Journal of Information Systems Engineering and Management
2025, 10(9s)
e-ISSN: 2468-4376
https://www.jisem-journal.com/

Research Article

Use of AIML Powered Algorithm to Detect Illicit Activity Inside the Bitcoin Organisation

Jaykrishna Joshi[1] R. P. Sharma[2] Aboo Bakar Khan [3]

[1] *Faculty, Department of Data Science, Mukesh Patel school of Technology Management and Engineering, NMIMS University, Mumbai, 400056,Research Scholar, CSMU,*
Navi Mumbai,Maharashtra, India.
[2,3]*Chhatrapati Shivaji Maharaj University, Navi Mumbai, Maharashtra, India.*

ARTICLE INFO

Received: 26 Oct 2024

Revised: 22 Dec 2024

Accepted: 01 Jan 2025

ABSTRACT

When the technology behind Bitcoin was first revealed in the form of a white paper in 2009 and the corresponding reference implementation was released subsequently. Bitcoin has been accused by critics for pro- viding and shielding a sanctuary to criminal operations. A wide range of illegal means are used by people taking cover behind the sweeping of namelessness (anonymity). Revealing these substances is most crucial point for legal examinations. State-of-the-art techniques use Artificial Intelligence for comparing and identifying these actors but concentrate on a limited number of illegal trades. The ongoing research embarks to resolve the issue by executing a machine-learning enabled auto- mated rule based classification for various types of illegal activities, viz., ponzi schemes, blackmailers, frauds, scams, extortionists, spam- mers, gambling websites, darknet markets, terrorists and sextortionists.

Keywords: Bitcoin, Network Science, Graph Algorithms, Exploratory Data Analysis

INTRODUCTION

Both social and antisocial elements have been drawn to bitcoin[1]. It is social from one point of view since it ensures the exchange of substantial value and maintains confidence without the need for an intermediary. It also makes it more difficult to police questionable interactions because of the confidentiality and security [2-4]. Since the inception of Bitcoin in 2009, the first two years have seen a modest uptake, with less than 1000 addresses and 10,000 daily trades. Serious contenders, including as money laundering organisations[5-6], betting sites, trading platforms, financial sponsors, examiners, and coin mining companies, entered the cryptocurrency industry between 2012 and 2016. The During the second phase of Bitcoin's growth, which began in 2012, Ponzi schemes, tax evasion[7], theft, fraud[8,9], extortion, and other illicit activities increased. These activities took use of the pseudo-anonymity that Bitcoin was managing to trick the review trail. According to estimates, $770 million worth of bitcoins were transferred for illegal purposes[10,11] in 2017, 46% of all bitcoin transactions were illegal, and 25% of bitcoin clients expressed suspicion[12]. A substantial body of research has been done on Bitcoin, analysing how different criminal activities are identified, such as deanonymizing components[13], identifying botnets[14], illegal exchanges[10], identifying suspicious bitcoin clients[15,16], terrorists[17], ponzi schemes[18-20], darknet markets[21], ransomwares[22], human dealers[23], money laundering[24,25], identifying tax evasion[8,26-28], coin mixing[29], bitcoin trades[30,31], illegal exchanges[32,33], identifying bitcoin wallets[34], and identifying bitcoin miners[8,35]. Forensic investigations into Bitcoin have thus far benefited from the application of machine learning.

The present study's primary benefits are:

- extensive data collection and data cleaning for building a dataset
- feature engineered from the database for each bitcoin entity
- application programming interface used for constructing link betweenmultiple bitcoin address to a same bitcoin id

- developing machine learning model by training, validating and testing
- hyper-parameter tuning ad conclusion framing with future scope

A collection of 1216 Bitcoin wallets was extracted from the Blockchain source in order to test the method. To get the model ready to separate 16 distinct licit-illegal client classes, nine features were created. The suggested approach outperformed three current benchmark algorithms during comprehensive numerical testing. The findings indicate that the suggested model's particularity and responsiveness were comparable to those of other models. RAM and computer memory use were also confirmed to show that the suggested work could be applied to actual research.

CONVERSION OF THE RAW DATA OF BITCOIN BLOCKCHAIN TO NETWORK STRUCTURE

The raw data of the Bitcoin blockchain dataset in crude structure was acquired from VJTI Blockchain lab. The size of the dataset was 268GB and comprised of blockchain as blk.data records. This crude information was then converted by preprocessing to comma separated value files by utilizing the blockchain parser worked by the Veermata Jijabai Tecchnological Institute Blockchain lab. Every exchange (tx) is distinguished in blockchain by a one of a kind hash (tx hash: ID) and has a timestamp, which is the UNIX season of the exchange. Considered Exchanges begin on January 3, 2009, at 12:45:05 GMT, and continue through May 10, 2023, at 13:20:00 GMT is analyzed. Bitcoin substances were recognized utilizing an application programming interface (API) [36]. The classes recognized using the API are given below:

- Exchanges (E): these entities allow exchanging of BTC to government issued types of money and are link between BTC users and fiat currencies
- Pools (P): these are organizations or groups or even individuals BTC clients

  join their computational processing power like CPU, GPU for mining blocks
- Gambling (G): these are organizations or groups or even individuals or onlinegaming portals that are related to gambling
- Wallets (W): these are financial instruments that store BTC private keys
- Payment entryways (PG): these are organizations or groups or even indi- viduals that allow payments to be made and accepted in BTCs
- Miner (M): these are organizations or individuals who mine block by finding the correct hash
- Darknet markets (DM): these are selling and purchasing merchandise that cannot be sold on traditional marketplaces utilizing BTCs
- Mixers (MX): combine a user's Bitcoin with those of other users in order to obfuscate the transaction trace
- Trading destinations (T): These represent the buying prices in Bitcoins
- P2Plenders (P2P): Crowdsourcing Bitcoins to provide credits to both small and large business owners
- Faucets (F): these are reward in BTCs to supporters or those perform a

  certain task
- Explorer (E): These educational websites provide an API for examining the history and transactions of Bitcoin
- P2PMarket (P2PM These are marketplaces for recycled goods where buyers may get in touch with sellers and make payments in bitcoins.
- Bond markets (B): these are buying securities or obligation instruments in BTC

- Associate advertisers (AA): paid-to-click in bitcoins
- Video Recording (VR): these are bitcoin based payments for review recording.
- Money launderers (M): these convert government issued types of money to BTC by using off-shore accounts in tax havens

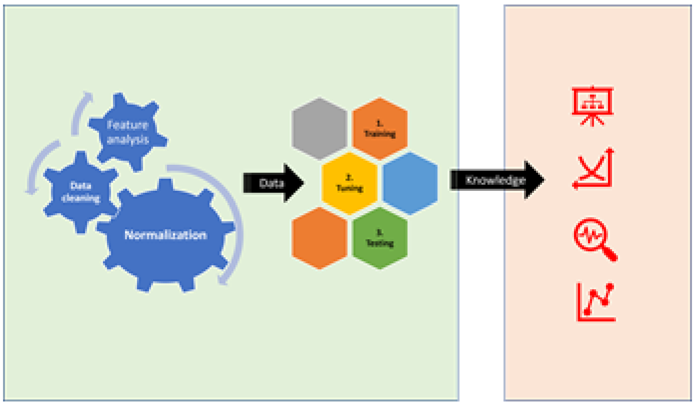


Fig. 1 Parsing through the Bitcoin blockchain dataset

- Cyber-security suppliers (CSP): these provide network safety devices andinfrastructure items for BTC
- Cyber-crooks (CC): these are organizations or groups or even individuals

  blacklisted entities involved in money laundering or terrorism by state runadministrations
- Ponzi (PZ): high yield speculation financial instruments or scams

By parsing through the Bitcoin blockchain dataset (Figure 1), wallet were created by clustering all bitcoin addresses which could belong to a single entity. The heuristic utilized for grouping [37] is based on the principle that all addresses that belong to the same user id [24, 25, 37]. The most important lim-itations are the extensive feature engineering needed for each bitcoin user id. The features need to be engineered from the bitcoin database and calculated before these features can be sent to the machine learning model for prediction.This drawback is however not a serious flaw and is common to machine learn- ing models. With the help of features the model transparents learns the link from response variables to predictors.

1.1 Construction of machine learning-enabled classifier

Tree-based classifiers were seen to have broad use cases contrasted with troupes of other regressors. Random forest is an illustration of this regressor. It shows how each tree in the forest is worked by the stowing approach. Besides, while building the tree hierarchical, the ideal choice rule for every tree to assemble the branches is found either from all feature indicators or an irregular subset of them. The first execution permitted each tree in the forest to decide in favorof a class and utilized the larger part rule for choosing the last expectation. Substitute executions normal the singular trees' forecast for choosing the last expectation.

To combine the individual trees outputs we use one of the following methods, **averaging** the forecast of numerous procedures to get the last expec-tation, **voting** in which the last forecast is concluded in view of the greater part

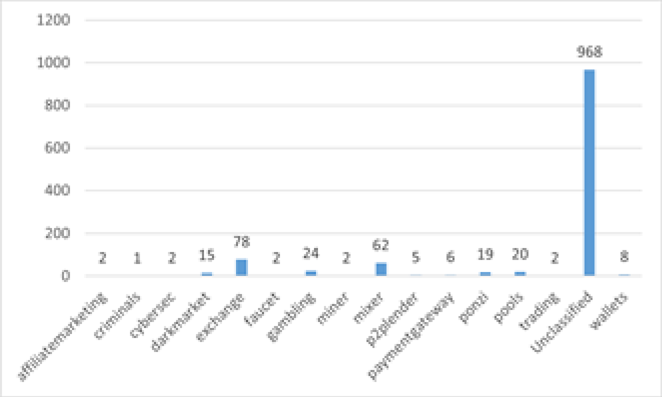


Fig. 2 Bitcoin blockchain-labeled dataset for supervised learning

vote of the various methods, **pasting** in which different models are prepared on randomly chosen tests without substitution in the information, **bagging** where various models are prepared on randomly chosen data-sets drawn with substi- tution from the information, **random sub-spaces** where different models are prepared on arbitrarily chosen features from the information, and **random patches** where numerous models are prepared on randomly chosen features and data without substitution from the information. Thus, multiple estimators are used for learning different aspects of the data-set.

PREDICTION RESULTS

Log loss should be minimized and accuracy, detection rate, kappa and speci- ficity should be maximized in model selection. Figure 3 illustrates specificity and detection rate of the four models - SVM, LogReg, RF with proposed model on the bitcoin dataset.

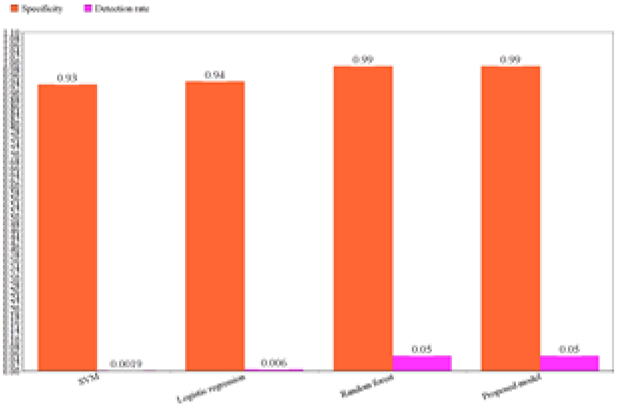


Fig. 3 Training set performance: specificity and detection rate

The specificity and detection rate of the random forest model and proposed model is equal. The other models such as SVM and logistic regression is have nearly equal specificity yet on detection rate they are performing far inferior. Further, the four models were evaluated on their training performance on mul-tiple parameters (Figure 4) - log loss, AUC, prAUC, Accuracy and Kappa. The log loss of random forest and proposed model was better than SVM and logis- tic regression. Similarly, AUC, prAUC, accuracy and kappa were also better for the proposed model compared with SVM and logistic regression. On two parameters, accuracy and kappa the proposed model tied with random forest. The results prove that tree based models were better at learning complex non-linear patterns in the training data compared to non-parametric model like SVM or a linear model like logistic regression.

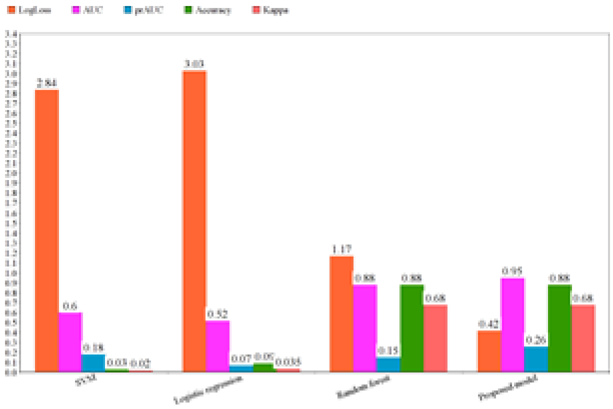


Fig. 4 Training set performance: accuracy, detection rate, area under curve (AUC), precision-recall area under curve (prAUC), log loss and kappa

The test of generalization ability of the models was evaluated on basis of several criteria - accuracy and kappa (Figure 5). The test for accuracy and kappa shows the tie between random forests and kappa. However, the proposed model having more tunable parameters led to slightly lower performance than random forests. The p-value which should be low or nearly zero for a hypoth- esis to be rejected is low for random forest and proposed model. Although accuracy and kappa are aggregate parameters of performance but these may not reflect the ability of the models to detect the classes of illegal activity that is important in the current paper.

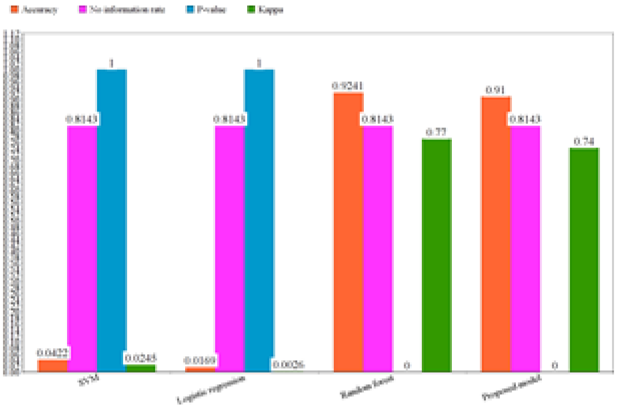
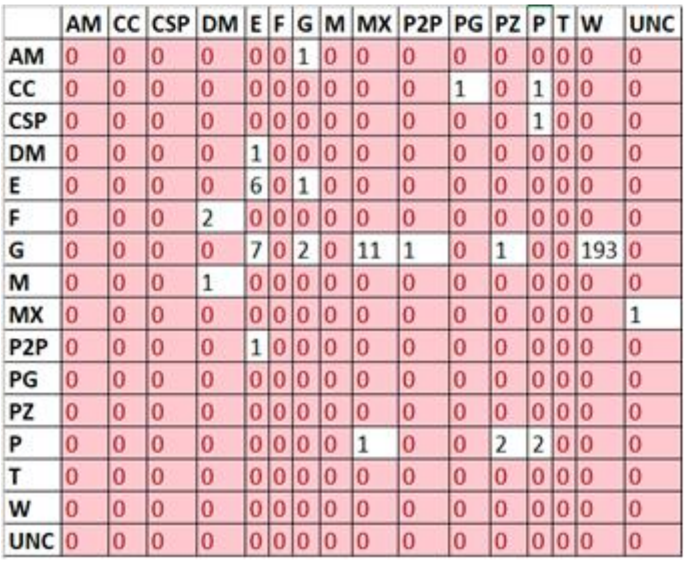


Fig. 5 Test set performance: accuracy and kappa

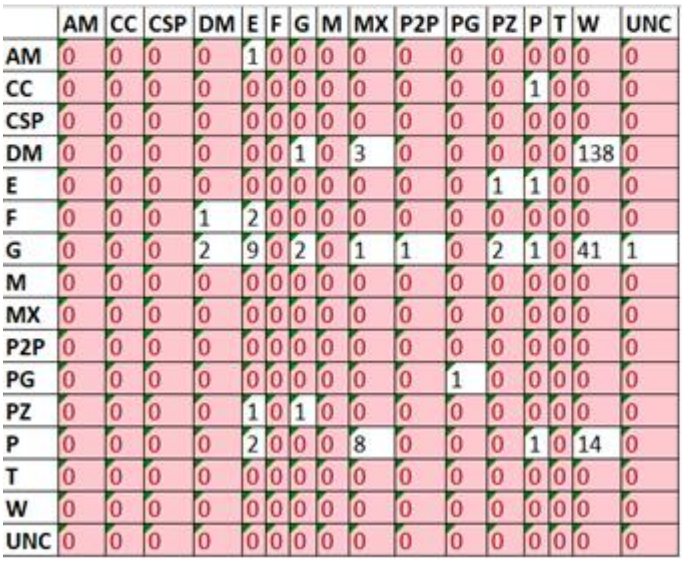
The confusion matrix is illustrated in Figure 6 for the predictions of SVM on the test set. Exchanges and Pools could be recognized however the rest of the classes were misclassified by the model.



	AM	CC	CSP	DM	E	F	G	M	MX	P2P	PG	PZ	P	T	W	UNC
AM	0	0	0	0	0	0	1	0	0	0	0	0	0	0	0	0
CC	0	0	0	0	0	0	0	0	0	0	1	0	1	0	0	0
CSP	0	0	0	0	0	0	0	0	0	0	0	0	1	0	0	0
DM	0	0	0	0	1	0	0	0	0	0	0	0	0	0	0	0
E	0	0	0	0	6	0	1	0	0	0	0	0	0	0	0	0
F	0	0	0	2	0	0	0	0	0	0	0	0	0	0	0	0
G	0	0	0	0	7	0	2	0	11	1	0	1	0	0	193	0
M	0	0	0	1	0	0	0	0	0	0	0	0	0	0	0	0
MX	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	1
P2P	0	0	0	0	1	0	0	0	0	0	0	0	0	0	0	0
PG	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0
PZ	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0
P	0	0	0	0	0	0	0	0	1	0	0	2	2	0	0	0
T	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0
W	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0
UNC	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0

Fig. 6 Confusion matrix of SVM classifier on Test set

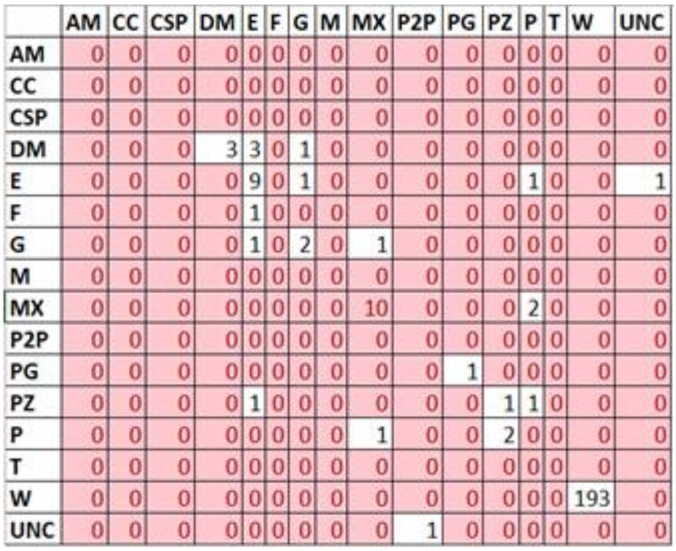
The confusion matrix is illustrated in Figure 7 for the predictions of logistic regression on the test set. Only payment gateway could be recognized howeverthe rest of the classes were misclassified by the model.



	AM	CC	CSP	DM	E	F	G	M	MX	P2P	PG	PZ	P	T	W	UNC
AM	0	0	0	0	1	0	0	0	0	0	0	0	0	0	0	0
CC	0	0	0	0	0	0	0	0	0	0	0	0	1	0	0	0
CSP	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0
DM	0	0	0	0	0	0	1	0	3	0	0	0	0	0	138	0
E	0	0	0	0	0	0	0	0	0	0	0	1	1	0	0	0
F	0	0	0	1	2	0	0	0	0	0	0	0	0	0	0	0
G	0	0	0	2	9	0	2	0	1	1	0	2	1	0	41	1
M	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0
MX	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0
P2P	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0
PG	0	0	0	0	0	0	0	0	0	0	1	0	0	0	0	0
PZ	0	0	0	0	1	0	1	0	0	0	0	0	0	0	0	0
P	0	0	0	0	2	0	0	0	8	0	0	0	1	0	14	0
T	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0
W	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0
UNC	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0

Fig. 7 Confusion matrix of Logistic Regression classifier on Test set

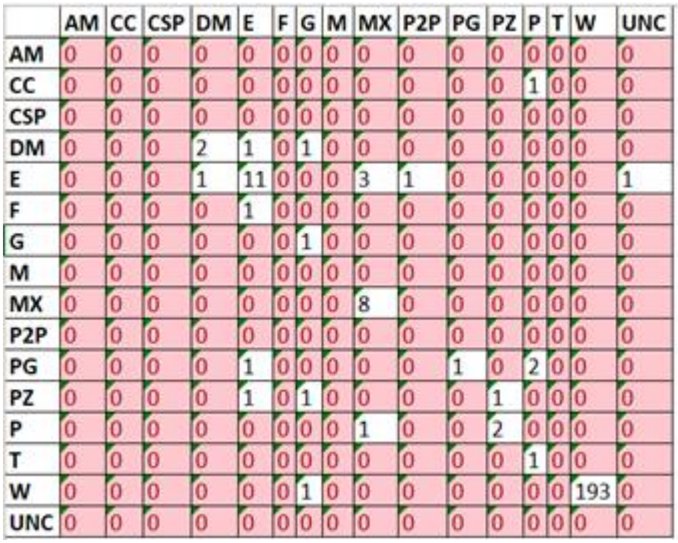
The confusion matrix is illustrated in Figure 8 for the predictions of ran- dom forests on the test set. Darknet markets, Wallets, Exchanges, Gambling, Payment gateways could be recognized however the rest of the classes were misclassified by the model.



	AM	CC	CSP	DM	E	F	G	M	MX	P2P	PG	PZ	P	T	W	UNC
AM	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0
CC	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0
CSP	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0
DM	0	0	0	3	3	0	1	0	0	0	0	0	0	0	0	0
E	0	0	0	0	9	0	1	0	0	0	0	0	1	0	0	1
F	0	0	0	0	1	0	0	0	0	0	0	0	0	0	0	0
G	0	0	0	0	1	0	2	0	1	0	0	0	0	0	0	0
M	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0
MX	0	0	0	0	0	0	0	0	10	0	0	0	2	0	0	0
P2P	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0
PG	0	0	0	0	0	0	0	0	0	0	1	0	0	0	0	0
PZ	0	0	0	0	1	0	0	0	0	0	0	1	1	0	0	0
P	0	0	0	0	0	0	0	0	1	0	0	2	0	0	0	0
T	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0
W	0	0	0	0	0	0	0	0	0	0	0	0	0	0	193	0
UNC	0	0	0	0	0	0	0	0	0	1	0	0	0	0	0	0

Fig. 8 Confusion matrix of Random Forest classifier on Test set

The confusion matrix is illustrated in Figure 9 for the predictions of the proposed model on the test set. Darknet markets, Wallets, Exchanges, Gam- bling, Payment gateways and Mixers could be recognized however the rest of the classes were misclassified by the model. The important distinction with random forests is that mixers are identified correctly by the proposed model.



	AM	CC	CSP	DM	E	F	G	M	MX	P2P	PG	PZ	P	T	W	UNC
AM	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0
CC	0	0	0	0	0	0	0	0	0	0	0	0	1	0	0	0
CSP	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0
DM	0	0	0	2	1	0	1	0	0	0	0	0	0	0	0	0
E	0	0	0	1	11	0	0	0	3	1	0	0	0	0	0	1
F	0	0	0	0	1	0	0	0	0	0	0	0	0	0	0	0
G	0	0	0	0	0	0	1	0	0	0	0	0	0	0	0	0
M	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0
MX	0	0	0	0	0	0	0	0	8	0	0	0	0	0	0	0
P2P	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0
PG	0	0	0	0	1	0	0	0	0	0	1	0	2	0	0	0
PZ	0	0	0	0	1	0	1	0	0	0	0	1	0	0	0	0
P	0	0	0	0	0	0	0	0	1	0	0	2	0	0	0	0
T	0	0	0	0	0	0	0	0	0	0	0	0	1	0	0	0
W	0	0	0	0	0	0	1	0	0	0	0	0	0	0	193	0
UNC	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0

Fig. 9 Confusion matrix of Proposed classifier on Test set

Data imbalance was handled in multiple methods: first xavier initializer was used to initialize the weights and the bias of the different layers. Then, the weights were assigned to the class as per their occurrence and finally the batch size was increased during training which caused the model to encounter a few samples of each class during the training phase.

CONCLUSION AND FUTURE WORKS

The model we used is based on the traditional graph neural network (2017) with a small difference in the message passing mechanism (related to use of convolution filters) and our paper focuses on effectively using it for bitcoin transaction classification. For the current paper the research gaps we identified through literature search were: existing research focused on limited number of entities that carried out illegal activities on blockchain network, existing works focused on different and limited set of features, these works focused on less amount of data, there was a need to create a up-to-date study consideringthe fast changing landscape. To fulfill these research gaps, the current paper proposed a machine learning model trained on 19 different features engineeredfrom raw data. The results are promising and the approach can be used for real-time systems as well.

REFERENCES

[1] Turner, A., Irwin, A.S.M.: Bitcoin transactions: a digital discovery of illicit activity on the blockchain. Journal of Financial Crime (2018)

[2] Nerurkar, P., Pavate, A., Shah, M., Jacob, S.: Performance of internal cluster validations measures for evolutionary clustering. In: Computing, Communication and Signal Processing, pp. 305–312. Springer, (2019)

[3] Nerurkar, P., Chandane, M., Bhirud, S.: Survey of network embedding techniques for social networks. Turkish Journal of Electrical Engineering & Computer Sciences 27(6), 4768–4782 (2019)

[4] Nakamoto, S.: Bitcoin: A peer-to-peer electronic cash system. Technical report, Manubot (2019)

[5] Kumar, A., Abhishek, K., Ghalib, M.R., Nerurkar, P., Shah, K., Chan- dane, M., Bhirud, S., Patel, D., Busnel, Y.: Towards cough sound analysis using the internet of things and deep learning for pulmonary disease pre- diction. Transactions on emerging telecommunications technologies, 4184 (2020)

[6] Nerurkar, P., Chandane, M., Bhirud, S.: Understanding structure and behavior of systems: a network perspective. International Journal of Information Technology, 1–15 (2019)

[7] Chheda, H., Nerurkar, P.: Malware detection using machine learning. In: Knowledge Graphs and Semantic Web: Second Iberoamerican Conference and First Indo-American Conference, KGSWC 2020, M´erida, Mexico, November 26-27, 2020, Proceedings, vol. 1232, p. 61 (2020). Springer Nature

[8] Nerurkar, P., Shirke, A., Chandane, M., Bhirud, S.: Empirical analysis of data clustering algorithms. Procedia Computer Science 125, 770–779 (2018)

[9] Nerurkar, P., Shirke, A., Chandane, M., Bhirud, S.: A novel heuristic for evolutionary clustering. Procedia Computer Science 125, 780–789 (2018)

[10] Lee, C., Maharjan, S., Ko, K., Hong, J.W.-K.: Toward detecting ille- gal transactions on bitcoin using machine-learning methods. In: Zheng, Z., Dai, H.-N., Tang, M., Chen, X. (eds.) Blockchain and Trustworthy Systems, pp. 520–533. Springer, Singapore (2020)

[11] Kumar, A., Abhishek, K., Kumar Singh, A., Nerurkar, P., Chandane, M., Bhirud, S., Patel, D., Busnel, Y.: Multilabel classification of remote sensed satellite imagery. Transactions on emerging telecommunications 12 technologies 32(7), 3988 (2021)

[12] Foley, S., Karlsen, J.R., Putnin¸ˇs, T.J.: Sex, drugs, and bitcoin: How much illegal activity is financed through cryptocurrencies? The Review of Financial Studies 32(5), 1798–1853 (2019)

[13] Liu, T., Ge, J., Wu, Y., Dai, B., Li, L., Yao, Z., Wen, J., Shi, H.: A new bitcoin address association method using a two-level learner model. In: Wen, S., Zomaya, A., Yang, L.T. (eds.) Algorithms and Architectures for Parallel Processing, pp. 349–364. Springer, Cham (2020)

[14] Zarpel˜ao, B.B., Miani, R.S., Rajarajan, M.: Detection of bitcoin-based botnets using a one-class classifier. In: Blazy, O., Yeun, C.Y. (eds.) Information Security Theory and Practice, pp. 174–189. Springer, Cham (2019)

[15] Yang, L., Dong, X., Xing, S., Zheng, J., Gu, X., Song, X.: An abnormal transaction detection mechanim on bitcoin. In: 2019 International Con- ference on Networking and Network Applications (NaNA), pp. 452–457 (2019). IEEE

[16] Zhang, Z., Zhou, T., Xie, Z.: Bitscope: Scaling bitcoin address de- anonymization using multi-resolution clustering

[17] Nerurkar, P., Chandane, M., Bhirud, S.: Measurement of network-based and random meetings in social networks. Turkish Journal of Electrical Engineering & Computer Sciences 27(2), 765–779 (2019)

[18] Pavate, A., Nerurkar, P., Chaudhary, A., Bansode, R., Shah, M.: Clump approach for animal concern system

[19] Pavate, A., Nerurkar, P.: Performance analysis of cloud based penetration testing tools. International Journal of Advanced Research in Computer Science 4(3), 3988 (2014)

[20] Gentyala, V., Nerurkar, P.: Geolocation events based auto theme changer for browsers. International Journal of Advanced Research in Computer Science 4(3), 3988 (2013)

[21] Nerurkar, P., Chandane, M., Bhirud, S.: Representation learning for social networks using homophily based latent space model. In: Proceedings of the International Conference on Omni-Layer Intelligent Systems, pp. 38–43 (2019)

[22] Akcora, C.G., Li, Y., Gel, Y.R., Kantarcioglu, M.: BitcoinHeist: Topolog- ical Data Analysis for Ransomware Detection on the Bitcoin Blockchain (2019)

[23] Portnoff, R.S., Huang, D.Y., Doerfler, P., Afroz, S., McCoy, D.: Backpage and bitcoin: Uncovering human traffickers. In: KDD '17 (2017)

[24] Nerurkar, P., Chandane, M., Bhirud, S.: Community detection using node attributes: A non-negative matrix factorization approach. In: Computa- tional Intelligence: Theories, Applications and Future Directions-Volume I, pp. 275–285. Springer, (2019)

[25] Nerurkar, P., Chandane, M., Bhirud, S.: Understanding structure and behavior of systems: a network perspective. International Journal of Information Technology, 1–15 (2019)

[26] Yin, H.S., Vatrapu, R.: A first estimation of the proportion of cybercrim- inal entities in the bitcoin ecosystem using supervised machine learning. In: 2017 IEEE International Conference on Big Data (Big Data), pp. 3690–3699 (2017). IEEE

[27] Nerurkar, P.A., Chandane, M., Bhirud, S.: Exploring convolutional auto- encoders for representation learning on networks. Computer Science 20 (2019)

[28] Nerurkar, P., Chandane, M., Bhirud, S.: Empirical analysis of synthetic and real networks. International Journal of Information Technology, 1–13 (2019)

[29] Nan, L., Tao, D.: Bitcoin mixing detection using deep autoencoder. In: 2018 IEEE Third International Conference on Data Science in Cyberspace (DSC), pp. 280–287 (2018)

[30] Pavate, A., Nerurkar, P.: Study of angular js: A client side javascript framework for single page applications. International journal of con- temporary research in computer science and technology 1(4), 3988 (2015)

[31] Pavate, A., Chaudhary, A., Nerurkar, P., Mishra, P., Shah, M.: Cui- sine recommendation, classification and review analysis using supervised learning. In: 2020 International Conference on Convergence to Digital World-Quo Vadis (ICCDW), pp. 1–6 (2020). IEEE

[32] Pham, T., Lee, S.: Anomaly detection in bitcoin network using unsuper- vised learning methods. arXiv preprint arXiv:1611.03941 (2016)

[33] Kumar, A., Kolnure, S.N., Abhishek, K., Nerurkar, P., Ghalib, M.R., Shankar, A., et al.: Advanced deep learning algorithms for infectious disease modeling using clinical data-a case study on covid-19. Current Medical Imaging (2021)

[34] Aiolli, F., Conti, M., Gangwal, A., Polato, M.: Mind your wallet's privacy: Identifying bitcoin wallet apps and user's actions through network traffic analysis. (2019). https://doi.org/10.1145/3297280.3297430

[35] Nerurkar, P., Bhirud, S.: Modeling influence on a social network using interaction characteristics. Int. J. Comput. Math. Sci 6(8), 152–160 (2017)

[36] Janda, A.: WalletExplorer. com: Smart Bicoin Block Explorer (2016)

[37] Maesa, D.D.F., Marino, A., Ricci, L.: The bow tie structure of the bitcoin users graph. Applied Network Science 4(1), 56 (2019)