A BITCOIN TRANSACTION NETWORK USING CACHE BASED PATTERN MATCHING RULES

Dr. B. Subba Reddy[1], N. Ashwitha Reddy[2], R. Naveena Reddy[2], R. Keerthi Reddy[2]

[1]Professor & HOD, [1]UG Scholar, [1,2]Department of Information Technology

[1,2]Malla Reddy Engineering College for Women (A), Maisammaguda, Medchal, Telangana.

ABSTRACT

Crypto currencies usage increasing every year around the world. The Bitcoin is the one of the famous cryptocurrencies, which is an unofficial usable currency in various nations. The bitcoin transactions are increasing, which needs to be monitored carefully. However, the conventional methods are failed to analyze the bitcoin transaction effectively. Therefore, this work focused on development of bitcoin transaction network (BTN) using pattern matching rules (PMR). Initially, the dataset preprocessing is carried out to identify the missed symbols, unknown characters from forensic blockchain dataset. Then, Petri-Net model applied on preprocessed dataset, which identifies the time stamp, transaction id, work tera hash, and work error properties. The Petri-Net model mainly used to parse and build the BTN model. Then, PMR conditions are developed to extract the transaction addresses extracted with time stamp details. So, PMR detects the illegal payment addresses by matching the known data with illegal (spam) addresses. Further, cache based PMR (CPMR) is also applied to detect the fraud transaction, which store all previous detected illegal payment addresses. So, for every new transaction, CPMR will ignore all those previously stored (detected) illegal payment addresses. This phenomenon causes reduction of fraud transaction detection time and processing becomes faster. The simulations shows that the proposed method resulted in reduced transaction processing time (TPT), fraud transaction detection time (FTDT), and improved fault transaction detection accuracy (FTDA) as compared to conventional methods.

Keywords: Crypto currency, bitcoin transaction, pattern matching rules.

1. INTRODUCTION

Bitcoin's meteoric rise to prominence as a viable alternative form of money over the last several years has been an unavoidable consequence of Satoshi Nakamoto's decision to launch the cryptocurrency in the first place. At the end of 2017, it was observed that the market capitalization of Bitcoin had surpassed $200 billion at that point. Bitcoins are often not linked to their users' identities, which might include things like user names, residence addresses, and other forms of personal identifying information. As a result of the pseudonymous character of Bitcoin, it is mistakenly thought of as a type of anonymous money on the Internet. Additionally, it is mistakenly believed that Bitcoin facilitates untraceable transactions during unlawful deals.

It is often not a problem to track Bitcoins that are connected with a recognised address. However, because to the murky and unreliable nature of the addresses used by criminals, monitoring Bitcoins has proven to be difficult. To that end, the purpose of this article is to identify questionable addresses based on the typical patterns and characteristics of financial transactions. In a broad sense, some transactions could demonstrate commonalities and common patterns. For instance, Bitcoin transactions that are used to accumulate Bitcoins often connect numerous input addresses with one output address. In the process of tracing unknown and suspicious transactions, doing an analysis of the connections that exist between such input and output addresses may provide helpful information.

In this research, an expanded safe Petri net (9)-based model to simulate Bitcoin transactions, which is named the Bitcoin Transaction Net, is proposed (BTN). Both the static and dynamic aspects of

Bitcoin transactions may be described using the cryptocurrency's structural characteristics and dynamic semantics, respectively. To establish Bitcoin transaction patterns for the purpose of evaluating and discovering suspicious addresses using our pattern matching approach, we have identified nineteen characteristics, both static and dynamic, that are associated with Bitcoin transactions. Another important addition that our technique has made is the creation of the Bitcoin gene, which is included into the transitions of the Petri net. When a transaction takes place, there are specified to be three different gene operations that may take place: merging, splitting, and dyeing. Bitcoin gene not only describes the strength of links between addresses but also reveals whether or not an address has a relationship with certain other addresses. Bitcoin gene is a tool that enables users to track and correctly evaluate the movement of bitcoins in an expedient and accurate manner. In addition, this study presents a collection of match criteria that, when combined, may be used to discover suspicious transactions and get addresses associated with such transactions. In conclusion, a marginal distribution analysis of transaction pattern features has been incorporated into the model that has been proposed. This has been done in order to get rid of some of the false positive samples that have been identified and to improve the accuracy of the identified suspect addresses.

2. LITERATURE SURVEY

The owner of bitcoin addresses an is unknown and is under suspicion. However, the owner of Bitcoin addresses a may be inferred if the owner of bitcoin address, which is inside the same cluster as a, is known. Addresses are divided into clusters [9], when they are utilized as transaction inputs. Addresses a and b, for instance, are grouped together into a single cluster if they are used as inputs for transaction t1. Numerous research [10] make advantage of this input address clustering technique. A user graph was built using the bitcoin address clustering (BAC) method, and significant users were identified using PageRank. To recover the "change" from whatever transaction the user has issued.

In addition to clustering addresses using the input and change address clustering methods [11], they also assessed the efficacy of the change address clustering approach. BitIodine is a modular framework developed in [12], that parses the blockchain, groups address that are probably owned by the same person or group of users, and visualizes complicated data taken from the Bitcoin network. The two clustering techniques are also used by BitIodine to group addresses. These clusters of addresses utilized as vertexes in several previous flow analysis techniques [13] and the transaction interactions between vertexes as direction edges. Bitcoins often go from vertexes to vertexes via edges. In their basic Bitcoin flow analysis technique, in [14] authors initially grouped Bitcoin addresses before connecting the clusters using connections made by transactions. Finally, both statistical and graphical tools have been used to study the graph. The hybrid graph [15] was used to examine the graph structure's characteristics that could impact anonymity. But none of these studies have placed enough attention on studying Bitcoin transaction trends.

Transactions involving Bitcoin have been examined using modified Petri-Net [16]. Bitcoin addresses are represented by Petri-Net locations and transitions. This Petri-Net model employed to group addresses and discovered common patterns of behavior, such as the use of a specific address just once. In [17] authors examined disposable addresses to addresses using machine learning based approaches. A power-law distribution characterizes the lengths of these chains. The Bitcoin addresses were employed in these two models as Petri-Net locations or inputs for Bitcoin transactions. On the BTN, inputs for transactions are often coins rather than addresses. As a result, such models are unable to assess and quantify transaction aspects effectively. The expanded Petri-Net for the study of Bitcoin transactions that were presented in contrast to the current approaches that seek to identify behavior factors underlying Bitcoin transactions. According to authors [18], it is possible to recognize and validate Bitcoin users by examining the characteristics of their transactions over time. A data visualization tool called BitCone view was created in [19], to demonstrate the efficiency. They conducted a thorough measuring study of information on the Silk Road that was gathered by web crawling. The data characters have been shown using these visualization techniques. This may use visual perception to identify the transaction patterns in a block. However, this approach is unable to identify subtle trends in large-scale transactional data. BlockChainVis [20] is a program uses visual analytics methods to filter out unwanted information and graphically examine the transactions. Users of BlockChainVis may create simple filters to exclude unwanted information

The research conducted by Pinna [21] using Petri net looked at disposable addresses, sometimes known as addresses that are only used once. Transactions are thought to form chains, and the lengths of these chains are thought to follow a power-law distribution, according to the writings of [21]. In these two models, Bitcoin addresses were employed as Petri net sites or inputs for Bitcoin transactions. However, in the Bitcoin transaction net, the inputs of Bitcoin transactions are not often addresses but rather currencies. The outputs of Bitcoin transactions are generally Bitcoins. Consequently, such models are unable to examine and quantify the aspects of transactions effectively. In this study, an expanded form of Petri nets was presented for the analysis of Bitcoin transactions. This form of Petri nets organically combines crucial Bitcoin elements, such as the transaction, the input and output, the address, the bitcoin amount, the transaction time, and so on.

In contrast to the current approaches, which focus on identifying the behaviour patterns that are behind Bitcoin transactions, our method seeks to create transaction patterns based on the attributes of transactions and then locate problematic addresses on the basis of the patterns. Monaco [22] established and validated an assumption that it is possible to identify and verify Bitcoin users by observing the characteristics of Bitcoin transactions as they evolve over time. This assumption remains true. This investigation came to the conclusion, after doing an analysis of the behavioural characteristics utilising 366 user samples, that the behavioural patterns seen over time may be utilised to deprive a user; however, this information was not further developed into a model. In a manner similar to that of Monaco [22], Harlev et al. [23] gathered 434 training samples and using the supervised machine learning approach in order to categorise unknown items into predetermined groups. In contrast, fraudsters in the real world aim to conceal the Bitcoin addresses they use. Because it is impossible to locate their addresses in order to assess the characteristics of their transactions, the practical usefulness of these methods is restricted because there are no known samples. The approach that we have developed, in contrast to the methods that they use, does not need such known samples. A transaction pattern may be defined using any known information, such as information from information agencies, and addresses that fit the pattern can be found using our suggested technique.

In addition, data visualisation techniques have been used in the process of Bitcoin transaction analysis. Coin mixing services were evaluated for their ability to thwart tracing efforts by Moser et al. [24]. A data visualisation tool known as BitConeView was created by Battista et al. [25] to demonstrate how successful coin mixing services are. Christin [26] carried out an exhaustive measuring examination of the data acquired from web crawling that pertained to Silk Road. The data characters have been shown using these several approaches of data visualisation.

Both Kondor et al. [27] and Maesa et al. [18] investigated the topology of the Bitcoin transaction network by measuring the features of the network, and they presented the findings using a variety of ways for visualising the data. A systematic top-down visualisation of Bitcoin systems was provided by McGinn et al. [28]. This visualisation is able to locate transaction patterns in a block via the use of visual perception. However, this approach is unable to discover minor transaction patterns that are hidden behind big transactions. BlockChainVis is a programme that was created by Bistarelli and colleagues [29] that uses methods from visual analytics to filter away unneeded information in order to do a visual analysis of the transactions. BlockChainVis gives users the ability to establish simple rules to filter out unwelcome data. The authors of [24-26] concentrated on the visualisation of certain aspects of the Bitcoin transactions for particular reasons, while the authors of [18, 27, 28] chose to visualise the Bitcoin Blockchain as a whole. As a consequence of this, it is simple to overlook some particulars. The efforts of [29] introduced a set of configurable filters that may be used to discover certain addresses or transactions. In a manner similar to [22], this technique analysed transaction characteristics individually while ignoring the process of constructing a transaction pattern. The techniques of visualisation often rely on one's visual sense in order to get results. On the other hand, because of the inherent limitations of the human brain, some findings are often overlooked. Instead of relying on human visual perception, our approach has the pattern-matching algorithm handle the task of comparing transaction patterns. As a result, it is more effective and almost eliminates the risk of overlooking things. The approach that we have developed utilises visualisation methods to show marginal distributions of a variety of transaction characteristics in order to filter out a portion of the false positive samples. However, these techniques are not used to directly analyse transaction feature data. As a result, the limitations that are associated with the visualisation approaches that have been discussed before are not inherited by our method.

3. PROPOSED SYSTEM

Since Satoshi Nakamoto first introduced bitcoin, its popularity as an alternate method of payment has grown significantly over the last several years [1]. At the end of 2021, it was estimated that the market value of Bitcoin had surpassed $200 billion. Bitcoins are often not linked to user identities like usernames. Due to its pseudonymous character [2], Bitcoin is mistakenly thought of as an anonymous mode of payment on the Internet and as a means of enabling untraceable transactions during illicit dealings. Tracking Bitcoins linked to a known address is often not a problem [3]. However, it has been difficult to trace Bitcoins since criminals often use ambiguous and hazy addresses.

Figure 1 shows the various bitcoin frauds occurred in different countries [4] like Vietnam, united states, United Kingdom, Ukraine, turkey, south Africa, Russia, south Africa, and China. The bitcoin frauds are majority based on darknet markets, ransomware, scams, and stolen funds [5]. In order to deal with this, various works aims to separate bitcoin fraud addresses. Generally speaking, some transactions may show commonalities and recurring trends. For instance, bitcoin transactions [6] were used to accumulate Bitcoins often link an output address to a number of input addresses. When monitoring ambiguous and improbable transactions, examining the connections between such input and output addresses may provide insightful information. However, such analysis involves additional challenges [7] like defining the characteristics of bitcoin transactions, successfully identifying the characteristics that can be used to identify suspects.

With the help of our pattern matching technology, we have discovered static and dynamic Bitcoin transaction attributes that identify Bitcoin transaction patterns for analysis and locating questionable addresses. The evolution of the Bitcoin gene, which is integrated in Petri-Net transitions [8], is another significant addition. The movement of Bitcoins may be quickly and reliably tracked and analyzed using bitcoin transaction. Additionally, based on the combinations of match rules, this study suggests a set of match criteria to discover transactions and get suspicious addresses [9].

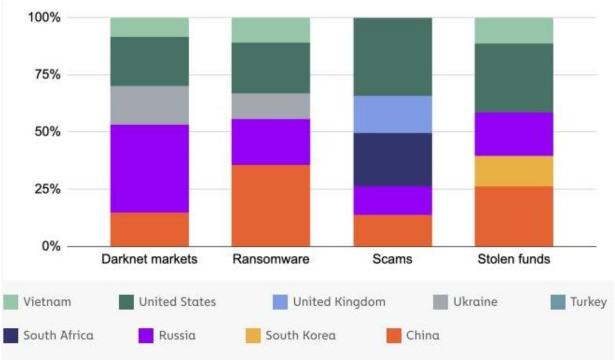


Fig. 1: Bitcoin frauds in various countries.

This article developed BTN utilizing PMR. Pre-processing the forensic blockchain dataset identifies missing symbols and unfamiliar characters. After preprocessing, Petri-Net model identifies time stamp, transaction id, work tera hash, and work error attributes. Petri-Net parses and builds BTN. PMR conditions extract transaction addresses with time stamps. CPMR also stores all prohibited payment addresses to identify fraud transactions. CPMR will disregard any previously recorded unlawful payment addresses for each new transaction. Simulations showed that the suggested strategy lowered TPT, FTDT, and improved FTDA compared to existing methods.

System architecture

Criminals, on the other hand, plan to conceal their Bitcoin addresses in the real world. Due to the paucity of known samples, it is challenging to locate their locations in order to study the transaction attributes, which restricts their practical application. Figure 2 shows the proposed BTN framework. This effort focused on the creation of BTN utilizing PMR. Initially, dataset pre-processing is performed to discover missing symbols and unfamiliar characters in the forensic blockchain dataset. Here, the information is saved into the database using an open-source program called Bitcoin Database Generator. The Petri-Net model is then used to the pre-processed dataset, identifying the time stamp, transaction id, work tera hash, and work error attributes. The Petri-Net model is primarily used to parse and construct the BTN model. Then, PMR conditions are created to retrieve the collected transaction addresses with time stamp data. As a result, PMR identifies illicit payment addresses by comparing known data to illegal addresses. Furthermore, CPMR is used to identify fraudulent transactions, which stores all previously recognized unlawful payment addresses. As a result, for each new transaction, CPMR will disregard any previously recorded (detected) unlawful payment addresses. This effect reduces the time required to identify fraud in transactions and speeds up processing. When compared to existing approaches, the simulations demonstrate that the suggested method TPT, FTDT, and enhanced FTDA.

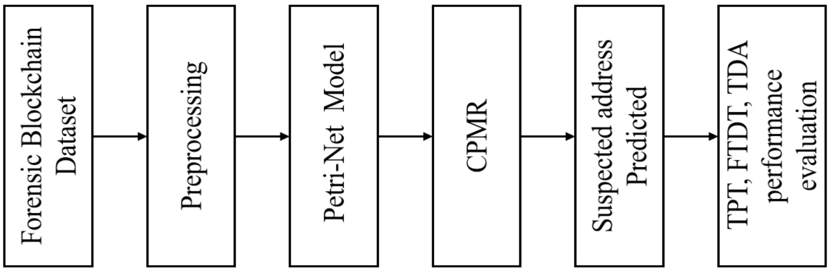

Forensic Blockchain Dataset
Preprocessing
Petri-Net Model
CPMR
Suspected address Predicted
TPT, FTDT, TDA performance evaluation

Fig. 2: Proposed BTN-CPME block diagram.

Pre-processing

The raw forensic blockchain dataset contains noises, missing values, which caused to complicated training of CPMR model. Further, it will reduce the classification, prediction performance. So, the data preprocessing operation is performed to overcome these problems. The preprocessing operation will replace unknown symbols, missing vales with the known nearest values. The efforts of filtering options that may be used to discover certain transactions or addresses. This approach defined a transaction pattern and instead took into account transaction characteristics independently. Methods of visualization often rely on visual perception to get outcomes. However, certain outcomes often go unnoticed because of the capacity limitations of the human brain. In our solution, the pattern matching algorithm instead of visual perception is used to match transaction patterns. As a result, it is more effective and seldom overlooks details. In order to filter out certain false positive samples using our suggested strategy, marginal distributions of several transaction characteristics are shown using visualization methods rather than being directly analyzed.

Petri-Net Model

A formal mathematical model called a Petri-Net, which is used to explore concurrent and asynchronous processes in distributed systems. An alternative name for it is a place/transition (PT) net. It was initially developed in 1962 by Carl Adam Petri. It is a bipartite directed graph with two different kinds of nodes, locations, and transitions. Directed arcs link the locations with the transitions, indicating which locations serve as inputs before transitions take place and outputs once they do. Arcs can only link locations to transitions or locations to transitions. Tokens are stored in places. Transitions cannot keep any tokens, but places may store an endless amount of them. The distribution of tokens among locations determines the state or marking of a Petri-Net. Figure 3 depicts a straightforward net with all the components of a Petri-Net, where the circles represent locations and the rectangle a transition. The formal definition of a Petri-Net is a tuple N = (P, T, F, M0), where P and T are disjoint finite sets of locations and transitions, respectively, F is a set of arcs (or incidence function), and M0 is the initial marking where M0: 1, 2, 3, J.

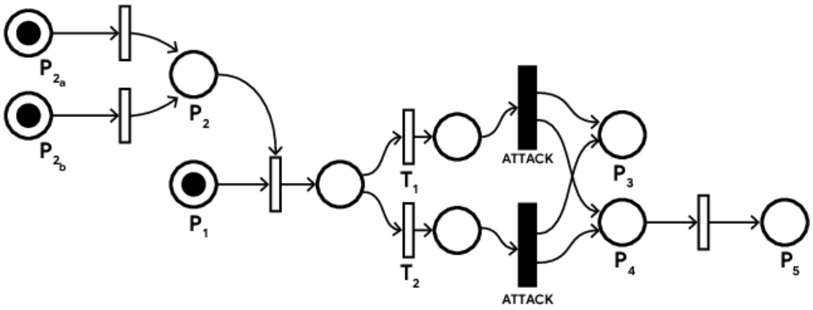


Fig. 3: Operational flow of Petri-Net.

The Petri-Net are more effective at catching concurrent actions as an assault progressed. Petri-Net have since been used to simulate physical and digital assaults on a variety of systems and networks. An innovative approach for studying the BTN was suggested in this research. This system formalizes Bitcoin transactions as an extended Safe Petri-Net known as BTN. The static and dynamic properties of a Bitcoin transaction are described by its structure and semantic features. The Bitcoin flow analysis may exploit the gene characteristic of bitcoins. Different transaction patterns may be developed based on the qualities that have been stated. It is possible to identify the addresses that fit the patterns. Based on a review of actual case studies, the suggested technique has been shown to be a useful tool for forensic investigation of future Bitcoin transactions. Pattern expressions are manually designed for our investigations. The next stage will be to create a compiler to automatically turn patterns into code. We shall then keep looking on ways to preserve BTN's interim states. In our tests, the Bitcoin

Blockchain is parsed using the open-source application bitcoin database generator. The performance of the analysis is impacted since it does not retrieve information about block and transaction ordering.

CPMR Prediction

The CPMR to locate suspected addresses that does not fit a predetermined pattern of bitcoin transactions. Directly describing a complex pattern, however, is difficult. As a result, we provide guidelines for defining a pattern using logical expressions. Figure 4 shows suspected activity detection using CPMR. A collection of attributes describes a pattern and collection of feature expressions constitutes a property. According to this, a feature expression is a logical expression over features. In actuality, all three expressions—pattern, property, and feature—are logical expressions over features. A feature expression is used to characterize a Bitcoin transaction feature's personality. An element in a pattern is described by a property expression. An expression of a pattern depicts a pattern. In general, we should examine the elements that make up a pattern before attempting to describe it. A property should then be specified by one or more feature expressions for each aspect.

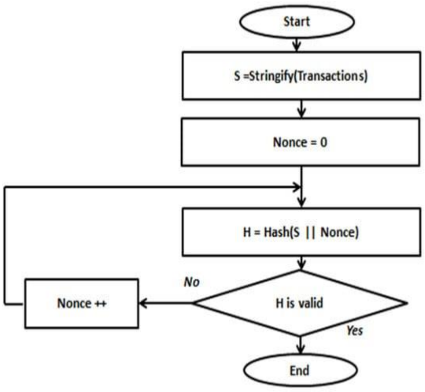


Fig. 4: Suspected address prediction using CPMR.

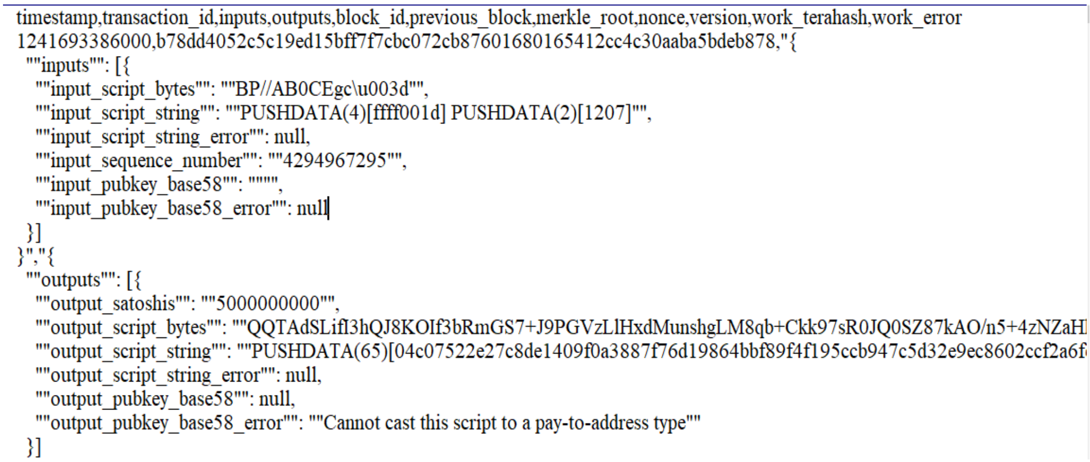
The nonce N that generates a valid hash, as shown in Figure 4, represents the precise number of hashes that were executed in order to find the valid address and suspected address. As a result, the time T needed to mine a block with a specified hash power H can be accurately calculated using the straightforward formula T=H /N. Since the nonce is used to create the lock hash when a new block is mined and the block mining time is known to all network peers, it is simple to determine the hash rate that was used. Only if the newly proposed block was hashed at the permitted hash rate should it be approved

4. Results and Discussion

This section gives the detailed results analysis of proposed method, which are implemented using BTN-CPMR model.

Dataset

This Data Set associates actual entities with Bitcoin transactions that fall into the licit and illegal categories, such as exchanges, wallet providers, miners, and other licit service providers (scams, malware, terrorist organizations, ransomware, Ponzi schemes, etc.). Sorting the graph's illegal and legitimate nodes is the job at hand with this dataset. The information, which includes 200,000 transactions totaling more than $6 billion, will be used to assist the bitcoin industry detect dishonest individuals. The biggest collection of annotated bitcoin transaction data in the world has been created by researchers at MIT's IBM-funded AI Lab and blockchain forensics firm Elliptic. The labeling draws attention to distinctive transaction features and may be used to identify criminal actors operating in the cryptocurrency industry." Figure 5 shows the sample dataset with time stamp, transaction id, work tera hash, and work error properties.



```
timestamp,transaction_id,inputs,outputs,block_id,previous_block,merkle_root,nonce,version,work_terahash,work_error
1241693386000,b78dd4052c5c19ed15bff7f7cbc072cb87601680165412cc4c30aaba5bdeb878,"{
 ""inputs"": [{
  ""input_script_bytes"": ""BP//AB0CEgc\u003d"",
  ""input_script_string"": ""PUSHDATA(4)[ffff001d] PUSHDATA(2)[1207]"",
  ""input_script_string_error"": null,
  ""input_sequence_number"": ""4294967295"",
  ""input_pubkey_base58"": """",
  ""input_pubkey_base58_error"": null
 }]
}","{
 ""outputs"": [{
  ""output_satoshis"": ""5000000000"",
  ""output_script_bytes"": ""QQTAdSLifl3hQJ8KOIf3bRmGS7+J9PGVzLlHxdMunshgLM8qb+Ckk97sR0JQ0SZ87kAO/n5+4zNZaH
  ""output_script_string"": ""PUSHDATA(65)[04c07522e27c8de1409f0a3887f76d19864bbf89f4f195ccb947c5d32e9ec8602ccf2a6f
  ""output_script_string_error"": null,
  ""output_pubkey_base58"": null,
  ""output_pubkey_base58_error"": ""Cannot cast this script to a pay-to-address type""
 }]
```

Fig. 5: Sample dataset.

Performance evaluation

In Figure 6, x-axis represents total withdraw from account 0 to 1 and vice versa and y-axis represents number of gather addresses for that withdrawal. In Figure 7, x-axis represents number of account ID and y-axis represents number of deposit transaction made by that account. Further, Table 1 shows that the proposed BTN-CPMR protocol resulted in higher security standards compared to BAC [10], BitIodine [13], and BlockChainVis [20]. Because, the proposed BTN-CPMR approach reduced the TPT (ms), FTDT (ms), and increased the FTDA (%).

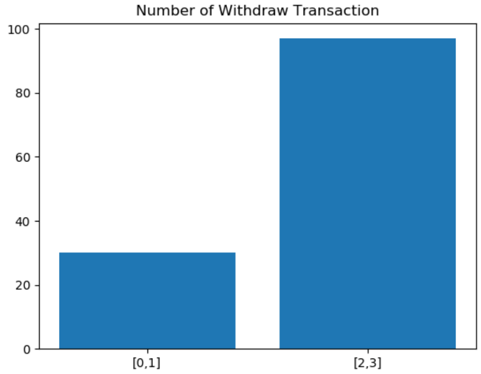


Fig. 6: Number of withdraw transactions.

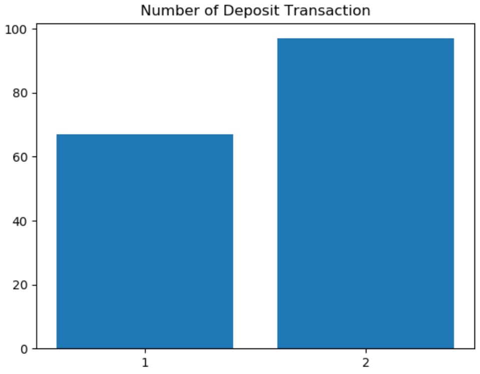


Fig. 7: Number of withdraw transactions.

Table. 1: Performance comparison.

Method	FTDA (%)	TPT (ms)	FTDT (ms)
BAC [10]	91.056	43.614	42.516
BitIodine [13]	92.969	21.661	35.905
BlockChainVis [20]	93.636	17.308	17.456
Proposed BTN-CPMR	98.927	9.352	8.440

5. CONCLUSION

The primary emphasis of this effort was placed on the construction of the BTN-CPMP. In the beginning, the dataset is preprocessed so that any missing symbols or unfamiliar characters in the forensic blockchain dataset may be located and accounted for. The preprocessed dataset is then subjected to a Petri-Net model application, which detects attributes such as the time stamp, transaction id, work tera hash, and work error. The Petri-Net model was primarily used in order to construct and parse the BTN model. The PMR criteria needed to extract the transaction addresses together with the time stamp data are then generated. Therefore, PMR is able to identify illicit payment addresses by comparing the known data with illegal addresses (spam addresses). In addition, a CPMR is used in order to identify fraudulent transactions. This PMR keeps a record of all unlawful payment addresses that have been identified in the past. Therefore, for every new transaction, CPMR will disregard all of those previously recorded (detected) unlawful payment addresses. This will protect the integrity of the network. This phenomenon produces a decrease in the amount of time needed to identify fraudulent transactions, resulting in a speedup of the processing. According to the results of the simulations, the proposed method led to a reduction in the amount of time required for the processing of transactions i.e., TPT, the amount of time required to detect fraudulent transactions i.e., FTDT, and an improvement in the FTDA when compared to the conventional methods. Further, this work can be extended with deep learning models for improved performance.

REFERENCES

[1] S. Nakamoto, "Bitcoin: A peer-to-peer electronic cash system," 2008.

[2] D. Bryans, "Bitcoin and money laundering: mining for an effective solution," Indiana Law Journal, vol. 89, pp. 1-33, 2014.

[3] M. J. Barratt, "SILK ROAD: EBAY FOR DRUGS: The journal publishes both invited and unsolicited letters," Addiction, vol. 107, pp. 683-683, 2012.

[4] M. Dittus, J. Wright, and M. Graham, "Platform Criminalism: The'lastmile'geography of the darknet market supply chain," in proceedings of the 2018 World Wide Web Conference on World Wide Web, 2018, pp. 277- 286.

[5] G. White. UK company linked to laundered Bitcoin billions, BBC, (2018). Available: https://www.bbc.com/news/technology-43291026

[6] N. J. Ajello, "Fitting a Square Peg in a Round Hole: Bitcoin, Money Laundering, and the Fifth Amendment Privilege Against SelfIncrimination," Brooklyn Law Review, vol. 80, p. 4, 2015.

[7] P. Reynolds and A. S.M. Irwin, "Tracking digital footprints: anonymity within the bitcoin system," Journal of Money Laundering Control, vol. 20, pp. 172-189, 2017.

[8] F. Reid and M. Harrigan, "An Analysis of Anonymity in the Bitcoin System," in proceedings of 2011 IEEE Third International Conference on Privacy, Security, Risk and Trust and 2011 IEEE Third International Conference on Social Computing, 2011, pp. 1318-1326.

[9] S. Göbel, A Polynomial Translation of Mobile Ambients Into Safe Petri Nets: Understanding a Calculus of Hierarchical Protection Domains: Springer, 2016.

[10] D. Ron and A. Shamir, "Quantitative Analysis of the Full Bitcoin Transaction Graph," in proceedings of International Conference on Financial Cryptography and Data Security Berlin, Heidelberg, 2013, pp. 6-24.

[11] M. Fleder, M. S. Kester, and S. Pillai, "Bitcoin transaction graph analysis," arXiv preprint arXiv:1502.01657, 2015.

[12] E. Androulaki, G. O. Karame, M. Roeschlin, T. Scherer, and S. Capkun, "Evaluating User Privacy in Bitcoin," in proceedings of International Conference on Financial Cryptography and Data Security, Berlin, Heidelberg, 2013, pp. 34-51.

[13] S. Meiklejohn, M. Pomarole, G. Jordan, K. Levchenko, D. McCoy, G. M. Voelker, et al., "A fistful of bitcoins: characterizing payments among men with no names," presented at the Proceedings of the 2013 conference on Internet measurement conference, Barcelona, Spain, 2013.

[14] M. Spagnuolo, F. Maggi, and S. Zanero, "BitIodine: Extracting Intelligence from the Bitcoin Network," in proceedings of International Conference on Financial Cryptography and Data Security, Berlin, Heidelberg, 2014, pp. 457-468.

[15] M. Harrigan and C. Fretter, "The unreasonable effectiveness of address clustering," in proceedings of 2016 Intl IEEE Conferences on Ubiquitous Intelligence & Computing, Advanced and Trusted Computing, Scalable Computing and Communications, Cloud and Big Data Computing, Internet of People, and Smart World Congress (UIC/ATC/ScalCom/CBDCom/IoP/SmartWorld), 2016, pp. 368-373.

[16] C. Zhao and Y. Guan, "A GRAPH-BASED INVESTIGATION OF BITCOIN TRANSACTIONS," in proceedings of Advances in Digital Forensics XI, Cham, 2015, pp. 79-95.

[17] D. D. F. Maesa, A. Marino, and L. Ricci, "Uncovering the Bitcoin Blockchain: An Analysis of the Full Users Graph," in proceedings of 2016 IEEE International Conference on Data Science and Advanced Analytics (DSAA), 2016, pp. 537-546.

[18] D. Di Francesco Maesa, A. Marino, and L. Ricci, "Data-driven analysis of Bitcoin properties: exploiting the users graph," International Journal of Data Science and Analytics, September 25 2017.

[19] M. Ober, S. Katzenbeisser, and K. Hamacher, "Structure and anonymityof the bitcoin transaction graph," Future internet, vol. 5, pp. 237-250, 2013.

[20] A. Pinna, R. Tonelli, M. Orrú, and M. Marchesi, "A Petri Nets Model for Blockchain Analysis," arXiv preprint arXiv:1709.07790, 2017.

[21] A. Pinna, "A Petri Net-based Model for Investigating Disposable Addresses in Bitcoin System," in proceedings of Knowledge Discovery on the WEB, 2016, pp. 1-4.

[22] J. V. Monaco, "Identifying Bitcoin users by transaction behavior," in proceedings of SPIE Defense + Security, 2015, p. 15.

[23] M. A. Harlev, H. Sun Yin, K. C. Langenheldt, R. Mukkamala, and R. Vatrapu, "Breaking Bad: De-Anonymising Entity Types on the Bitcoin Blockchain Using Supervised Machine Learning," in proceedings of the51st Hawaii International Conference on System Sciences, 2018, pp. 1-10.

[24] M. Möser, R. Böhme, and D. Breuker, "An inquiry into money laundering tools in the Bitcoin ecosystem," in proceedings of APWG eCrime Researchers Summit, 2013, pp. 1-14.

[25] G. D. Battista, V. D. Donato, M. Patrignani, M. Pizzonia, V. Roselli, and R. Tamassia, "Bitconeview: visualization of flows in the bitcoin transaction graph," in proceedings of IEEE Symposium on Visualization for Cyber Security (VizSec), 2015, pp. 1-8.

[26] N. Christin, "Traveling the silk road: a measurement analysis of a large anonymous online marketplace," presented at the Proceedings of the 22nd international conference on World Wide Web, Rio de Janeiro, Brazil, 2013.

[27] D. Kondor, M. Pósfai, I. Csabai, and G. Vattay, "Do the rich get richer? An empirical analysis of the Bitcoin transaction network," PloS one, vol. 9, pp. 1-10, 2014.

[28] D. McGinn, D. Birch, D. Akroyd, M. Molina-Solana, Y. Guo, and W. J. Knottenbelt, "Visualizing dynamic bitcoin transaction patterns," Big data, vol. 4, pp. 109-119, 2016.

[29] S. Bistarelli and F. Santini, "Go with the -Bitcoin- Flow, with Visual Analytics," presented at the Proceedings of the 12th International Conference on Availability, Reliability and Security, Reggio Calabria, Italy, 2017.

[30] Y. Wu, A. Luo, and D. Xu, "Forensic Analysis of Bitcoin Transactions,"in proceedings of 2019 IEEE International Conference on Intelligence and Security Informatics (ISI), 2019, pp. 167-169.

[31] ladimolnar. BitcoinDatabaseGenerator, (2017). Available: https://github.com/ladimolnar/BitcoinDatabase Generator

[32] Wikipedia. Mt.Gox, (2019). Available: https://en.wikipedia.org/wiki/Mt._Gox

[33] WizSec. The missing MtGox bitcoins, (2015). Available: https://blog.wizsec.jp/2015/04/the-missing-mtgox-bitcoins.html