, ... Trong phạm vi luận văn chúng ta chọn thời gian một phiên giao dịch là 30 phút.

Vậy, bài toán cần giải quyết là đi dự đoán giá trị BTC trong phiên tiếp theo sẽ tăng hay giảm so với phiên hiện tại. Cụ thể, gọi n là phiên hiện tại và n_{close} là giá đóng phiên hiện tại, $(n+1)$ là phiên tiếp theo và $(n+1)_{close}$ là giá đóng phiên tiếp theo. Nếu $(n+1)_{close} > n_{close}$ thì giá tăng - Up, ngược lại thì giá giảm - $Down$.

Sau khi cụ thể được yêu cầu bài toán, ta sẽ đi đặc tả hướng tiếp cận giải quyết vấn đề. Máy học là lựa chọn của luận văn này, cụ thể phương pháp giải quyết sẽ sử dụng giải thuật phân lớp để dự đoán nhãn của phiên giao dịch sẽ là Up hay $Down$.

1.3 Mục tiêu của đề tài

Vấn đề cơ bản của việc đầu tư là lợi nhuận, bám sát với mục tiêu này phương hướng đề ra sẽ đi giải quyết bài toán cụ thể như sau.

Sử dụng USD để mua/bán BTC, với mỗi phiên giao dịch là 30 phút, chúng ta sẽ đi dự đoán giá trị BTC trong phiên tiếp theo sẽ tăng hay giảm - bài toán phân lớp trong Máy học.

Để thực hiện được điều đó chúng ta cần vạch ra những bước đi cụ thể để hiện thực mục tiêu:

- Thu thập, xử lí dữ liệu BTC.
- Áp dụng các giải thuật phân lớp vào tập dữ liệu có được.
- Đánh giá trên lý thuyết hệ thống.
- Vận hành, khảo sát và đánh giá hệ thống trên thực tế.
- Xây dựng, hoàn thiện sản phẩm.

Sản phẩm hoàn thiện mà người dùng được sử dụng sẽ là một Ứng dụng nền Web cung cấp các thông tin, quan điểm để tham khảo cho việc đầu tư.

1.4 Phương pháp thực hiện đề tài

Vì bài toán dự đoán về xu hướng giá trị BTC hầu như chưa có bất kì công trình hoặc bài báo nào được công bố công khai (theo tìm hiểu của cá nhân) nên việc phải tham khảo các hướng giải quyết đã từng có là bất khả thi. Thay vào đó chúng ta sẽ đi tham khảo các bài báo, công trình có mức độ liên quan khá cao như dự đoán xu hướng giá vàng và giá cổ phiếu - các tài liệu này được dẫn tại phần tài liệu tham khảo. Từ những kinh nghiệm của các bài báo, bản thân sẽ đúc kết một vài phương pháp tổng quát, từ đó áp dụng ngược trở lại cho vấn đề dự đoán xu hướng giá trị BTC.

Đồng thời, ngoài việc tham khảo các công trình liên quan, bản thân còn phải sử dụng chính những kinh nghiệm về khai phá dữ liệu và kiến thức Máy học, để áp dụng vào nhằm đem lại kết quả tốt nhất. Việc tìm ra lời giải tốt nhất sẽ tiến hành theo phương pháp so sánh các giải thuật, chúng ta sẽ đi chạy các giải thuật phân lớp khác nhau từ đó đánh giá xem giải thuật nào là tốt hơn và từ đó sẽ tập trung tối ưu cho giải thuật đó.

Sản phẩm hoàn thiện là sản phẩm đã được chạy và khảo nghiệm trên thực tế, vì vậy sau khi xây dựng hoàn chỉnh, hệ thống sẽ được chạy thực tế và đánh giá kết quả trong một khoảng thời gian.

1.5 Bố cục luận văn

Để phục vụ tốt cho việc phát triển sau này, bố cục luận văn sẽ được trình bày theo hướng diễn dịch và được chia thành các phần nhỏ để người đọc có thể nắm bắt nội dung.

Trước hết, chúng ta sẽ đi tìm hiểu qua các công trình liên quan nhằm hiểu được công việc chúng ta sẽ làm là gì, và những hướng giải quyết tổng quát đã được sử dụng ra sao.

Sau đó, phần nền tảng lý thuyết sẽ đề cập đến các kiến thức liên quan đến Bitcoin, một số khái niệm về tài chính, cũng như lý thuyết giải thuật MNN dùng cho phân lớp để phục vụ cho việc đọc hiểu nội dung các chương sau, đặc biệt là phục vụ cho quá trình phân tích giải thuật phân lớp trong Máy học.

Cuối cùng, thu thập dữ liệu và khai phá dữ liệu cho phù hợp với giải thuật, chạy giải thuật, đánh giá giải thuật và hiện thực sản phẩm.

Chương 2

Những công trình liên quan

Như đã nhắc tới trước đó, các công trình về dự đoán xu hướng giá trị Bitcoin hầu như chưa có hoặc chưa được công khai vì thế mà việc tiếp cận chính xác vấn đề là điều không thể. Thay vào đó chúng ta sẽ đi sử dụng các vấn đề liên quan khác như là dự đoán xu hướng giá trị vàng và dự đoán xu hướng giá trị cổ phiếu. Hai công trình cụ thể được tham khảo trong luận văn là:

1. Predicting Gold Prices - Megan Potoski [3]
2. Machine Learning in Stock Price Trend Forecasting - Yuqing Dai & Yuning Zhang [4]

Ở bài báo thứ nhất - Predicting Gold Prices - đã đề cập đến hai giải thuật phân lớp là SVM và LR. Trong đó, vì va vấp với vấn đề mất cân đối trong tập dữ liệu (nhãn positive lớn hơn rất nhiều sao với nhãn negative) nên SVM chỉ được đề cập như một phép so sánh và không được sử dụng trong quá trình giải quyết vấn đề chính. Thay vào đó, LR được sử dụng để giải quyết bài toán phân lớp với kết quả khá khả quan.

LR (Optimal Feature Set):

Precision	69.90%
Recall	72.31%
Accuracy	69.30%

Bảng 2.1: Bảng đánh giá - Predicting Gold Prices

Ở đây, ta nhận thấy bài báo sử dụng ba tham số đánh giá, chưa vội quan tâm đến ý nghĩa từng tham số ta có thể hiểu rằng các tham số này càng cao thì tương đương với giải thuật càng được xem là tốt. Chi tiết ba tham số này sẽ được nhắc đến ở phần Nền tảng lý thuyết.

Bước qua bài báo thứ hai - Machine Learning in Stock Price Trend Forecasting - nhóm tác giả đã sử dụng bốn giải thuật đó là:

- GDA
- LR
- SVM
- QDA

Kết quả đánh giá của 4 giải thuật được nhóm tác giả trình bày:

Model	LR	GDA	QDA	SVM
Accuracy	44.5%	46.4%	58.2%	55.2%

Bảng 2.2: Bảng đánh giá - Machine Learning in Stock Price Trend Forecasting

Thật sự kết quả cho ra không tốt so với bài báo thứ nhất và tham số đánh giá chỉ sử dụng một tham số đó là Accuracy, chúng ta không thể dựa vào đó để đánh giá một cách toàn diện về độ hiệu quả của giải thuật. Nhưng riêng trong công trình này, nhóm tác giả có nêu ra Next-Day Model nhằm dự đoán xu hướng giá cổ phiếu trong ngày tiếp theo và có vẻ khá tương đồng với vấn đề đặt ra trong phạm vi luận văn này.

Tổng quan qua hai công trình và tham khảo một số công trình khác, nhận thấy đa số các hướng tiếp cận đều đi theo một phương pháp tổng quát chung, nó bao gồm các bước cơ bản như:

1. Xây dựng không gian vector thuộc tính phù hợp với tính chất bài toán
2. Sử dụng các giải thuật phân lớp điển hình trong Máy học như là SVM, LR ...
3. Đánh giá giải thuật bằng các tham số Accuracy, Recall, Precision.

Từ những đục kết trên, bản thân nhận thấy các bước trên cũng chính là phương pháp nên dùng để tiếp cận đề tài. Ngoài ra, nhận thấy ở hai công trình trên chưa hề sử dụng một giải thuật rất được phổ biến hiện nay, nó nổi lên như một đại diện của Deep Learning đó là Multilayer Neural Network. Do đó mà luận văn này sẽ sử dụng Multilayer Neural Network như là một giải thuật chính trong quá trình so sánh và đánh giá so với các giải thuật phân lớp khác.

Chương 3

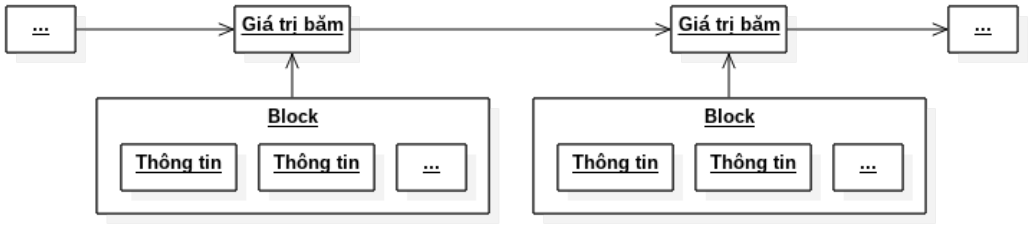
Nền tảng lý thuyết

3.1 Bitcoin

Các hình thức thương mại trên Internet ngày này hầu như đều dựa vào một tổ chức bên thứ ba đáng tin cậy để xử lý các hoạt động thanh toán điện tử. Tuy rằng sau nhiều năm phát triển, các tổ chức bên thứ ba này đều đã nâng cao mức độ tin cậy, an toàn nhưng đa số vẫn còn tồn tại những điểm yếu: không thể tránh khỏi những tranh chấp, phí trung gian, đòi hòi phải cung cấp các thông tin cá nhân... Và Bitcoin - hệ thống tiền điện tử ngang hàng (A Peer-to-Peer Electronic Cash System) được sinh ra để giải quyết các vấn đề trên [2].

3.1.1 Máy chủ nhãn thời gian - Timestamp Server

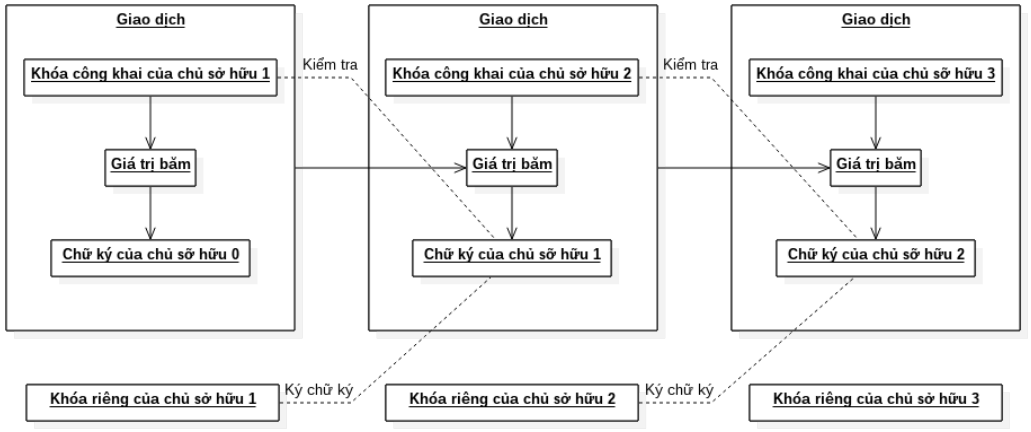
Máy chủ nhãn thời gian hoạt động bằng cách lấy giá trị băm của block liền trước và thông tin của block hiện tại, cho qua hàm băm để được một giá trị băm mới. Giá trị băm sau khi được tính toán sẽ được công bố rộng rãi và giá trị băm này chứng minh rằng block tồn tại, các block được nối với nhau thành một chuỗi xác định.



Hình 3.1: Máy chủ nhãn thời gian

3.1.2 Giao dịch - Transaction (trên Blockchain)

Bitcoin tổ chức các giao dịch bằng cách xây dựng một chuỗi các chữ ký số. Một địa chỉ có chứa một lượng BTC được gọi là một chủ sở hữu, một chủ sở hữu chuyển một lượng BTC cho một chủ sở hữu khác - người thụ hưởng - bằng cách ký lên giá trị băm (hash), trong đó giá trị băm là kết quả sau khi đi qua hàm băm của tổ hợp giá trị băm giao dịch trước với địa chỉ người thụ hưởng.



Hình 3.2: Giao dịch

3.1.3 Proof-of-Work

Proof-of-Work được hiểu là bằng chứng để chứng minh quá trình lao động, nó dùng để kiểm tra quá trình tạo ra kết quả hợp lệ là một quá trình "lao động" có sử dụng và tiêu tốn tài nguyên.

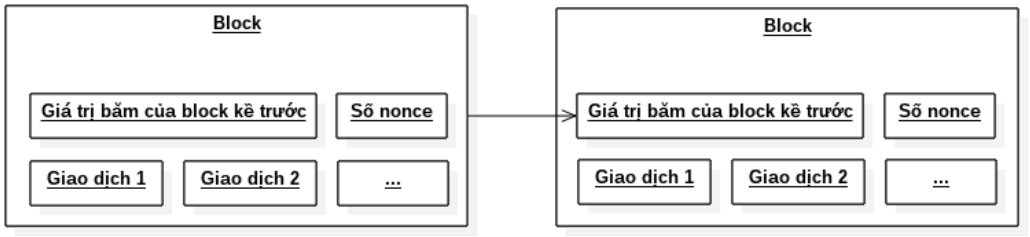
Proof-of-Work được sử dụng trong Bitcoin có cơ chế dựa trên hàm băm, ví dụ như SHA-256. Quá trình proof-of-work là quá trình đi tăng một con số - gọi là số *nonce* - sao cho giá trị băm của số *nonce* này cho kết quả đầu ra phải thỏa mãn tồn tại n bit 0 ở vị trí đầu, với n xác định và được gọi là số bit 0 yêu cầu.

3.1.4 Blockchain

Blockchain được hình thành dựa trên sự kết hợp giữa máy chủ nhãn thời gian và proof-of-work. Blockchain là một chuỗi các block được kết nối một cách luận lý với nhau thông qua các mỗi quan hệ toán học và mật mã, các

quan hệ này đảm bảo cho hệ thống luôn đúng đắn, không thể sửa và dễ dàng để kiểm tra. Block mới được sinh ra phải dựa trên quá trình proof-of-work.

Quá trình hình thành blockchain được bắt đầu bằng proof-of-work, các peer sẽ đi tìm số *nonce* sao cho sau khi cho qua hàm băm kết quả đạt được là một giá trị băm thỏa mãn số bit 0 yêu cầu. Số *nonce* vừa được tìm ra sẽ được đưa và block mới cùng với các thông tin khác như: thông tin các giao dịch, giá trị băm của block kề trước... Tiếp tục như vậy, các block mới được sinh ra và được kết nối với block cuối cùng của chuỗi.



Hình 3.3: Blockchain

Vì hệ thống có tính phân tán nên trên toàn mạng sẽ có nhiều phiên bản của blockchain, cũng chính vì thế để giải quyết tính đồng nhất, chỉ blockchain có độ dài lớn nhất mới được xem là blockchain hợp lệ. Đồng thời để kiểm soát được tốc độ sinh block mới, hệ thống sẽ quy định một độ khó, nếu toàn mạng có tốc độ sinh block (số block được sinh ra trong một giờ đồng hồ) cao hơn mức quy định, độ khó sẽ tăng lên để điều chỉnh lại tốc độ của toàn mạng.

3.1.5 Mạng - Network

Mỗi thành viên (máy tính, phần cứng ASIC, thiết bị di động...) khi tham gia vào quá trình tính toán của toàn mạng thì sẽ được xem như một node. Toàn mạng sẽ hiện thực hệ thống bằng cách thực hiện các bước như sau:

1. Một giao dịch mới được truyền đi cho tất cả các node (broadcast).
2. Mỗi node sẽ lựa chọn và thu thập các giao dịch để đưa vào block.
3. Mỗi node sẽ thực hiện proof-of-work, tìm ra số *nonce*.
4. Khi một node hoàn thành proof-of-work, node này sẽ đóng block và truyền đi toàn tất cả các node khác.

5. Các node khác sẽ kiểm tra thông tin của block nhận được (thông tin các giao dịch, thông tin proof-of-work...) và chấp nhận block này nếu tất cả các thông tin đều được kiểm tra chính xác.

6. Các node sẽ thể hiện sự chấp nhận của mình bằng cách thực hiện proof-of-work để sinh ra block mới block này sẽ được gắn vào liền sau block mà node đã chấp nhận (thêm giá trị băm của block trước mà node chấp nhận vào trong block mới sinh ra).

Lưu ý, một giao dịch mới không nhất thiết phải được truyền đến tất cả các node. Chỉ cần việc truyền đến số node đủ nhiều để đảm bảo việc sẽ được đưa vào một block và được đóng trong blockchain với độ dài lớn nhất. Cũng như vậy đối với block, block không nhất thiết phải được truyền đến tất cả các node, khi một node nhận được một block kế block bị thiếu, bằng quá trình kiểm tra node có thể biết được và yêu cầu các node khác trong mạng gửi cho node này block bị thiếu sót.

3.1.6 Phần thưởng khích lệ

Trong tập các giao dịch được đóng trong một block sẽ luôn tồn tại một giao dịch đặc biệt, giao dịch khác với các giao dịch bình thường, nó không có người chủ sở hữu mà chỉ có người thụ hưởng. Điều này giải thích cách mà BTC mới được sinh ra, cứ mỗi block được tìm ra nhờ quá trình proof-of-work sẽ có một lượng BTC được sinh ra và chính là phần thưởng cho người tạo ra block, điều này đồng nghĩa địa chỉ người thụ hưởng chính là địa chỉ của người tạo ra block.

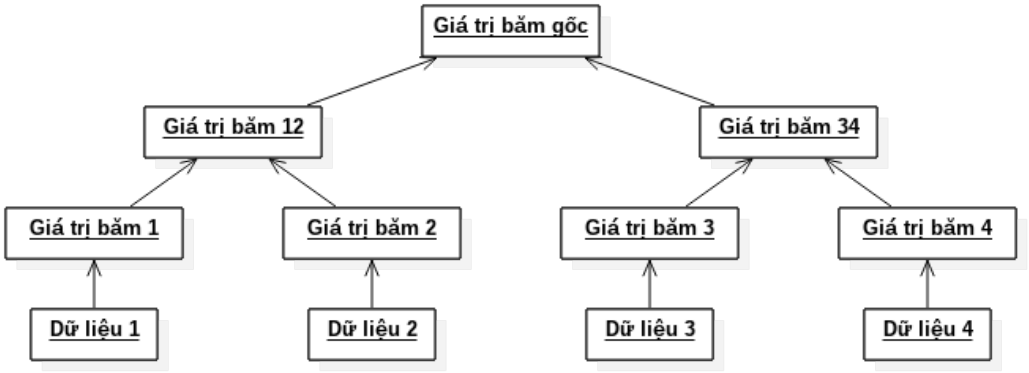
Ngoài ra, phần thưởng khích lệ khi tạo ra được một block còn bao gồm cả phí giao dịch từ các giao dịch đã được đóng trong block. Phí giao dịch thường rất nhỏ và không đáng kể ở thời điểm hiện tại.

3.1.7 Tổ chức lưu trữ thông tin giao dịch

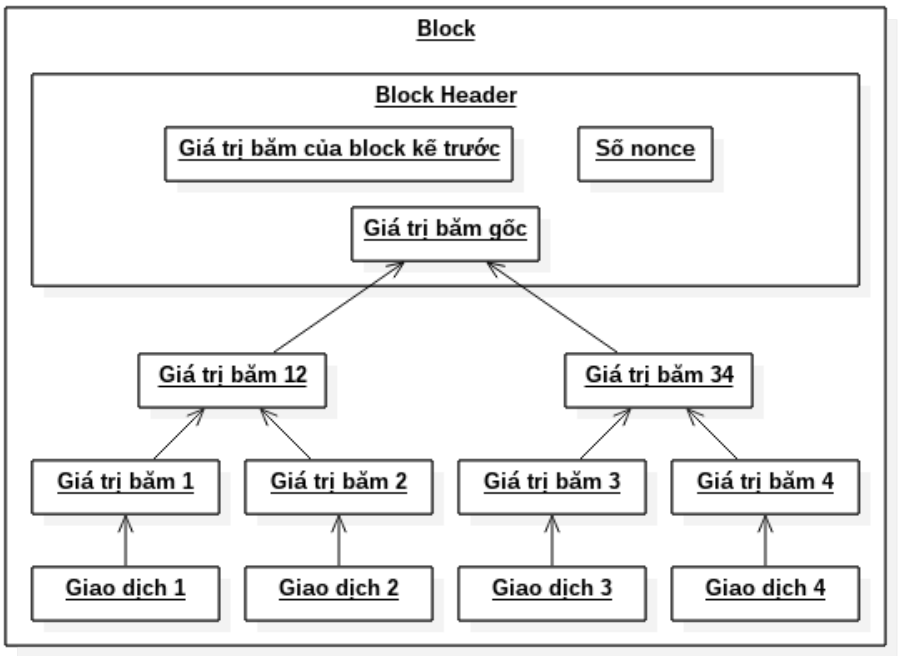
Đối với các node là các hệ thống máy tính lớn, khả năng lưu trữ và xử lý mạnh thì việc lưu một block với đầy đủ các thông tin không gặp nhiều vấn đề. Nhưng đối với các thiết bị di động hoặc các thiết bị khác với tài nguyên lưu trữ và xử lý tương đối hạn hẹp thì việc lưu một blockchain đầy đủ là khá khó khăn.

Cây Merkle là một cấu trúc tổ chức dữ liệu, trong đó giá trị của node cha sẽ là kết quả hàm băm tất cả các giá trị (nhãn hoặc dữ liệu) của nốt con. Các nốt không phải lá thì giá trị sẽ là nhãn - kết quả hàm băm, các nốt lá sẽ có giá trị là dữ liệu cần được tổ chức.

Bitcoin sử dụng cây Merkle để tổ chức các giao dịch, nốt cao nhất của cây được gọi là giá trị băm gốc (Root hash) và giá trị này sẽ được lưu vào block. Ở đây, ta thấy việc thay đổi bất kỳ một giá trị nào trong cây cũng sẽ dẫn đến việc thay đổi giá trị băm gốc, vì thế giá trị băm gốc khi được lưu vào block nó có chức năng dùng để kiểm tra lại các giao dịch trong block đó là toàn vẹn hay không.



Hình 3.4: Cây Merkle



Hình 3.5: Cấu trúc tổ chức giao dịch trong một block

Một node với tài nguyên hạn chế khi muốn lưu blockchain không nhất thiết phải lưu đầy đủ thông tin của từng block trong blockchain, thay vào đó node có thể lược bỏ các thông tin về giao dịch được đóng trong block và chỉ lưu giá trị băm gốc của các giao dịch này. Điều này làm giảm chi phí về lưu trữ nhưng vẫn đảm bảo được tính toàn vẹn, khi muốn xác minh bất kỳ giao dịch nào, node chỉ cần yêu cầu các giao dịch trong block và tính toán lại giá trị băm gốc, nếu giá trị băm nào giống với giá trị băm gốc được lưu nghĩa là các giao dịch hoàn toàn hợp lệ.

3.2 Một số khái niệm về tài chính

3.2.1 Phiên giao dịch và các giá trị cơ bản

Gọi T là một mốc thời gian bất kỳ, P là khoảng thời gian được chọn là một phiên giao dịch. Ta có thể nói một cách đơn giản là phiên giao dịch được mở tại thời điểm T và được kết thúc tại thời điểm $T + P$.

Cụ thể, giả sử chọn mốc mở phiên là 9:00am và phiên giao dịch có thời hạn là 30 phút, điều đó có nghĩa là kết thúc phiên giao dịch sẽ là 9:30am.

Các thông tin của một phiên giao dịch:

- Giá mở phiên: là giá bán của một giao dịch gần nhất sau thời điểm T. Ví dụ tại thời điểm 9:01am có một giao dịch bán 1 BTC là \$779 và trong khoảng thời gian 9:00am đến 9:01am không hề có bất kỳ giao dịch nào khác ngoại trừ giao dịch này, thì ta có thể nói giá mở phiên sẽ là \$779.

- Giá đóng phiên: là giá bán của một giao dịch gần nhất trước thời điểm $T + P$.

- Giá phiên cao nhất: là giá bán cao nhất của một giao dịch trong khoảng thời gian diễn ra phiên giao dịch, cụ thể là từ thời điểm T đến thời điểm $T + P$. Ví dụ, trong khoảng thời gian 9:00am (thời điểm mở phiên) đến thời gian 9:30am (thời điểm đóng phiên) có một giao dịch BTC với giá là \$801 và là giao dịch có giá trị cao nhất. Vậy ta có thể nó giá phiên cao nhất là \$801.

- Giá phiên thấp nhất: là giá bán thấp nhất của một giao dịch trong khoảng thời gian diễn ra phiên giao dịch, cụ thể là từ thời điểm T đến thời điểm $T + P$.

- Lượng giao dịch: tổng giá trị USD được dùng để mua/bán BTC trong một phiên giao dịch.

- Trung bình giao dịch: giá trị USD trung bình của tất cả các giao dịch diễn ra trong khoảng thời gian một phiên giao dịch.

3.2.2 Rate of Change

Đại lượng đo sự khác nhau của giá tại phiên thứ x so với n phiên trước đó. Giá sử $P(x)$ là giá của phiên thứ x thì:

$$ROC_n(x) = \frac{P(x) - P(x-n)}{P(x-n)}$$

Nếu $ROC > 0$ thì giá thị trường đang có xu hướng đi lên (tăng giá). Ngược lại, với $ROC < 0$ thì giá thị trường đang có xu hướng giảm xuống.

3.2.3 Stochastic Oscillator

Đại lượng dùng để đo xu hướng mua/bán của thị trường tại thời điểm phiên x thông qua n phiên trước đó. Giả sử:

L_n = giá phiên thấp nhất trong n phiên
H_n = giá phiên cao nhất trong n phiên
$P(x)$ = giá của ngày x

$$\%K = \frac{P(x) - L_n}{H_n - L_n}$$

Nếu $\%K$ nhỏ hơn 20 thì thị trường đang có xu hướng mua vào và nếu lớn hơn 80 thì thị trường đang có xu hướng bán ra.

3.3 Máy học

3.3.1 Khái niệm cơ bản

3.3.1.1 Máy học

Máy học có hai cách định nghĩa chính và đang được chấp nhận phổ biến:

- Theo Arthur Samuel: *"Là một lĩnh vực nghiên cứu mà nó cung cấp cho máy tính khả năng học hỏi mà không cần lập trình một cách tường minh."*

- Theo Tom Mitchell: *"Một chương trình máy tính được chấp nhận là học hỏi được kinh nghiệm E bằng cách thực hiện một vài tác vụ T theo phép đo hiệu năng P, nếu và chỉ nếu việc thực thi các tác vụ trong T được đo bởi phép đo P đem lại kết quả là kinh nghiệm E được cải thiện."*

3.3.1.2 Học có giám sát - Supervised Learning

Chúng ta được cho một tập dữ liệu đã biết với các đầu vào và đầu ra tương ứng nhau. Ý tưởng là chúng ta sẽ đi tìm mối quan hệ giữa đầu vào và đầu ra, đó chính là học có giám sát.

Vấn đề của học có giám sát được phân loại thành hai vấn đề chính là hồi quy - regression và phân lớp - classification. Trong vấn đề hồi quy, chúng ta sẽ cố gắng dự đoán kết quả đầu ra tiếp theo một cách liên tục, nghĩa là chúng ta đi tìm ra một hàm đầu ra liên tục tổng quát với biến là các đặc trưng đầu vào. Còn với vấn đề phân lớp, chúng ta thay vì cố gắng dự đoán kết quả liên tục thì ta sẽ đi dự đoán chúng theo hướng rời rạc, hiểu theo một cách khác là chúng ta đi tìm một phép phân loại rời rạc cho các biến đầu ra với các biến đầu vào.

3.3.1.3 Học không giám sát - Unsupervised Learning

Học không giám sát cho phép chúng ta tiếp cận các vấn đề mà ta chưa hề hoặc biết rất ít kết quả của chúng ta sẽ trông như thế nào. Chúng ta có thể xây dựng cấu trúc của dữ liệu mà không cần thiết phải biết mối quan hệ của các biến đó.

Chúng ta thực hiện việc này dựa trên ý tưởng gom cụm dữ liệu bằng cách xem xét mối quan hệ giữa các đặc trưng của dữ liệu. Các hướng tiếp cận dựa trên nhưng phương pháp như vậy thường được gọi là gom cụm - clustering.

3.3.2 Thông số đánh giá

Có ba tham số cơ bản dùng để xem xét và đánh giá giải thuật trong Máy học. Gọi:

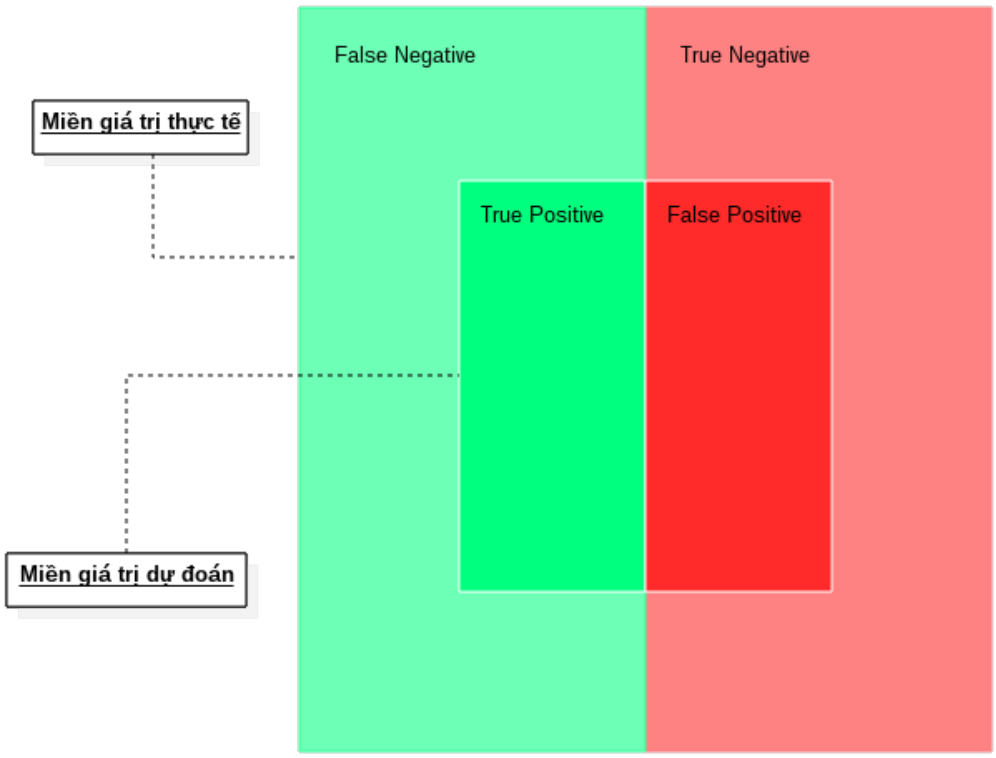
- True positive là TP
- False positive là FP
- True negative là TN
- False negative là FN

Thì:

$$Accuracy = \frac{TP + TN}{TP + FP + TN + FN}$$

$$Precision = \frac{TP}{TP + FP}$$

$$Recall = \frac{TP}{TP + FN}$$



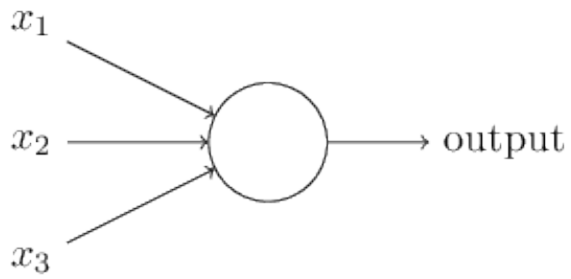
Hình 3.6: Thông số đánh giá

3.3.3 Mạng neural - Neural Network

Học sâu - Deep Learning - là một nhánh của Máy học, đại diện cho hướng tiếp cận gần với cái nhìn thực tế, học nhiều cấp và học từ bản chất dữ liệu. Học sâu thường giải quyết rất tốt với các loại dữ liệu mang tính "con người" như hình ảnh, âm thanh ... Để có được những tính chất này, Học sâu đã đưa ra các giải thuật mạng neural với cấu tạo nhiều lớp, mỗi lớp lại được cấu tạo từ nhiều phần tử nhỏ hơn. Mỗi phần tử bên trong đi giải quyết các phép toán rất đơn giản, nhưng khi được ghép nối lại thành một mạng neural hoàn chỉnh chúng có thể giải quyết các bài toán phức tạp hơn rất nhiều, điều này hoàn toàn tương tự với các hoạt động của bộ não người. [7]

3.3.3.1 Cấu trúc một Perceptron

Một perceptron sẽ có các input $x_1, x_2, ...$ và output sẽ là một giá trị nhị phân.



Hình 3.7: Perceptron

Một ví dụ đơn giản dựa vào hình trên, ta thấy perceptron này có 3 input là x_1, x_2, x_3 , giả sử đi kèm với mỗi input sẽ có một giá trị trọng số w_1, w_2, w_3. Output được định nghĩa là 0 và 1, nhận giá trị 0 khi $\sum_j w_j x_j$ nhỏ hơn giá trị ngưỡng và 1 khi lớn gơn giá trị ngưỡng.

Biểu diễn đại số:

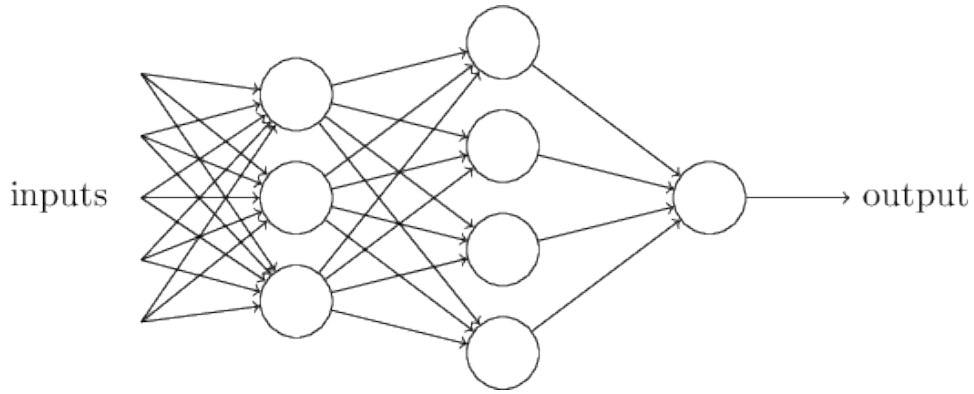
$$output = \begin{cases} 1 & if \ \sum_j w_j x_j > threshold \\ \\ 0 & if \ \sum_j w_j x_j \leq threshold \end{cases}$$

Các hàm số như trên được gọi là activation function, có nhiều loại activation function khác nhau như: $sigmoid, tang...$

3.3.3.2 Multilayer Neural Network

Hiển nhiên, một perceptron không thể mô phỏng nên được một bộ não người, để có thể đưa ra một quyết định tương tự như bộ não người các perceptron này cần được kết nối với nhau thành một mạng lưới - Multilayer Neural Network.

Multilayer Neural Network được cấu thành bằng cách sắp xếp các perceptron thành từng lớp. Các perceptron ở mỗi lớp sẽ kết nối với tất cả các perceptron ở các lớp liền kề, cột những perceptron đầu tiên được gọi là input layer, chúng có chức năng tiếp nhận các input để cho ra các output. Các output ở lớp trước sẽ chính là input cho các perceptron ở lớp tiếp theo. Các perceptron ở lớp cuối cùng được gọi là output layer, trong trường hợp này đặc biệt chỉ có duy nhất một perceptron. Còn lại các lớp perceptron khác được gọi là hidden layer.

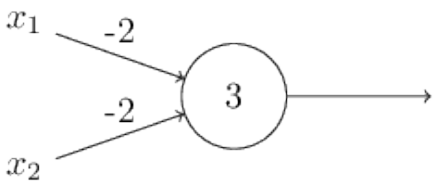


Hình 3.8: MNN

Giả sử input của perceptron là $x_1, x_2, ...$ tương ứng là đó là các trọng số $w_1, w_2, ...$ Thêm vào đó định nghĩa về bias, ở đây bias là một giá trị đại diện độ lệch của từng perceptron và được ký hiệu $b_1, b_2, ...$ Ta có biểu diễn của activation function:

$$output = \begin{cases} 1 & if \sum_j w_j x_j + b_i > 1 \\ 0 & if \sum_j w_j x_j + b_i \leq 0 \end{cases}$$

Ví dụ:



Hình 3.9: Ví dụ perceptron với giá trị bias

Ta có $w_1 = w_2 = -2$ và $b = 3$, khi đó nếu input $x_1 = 1, x_2 = 0$ suy ra $w_1 * x_1 + w_2 * x_2 + b = (-2) * 1 + (-2) * 0 + 3 = 1$, ta có thể chọn $threshold = 0$ vì $1 > 0$ nên $output = 1$.

3.3.3.3 Sigmoid Function - Hàm Sigmoid

Với dạng activation function được định nghĩa ở trên, giá trị của activation function gần như không có giới hạn. Vậy tại sao việc không có giới hạn lại cần được quan tâm. Trong một trường hợp cụ thể, với việc sử dụng activation function như trên có thể dẫn đến trường hợp đầu ra của một perceptron sẽ nhận giá trị rất lớn - giả sử là 1000, những một perceptron khác sẽ nhận giá trị rất bé - giả sử 0.001. Vì thế khi đến lớp tiếp theo thì gần như perceptron

cho kết quả đầu ra là giá trị bé sẽ mất đi độ ảnh hưởng và làm mất cân đối cho toàn mạng.

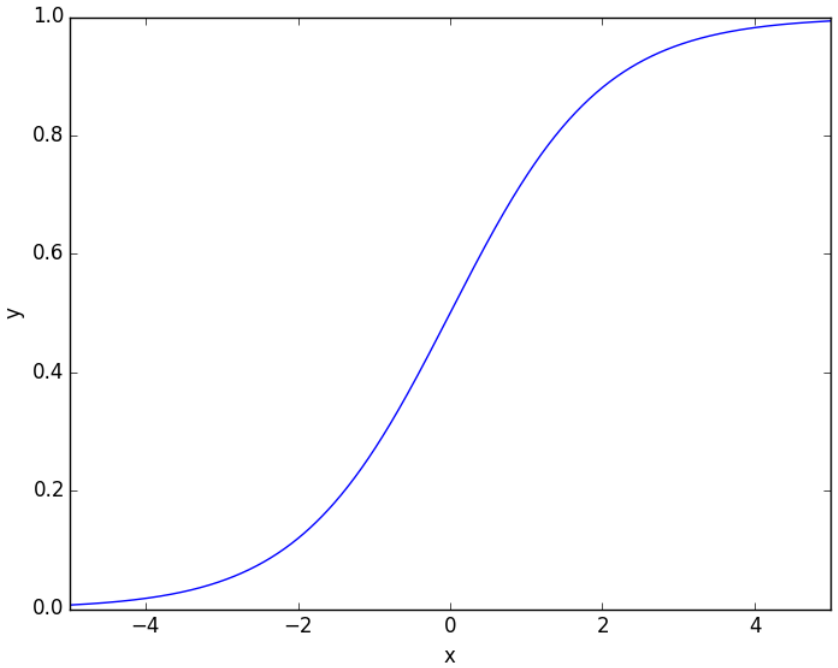
Do đó để giới hạn giá trị của activation function chúng ta sẽ sử dụng hàm sigmoid. Sigmoid function được định nghĩa như sau:

$$\sigma(z) = \frac{1}{1 + e^{-z}}$$

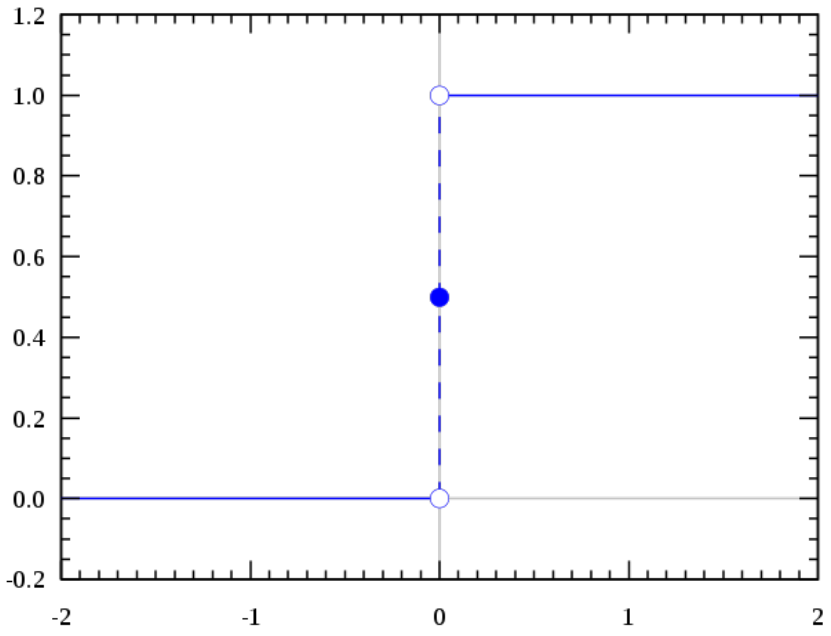
Áp dụng Sigmoid function vào activation function ta có activation function dạng sigmoid và khi đó activation function của chúng ta sẽ có dạng:

$$\frac{1}{1 + exp(-\sum_j w_j x_j - b)}$$

Lúc này ta có một activation function có giá trị được giới hạn trong khoảng từ 0 đến 1. Nhưng chú ý, giá trị của activation function là liên tục, để rời rạc hóa giá trị của activation function ta có thể sử dụng một phương pháp quen thuộc - sử dụng threshold. Điển hình ta chọn threshold = 0.5, nếu lớn hơn thì activation function sẽ nhận 1 và ngược lại sẽ nhận 0.



Hình 3.10: Đồ thị hàm sigmoid



Hình 3.11: Đồ thị rời rác hóa hàm sigmoid

3.3.3.4 Giải thuật lan truyền ngược

Sau khi đã có xây dựng thành công một mô hình Multilayer Neural Network, công việc cuối cùng là cung cấp khả năng tự học hỏi từ đó để bản thân mạng có thể tự xây dựng mô hình và đưa ra các quyết định cụ thể.

Cụ thể, khi nhìn lại một Multilayer Neural Network với activation function là sigmoid function thì các tham sô w, b là chưa biết và việc cung cấp khả năng tự học hỏi chính là cung cấp một giải thuật giúp mạng tìm được các tham số w, b với một tập kinh nghiệm - hay tập huấn luyện - x, y cụ thể, trong đó x là input và y là output tương ứng với từng bộ x. Giải thuật lan truyền ngược là một trong nhưng giải thuật chúng ta cần tìm.

Trước tiên chúng ta cần đi qua một số ký hiệu:

- w là vector của các giá trị trọng số

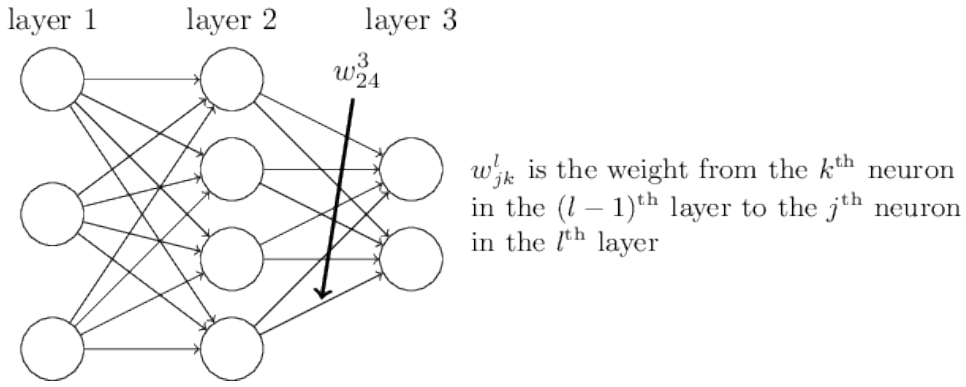
$$w = \begin{bmatrix} w_1 \\ \vdots \\ w_n \end{bmatrix}$$

- b là vector của các giá trị bias

$$b = \begin{bmatrix} b_1 \\ \vdots \\ b_m \end{bmatrix}$$

- σ là sigmoid function
- $a(\sigma)$ là activation function có dạng sigmoid

Biểu diễn activation function:



Hình 3.12: Weight Notation example

Ví dụ như hình trên, trọng số xuất phát từ perceptron thứ 4 thuộc layer thứ 2 và kết thúc tại perceptron thứ 2 thuộc layer thứ 3 được ký hiệu là w^3_{24}.

Tương tự như vậy với bias và activation function của perceptron thứ j thuộc layer thứ l của mạng sẽ được kí hiệu thứ tự là b^ℓ_j, a^ℓ_j. Ví dụ, bias của perceptron thứ 3 thuộc layer thứ 2 sẽ là b^2_3 và activation function của perceptron thứ 1 thuộc layer thứ 3 sẽ là a^3_1.

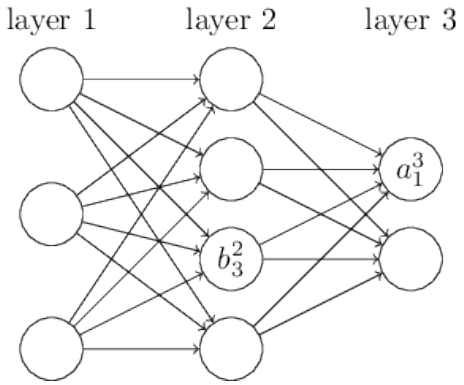
Lúc này ta có biểu diễn toán học đầy đủ của activation function:

$$a^\ell_j = \sigma(\sum_k w^\ell_{jk} a^{\ell-1}_k + b^\ell_j)$$

Với ký hiệu vector ta có thể tổng quát phát biểu với dạng:

$$a^\ell = \sigma(w^\ell a^{\ell-1} + b^\ell)$$

Cost function: Trước khi đi vào hiểu được giải thuật lan truyền ngược có thể làm gì, chúng ta cần phải biết một định nghĩa cost function. Vậy cost function là gì? Đúng theo tên của hàm, nó dùng để đo lường chi phí của



Hình 3.13: Bias Notation example

thuật toán. Chi tiết:

$$C = \frac{1}{2n} \sum_x \|y(x) - a^L(x)\|^2$$

Ta có thể thấy, dạng hàm số trên hết sức quen thuộc với định nghĩa độ lệch chuẩn trong xác suất thống kê nhưng đã được biến đổi một chút. Thay vì giá trị kỳ vọng và các điểm xác suất, cost function sử dụng giá trị thực tế y của tập dữ liệu và giá trị $y = a$ là giá trị y tính toán được từ x với w và b. Vậy ta có thể hiểu được, cost function tính toán độ sai lệch của giá trị a so với y kỳ vọng thực tế. Do đó, cost function càng nhỏ thì biểu diễn giá trị của MNN sẽ càng gần với thực tế.

Để tìm được giá trị cực tiểu cho cost function ta sẽ thực hiện vòng lặp:

$$w_{ij}^{(\ell)} := w_{ij}^{(\ell)} - \eta \frac{\sigma}{\sigma w_{ij}^{(\ell)}} C(w, b)$$

$$b_i^{(\ell)} := b_i^{(\ell)} - \eta \frac{\sigma}{\sigma b_i^{(\ell)}} C(w, b)$$

Trong đó η là tỉ lệ học - learning rate, việc hội tụ về giá trị cực tiểu với tốc độ và độ chính xác phụ thuộc vào tỉ lệ này.

Vậy, đi qua một quá trình tìm hiểu về MNN, ta có thể hiểu được việc học hỏi kinh nghiệm của mạng cốt lõi vẫn là việc tìm ra bộ w và b tương ứng với x, y của bộ dữ liệu luyện tập, và để tìm ra được w và b ta có thể sử dụng giải thuật lan truyền ngược.

Chương 4

Phân tích và thiết kế hệ thống

4.1 Xây dựng Multilayer Neural Network

4.1.1 Feature Selection - Dữ liệu luyện tập

Một trong những yếu tố hết sức quan trọng trong Máy học đó chính Feature. Feature chính là các giá trị thuộc tính đại diện cho tập dữ liệu luyện tập, ví dụ chúng ta có tập dữ liệu về loài chim thì có thể feature chính là các thông số về độ dài sải cánh, màu lông, vùng sinh sống... Một giải thuật có thể học được "kinh nghiệm" nhanh hay chậm, chính xác hay sai lệch phụ thuộc rất nhiều vào yếu tố feature. Vì vậy quá trình khai phá dữ liệu là hết sức cần chú ý.

Tập dữ liệu về các phiên giao dịch Bitcoin được thu thập từ ngày 20/2/2015 đến ngày 29/10/2016 và có tổng cộng 29634 phiên giao dịch.

Gọi S là đại diện cho một phiên giao dịch, các feature được xây dựng như sau:

- 10 feature RDP: $\{\ loop\{RDP_1(S_{i+j})\}_i\ \}_j$ Với $i \in [0:9]$, $j \in [0:29634]$
- 1 feature SO. Với $j \in [0:29625]$:

$$\{\%K_j = \frac{P(j+9) - L_{10}}{H_{10} - L_{10}}\}_j$$

- 1 feature ROC. Với $j \in [9:29634]$:

$$\{ROC_{10}(j) = \frac{P(j) - P(j-9)}{P(j-9)}\}_j$$

Ở đây, ta đã chủ ý chọn mỗi feature vector được hình thành bởi 10 phiên giao dịch. Các giá trị SO và ROC đều được tính trong thời gian là 10 phiên

giao dịch. Sau khi đã có feature, ta cần label để phân lớp tập luện tập. Ở đây đơn giản, nếu giá Bitcoin ở phiên thứ 11 lớn hơn phiên thứ 10 thì label sẽ là 1, ngược lại sẽ là 0. (Phiên 11 chính là phiên thứ 1 của nhóm 10 phiên liền sau nhóm 10 phiên hiện đang xét).

$$label_i = \begin{cases} 1 & if\ P_i(10) > P_{i+1}(1) \\ 0 & if\ P_i(10) \leq P_{i+1}(1) \end{cases}$$

4.1.2 Training - Học giải thuật

Bên cạnh chạy giải thuật Multilayer Neural Network, chúng ta sẽ chạy các giải thuật khác nhằm so sánh và đánh giá giải thuật chính.

Các giải thuật được chọn chạy:

- Multilayer Neural Network - MNN
- Support Vector Machine - SVM
- K-Nearest Neighbors - KNN
- Logistic Regression - LR

Sau khi chạy xong ta ghi nhận kết quả của các giải thuật được đề cập dưới dạng các tham số đánh giá sau:

- Accuracy
- Recall
- Precision

4.1.3 Validation - Đánh giá giải thuật

Để có được kết quả đánh giá, chúng ta sẽ chia tập dữ liệu ra hai phần:

- Training data: chiếm 7/10 tổng số dữ liệu, dùng để chạy trong quá trình học của giải thuật.
- Validation data: chiếm 3/10 tổng số dữ liệu, dùng để chạy trong quá trình đánh giá giải thuật.

	KNN	LR	SVM	MNN
Accuracy	62.93%	66.24%	66.40%	69.86%
Precision	44.69%	18.18%	0%	60.50%
Recall	43.62%	0.15%	0%	29.55%

Bảng 4.1: Bảng đánh giá

Kết quả chạy giải thuật:

Trước tiên theo bảng đánh giá, ta có các giải thuật LR và SVM cho kết quả Accuracy là gần khoảng 66%, nhưng khi nhìn và chi tiết các giá trị Precision và Recall ta nhận thấy các giải thuật này hầu như chỉ dự đoán kết quả là Down cho tất cả trường hợp. Điều này hoàn toàn không có ý nghĩa để dự đoán đầu tư.

Xét đến KNN và MNN, đối với KNN ta có thể thấy giải thuật có xu hướng cân bằng các giá trị Accuracy, Precision và Recall. Nhưng đối với MNN, giải thuật có xu hướng tối ưu hóa Accuracy và Precision. Vậy câu hỏi đặt ra ở đây là kết quả nào có giá trị đầu tư hơn?

Chú ý đến Recall, dựa theo định nghĩa thì Recall có thể hiểu nếu trong thực tế có 10 phiên là Up thì KNN sẽ dự đoán đúng khoảng 4 lần và MNN sẽ dự đoán đúng khoảng 3 lần. Nhìn thoáng qua có vẻ như Recall cao thì sẽ có ý nghĩa trong việc đầu tư hơn, nhưng hay khoan kết luận.

Xét đến Precision, ta có thể hiểu Precision là, với 10 lần dự đoán sẽ có phiên Up thì KNN sẽ đúng khoảng 4 lần và MNN sẽ dự đoán đúng 6 lần. Giả sử, mức độ tin tưởng của chúng ta vào hệ thống là 100%, cứ mỗi lần hệ thống dự đoán có phiên Up thì ta sẽ bỏ tiền đầu tư. Điều đó đồng nghĩa, nếu theo KNN sẽ có 6 lần ta chịu lỗ vì hệ thống dự đoán sai và với MNN thì ta sẽ có 4 lần ta chịu lỗ.

Quay lại với Recall, giá trị này không đo đạt được việc chúng ta sẽ lợi nhuận hoặc thua lỗ ra sao mà thực ra là giá trị đo đạt khả năng tận dụng cơ hội của hệ thống.

Tới lúc này, ta có thể kết luận, bộ giá trị chiếm ưu tiên cao hơn sẽ là Accuracy và Precision. Điều đó cũng có nghĩa là giải thuật Multilayer Neural Network nên là lựa chọn để tiếp cận giải quyết vấn đề này.

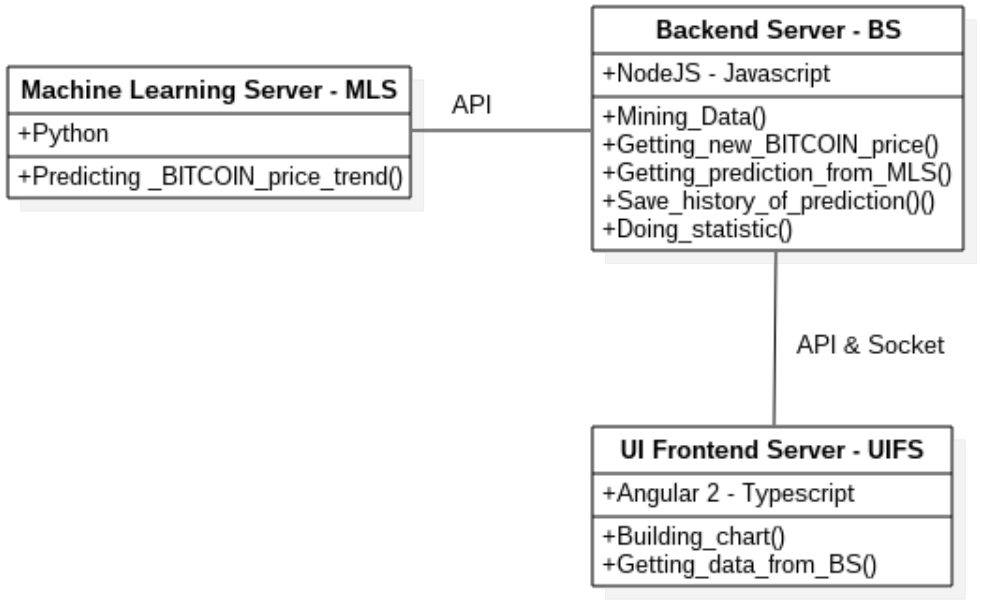
4.2 Xây dựng hệ thống - Web Application

4.2.1 Tổng quan hệ thống

Hệ thống được xem xét và được thiết kế với 3 khối server chức năng:

- Hệ thống Machine Learning server
- Hệ thống Backend server
- Hệ thống UI Frontend server

Các khối hệ thống giao tiếp với nhau bằng API và Socket - đối với các chức năng realtime.



Hình 4.1: System Structure

4.2.2 Hệ thống Machine Learning Server

Đây là hệ thống cốt lõi của của sản phẩm, nó đảm nhiệm khối chức năng dựa vào các tham số được truyền vào để đưa ra giá trị nhãn tương ứng cho bộ tham số đó.

Cụ thể, để đưa ra một dự đoán, hệ thống yêu cầu các tham số đầu vào

phải được xây dựng theo mô tả của Feature Selection - 12 features.

Trong hệ thống Machine Learning Server, được chia nhỏ thành hai phần:

1. Prediction: bao gồm các chức năng đọc mô hình Multilayer Neural Network đã xây dựng, chạy mô hình với tham số truyền vào và lấy các kết quả đầu ra. Kết quả đầu ra có giá trị nhãn Up-Down và xác suất dự đoán.
2. Django: bao gồm các chức năng để hình thành một API server ví dụ như tiếp nhận các yêu cầu thông qua API, phản hồi các yêu cầu...

Vì tính chất hỗ trợ tốt cho Máy học nên Python được lựa chọn là ngôn ngữ để phát triển hệ thống này.

4.2.3 Hệ thống Backend Server

Vì bản thân hệ thống Machine Learning Server không có các khối chức năng liên quan đến việc lấy dữ liệu giá Bitcoin cũng như khai phá dữ liệu nên hệ thống Backend Server được xây dựng để thực hiện các chức năng này. Đồng thời, Backend Server còn là cầu nối giữa trải nghiệm người dùng (hệ thống UI Frontend Server) và hệ thống Machine Learning Server.

Để thực hiện được công việc trên, hệ thống bao gồm được xây dựng các chức năng:

1. Cập nhật giá Bitcoin: thông qua các public API được các sàn giao dịch Bitcoin cung cấp, các hàm lấy giá được chạy liên tục để cập nhật giá Bitcoin mới nhất nhằm phục vụ cho quá trình dự đoán.
2. Khai phá dữ liệu: dữ liệu được các hàm cập nhật giá Bitcoin lấy được vẫn còn ở dạng thô, chưa qua xử lý. Khai phá dữ liệu là biến đổi các dữ liệu này về các bộ tham số có ý nghĩa với Máy học, các giá trị này mới đích thực dùng để làm đầu vào dự đoán xu hướng giá trị Bitcoin.
3. Giao tiếp với hệ thống Machine Learning Server: truyền tham số đi và nhận kết quả trả về từ hệ thống Machine Learning Server thông qua API.
4. Lưu trữ và thống kê dữ liệu: thực hiện việc lưu trữ dữ liệu, từ đó tạo nên một hệ thống các dữ liệu phục vụ cho việc phân tích, thống kê để cung cấp cho người dùng đầu cuối. Đó là các thông tin hết sức quý giá phục vụ cho các nhà đầu tư.

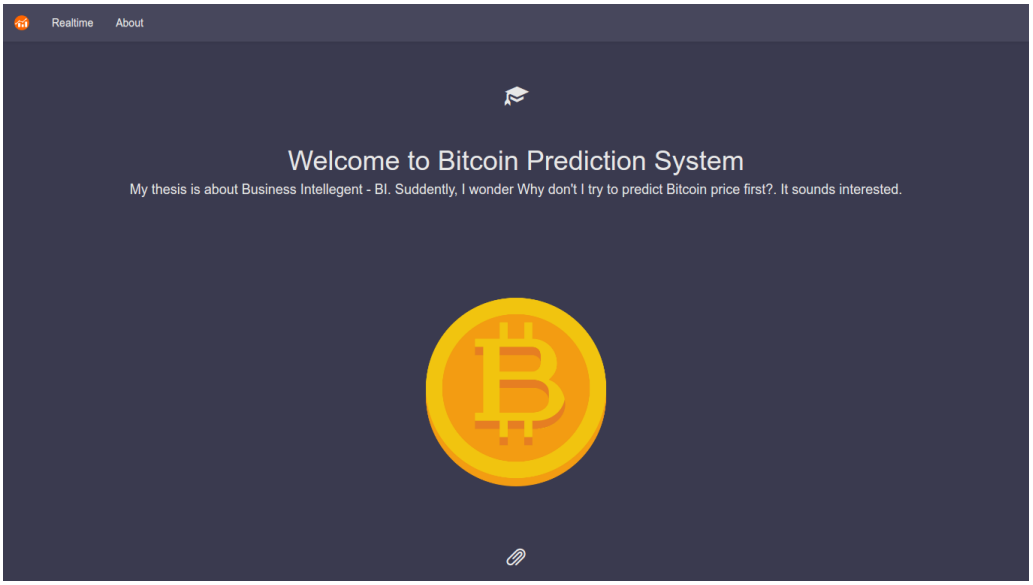
5. Giao tiếp với hệ thống UI Frontend Server: đưa ra những API chức năng nhằm phục vụ cho UI Frontend Server. Ví dụ như: yêu cầu dữ liệu dự đoán, yêu cầu thống kê đúng/sai, yêu cầu dữ liệu giá cho biểu đồ...

Với khả năng xử lý nhanh, được hỗ trợ tốt nên NodeJS được dùng để phát triển hệ thống. Đồng thời, cơ sở dữ liệu của hệ thống là MongoDB vì tính linh hoạt trong cấu trúc dữ liệu và khả năng mở rộng cao.

4.2.4 Hệ thống UI Frontend Server

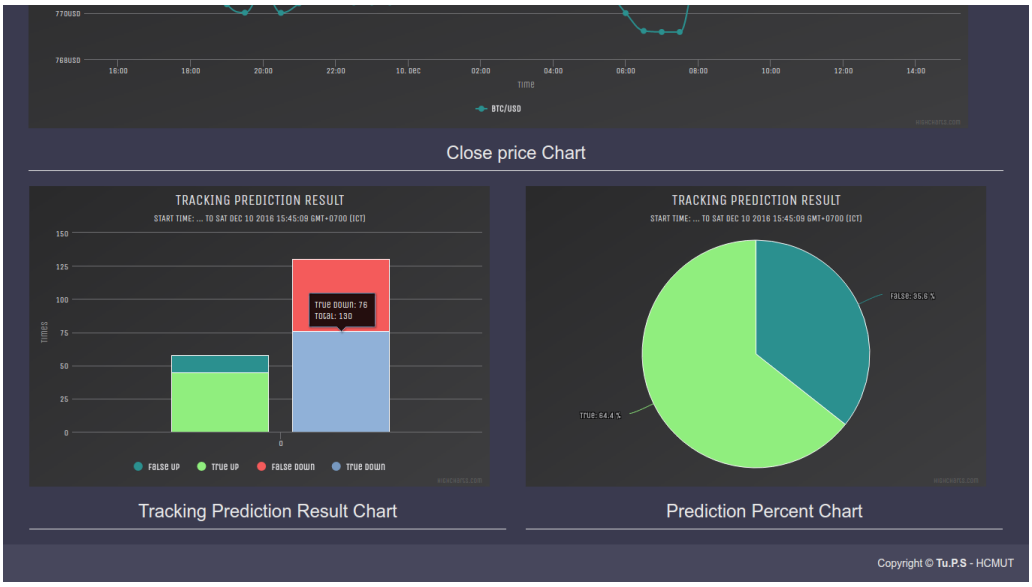
Hệ thống UI Frontend Server là một giao diện người dùng, nó cho phép người dùng có thể tiếp cận với các chức năng của toàn bộ hệ thống một cách dễ dàng. Hệ thống bao gồm nhiều biểu đồ, cũng như tham số cung cấp các thông tin có ý nghĩa đầu tư - dự đoán xu hướng giá trị Bitcoin - đồng thời với đó, là các thông tin về độ tin cậy của hệ thống, các thống kê về lịch sử dự đoán...

Một số hình ảnh về hệ thống thực tế.



Hình 4.2: UI Frontend Server 1

Hình 4.3: UI Frontend Server 2



Hình 4.4: UI Frontend Server 3

Hệ thống UI Frontend Server được xây dựng theo xu hướng one-page, cũng chính vì vậy mà Angular 2 là lựa chọn phù hợp, với khả năng phát triển nhanh, hỗ trợ tốt từ các bên thứ 3.

Chương 5

Kết luận và hướng phát triển

5.1 Kết luận

Kết thúc đề tài, sản phẩm cuối cùng được hoàn thiện là một công cụ nền Web hỗ trợ, cung cấp các thông tin có giá trị tham khảo để đầu tư Bitcoin. Dựa trên các con số lý thuyết, khả năng dự đoán chính xác là rất khả quan và đặc biệt, giải thuật được tối ưu cho phù hợp với góc nhìn của một người đầu tư.

Với không nhiều sai lệch khi so sánh bên cạnh các con số lý thuyết, khi hệ thống được cho chạy thực tế trong vòng 4 ngày liên tiếp (Cụ thể từ 22:30:00 13/11/2016 đến 20:30:00 17/11/2016) đã cho ra kết quả:

Accuracy	Precision	Recall
64.4%	77.6%	45.5%

Bảng 5.1: Bảng đánh giá hệ thống thực tế

Các tham số đánh giá chạy thực tế như vậy, có thể thấy với một lần đầu tư ta có tới hơn 70% là có lợi nhuận. Tuy vậy, bất kỳ một hệ thống cũng vẫn sẽ có những điểm thiếu sót.

Vì giới hạn của thời gian thực hiện đề tài, phạm vi của đề tài cũng được thu hẹp để phù hợp nên vì thế đã bỏ qua một số yếu tố thị trường ảnh hưởng khá lớn đối với hướng giải quyết. Trong lúc này, bản thân có thể nhận ra hai vấn đề:

- Phí giao dịch: ở tất cả các sàn giao dịch, đều có một khoảng phí trung gian từ 0.1% đến 0.3% và phí này được trừ trực tiếp vào các giao dịch. Hướng tiếp cận của đề tài bỏ qua hoàn toàn yếu tố này và có thể hiểu là phí bằng 0%

- Biên độ lợi nhuận và thua lỗ: chúng ta cũng đã bỏ qua yếu tố này, mặc dù dựa theo đánh giá thì số lần đầu tư lợi nhuận sẽ nhiều hơn thua lỗ. Nhưng, chúng ta không thể kết luận việc đầu tư sẽ chắc chắn đem về lợi nhuận. Hãy nói đến một trường hợp xấu, biên độ lợi nhuận chỉ có $1 cho mỗi lần nhưng biên độ thua lô lại là $100, tại đây chúng ta có thể thấy là việc đầu tư không hề có lợi.

Việc nhìn nhận được các vấn đề trên không hẳn là điều tồi tệ, mà ngược lại giúp chúng ta có thể hiểu rõ bài toán và đưa ra những hướng phát triển tiếp theo.

5.2 Hướng phát triển

Với các vấn đề còn tồn tại được nêu ra bên trên (Mục 5.1), giai đoạn tiếp theo của đề tài là đi giải quyết vẫn đề tài như hiện giờ nhưng thêm vào đó là yếu tố phí giao dịch. Tuy là một yếu tố nhỏ nhưng nó dẫn đến việc thay đổi hoàn toàn bộ dữ liệu ban đầu, điều này đồng nghĩa toàn bộ hệ thống hiện giờ sẽ không tương thích. Vì thế, cần thực hiện lại quá trình xây dựng giải thuật từ đầu.

Mặc khác, việc chỉ học duy nhất từ tập dữ liệu về giá Bitcoin là không đủ để đưa ra một dự đoán chính xác cao. Ngày nay, mạng xã hội đang phát triển như vũ bão, đây là một kênh thông tin cực kỳ quý giá, chính vì vậy mà hệ thống ở giai đoạn phát triển tiếp theo sự tận dụng tài nguyên này.

Phát triển hệ thống xử lý ngôn ngữ tự nhiên, xây dựng hệ thống lắng nghe các thông tin tài chính, chính trị có ảnh hưởng tới giá trị Bitcoin, phân tích, đánh giá và cho cân bằng với hệ thống học từ dữ liệu giá Bitcoin để cho ra một dự đoán tổng quát và chính xác hơn.

Đồng thời, hệ thống có thể mở rộng ra cho nhiều cryptocurrency khác như Ethereum, Zcash, Monero...

Tài liệu tham khảo

[1] https://vi.wikipedia.org/wiki/Bitcoin. *Wikipedia - BITCOIN*. Trích dẫn vào tháng 11/2016

[2] Satoshi Nakamoto. *Bitcoin: A Peer-to-Peer Electronic Cash System*.

[3] Megan Potoski. *Predicting Gold Prices*. CS229, Autumn 2013

[4] Yuqing Dai & Yuning Zhang. *Machine Learning in Stock Price Trend Forecasting*. 2013

[5] Andrew Ng. *Lecture Notes – CS229 Machine Learning*. 2012

[6] Andrew Ng. *Section Notes – CS229 Machine Learning*. 2012

[7] Michael Nielsen. *Neural Networks and Deep Learning - Free Online Book*. Jan 2016