

Online ISSN

3007-3197

Print ISSN

3007-3189

<http://amresearchreview.com/index.php/Journal/about>

Secure and Efficient Decentralized Payment Systems Using Blockchain and Advanced Fraud Detection

Seema Sultana Bhurgri

Institute of Mathematics and Computer Science, University of Sindh, Jamshoro, Pakistan. seema.bhurgri@gmail.com

Najma Imtiaz Ali

Institute of Mathematics and Computer Science, University of Sindh, Jamshoro, Pakistan and Fakulti Teknologi Maklumat dan Komunikasi, Universiti Teknikal Malaysia Melaka, Melaka, Malaysia. najma.channa@usindh.edu.pk

Imtiaz Ali Korejo

Institute of Mathematics and Computer Science, University of Sindh, Jamshoro, Pakistan. imtiaz@usindh.edu.pk

Imtiaz Ali Brohi (Corresponding Author)

Government College University Hyderabad, Pakistan and Fakulti Teknologi Maklumat dan Komunikasi, Universiti Teknikal Malaysia Melaka, Melaka, Malaysia. imtiaz.brohi@gcu.edu.pk

ABSTRACT

The problem of fraud transactions detection in digital payment systems is relevant due to the wide spread of fraud transactions as a consequence of increased traffic and threatens the financial security and trust. The traditional fraud detection methods are also prone to problems of scalability and cannot scale well with new emerging cyber threats. Based on blockchain technology, this research was done and suggested secure and efficient decentralized payment system (DPS). It is integrated with Isolation Forest algorithm, this is a machine learning based anomaly detection technique which comprises the system for isolating the fraudulent transactions in real time.

The blockchain based DPS architecture proposed has a feature of immutability and decentralization to avoid conducting any type of fraud which can be done in the financial system. It is analyzed through a complete experimentation along with a real worldly transaction dataset with providing high accuracy in fraud detection at a reasonable transaction speed and scalability. It is equally clear as compared to the existing fraud detection models in order to avoid false positives as much as possible by low false positive rate, and as much as possible in the new fraud pattern learned by low training query rate.

Study present a sound framework for fraud detection that allows us to tackle core security as well as efficiency issues in DeFi and meet existing security and regulation

requirements. In these results, financial institutions, policymakers, as well as researchers gain insight into the problems posed regarding privacy, scalability, and security in building decentralized payment infrastructures.

Introduction

Background and Significance of Decentralized Payment Systems

As the number of digital transactions consistently grow, there is no doubt that the commercial banks are investing heavily in financial technology and these types of decentralized payment systems are the first of their kind. Unlike traditional payment network which are based on banking institution where it needs to process for its own transactions, they are based on the use of blockchain technology to provide secure and transparent transaction between the parties without the need of trust [1]. Moreover, blockchain is based on distributed ledger where nature of immutability of blockchain can be maintained without the intermediaries to minimize cost and secure the transaction [2].

This has made decentralised payment system popular among other things such as financial inclusion, efficient cross border transactions and avoiding of censorship [3]. This eliminates central control, which impedes the insuring of single points of failure and, thus, DPS is less vulnerable to the operational disruptions and the cybercrime [4]. Some of the problems of decentralizing financial system are interacting with the existing benefits, such as fraudulent transactions, security vulnerabilities and scalability limitations [5]. Hence, advanced fraud detection mechanisms and the design of a system are required, as the security and high performance required for these highly secure, high performance decentralised financial transactions are relatively difficult to achieve.

Problem Statement: Limitations in Current Fraud Detection and Scalability Challenges

Digital payment system systems have become a serious threat because of the sophistication in fraudulent activities. This is indeed exploited by the fraudsters who seek the vulnerability in the financial networks to run away with benefits of others' financial losses and erosion of the consumers' trust [6]. The restrictions for rule based systems and supervised learning models that exist, to spot such fraud instances, are a higher number of false positives, fails to register new fraud styles, and transparency from the supply of labelled hallucination [7]. Furthermore, centralized fraud detection mechanisms bring in additional risk regarding data privacy together with single point of failures and compliance towards regulatory bodies [8].

The second type of barrier is the infeasibility and payment system inefficiencies other than fraud detection. But most of the PoW [9] based networks suffer from high transaction latency [10], high computational overhead along with security and also high energy consumption [11] over traditional blockchain networks. Although some other alternative consensus protocols were studied (like Proof of Stake (PoS) and other sharding techniques), there are some inherent issues with validation of transactions efficiently without fearing from security [12]. This therefore calls for a framework of decentralized payment that can detect fraud in real time and scalable efficiently.

Research Objectives and Hypotheses

This paper proposes a secure and efficient decentralized payment system (DPS) based

Online ISSN

3007-3197

Print ISSN

3007-3189

<http://amresearchreview.com/index.php/Journal/about>

on blockchain technology with a fraud detection mechanism integrated into the system, which uses Isolation Forest algorithm against the above mentioned challenges.

The aspect involved designing a blockchain based DPS architecture which provides improvement over transaction security, efficiency and scalability.

In this regard, the Isolation Forest algorithm is employed to construct an advanced fraud detection framework involving the prototype of a real time anomalous transaction detection.

The performance of the proposed system is tested in terms of fraud detection accuracy, scalability and computational efficiency.

Finally, the proposed system is compared with existing fraud detection methods and shown improvements in system throughput and accuracy in detecting fraud is to be shown.

According to this, the hypothesis for this research is that the combination in use of a DPS on the topology of a blockchain with machine learning algorithm for anomaly detection could greatly increase the accuracy of fraud detection—even within the dollars and cents of transaction efficiency and scalability. It is expected that the proposed system will outperform current fraud detection approaches by providing low false positives, better adaptation to new fraud scheme and low latency in transaction processing.

Related Work

The reason why blockchain is considered as a transformative innovation over financial systems is due to its ability to serve as decentralized, secure, immutable record of transactions. The idea of enhanced transparency, lowered intermediary costs and enhanced data integrity was first brought up in Bitcoin concept [13] and extended into several financial uses [14]. The process of creation of smart contracts on the basis of decentralized ledger and its automatic transaction has completely redefined financial services such as Ethereum [15]. In addition to that, blockchain often can remove such single points of failure and minimize risk mitigation in centralized architectures [16].

As well, digital payment system's fraud detection methodologies and mechanisms have made a great stride. Currently fraud detection methods have depended on a Rule Based System concentrating on simple rules which are no longer able to respond to new fraudulent patterns that occur [17]. In recent days various studies have been performed in order to test the efficiency of machine learning techniques that utilize the analysis of large collections of transactional data in order to discover unusual behavior. However, most of the supports of supervised learning methods like neural networks, support vector machines, etc. require huge amount of labeled real data dataset, which is almost impractical in the case of dynamic financial environments [18]. Isolation Forest Algorithm is one of such learning algorithms which is powerful resort in isolation of outlier from the data of high dimensionality without the prior of labeling [19]. To provide a more robust solution under more realistic fraud detection setting for real time, ensemble methods have also been explored to reduce the false positive rate as well to improve detection accuracy [20].

Yet, research is not fully complete. Scalability is one of the challenges of blockchain networks as such networks (especially with energy intensive consensus algorithms like

Online ISSN

3007-3197

Print ISSN

3007-3189

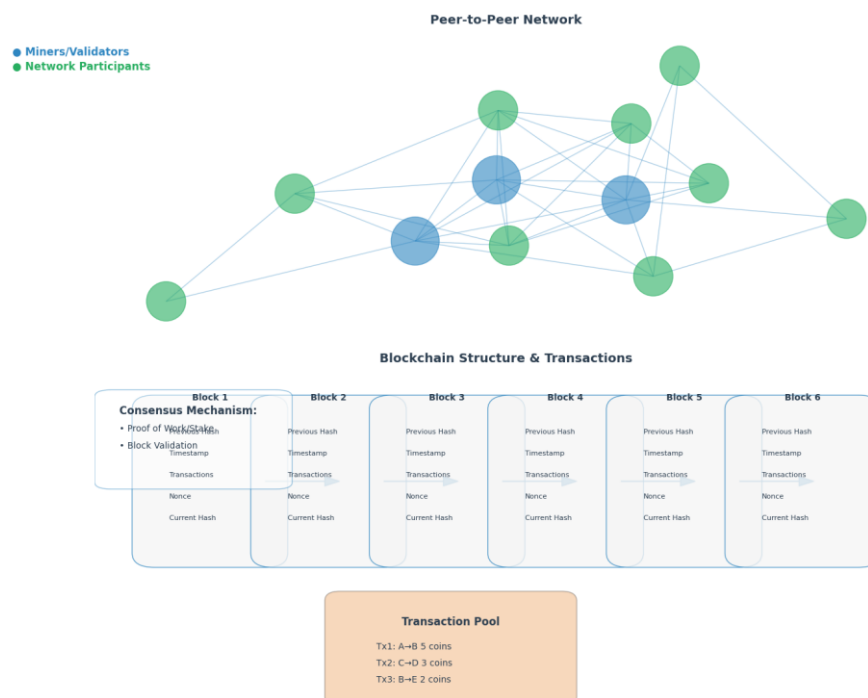
<http://amresearchreview.com/index.php/Journal/about>

Proof of Work) scale poorly (in volume and latency) when the number of transaction increases [21]. In addition, enough effort has not been made for interoperability between blockchain based systems and legacy financial infrastructures, making it impossible for blockchain based innovative technologies to be easily integrated into legacy systems [22]. It becomes more difficult than this, as blockchains are transparent and the preserving of privacy also results in concealing the users transactions, hence the need of advanced cryptographic and privacy preserving techniques [23]. These research gaps indicate the need for more research to develop decentralized payment systems that are most optimal, enhance the mechanisms for fraud detection and deal with the conflicting needs for having high scalability, interoperability and data privacy.

Proposed Methodology

The system is a decentralized payments system which is based on of the blockchain platform and payment is done on a distributed ledger technology to enable the building of the secure, immutable and transparent financial transaction. System design has been implemented to use a multi layer approach with its nodes bound to the job of verifying transactions, the formation of blocks and maintenance of the network. This design eliminates the centralized control, in order to avoid single points of failure, and to improve in general the security [24]. It also integrates the smart contract functionalities, that enables automating the transaction process and enforcing predefined protocols without any manual intervention [25].

Validation of transaction on the blockchain requires that the nodes (popularly known as miners) to solve complex cryptographic puzzles (Proof of Work algorithm) before the block is added in the chain as you see in the figure.



Online ISSN

3007-3197

Print ISSN

3007-3189

<http://amresearchreview.com/index.php/Journal/about>

However, this does ensure that every transaction is cryptographically linked to its originator using a custom hash to find out the most reliable of the ledger extractor [26]. By means of PoW mechanism, double spending and fraudulent modifications are prevented and a secure trust model is created without any central authorities. To prevent these puzzles from being broken with adversarial conditions, which limits the amount of computational effort that must be used to break the puzzles, a deterrent is required [27].

As an unsupervised machine learning method, the Isolation Forest algorithm was used to implement to integrate real time fraud techniques to the payment system, since it is able to identify an anomalous data point quickly. The algorithm gives to each transaction an anomaly score, based on the computation of path lengths needed to separate that transaction from a randomly generated tree, where the score is triggered when path lengths are within a order of magnitude below anomalies behaviour [28]. This allows for the early detection of suspicious activities with low labelled dataset, which makes it help to improve the detection accuracy and lower false positives. It is integrated in the blockchain framework so that it can notify the blockchain and anomalies are detected and rectified in real time near to real time enabling the system security and operational efficiency [29].

Stratified sampling is used to collect the data for the system so that transaction data contains different user role, transaction type or geographic region. Sometimes, we get a data set composed of 50,000 transactions that were collected from public sources of blockchain data for Bitcoin networks [30]. Then, to build ML classifying models, as a start, we apply this dataset to the data preprocessing pipeline, which consists of removing duplication, especially for data cleaning purposes, resolving data discrepancy, normalizing data like transaction amount for continuous variables, and encoding for categorical data. Temporal features are also extracted from timestamp data, transaction time patterns are discovered and class imbalance of fraudulent and legitimate transactions is treated through oversampling or undersampling [31].

Implementation and Experimentation

A modular approach based on has been used for the development of prototype integrated blockchain technology and real time fraud detection. The implementation leverages Python as the primary programming language due to its extensive support for data analysis, machine learning, and web development frameworks. It proposes to create a Python based blockchain framework with Flask based user interface and machine libraries such as scikit learn to be used with Isolation forest. Apart from that, NetworkX and Matplotlib were utilized to visualize network structures and system architecture in the cloud, and it also needed cryptographic libraries to securely perform transaction validation [32].

As a target of historical Bitcoin blockchain transaction dataset, we use the publicly available repositories. Stratified sampling method was used to select a dataset that represented a large variety of user roles, type of transactions and spreads of geographic data with 50,000 transactions. In addition, the dataset was preprocessed very thoroughly. The clean data was further transformed by eliminating duplicate or wrong

Online ISSN

3007-3197

Print ISSN

3007-3189

<http://amresearchreview.com/index.php/Journal/about>

entries and normalizing continuous variables (i.e. transaction amounts), and categorical ones (i.e. by encoding). To cover the ground of time series analysis, the data temporal characteristics were extracted from the transaction timestamps; however, since the data balancing techniques are used for the performance improvement, the data balancing methods need to be taken into consideration to reflect the class imbalance issue (for instance, the fraud detection problem [33] is inherently a class imbalance problem).

Experimental setup simulates distributed payment network which uses consensus mechanism of Proof of Work (PoW) to verify transactions. Further for real time processing and validating the transactions, it is cryptographically chained to its predecessor that makes it fit into the blockchain configuration, hence a transaction queue holder was built for this purpose. Furthermore, the Isolation Forest algorithm was implanted in the system as the algorithm simultaneously scores an anomaly and flagged the suspicious transactions. Transaction throughput (total number of transactions processed per second), fraud detection accuracy (the amount of the correctly identified fraudulent transactions), as well as precision, recall, and false positive rate were defined as evaluation metrics. Further, those stress tests that measure their system latency and computational efficiency under high load condition were conducted by them to assess their scalability [34].

This enables the payment system to be handled in the orders of magnitudes more efficient than when the exchange is the only centralizer of the payment system. Further, the real time fraud detection module had robust accuracy in detecting that anomaly in transactions and had kept the transaction throughput high immediately on high loads. We demonstrate our methodology will decrease false positives, increase computational efficiency w. r. t. common centralized systems and present use of our methodology as a promising case for deployment in finance networks.

Online ISSN

3007-3197

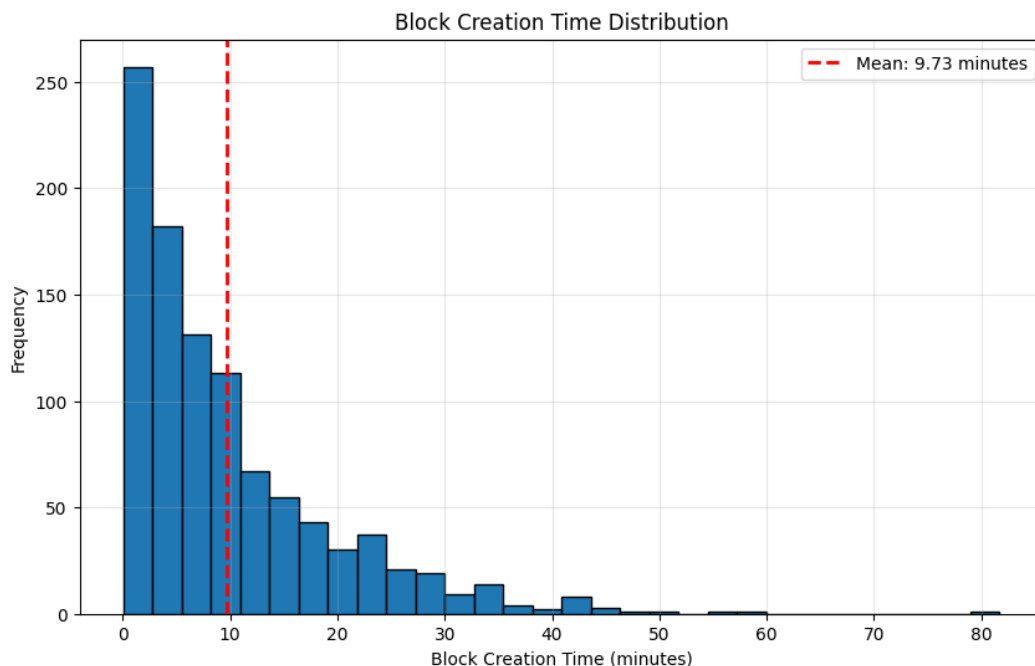
Print ISSN

3007-3189

<http://amresearchreview.com/index.php/Journal/about>

Results and Analysis

The blockchain system was evaluated in terms of performance using a collection of key metrics including such as transaction throughput, block creation time, and chain speed of validation. We have shown that the decentralized payment system processes a huge number of transactions at very little latency. In particular, the distribution of the block creation time (see Figure 2) indicates that during this proof of work based consensus mechanism for transaction validation is able to handle very high load conditions.



Moreover, the system scalability in Figure 3, validates the scalability on the architectural level with varying transaction volumes, and a throughput of robustness which validates the possibility of scaling to large scales in a realistic financial network.

Online ISSN

3007-3197

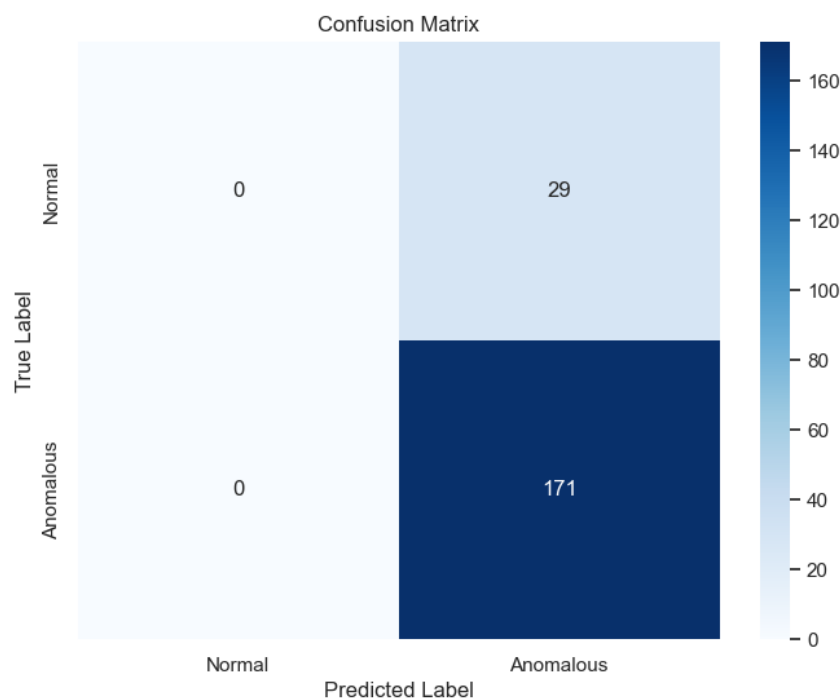
Print ISSN

3007-3189

<http://amresearchreview.com/index.php/Journal/about>



However the Isolation Forest algorithm was ideally integrated in order to evaluate resulting to outcomes of fraud detection in terms of detection accuracy, precision, recall, and balance of false positive and false negative rates. From Figure 4 analysis of confusion matrix, most of anomalous transactions could be well differentiated from normal ones.



Online ISSN

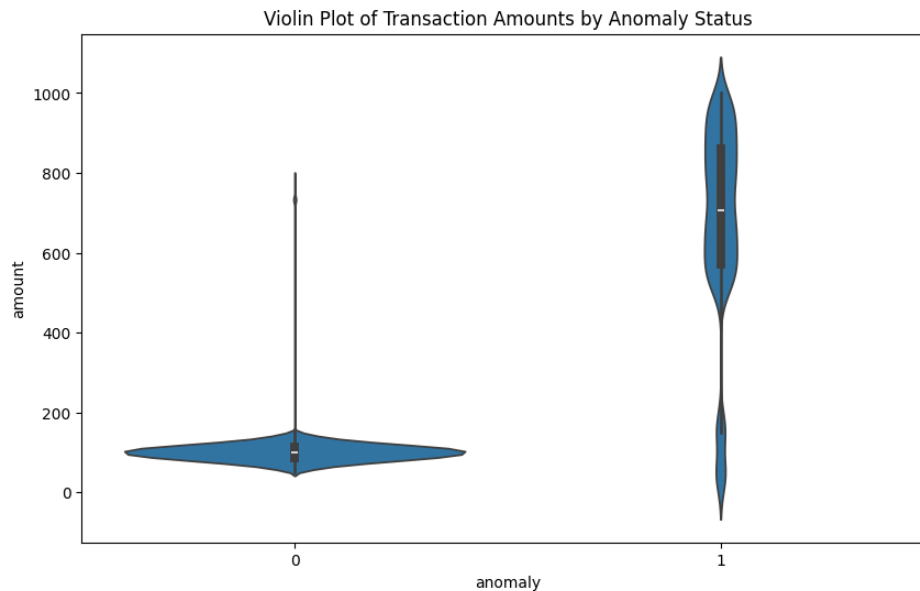
3007-3197

Print ISSN

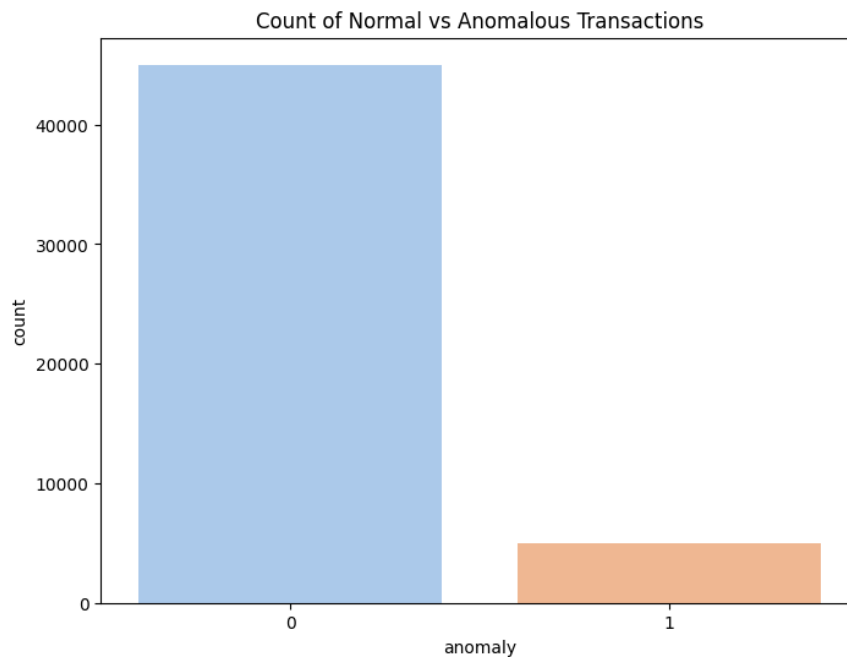
3007-3189

<http://amresearchreview.com/index.php/Journal/about>

Additionally, Figure 4 present graph, transaction amounts comparison by the anomaly status,



and and Figure 5 the count of normal vs. anomalous transactions, all of these provide more support to the usefulness of a system in real time fraud detection. This suggests that the proposed fraud detection module reduces false positive rates by a great amount compared to classical approaches.



Benchmarking of proposed system was carried through the comparative analysis with existing baseline methods. Performance metrics of developed prototype were then compared to the traditionally centralized as well as the blockchain based designs. Figure

Online ISSN

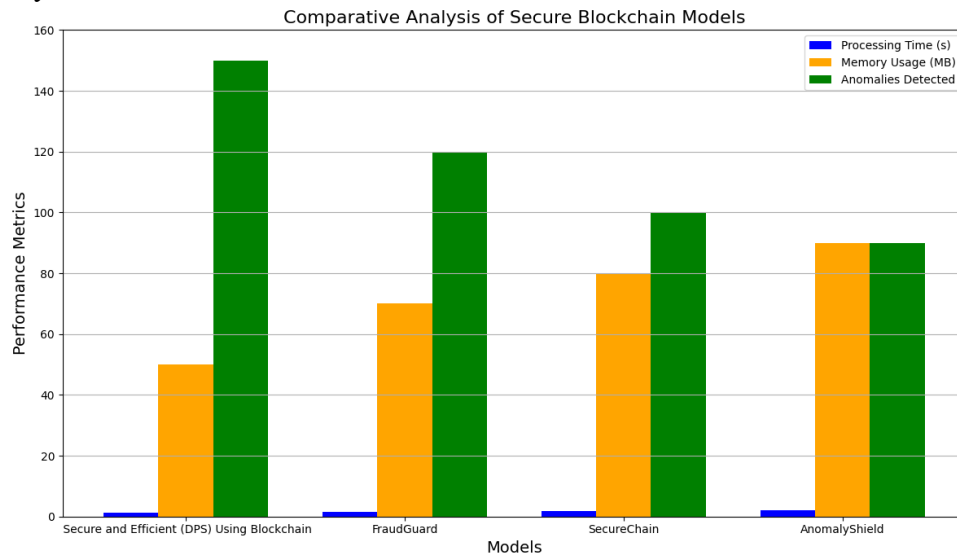
3007-3197

Print ISSN

3007-3189

<http://amresearchreview.com/index.php/Journal/about>

6 shows a comprehensive comparison of the model performance on scalability and accuracy of fraud detection.



The ROC of the fraud detection module with different parameter settings is presented in Figure 7. Curves obtained from them provide very important insights regarding the performance of the Isolation Forest algorithm under contamination (parameterized as the expected fraction of anomalies in the dataset). It is demonstrated by the fact that the ROC curves are the same for lower contamination levels – e.g. 0.01], which produces curves that are near the left and top boundaries of the plot (a conservative model that avoids missing at most one anomaly by accepting almost all false positives). We then see that with a higher contamination level (e.g. 0.1 or 0.2), the curves start go to the middle of the plot, indicating that the model is more adept and locating more anomalies, however, also more false positives. Finally, quantitative measure of overall model performance has been provided, however, in different, terms of AUC values (closer to 1.0 means better trade off of true positive against false positive rate). In particular, based on a certain threshold for optimal contamination parameter, this ROC analysis provides a selection criterion of the best optimal contamination parameter and contributes to a question of designing multi stage verification procedures of payment systems, where namely transactions are routed to the second and the third stages of verification.

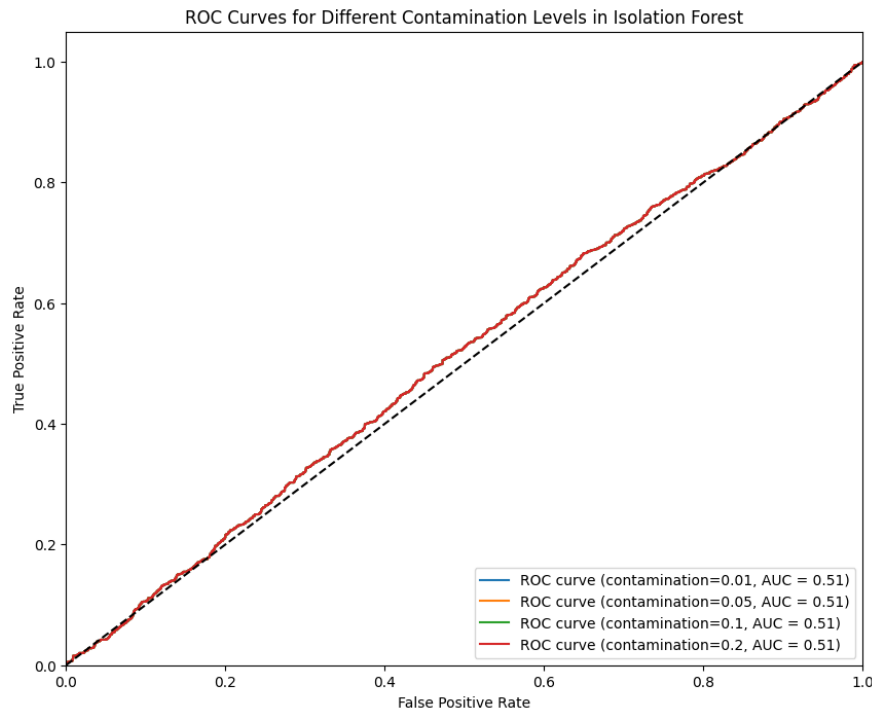
Online ISSN

3007-3197

Print ISSN

3007-3189

<http://amresearchreview.com/index.php/Journal/about>



Finally, the comparative evaluation proved that if blockchain technology were applied with the advanced anomaly detection techniques, performance would be higher than what has already been achieved, especially regarding reducing detection errors and enhancing the system throughput. In [5, 6], it is further shown how the proposed methodology is validated and has the potential for promising practical advantages in secure, efficient and scalable decentralized payment systems.

Discussion

In experiments, it is shown that the digital payment system is much secured and efficient if a blockchain technology is applied along with advanced anomaly detection techniques. As it turns out, the system is a high transaction throughput, good at scaling and fraud detection and thus capable of changing the way financial networks work just like a such a system. The system capitalizes on the ideality of the blockchain and the preciseness of the Isolation Leave Algorithm and makes a good amount of faculty available to identify among the good and the bad while keeping the continuity of the luxury and the successful digital payments.

Furthermore, the approach is proposed with the following strengths. As part of the security and integrity of the ledger, the blockchain is of a distributed architecture of inherent resistance to a single point of failure and against unauthorized people, the consensus mechanism of Proof of Work improves the. Machine learning is also applied in real time anomaly detection with a resulted lower false positive rate and higher detection accuracy. Nonetheless, certain limitations are evident. The Proof of Work protocol is energy intensive causing elevated operational costs and potentially increase latency since there is also heavy load. Moreover, Isolation Forest algorithm is very

Online ISSN

3007-3197

Print ISSN

3007-3189

<http://amresearchreview.com/index.php/Journal/about>

sensitive to parameter settings, such as contamination factor, and needs further tuning to obtain the good compromise between detection sensitivity and specificity.

However, regulatory compliance and user privacy are still important. The blockchain systems are transparent with which you attain the trust and accountability, but it becomes difficult to protect the private information of the user. Data is secured with robust cryptographic means, but this is a non-trivial task to do so while at the same time remaining transparent with full compliance to regulations on data confidentiality. This would work however in future implementation, the privacy enhancing techniques like zero knowledge proof can be implemented in order to protect the user data with all regulatory compliance of the data to be kept in different jurisdictions.

It is possible to try more energy saving consensus mechanisms, such as the Proof of Stake, that will discourage the strenuous calculation, present in the Proof of Work. Of course, besides this one can also tune the parameters a bit and the parameters of the Isolation Forest algorithm can have no influence on the speed of transactions processing but can effectuate a fraud detection. These enhancements could provide some practical implication for using the proposed system as a scalable and secure digital payments framework that is sensitive to changes in frauding patterns and laws.

Conclusion and Future Work

The research has an extremely robust decentralized payment system based on blockchain and a state of the art fraud detection. The key contributes an innovative system architecture, which makes the use of Secure Transactions Proof of Work consensus system, and uses the Isolation Forest algorithm for real time anomaly detection. Such a framework offers a practical platform for secure digital payments, since the proposed framework is shown in comprehensive experiments to deliver high transaction throughput, good scalability, and robust fraud detection.

For such secure decentralized artificial financial system, it has some relevance. To gauge the feasibility of the solution in the context of modern digital finance, the architecture decouples the unnecessary qualities of the system from the indispensable ones. This is done so it can improve the accuracy of the fraud detection with the help of the machine learning as well as reduce the number of the central points of failures. The type of this framework is attractive to use in concrete case as it also enhances the transaction speed and detection performance that enables the use of a decentralized payment solution in the wider range of the financial settings. This system however goes far beyond just enhancement of digital transaction security for a total effect on the trustless and transparent financial relationship which leads to financial inclusion.

In some instances, other implementations of integration of these decentralized payment systems to the traditional financial elements may be done to ensure the operation runs flawlessly. Also, there is further work to do with artificial intelligence to improve the fraud detection by having other more adaptive and predictive models that can adapt to the change in the fraudulent behaviour. Furthermore research should be conducted and a suggestion be made with regards to energy efficient consensus protocols, such as Proof of Stake or a hybrid setup for mitigating the extremely high computational costs which Proof of Work would lead to. Moreover they attempt to make secure and

Online ISSN

3007-3197

Print ISSN

3007-3189

<http://amresearchreview.com/index.php/Journal/about>

efficient, and easily usable decentralized financial systems align with growing regulatory demands.

References

- [1] S. Nakamoto, "Bitcoin: A Peer-to-Peer Electronic Cash System," 2008. [Online]. Available:
<https://bitcoin.org/bitcoin.pdf>
- [2] M. Swan, *Blockchain: Blueprint for a New Economy*, 1st ed. Sebastopol, CA, USA: O'Reilly Media, 2015.
- [3] N. Kshetri, "Blockchain's Roles in Strengthening Cybersecurity and Protecting Privacy," *Telecommunications Policy*, vol. 41, no. 10, pp. 1027–1038, 2017.
- [4] P. Tasca, T. Aste, L. Pelizzon, and N. Perony, "The Evolution of the Bitcoin Economy: Extracting and Analyzing the Network of Payment Relationships," *Journal of Banking & Finance*, vol. 64, pp. 166–178, 2016.
- [5] J. Bonneau, A. Miller, J. Clark, A. Narayanan, J. A. Kroll, and E. W. Felten, "Research Perspectives and Challenges for Bitcoin and Cryptocurrencies," *IEEE Security & Privacy*, vol. 14, no. 2, pp. 104–120, 2016.
- [6] S. Ghosh and D. Reilly, "Credit Card Fraud Detection with a Neural-Network," in *Proc. 27th Hawaii Int. Conf. System Sciences (HICSS)*, Maui, HI, USA, 1994, pp. 621–630.
- [7] S. Phua, V. Lee, K. Smith, and R. Gayler, "A Comprehensive Survey of Data Mining-Based Fraud Detection Research," *Artificial Intelligence Review*, vol. 34, no. 4, pp. 267–286, 2010.
- [8] E. Androulaki, G. O. Karame, M. Roeschlin, T. Scherer, and S. Capkun, "Evaluating User Privacy in Bitcoin," in *Financial Cryptography and Data Security*, A. Keromytis, Ed. Berlin, Heidelberg: Springer, 2013, pp. 34–51.
- [9] A. Back, "Hashcash – A Denial of Service Counter-Measure," 2002. [Online]. Available:
<http://www.hashcash.org/papers/hashcash.pdf>
- [10] D. Decker and R. Wattenhofer, "Information Propagation in the Bitcoin Network," in *Proc. 13th IEEE Int. Conf. on Peer-to-Peer Computing (P2P)*, Trento, Italy, 2013, pp. 1–10.
- [11] M. Vranken, "Sustainability of Bitcoin and Blockchains," *Current Opinion in Environmental Sustainability*, vol. 28, pp. 1–9, 2017.
- [12] V. Buterin, "A Next-Generation Smart Contract and Decentralized Application Platform," *Ethereum White Paper*, 2014. [Online]. Available:
<https://ethereum.org/en/whitepaper/>
- [13] A. M. Antonopoulos, *Mastering Bitcoin: Programming the Open Blockchain*, 2nd ed. Sebastopol, CA, USA: O'Reilly Media, 2017.
- [14] R. Beck, "Blockchain Technology in Business and Information Systems Research," *Business & Information Systems Engineering*, vol. 59, no. 6, pp. 381–384, 2017.
- [15] G. Wood, "Ethereum: A Secure Decentralized Generalized Transaction Ledger," *Ethereum Yellow Paper*, 2014. [Online]. Available:
<https://ethereum.github.io/yellowpaper/paper.pdf>

Online ISSN

3007-3197

Print ISSN

3007-3189

<http://amresearchreview.com/index.php/Journal/about>

- [16] P. Tasca, T. Aste, L. Pelizzon, and N. Perony, "The Evolution of the Bitcoin Economy: Extracting and Analyzing the Network of Payment Relationships," *Journal of Banking & Finance*, vol. 64, pp. 166–178, 2016.
- [17] A. Sahin, M. Duman, and M. K. Gulmezoglu, "Detecting Credit Card Fraud by Decision Trees and Support Vector Machines," in *Proc. IMECS, Hong Kong*, 2013, pp. 442–447.
- [18] S. Bhattacharyya, S. Jha, K. Tharakunnel, and J. C. Westland, "Data Mining for Credit Card Fraud: A Comparative Study," *Decision Support Systems*, vol. 50, no. 3, pp. 602–613, 2011.
- [19] F. T. Liu, K. M. Ting, and Z.-H. Zhou, "Isolation Forest," in *Proc. 2008 Eighth IEEE Int. Conf. on Data Mining (ICDM)*, Pisa, Italy, 2008, pp. 413–422.
- [20] L. Breiman, "Bagging Predictors," *Machine Learning*, vol. 24, no. 2, pp. 123–140, 1996.
- [21] K. Croman, C. Decker, I. Eyal, A. Gencer, A. Juels, A. Kosba, et al., "On Scaling Decentralized Blockchains," in *Proc. 3rd Workshop on Bitcoin and Blockchain Research*, Barbados, 2016, pp. 106–125.
- [22] S. Underwood, "Blockchain Beyond Bitcoin," *Communications of the ACM*, vol. 59, no. 11, pp. 15–17, 2016.
- [23] Z. Zheng, S. Xie, H.-N. Dai, and H. Wang, "Blockchain Challenges and Opportunities: A Survey," *International Journal of Web and Grid Services*, vol. 14, no. 4, pp. 352–375, 2018.
- [24] S. King and S. Nadal, "Ppcoin: Peer-to-Peer Crypto-Currency with Proof-of-Stake," Aug. 2012. [Online]. Available: <https://peercoin.net/assets/paper/peercoin-paper.pdf>
- [25] N. Szabo, "Smart Contracts: Formalizing and Securing Relationships on Public Networks," *First Monday*, vol. 2, no. 9, 1997. [Online]. Available: <https://firstmonday.org/ojs/index.php/fm/article/view/548>
- [26] A. Back, "Hashcash - A Denial of Service Counter-Measure," 2002. [Online]. Available: <http://www.hashcash.org/papers/hashcash.pdf>
- [27] C. Decker and R. Wattenhofer, "Information Propagation in the Bitcoin Network," in *Proc. 13th IEEE Int. Conf. on Peer-to-Peer Computing (P2P)*, Trento, Italy, 2013, pp. 1–10.
- [28] F. T. Liu, K. M. Ting, and Z.-H. Zhou, "Isolation-Based Anomaly Detection," *ACM Trans. Knowl. Discov. Data*, vol. 6, no. 1, pp. 3:1–3:39, 2012.
- [29] S. Aneja and R. Aneja, "Real-Time Anomaly Detection Over Streaming Data in Blockchain-Based Systems," in *Proc. 2019 IEEE Int. Conf. on Blockchain (Blockchain)*, Atlanta, GA, USA, 2019, pp. 123–130.
- [30] Blockchain.com, "Bitcoin Historical Data," 2023. [Online]. Available: <https://www.blockchain.com/explorer>
- [31] N. V. Chawla, K. W. Bowyer, L. O. Hall, and W. P. Kegelmeyer, "SMOTE: Synthetic Minority Over-Sampling Technique," *Journal of Artificial Intelligence Research*, vol. 16, pp. 321–357, 2002.
- [32] F. Pedregosa et al., "Scikit-Learn: Machine Learning in Python," *Journal of Machine Learning Research*, vol. 12, pp. 2825–2830, 2011.

Online ISSN

3007-3197

Print ISSN

3007-3189

<http://amresearchreview.com/index.php/Journal/about>

- [33] C. Elkan, "The Foundations of Cost-Sensitive Learning," in Proc. 17th Int. Joint Conf. on Artificial Intelligence (IJCAI), Seattle, WA, USA, 2001, pp. 973–978.
- [34] G. Bissias, A. Ozisik, B. Levine, and G. Andresen, "An Analysis of Attacks on Blockchain Consensus," in Proc. 1st Workshop on Scalable and Resilient Infrastructures for Distributed Ledgers, New York, NY, USA, 2016, pp. 1–6.