Periodicals of Engineering and Natural Sciences ISSN 2303-4521
Vol. 8, No. 3, September 2020, pp.1911-1923

Decentralized security and data integrity of blockchain using deep learning techniques

Sazeen Taha Abdulrazzaq[1], Farooq Safauldeen Omar[2], Maral A. Mustafa[3]
[1, 2] Kirkuk Technical Collage, Northern Technical University
[3] Kirkuk Technical Institute, Northern Technical University

ABSTRACT

Since the introduction of blockchain, cryptocurrencies have become very attractive as an alternative digital payment method and a highly speculative investment. With the rise in computational power and the growth of available data, the artificial intelligence concept of deep neural networks had a surge of popularity over the last years as well. With the introduction of the long short-term memory (LSTM) architecture, neural networks became more efficient in understanding long-term dependencies in data such as time series. In this research paper, we combine these two topics, by using LSTM networks to make a prognosis of decentralized blockchain security. In particular, we test if LSTM based neural networks can produce profitable trading signals for different blockchains. We experiment with different preprocessing techniques and different targets, both for security regression and trading signal classification. We evaluate LSTM based networks. As data for training we use historical security data in one-minute intervals from August 2019 to August 2020. We measure the performance of the models via back testing, where we simulate trading on historic data not used for training based on the model's predictions. We analyze that performance and compare it with the buy and hold strategy. The simulation is carried out on bullish, bearish and stagnating time periods. In the evaluation, we find the best performing target and pinpoint two preprocessing combinations that are most suitable for this task. We conclude that the CNN LSTM hybrid is capable of profitably forecasting trading signals for securing blockchain, outperforming the buy and hold strategy by roughly 30%, while the performance was better. The LTSM method used by current system for encrypting passwords is efficient enough to mitigate modern attacks like man in the middle attack (MITM) and DDOS attack with 95.85% accuracy

Keywords: Blockchain, throughput, deep learning, LTSM, security, bitcoin, DDOS, MITM.

Corresponding Author:

Sazeen Taha Abdulrazzaq
Kirkuk Technical Collage,
Northern Technical University, Kirkuk, Iraq
E-mail: sazeentaha4@ntu.edu.iq

1. Introduction

Deep neural networks are a subset of artificial intelligence and their concept is also commonly referred to as deep learning. The core idea behind neural networks was inspired by the brain and has been around for decades. Due to improved learning methods, increasing computational power and large datasets, deep learning has risen in popularity over the last years and is a field of high interest in today's computer science [1]. Neural networks have had success in solving very complex tasks, long thought to be out of reach for computers, e.g. speech recognition [2], image/video classification, automated translation, text generation, self-driving cars [3] and many more. A very notable accomplishment for neural networks was when the technology company Google introduced a system called Duplex at their developer conference Google I/O in 2018 as mentioned in [4]. Duplex can allegedly make phone calls to book appointments or reservations with no human input necessary, having a natural sounding voice as well as using and understanding nuances of the English language. In the future, many more applications are conceivable and deep learning might replace call centers for providing automated support, assist in elderly care, aid during surgeries and so on. Another IT topic which has been receiving an increasing amount of attention since 2008 is everything related to the blockchain technology [5]. While a blockchain is merely a cryptographically hashed, linked list, it creates possibilities for various applications. One of the many concepts arising from it are decentralized applications and smart contracts [6], agreements that are cryptographically enforced and therefore eliminating the need for notaries, first proposed in [7].

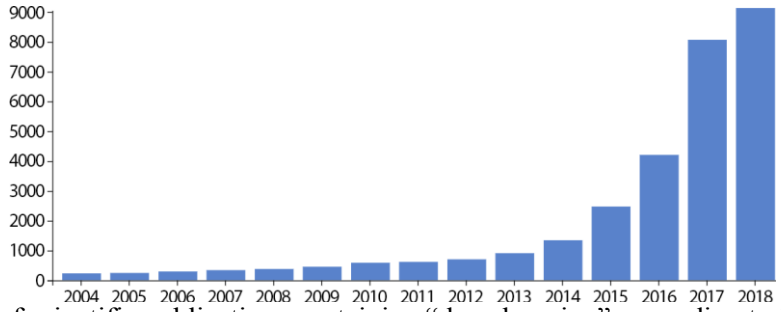

Figure 1. Number of scientific publications containing "deep learning", according to *Web of Science* [7]

However, one of the first and arguably the most popular use of blockchains was for cryptocurrencies, namely in Bitcoin as a public and tamper-proof ledger containing all transactions [8]. Cryptocurrencies have attracted many investors and have increased their market capitalization to over 100 billion US dollars. Aside from being a cryptographically tamper-proof form of digital payment, cryptocurrencies have several other advantages over conventional fiat currencies, such as not relying on a trusted third party for carrying out transactions or being able to transfer money using pseudonyms as mentioned in [9]. Bitcoin and other cryptocurrencies are traded on exchanges for one another or for fiat currencies like US dollars. The security fluctuation for cryptocurrencies is generally rather high. It is not clear, where this volatility stems from, which factors influence the security in what way and if it is possible to predict these fluctuations. Analyzing the security of cryptocurrencies using deep neural networks is an interesting way to combine aspects of both these topics, to investigate the performance of neural networks in that domain and to find out if the security of cryptocurrencies can be predicted and to what extent.

1.1. Problem statement

Blockchain technology can be used to authenticate, authorize, and audit data generated by devices. Also, the need to trust in the third party is eliminated due to its decentralized nature which cannot be altered by the unauthorized user. Blockchain ensures adequate security and protection for IoT systems with its distributed nature through the cryptographic processes it uses with vulnerabilities like DDOS and Man in the Middle attacks. Moreover, the hashing algorithm built upon blockchains provides it with the opportunity to create a reliable sensitive IoT application operating without many dependencies on environmental trust. The convergence of blockchain technology and IoT is on the agenda for many firms in different sectors, and there are already projects, solutions, and ideas in countless possible artificial intelligence (AI) applications, including smart city, smart cars, smart grid, smart health, supply chain, and digital identity management and in some other applications yet to be pronounced. In a blockchain network, every single block that follows the other must be changed in order to make a change to a single block as they are all connected and the next block contains information about the previous block and it continues like that in a chain. And even if all the subsequent blocks following the altered block were changed, verification would still fail, because it will be recorded in blocks that the subsequent copies of the chain had tampered with it.

1.2. Aim of study

The main objective of this thesis is to survey researches related to security of deep learning based systems with Blockchain. The term 'security' if the question is put out to public opinion, enterprises might say revenues, consumers might say utility, but interoperability, security, compliance, privacy, and reliability are major barriers to industrial growth. Our proposed system provides support for the development of advanced applications for easy use but, if the security measures are not adequately put into effect, it may result to life threatening attacks, issues such as individuals subjected to physical attacks such as robbery or kidnapping may as a result of the breach of the smart alarm and other devices connected to the network.

- Is it possible to forecast the security of blockchains with respect to different types of attacks (i.e. DDOS, Man in the Middle) based on historic security data and if yes, to what extent?
- Are data integrity strategies based on these predictions or secure trading signals able to generate profit, perform better as the security development or both? How does this performance vary in different market situations?

- Are the securities of blockchain/cryptocurrencies influencing one another? i.e. does the decentralized blockchain security influence the centralized blockchain security?
- The decentralized access control system provides transparency and equality among the participating organizations.
- It enables the immutability of data to prevent manipulation, modification, falsification, and deletion of blockchain with different cryptocurrencies.
- Does LTSM neural networks perform better than CNN?

We create range of solution for firms and individuals, not least the potential for data sabotage, malfunctions and device hijack. By storing data on a distributed network, the it eliminates the risks that come with data being held centrally in a data farm, Blockchain makes use of powerful SHA256 encryption and generates a secret key only known to the user, this secret key is then used to sign transaction which will be attached to a public key.

2. Background

Professional investors as well as banks that invest a lot of money in managers for managed funds, market analysis and so on make it apparent that there are at least numerous people that believe in being able to outperform the market. Analyzing the stock market over the years has resulted in finding several anomalies. An example for such an anomaly is the January effect, an effect where stock security performs better in January compared to other months [10]. This effect is sometimes attributed to selling one's assets at the end of the year and rebuying them at the beginning of the new year for tax purposes. Aside from occurring at a certain point in time, anomalies can also appear based on the historic security (e.g. momentum effect) or the company fundamental data (e.g. earnings-security anomaly). The momentum effect is the observation that increasing (decreasing) stock security tend to continue to increase (decrease) [10]. The earnings-security anomaly is the observation that the stocks of companies with a smaller security/earnings ratio tend to perform better than others [11]. Finally, large speculative bubbles followed by market crashes stem from over-/undervalued stock security.

The existence of professional investors like Warren Buffet who consistently outperform the market over long periods of time is obviously not disputed. According to theories like the EMH, these successes should not be possible over the long term. Furthermore, banks that invested more in any form of market analysis or algorithmic trading should be at a major disadvantage. Algorithmic trading utilizes pre-defined rules based largely on historic security and volume [12] and should therefore not be able to outperform the market according to the EMH. Yet the effort in algorithmic trading is so high, that in 2012 algorithmic trading accounted for 85% of the volume according to researcher in [12]. Another claim is, that people acting based on common stock analysis strategies generate a situation where a prediction becomes a self-fulfilling prophecy.

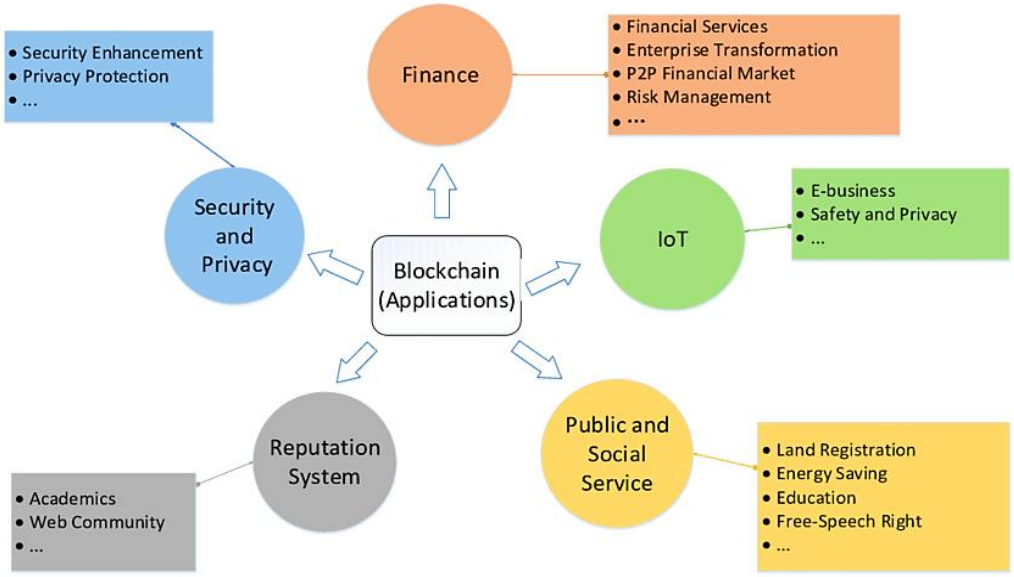

Figure 2. The up to date global usage and representative application domains of blockchain [13]

Cryptocurrencies are a form of digital asset that is secured by means of cryptography and are usually decentralized, meaning they do not rely on a trusted third party for transactions like banks or credit card companies. Instead they handle transactions in a public ledger, for example a blockchain. They generally have no intrinsic value, but are exchanged for fiat currencies like US dollars, Japanese yen or euros based on supply and demand. The security fluctuates substantially. The following subsections will go over the fundamentals of cryptocurrencies using Bitcoin as example, some alternative cryptocurrencies (Altcoins) and the characteristics of trading cryptocurrencies.

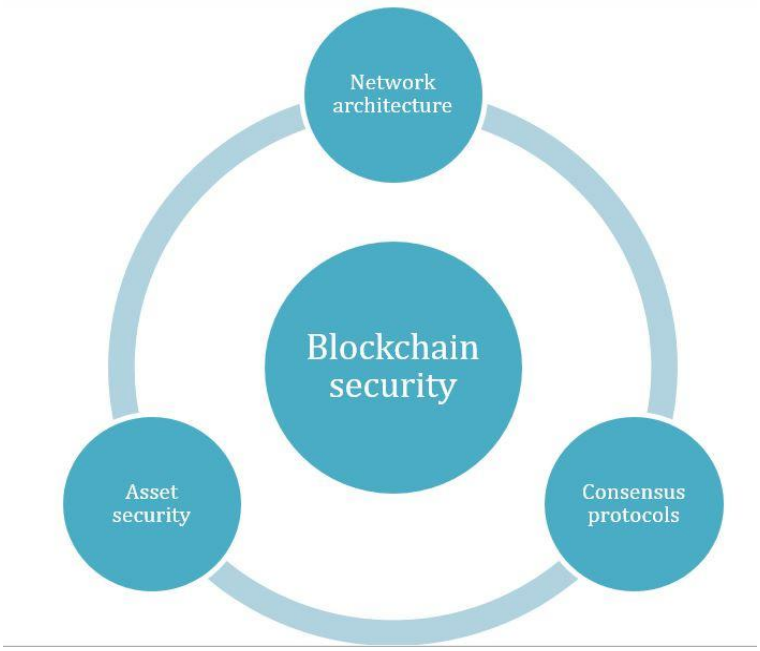

Figure 3. The legality and security factors of blockchain technology [14]

Bitcoin's popularity has increased over the last years. Its value in USD, while having been volatile from the beginning, rose steadily from a few cents until reaching its peak of almost 20,000 US dollars for one Bitcoin in December 2017. From then it dropped to around 3,500 US dollars as of January 2019. Bitcoins can be traded for traditional currencies on Bitcoin exchanges. Because of this popularity and the relatively high trading volume, there have been many exchanges for Bitcoin over the years. Some of these exchanges were allegedly associated to illegal activities and shut down, the most prominent case being by researchers in [15]. This as well as Bitcoin being used for payments at numerous illegal darknet sites brought some negative publicity.

Bitcoin also has some inherent flaws. One of the problems is scalability. The blockchain's size surpassed 200 GB of size in early 2019 and will grow steadily. The size of blocks is limited and only about 4,000 transactions fit into one block. Because a block is mined every 10 minutes, this means that only around 7 transactions can be handled per second on average, a rather small number compared to for instance credit card systems as mentioned in [15]. This can result in very long waiting times or high fees in the Bitcoin system when carrying out transactions. Finally, as mentioned briefly above, Bitcoin is not completely anonymous, only pseudonymous. There are ways of tying different Bitcoin addresses together (hashes of public keys) that belong to the same person. Because there generally has to be some sort of interface to conventional money, usually via exchanges, there are points where personal information could be leaked. At the very least these exchanges have to be regarded as trusted third parties, something that Bitcoin's goal was to avoid. If one's information gets linked with a Bitcoin address (or all of that persons Bitcoin addresses), every purchase ever made is visible in the (public) blockchain.

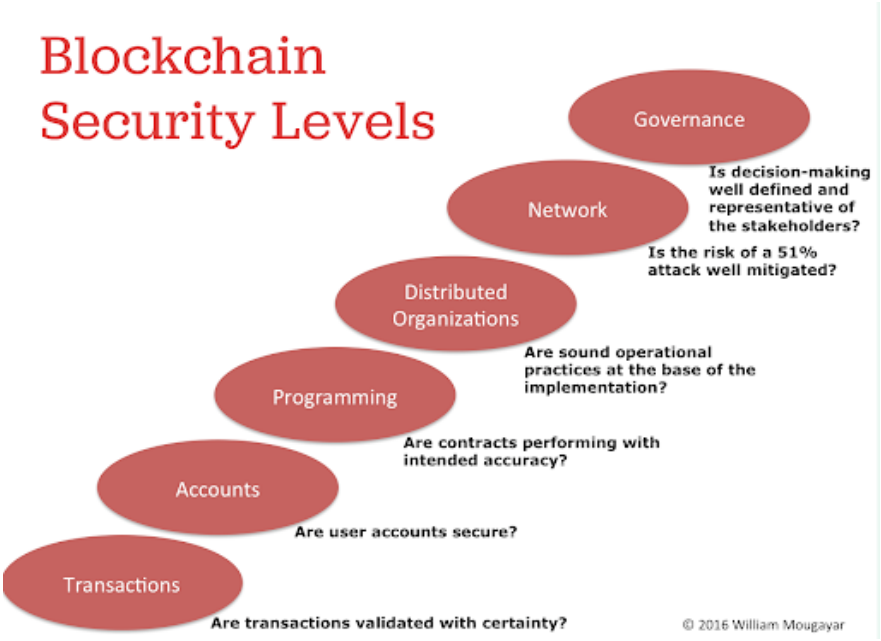

Figure 4. The six multi-layer security levels of blockchain for certain transection [16]

Implementing changes into Blockchain is difficult, because the users have to agree and update their client. Otherwise a fork occurs, i.e. the cryptocurrency splits into two new ones, one that accepted the changes and one that did not. This happened for instance when Bitcoin split into Blockchain and Blockchain Cash. Due to this criticism and the difficulties faced when implementing changes into the Blockchain protocol, along with the immense hype around cryptocurrencies in general, many alternative cryptocurrencies (altcoins) have emerged over the years. Some of them will be presented in the next section.

3. Methodology

The blockchain is network of incorruptible digital ledger of information exchange which does not store only history of financial transactions like in Blockchain which its popularly known for, but capable of storing everything of value. To a layman, blockchain is a giant collection of public records which cannot be erased, deleted or edited. As there exist no central computer or device on which the entire chain is saved making it a distributed and decentralized network. Rather, each block nodes involved in transactions keeps a copy of the transactions and the data of the previous are saved in the new blocks continuously. Data records are continuously added to the chain, which made it ever-growing.

A major element that constitute blockchain are:
• Transactions: These are the actions initiated by each participating nodes in the system.
• Blocks: These are the recorded transactions, they are arranged in sequence and are in their original form. The block also record timestamp of when the transactions were added.

Blockchain application is numerous, which include cryptocurrency, smart contracts, music, real estate, fraud detection, identity, internet of things etc. In this research, we will be looking into the application of Blockchain to the security of internet of things. A recent idea that has to do with our newly adopted technology: Internet-of-Things is being powered by blockchain. Spending on the IoT market keeps growing and it is predicted to reach about $1 Trillion mark in few years. Blockchain-Internet-of-Things convergence have the opportunity to provide the paramount mechanism to monitor the billions of smart-devices coming online histories over the coming years by making use of its incorruptible permanent ledger.

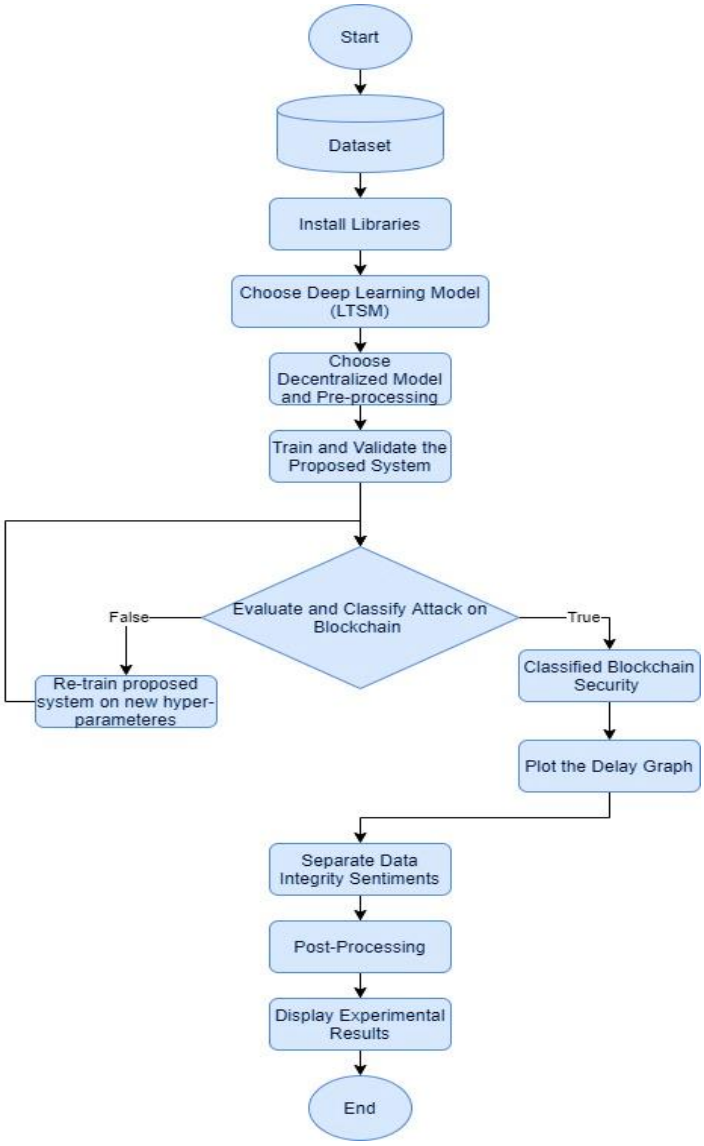

Figure 5. Flow diagram of approach being followed

Confidentiality, Integrity, and Availability are the major requirements needed to be addressed by any security design, to ensure that only authorized user to have access to data, to ensure transfer and delivery of data when needed without it being altered. This approach effectively secures the devices in the blockchain by ensuring that they cannot be reached directly but rather, all transactions have to pass through a third party device called miner which authorize all transaction before forwarding them to the devices. Although there is an increase in transaction delay compared to the existing smart home gateway products, these delays occur as a result of authenticating the user, generating a shared key, matching of keys etc. but this delay doesn't have a negative impact on the availability of the device.

Table 1. Security Requirements Evaluation

Requirements	**Actions**
Confidentiality	Achieved by using symmetric encryption.
Integrity	Hashing the shared keys is used to achieve integrity.
Availability	Limiting the number of transaction accepted by the devices and the miner will help in achieving this.
User Control	Accomplished by saving data's in the blockchain.
Authorization	The usage of policy header and shared keys.

3.1. Decentralized Security Model with Types

A decentralized approach to blockchain will substantively reduce the cost of installation and maintenance of large centrally located data farms and allocate computational and storage requirement to other billions of devices which IoT network is made up of, by adopting homogenize peer-to-peer communication model in the processing the billions of information that passes through various devices. With this approach, a halt or fault in a node will not bring the whole network down as transactions are recorded on every participating node. The use case we will be surveying for this research is the smart home how to use blockchain technology to improve its security. It was seen in previous findings that about 54% more people leaves in bigger cities while about 46%them leaves in rural areas, and by 2050 this number is projected to further increase by about 66%, this will in turn have an impact on the growth of blockchain technology.

Figure 6. The mapping data privacy difference between various blockchain technologies [17]

3.1.1. Man-in-the-Middle Attack in Blockchain

This attack endangers privacy. It can be a dangerous attack because when the attacker secretly intercepts data ledgers with the same public keys, they are made to believe that the communication is going on directly between devices whereas, the attacker is already compromising by revealing the ID of the user. To curtail this type of attack, a unique key is used to store each data, the miner generates a unique ledger of data for each of the device and stored on the cloud using the different public key. A unique key is used by a miner for each transaction.

3.1.2. DDOS Attack in Blockchain

Our approach has multiple layers of defense, the first makes it difficult for a hacker to install a malware directly on devices since it can't be accessed directly as all transaction has to pass through the miner. Another layer of defense is for instance if the attacker breaks the first and managed to infect the devices. All outgoing traffic will need to be examined by the policy header for authorization and since the DDOS attack request will not be authorized by the miner, there would be no exit on the blockchain network.

3.2. Training Decentralized Secure Blockchain Model

The models were trained on 95% of the data, while the rest of the data was used for validation and simulation. The training was carried out in 10 epochs each, the trained model after every epoch was saved with total 50 epochs. Every saved model was then used to simulate trading on the validation data, i.e. the remaining 5% of the data. The model provides a trading decision for every minute of the test data. It is assumed that every trading decision is carried out without delay at market security, i.e. the current closing security. For every trade, a fee of 0.075% is deducted from the simulation value. The models might perform differently depending on the market situation of the testing data, i.e. its performance differs in a period where the blockchain security is rising rapidly (bullish) compared to when the security is dropping (bearish) or stays more or less the same (stagnating). To make the results more conclusive, the experiments were carried out three times. Of the historic security data, three different 5% regions or sectors are selected. The security progression of along with these sectors. All of the three different 5% data sectors were used as validation data, while the remaining 95% of the data was used for training. In sector one the security stays more or less the same (-8%). In the second sector, the security drops to about 45% and in the third the security increases to 186%. In every sector the same combinations are separately trained and tested.

Based on our requirements, we ended up choosing Keras with TensorFlow as backend for our deep learning framework. Therefore, Python is the programming language of our choice and we selected the rest of the

technologies to fit. For preprocessing we use scikit-learn, which is a Python package for deep learning. For other tasks we chose appropriate Python packages. The following technologies were used to build the prognosis tool:

- Python 3.7.6 as programming language.
- TensorFlow 1.12 GPU (with Keras) to build and train the neural networks, using CUDA 9 and cuDNN 7 for hardware acceleration.
- Scikit-learn, a python package for data preprocessing.
- pandas, a python package for data representation and handling.
- Several other python packages such as numpy, joblib, requests, websockets and asyncio for tasks such as fetching the historical data from Binance's public API.

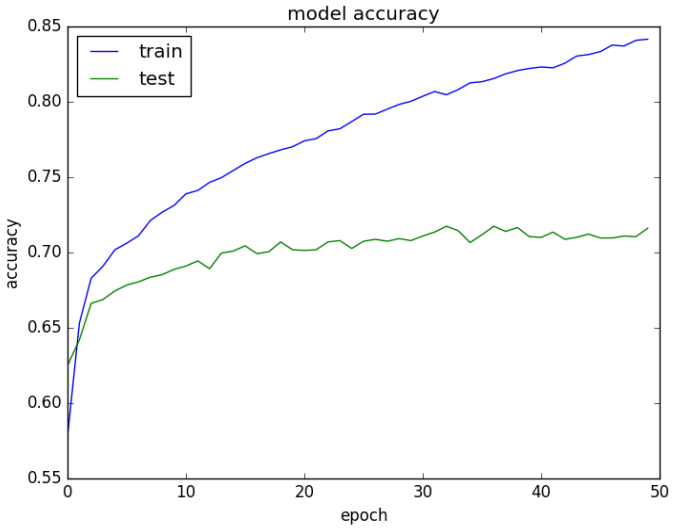

Figure 7. The system being trained on 50 epochs using LTSM

3.3. LTSM Based Neural Network Model

To measure the performance of different neural network models, an important requirement for the software tool is to make the creation of new neural networks and their integration with the different targets and preprocessing techniques simple and straightforward. To achieve this, the output layer is dynamically adapted depending on the used target. The regression targets have one output node, while the classification targets have two output nodes for the binary target or three output nodes for the best strategy target.

Three models are then created for further evaluation. All of them are LSTM-based neural networks, with one of them being a mixture of LSTM and CNN. The networks all have dropout after the LSTM layer to prevent overfitting. After the LSTM and dropout layer there is a batch normalization layer, which normalizes the data within batches to speed up training. After these layers, there is one dense (or fully connected) layer followed by an output layer.

A *time window (*or *sequence length*) of 200 was chosen. The inputs are fed in batches of 64. The activation function of the LSTM is the *tanh* function. For the output layer a linear (for regression targets) or a softmax (for classification targets) activation function is used.

- The first neural network model used is a rather basic one. It consists of one LSTM layer with 128 units, followed by a dropout layer and a batch normalization layer. Afterwards there is a dense layer with 32 nodes and a rectifier activation function as well as an output layer with one, two or three nodes, depending on the target. The second and the third model expand on this architecture.
- The second neural network consists of an LSTM layer with 128 units, with dropout and batch normalization repeated three times. This is followed by a dense layer with 32 nodes and a rectifier activation function and the output layer.
- The third model adds a one-dimensional convolution layer with kernel size 3 and a rectifier activation function. This is followed by a one-dimensional max pooling layer with a pooling size of 4. After this, the model consists of an LSTM layer with 128 units, dropout and batch normalization. Finally, there is a

dense layer with 64 units and a *leaky* rectifier activation function ($f(x) = \max(x, 0.001x)$) and the output layer.

There is no definitive best neural network architecture for a problem, nor are there final rules for constructing one. The models are usually created intuitively and by experimenting. We created the first model to be a minimalist LSTM network. Based on this model, we created several others, each altering one aspect, such as the number of layers, adding convolution, changing the number of nodes, etc. We did some brief testing on these models and selected two of them (model 2 and 3) for further evaluation.

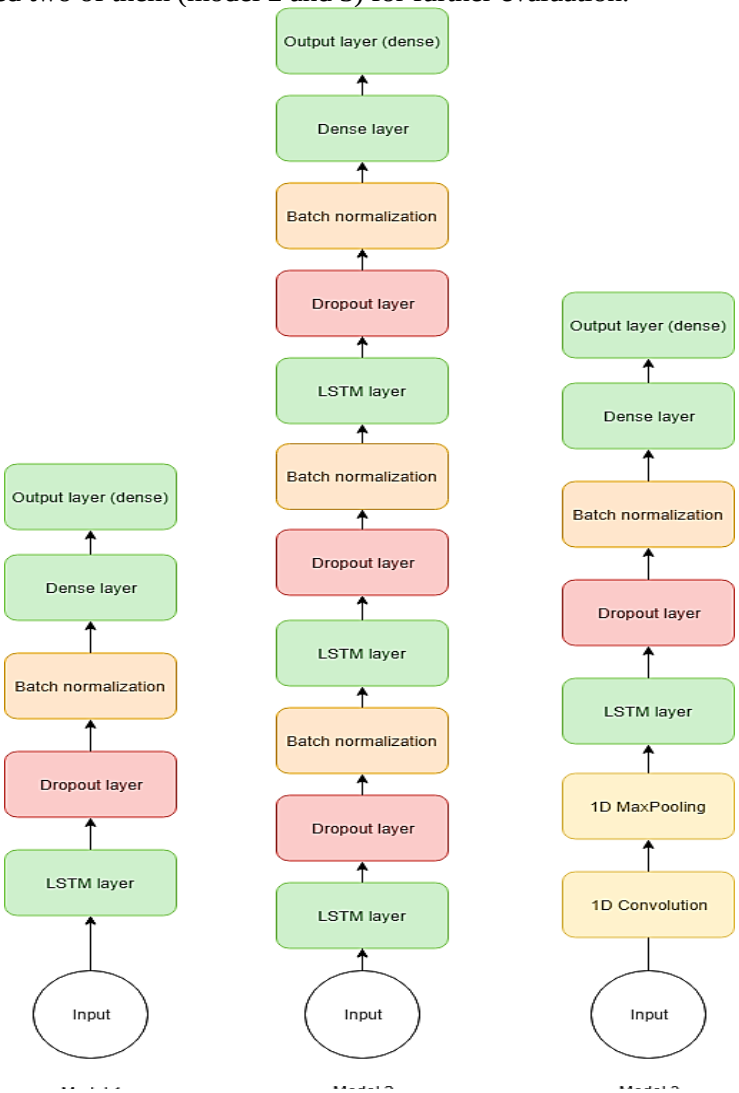

Figure 8. Architecture of the three different models used

These models are trained using the supplied, preprocessed data on a target. As a cost function, the mean squared error (MSE) is used in regression and the categorical cross entropy for classification. The training happens through backpropagation using an optimization algorithm called Adam. This method keeps an adaptive learning rate for every weight and is an improvement over conventional gradient descent.
Only a certain amount of the data is used for training, in our case 95%. The rest is used for validation and simulation. The neural networks are trained for 10 epochs or more. The idea is to save the weights of the model after every epoch. This is useful for reconstructing the models at any training stage later on and to evaluate the performance of every processing step.

4. Results

Due to its decentralized nature, blockchain integrity have been tested and implemented upon bitcoin and its gaining fast reputation in the IoT ecosystem. blockchain major building block is its distributed ledger and public key encryption which is promising in the deep learning sector for data monitoring. Deep learning based

secure underlying architecture was discussed, its growth and impact on the society, damages that could be caused when not appropriately used, the need to improve its security, and investment of different sectors into blockchain security was also looked in. It is resulted that blockchain due to its integrity and its incorruptible ledger mechanism will adequately ensure safety against attack on secure systems. The hashing algorithm used by current system for encrypting passwords isn't efficient enough to mitigate modern attacks, as not only user authentication should be required to have access, control data and transaction involved in the interoperability of various connected devices but also the transactions should be assigned a public key that will be signed and authorized with a secret key known only to the user and get verified before access and control will be granted.

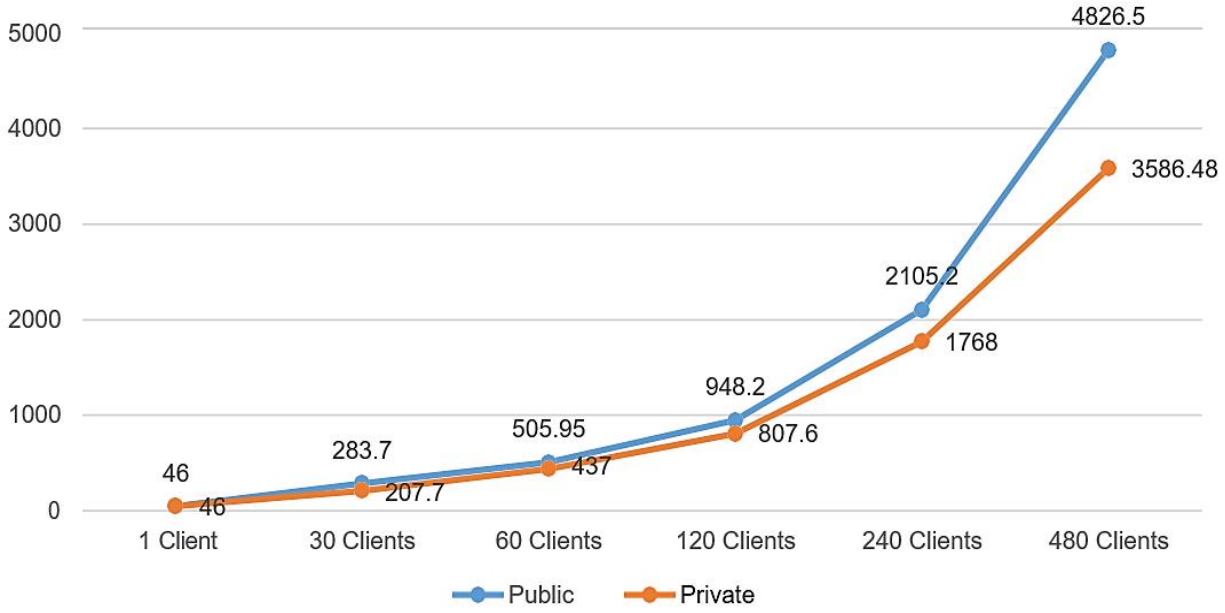

Figure 9. The prediction ratio of *Man in the Middle* (MITM) attack on public and private blockchain servers with several number of clients maintaining their data integrity

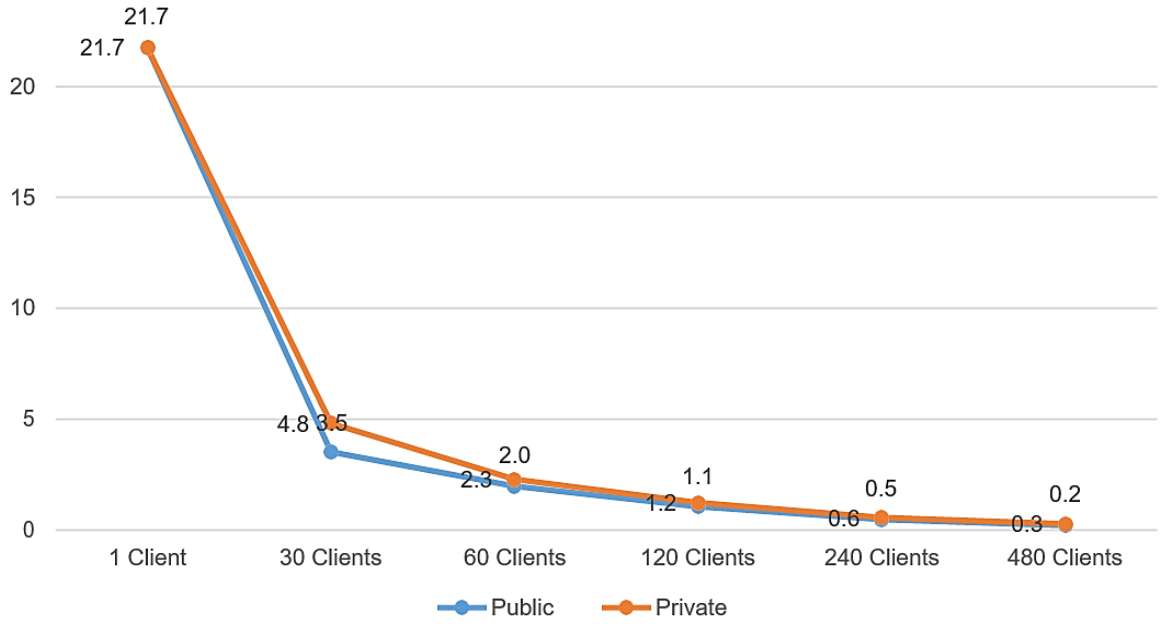

Figure 10. Decentralized security blockchain throughput with no delay on public and private blockchain servers for *man in the middle* (MITM) attack

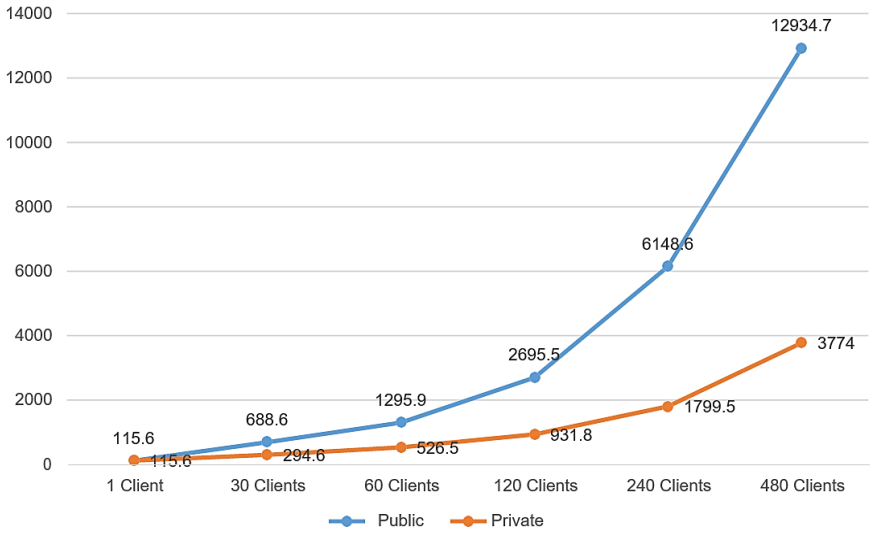

Figure 11. The prediction ratio of *DDOS* attack on public and private blockchain servers with several number of clients maintaining their data integrity.

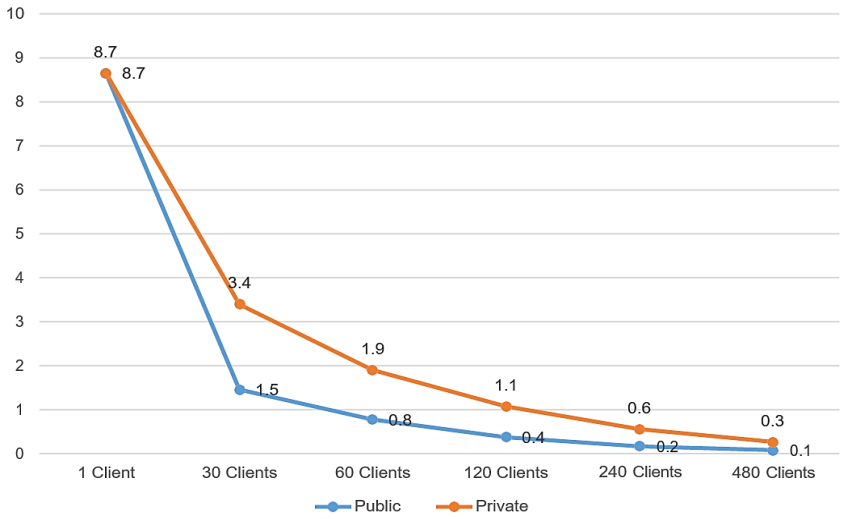

Figure 12. Decentralized security blockchain throughput with no delay on public and private blockchain servers for *DDOS* attack

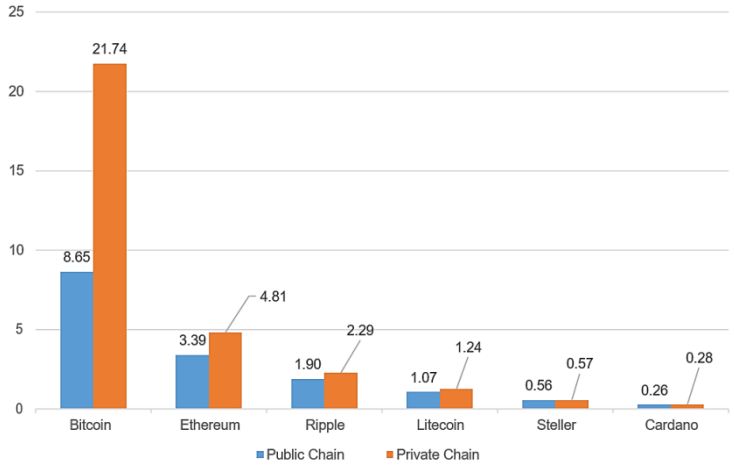

Figure 13. The overall blockchain security throughput on different cryptocurrencies being evaluated on public and private blockchain servers maintain data integrity

5. Discussion

Sources relevant to this research objective were gathered from the various platforms. After searching with various keywords, the terms securing deep learning based blockchain search string was one of our preferred keywords, another possible search string would have been blockchain, but we needed more than information on just blockchain, how it can be used to ensure integrity should be considered. Even though, blockchain part of the search term, various pre-researched documents that were similar to usually to cryptocurrencies economic topics were majority of the search results, instead of findings that are similar to the technical area of blockchain technology.
Hence, the objective of the used methodology was to search and analyses similar researches to the technical aspects of blockchain technology and more importantly how it can be utilized in securing blockchain systems, we decided to drop the single term blockchain. It is believed that by making use of the search string blockchain and deep learning, most of the research materials that considers the working perspective on blockchain were brought forward. Also, it looks like when a Bitcoin-related research material omits the term blockchain and LTSM method within its meta-data, the material will likely be about the cryptocurrency economic aspect of it.

6. Conclusion

Due to its decentralized nature, blockchain integrity have been tested and implemented upon bitcoin and its gaining fast reputation in the deep learning ecosystem. Blockchain major building block is its distributed ledger and public key encryption which is promising in the artificial intelligence and deep learning sector for data monitoring and data integrity. LTSM underlying architecture was discussed, its growth and impact on the society, damages that could be caused when not appropriately used, the need to improve its security, and investment of different sectors into blockchain security was also looked in. It is concluded that blockchain due to its integrity and its incorruptible ledger mechanism will adequately ensure safety against attack on blockchain systems. The LTSM method used by current system for encrypting passwords is efficient enough to mitigate modern attacks like man in the middle attack (MITM) and DDOS attack with 95.85% accuracy, as only user authentication should be required to have access, control data and transaction involved in the interoperability of various connected devices but also the transactions should be assigned a public key that will be signed and authorized with a secret key known only to the user and get verified before access and control will be granted on both public and private blockchain servers with several clients.

References

[1] I. Al-Barazanchi, S. A. Shawkat, M. H. Hameed, and K. S. L. Al-Badri, "Modified RSA-based algorithm: A double secure approach," *Telkomnika (Telecommunication Comput. Electron. Control.*, vol. 17, no. 6, pp. 2818–2825, 2019.
[2] M. Andoni *et al.*, "Blockchain technology in the energy sector: A systematic review of challenges and opportunities," *Renewable and Sustainable Energy Reviews*. 2019.
[3] L. Wu, K. Meng, S. Xu, S. Q. Li, M. Ding, and Y. Suo, "Democratic Centralism: A Hybrid Blockchain Architecture and Its Applications in Energy Internet," *Proc. - 1st IEEE Int. Conf. Energy Internet, ICEI 2017*, pp. 176–181, 2017.
[4] T. ai, X.; Sun, H.; Guo, Q. Electricity transactions and congestion management based on blockchain in energy internet. Power Syst. Technol., 40, 3630–3638, 2016.
[5] Z. hang, N.; Wang, Y.; Kang, C.; Chen, J.; Dawei, H. Blockchain technique in the energy internet: Preliminary research framework and typical applications. Proc. CSEE 2016, 36, 4011–4012, 2016.
[6] N. Z. Aitzhan and D. Svetinovic, "Security and Privacy in Decentralized Energy Trading Through Multi-Signatures, Blockchain and Anonymous Messaging Streams," *IEEE Trans. Dependable Secur. Comput.*, vol. 15, no. 5, pp. 840–852, 2018.
[7] H. R. Abdulshaheed, S. A. Binti, and I. I. Sadiq, "A Review on Smart Solutions Based-On Cloud Computing and Wireless Sensing," *Int. J. Pure Appl. Math.*, vol. 119, no. 18, pp. 461–486, 2018.
[8] Ding, W.; Wang, G.; Xu, A.; Hong, C. Research on key technologies and information security issues of energy blockchain. Proc. CSEE 2018, 38, 1026–1034, 2018.

[9] B. Li, J. Zhang, B. Qi, D. Li, K. Shi, and G. Cui, "Block chain: Supporting technology of demand side resources participating in grid interaction," *Dianli Jianshe/Electric Power Constr*, . 2017, 38, 1–8.
[10] S. Mhanna, G. Verbic, and A. C. Chapman, "Adaptive admm for distributed ac optimal power flow," *IEEE Trans. Power Syst.*, vol. 34, no. 3, pp. 2025–2035, 2019, doi: 10.1109/TPWRS.2018.2886344.
[11] J. He, L. Liu, W. Li, and M. Zhang, "Development and research on integrated protection system based on redundant information analysis," *Prot. Control Mod. Power Syst.*, vol. 1, no. 1, pp. 1–13, 2016.
[12] S. Liu, X. P. Liu, and A. El Saddik, "Denial-of-Service (dos) attacks on load frequency control in smart grids," *2013 IEEE PES Innov. Smart Grid Technol. Conf. ISGT 2013*, no. February 2019, pp. 1–6, 2013.
[13] H. Wang, Z. Zheng, S. Xie, H. N. Dai, and X. Chen, "Blockchain challenges and opportunities: a survey," *Int. J. Web Grid Serv.*, vol. 14, no. 4, p. 352, 2018.
[14] I. A. B. Sawsan Ali Hamid , Rana Alauldeen Abdalrahman , Inam Abdullah Lafta, "Web Services Architecture Model to Support Distributed Systems," *J. SOUTHWEST JIAOTONG Univ. Vol.*, vol. 54, no. December, pp. 52–57, 2019.
[15] G. Liang, J. Zhao, F. Luo, S. R. Weller, and Z. Y. Dong, "A Review of False Data Injection Attacks Against Modern Power Systems," *IEEE Trans. Smart Grid*, vol. 8, no. 4, pp. 1630–1638, 2017.
[16] S. Saberi, M. Kouhizadeh, J. Sarkis, and L. Shen, "Blockchain technology and its relationships to sustainable supply chain management," *Int. J. Prod. Res.*, 2019.