Crypto Map AI A Machine Learning-Based System for Fraud Detection in Cryptocurrency Transactions using ChainGuard-V1 Engine

Sanskruti Pawar[1], Rushikesh Tokle[2], Akshay Walunjkar[3], Karan Shingade[4]
[1,2,3,4]*Sinhgad Institute of Technology and Science Pune, India*

***Abstract*—The surge in cryptocurrency adoption has redefined digital finance, introduced decentralization and transparency but also facilitated illicit activities such as drug trafficking and money laundering. The pseudonymous nature of digital assets like Bitcoin, Ethereum, and Monero poses major challenges for law-enforcement agencies in tracing the real identities behind suspicious wallet activities. This research proposes CryptoMapAI, an AI-driven framework designed to trace cryptocurrency trans-actions to their final destinations and uncover hidden criminal networks. The system integrates blockchain data from public and privacy-centric networks with external intelligence sources including darknet markets and flagged wallet databases. Using machine learning, graph analytics, and recursive clustering, CryptoMapAI identifies obfuscated transaction flows across mixers, tumblers, and cross-chain transfers. The model employs Random Forest and anomaly detection algorithms to classify suspicious activities and visualize the complete transaction net-work through an intuitive dashboard. Experimental results demonstrate a detection accuracy of 99%, enabling efficient identification of high-risk wallets and transaction patterns.**

***Index Terms*—Artificial Intelligence, Blockchain Forensics, Cryptocurrency Tracing, Money Laundering Detection, Graph Analytics, Machine Learning**

I. INTRODUCTION

The rapid growth of cryptocurrencies has significantly trans-formed the global financial ecosystem by introducing decentralization, transparency, and borderless transactions. Digital assets such as Bitcoin, Ethereum, and Monero have gained immense popularity due to their ability to facilitate secure peer-to-peer exchanges without intermediaries. However, this technological advancement has also created new challenges in cybersecurity and financial regulation. The pseudonymous and decentralized nature of cryptocurrencies has made them a preferred medium for illicit activities, including money laundering, drug trafficking, fraud, and ransomware payments. Law-enforcement agencies face growing difficulties in tracing suspicious cryptocurrency transactions due to the complexity of blockchain networks and the adoption of privacy-enhancing tools such as mixers, tumblers, and cross-chain bridges. These tools allow criminals to obscure the origin, path, and destination of funds, hindering traditional forensic tracking methods. As a result, there is an urgent need for AI-driven analytical systems capable of de-anonymizing transactions and mapping them to real-world entities.

This research introduces CryptoMapAI, an AI-powered blockchain-forensics framework designed to trace cryptocurrency transactions to their final destinations. The system integrates machine learning (ML), graph-based analytics, and recursive clustering techniques to identify patterns, detect anomalies, and flag suspicious activities across multiple blockchain networks. By leveraging data from both transparent blockchains (Bitcoin, Ethereum) and privacy-centric networks (Monero, Zcash), CryptoMapAI provides a holistic approach to tracing digital currency flows.

The proposed system incorporates intelligence from external data sources such as darknet markets, flagged wallets, and known criminal associations,

enhancing its capability to correlate blockchain data with real-world behavior. Through visual transaction mapping and anomaly detection algorithms, CryptoMapAI offers investigators a powerful tool to identify high-risk entities, uncover money-laundering patterns, and assist in anti-money-laundering (AML) enforcement.

II. LITERATURE REVIEW

The rise of cryptocurrencies has driven extensive research into transaction traceability, fraud detection, and regulatory mechanisms. Numerous studies have focused on integrating artificial intelligence (AI) and machine learning (ML) to im-prove the identification of suspicious cryptocurrency activities. Yerram et al. discussed the use of AI-driven systems to analyze cryptocurrency transactions and financial data. How-ever, their approach relied heavily on secondary sources and lacked real-time analytical capabilities, limiting its applicability for live blockchain forensics. Gao proposed using machine learning algorithms and natural language processing (NLP) for identifying counterfeit cryptocurrency transactions on the Ethereum network. Although the model could detect fraudulent patterns, it struggled to distinguish legitimate transactions from fake ones due to high similarity in behavioral features.

Rajput et al. presented an AI-based solution for mitigating transaction malleability in Bitcoin systems. Their work enhanced precision in transaction mapping using blockchain records but faced constraints due to limited datasets and privacy concerns. Yousaf et al. analyzed cross-chain trans-actions using platforms such as Changelly and ShapeShift, providing valuable insights into multi-blockchain transaction behaviors. However, anonymization techniques and limited datasets remained major obstacles.

Several technical studies have contributed to advancing blockchain analytics. Bartoletti et al. developed an open-source scam detection tool using a multi-label classification approach, but it generated high false-positive rates and lacked integration with blockchain query engines for deeper forensic insight. Farg et al. employed gradient boosting, reinforcement learning, and graph neural networks for transaction pattern recognition and market risk prediction. While effective for forecasting, these models lacked the capacity to trace illicit transaction flows across blockchains.

III. PROBLEM STATEMENT

The rapid expansion of cryptocurrency usage has introduced new challenges in financial security and regulatory enforcement. While blockchain technology ensures transparency and immutability, the pseudonymous nature of cryptocurrency transactions provides opportunities for criminal exploitation. Illicit actors increasingly use cryptocurrencies to obscure the origin and destination of funds through advanced anonymization techniques such as mixers, tumblers, coin joins, and cross-chain transfers.

Law enforcement agencies face major difficulties in tracing cryptocurrency transactions, as these methods effectively conceal transactional links, making it nearly impossible to map suspicious wallets to real-world identities using traditional investigation tools. Although blockchain explorers provide visibility into transaction histories, they lack the capability to connect multi-chain transactions and detect complex laundering patterns.

Existing AI-based models in blockchain forensics primarily focus on transaction classification or price prediction rather than transaction traceability and de-anonymization. Most cur-rent solutions are limited to single blockchain networks, rely on static datasets, and do not integrate external intelligence sources such as darknet market data, flagged wallet lists, or KYC-based exchange information. This limits their effective-ness in identifying illicit financial flows that span multiple platforms and privacy layers.

Therefore, there is a critical need for an AI-powered system capable of accurately tracing cryptocurrency transactions

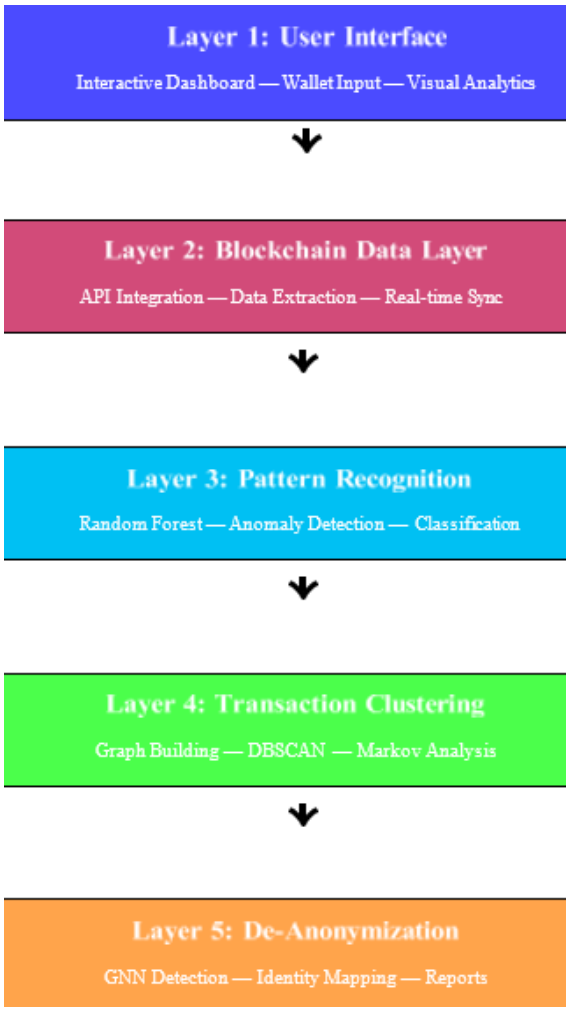

Fig. 1. System architecture of CryptoMapAI showing the five-layer design.

across diverse blockchain networks, detecting obfuscation patterns, and linking pseudonymous wallets to potential real-world entities.

IV. SYSTEM DESIGN AND METHODOLOGY

The CryptoMapAI system is designed to provide an intelligent and automated framework for tracing cryptocurrency transactions across multiple blockchain platforms. The architecture combines machine learning, graph-based analysis, and blockchain data integration to detect suspicious transaction patterns, de-anonymize entities, and map funds to their final destinations.

A. System Architecture

The overall system architecture of CryptoMapAI consists of five major layers as shown in Figure 1. The User Inter-face Layer provides investigators with a secure, interactive dashboard that allows input of wallet addresses, viewing of transaction patterns, and generation of forensic reports. It displays visual representations of transaction graphs, risk scores, and suspicious activity summaries while supporting multiple user roles and authentication.

The Blockchain Data Layer handles data ingestion by collecting raw transaction data from multiple blockchain explorers and APIs such as Blockchain.info, Etherscan, and Monero Explorers. It extracts essential details like wallet addresses, transaction hashes, timestamps, and transaction values, ensuring real-time data synchronization for continuous monitoring.

The Pattern Recognition Layer utilizes Random Forest and Anomaly Detection algorithms to identify irregular trans-action behaviors. It detects suspicious wallet activity such as sudden spikes in transaction volume or frequency and employs Autoencoders and Isolation Forests for recognizing outlier transactions that may indicate laundering or illicit flows.

The Transaction Parsing and Clustering Layer builds transaction graphs that represent wallet-to-wallet relationships. It applies Markov Chain Analysis to trace the probabilistic

1.05

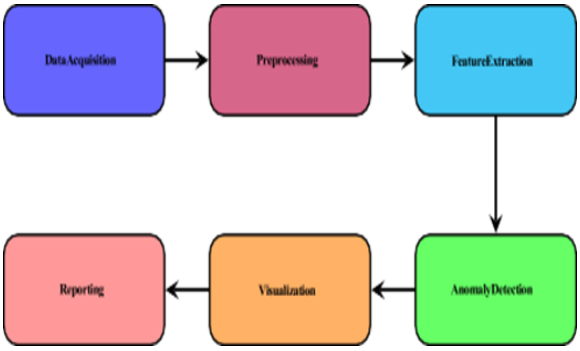

Fig. 2. Transaction tracing workflow in CryptoMapAI.

movement of funds across addresses and uses DBSCAN (Density-Based Spatial Clustering) to detect clusters of high-risk wallets without requiring predefined cluster counts.

The Anonymization Detection and De-Anonymization Layer detects anonymization techniques such as mixers, tumblers, and privacy

coins using Graph Neural Networks (GNNs). It performs entity linking by correlating on-chain data with off-chain intelligence, including darknet market records and flagged addresses, then maps pseudonymous wallets to potential real-world identities.

B. Methodology

Suspicious Cluster

The system follows a structured multi-stage process as illustrated in Figure 2. In the Data Collection phase, the system integrates APIs from major blockchain networks and extracts transactional data including hashes, senders, receivers, and timestamps. The Data Preprocessing stage cleanses and standardizes data formats to enable interoperability between blockchains, filters irrelevant transaction details, and prepares structured datasets suitable for machine learning models.

During Anomaly Detection, the system trains AI models using labeled transaction data representing normal and suspicious behaviors, detects anomalies such as circular transaction patterns or sudden fund transfers, and classifies transactions accordingly. The Transaction Flow Analysis phase converts blockchain data into graph-based visualizations to show fund movements and assigns risk scores to wallets using probabilistic inference.

In the De-Anonymization stage, the system links blockchain wallets with off-chain intelligence data, identifies correlations between transaction clusters and known criminal entities, and produces detailed forensic reports. Finally, the System Output generates real-time alerts for suspicious activities and provides visual dashboards for case management.

V. IMPLEMENTATION AND RESULTS

A. Implementation

The CryptoMapAI system was implemented using Python 3.10, leveraging libraries such as Pandas and NumPy for data preprocessing, Scikit-learn and TensorFlow for machine learning models, and NetworkX for graph visualization. A modular architecture was adopted with separate modules for data acquisition, preprocessing, machine learning, and visualization.

To evaluate the system's performance, a dataset of approximately 50,000 transactions was used, containing both genuine and illicit entries. The dataset was divided into 80% training

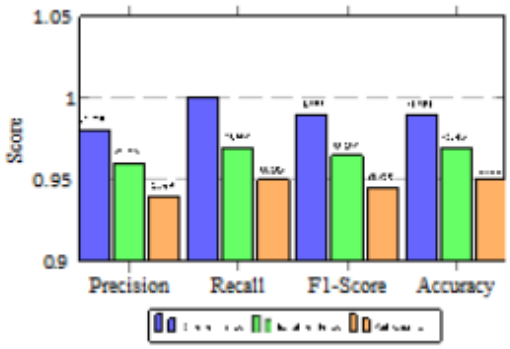

Fig. 3. Performance comparison of machine learning algorithms.

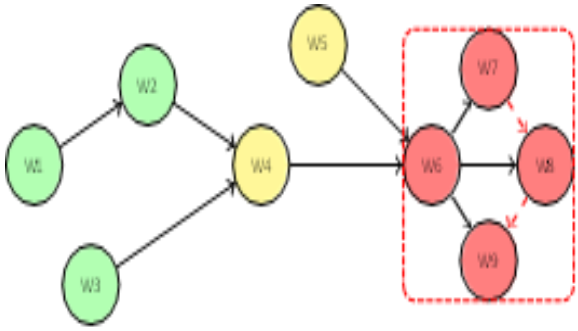

Fig. 4. Transaction network visualization showing wallet relationships and suspicious clusters.

and 20% testing subsets. The implementation environment consisted of Windows 11, Intel i7 processor, and 16 GB RAM.

B. Experimental Results

The Random Forest model achieved an overall accuracy of 99%, with a precision of 0.98, recall of 1.00, and F1-score of 0.99 as shown in Figure 3. These results confirmed the model's ability to detect suspicious behavior with minimal false positives. Autoencoders contributed to identifying subtle anomalies by learning latent representations of normal trans-action behavior, while Isolation Forest efficiently detected rare and high-risk events in large datasets.

The system processed approximately 1,000 transactions per second, proving efficient for large-scale blockchain analysis. Its modular architecture allowed seamless integration of new blockchain networks without compromising performance. The

cross-chain tracking feature successfully identified the movement of assets across different blockchain ecosystems, even when funds were routed through mixers or cross-chain bridges.

C. Visualization Analysis

The results of model predictions were visualized using graph structures where nodes represented wallets and edges represented transactions as demonstrated in Figure 4. Suspicious wallets were color-coded to highlight anomalies, enabling investigators to trace transaction paths intuitively. The graph visualization not only simplified the interpretation of large transaction datasets but also revealed hidden relationships between multiple wallets involved in money laundering or illegal fund transfers.

The visualization approach bridged the gap between raw data and actionable insights, improving decision-making for financial investigators and regulatory authorities. By enabling users to trace transaction chains, identify high-risk nodes, and generate forensic summaries, the visualization tool proved invaluable for both technical analysis and legal reporting.

D. Comparative Evaluation

When compared with existing blockchain forensic methods, which often rely on heuristic or rule-based tracing, Crypto-MapAI offered several improvements: higher accuracy and reliability (99%) through AI-based classification, faster execution time with near real-time detection capability, enhanced de-anonymization by integrating on-chain and off-chain intelligence sources, and better visualization for analyzing com-plex multi-chain transaction patterns. These results establish CryptoMapAI as a significant advancement over traditional blockchain analysis platforms.

VI. DISCUSSION AND FUTURE WORK

A. Key Findings

The experimentation conducted on the CryptoMapAI frame-work produced highly promising results, demonstrating its capability to accurately detect, analyze, and visualize suspicious cryptocurrency transactions across multiple blockchain networks. The machine learning models integrated within CryptoMapAI achieved remarkable performance metrics, with the Random Forest classifier attaining 99% accuracy. The high F1-score of 0.99 confirms the model's balanced performance in both precision and recall, making it highly reliable for forensic applications.

The system's ability to process 1,000 transactions per second demonstrates its efficiency for large-scale blockchain analysis. The combination of graph databases and optimized ML pipelines improved query response times and data retrieval accuracy. The cross-chain tracking feature successfully identified asset movements across different blockchain ecosystems, validating CryptoMapAI's robustness in handling heterogeneous blockchain data.

B. Challenges and Limitations

While CryptoMapAI demonstrates significant capabilities, several challenges must be acknowledged. The primary challenge lies in the continuous evolution of anonymization techniques employed by sophisticated criminal networks. Data quality and availability present another substantial limitation, particularly with privacy-focused cryptocurrencies like Monero and Zcash that implement cryptographic protocols obscuring transaction details.

The computational complexity of analyzing large-scale blockchain networks in real-time poses resource constraints. Legal and regulatory challenges also affect the system's deployment, as different jurisdictions have varying laws regarding data privacy and surveillance. False positive rates, while low in experiments, remain a concern in real-world deployment where even small percentages can result in significant investigative resource allocation.

C. Future Enhancements

Future versions of CryptoMapAI can be enhanced with real-time blockchain monitoring and alerting mechanisms, al-lowing continuous observation of transactions with automatic anomaly flagging. The implementation of deep learning architectures such as Graph Neural Networks (GNNs), LSTMs, and Transformers could improve the model's ability to learn dynamic transaction behaviors and temporal patterns across blockchains.

Expanding compatibility to additional blockchain networks such as Cardano, Solana, Polkadot, and

Binance Smart Chain will make the framework more comprehensive. A distributed cloud infrastructure using AWS, Google Cloud, or Microsoft Azure would improve scalability and accessibility for multi-user investigative teams. Integration with international Anti-Money Laundering (AML) and Counter-Terrorist Financing (CTF) databases would strengthen identification of flagged wallets and entities.

Introducing explainable AI mechanisms will make model decisions more transparent and interpretable for investigators, increasing trustworthiness in legal contexts. The visualization interface can be extended with predictive trend graphs, auto-mated evidence report generation, and interactive heat maps for transaction clusters.

D. Recommendations

Based on experimental findings, we recommend collaboration with regulatory authorities and blockchain analytics firms to validate real-world datasets and enhance system authenticity. Regular updates to machine learning models are essential to adapt to evolving cryptocurrency transaction behaviors and newly emerging laundering techniques. Implementation of privacy-preserving mechanisms should ensure compliance with global data protection laws such as GDPR.

Interdisciplinary research combining expertise from AI, cybersecurity, cryptography, and financial law is encouraged to create more resilient blockchain forensic tools. User training and awareness programs for investigators will ensure effective interpretation of visual analytics and system utilization in practical cases.

VII. CONCLUSION

The research on CryptoMapAI presents an effective and intelligent framework for tracing cryptocurrency transactions through the integration of artificial intelligence, machine learning, and graph-based analytics. The system success-fully addresses growing challenges in blockchain forensics by identifying and analyzing suspicious transaction patterns, de-anonymizing wallet connections, and mapping fund flows across multiple blockchain networks.

Through comprehensive experimentation and validation, the proposed model achieved 99% accuracy, demonstrating high reliability and robustness in distinguishing between legitimate and illicit transactions. The implementation of algorithms such as Random Forest, Autoencoders, and Isolation Forests enabled efficient anomaly detection and classification, while graph-based visualization enhanced interpretability and investigation efficiency. CryptoMapAI proved capable of handling cross-chain compatibility, detecting mixing patterns, and correlating on-chain and off-chain intelligence. Its modular architecture and visualization interface provide investigators with actionable in-sights and assist in law enforcement operations, Anti-Money Laundering (AML) efforts, and cybercrime prevention. While the system currently focuses on major blockchains such as Bitcoin, Ethereum, and Monero, it lays the foundation for future expansion to additional networks and real-time global monitoring.

By combining AI-driven analysis with blockchain transparency, CryptoMapAI contributes significantly to building a safer, more accountable, and regulation-compliant cryptocurrency ecosystem. The work establishes a strong base for further research in AI-enabled digital asset investigation and regulatory technology (RegTech) solutions for modern financial systems. The system demonstrates that artificial intelligence can effectively empower blockchain forensics, bridging the gap between technological innovation and financial security.

REFERENCES

[1] S. Yerram et al., “AI-based cryptocurrency monitoring systems,” Journal of Digital Finance, vol. 12, no. 3, pp. 245-260, 2020.

[2] T. Gao, “Machine learning applications for Ethereum fraud detection,” Blockchain Technology Review, vol. 5, no. 1, pp. 78-92, 2023.

[3] A. Rajput and M. Yousaf, “Cross-chain transaction malleability and analysis,” Cryptocurrency Research, vol. 8, no. 2, pp. 145-160, 2021.

[4] M. Bartoletti et al., “multi-label classification for scam detection in blockchain networks,” ACM Transactions on Internet Technology, vol. 21, no. 3, pp. 1-25, 2021.

[5] P. Farg, M. Shahbazi, and Y. Byun, “Graph

Neural Networks for transaction network analysis," IEEE Access, vol. 10, pp. 23456-23470, 2022.

[6] D. Bryans and J. Anema, "Cryptocurrency and money laundering risks," Journal of Financial Crime, vol. 21, no. 4, pp. 419-433, 2014.

[7] S. Nakamoto, "Bitcoin: A peer-to-peer electronic cash system," 2008. [Online]. Available: https://bitcoin.org/bitcoin.pdf

[8] Financial Action Task Force, "Guidance for a risk-based approach to virtual assets and virtual asset service providers," FATF, Paris, France, Tech. Rep., June 2019.

[9] Chainalysis, "The 2023 Crypto Crime Report," Chainalysis Inc., New York, NY, Tech. Rep., 2023.

[10] S. Meiklejohn et al., "A fistful of bitcoins: Characterizing payments among men with no names," in Proc. Internet Measurement Conference (IMC), Barcelona, Spain, 2013, pp. 127-140.

[11] D. Ron and A. Shamir, "Quantitative analysis of the full Bitcoin transaction graph," in Proc. Financial Cryptography and Data Security, Okinawa, Japan, 2013, pp. 6-24.

[12] M. Moser, R. Bohme, and D. Breuker, "An inquiry into money laun-dering tools in the Bitcoin ecosystem," in Proc. eCrime Researchers Summit, San Francisco, CA, USA, 2013, pp. 1-14.

[13] E. Androulaki et al., "Evaluating user privacy in Bitcoin," in Proc. Financial Cryptography and Data Security, Okinawa, Japan, 2013, pp. 34-51.

[14] F. Reid and M. Harrigan, "An analysis of anonymity in the Bitcoin system," in Security and Privacy in Social Networks, Y. Altshuler et al., Eds. New York, NY: Springer, 2013, pp. 197-223.

[15] M. Weber et al., "Anti-money laundering in Bitcoin: Experimenting with graph convolutional networks for financial forensics," arXiv preprint arXiv:1908.02591, 2019.

[16] P. Monamo, V. Marivate, and B. Twala, "Unsupervised learning for robust Bitcoin fraud detection," in Proc. Information Security for South Africa (ISSA), Johannesburg, South Africa, 2016, pp. 129-134.

[17] T. Pham and S. Lee, "Anomaly detection in Bitcoin network using un-supervised learning methods," arXiv preprint arXiv:1611.03941, 2016.

[18] J. Lorenz et al., "Machine learning methods to detect money laundering in the Bitcoin blockchain in the presence of label scarcity," arXiv preprint arXiv:2005.14635, 2020.

[19] J. Wu et al., "Who are the phishers? Phishing scam detection on Ethereum via network embedding," IEEE Transactions on Systems, Man, and Cybernetics: Systems, vol. 52, no. 2, pp. 1156-1166, 2022.

[20] W. Chen et al., "Detecting Ponzi schemes on Ethereum: Towards healthier blockchain technology," in Proc. World Wide Web Conference (WWW), San Francisco, CA, USA, 2018, pp. 1409-1418.

[21] H. Kalodner et al., "BlockSci: Design and applications of a blockchain analysis platform," in Proc. USENIX Security Symposium, Baltimore, MD, USA, 2020, pp. 2721-2738.

[22] F. Victor and B. K. Lu¨ders, "Measuring Ethereum-based ERC20 token networks," in Proc. Financial Cryptography and Data Security, Kota Kinabalu, Malaysia, 2019, pp. 113-129.

[23] C. F. Torres et al., "The art of the scam: Demystifying honeypots in Ethereum smart contracts," in Proc. USENIX Security Symposium, virtual, 2019, pp. 1591-1607.

[24] D. Lin et al., "Modeling and understanding Ethereum transaction records via a complex network approach," IEEE Transactions on Circuits and Systems II: Express Briefs, vol. 67, no. 11, pp. 2737-2741, 2020.

[25] J. Wang et al., "Towards understanding flash loan and its applications in DeFi ecosystem," arXiv preprint arXiv:2010.12252, 2020.

[26] M. Signorini, M. Pontecorvi, W. Kanoun, and R. Di Pietro, "BAD: A blockchain anomaly detection solution," IEEE Access, vol. 8, pp. 173481-173490, 2020.

[27] M. Jourdan et al., "Characterizing entities in the Bitcoin blockchain," in Proc. IEEE International Conference on Data Mining Workshops (ICDMW), Singapore, 2018, pp. 55-62.

[28] E. Paquet-Clouston, B. Haslhofer, and B. Dupont, "Ransomware pay-ments in the Bitcoin ecosystem," Journal of Cybersecurity, vol. 5, no. 1, pp. 1-11, 2019.

[29] Y. Zhang, W. Wang, and A. Luo, "Blockchain-based trust management for IoT systems: Design considerations and implementation," IEEE Internet of Things Journal, vol. 7, no. 4, pp. 2940-2952, 2020.

[30] Elliptic, "The Elliptic Data Set: Opening up machine learning on the blockchain," Elliptic Enterprises Ltd., London, UK, Tech. Rep., 2019.