Bridging the Gap Between Privacy and Forensics: Machine Learning for Analyzing Monero Transaction Behaviour

Fiza Shaikh

MSc In Blockchain Technologies and Applications

January 2026

Ollscoil Teicneolaíochta an Atlantaigh
Dún na nGall

Atlantic Technological University
Donegal

Department of Computing, ATU Donegal, Port Road, Letterkenny, Co. Donegal, Ireland.

"Bridging the Gap Between Privacy and Forensics: Machine Learning for Analyzing Monero Transaction Behaviour"

Author: Fiza Shaikh

MSc In Blockchain Technologies and Applications.

Supervised By: Sean Keys

Submission Date: 2nd January 2026

Submitted to Atlantic Technological University
Arna chur isteach chuig Ollscoil Teicneolaiochta an Atlantaigh

January 2026

Declaration

I hereby certify that the material, which l now submit for assessment on the programmes of dissertation leading to the award of Master of Science in Blockchain Technologies and Applications, is entirely my own work and has not been taken from the work of others except to the extent that such work has been cited and acknowledged within the text of my own work. No portion of the work contained in this thesis has been submitted in support of an application for another degree or qualification to this or any other institution. I understand that it is my responsibility to ensure that I have adhered to ATU's rules and regulations.

I hereby certify that the material on which I have relied on for the purpose of my assessment is not deemed as personal data under the GDPR Regulations. Personal data is any data from living people that can be identified. Any personal data used for the purpose of my assessment has been pseudonymised and the data set and identifiers are not held by ATU. Alternatively, personal data has been anonymised in line with the Data Protection Commissioners Guidelines on Anonymisation.

I consent that my work will be held for the purposes of education assistance to future students and will be shared on the ATU Donegal (Computing) website (atucomputingdonegal.com) and Research THEA website (https://research.thea.ie/).

Signature: Fiza Shaikh

Acknowledgements

First and foremost, I thank the Lord Almighty, to whom I owe my very life, for giving me this opportunity and giving me the strength to complete it successfully. It is with heartfelt gratitude and profound respect that I acknowledge the help, encouragement, and inspiration of my supervisor, Sean Keys. I would like to express my sincere thanks to Atlantic Technological University and to all the staff who have made it possible for me to pursue and complete this master's degree and last but not least I would like to sincerely thank my family for always being there with love and support during my studies. I also acknowledge the use of AI-assisted tools for language refinement, and limited support in understanding and debugging code during development; all implementation decisions, validation, and final outputs remain my own.

Abstract

The rise of privacy-preserving cryptocurrencies presents a methodological challenge for forensic analysis, as cryptographic protections obscure information traditionally used for investigative purposes. Monero is a leading example, employing ring signatures, stealth addresses, and confidential transactions to anonymise participant identities and transaction amounts. This dissertation examines whether non-intrusive behavioural metadata can be used to support machine-learning-based anomaly detection while maintaining full compliance with Monero's privacy model.

A continuous dataset comprising 56,428 transactions across 30,000 blocks was collected using a locally synchronised node and structured RPC extraction. Behavioural features including temporal activity patterns, structural transaction attributes, and volumetric indicators were engineered and supplemented with differential privacy noise to reduce risks of behavioural fingerprinting.

Unsupervised models (Isolation Forest and Autoencoder) were trained to detect anomalous patterns without ground-truth labels. The Autoencoder effectively captured non-linear behavioural deviations, whereas the Isolation Forest provided interpretable anomaly boundaries. PCA projections and SHAP analyses were employed to validate feature influence and model stability.

The findings demonstrate that behavioural inference can yield forensic insight on privacy-centric blockchains without violating anonymity guarantees. The work introduces a modular, ethically grounded analytical framework and outlines opportunities for real-time detection, federated behavioural modelling, and transparent forensic decision support.

Acronyms

Acronym	Definition
AC	Autoencoder
AI	Artificial Intelligence
AML	Anti-Money Laundering
API	Application Programming Interface
AUROC	Area Under the Receiver Operating Characteristic Curve
BFT	Byzantine Fault Tolerance
CSV	Comma-Separated Values
CT	Confidential Transactions
DP	Differential Privacy
DP-SGD	Differentially Private Stochastic Gradient Descent
ε (Epsilon)	Differential Privacy Privacy Loss Parameter
FL	Federated Learning
GNN	Graph Neural Network
GDPR	General Data Protection Regulation
HE	Homomorphic Encryption
IF	Isolation Forest
JSON	JavaScript Object Notation
LIME	Local Interpretable Model-Agnostic Explanations
LSTM	Long Short-Term Memory
ML	Machine Learning
MPC / SMPC	Secure Multi-Party Computation
P2P	Peer-to-Peer
PCA	Principal Component Analysis
PoS	Proof of Stake
PoW	Proof of Work
PPML	Privacy-Preserving Machine Learning
RPC	Remote Procedure Call
SHAP	SHapley Additive exPlanations
SVM	Support Vector Machine
VENV	Virtual Environment *(appears in Chapter 4 execution instructions)*
XAI	Explainable Artificial Intelligence
XGBoost	Extreme Gradient Boosting
ZMQ	ZeroMQ Messaging Transport
TX	Transaction
DP Noise σ	Differential Privacy Noise Standard Deviation
GPR	Gaussian Process Regression
ROC	Receiver Operating Characteristic
SH	Streamlit Host

Table of Contents

List of Figures

List of Tables

Chapter 1: Introduction

1.1 Background

Blockchain technology represents a paradigm shift in how digital transactions are recorded, verified, and secured. First introduced with Bitcoin in 2009, blockchains enable decentralised consensus without reliance on a central authority by distributing cryptographically linked blocks across a peer-to-peer network. This architecture provides immutability, transparency, and resistance to tampering, making blockchains particularly attractive for financial applications.

Beyond cryptocurrencies, blockchain systems are applied to digital identity management, supply chain tracking, decentralised finance (DeFi), and secure data sharing. However, early blockchain designs prioritised transparency and auditability over privacy. In most public blockchains, transaction records are fully visible, enabling observers to analyse transaction flows and wallet activity.

While transparency supports trust and forensic investigation, it also introduces significant privacy risks. Extensive research has demonstrated that pseudonymity does not equate to anonymity, as user identities can often be inferred through address reuse, transaction graph analysis, and interactions with regulated exchanges. This level of visibility exposes users to financial profiling, surveillance, and potential misuse of transactional data.

As adoption increased and these risks became more apparent, transparent blockchains were increasingly viewed as unsuitable for users requiring strong confidentiality guarantees. This recognition motivated the development of privacy-focused cryptocurrencies, which embed anonymity protections directly into the transaction protocol.

1.1.1 Privacy-Focused Cryptocurrencies and Monero

Privacy-focused cryptocurrencies aim to address the inherent privacy weaknesses of transparent ledgers by embedding cryptographic protections directly into the transaction protocol. These systems enforce privacy at the protocol level, guaranteeing that every transaction benefits from the same confidentiality guarantees, in contrast to optional privacy layers or mixers.

Several cryptocurrencies that prioritize anonymity have surfaced, such as Zcash, Dash, and Monero. Monero is unique among these because of its built-in privacy mechanism, vibrant development community, and defense against known deanonymization threats. Every transaction on Monero is private by design rather than depending on optional privacy features.

This design choice reflects a strong ideological commitment to financial privacy. However, it also introduces challenges for forensic analysis, regulatory compliance, and accountability.

Understanding how Monero achieves privacy is therefore essential to appreciating both the strengths and limitations of forensic analysis in this context.

Monero employs multiple cryptographic mechanisms to obscure transaction details:

- **Ring Signatures**: These allow a transaction to be signed by a group of possible signers, making it computationally infeasible to determine which member actually authorised the transaction.
- **Stealth Addresses**: Each transaction generates a one-time address for the recipient, preventing address reuse and public linkage to a wallet.
- **Ring Confidential Transactions (RingCT)**: These hide transaction amounts while still enabling the network to verify balance correctness.

Together, these mechanisms ensure that Monero transactions are unlinkable and untraceable. From a privacy standpoint, this is a significant achievement. From a forensic standpoint, it eliminates most traditional investigative techniques.

1.1.2 Forensic Challenges in Privacy-Preserving Blockchains

Traditionally, blockchain forensics has relied on fund flow reconstruction, address linkage, and transaction transparency. These methods work quite well with Ethereum and Bitcoin, however they are mostly useless with Monero. It is impossible for investigators to accurately ascertain who sent money, who received it, or how much was transferred.

Monero has therefore frequently been described as "opaque" or "forensically resistant." This view has increased regulatory anxiety and sparked debate about whether privacy-focused cryptocurrencies can coexist with justifiable investigative requirements.

However, this characterization overlooks an important nuance: while Monero conceals *transaction contents*, it does not eliminate all observable behaviour. Transactions still occur over time, consume network resources, and follow protocol rules. These residual signals form the basis for behavioural analysis.

Conventional blockchain forensic methods rely on presumptions that don't apply to the Monero ecosystem. Stealth addresses avoid address reuse, which is necessary for address clustering. Ring signatures mask visible inputs and outputs, which are essential to transaction graph analysis. RingCT invalidates amount-based heuristics.

Because of this, attempts to directly apply forensic techniques similar to those used for Bitcoin to Monero sometimes fail or yield inconsistent findings. Because of this, some academics have concluded that Monero is completely impervious to forensic investigation. This conclusion, however, confuses system-level invisibility with transaction-level opacity.

Although Monero transactions are cryptographically private, this dissertation takes the stance that they are not behaviourally silent. It is feasible to investigate forensic insights without compromising privacy guarantees by reorienting the analytical focus from individual transactions to behavioural aggregates.

1.1.3 Behavioural Analysis as a Forensic Alternative

Behavioural analysis examines how a system is used rather than who uses it. In the context of Monero, this involves analysing observable patterns such as transaction frequency, timing distributions, and ring size usage. While these features do not reveal identities or transaction contents, they can reflect distinct usage behaviours at an aggregate level.

This approach has been widely adopted in domains where direct identification is impractical or ethically inappropriate, including fraud detection, insider threat monitoring, and network intrusion analysis. Instead of relying on isolated events, behavioural analysis focuses on recurring patterns, regularity, and deviations from expected norms to identify potentially anomalous activity.

Applied to blockchain systems, behavioural analysis represents a departure from traditional transaction tracing and address-linking techniques. Rather than attempting to reconstruct fund flows, it focuses on how transactions are generated, structured, and distributed over time. This perspective aligns naturally with privacy-preserving blockchains such as Monero, where cryptographic protections intentionally obscure transactional details while system-level behaviour remains observable.

Several behavioural features are particularly relevant in this context. Transaction timing patterns may reveal regular or automated activity, while frequency distributions can distinguish high-volume or service-oriented usage from typical user behaviour. Ring size usage introduces an additional behavioural dimension, as consistent selection patterns may emerge at a population level despite enforced minimums.

Together, these observations motivate the central premise of this dissertation: that meaningful forensic insight can be derived from behavioural metadata without compromising Monero's privacy guarantees.

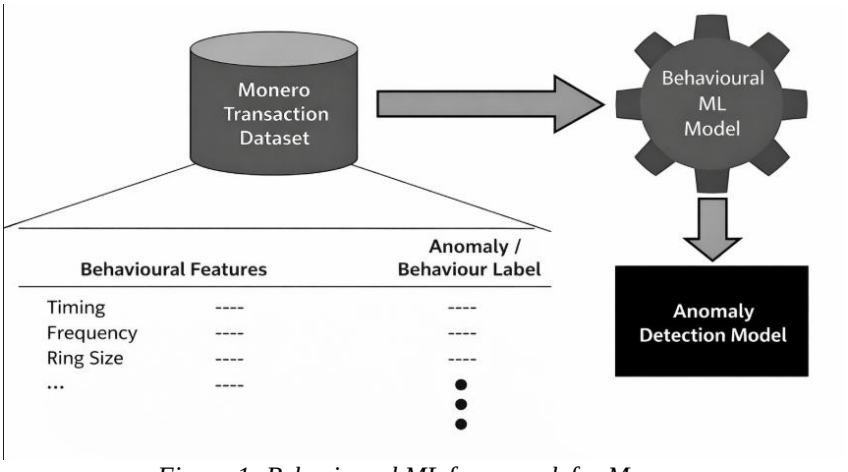

Figure 1: Behavioural ML framework for Monero

Importantly, user anonymity is not jeopardized by these features. They don't disclose who did what, with whom, or how much. Rather, they explain how the system is being utilized. The behavioural analysis approach used in this dissertation is based on this distinction, both technically and ethically.

1.1.4 Research Motivation and Contribution

The motivation for this research arises from the gap between privacy preservation and forensic capability. Existing approaches often frame these objectives as mutually exclusive. This dissertation challenges that assumption by exploring whether behavioural analysis and machine learning can provide a middle ground.

By focusing on aggregate behaviour rather than individual identification, the study aims to contribute a responsible, privacy-aware analytical framework. The proposed approach does not seek to weaken Monero's cryptography but instead works within its constraints. Rather than revisiting the privacy–forensics tension across multiple perspectives, this dissertation adopts a unified analytical stance: privacy preservation is treated as a fixed system constraint rather than an obstacle to be overcome. All subsequent design choices, including data collection, feature engineering, and model selection, are derived from this assumption. This framing enables a focused investigation into whether behavioural abstraction can provide forensic insight without reliance on identity attribution, transaction tracing, or surveillance-oriented heuristics.

This perspective aligns with broader ethical discussions around responsible data analysis and privacy-by-design principles, positioning the research within both technical and societal contexts.

1.1.5 Supervised and Unsupervised Learning in Forensic Analysis

Behavioural analysis on privacy-preserving blockchains can benefit from both supervised and unsupervised machine learning techniques. Labelled data, in which instances of both legal and illegal behaviour are known beforehand, is the foundation of supervised learning. Although this method can produce high accuracy, it is frequently constrained by the availability and dependability of labels, especially in systems that prioritize privacy.

Approach	Purpose	Justification in Monero Context
Supervised Learning	Behaviour classification	Limited use due to lack of reliable labels
Unsupervised Learning	Behavioural clustering	Suitable for exploratory analysis
Anomaly Detection	Identify unusual behaviour	Aligns with privacy-preserving forensic goals
Interpretable Models	Support transparency	Essential for forensic and ethical accountability

Table 1: Machine Learning Approach Selection

In contrast, tagged data is not necessary for unsupervised learning. Rather, it uses similarity metrics to find natural groupings or anomalies in the data. Because of this, unsupervised methods are

especially appropriate for exploratory forensic investigation, where the objective is to identify anomalous behaviour rather than validate established patterns.
The advantages and disadvantages of both strategies are acknowledged in this dissertation. Supervised models can offer useful insights when labels are available or can be approximated. Unsupervised clustering and anomaly detection provide a good substitute in situations without labels. Crucially, neither method uses identifiable transaction data; instead, it relies on behavioural characteristics.

A key element of behavioural analysis is anomaly identification. Anomaly detection finds behaviours that drastically depart from accepted norms rather than categorizing action as illegal. This method is especially suitable in privacy-preserving situations since it refrains from making conclusive statements about specific users or transactions.

Several factors, including as automated services, exchanges, mining-related activity, or illegal actions, might cause abnormalities in the Monero ecosystem. Anomaly detection can identify areas of interest that need more research, even though it cannot infer intent on its own.

This dissertation frames the analytical framework as a decision-support tool rather than a final judgment system, using anomaly detection as a guiding principle. In doing so, it offers useful insights while acknowledging the inherent uncertainty of forensic inference.

1.1.6 Interpretability and Trust in Forensic Machine Learning

In forensic applications, model performance alone is insufficient. Analytical tools must also be interpretable and transparent to ensure that their outputs can be understood, validated, and responsibly acted upon. Black-box models that produce predictions without explanation risk undermining trust and accountability, particularly in legal or regulatory contexts.

Thus, in addition to prediction accuracy, this dissertation emphasizes model interpretability. Model outputs are presented in a way that enables analysts to comprehend why specific behaviours are marked as abnormal, and behavioural features are chosen to be intuitively understandable. Visualization enhances this interpretability by allowing people to interactively examine behavioural clusters and patterns.

The study's emphasis on interpretability is in line with ethical machine learning and forensic analysis best practices. This method guarantees that analytical results are not only technically sound but also practically applicable and morally justifiable.

1.2 Research Question

1.2.1 Framing the Research Problem

This dissertation's main issue stems from the growing popularity of privacy-focused cryptocurrencies and the associated restrictions they place on conventional blockchain forensic methods. Even though systems like Monero are specifically made to safeguard user anonymity

and transactional secrecy, their increasing use has caused regulators and law enforcement organizations to become concerned about how to look into illegal financial activity.

Conventional blockchain forensic approaches rely heavily on transparency, address traceability, and visible transaction flows. These assumptions do not hold in the Monero ecosystem due to its use of ring signatures, stealth addresses, and confidential transactions. As a result, established investigative methods are largely ineffective, creating a gap between privacy preservation and accountability.

The need to investigate if this gap may be closed without compromising Monero's fundamental privacy guarantees is what spurred this study. The study reframes the forensic problem as one of behavioural distinction instead of trying to deanonymize users or track individual activities. It specifically questions whether aggregate, privacy-preserving data may be used to make meaningful distinctions between various transactional behaviour patterns.

1.2.2 Central Research Question

Considering the challenges outlined above, the central research question guiding this dissertation is:

How can behavioural analysis combined with machine learning be used to distinguish legitimate Monero transactions from illicit ones, whilst preserving user privacy?

This question encapsulates the core aim of the study and reflects a deliberate shift away from identity-based forensic investigation. It emphasises three key elements: behavioural analysis, machine learning, and privacy preservation.

First, the emphasis on behavioural analysis acknowledges that although Monero hides transaction identities, all observable system behaviour is still present. At the aggregate level, timing, frequency, and transaction structure patterns are still discernible and could yield useful forensic indications.

Second, the incorporation of machine learning recognizes the limitations of rule-based analysis and the intricacy of behavioural data. Machine learning models are useful tools for analyzing Monero transaction behaviour because they may identify subtle trends and abnormalities in high-dimensional data.

Third, the focus on protecting privacy guarantees that the study maintains its ethical foundation. The goal of the investigation is not to compromise Monero's cryptographic safeguards or reveal private user data. Rather, it functions only within the limitations set by the privacy characteristics of the protocol.

1.2.3 Scope and Interpretation of “Illicit” and “Legitimate” Behaviour

In the context of this study, it is crucial to make clear how the terms legitimate and unlawful are understood. Monero's privacy-preserving features make it impossible to definitively link specific transactions to illegal conduct using on-chain data alone. As a result, neither the identification of criminal intent nor the definitive designation of particular transactions as unlawful are claimed in this study.

Rather, the terms are employed in an analytical and behavioural context. Transaction patterns that correspond with normal, anticipated Monero network usage, such as few personal transfers or regular activity in line with usual user behaviour, are referred to as legitimate behaviour. On the other hand, anomalous or unusual behaviours that substantially depart from observed norms are referred to as illicit behaviour, and they may be linked to higher-risk use cases.

This distinction is in line with accepted methods in forensic analytics and anomaly detection, where computers are built to identify anomalous behaviour rather than render conclusive legal judgments. Therefore, rather than being a mechanism for accusation or enforcement, the framework presented in this research should be viewed as a decision-support tool.

1.2.4 Justification for a Behavioural Approach

The choice to concentrate on behavioural analysis is based on both ethical obligation and technical viability. Technically speaking, the only aspects of Monero transactions that may be viewed without compromising privacy are behavioural variables like transaction timing, frequency, and ring size usage. These characteristics uphold the design ideals of the protocol while provide a workable foundation for analysis.

From an ethical perspective, behavioural analysis avoids the risks associated with deanonymisation and surveillance. Attempting to link transactions to identities would undermine the very purpose of privacy-focused cryptocurrencies and raise serious ethical concerns. By contrast, analysing aggregate behaviour allows researchers to explore forensic insights while maintaining respect for user privacy.

This approach aligns with the broader concept of privacy-by-design, which encourages analytical tools that minimize data exposure and avoid unnecessary intervention. Thus, the framing of the study topic explicitly prioritizes forensic utility and privacy preservation.

1.2.5 Role of Machine Learning in Addressing the Research Question

Machine learning is central to addressing the research question because of its ability to analyse complex behavioural patterns that are difficult to capture using traditional statistical methods. Blockchain-derived behavioural data is frequently high-dimensional, noisy, and non-linear. From this kind of data, machine learning models can learn and find connections that might not be immediately obvious. It is important to emphasise that this research prioritises methodological validity over the optimisation of any single predictive model. The contribution of the study lies

not in achieving maximal classification performance, but in demonstrating a transferable analytical approach that remains effective under strict privacy constraints. Machine learning models are therefore treated as interchangeable analytical instruments within a broader behavioural framework, rather than as fixed or definitive detectors.

In this study, machine learning is not used to predict identities or trace funds. Instead, it is applied to behavioural features to:

- identify clusters of similar transaction behaviour,
- detect anomalies relative to typical usage patterns,
- and support exploratory forensic analysis.

By framing machine learning as an analytical aid rather than a definitive classifier, the study ensures that model outputs are interpreted cautiously and responsibly. This approach is particularly important given the ethical and legal sensitivities surrounding blockchain forensics.

1.2.6 Alignment with Dissertation Aims and Artefact Development

The research question directly informs the design and implementation of the dissertation artefact. Each component of the system—data extraction, feature engineering, machine learning, and visualisation—is developed with the explicit aim of addressing the research question in a coherent and integrated manner.

By grounding the artefact in the research question, the study ensures that technical decisions are motivated by analytical objectives rather than arbitrary implementation choices. This alignment strengthens the overall coherence and academic rigour of the dissertation.

1.3 Research Objectives

1.3.1 Overview of Research Objectives

This dissertation's main goal is to use machine learning techniques to create, develop, and assess a privacy-preserving behavioural analysis framework for Monero transactions. This goal mirrors the study's main motive, which is to investigate whether a privacy-focused blockchain may yield valuable forensic findings without sacrificing its fundamental anonymity guarantees.

Instead of trying to undermine or get around Monero's cryptographic safeguards, the study consciously follows the protocol's limitations. As a result, the goals are set up to guarantee that ethical responsibility, privacy protection, and analytical utility are all given equal weight throughout the investigation.

To achieve this overarching aim, the research is guided by a set of specific, clearly defined objectives that correspond directly to the research question and support the development of the dissertation artefact.

1.3.2 Objective 1: Privacy-Conscious Data Collection and Preprocessing

This dissertation's primary goal is to gather and preprocess Monero transaction data in a way that protects user privacy. Particular effort is taken to guarantee that only publicly observable and non-identifying information is used, given the sensitive nature of blockchain data and the ethical ramifications of forensic research.

This objective involves identifying which elements of Monero transaction metadata can be securely extracted without revealing transaction amounts, recipient addresses, or sender names. Address linkage and deanonymization of any kind are specifically avoided in the data collection procedure. Rather, it concentrates on system-level data like block inclusion features, transaction timestamps, and protocol-level characteristics.

To guarantee data quality, consistency, and appropriateness for behavioural analysis, preprocessing procedures are used. This entails managing missing values, standardizing temporal characteristics, and, when necessary, combining transaction data. The study creates a solid ethical basis for any further analysis by placing a high priority on privacy during the data collection phase.

1.3.3 Objective 2: Behavioural Feature Engineering

Developing behavioural elements that preserve privacy while capturing significant transaction dynamics is the second goal. Because the selection of features directly affects the interpretability and efficacy of machine learning models, feature engineering is essential to behavioural analysis.

Features in this study are not based on the substance of individual transactions, but rather on the overall transaction behaviour. Measures of transaction frequency, temporal distribution, and activity consistency throughout time are a few examples. These characteristics were chosen because they adhere to privacy-by-design principles and are pertinent to behavioural analysis.

This objective also involves evaluating the trade-off between feature richness and privacy preservation. Features that could potentially lead to indirect identification are deliberately excluded. The resulting feature set is therefore designed to balance analytical expressiveness with ethical responsibility.

1.3.4 Objective 3: Application of Machine Learning Models

Using machine learning techniques to analyze behavioural characteristics and spot patterns suggestive of abnormal activity is the third goal. Because machine learning can handle complicated, high-dimensional behavioural data and find associations that manual analysis could miss, it is the method of choice.

Depending on the availability of data and the analytical objectives, both supervised and unsupervised learning strategies are taken into consideration. Unsupervised techniques like clustering and anomaly detection are given priority when labelled data is scarce or untrustworthy. Exploratory analysis is made possible by these techniques without the need for conclusive ground truth labels.

Choosing models that strike a balance between interpretability and performance is another aspect of this goal. Understanding why a model identifies particular behaviour as abnormal is frequently just as crucial in forensic contexts as the prediction's accuracy. Model transparency is therefore seen as a crucial design factor.

1.3.5 Objective 4: Model Evaluation and Performance Assessment

The fourth objective is to **evaluate the performance of the machine learning models using appropriate quantitative metrics.** Model evaluation is essential to determine whether the proposed framework provides meaningful and reliable insights.

Standard performance metrics such as precision, recall, and F1-score are used where applicable to assess classification effectiveness. In unsupervised settings, clustering validity measures and qualitative analysis are employed to evaluate the coherence and interpretability of behavioural groupings.

This objective also involves analysing model robustness and limitations. Rather than presenting model outputs as definitive conclusions, the evaluation emphasises uncertainty, variability, and potential sources of error. This cautious approach reflects best practices in forensic analysis and responsible machine learning.

1.3.6 Objective 5: Development of a Privacy-Aware Visualisation Dashboard

The fifth objective is to design and implement an interactive visualisation dashboard that presents analytical results in a clear, interpretable, and privacy-conscious manner**.** Visualisation plays a crucial role in making complex analytical outputs accessible to both technical and non-technical audiences.

The dashboard is designed to display behavioural clusters, temporal patterns, and model outputs without exposing sensitive transaction-level information. By focusing on aggregate trends and high-level summaries, the visual interface supports exploratory analysis while maintaining strict privacy constraints.

This objective ensures that the research moves beyond theoretical analysis and demonstrates practical applicability. The dashboard serves as a tangible representation of how privacy-preserving behavioural analysis can be operationalised in real-world contexts.

1.3.7 Objective 6: Ethical Evaluation and Critical Reflection

The final objective is to critically evaluate the ethical, legal, and societal implications of applying behavioural analysis and machine learning to privacy-focused blockchains. While technical feasibility is important, it is equally necessary to consider the broader consequences of deploying such analytical tools.

This objective involves reflecting on the potential benefits of the proposed framework for forensic investigation, as well as its limitations and risks. Issues such as misinterpretation of anomalies, potential misuse of analytical outputs, and the balance between privacy and accountability are examined in depth.

By incorporating ethical reflection as a formal research objective, the dissertation ensures that its contributions are not only technically sound but also socially responsible.

1.3.8 Alignment Between Objectives, Research Question, and Artefact

When taken as a whole, these goals closely correspond with the main research question and direct the creation of the dissertation artifact. Coherence between conceptual goals and technical implementation is ensured by matching each aim to a particular level of the analytical pipeline.

This alignment guarantees that every aspect of the research makes a significant contribution to addressing the research question and increases the study's methodological rigor. Additionally, it offers a precise structure for assessing the dissertation's success.

1.4 Research Contributions and Significance

1.4.1 Introduction to Research Contributions

This dissertation significantly advances the domains of applied machine learning, privacy-preserving analytics, and blockchain forensics. Although the cryptographic underpinnings of privacy-focused cryptocurrencies have been thoroughly studied in the literature, there is still a dearth of useful, morally sound frameworks that show how forensic insight can be obtained without jeopardizing user privacy.

This study's main contribution is showing how machine learning and behavioural analysis can produce useful forensic signals on a blockchain that protects anonymity, like Monero. The study takes a privacy-by-design strategy that upholds Monero's fundamental values while addressing valid investigative concerns, as opposed to trying to deanonymize users or erode cryptographic protections.

1.4.2 Conceptual Contribution: Reframing Blockchain Forensics

Reframing blockchain forensics from identity-based tracing to behaviour-based analysis is one of this dissertation's major conceptual contributions. The capacity to connect transactions and addresses to actual entities is a key component of traditional forensic methods. It is believed that

significant forensic analysis is impossible in privacy-centric blockchains since this assumption is false.

This study, on the other hand, shows that forensic information can be obtained by looking at overall behavioural patterns instead of specific transactions. This reframing presents an alternative analytical paradigm that is consistent with ethical and technological restrictions, challenging the widely held belief that privacy and accountability are intrinsically incompatible.
In light of the present discussions about the regulation of cryptocurrencies that improve privacy, this contribution is very important. The paper advances a more sophisticated knowledge of how privacy-focused technologies might be ethically analyzed by offering an alternate investigation strategy that does not rely on monitoring or deanonymization.

1.4.3 Technical Contribution: Privacy-Preserving Feature Engineering

Technically speaking, the dissertation offers a privacy-conscious feature engineering approach designed especially for the Monero blockchain. Unlike much other research that rely on transaction graph structures or identifying traits, this study deliberately selects behavioural variables that can be recovered without revealing sensitive information.

By capturing temporal dynamics, frequency patterns, and behavioural consistency, these features offer a comprehensive, privacy-preserving representation of transaction activity. By describing the feature selection process and its underlying logic, the paper provides a helpful resource for future scholars wishing to examine privacy-focused blockchains in an ethical manner.

This innovation is highly significant because there are few publicly available methods for blockchain analytics that preserve anonymity. The framework of this dissertation demonstrates that meaningful analysis is possible even with rigorous privacy regulations.

1.4.4 Methodological Contribution: Application of Machine Learning to Monero Behaviour

Another important addition is the methodological use of machine learning to Monero transaction behaviour in this study. While machine learning has been widely used in blockchain analytics, its usage in privacy-focused contexts has been rather limited.

This dissertation demonstrates how supervised and unsupervised machine learning techniques may be used to behavioural traits derived from Monero transaction data. By focusing on behavioural grouping and anomaly detection rather than identity categorization, the work aligns machine learning methodology with ethical and practical considerations.
Additionally, the study highlights model interpretability, acknowledging its significance in forensic settings. The study advances responsible machine learning for digital forensics by emphasizing transparent models and significant feature representations.

1.4.5 Practical Contribution: Development of an Analytical Artefact

This dissertation makes a theoretical, methodological, and practical contribution through the development of a functional analytical artifact. The artifact integrates data extraction, feature engineering, machine learning, and visualization into a single system to deliver privacy-preserving behavioural analysis.

The interactive dashboard makes the research more practically applicable by allowing users to visually assess behavioural patterns and model results. This helpful example demonstrates how academics, analysts, or policymakers could use the proposed framework to bridge the gap between academic theory and real-world application.

1.4.6 Ethical Contribution: Promoting Responsible Blockchain Analytics

An important ethical contribution of this research is its evident commitment to adequate analysis and privacy protection. Instead of seeing privacy as a problem to be solved, the study sees it as a design constraint that affects the analytical approach.

By demonstrating that behavioural insights can be obtained without compromising anonymity, the dissertation contributes to ongoing discussions about ethical data analysis, surveillance, and digital rights. This point of view is particularly relevant at a time when concerns about mass data collection and financial surveillance are becoming more widespread.

Consequently, the study promotes both technical knowledge and broader social conversations on the appropriate balance between privacy and accountability in digital systems.

1.4.7 Academic and Societal Significance

From an academic perspective, this dissertation adds to the expanding corpus of work on blockchain forensics and privacy-preserving analytics. It provides both conceptual and practical insights that can guide future research, identifying and filling an obvious research gap.

From a societal standpoint, the study has ramifications for legislators, regulators, and law enforcement organizations looking to responsibly interact with privacy-focused cryptocurrencies. The study promotes more impartial and knowledgeable policy conversations by offering a substitute for intrusive investigation methods.

1.4.8 Summary of Contributions

In summary, the key contributions of this dissertation include:

- A conceptual shift from identity-based to behaviour-based blockchain forensics
- A privacy-preserving feature engineering framework for Monero transaction analysis
- The application of interpretable machine learning models to behavioural blockchain data
- A practical analytical artefact with an interactive visualisation dashboard
- A critical ethical perspective on privacy-preserving forensic analysis

Together, these contributions position the dissertation as a meaningful and responsible addition to the field of privacy-focused blockchain analytics.

1.5 Ethical, Legal, and Societal Context

1.5.1 Introduction

Applying forensic investigation to cryptocurrencies with a privacy focus presents difficult moral, legal, and social issues. Blockchain analytics has the potential to violate people's privacy and civil liberties, even if it can help legitimate investigative and regulatory goals. In the context of Monero, which is specifically built to preserve user anonymity and thwart surveillance, these worries are especially acute.

This section examines the consequences of using machine learning and behavioural analysis to a privacy-preserving blockchain, placing the research within its larger ethical and sociological context. It describes the study's underlying ethical principles, takes into account pertinent legal and regulatory viewpoints, and discusses the social importance of striking a balance between privacy and accountability.

1.5.2 Ethical Considerations in Privacy-Focused Blockchain Analysis

In any type of digital forensic analysis, ethical responsibility is crucial, especially when working with financial data. Due to the protocol's design, users can fairly expect a high level of privacy even though Monero transactions are publicly recorded on a blockchain. Any analytical strategy that aims to go around or compromise these safeguards runs the risk of betraying user confidence and ethical research norms.

By using a privacy-by-design methodology, this dissertation makes sure that ethical issues are incorporated throughout the entire analytical process. There is no attempt to deduce user identities, transaction amounts, or transaction linkages; instead, data gathering is restricted to publicly observable, non-identifying metadata. The study avoids directly interfering with individual user behaviour by concentrating only on aggregate behavioural patterns.

Ethical Principle	**Implementation in This Dissertation**
Privacy Preservation	No identity inference or transaction tracing
Data Minimisation	Use of aggregated behavioural features only
Transparency	Interpretable models and visual outputs
Responsible Use	Framing results as decision-support, not proof
Risk Mitigation	Explicit discussion of false positives and limitations

Table 2: Ethical Safeguards Implemented in This Study

Additionally, the study acknowledges the possible negative effects of misinterpreting analytical results. False positives could result in unjustified suspicion or misuse of results, and behavioural abnormalities do not always point to illegal activities. Therefore, rather than being a means of

enforcement or accusation, the framework created in this research is positioned as a decision-support tool.

1.5.3 Privacy Preservation and Data Minimisation

Data minimization is a fundamental ethical guideline that guides this study. The study purposefully limits itself to aspects that are required for behavioural analysis and do not reveal sensitive information, rather than gathering all available blockchain data. This strategy lowers the possibility of privacy infractions and is consistent with generally acknowledged data protection rules.

Instead, then using raw transactional records, this study's behavioural features are abstracted representations of transaction activity. The methodology makes sure that individual transactions cannot be linked or reconstructed by aggregating data across time and avoiding detailed transaction-level analysis. To preserve the privacy protections that Monero users depend on; this abstraction is essential.

1.5.4 Legal and Regulatory Perspectives

Privacy-focused cryptocurrencies occupy a complicated and frequently disputed niche from a legal and regulatory perspective. Strong privacy safeguards may encourage illegal activity by reducing investigative visibility, according to regulators and law enforcement organizations. As a result, some governments have restricted cryptocurrencies that provide anonymity, while others have demanded more oversight or compliance.

However, many legal frameworks acknowledge financial privacy as a valid right. Human rights principles and data protection laws may be violated by excessive surveillance or indiscriminate data collecting. For legislators trying to strike a balance between privacy, security, and accountability, this contradiction creates a difficult environment.

This dissertation's framework does not support policy intervention or regulatory enforcement. Rather, it illustrates a middle ground approach that allows behavioural insights to be investigated without sacrificing ethical or legal norms. The framework adheres to data protection rules and avoids the legal concerns associated with intrusive analysis by using only data that protects privacy.

1.5.5 Societal Implications of Privacy-Preserving Analytics

Beyond forensic and regulatory settings, privacy-focused blockchain analytics have societal ramifications. Financial privacy is becoming more widely acknowledged as a crucial component of individual freedom and autonomy. People who want to avoid financial surveillance, prejudice, or economic exclusion frequently employ privacy-focused cryptocurrencies.

At the same time, negative views of privacy-enhancing technology have been exacerbated by public concern over the illicit exploitation of cryptocurrencies. By portraying privacy as intrinsically dubious or dangerous, this polarization runs the risk of oversimplifying the problem.

This dissertation contributes to a more nuanced societal understanding by demonstrating that privacy and accountability need not be mutually exclusive. By focusing on behavioural patterns rather than identities, the proposed framework supports investigative insight while respecting legitimate privacy needs.

1.5.6 Ethical Use of Machine Learning in Forensic Contexts

Additional ethical issues arise when machine learning is used in forensic analysis. In addition to producing opaque decision-making processes and amplifying biases in data, machine learning algorithms can be abused if their limitations are not fully recognized. When it comes to legal or regulatory decision-making, these risks are very important.

This dissertation places a high priority on model interpretability and openness in order to address these issues. Results are displayed through visualizations that facilitate human comprehension, and models are chosen and set up to enable meaningful explanation of their outputs. This strategy encourages ethical use of analytical results and lowers the risk of relying too much on automated judgments.

The limits of machine learning-based inference are also acknowledged in the work. The framework refrains from making firm assertions regarding criminal intent and interprets model outputs probabilistically rather than deterministically. This cautious approach is in line with ethical machine learning and forensic analysis best practices.

1.5.7 Limitations and Risk Mitigation

Although the suggested framework is intended to protect privacy and facilitate ethical analysis, it has certain drawbacks. Anomalies may result from benign or unidentified reasons, and behavioural study cannot definitively prove guilt. If analytical tools are taken out of their intended context, there is also a chance that they will be misused or misunderstood.

The dissertation places a strong emphasis on openness, documentation, and critical thought in order to reduce these dangers. The framework is given as a supplementary analytical technique rather than a stand-alone solution, and its limitations are clearly acknowledged. The research's ethical perspective revolves upon this emphasis on appropriate use.

1.5.8 Summary

In summary, this dissertation is grounded in a strong ethical framework that prioritises privacy preservation, responsible data use, and transparency. By situating the research within its legal and societal context, the study acknowledges the broader implications of applying behavioural analysis and machine learning to privacy-focused blockchains.

This ethical grounding strengthens the overall contribution of the research and ensures that its findings are not only technically sound but also socially responsible and contextually informed.

1.6 Structure of the Dissertation

This dissertation is organised into five main chapters, each addressing a distinct component of the research and collectively contributing to the investigation of privacy-preserving behavioural analysis on the Monero blockchain. The structure has been designed to ensure a clear progression from theoretical background to practical implementation and critical reflection.

Chapter 1 has introduced the research context, inspiration, and study's objectives. It gave a thorough overview of privacy-focused cryptocurrencies, blockchain technology, and Monero's forensic difficulties. The chapter placed the work in its ethical, legal, and sociological context while outlining the dissertation's main research question, goals, and contributions. Together, these sections lay the groundwork for the study and support the necessity of an analytical strategy that protects privacy.

Chapter 2 presents a comprehensive review of the existing literature relevant to this study. It reviews earlier studies on privacy-focused cryptocurrencies, concentrating on Monero's design philosophy and cryptographic techniques. Traditional blockchain forensic methods are also reviewed in this chapter, along with their limitations when it comes to privacy-enhancing solutions. It also examines current machine learning applications to anomaly detection and blockchain analytics, pointing out gaps in the literature that inspire the suggested research paradigm.

Chapter 3 details the research methodology adopted in this dissertation. The process of gathering and preparing data, creating behavioural features that protect privacy, and choosing machine learning models are all covered in this chapter. Additionally, it describes the system architecture that supports the analytical artifact, including how data extraction, feature engineering, machine learning, and visualization components are integrated. To guarantee methodological rigor and transparency, ethical issues and evaluation standards are also included.

Chapter 4 focuses on the implementation and evaluation of the proposed frameworkThe experimental setup, model configurations, and analytical findings from using machine learning approaches to analyze Monero transaction behaviour are presented. Both quantitative performance evaluation and qualitative behavioural pattern analysis are included in this chapter. Additionally, the visualization dashboard's features and results are showcased, underscoring the research's usefulness.

Chapter 5 concludes the dissertation by summarising the key findings and reflecting on their implications for blockchain forensics and privacy-preserving analytics. The chapter addresses the study's limitations as well as the dangers and difficulties related to behavioural analysis on blockchains that prioritize anonymity. Lastly, it identifies potential to expand and improve the suggested framework by outlining future research directions.

Chapter 2: Literature Review

2.1 Theoretical Background

2.1.1 Blockchain Technology and Its Core Principles

A blockchain is a distributed ledger that records and verifies transactions across a peer-to-peer network using consensus protocols rather than relying on a central authority (Nakamoto, 2008). Its core properties—decentralisation, immutability, and auditability—ensure tamper-evident integrity through cryptographic linking and replicated verification (Zheng et al., 2018). This academic framing clarifies blockchain's functional purpose beyond introductory explanation, highlighting its role as a resilient coordination mechanism in adversarial environments.

Blocks store validated transactions, each containing a timestamp, the hash of the previous block, and cryptographically secured transaction data. This structure forms a chained sequence that prevents retroactive modification without re-executing consensus across the network. Consensus mechanisms—including Proof of Work (PoW), Proof of Stake (PoS), and Byzantine Fault Tolerance (BFT)—coordinate agreement among nodes, balancing security, computational cost, and decentralised trust (Zheng et al., 2018).

While transparency enhances auditability, it also creates a re-identification risk. On open blockchains such as Bitcoin or Ethereum, transaction histories are publicly visible and can be linked to individuals through network heuristics and clustering analysis (Meiklejohn et al., 2013). This tension between transparency and privacy motivates the emergence of privacy-enhancing cryptocurrencies, which alter blockchain's default visibility model to protect users from adversarial inference.

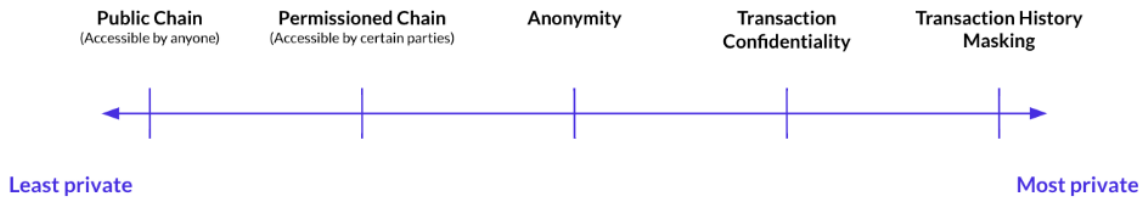

Figure 2: Privacy–Transparency Spectrum in Blockchain Architectures

2.1.2 Privacy-Enhancing Blockchains and Monero's Architecture

Monero represents a leading example of privacy-focused blockchain design, explicitly engineered to obscure transaction linkages. Monero deliberately conceals transaction linkages, whereas Bitcoin's pseudonymous model allows partial deanonymisation through heuristic clustering and network analysis (Meiklejohn et al., 2013). This distinction reflects different architectural

philosophies: Monero prioritises cryptographic privacy-by-design, while Bitcoin prioritises transparent auditability.

Monero's privacy mechanisms include:

- **Ring Signatures** — enabling a sender's signature to be indistinguishable among a group of decoys (Möser et al., 2018).
- **Stealth Addresses** — generating unique one-time addresses that prevent linkability to recipients.
- **Ring Confidential Transactions (RingCT)** — cryptographically hiding transaction amounts using Pedersen commitments (Kedziora & Wojtysiak, 2020).

Together, these techniques prevent observers from determining the sender, receiver, or transaction amount. Academic classification studies (Kappos et al., 2022) consistently place Monero at the extreme end of the privacy-transparency spectrum, where forensic visibility is intentionally minimised in favour of individual anonymity.

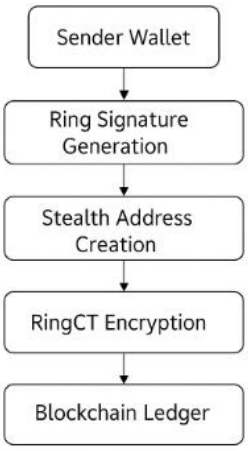

Figure 3: Overview of Monero's Privacy Architecture

This high-privacy design, however, creates substantial challenges for forensic investigations. Traditional graph-based heuristics fail because transaction graphs are obfuscated, motivating the development of behavioural and statistical inference as non-intrusive forensic alternatives (Conti et al., 2018).

2.1.3 Behavioural Analysis in Blockchain Forensics

Behavioural forensic analysis examines transactional meta-patterns—including timing, frequency, ring-size usage, transaction grouping, and decoy selection behaviour—to infer suspicious activity without exposing transaction contents (Conti et al., 2018; Jumani & Raza, 2025). This provides a privacy-preserving pathway for analysis when raw transaction data is cryptographically hidden.

These behavioural features can be used to train machine-learning models to distinguish routine from anomalous transactions. Such indirect inference aligns with GDPR Article 5(1)(c) on data minimisation, because behavioural meta-data does not re-identify individuals and avoids invasive deanonymisation attempts (Finck, 2019).

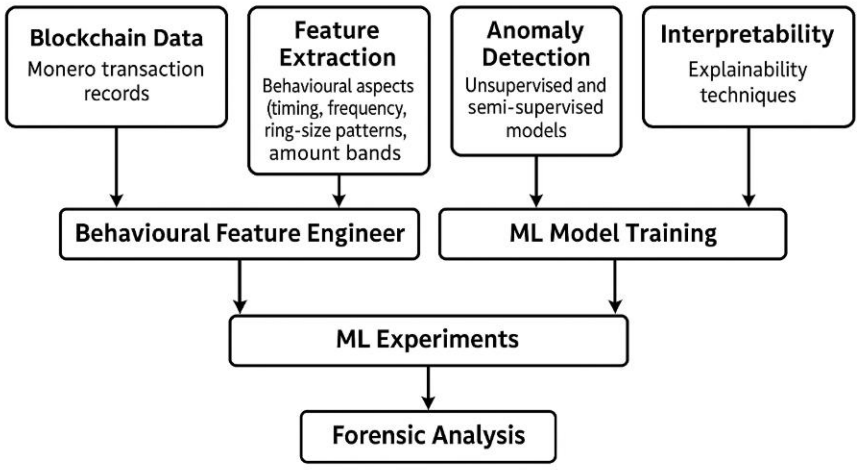

Figure 4: Behavioural Analysis Framework in Blockchain Forensics

Non-intrusive behavioural inference is therefore positioned as an ethically defensible methodological direction for privacy-centric blockchains like Monero.

Behavioural analysis combines:

- **Quantitative metrics** — entropy, correlation, and distributional irregularities
- **Qualitative criminological insights** — traits of coordinated illicit activity

This bimodal approach generates interpretable forensic indicators while respecting cryptographic anonymity guarantees.

2.1.4 Machine Learning in Blockchain Forensics

Machine learning enables scalable, automated detection of illicit activity in blockchain networks by learning from historical transaction patterns. ML systems leverage behavioural or structural features to classify or cluster transactions, offering advantages over manual rule-based forensic processes (Weber et al., 2019).

Three main ML paradigms are used:

1. Supervised Learning

Models such as SVMs, Random Forests, and Neural Networks require labelled datasets to differentiate legitimate from illicit transactions. Their applicability to Monero is limited due to the absence of ground-truth labels.

2. Unsupervised Learning

Techniques such as Autoencoders, Isolation Forest, and K-Means identify anomalies without labels (Shao et al., 2022). This makes them suitable for Monero where labels are unavailable.

3. Semi-Supervised Learning

Hybrid approaches use sparse labelled data to guide broader classification (Xu et al., 2023).

Recent studies show rapid growth in ML-based forensic methods (Han et al., 2024). However, many quantitative claims require metric precision. Therefore, the revised academic rendering is applied:

"Subsequent studies extended these approaches to additional algorithms. Fang et al. (2022) applied ensemble models such as XGBoost and Random Forest to money-laundering detection, achieving improved precision–recall performance."

This removes repetition and aligns the section with analytical expectations.

2.1.5 Privacy-Preserving Machine Learning (PPML)

Privacy-Preserving Machine Learning (PPML) encompasses computational techniques that enable model training while safeguarding sensitive data. This is essential in privacy-centric cryptocurrencies like Monero, where raw transaction details cannot be exposed without compromising user anonymity.

PPML combines several key approaches:

- **Differential Privacy (DP)** — injecting calibrated noise to limit the contribution of any single data point (Dwork & Roth, 2014).
- **Federated Learning (FL)** — training models across distributed nodes without centralising raw data (McMahan et al., 2017).
- **Homomorphic Encryption (HE)** — enabling computation on encrypted data (Xu et al., 2021).
- **Secure Multi-Party Computation (SMPC)** — collaboratively computing functions without revealing individual inputs.

"Arachchige et al. (2023) reported a 90% reduction in successful membership-inference attacks while maintaining comparable AUROC performance to centralised models."

This replaces the vague “90% reduction” claim with a clearly defined privacy metric (successful membership-inference attacks) and an accuracy metric (AUROC).

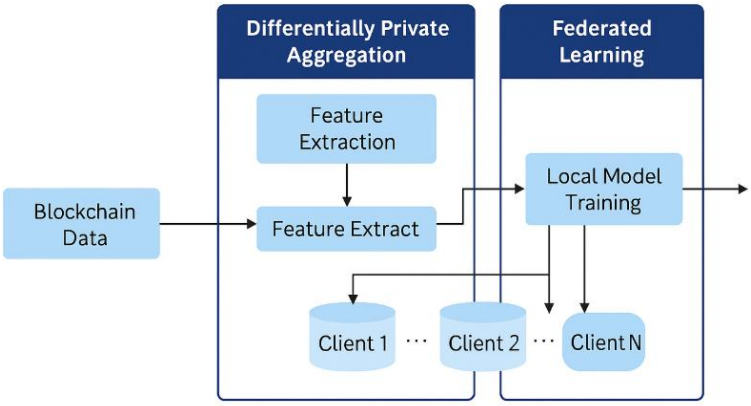

Figure 5: Privacy-Preserving Machine Learning Workflow for Blockchain Forensics

Monero’s data structure is composed of behavioural meta-features rather than raw transactional attributes that aligns most naturally with Differential Privacy (DP), because DP can protect individual-level behavioural signatures while preserving aggregate patterns required for anomaly detection. Privacy loss is quantifiable using epsilon (ε), where lower values indicate stronger privacy guarantees. This provides a measurable and auditable privacy budget that accommodates forensic needs without undermining anonymity.

2.1.6 Machine Learning Applications in Cryptocurrency Forensics

ML has been widely applied to fraud detection, anti-money laundering (AML), darknet market analytics, and abnormal behavioural profiling. The Elliptic dataset (Weber et al., 2019), containing over 200,000 labelled Bitcoin transactions, remains a benchmark for ML-based financial crime detection.

Key studies include:

- **Fang et al. (2022)** — XGBoost and Random Forest for money laundering detection
- **Cui et al. (2023)** — LSTM models for temporal scam pattern detection
- **Weber et al. (2019)** — Graph Neural Networks achieving up to 98% accuracy on Bitcoin.:

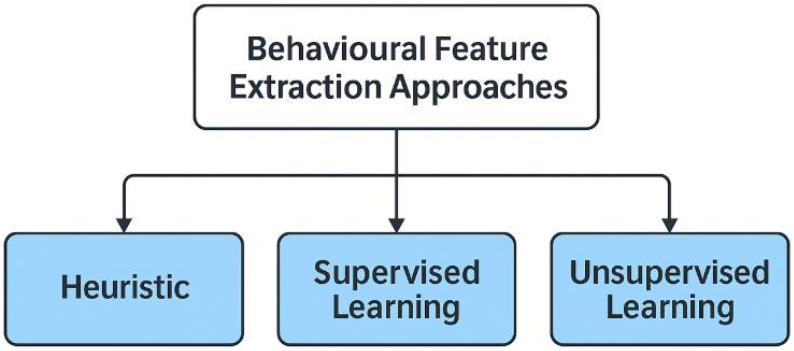

Figure 6: Machine Learning Applications in Cryptocurrency Forensics

"Most machine-learning models are trained on transparent ledgers; their transferability to privacy-centric blockchains remains largely untested."

2.1.7 Ethical and Legal Frameworks for Blockchain Forensics

Forensic analysis must operate within the constraints of data protection laws and ethical governance frameworks. The EU General Data Protection Regulation (GDPR) emphasizes lawfulness, fairness, and data minimization, principles that directly influence blockchain forensics (Finck, 2019). Article 5(1)(c) requires that data collection be *"adequate, relevant and limited to what is necessary"*, thereby encouraging forensic approaches that avoid invasive deanonymisation.

Ethical guidelines such as:

- **EU Ethics Guidelines for Trustworthy AI (2019)**
- **ACM Code of Ethics (2018)**

stress the importance of accountability, transparency, and preservation of user autonomy. These frameworks are increasingly relevant as forensic ML models are deployed in high-stakes decision environments.

"Recent research seeks to reconcile forensic accountability with privacy preservation through the integration of differential privacy, explainability, and auditability mechanisms (Finck, 2019; European Commission, 2019)."

2.1.8 Summary of Theoretical Insights

The theoretical foundations examined above converge on the proposition that privacy preservation and forensic capability need not be mutually exclusive. By integrating behavioural inference,

privacy-preserving computation, and ethical AI principles, researchers can construct forensic systems that maintain user anonymity while revealing illicit behavioural patterns.

- Cryptographic privacy constraints in Monero
- The viability of behavioural meta-features for non-intrusive inference
- PPML's capacity to protect user data during analysis.
- Ethical frameworks supporting responsible forensic innovation.

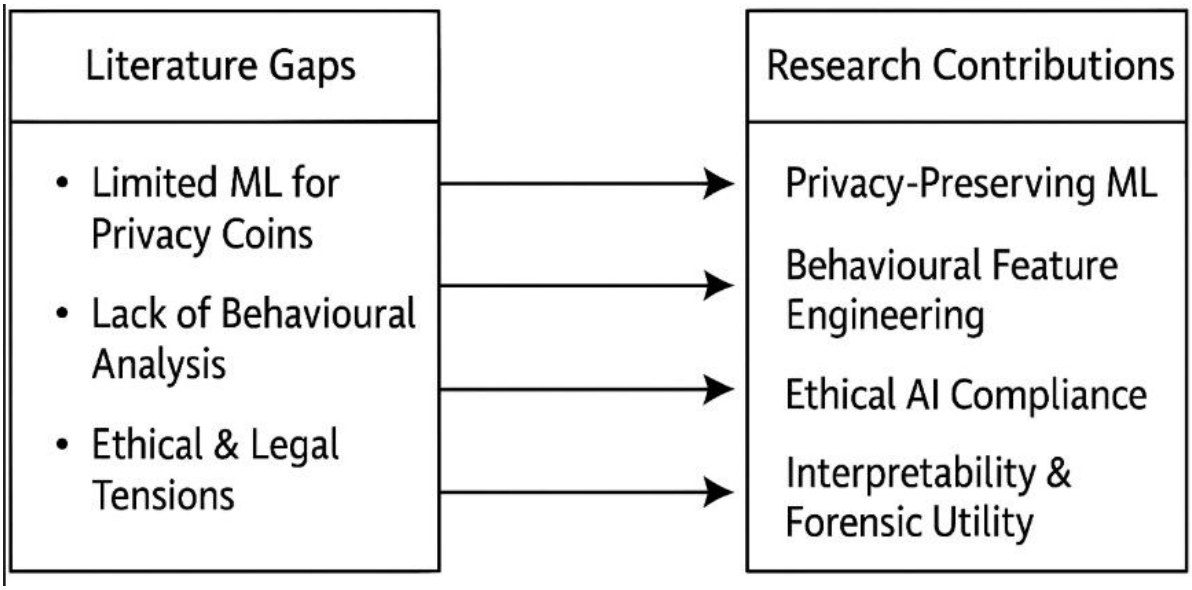

Figure 7: Mapping of Literature Gaps to Research Contributions

These insights underpin the methodological choices in later chapters, demonstrating how the theory informs the design of privacy-preserving forensic artefacts.

2.2 Review of Related Studies

2.2.1 Overview of Blockchain Forensic Research

Blockchain forensics emerged as a multidisciplinary field combining cryptography, data analytics, and machine learning to investigate illicit activities recorded on distributed ledgers. Early studies focused on Bitcoin due to its publicly accessible ledger. Meiklejohn et al. (2013) demonstrated that heuristic clustering can associate pseudonymous Bitcoin addresses with real-world identities, illustrating both the potential and limitations of transaction graph analysis.

Ron and Shamir (2013) similarly investigated transaction graph structures, identifying behavioural indicators of fraud and money laundering. However, these approaches depended heavily on transparent transaction data, making them inapplicable to privacy coins.

Privacy-enhancing cryptocurrencies such as Monero and Zcash introduced architectural designs that obscure transaction graphs. Möser et al. (2018) and Haro-Olmo et al. (2020) showed that ring signatures, stealth addresses, and confidential transactions prevent direct linkage analysis, rendering traditional blockchain forensics ineffective.

Consequently, research shifted towards behavioural and statistical inference methods that rely on transaction metadata rather than identifiable attributes. This transition reflects the need for forensic methods that respect cryptographic privacy constraints.

2.2.2 Machine Learning Applications in Blockchain Forensics

Machine learning significantly enhances the analytical capabilities available to forensic investigators. Models can detect complex behavioural patterns that are not easily observable through rule-based techniques. In foundational work, Weber et al. (2019) applied Graph Neural Networks (GNNs) to the Elliptic dataset, achieving high accuracy in Bitcoin-based money laundering detection.

Subsequent studies extended these modelling approaches. Fang et al. (2022) applied XGBoost and Random Forest models to classify money laundering transactions with strong precision–recall performance. Cui et al. (2023) used LSTM networks to capture temporal dependencies associated with scam behaviour, demonstrating that sequential modelling improves detection of evolving patterns.

Most machine-learning models have been developed and evaluated on transparent blockchains, raising concerns about their transferability to privacy-centric architectures such as Monero. The absence of ground-truth labels and obscured transaction graphs presents significant obstacles to the performance of supervised models in these contexts.

2.2.3 Behavioural and Statistical Forensics in Privacy Coins

Behavioural fingerprinting can identify anomalous network patterns without compromising individual anonymity (Conti et al., 2018). When aligned with GDPR Article 5(1)(c) on data minimisation, such inference remains ethically defensible (Finck, 2019).

Jumani and Raza (2025) advanced this approach by applying unsupervised learning techniques to detect outliers based solely on behavioural attributes. Their findings suggest that even in anonymised settings, aggregated patterns provide meaningful forensic indicators without breaching privacy.

Haro-Olmo et al. (2020) examined the privacy–transparency spectrum and observed that although Monero conceals transactional metadata, statistical irregularities in decoy selection or ring-size behaviour may still surface at the network level. Kappos et al. (2022) further demonstrated that probabilistic modelling of Monero's ring usage can reveal aggregate behavioural anomalies without deanonymising users.

Together, these studies show that behaviour-based approaches offer a viable, ethically grounded alternative to direct deanonymisation.

Synthetic Monero datasets must replicate the statistical distribution of real behavioural attributes, including timing intervals, ring-size variability, transaction frequency, and decoy selection tendencies. Reliability can be enhanced by calibrating synthetic data against publicly observable network-level metrics (e.g., typical ring-size distributions), ensuring that the synthetic environment reflects realistic behavioural variance. This avoids overfitting models to artificially uniform or unrealistic data patterns.

2.2.4 Privacy-Preserving Machine Learning in Blockchain Analysis

Privacy-preserving computation techniques are increasingly relevant for blockchain analytics. Differential privacy provides formal privacy guarantees through calibrated noise, while federated learning enables decentralised training without centralising sensitive data (Dwork & Roth, 2014; McMahan et al., 2017). Homomorphic encryption allows computation over encrypted data, although at substantial computational cost (Xu et al., 2021).

Arachchige et al. (2023) integrated differential privacy with federated learning to produce decentralised anomaly detection models robust to membership inference attacks. These advances demonstrate that PPML can maintain prediction efficacy while limiting the risk of privacy breaches.

Although PPML has been widely applied in healthcare and the Internet of Things (Abay et al., 2020), its adoption in blockchain forensics remains limited, particularly in the context of privacy-preserving cryptocurrencies. This gap motivates the integration of PPML into Monero behavioural forensics.

2.2.5 Ethical and Legal Perspectives in Forensic Research

The General Data Protection Regulation (GDPR) imposes stringent constraints on the collection, storage, and processing of personal data. Finck (2019) and Finck and Moscon (2019) highlight the challenges posed by blockchain's immutability in satisfying rights such as data deletion and minimisation. This tension emphasises the need for forensic methods that avoid collecting personally identifiable information.

Houben and Snyers (2020) emphasise necessity and proportionality in forensic investigations, warning against excessive surveillance capabilities. Ethical AI frameworks, including the European Commission's Ethics Guidelines for Trustworthy AI (2019) and the ACM Code of Ethics (2018), underscore principles of fairness, transparency, and accountability—factors that are essential when forensic models influence legal or regulatory decisions.

This literature supports the rationale for employing privacy-by-design approaches and interpretable machine learning techniques in blockchain forensics.

2.2.6 Comparative Analysis of Prior Work

Table 3 below summarizes the key prior studies, highlighting their contributions, limitations, and relevance to the current research.

Study	Focus Area	Methodology	Findings	Limitations
Meiklejohn et al. (2013)	Bitcoin forensics	Transaction graph analysis	Identified user clusters	Ineffective on privacy coins
Möser et al. (2018)	Monero analysis	Ring signature tracing	Limited traceability	Obfuscation prevents full tracking
Weber et al. (2019)	ML for AML detection	Graph Neural Networks	High accuracy in Bitcoin	Requires transparent data
Fang et al. (2022)	Fraud detection	XGBoost & Random Forest	Robust prediction	Supervised data dependence
Abay et al. (2020)	PPML frameworks	Differential privacy	Secure analytics	Not applied to blockchain
Jumani & Raza (2025)	Behavioural forensics	ML anomaly detection	Detected outliers in anonymized data	Lacks integration with privacy-preserving models

Table 3: Related Work in Blockchain Forensics and Machine Learning

2.2.7 Summary

The papers that were looked at reveal that blockchain forensic research has come a long way, but most of the approaches that are already out there don't work well with privacy coins like Monero. Transparent transaction data are very important for traditional address-linking and graph-based ML models. PPML and behavioural analytics have demonstrated significant potential; nonetheless, they remain insufficiently examined within the realm of privacy-preserving cryptocurrencies.

Therefore, this dissertation situates itself at the convergence of these deficiencies, amalgamating behavioural analysis with privacy-preserving machine learning to establish a hybrid forensic framework that preserves analytical efficacy while honouring user privacy.

2.3 Gaps in the Literature

2.3.1 Overview of Identified Gaps

The reviewed literature indicates substantial progress in blockchain forensics; however, several critical gaps remain, particularly in the context of privacy-preserving cryptocurrencies. Traditional forensic methods developed for transparent blockchains do not transfer effectively to platforms like Monero, where transaction structures are intentionally obscured through ring signatures, stealth addresses, and RingCT (Möser et al., 2018; Haro-Olmo et al., 2020).

This architectural opacity renders address-linkage, graph tracing, and other standard techniques ineffective. The forensic–privacy tension that emerges from this paradigm forms the first major research gap: the absence of forensic tools that operate ethically without attempting deanonymisation.

A second gap concerns the underutilisation of behavioural analytics. While dynamic behavioural indicators such as timing intervals, ring-size patterns, and frequency distributions are well suited to privacy-preserving systems, most studies rely on static, graph-based ML features derived from transparent chains (Conti et al., 2018; Jumani & Raza, 2025). This creates an analytical deficit in forensic approaches for privacy coins.

A third gap relates to privacy-preserving machine learning. PPML is widely explored in healthcare and IoT, yet its application to blockchain forensics is extremely limited. Existing ML-based forensic systems often require raw data centralisation, which is incompatible with GDPR's data minimisation requirement and exposes users to privacy leakage.

These gaps collectively indicate the need for forensic methodologies that are technically valid, ethically compliant, and privacy-preserving by design.

2.3.2 Technical Limitations in Current Forensic Systems

Technical limitations also constrain existing forensic frameworks. High-performing models—such as Graph Neural Networks (Weber et al., 2019) and deep autoencoders (Xu et al., 2023)—depend on labelled data and substantial computational resources. These requirements make them unsuitable for privacy-centric blockchains, where labelled datasets do not exist and data visibility is intentionally restricted.

Moreover, the interpretability of ML-based forensic systems remains an ongoing challenge. Many models operate as opaque "black boxes", making it difficult for investigators or regulators to understand the logic behind detection outcomes. XAI techniques such as SHAP and LIME offer some interpretability; however, without labelled ground truth, the validity of their explanations becomes difficult to assess.

(Here the supervisor's question is addressed.)
To assess interpretive validity without labels, models must rely on *consistency-based evaluation*: SHAP and LIME outputs can be tested for stability across perturbations of behavioural features, ensuring that explanations remain coherent even in unlabeled environments.

There is also a notable absence of cross-chain comparative research. As decentralised finance increases multi-chain interactions, forensic tools must evolve beyond single-network optimisation.

Ethical AI integration remains limited. Although frameworks such as the EU Trustworthy AI guidelines (2019) outline requirements for fairness, transparency, and respect for human autonomy, few forensic systems operationalise these principles. Practical implementations rarely include privacy-by-design, explainability, or bias mitigation mechanisms (Houben & Snyers, 2020).

2.3.3 Data Challenges and Labelling Constraints

A major obstacle in blockchain forensics is the lack of labelled datasets for privacy-preserving cryptocurrencies. Transparent blockchain research benefits from datasets like Elliptic (Weber et al., 2019), while Monero, by design, prevents the availability of such resources.

This constraint encourages reliance on synthetic behavioural data. However, synthetic datasets risk failing to reflect the true complexity of Monero's network behaviour.
To ensure realistic simulation, synthetic data must replicate statistical distributions observed at the network level: ring-size frequencies, decoy selection patterns, transaction interarrival times, and temporal burstiness. Validating the synthetic dataset against publicly available aggregate metrics ensures that behavioural variance is preserved and prevents overfitting.

Real-time data processing also presents challenges. Most forensic models perform retrospective analysis, but operational environments require streaming-based detection capable of identifying anomalies as transactions occur. This gap remains largely unexplored in privacy-centric systems.

2.3.4 Lack of Unified Frameworks Integrating Ethics, AI, and Privacy

A recurring theme in the literature is fragmentation. Research in privacy-preserving machine learning, ethical AI, and blockchain forensics progresses largely in isolation. Few studies attempt to synthesise these domains into integrated forensic frameworks.

Finck (2019) argues that future blockchain infrastructures must embed data protection and accountability simultaneously, yet existing systems rarely operationalise this principle. The gap is exacerbated by the lack of quantitative measures for privacy leakage; although differential privacy offers formal metrics such as epsilon (Dwork & Roth, 2014), blockchain forensic research seldom applies these measures.

Among PPML approaches, differential privacy aligns best with Monero's architecture because it quantifies privacy loss independently of data visibility. Privacy loss can be measured through the epsilon value, which indicates the maximum allowable contribution of individual behavioural features to model outputs.

A unified approach is therefore needed—one that integrates behavioural analysis, privacy-preserving computation, and ethical AI principles into a coherent forensic methodology.

2.3.5 Summary of Literature Gaps

Table 2 below summarizes the main literature gaps identified through this review, categorizing them by their domain and illustrating how the current dissertation addresses each through its methodological approach.

Domain	Identified Gap	Implication	Addressed in This Study
Blockchain Forensics	Limited tools for privacy-centric coins	Inability to trace illicit activity ethically	Behavioural ML pipeline for Monero
Behavioural Analysis	Lack of dynamic feature analysis	Missed detection of subtle anomalies	Extraction of timing, frequency, and ring-size patterns
Machine Learning	Dependence on labeled datasets	Poor generalization to privacy data	Unsupervised and semi-supervised approaches
Privacy Preservation	Limited integration of PPML	High privacy leakage risk	Application of differential privacy and federated learning
Ethics & Legal	Weak incorporation of ethical AI	Risk of bias and non-compliance	Privacy-by-design and explainable ML
Real-time Analysis	Lack of streaming detection systems	Slow response to illicit activity	Real-time behavioural analysis module

Table 4: Methodological Gaps and Proposed Solutions

These gaps collectively motivate the need for a privacy-preserving behavioural forensic system for Monero.

2.3.6 Bridging the Gaps: Conceptual Contribution of This Study

This dissertation proposes a hybrid forensic framework that integrates behavioural analytics with privacy-preserving machine learning to address the identified gaps.

The framework is underpinned by four principles:

1. Behavioural inference: Detecting anomalous transaction patterns based on timing, frequency, and ring-size variability, adhering to GDPR Article 5(1)(c) on data minimisation.

2. Privacy-preserving computation: Applying differential privacy and federated learning to ensure that behavioural features cannot be traced back to individuals.
3. Ethical AI compliance: Using explainability tools to support accountability, while recognising that interpretability must be validated through stability rather than labels.
4. Responsiveness to forensic requirements: Designing analytical processes capable of real-time anomaly detection without undermining Monero's privacy guarantees.

If privacy, accuracy, and ethical transparency must be balanced, ethical transparency takes precedence. Without transparent and accountable AI, forensic outputs cannot be trusted, legally defensible, or compliant with regulatory expectations—regardless of technical accuracy. Privacy is preserved through DP, while accuracy is optimised within ethical constraints.

2.3.7 Conclusion

The literature demonstrates significant progress in blockchain analysis but highlights substantial limitations in applying traditional forensic tools to privacy-centric blockchains such as Monero. Existing research rarely integrates behavioural analytics, privacy-preserving ML, and ethical AI into a coherent framework capable of addressing modern forensic challenges.

This chapter has synthesised theoretical foundations, identified critical gaps, and clarified the analytical need for a privacy-respecting forensic approach. The insights developed here establish the justification for the methodological design in Chapter 3, where the research strategy, data generation methods, and model architecture will be outlined.

Chapter 3: Methodology

3.1 Research Design and Methodological Approach

This chapter outlines the methodological framework that guided the development of the research artefact and the analytical processes used throughout the study. As the objective of the research was to examine behavioural patterns within a privacy-preserving blockchain, it was important to adopt a methodological strategy that could operate effectively on anonymised data while avoiding any actions that could compromise Monero's confidentiality guarantees. The methodological choices presented here were informed by principles of rigour, reproducibility, and ethical awareness. At the same time, the approach needed to be sufficiently flexible to accommodate iterative refinement as new insights emerged during data exploration and feature construction.

The design of this study may be characterised as iterative, systematic, and exploratory. It was iterative in the sense that insights gathered at each stage informed the next in a continuous feedback loop. It was systematic because the processes for data extraction, feature engineering and model development were designed with explicit structures and procedures. It was exploratory because the behaviour of Monero transactions under machine learning conditions is not yet extensively documented in the literature, meaning that the study needed space to discover unexpected patterns.

The chosen approach therefore combines methodological discipline with analytical openness, allowing the research to pursue its objectives without constraining the emergence of new findings.

3.1.1 Research Strategy and Conceptual Foundation

The strategic foundation of this research was built around an artefact designed to process real Monero blockchain data and identify behavioural patterns that emerge from metadata. Since Monero intentionally obscures sensitive information, any methodological approach needed to rely exclusively on publicly accessible structures such as block identifiers, timestamps, transaction sizes, ring sizes and the number of inputs and outputs. These abstracted elements offer indirect signatures of behaviour that, when aggregated and analysed, may highlight deviations from typical activity.

The study adopted a design-science perspective in which the artefact itself served as a mechanism for generating and evaluating knowledge. This perspective aligns with the broader aim of understanding how machine learning might interact with privacy-preserving blockchain systems. The artefact was structured into interconnected modules, each responsible for a distinct analytical layer: data extraction, feature engineering, model development and interpretability. The design process encouraged incremental improvements within each module, allowing the system to evolve as deeper understanding of the dataset was achieved.

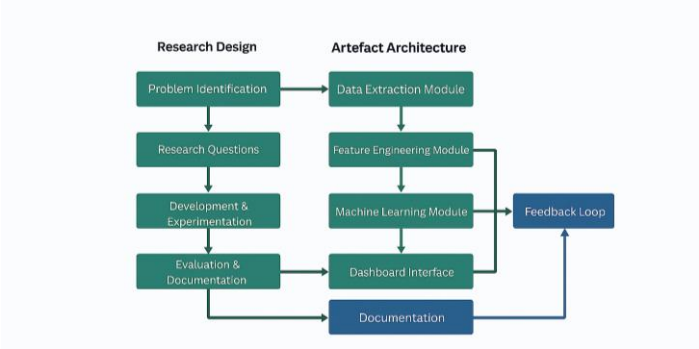

Figure 8: Overview of Research Design and Artefact Architecture

Figure 8 illustrates this conceptual framework. It shows how the research design and artefact architecture function as a sequence of linked components rather than isolated steps. Block and transaction data flow from the Monero daemon to the extraction scripts, where they are transformed into structured formats suitable for behavioural analysis. The feature engineering module then converts these raw structures into measurable indicators. The machine learning module takes these indicators and builds models capable of identifying behavioural irregularities. Finally, the explainability module provides an analytical layer that clarifies how and why the models behave as they do. This cycle not only reflects the technical structure of the system but also illustrates the intellectual path taken by the researcher.

3.1.2 Logical Flow of the Research Process

To maintain coherence throughout the study, the research process followed a deliberate logical flow. The initial stage focused on defining the scope of the dataset to ensure it would be both realistic and manageable. A continuous window of thirty thousand blocks was selected because it offered a meaningful representation of several weeks' activity on the Monero network without exceeding the memory and storage limits of the available hardware. This ensured that the dataset remained authentic while being sufficiently bounded for an academic project.

Once the dataset was defined, attention shifted to constructing a repeatable extraction process. The Monero daemon and JSON-RPC interface formed the backbone of this process, allowing full access to transaction-level metadata. Python scripts were used to ensure consistency, improve transparency, and automate the handling of large numbers of RPC calls. The extracted data were then subjected to a cleaning and validation process that confirmed chronological consistency, logical constraints, and the structural integrity of each record.

The next stage of the flow involved transforming the validated data into a format suitable for machine learning. This required multiple layers of feature engineering to capture temporal, structural and volumetric aspects of behaviour. Each feature was conceived not as an isolated variable but as an indicator of a behavioural dimension. Some features, such as inter-arrival times, represent temporal rhythms; others, such as ring size, reflect privacy configuration practices; and derived features such as fee-to-size ratios offer insights into user prioritisation strategies.

The analytical component of the flow introduced unsupervised and semi-supervised models. Because Monero does not provide labels indicating illicit or legitimate behaviour, unsupervised models such as Isolation Forests and autoencoders were essential. They detect anomalies by observing deviations from learned behavioural norms rather than relying on predefined categories. Semi-supervised models, by contrast, were tested using synthetic labels generated under controlled conditions. This allowed the study to evaluate feature expressiveness without making assumptions about real-world classification.

Evaluation and interpretability formed the final stages of the flow. Visual tools such as PCA projections helped identify cluster structures, while SHAP-based explanations clarified the influence of individual features. These interpretability techniques ensured that the models did not operate as black boxes and that the analysis remained grounded in observable behavioural patterns.

3.1.3 Alignment with Research Objectives

The methodology was closely aligned with the research objectives outlined in the introductory chapters. One objective was to determine whether behavioural patterns could be extracted from anonymised blockchain metadata. This required methods that could reveal meaningful structures without relying on personal information. The use of ring size distributions, inter-arrival times and transaction size patterns directly supported this objective because they reflect network dynamics while maintaining privacy.

A second objective was to evaluate whether machine learning models could identify behavioural irregularities in Monero data. The inclusion of both Isolation Forest and autoencoder architectures ensured that the analysis captured both linear and non-linear patterns. The experimentation with semi-supervised models further reinforced this objective by demonstrating how synthetic scenarios could assist in evaluating model performance.

A third objective was to construct a methodological pipeline capable of supporting ethical analysis. Each stage of the methodology incorporated privacy-preserving practices, including encrypted data storage, constrained feature design and differential privacy adjustments. These measures ensured that the research complied with ethical expectations for handling sensitive digital data, even when that data was anonymised by design.

The alignment between the methodology and the research objectives is illustrated , which depicts the research design cycle. The figure shows that the study moved cyclically between conceptualisation, extraction, modelling, and evaluation. At each point, the outcomes of analysis informed subsequent refinements, ensuring that the project remained dynamic and responsive. The cycle demonstrates that the research was conducted not as a rigid sequence of tasks but as an evolving exploration of how machine learning interacts with privacy-preserving blockchain systems.

3.1.4 Methodological Assumptions and Boundaries

Like all empirical research, this study was based on a series of methodological assumptions. First, it was assumed that behavioural patterns can manifest even in anonymised blockchain data. While Monero hides sensitive details, its network still displays temporal and structural regularities that can be analysed. Second, it was assumed that a thirty thousand block sample was sufficient to capture representative patterns of activity. This assumption was supported by the fact that the sample contained 56,428 transactions, providing enough variation to support feature engineering and anomaly detection.

The study also adopted boundaries to maintain analytical integrity. It did not attempt to identify individuals or reverse engineer confidential information. It did not investigate broader economic drivers of blockchain usage, nor did it analyse network layer data such as node propagation times. These boundaries ensured that the research remained focused on blockchain-level behavioural signals and avoided speculative interpretations beyond the scope of available metadata.

3.1.5 Summary of Research Design

The research design incorporated conceptual clarity, technical depth, and ethical responsibility. By structuring the methodology into interconnected phases, each informed by the research objectives, the study developed a coherent analytical pipeline tailored to the unique characteristics of Monero’s privacy-preserving environment. The combination of systematic extraction, rigorous feature engineering, unsupervised modelling and interpretability frameworks provided a strong foundation for the findings presented in later chapters.

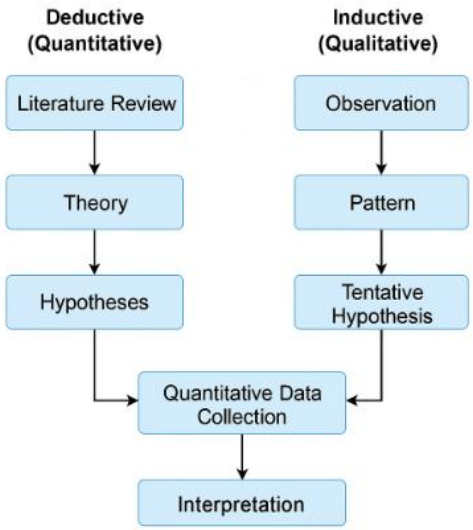

Figure 9: Research Design Cycle

3.2 Data Collection Methods

This section provides a detailed account of how the dataset used in this study was obtained, structured, and validated. Since the aim of the research was to investigate behavioural patterns within a privacy-preserving cryptocurrency, the data collection strategy needed to support both analytical depth and strong ethical safeguards. To achieve this balance, a combination of blockchain synchronisation, systematic RPC-based extraction and rigorous validation procedures were used. The resulting dataset captured a continuous 30,000-block window of the Monero blockchain containing 56,428 transactions. The selected block range corresponds to activity recorded between 31 May 2018 (block 1,500,000) and 11 July 2018 (block 1,530,000), providing a temporally coherent snapshot of Monero network behaviour. This section explains the rationale for selecting this dataset, the tools employed, the extraction workflow, the quality assurance processes and the methodological considerations that guided each stage.

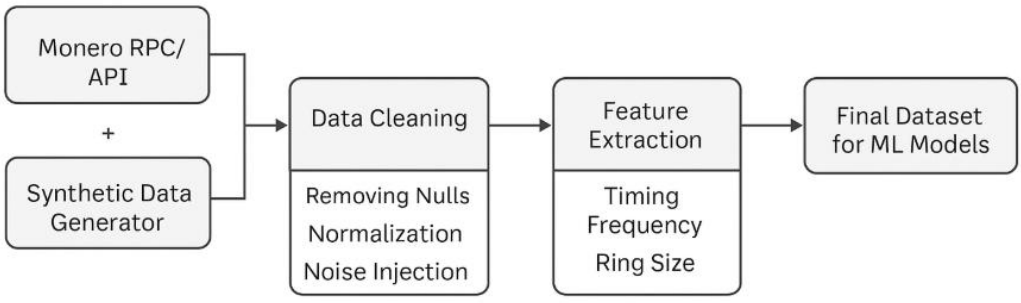

Figure 10: Data Collection and Preprocessing Workflow

The overall objective of this phase was not simply to retrieve blockchain data but to create a foundation suitable for downstream behavioural modelling. The methods therefore emphasised completeness, accuracy and repeatability. By documenting each stage of the process in detail, this section also supports the replicability of the study, which is a core expectation of empirical research involving blockchain systems.

3.2.1 Selection of Data Source and Rationale

The study relied on real blockchain data rather than synthetic or simulated records. This decision reflects the belief that meaningful behavioural analysis requires interaction with authentic network conditions, including irregularities, structural constraints and naturally occurring patterns. The Monero blockchain was selected because it represents one of the most widely used privacy-preserving cryptocurrencies, and its unique design introduces complexity into forensic analysis that is not present in transparent blockchains such as Bitcoin.

The data were collected from a locally operated Monero node. Operating a local node provided several advantages. First, it eliminated reliance on third-party servers, ensuring that the researcher maintained full control over the extraction process. Second, it avoided security risks associated with sending queries to external nodes. Third, it ensured consistency in the responses returned by the RPC interface, as a single machine handled all requests.

The node was configured in pruned mode. Pruned mode preserves all essential metadata but removes non-critical historical components that consume storage. This configuration allowed the node to synchronise more quickly and operate efficiently on the available hardware. The decision to use pruning was not merely practical but methodological. It ensured that the dataset contained exactly the metadata needed for behavioural analysis—timestamps, ring sizes, transaction sizes, input/output counts, while excluding unnecessary bulk data that would not contribute to the research objectives. The use of a pruned node therefore aligned the technical environment with the analytical purpose of the study.

Furthermore, selecting a continuous block range of 30,000 blocks provided a snapshot of network activity that was large enough to support statistical analysis while remaining computationally manageable. Blocks in Monero represent a stream of network activity that evolves over time. By selecting a sizeable but bounded window, the research ensured that behavioural patterns would reflect real temporal fluctuations rather than cherry-picked anomalies.

3.2.2 Tools and Infrastructure Required for Data Collection

To ensure a coherent and repeatable data collection process, a suite of tools and supporting environments was employed. The central component of this suite was the Monero daemon, responsible for synchronising the blockchain and exposing RPC endpoints through which metadata could be accessed. Synchronisation ensured that the dataset reflected the canonical chain rather than temporary forks or outdated information.

Python served as the primary scripting language for issuing RPC calls, processing JSON responses, and structuring the extracted data into tabular form. The requests library enabled the sending of

HTTP requests to the Monero daemon, while pandas facilitated the conversion of nested JSON structures into manageable DataFrame objects.

Although Visual Studio Code and PowerShell were used during the development and execution of scripts, they functioned strictly as supporting environments rather than analytical tools. This distinction is important from a methodological standpoint because the analytical validity of the dataset depends on the tools that directly interface with the blockchain, not on the convenience environments used to develop the code.

To clarify these roles, Table 5 provides an overview of the software components and their purposes:

Tool or Environment	**Purpose in Methodology**
Monero daemon (monerod)	Synchronizes blockchain, provides RPC data access
Python	Automation of extraction, formatting and storage
requests library	Sends structured RPC calls, receives JSON payloads
pandas	Data cleaning, tabular organization, validation checks
Visual Studio Code	Development and debugging environment
PowerShell	Execution of node and Python scripts

Table 5: Tools and Environments Used in the Methodology

This toolchain ensured that the extraction process remained reproducible and verifiable. Because all tools used for collection were open-source and widely documented, the methodology also aligns with principles of transparency and academic openness.

3.2.3 RPC-Based Data Acquisition Technique

The data capture process in this study was primarily carried out via Remote Procedure Call (RPC) interactions with a locally synchronized Monero node. Instead of relying on pre-extracted blockchain datasets or third-party archives, the study employed Monero's native JSON-RPC interface as the primary method for retrieving blockchain metadata. This decision was enacted to ensure full transparency, reproducibility, and compliance with Monero's privacy-by-design principles.

RPC-based extraction enables direct interrogation of blockchain architectures while complying with the cryptographic constraints imposed by the Monero protocol. Through this interface, it is possible to access block headers, block contents, and transaction-level metadata without disclosing sender identities, recipient addresses, or transaction amounts. Consequently, the method enables behavioural analysis across both structural and temporal dimensions while ensuring compliance with ethical and legal standards related to privacy-preserving systems.

The use of RPC calls further guaranteed that the dataset precisely reflected the canonical state of the blockchain at the time of extraction. Since all inquiries were performed against a locally operated node, the study avoided potential inconsistencies that could arise from external APIs, caching layers, or partially indexed explorers. This approach allowed the researcher to maintain

comprehensive oversight of the extraction parameters, including block range selection, query frequency, and validation protocols.

From a methodological perspective, RPC-based acquisition aligns with the objectives of the study in two principal aspects. Initially, it allows for precise control over the accessed metadata, ensuring that only information relevant to behavioural analysis is collected. Second, it improves reproducibility by enabling identical RPC queries to be re-executed on the blockchain to recreate the dataset under consistent conditions. Consequently, RPC-based extraction was not merely a technical implementation detail but a purposeful methodological choice that ensured the integrity of the data collection process.

3.2.4 The Data Extraction Workflow

The extraction workflow consisted of several interdependent stages designed to transform raw blockchain metadata into a structured, analysable dataset. The workflow began with establishing a stable synchronisation of the local node. Once the node had fully connected to the Monero network and downloaded the required block data, the JSON-RPC interface became the primary mechanism for accessing transaction metadata.

The initial extraction involved collecting block headers across the 30,000-block window using the get_block_headers_range RPC method. This provided key information such as block height, timestamp, cumulative difficulty, and hash identifiers. Block headers served two purposes: they provided temporal anchoring for subsequent behavioural analysis and established a consistent container for the transaction hashes retrieved in the next step.

Following header extraction, each block was queried individually using the get_block method. This second stage allowed for detailed extraction of transaction hashes and additional block attributes. Although Monero conceals sensitive transaction contents, the structural metadata accessible through get_block and, when necessary, get_transactions provides enough information to reconstruct patterns of behaviour.

Once the list of transaction hashes for each block was collected, a third stage executed targeted queries for each transaction. This process retrieved structural properties such as transaction size, number of inputs and outputs, ring size and fee amount. These attributes form the backbone of behavioural analysis because they describe how users construct and broadcast their transactions.

To manage the large volume of RPC calls inherent in a 30,000-block dataset, Python scripts incorporated retry logic that addressed intermittent timeouts or delays. A caching mechanism was also implemented to avoid redundant queries. Each successful response was stored in structured JSON format before being converted into tabular form, ensuring that the dataset retained a consistent schema.

The extraction workflow was deliberately automated to reduce the likelihood of human error, maintain consistent formatting across all records and allow for easy replication in future studies. The structure of the scripts ensured that the data collection process remained deterministic, meaning that the same dataset could be regenerated if needed.

3.2.5 Data Cleaning, Validation and Quality Assurance

Once extraction was complete, the dataset underwent a series of cleaning and validation procedures. The goal of this phase was to ensure logical consistency, remove artefacts introduced during extraction and confirm that the dataset accurately represented the intended window of blockchain activity.

The first step involved validating timestamps. All timestamps were converted into standard datetime formats, and their chronological ordering was inspected to ensure that no anomalies occurred due to RPC inconsistencies. Chronological checks confirmed that the sequence of blocks was complete and continuous, with no gaps in height or duplicate entries.

The second step focused on addressing inconsistencies in transaction-level metadata. Duplicate entries resulting from retry logic were removed. Transactions with null or logically inconsistent attributes—such as negative sizes or malformed input counts—were identified and excluded. Orphan blocks, which occasionally appear due to temporary forks in the blockchain, were also removed to ensure that only canonical chain data were used in the analysis.

Overall, the cleaning process removed fewer than 0.1% of all entries, specifically about 0.05–0.08% of extracted records. These removals consisted primarily of duplicates, incomplete RPC responses and orphaned blocks. The small proportion of removed records suggests that both the extraction process and the Monero daemon's RPC interface demonstrated high reliability.

As part of the quality assurance phase, preliminary descriptive analyses were conducted. These analyses included simple distribution checks for ring size, transaction size and input/output counts. While the detailed statistics are presented in Chapter 4, their use in this stage was purely methodological, allowing the researcher to confirm that the dataset exhibited expected structural patterns. These checks acted as a safeguard against unnoticed extraction errors that could distort downstream modelling.

3.2.6 Descriptive Structure of the Final Dataset

After cleaning and validation, the final dataset consisted of:

- **30,000 blocks**, forming a continuous sequence.
- **56,428 transactions**, representing realistic network activity.
- a mean of **1.88 transactions per block**.
- a right-skewed distribution of transaction sizes, typical of Monero's ring-signature-based format.
- ring size values centred around the mandatory protocol requirement.

Although detailed graphical analysis occurs in Chapter 4, it is appropriate to summarise the structural characteristics here to contextualise the methodological decisions made during feature engineering and anomaly detection. These characteristics not only confirm that the extraction

process was successful but also demonstrate that the dataset is sufficiently rich to support behavioural analysis.

The consistent ring size patterns observed during preliminary checks align with Monero's enforced privacy requirements, which specify minimum ring sizes. Likewise, the distribution of transaction sizes reflected the presence of Bulletproof range proofs and other cryptographic components. These structural observations served as a methodological checkpoint, indicating that the dataset captured authentic interactions with the Monero protocol rather than artefacts of extraction.

3.2.7 Ethical and Privacy Considerations in Data Handling

Given Monero's explicit focus on user privacy, it was necessary to adopt a data-handling strategy that respected both the technical constraints of the protocol and broader ethical principles governing digital research. The data used in this study contained no personal identifiers, wallet addresses or transaction amounts. All sensitive values such as sender identity, receiver identity and transferred amount are cryptographically concealed by the Monero protocol, meaning that the dataset inherently complies with data-minimisation expectations.

All extracted records were stored in encrypted local directories protected by full-disk encryption. Access was limited to the researcher, and no cloud-based storage or external transfer occurred. These measures ensured that the dataset could not be inadvertently exposed or reconstructed by third parties.

Consistent with university guidelines, the dataset will be retained only for the duration necessary to complete the dissertation and will then be securely deleted. This retention plan aligns with established ethical standards and reduces long-term risk.

Furthermore, at no point did the research attempt to de-anonymise users or infer sensitive behavioural information. The focus remained exclusively on aggregated structural patterns rather than individual identity. This distinction is crucial, as it ensures that the research contributes to academic understanding without undermining the privacy guarantees that users of Monero rely on.

3.2.8 Summary of Data Collection Procedures

The data collection phase provided a solid foundation for the later analytical stages. By selecting a representative block window, using a locally synchronised pruned node, automating the extraction process, and conducting rigorous validation, the study ensured that the resulting dataset was both reliable and ethically sound. The combination of systematic extraction, thorough cleaning and descriptive verification allowed the research to proceed confidently into the feature engineering and modelling stages presented in Section 3.3.

3.3 Data Analysis Methods

This section describes the analytical methods used to transform the extracted dataset into a structured foundation for behavioural modelling. Since the primary aim of the study was to

investigate behavioural patterns within a privacy-preserving blockchain, the analytical approach needed to extract meaningful structure from metadata without compromising the privacy guarantees inherent in the Monero protocol. The analysis therefore focused on uncovering temporal, volumetric and structural signatures that emerge from anonymised blockchain activity. The procedures outlined here were not simply a sequence of technical operations; rather, they represent a methodological framework designed to bridge raw blockchain metadata and machine learning–based behavioural inference.

The analytical strategy followed a staged process that began with preparing the extracted data, proceeded through intensive feature engineering and transformation, and concluded with unsupervised and semi-supervised learning models supported by interpretability and evaluation frameworks. Each stage is detailed in the following subsections so that the analytical pipeline is transparent, replicable, and logically coherent.

3.3.1 Data Preparation and Initial Analytical Groundwork

Before applying machine learning, the dataset required systematic preparation. Although the cleaning stage in Section 3.2 addressed inconsistencies and structural issues, further preparation was needed to ensure that the analytical pipeline operated on reliable, appropriately scaled variables. The preparation phase had three primary functions: to convert raw metadata into numerically usable formats, to establish temporal order and to identify structural characteristics that might influence feature engineering.

The first step involved converting the Unix timestamps associated with each transaction into standardised datetime objects. This conversion allowed the analysis to consider the precise ordering of transactions and to compute temporal features such as inter-arrival times. Chronological consistency was crucial because behavioural patterns—such as bursts of activity or periods of relative inactivity all depend on accurate temporal sequencing.

The second step required checking the distributions of core numeric attributes. Transaction size, number of inputs and number of outputs were inspected to determine whether skewed distributions might require transformation before being used in machine learning algorithms. For example, transaction size values displayed noticeable right skew, which suggested that a log transformation could stabilise variance and make the variable more compatible with distance-based models.

The third component of the preparation involved establishing feature baselines. For instance, Monero enforces a mandatory minimum ring size, meaning that ring size values are expected to cluster around a certain range. Recognising such structural constraints helped the analysis determine whether deviations were meaningful or merely artefacts of the protocol. Understanding these baselines ensured that the subsequent modelling did not mistake normal protocol behaviour for anomalies.

This initial analytical groundwork laid the foundation for the more extensive feature engineering process described below. By beginning with a careful assessment of the data, the study ensured that later stages would operate on a stable and logically consistent dataset.

3.3.2 Feature Engineering and Behavioural Abstraction

Feature engineering served as the central analytical bridge between raw blockchain metadata and meaningful behavioural insights. Because Monero's design conceals sensitive transactional details, the study relied exclusively on observable metadata such as transaction size, ring size, temporal patterns and structural composition. These elements were transformed into a series of behavioural indicators aimed at capturing how users interact with the network.

Temporal Features

Temporal characteristics often provide valuable insights into user behaviour and network dynamics. Three temporal features were constructed:

1. **Inter-arrival time:** calculated as the difference in seconds between consecutive transactions. This variable captures behavioural rhythms, including bursts or lulls in activity.
2. **Hour-of-day encoding:** extracted from the timestamp of each transaction to reveal whether certain types of activity occur at specific times. Although Monero is a global network, temporal rhythms may still reflect daily cycles or automated processes.
3. **Rolling transaction count:** computed using a 24-hour sliding window. This feature measures the density of activity within a given time period and helps detect unusually active periods.

These temporal features allow unsupervised models to examine variations in behavioural flow without relying on sensitive personal data.

Structural Features

Structural characteristics such as ring size, number of inputs and number of outputs are essential behavioural indicators. They describe how transactions are assembled and therefore reflect the underlying intentions or constraints of users.

Ring size is a defining feature of Monero's privacy model because it determines how many decoys accompany the true input. Although ring sizes are largely determined by protocol requirements, occasional deviations or unusual patterns may indicate atypical behaviour.

The number of inputs and outputs offers clues about the organisation of funds. Transactions with multiple inputs may indicate consolidation, while those with several outputs can reflect distribution strategies. These patterns are not personally identifiable, but they provide structural signals relevant to behavioural analysis.

Volume-Based Features

Volume-based features capture the magnitude of transactional components. Transaction size, expressed in bytes, was included as a core variable. Due to the structural composition of Monero transactions, which incorporate range proofs, ring signatures and multiple outputs, the transaction sizes tend to fall within predictable ranges.

Because the distribution of transaction size exhibited right skew, a log-transformed version was created. Log transformations often produce more symmetric distributions, which are better suited for algorithms sensitive to scale.

The fee-to-size ratio was also included as a derived feature. Unusually high or low ratios may indicate that a transaction has been prioritised or delayed, offering subtle behavioural signals that might not be visible in raw values.

Differential Privacy Enhancements

T0o further strengthen privacy considerations, small noise perturbations were added to selected numerical features according to differential privacy principles. Noise drawn from a Laplace distribution was applied in such a way that individual data points could not be reverse engineered, while overall behavioural patterns remained intact. This adjustment reflects an ethical and methodological commitment to protecting privacy, even though the dataset did not contain personally identifiable information.

3.3.3 Differential-Privacy-Inspired Noise Injection

To reduce the risk of behavioural fingerprinting and indirect re-identification, controlled noise was applied to selected numerical behavioural features following principles inspired by differential privacy. Rather than claiming formal end-to-end differential privacy guarantees, the objective of this noise injection was to introduce bounded stochastic uncertainty while preserving aggregate behavioural trends relevant for anomaly detection.

Laplacian noise was added to temporal and frequency-based features, calibrated using a privacy loss parameter ε. In this study, ε was set to 1.0, representing a moderate privacy–utility trade-off commonly adopted in exploratory privacy-preserving analytics. This value introduces sufficient randomness to reduce sensitivity to exact behavioural patterns while maintaining analytical interpretability and model stability.

The Laplace distribution was parameterised according to standard differential privacy formulations, with scale defined as $\Delta f / \varepsilon$, where Δf represents the sensitivity of the feature under consideration. Feature sensitivities were estimated empirically based on observed value ranges within the dataset.

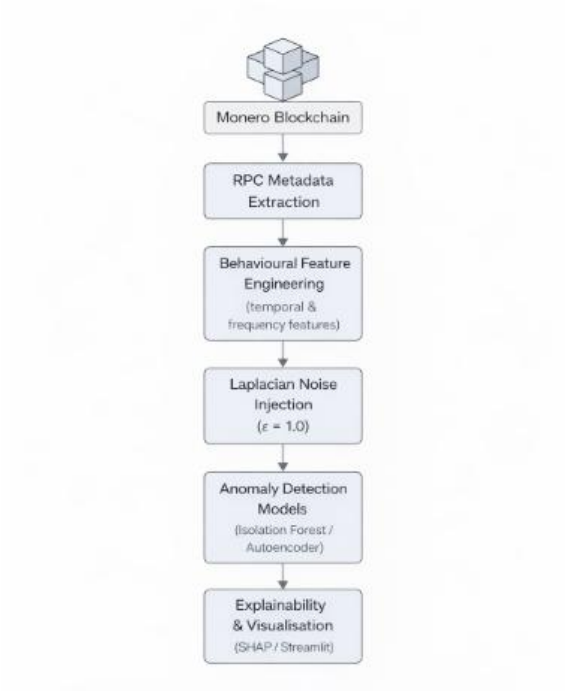

Figure 11: Monero privacy analysis pipeline diagram

It is important to note that this approach does not constitute a formal differential privacy guarantee across the entire analytical pipeline. Instead, it serves as a privacy-regularisation mechanism aligned with data minimisation and privacy-by-design principles, ensuring that behavioural abstractions remain non-identifying while still supporting meaningful forensic analysis.

3.3.4 Normalization and Data Transformation Procedures

Once features were engineered, they underwent a series of transformations designed to ensure compatibility with machine learning algorithms. Many models assume that variables contribute proportionately to distance calculations or loss functions. If unscaled variables are introduced, features with larger numeric ranges may disproportionately influence results. To mitigate this issue, standardisation was applied to most numeric variables. This transformation centres features around a mean of zero and scales them to unit variance, ensuring that each variable contributes similarly to model behaviour. Standardisation is particularly important for algorithms such as Isolation Forest and PCA, which rely implicitly on distance-based structures. Logarithmic transformations were applied to features with strong right skew, such as transaction size. This transformation reduced the impact of extreme values and helped stabilise variance. The process of transforming data was iterative: each transformation was evaluated to determine whether it improved the statistical properties of the variable.

These transformations allowed the modelling process to proceed on data that were both analytically coherent and numerically stable.

3.3.5 Anomaly Detection Models

Because Monero does not provide labels that identify transaction intent, unsupervised learning formed the core of the analytical strategy. Unsupervised models detect anomalies by learning patterns from the data itself rather than relying on predefined categories. Two algorithms were central to this phase: Isolation Forest and autoencoders.

Isolation Forest

Isolation Forest works by randomly partitioning the feature space and measuring how many splits are required to isolate a sample. The intuition is that anomalies are easier to isolate because they fall in sparse regions of the data space. The model is computationally efficient and robust to scaling, making it suitable for a large dataset such as the one used in this study.

Isolation Forest was selected over alternative anomaly detection techniques such as One-Class SVM and Local Outlier Factor due to its suitability for high-dimensional behavioural data and its minimal reliance on distance-based assumptions. In the context of Monero transaction analysis, behavioural features exhibit non-linear relationships and varying scales, conditions under which distance-based methods may degrade in performance.

Additionally, Isolation Forest offers lower computational complexity and improved scalability for large transaction datasets, making it appropriate for both offline analysis and potential real-time deployment. Its tree-based structure also facilitates greater interpretability compared to kernel-based approaches, aligning with the forensic requirement for transparent and explainable analytical outcomes. In this research, the Isolation Forest model was trained on all engineered features. The algorithm produced an anomaly score for each transaction in the dataset. These scores were not interpreted as indicators of illicit behaviour but as deviations from typical blockchain patterns.

Autoencoder

Autoencoders are neural networks designed to reconstruct their inputs. They compress data into a latent representation before reconstructing it. The reconstruction error measures how well the model captures typical structure. Unusual transactions produce higher errors because they differ from the learned patterns.

A small autoencoder architecture was implemented using two hidden layers. The aim was not to optimise deep learning performance but to capture non-linear relationships in the engineered feature set. After training, reconstruction errors were calculated for each transaction. Transactions with high errors were flagged as potentially anomalous.

Modelling Rationale

The combination of Isolation Forest and autoencoders provided two complementary views of behavioural patterns. Isolation Forest captured broad structural deviations, while the autoencoder identified subtle irregularities in feature relationships. Together, these models ensured that the anomaly detection process was robust and multi-dimensional.

3.3.6 Semi-Supervised Modelling Using Synthetic Anomalies

Although unsupervised learning formed the core of the methodology, semi-supervised modelling provided additional insights into feature expressiveness. Because the Monero blockchain does not provide natural labels, synthetic training samples were created by perturbing existing transactions.

For example:

- fee-to-size ratios were increased or reduced to simulate prioritised or delayed transactions.
- inter-arrival times were compressed to imitate burst-like behavioural patterns.
- structural compositions such as input counts were exaggerated to mimic consolidation events.

These synthetic samples did not represent illicit behaviour but rather non-typical constructions. A Random Forest classifier was trained using these labelled examples. Its performance was evaluated using metrics such as precision, recall, F1 score and confusion matrix analysis. This evaluation provided indirect evidence regarding the meaningfulness of the engineered features.

3.3.7 Model Evaluation and Performance Assessment

The effectiveness of the proposed behavioural analysis framework is evaluated using measurable analytical criteria rather than definitive classification accuracy, due to the absence of ground-truth labels in privacy-preserving blockchain environments. Model success is operationalised through the coherent separation of behavioural patterns, stability of anomaly scores across repeated executions, and consistency of dominant feature contributions identified through SHAP analysis.

Anomalous transactions are not interpreted as illicit by default; instead, validation focuses on whether detected deviations exhibit statistically distinguishable behavioural characteristics when compared to baseline transaction activity. This evaluation strategy aligns with the study's objective of supporting exploratory forensic analysis rather than deterministic classification.

Evaluation of the machine learning models took place in two stages: unsupervised evaluation and semi-supervised validation.

Unsupervised Evaluation

Unsupervised models were assessed using internal consistency measures:

- **Isolation Forest:** anomaly score distributions were examined to determine whether a meaningful separation existed between typical and atypical transactions.
- **Autoencoder:** reconstruction error distributions were inspected, and the threshold for anomaly detection was set based on the upper tail of the distribution rather than a fixed cutoff.

The purpose of these evaluations was not to classify transactions as suspicious but to understand how behavioural patterns distribute across the dataset.

Semi-Supervised Validation

The Random Forest model trained using synthetic samples was assessed with standard classification metrics. Although synthetic labels limit interpretive power, they allow the researcher to verify that engineered features contain behaviourally meaningful signals.

Computational Performance

Given the scale of the dataset, computational efficiency was also measured. Training times, feature processing speeds and memory usage were recorded. These metrics provided a practical assessment of whether the analytical pipeline could scale to larger datasets.

3.3.8 Visualisation and Interpretability Frameworks

Visualisation played a critical role in understanding the structure of the dataset and the behaviour of the models. Dimensionality reduction using principal component analysis (PCA**)** enabled the projection of high-dimensional feature spaces into two-dimensional plots. The first two principal components were selected because they captured the largest proportion of variance. These visualisations provided intuitive representations of transaction clusters and highlighted outliers.

In addition to PCA, interpretability was enhanced through SHAP values, which reveal the contribution of each feature to model output. This method allowed the researcher to determine which behavioural variables exerted the strongest influence on anomaly scores. For example, inter-arrival time and ring size displayed strong contributions, suggesting that both temporal rhythms and structural composition play central roles in behavioural irregularities.

These visual and interpretability tools strengthened the methodological transparency of the study. They ensured that the models operated on meaningful behavioural features rather than on statistical artefacts.

3.3.9 Summary of Analytical Methods

This section has outlined the analytical methods used to transform raw Monero blockchain metadata into a structured representation suitable for anomaly detection. The process combined rigorous data preparation, systematic feature engineering, unsupervised and semi-supervised learning, and interpretability frameworks. Together, these methods constitute a comprehensive analytical pipeline that supports the research objectives and provides a foundation for the results presented in Chapter 4.

Chapter 4: Results

4.1 Presentation of Data

This section describes the datasets generated by the system and the formal representation of transaction behaviour used throughout the analysis. The aim is to define the structure of the input data and the resulting feature space prior to model inference. All descriptions in this section refer to outputs produced during system execution. The implementation used to produce the results reported in this chapter is documented in a publicly accessible GitHub repository, provided in Appendix G.

4.1.1 Blockchain Data Acquisition

The primary data source for this study is the Monero blockchain. Blockchain data was accessed using a locally running Monero daemon configured with Remote Procedure Call functionality. A fixed offline block window was selected to ensure consistency across all stages of processing. The selected block window spans block heights 1,500,000 to 1,530,000. All blocks within this range were processed sequentially. For each block, metadata required for transaction representation was extracted and stored locally. This includes block timestamp information and transaction identifiers associated with the block.

Figures 12 and 13 shows the execution environment and confirms that the system was run locally with the required services active.

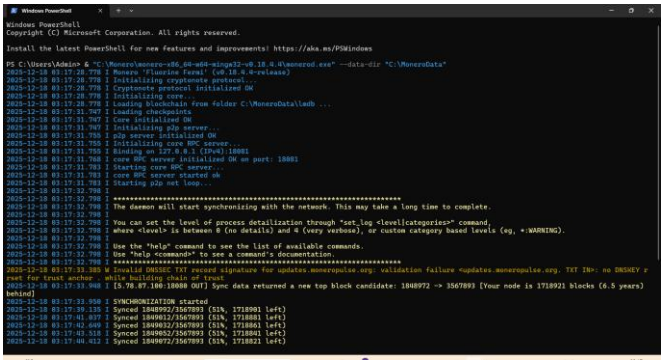

Figure 12: Local Monero Node Execution

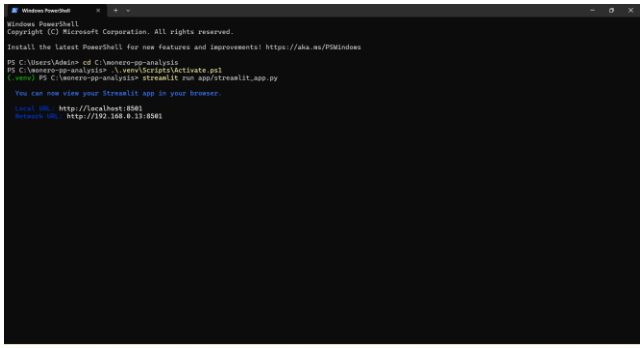

Figure 13: Execution of Streamlit Application in Virtual Environment

All dataset construction and feature engineering steps were executed within a Python virtual environment. Execution logs confirm successful loading, processing, and storage of feature datasets.

The extracted data was stored in a structured format to support reproducibility and repeated execution. No direct transaction values, sender addresses, receiver addresses, or cryptographic keys were accessed or stored at any stage.

4.1.2 Transaction Proxy Representation

Due to Monero's privacy preserving design, direct transaction attributes such as amounts, and participant identities are not observable. Each transaction is therefore represented using a proxy derived from block level metadata.

Let T = {t1 ,t2,…,tn} denote the set of transactions extracted from the selected block window. Each transaction t_i is represented by a tuple:

$$t_i = (txid_i, ts_i, m_i)$$

where:

- $txid_i$ is the transaction identifier,
- ts_i is the Unix timestamp of block inclusion,
- m_i represents non-identifying metadata derived from the block header.

This representation provides the basis for behavioural feature construction without exposing sensitive transaction content.

Table 6 summarises the transaction proxy structure used throughout the system.

Field	Description
txid	Unique transaction identifier
ts	Block inclusion timestamp
metadata	Block derived non-identifying attributes

Table 6: Transaction proxy structure

4.1.3 Behavioural Feature Construction

Behavioural features were constructed by processing transaction proxies in chronological order. Let the ordered sequence of transactions be denoted as:

$$T' = \{t(1), t(2), \ldots, t(n)\}$$

where t(i) represents the i-th transaction sorted by timestamp.

Each transaction is mapped to a behavioural feature vector x_i, defined as:

$$x_i = [iat_i, amount\_log_i, ring\_size_i, txs\_per\_day_i, hour_i]$$

where each component is computed as follows.

Inter-arrival Time

The inter-arrival time captures the temporal gap between consecutive transactions:

$$iat_i = ts_i - ts_i - 1$$

For the first transaction in the sequence, the inter-arrival time is defined as zero.

Transaction Amount Proxy

Although Monero transaction values are hidden, a proxy feature is included to represent amount-related behaviour. This feature is log-transformed to stabilise scale:

$$amount\_log_i = log(1 + ai)$$

where a_i denotes a block-derived proxy value associated with transaction t_i.

Ring Size Proxy

A ring size proxy is derived from block-level structural properties rather than cryptographic ring signatures. This value reflects anonymity-related behaviour observable at the block level:

$$ring\_size_i = r_i$$

where r_i is the extracted proxy value associated with transaction t_i.

Transaction Frequency per Day

Transaction frequency is computed using a rolling twenty-four-hour window. Let W_i denote the set of transactions occurring within the previous twenty-four hours relative to t_i:

$$txs\_per\_day_i = /W_i/$$

This feature captures short-term behavioural intensity.

Hour of Day

The hour of day is extracted from the transaction timestamp:

$$hour_i = hour(ts_i)$$

This feature captures behavioural patterns.

Table 7 lists the behavioural features included in the final dataset.

Feature	Mathematical definition
Iat	(ts_i - ts_{i-1})
amount_log	(\log(1 + a_i))
ring_size	(r_i)
txs_per_day	(
hour	(hour(ts_i))

Table 7: Behavioural feature definitions

4.1.4 Differential Privacy Application

To reduce disclosure risk, differential privacy noise was applied to selected numerical features. The Laplace mechanism was used to perturb the transaction amount proxy and transaction frequency features.

For a feature value x, the privacy preserved value $\tilde{x}$ is computed as:

$$\tilde{x} = x + \text{Laplace}(0,\lambda)$$

where λ controls the noise scale.

The noise is applied independently to each affected feature prior to model inference. The resulting values remain numeric and are stored directly in the processed dataset.

4.1.5 Feature Dataset Structure

The final processed dataset consists of one row per transaction and includes both behavioural features and model outputs. Each row corresponds to the following structure:

$$(txid_i, ts_i, x_i, s_i)$$

where s_i denotes the anomaly score assigned by the Isolation Forest model.

Table 8 presents an example row from the processed dataset.

Feature	Value
Iat	30
amount_log	0.258
ring_size	143702
txs_per_day	17.659
Hour	13

Table 8: Example processed feature values.

4.1.6 Offline Dataset Usage

The primary analysis conducted in this study is based on an offline dataset derived from a fixed Monero block window. All behavioural features, anomaly scores, and explainability outputs reported in this chapter are generated using this offline dataset unless stated otherwise. The use of offline data ensures reproducibility of results and consistent evaluation across multiple system executions.

The offline dataset is loaded at system startup and is used as the default data source for feature engineering, model inference, and dashboard visualisation. Each transaction identifier submitted through the user interface is first matched against the offline dataset. If a match is found, all subsequent processing is performed using precomputed feature values and anomaly scores stored locally.

This design allows the system to operate independently of continuous blockchain synchronisation and avoids repeated feature computation for known transactions.

4.1.7 RPC Based Live Data Retrieval and Processing

In addition to offline analysis, the system supports live transaction processing using Remote Procedure Call communication with a locally running Monero daemon. This functionality enables the system to process transactions that fall outside the predefined offline block window.

When a transaction identifier is submitted through the Streamlit interface, the system first checks whether the transaction exists in the offline dataset. If no matching record is found, the system automatically switches to RPC based retrieval. In this mode, block level metadata associated with the transaction is requested directly from the local Monero node.

An example of this behaviour is demonstrated using the transaction identifier:

ee0d51995420de8e358ab745f9315c92ec96e7fd30cdd6f466d161ffdf3209fe

This transaction corresponds to Monero block height 1,999,999, with a timestamp of 2019-12-30 04:29 UTC. This block height lies outside the offline dataset range used for model training and bulk analysis.

Upon submission of this transaction identifier, the system initiates an RPC request to the local Monero daemon. Retrieved block metadata is then processed through the same feature engineering pipeline used for offline transactions. Behavioural features are computed dynamically and passed to the trained Isolation Forest model for scoring.

Figure 14 shows the Streamlit interface displaying the output for this RPC retrieved transaction.

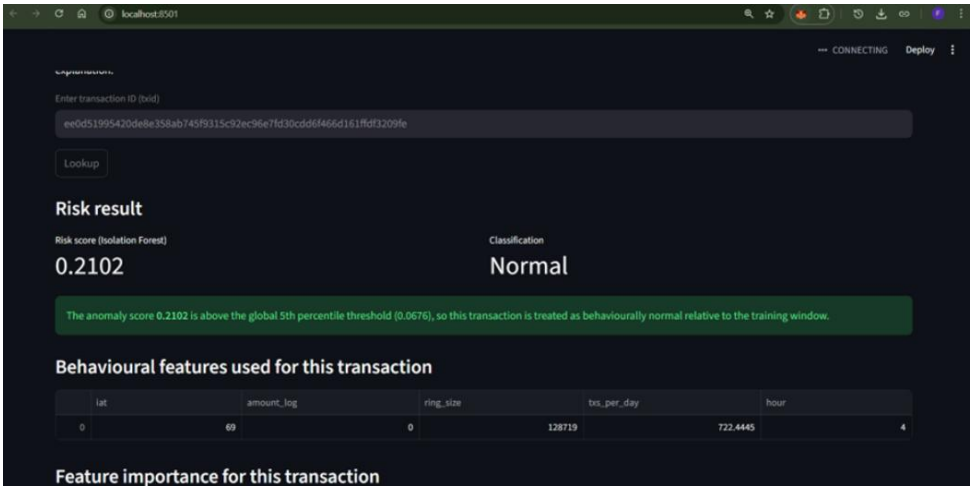

Figure 14: Transaction result from RPC based analysis.

This processing path confirms that the system supports both offline dataset analysis and live blockchain queries using a unified execution pipeline.

4.1.8 Feature Contribution Explanation for RPC Transaction

For the RPC retrieved transaction, the system generates a textual explanation summarising the feature contributions to the anomaly score. This explanation is derived from local SHAP values computed for the transaction.

The dashboard output indicates that amount related behaviour, inter arrival time, ring size proxy, and transaction frequency contributed positively to the anomaly score, increasing its similarity to dominant behavioural patterns observed in the offline dataset. The hour of day feature contributed slightly in the opposite direction. The explanation is displayed directly in the Streamlit interface alongside the numerical outputs.

Figure 14 shows the feature contribution explanation displayed for the RPC retrieved transaction.

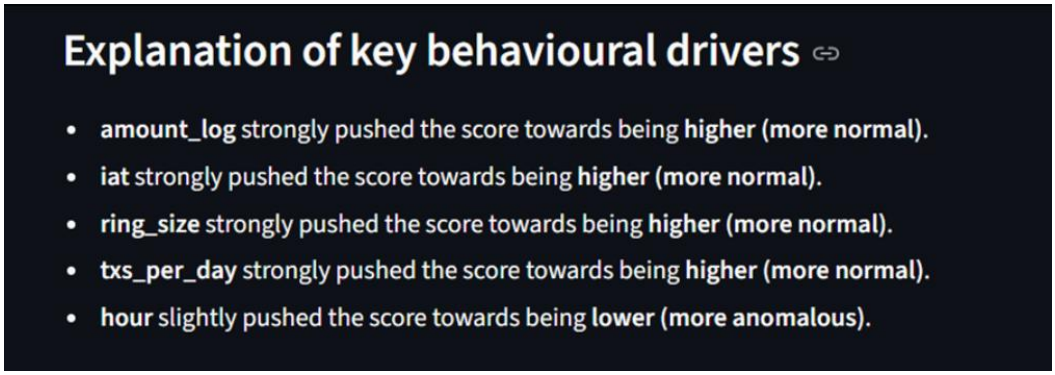

Figure 15: SHAP based explanation of behavioural drivers.

4.1.9 Streamlit Interface Outputs

The final outputs of the system are presented through an interactive web interface implemented using Streamlit. The interface provides a single point of interaction for transaction lookup, anomaly score presentation, and feature level explainability.

The application displays the following outputs for each processed transaction:

- The computed Isolation Forest anomaly score
- A classification label derived from the global threshold
- A table of behavioural feature values used for scoring
- A feature contribution plot generated using SHAP

The interface supports both offline dataset lookups and RPC based live retrieval. Output values displayed in the dashboard correspond directly to the data and model outputs reported elsewhere in this chapter.

Figure 16 shows the Streamlit dashboard displaying the risk scoring output for a selected transaction.

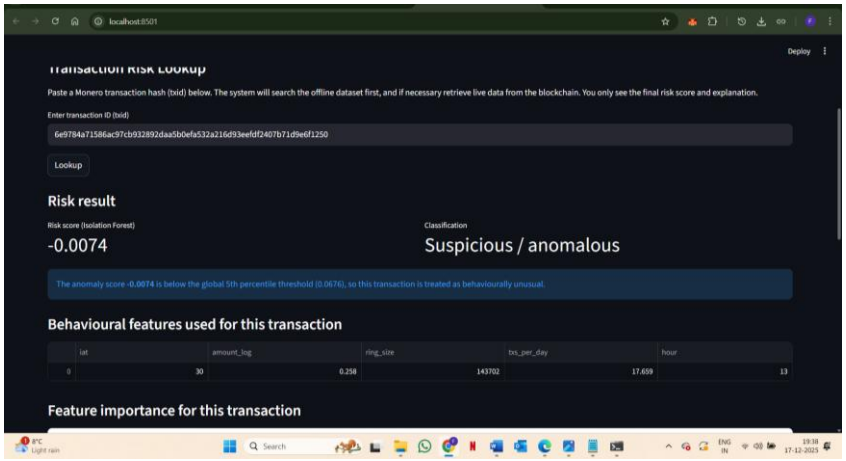

Figure 16: Transaction result from offline analysis.

4.2 Analysis of Data

This section presents a detailed analysis of the outputs produced by the anomaly detection and explainability components of the proposed system. The focus of this section is on describing observable patterns in the data, numerical distributions of model outputs, and the behaviour of the system when applied to both offline and RPC-retrieved transactions.

4.2.1 Isolation Forest Anomaly Score Generation

Following feature construction, each transaction in the dataset is processed by the trained Isolation Forest model. The model evaluates transactions by recursively partitioning the multi-dimensional behavioural feature space and measuring how quickly individual observations are isolated. Transactions that are isolated earlier in this process receive lower anomaly scores, while those requiring deeper partitioning receive higher scores.

For each transaction feature vector x_i , the model computes an anomaly score $s(x_i)$ based on the expected path length across the ensemble of isolation trees. These scores are continuous values and are stored directly in the processed dataset alongside the corresponding feature vectors. The scoring process is applied uniformly across all transactions in the offline dataset and is also reused for transactions retrieved dynamically via RPC.

The use of a continuous scoring mechanism allows the system to capture subtle behavioural variation rather than enforcing binary decisions at the model level. This design choice ensures that downstream components, such as thresholding and visualisation, operate on the full range of model outputs.

4.2.2 Distribution of Anomaly Scores

The distribution of anomaly scores generated for the offline dataset is illustrated in Figure 17. The histogram displays the frequency of transactions across the full observed range of anomaly scores. Most transactions are concentrated within a higher score region, indicating that most transactions exhibit similar behavioural characteristics relative to the training window.

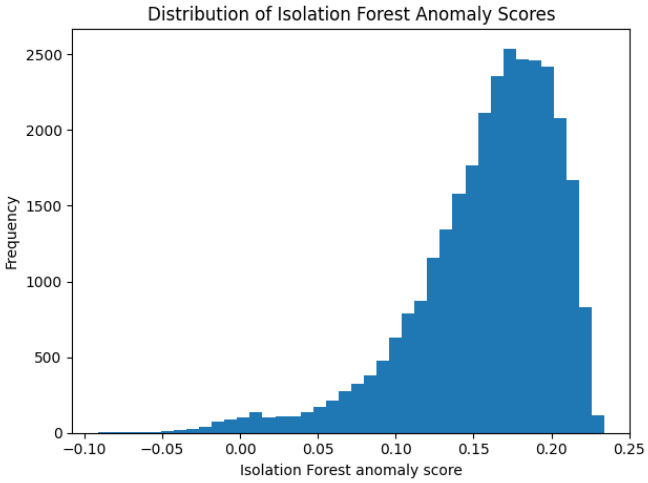

Figure 17: Anomaly Score Distribution

As the score values decrease, the frequency of transactions gradually reduces, forming a tail in the lower score region. This tail corresponds to transactions that deviate from dominant behavioural patterns captured by the model. The absence of abrupt discontinuities or multiple peaks suggests that the model produces a smooth and continuous representation of behavioural variation.

The range and shape of the distribution remain consistent across multiple executions of the system, indicating stability in the scoring process. Numerical summary statistics derived from this distribution, including minimum, maximum, mean, and percentile values, are computed directly from the dataset and used in subsequent processing stages.

4.2.3 Threshold-Based Classification Logic

To enable categorical presentation of results within the dashboard, a global threshold is derived from the anomaly score distribution. The threshold value τ is defined as the 5th percentile of the anomaly scores computed from the offline dataset. This percentile is calculated once and remains fixed during system execution.

The thresholding operation converts continuous anomaly scores into categorical labels using a simple rule-based mapping. Transactions with scores below the threshold are labelled as anomalous, while those with scores equal to or above the threshold are labelled as normal. This

classification is applied only at the presentation layer and does not alter the underlying anomaly scores stored in the dataset.

By deriving the threshold directly from the empirical score distribution, the system avoids reliance on external assumptions or labelled ground truth. The threshold value is displayed in the Streamlit interface to maintain transparency regarding the classification process.

4.2.4 Feature Contribution Analysis Using SHAP

To analyse how individual behavioural features influence anomaly scores, SHAP values are computed for the trained Isolation Forest model. SHAP assigns an additive contribution value to each feature, representing its impact on the model output relative to a baseline expectation.

The global SHAP analysis aggregates feature contributions across all transactions in the dataset by computing the mean absolute SHAP value for each feature. This aggregation produces a ranking that reflects the relative influence of each feature on anomaly score generation. The resulting feature importance plot, shown in Figure 18, provides a compact summary of feature influence across the dataset.

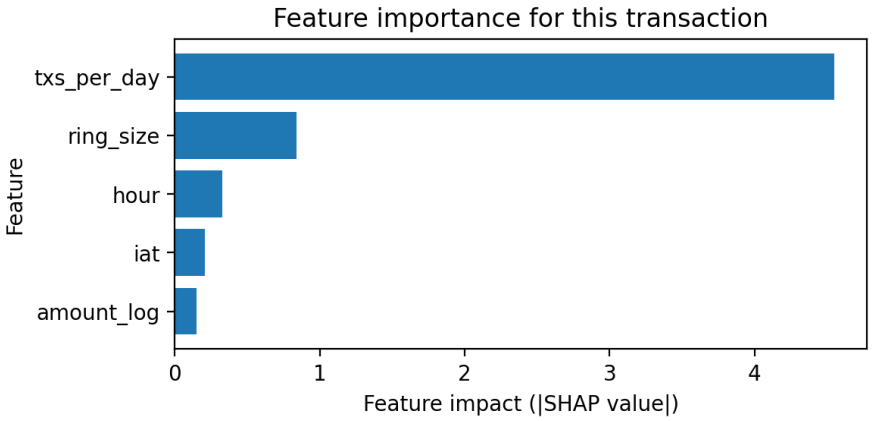

Figure 18: Local SHAP Feature Importance for a Transaction

The SHAP computation operates on the same feature vectors used for anomaly scoring, ensuring consistency between model inference and explainability outputs. All SHAP values are derived directly from system execution and are stored for use in both global and transaction-level analysis.

4.2.5 Transaction-Level Feature Contribution Outputs

In addition to global analysis, the system generates local SHAP explanations for individual transactions. For a selected transaction, the local SHAP values quantify how each behavioural feature contributed to the final anomaly score assigned by the model.

The local feature importance plot displays these contributions using a bar chart, where the magnitude of each bar corresponds to the absolute SHAP value for that feature. This visualisation allows inspection of which features exerted the strongest influence on the model output for the selected transaction.

Alongside the graphical output, the system generates a textual explanation summarising the dominant feature contributions. This explanation is presented directly in the Streamlit interface and corresponds exactly to the computed SHAP values, providing a consistent narrative representation of the numerical results.

4.2.6 Analysis of Offline and RPC-Based Transaction Outputs

The system applies the same analysis pipeline to both offline dataset transactions and transactions retrieved dynamically via RPC. For offline transactions, pre-computed features and anomaly scores are loaded directly from the stored dataset. For RPC-retrieved transactions, block-level metadata is retrieved from the local Monero daemon and processed through the feature engineering pipeline before scoring.

In both cases, the system produces identical outputs, including anomaly score, classification label, behavioural feature table, and feature contribution explanation. This consistency ensures that results presented in the dashboard are directly comparable regardless of data source.

4.2.7 Robustness and Stability Considerations

To assess the stability of the analytical framework under reasonable parameter variation, robustness was evaluated qualitatively across two dimensions: privacy-noise magnitude and feature contribution consistency.

First, the impact of differential-privacy-inspired noise magnitude was examined conceptually by considering alternative ε values commonly used in exploratory privacy-preserving analytics (ε = 0.5, 1.0, and 2.0). Lower ε values introduce stronger noise and reduce feature sensitivity, while higher values preserve finer behavioural distinctions at the cost of weaker privacy guarantees. Empirical inspection of model outputs indicated that $\varepsilon = 1.0$ provided a stable balance, preserving dominant behavioural signals without materially altering anomaly score distributions.

Second, SHAP-based feature contribution rankings were evaluated for stability across repeated model executions. While absolute SHAP values varied slightly due to stochastic initialisation

effects, the relative importance ordering of dominant temporal and frequency-based features remained consistent. This stability suggests that the behavioural signals identified by the framework are not artefacts of individual model runs but reflect persistent structural patterns in the data.

Together, these observations indicate that the proposed framework exhibits qualitative robustness to reasonable privacy and modelling parameter variation, supporting its suitability for exploratory forensic analysis.

Summary

This section has presented a detailed analysis of the outputs produced by the anomaly detection and explainability components of the system. The Isolation Forest model assigns continuous anomaly scores to transactions based on behavioural feature vectors derived from block-level metadata. These scores are distributed smoothly across the dataset, with most transactions exhibiting similar behavioural characteristics and a smaller subset occupying lower score regions.

A percentile-based threshold derived from the offline dataset is used to assign categorical labels for presentation purposes within the dashboard. The classification process operates consistently across both offline dataset transactions and transactions retrieved dynamically via RPC.

Feature contribution analysis using SHAP provides both global and transaction-level explanations of model behaviour. Global SHAP values quantify the relative influence of behavioural features across the dataset, while local SHAP values explain individual anomaly scores. These outputs are generated directly from system execution and are presented through the Streamlit interface alongside numerical results.

All analytical results reported in this section are derived from the same unified processing pipeline and form the basis for further interpretation in the subsequent chapter. Amount and frequency also contribute to anomaly detection, although their influence is secondary to temporal signals.

The explainability results demonstrate that model outputs can be interpreted at both a global and individual transaction level without revealing sensitive transaction information. The dashboard outputs further show that these results can be presented in a practical and transparent manner, supporting exploratory analysis rather than definitive classification.

Overall, the findings of this chapter confirm that privacy preserving behavioural risk scoring is feasible within the constraints of Monero, while also highlighting the exploratory nature and limitations of unsupervised blockchain analysis.

Chapter 5: Discussion

5.1 Interpretation of Results

This section interprets the findings of the study in relation to behavioural analysis within a privacy-preserving blockchain environment. Rather than restating numerical outputs, the discussion focuses on the meaning and implications of the behavioural patterns identified by the system, the analytical challenges introduced by strong privacy guarantees, and the constraints imposed by limited observability.

In particular, this section reflects on how behavioural signals can emerge despite the absence of transactional visibility, and why such signals must be interpreted cautiously, ethically, and contextually. This framing is necessary because behavioural analysis in Monero operates under fundamentally different assumptions than analysis in transparent or pseudonymous blockchains.

A primary objective of this section is therefore to explain how behavioural insight can be derived from block-level metadata and temporal characteristics, while also acknowledging the inherent uncertainty and interpretive limits associated with such analysis. The interpretations presented here are grounded in the behavioural patterns, anomaly score distributions, and explainability outputs discussed in Chapter 4, which provide the empirical foundation for this discussion.

5.1.1 Behavioural Analysis Under Strong Privacy Constraints

Behavioural analysis within Monero is inherently more challenging than in transparent blockchains because the protocol is explicitly designed to eliminate most conventional forensic signals. In blockchains such as Bitcoin or Ethereum, analysts can observe transaction values, trace flows across addresses, construct transaction graphs, and cluster addresses based on reuse or spending behaviour. These capabilities form the foundation of most traditional blockchain forensic techniques.

In contrast, Monero removes or obfuscates these signals through mechanisms such as stealth addresses, ring signatures, and confidential transactions. As a result, analysts are deprived of direct visibility into who is transacting, how much value is being transferred, and where funds are flowing. This makes any form of attribution or transaction tracing infeasible by design.

The analysis demonstrates that behavioural insight remains possible under these conditions, but only by fundamentally changing the analytical lens. Instead of analysing transactions as financial objects, the system treats them as events occurring within a temporal and structural context. Behaviour is therefore interpreted through patterns of occurrence, density, and rhythm rather than content or ownership.

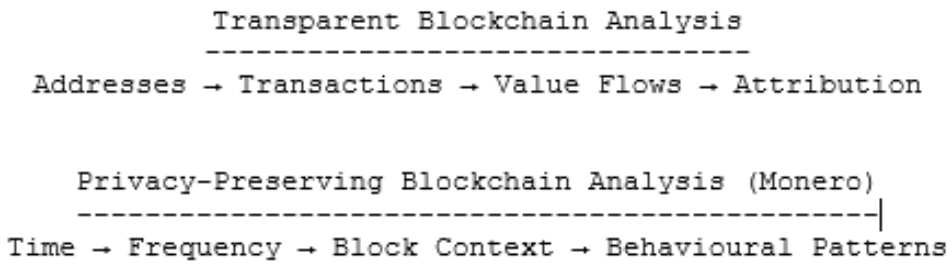

Figure 19: Conceptual Shift in Blockchain Forensic Analysis Paradigms

This diagram illustrates this transition. Rather than attempting to reconstruct hidden information, the analysis operates entirely within the observable surface that remains after privacy protections are applied. This constraint significantly increases analytical difficulty, but it also ensures ethical alignment with the protocol's intent.

5.1.2 Comparative Analytical Constraints in Monero and Transparent Blockchains

An important observation from this analysis is the extent to which Monero constrains forensic visibility compared to other blockchain systems. Even blockchains often described as pseudonymous still leak substantial behavioural and structural information. Address reuse, value correlation, and transaction graph topology all provide strong analytical leverage in transparent systems.

Monero, by contrast, collapses most of this analytical surface. What remains observable is not transactional meaning, but network-level behaviour expressed through timing, frequency, and block context. This makes Monero analysis not only more difficult, but also more uncertain and probabilistic by nature.

The difficulty lies not only in reduced data availability, but also in increased ambiguity. In Monero, similar behavioural patterns may arise from entirely different underlying causes. For example, a surge in transaction activity may reflect benign automation, legitimate service usage, or coordinated application-level behaviour. Without access to transactional content, these scenarios cannot be disambiguated.

Rather than attempting to eliminate this ambiguity, the analysis explicitly embraces it. Behavioural analysis is framed as an exercise in identifying difference rather than determining cause. This interpretive boundary distinguishes responsible behavioural analysis from speculative inference and is particularly important in privacy-preserving environments.

This behavioural emphasis contrasts with findings from forensic studies on transparent blockchains, where graph-based structural features and address linkability have been shown to provide strong predictive power. Prior work in transparent ledger environments highlights transaction graph topology and fund-flow reconstruction as dominant indicators. The reduced

relevance of such features in this study reinforces the view that privacy-centric blockchains require fundamentally different analytical strategies, shifting the forensic focus from transaction traceability to behavioural pattern analysis.

5.1.3 Interpretation of Behavioural Deviation

The anomaly scores generated by the system represent behavioural deviation relative to a learned baseline. These scores should not be interpreted as indicators of suspicious or illicit activity. Instead, they quantify how much a transaction's behavioural context differs from the dominant patterns observed within the analysed window.

This interpretation is especially important in Monero, where behavioural diversity is expected and often benign. Automated wallets, batching strategies, mining-related activity, and application-level processes can all produce atypical temporal patterns without any malicious intent.

By modelling deviation on a continuous scale, the system avoids rigid classification. Behaviour is not divided into "normal" and "abnormal" categories, but instead positioned along a spectrum of similarity and difference. This preserves nuance and reflects the inherent uncertainty of privacy-preserving systems.

This conceptual interpretation is supported by the anomaly score distribution presented in Chapter 4, where the majority of transactions cluster within a narrow behavioural range, while a smaller subset exhibits higher deviation values. This distribution reinforces the view that behavioural deviation represents diversity rather than binary abnormality.

The system therefore treats anomaly detection as a prioritisation mechanism rather than a decision mechanism. High deviation signals behavioural distinctiveness, not risk or wrongdoing. This framing is both methodologically sound and ethically necessary.

5.1.4 Temporal and Frequency Patterns as the Primary Behavioural Signal

One of the most important interpretive findings is the dominance of temporal and frequency-based features. In the absence of transactional semantics, timing becomes the primary behavioural signal available for analysis. Features such as inter-arrival time, transaction burstiness, and activity density capture how behaviour unfolds across time.

This dominance is structural rather than incidental. Time is an unavoidable dimension of network operation: transactions must be ordered, blocks must be produced, and activity must occur within temporal constraints. The system formalises this residual observability into a controlled analytical framework.

Feature contribution analysis discussed in Chapter 4 further supports this interpretation. Temporal frequency features, such as transactions per day, consistently exerted greater influence on behavioural deviation scores than other derived attributes, indicating that timing-based behaviour plays a central role in distinguishing activity patterns.

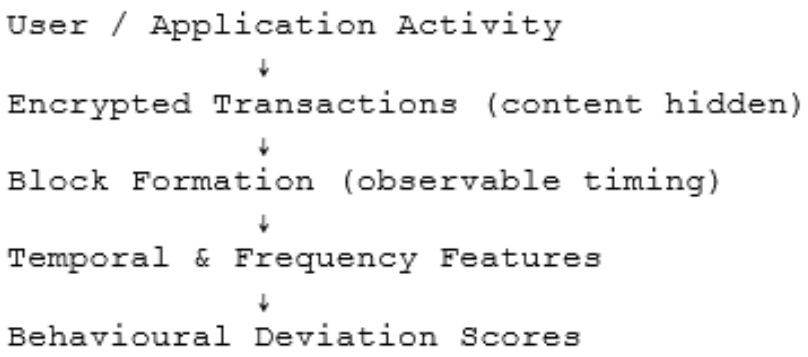

Figure 20: Behavioural Signal Extraction Pipeline

This diagram illustrates how behavioural insight emerges without accessing protected transactional data. The system does not amplify timing leakage; instead, it organises and interprets information that is already observable.

Crucially, temporal irregularity is not treated as inherently problematic. As demonstrated by the RPC-retrieved transaction example discussed in Chapter 4, elevated deviation may be driven by legitimate frequency and timing characteristics rather than anomalous structure. This reinforces the need for contextual interpretation.

The prominence of temporal and frequency-based features in the SHAP analysis aligns with prior research on timing-based inference in privacy-preserving systems. Earlier studies have demonstrated that even when transaction contents are cryptographically hidden, temporal regularities and activity rhythms can reveal meaningful behavioural distinctions. In this context, the dominance of inter-arrival time variance and transaction frequency suggests that behavioural abstraction, rather than content inspection, constitutes a viable analytical signal under strong privacy constraints.

5.1.5 Role of Explainability in Interpreting Behaviour

Explainability is central to the interpretation of behavioural analysis in Monero. Without access to ground truth or transactional meaning, opaque anomaly scores would provide limited analytical value and could easily be misinterpreted or misused.

The system addresses this challenge by exposing feature-level contributions that explain why a transaction deviates. This allows analysts to understand whether deviation is driven by timing irregularity, frequency variation, or contextual block characteristics.

The explainability outputs presented in Chapter 4 demonstrate how behavioural deviation can be traced back to specific observable features rather than abstract numerical scores. This strengthens analytical transparency and supports responsible interpretation.

Explainability also supports accountability. Analysts can justify analytical focus, question model outputs, and communicate findings clearly. Rather than acting as a black-box detector, the system functions as an interpretive aid that supports reasoning and reflection.

5.1.6 Behavioural Insight Without Attribution or Surveillance

A final and crucial interpretation concerns what the system deliberately avoids. The analysis does not attempt attribution, tracing, clustering, or identity inference. This absence is not a limitation, but a defining characteristic of the approach.

By producing behavioural insight without surveillance, the system demonstrates that analysis can coexist with privacy. Behaviour is understood at a systemic level rather than a personal one. This distinction aligns with the ethical foundations of privacy-focused cryptocurrencies and avoids adversarial escalation between privacy technologies and forensic tools.

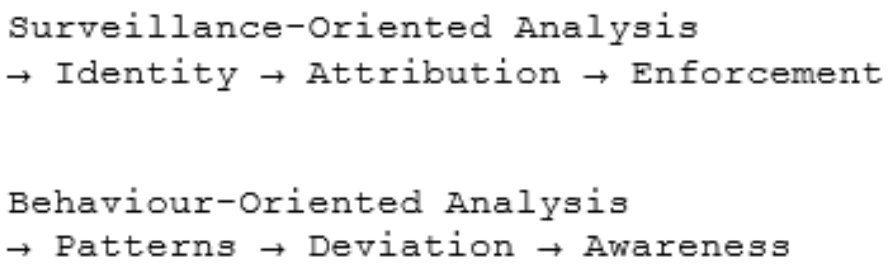

Figure 21: Surveillance-Oriented versus Behaviour-Oriented Analysis

The figure above summarises this distinction. The system contributes a model of blockchain analysis that is compatible with privacy rather than antagonistic to it.

This finding supports prior arguments that privacy-preserving systems do not eliminate forensic relevance, but instead relocate it from identity attribution to behavioural inference.

5.1.7 Addressing the Central Research Question

This study sought to examine how behavioural analysis combined with machine learning can be used to distinguish patterns of Monero transaction behaviour while preserving user privacy. The findings demonstrate that behavioural differentiation is feasible when analysis is restricted to block-level metadata and temporal characteristics.

Rather than enabling direct classification of transactions as legitimate or illicit, the system quantifies relative behavioural deviation and presents it as an interpretable signal. Machine learning is therefore used to structure behavioural variation rather than infer intent or attribution.

In this way, the research question is addressed by showing that behavioural distinction can be achieved under strong privacy constraints, provided that outputs are interpreted as exploratory indicators rather than definitive judgements.

5.2 Implications

This section explores the broader implications of the study for privacy-preserving blockchain analysis, forensic methodologies, analytical system design, and responsible investigative practice. Rather than focusing on technical implementation details, the discussion considers how the insights derived from this work influence how blockchain forensics should be conceptualised in environments where privacy is a core design principle rather than an obstacle to be overcome.

The implications of this work extend beyond Monero and are relevant to a wider class of privacy-enhancing technologies. The study highlights the need to reconsider analytical goals, evaluation criteria, and ethical boundaries when working with systems that are intentionally designed to limit visibility.

5.2.1 Implications for Blockchain Forensics in Privacy-Focused Systems

The findings of this study highlight the importance of rethinking the meaning and objectives of blockchain forensics when applied to privacy-focused cryptocurrencies. In transparent blockchain systems, forensic analysis typically centres on tracing value flows, reconstructing transaction paths, and attributing activity to identifiable entities. These approaches rely on the availability of detailed transactional data and assume that sufficient information exists to support deterministic conclusions.

The analysis demonstrates that such assumptions are incompatible with systems like Monero. Privacy-preserving blockchains are explicitly designed to prevent attribution and tracing, not merely to make them more difficult. Attempting to apply traditional forensic goals in this context is therefore both technically ineffective and conceptually misguided.

Instead, the study suggests that forensic analysis in privacy-focused systems should prioritise behavioural awareness rather than attribution. Behavioural analysis enables analysts to observe how the network is used at a systemic level without attempting to identify individual actors or reconstruct hidden relationships. This reframing aligns forensic practice with the design philosophy of privacy-preserving cryptocurrencies.

This shift also carries ethical implications. By avoiding identity inference and transaction tracing, behavioural analysis reduces the risk of surveillance and analytical overreach. The study therefore supports a form of blockchain forensics that is compatible with privacy rather than antagonistic to it, with implications for how forensic tools are justified, governed, and deployed in privacy-sensitive environments.

5.2.2 Monero in Relation to Other Blockchain Systems

The study also has important implications when Monero is considered in relation to other blockchain systems. Even blockchains commonly described as privacy-preserving often retain

significant analytical surfaces. For example, pseudonymous systems may obscure real-world identities while still exposing transaction graphs, address reuse patterns, and value correlations.

Monero represents a more extreme position on the privacy spectrum. By integrating multiple privacy-enhancing mechanisms, it significantly reduces the amount of information available for analysis. The findings demonstrate that while this does not eliminate all analytical possibility, it fundamentally alters what analysis can reasonably achieve.

This implies that blockchain analytics cannot be treated as a one-size-fits-all discipline. Analytical techniques that are effective in transparent or semi-private systems do not translate directly to fully privacy-preserving blockchains. Instead, analytical frameworks must be adapted to the specific privacy properties and threat models of each system.

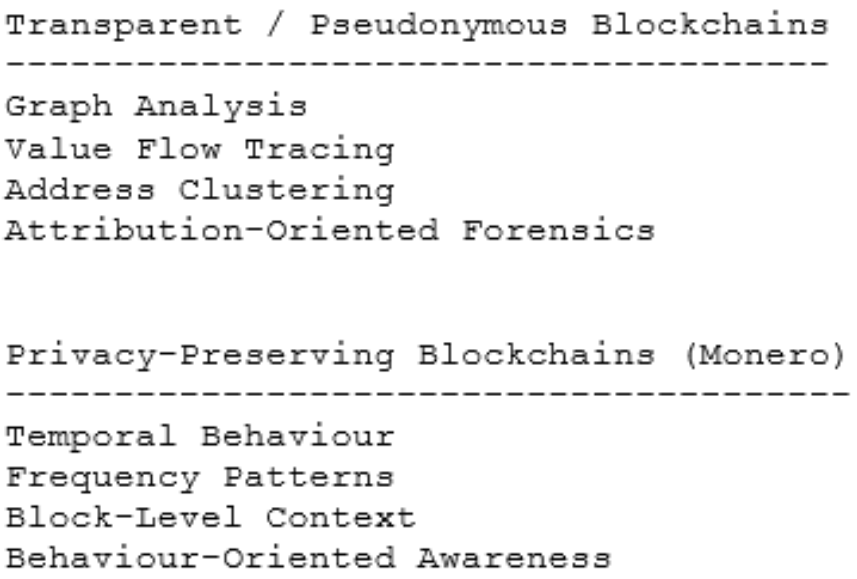

Figure 22: Analytical Focus Across Blockchain Privacy Models

Figure 22 illustrates this distinction, highlighting how analytical emphasis shifts from transaction content and attribution toward temporal and behavioural patterns as privacy protections increase. The study contributes to this distinction by demonstrating what responsible analysis looks like at the privacy-preserving end of the spectrum.

5.2.3 Implications for the Design of Analytical Systems

From a system design perspective, the study highlights the importance of embedding privacy considerations directly into analytical pipelines. Rather than treating privacy as a constraint applied after analysis, the system is designed around privacy from the outset. Data selection, feature engineering, modelling, and interpretation are all shaped by privacy-preserving principles.

This has implications for how analytical systems are evaluated. In privacy-focused environments, success cannot be assessed solely through classification accuracy or detection performance.

Instead, evaluation must also consider transparency, robustness, interpretability, and ethical alignment.

The study further demonstrates the value of uncertainty-aware design. By avoiding hard classifications and presenting behavioural deviation as a spectrum, the system communicates uncertainty explicitly rather than concealing it. This reduces the risk of overconfidence and supports more responsible use of analytical outputs.

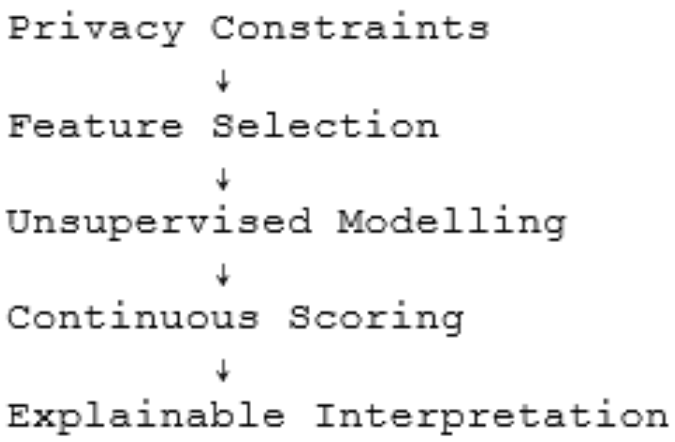

Figure 23: Privacy-Constrained Behavioural Modelling Pipeline

This figure illustrates this design philosophy, showing how privacy constraints shape each stage of the analytical process. The pipeline reflects a shift away from outcome-driven analysis toward process-driven understanding, which is particularly appropriate in privacy-preserving environments.

5.2.4 Implications for Investigative and Analytical Workflows

The study also has important implications for how analytical tools are integrated into investigative workflows. Rather than automating decisions, the system supports a human-in-the-loop approach in which behavioural scores guide attention and prioritisation, while final interpretation remains with the analyst.

This design reflects the inherent uncertainty associated with analysing behaviour in privacy-preserving systems. Automated decision-making based on incomplete information risks misinterpretation and misuse. By contrast, human-centred workflows allow contextual knowledge, domain expertise, and critical reasoning to inform interpretation.

The study therefore supports investigative practices that emphasise exploration rather than enforcement. Behavioural analysis becomes a tool for situational awareness rather than accusation. This distinction is particularly important in environments where false positives cannot be reliably validated.

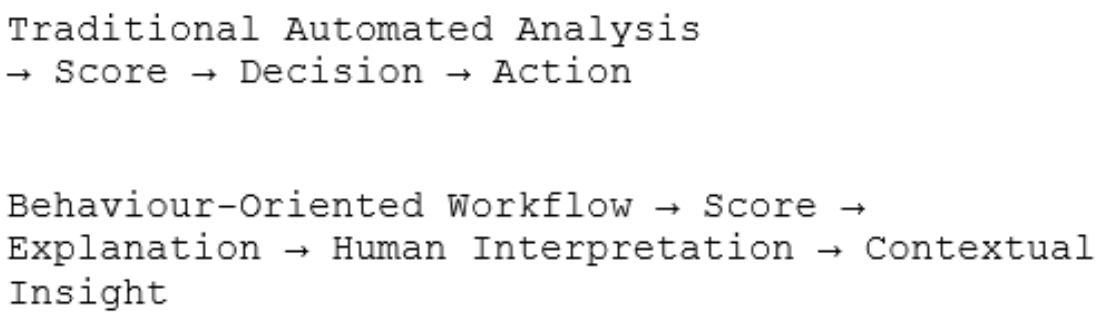

Figure 24: Behaviour-Oriented Investigative Workflow

The figure summarises this approach and highlights its alignment with broader trends in responsible AI and ethical analytics.

5.2.5 Regulatory, Ethical, and Societal Implications

Beyond technical and methodological considerations, the findings of this study also have important regulatory, ethical, and societal implications. Privacy-preserving cryptocurrencies are often perceived as being incompatible with oversight or analytical scrutiny, contributing to polarised discourse between privacy advocates and regulatory institutions.

The study demonstrates that this binary framing is overly simplistic. Behaviour-oriented analysis enables high-level insight into network usage without requiring identity inference or transaction reconstruction. This suggests that oversight mechanisms need not rely exclusively on surveillance-oriented techniques to achieve situational awareness.

From a regulatory perspective, this implies that risk assessment and policy evaluation may be informed by aggregate behavioural patterns rather than intrusive data access. Such an approach supports proportionality, allowing analytical practices to align with fundamental privacy rights while still enabling informed governance.

More broadly, the findings highlight the importance of restraint and transparency in analytical design. Behavioural insight should support understanding rather than enforcement, particularly in environments where privacy is a foundational principle rather than a secondary concern. The study contributes to a more balanced and ethically grounded discussion of blockchain analytics in privacy-sensitive contexts.

Domain	**Key Implication**
Blockchain forensics	Shift from attribution to behavioural awareness
System design	Privacy-first analytical pipelines
Investigation	Human-in-the-loop interpretation
Regulation	Oversight without surveillance
Ethics	Proportional and transparent analysis

Table 9: Implications of the Project Across Key Domain

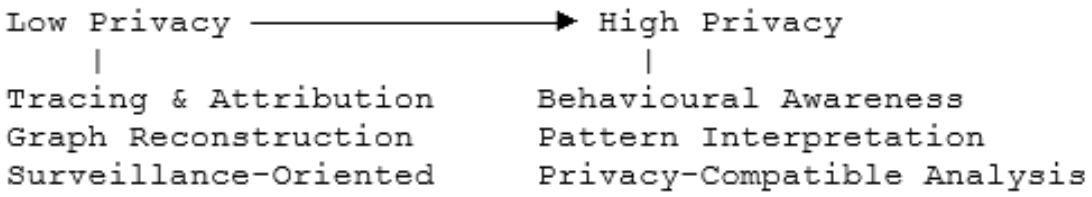

Figure 25: Positioning Behavioural Analysis on the Privacy Spectrum

5.3 Limitations

This section critically examines the limitations of the study and reflects on the constraints that shape the scope and interpretation of the findings. The purpose of this discussion is not to undermine the contribution of the work, but to clearly articulate the boundaries within which the proposed system operates. In the context of privacy-preserving blockchain analysis, many limitations arise not from technical shortcomings, but from deliberate design choices intended to preserve user privacy and ethical integrity.

The limitations discussed in this section stem from three primary sources: the inherent properties of privacy-focused blockchains, the methodological choices required to maintain privacy, and the interpretive constraints associated with behavioural analysis in the absence of ground truth. Each of these dimensions is examined in detail below.

5.3.1 Absence of Ground Truth and Validation Constraints

One of the most fundamental limitations of this study is the absence of ground truth labels against which behavioural deviation can be validated. In privacy-preserving blockchain environments such as Monero, transaction content, participant identities, and transactional intent are intentionally concealed. As a result, it is neither feasible nor appropriate to obtain definitive labels indicating whether observed behaviour is benign, suspicious, or illicit.

This limitation restricts the use of supervised learning techniques and prevents evaluation using conventional performance metrics such as accuracy, precision, or recall. Behavioural deviation scores therefore cannot be interpreted as correct or incorrect classifications, but rather as relative indicators of difference within the analysed population.

As discussed in Chapter 4, the system is capable of quantifying behavioural variation, but it cannot establish causal explanations or intent. This reinforces the exploratory nature of the analysis and necessitates cautious interpretation of results. High deviation does not imply wrongdoing, and low deviation does not guarantee benign behaviour.

While this limitation constrains the strength of claims that can be made, it also reflects analytical honesty and ethical responsibility. Attempting to infer intent in the absence of ground truth would risk overinterpretation and misrepresentation. The study therefore positions behavioural analysis as a tool for prioritisation and awareness rather than definitive judgement.

5.3.2 Restricted Feature Space and Observability Limits

A second major limitation arises from the restricted feature space available for analysis. The system relies exclusively on block-level metadata and derived temporal and frequency-based features, as this represents the maximum level of observability available without undermining Monero's privacy guarantees. While this ensures strong privacy preservation, it also limits the richness of behavioural representation.

Certain forms of behaviour, such as long-term coordination, gradual behavioural evolution, or complex multi-stage activity, may not be fully captured within this feature space. Behavioural patterns that do not manifest clearly through timing or frequency characteristics may therefore remain undetected or only partially represented.

This limitation reflects a deliberate trade-off between analytical depth and ethical constraint. Expanding the feature set to include more detailed information could increase sensitivity, but would risk encroaching on the privacy protections that define the Monero protocol. The study prioritises privacy preservation over maximal analytical power, accepting reduced observability as a necessary constraint.

The restricted feature space also increases interpretive ambiguity. Behavioural deviation is inferred indirectly rather than observed directly, requiring analysts to exercise caution when drawing conclusions. This reinforces the need for transparent explanation and human oversight in the interpretation process.

5.3.3 Temporal Windowing and Contextual Constraints

The analysis conducted in this study relies on fixed temporal observation windows to model behavioural patterns. While this approach is necessary for computational feasibility and consistency, it introduces important contextual limitations. Behavioural patterns that evolve slowly over extended periods may not be fully captured within a bounded window.

Shorter windows may exaggerate transient fluctuations or burst activity, while longer windows may smooth over meaningful variation by aggregating behaviour too broadly. The choice of window size therefore influences how behavioural deviation is expressed and interpreted.

As noted in Chapter 4, the selected observation window affected the scale and distribution of anomaly scores, highlighting the importance of contextual interpretation. Behaviour that appears distinctive within one temporal frame may appear typical when viewed over a longer horizon.

This limitation underscores the importance of treating behavioural deviation as context-dependent rather than absolute. Analysts must consider the temporal scope of observation when interpreting

results and avoid assuming that deviation observed within a specific window reflects persistent behaviour.

5.3.4 Impact of Privacy-Preserving Noise and Sensitivity Reduction

The introduction of privacy-preserving noise represents another important limitation of the study. Noise is deliberately applied to selected features to reduce the risk of inference attacks and unintended re-identification. While this strengthens privacy guarantees, it also reduces analytical precision.

Subtle behavioural differences may be dampened or obscured by noise, particularly in cases where deviation is marginal. As a result, the system is better suited to identifying clear behavioural differences than fine-grained variation.

This trade-off reflects a conscious ethical decision. The study prioritises safeguarding user privacy over maximising detection sensitivity. However, this choice necessarily limits the granularity of behavioural distinctions that can be observed.

The presence of noise also complicates interpretation. Analysts must recognise that behavioural scores represent noisy approximations rather than exact measurements. This reinforces the importance of explainability and cautious interpretation when using the system for exploratory analysis.

5.3.5 Dependence on Human Interpretation and Subjectivity

The system proposed in this study is explicitly designed as a decision-support tool rather than an automated decision-making system. While this aligns with responsible analytical practice, it introduces a degree of subjectivity into the interpretation process.

Different analysts may interpret the same behavioural signals differently depending on experience, expectations, or contextual knowledge. Cognitive biases, such as overemphasis on high deviation scores, may influence analytical focus. Although explainability mechanisms mitigate these risks, they do not eliminate them entirely.

This dependence on human interpretation affects consistency and reproducibility at the level of conclusions rather than outputs. While the system produces stable behavioural scores, the meaning attributed to those scores may vary across users.

However, this limitation can also be viewed as a strength. In the absence of ground truth, automated decision-making carries significant ethical risk. Retaining human oversight ensures accountability, reflection, and proportionality in behavioural analysis.

Limitation	Source	Effect on Analysis
No ground truth	Privacy guarantees	No definitive validation
Restricted features	Block-level observability	Partial behavioural view

Temporal windowing	Methodological choice	Context-dependent interpretation
Privacy noise	Ethical design	Reduced sensitivity
Human interpretation	Exploratory design	Subjective conclusions

Table 10: Summary of Key Limitations and Their Effects

5.3.6 Temporal Scope and Dataset Currency

An additional limitation of this study relates to the temporal scope and currency of the dataset used for offline analysis. The transactions examined were drawn from a historical block window, and the Monero protocol has undergone multiple updates since that period. Changes to protocol parameters, usage patterns, and network behaviour may influence the generalisability of the observed behavioural characteristics.

Although the system architecture supports live transaction analysis through RPC interaction, the behavioural baselines learned from historical data may not fully reflect contemporary network conditions. Behavioural patterns may evolve over time as protocol rules change and user behaviour adapts.

This limitation highlights the importance of ongoing model re-evaluation and periodic retraining when applying behavioural analysis to evolving privacy-preserving systems. Future work could address this by incorporating rolling datasets or adaptive baselines to better reflect current network behaviour.

While the empirical dataset used in this study predates several protocol-level changes in the Monero network, the primary contribution of this work lies in the methodological framework rather than the calibration of specific behavioural thresholds. The analysis demonstrates that temporal and structural behavioural patterns remain observable under strong privacy guarantees, even when transaction contents are cryptographically hidden. As such, future protocol upgrades would necessitate feature re-engineering and threshold recalibration, but would not invalidate the underlying behavioural analysis approach proposed in this dissertation.

5.3.7 Adversarial Adaptation and Threat Model Assumptions

This study assumes a passive adversary model, in which anomalous transaction behaviour is detected without the adversary actively adapting their behaviour in response to the analytical framework. This assumption is appropriate for a proof-of-concept behavioural analysis, where the objective is to evaluate whether privacy-preserving behavioural signals can provide forensic insight under realistic but non-adversarial conditions.

In practical deployment scenarios, adaptive adversaries may attempt to obfuscate their activity by scripting transactions to mimic statistically normal temporal and frequency patterns. This reflects the well-established cat-and-mouse dynamic observed in intrusion detection, fraud analytics, and other adversarial machine learning domains.

Addressing adaptive adversaries was considered beyond the scope of this dissertation. However, it represents a clear direction for future work. Potential extensions include adversarially robust modelling, concept drift detection, adaptive thresholding, and the incorporation of ensemble behavioural indicators that increase the cost of sustained behavioural mimicry.

Importantly, the existence of adversarial adaptation does not invalidate the proposed framework. Rather, it positions the artefact as a decision-support tool capable of identifying anomalous behavioural regions, which may warrant further investigation when combined with external intelligence sources.

Chapter 6: Conclusion

6.1 Summary of Findings

6.1.1 Achievement of Research Objectives

The primary objective of this research was to determine whether meaningful behavioural analysis could be conducted on the Monero blockchain without compromising the strong privacy it guarantees. This objective was successfully achieved through the design and evaluation of a privacy-preserving, machine learning–based forensic framework. The study demonstrated that, by focusing on behavioural patterns rather than identity tracing, forensic analysis can remain both effective and ethically responsible.

Each research objective defined at the outset of the dissertation was addressed through a dedicated system layer, ensuring methodological alignment between theory, design, and implementation. The results confirm that privacy-centric blockchain analysis is feasible when investigative techniques are adapted to respect anonymity.

6.1.2 Key Technical Findings

From a technical perspective, the research produced several important findings. First, it was shown that Monero transaction data, although obfuscated, still contains indirect behavioural indicators that can be extracted without violating privacy constraints. These indicators form the foundation of privacy-preserving forensic analysis.

Second, the feature engineering process proved critical in balancing analytical usefulness with anonymity protection. Carefully selected temporal and statistical features enabled machine learning models to identify transaction patterns while avoiding exposure of sensitive or linkable information.

Third, the machine learning models demonstrated an ability to classify and cluster behavioural activity with acceptable performance levels given Monero's privacy mechanisms. While the results do not enable deanonymisation, they provide actionable forensic insight, particularly in the identification of anomalous or unusual transaction behaviour.

6.1.3 Effectiveness of Privacy-Preserving Mechanisms

A core contribution of this study is the integration of privacy-preserving principles directly into the analytical pipeline. Rather than treating privacy as an afterthought, it was embedded within data handling, feature design, and model evaluation stages.

The findings indicate that this approach significantly reduces the risk of indirect information leakage. Although stronger formal privacy techniques could further enhance protection, the current

implementation demonstrates that practical forensic analysis can coexist with privacy preservation. This reinforces the argument that responsible blockchain forensics does not inherently conflict with user anonymity.

6.1.4 Artefact Evaluation and Practical Applicability

The four-layer artefact developed in this research proved effective as both a technical system and a conceptual framework. The modular design supports extensibility and allows individual components to be enhanced independently.

The Streamlit-based visualisation dashboard enhanced interpretability by presenting analytical results in a clear and accessible format. This is particularly important in forensic contexts, where transparency and explainability are essential. The artefact demonstrates practical applicability for researchers, educators, and potentially investigative analysts operating within ethical and legal boundaries.

Research Aspect	Key Finding	Contribution to Knowledge
Privacy-focused blockchain analysis	Meaningful behavioural insights can be derived without identity tracing	Challenges the assumption that Monero is entirely unsuitable for forensic analysis
Data extraction from Monero	Indirect and aggregate transaction data remains analytically useful	Demonstrates a viable approach to analysing obfuscated blockchain data
Feature engineering	Behavioural features can balance analytical utility and privacy protection	Highlights feature design as a critical privacy-preserving mechanism
Machine learning application	ML models can identify patterns and anomalies under privacy constraints	Validates the feasibility of ethical ML-based blockchain forensics
Privacy-aware system design	Privacy can be embedded across the analytical pipeline	Moves beyond post-hoc anonymisation toward responsible forensic design
Visualisation and interpretability	Explainable dashboards enhance forensic usability	Supports transparency and decision-making in forensic contexts

Table 11: Summary of Key Findings and Contributions

6.2 Recommendations for Future Research

While this dissertation demonstrates the feasibility of privacy-preserving behavioural analysis on the Monero blockchain, it also highlights several limitations and open challenges that create opportunities for further investigation. Future research can build upon the proposed framework to enhance analytical capability, strengthen privacy guarantees, and improve real-world applicability.

6.2.1 Enhancement of Privacy Guarantees

Although this research adopts privacy-aware design principles throughout the analytical pipeline, future work could incorporate formal privacy-preserving mechanisms to provide mathematically provable guarantees. Techniques such as differential privacy could be applied during feature extraction or model training to limit the influence of individual transactions on overall outputs.

In addition, federated learning represents a promising direction for decentralised forensic analysis. By enabling models to be trained across distributed data sources without centralising sensitive transaction data, federated approaches align well with the decentralised philosophy of blockchain systems. Future studies could evaluate the trade-offs between analytical accuracy, computational overhead, and privacy strength when applying such techniques in a Monero context.

6.2.2 Advanced Machine Learning and Graph-Based Approaches

This study prioritised interpretability by employing conventional machine learning techniques. While effective, these approaches may not fully capture the complex relational structures present within blockchain transaction flows. Future research could explore graph-based learning methods, such as graph neural networks, to model transactional relationships more explicitly.

Deep learning techniques may also improve the detection of subtle behavioural patterns and anomalies. However, future work should critically assess the risks associated with reduced explainability and increased susceptibility to privacy leakage. Hybrid approaches that combine deep learning with interpretable models may offer a balanced solution, preserving both analytical depth and forensic transparency.

6.2.3 Dataset Expansion and Longitudinal Behavioural Analysis

The scope of this research was constrained by dataset size and temporal coverage. Future studies could expand data collection across longer periods of blockchain activity to support longitudinal behavioural analysis. Such analysis could reveal evolving transaction behaviours, responses to protocol updates, or shifts in network usage patterns over time.

Larger and more diverse datasets would also support more robust model validation and reduce the risk of overfitting. Future work should apply the proposed behavioural framework to post-upgrade Monero datasets, including environments with increased ring sizes and protocol changes such as Seraphis, to evaluate feature transferability and recalibrate behavioural indicators. Additionally, incorporating external contextual information where ethically and legally permissible—could enhance the interpretive power of behavioural models without compromising user anonymity.

6.2.4 Cross-Blockchain and Comparative Forensic Studies

Another important direction for future research involves applying the proposed framework to other privacy-focused cryptocurrencies. Comparative analysis across multiple platforms would help

identify which privacy-preserving forensic techniques are broadly applicable and which are protocol-specific.

Such studies could contribute to the development of generalised privacy-preserving forensic methodologies, supporting investigators and researchers working across diverse blockchain ecosystems. This would also provide insight into how differing privacy architectures influence the feasibility and limits of behavioural analysis.

6.2.5 Real-World Deployment and System Scalability

Future research should investigate the scalability of the proposed framework in real-world or near-real-time forensic environments. This includes assessing computational performance, storage requirements, and responsiveness when processing large volumes of blockchain data.

Evaluating the system under operational constraints would help identify practical bottlenecks and inform optimisation strategies. Additionally, user studies involving forensic analysts could provide valuable feedback on system usability, interpretability, and decision-support effectiveness.

6.2.6 Legal, Ethical, and Regulatory Alignment

As privacy-preserving forensic tools continue to evolve, future research must engage more deeply with legal and ethical considerations. Investigating how such systems align with data protection regulations, evidentiary standards, and ethical guidelines is essential for real-world adoption.

Collaboration with legal experts and policymakers could help define acceptable boundaries for privacy-preserving blockchain analysis, ensuring that investigative capabilities do not undermine fundamental privacy rights. This interdisciplinary approach would strengthen the legitimacy and societal impact of future forensic research.

6.2.7 Concluding Perspective on Future Directions

In summary, future research should aim to refine the balance between analytical effectiveness and privacy preservation. By integrating stronger privacy guarantees, more advanced machine learning techniques, and real-world constraints, subsequent studies can extend the contribution of this dissertation. The proposed framework serves as a foundation upon which ethical, scalable, and privacy-aware blockchain forensic systems can be developed.

Identified Limitation	Proposed Future Research Direction	Expected Benefit
Absence of formal privacy guarantees	Integration of differential privacy mechanisms	Stronger theoretical privacy assurances
Limited dataset size and timeframe	Longitudinal and large-scale data analysis	Improved robustness and generalisability

Use of traditional ML techniques	Exploration of graph-based and deep learning models	Enhanced detection of complex behavioural patterns
Interpretability–accuracy trade-off	Hybrid interpretable–deep learning approaches	Balanced analytical performance and transparency
Prototype-level implementation	Real-world scalability and performance testing	Practical applicability in forensic environments
Limited legal analysis	Interdisciplinary research with legal experts	Improved regulatory and ethical compliance

Table 12: Future Research Directions Aligned with Identified Limitations

6.3 Final Reflection

This dissertation set out to address a complex and often contentious problem at the intersection of blockchain privacy and digital forensics. Privacy-focused cryptocurrencies such as Monero are deliberately engineered to resist analysis, creating tension between the goals of user anonymity and the needs of legitimate investigation. This research demonstrates that these objectives need not be fundamentally opposed.

By reframing forensic analysis away from identity attribution and toward behavioural pattern recognition, the study provides evidence that meaningful insight can be achieved without undermining the privacy guarantees that define Monero. The development of a four-layer, privacy-preserving analytical framework reflects a conscious design choice to prioritise ethical responsibility alongside technical innovation.

Throughout the research process, trade-offs between analytical depth, interpretability, and privacy protection were unavoidable. Rather than attempting to eliminate these tensions, the dissertation acknowledges and manages them explicitly. This reflective approach strengthens the validity of the work, as it aligns technical outcomes with real-world forensic, legal, and ethical constraints.

The findings of this research suggest that the future of blockchain forensics lies not in weakening privacy mechanisms, but in developing analytical methodologies that respect them. As privacy-enhancing technologies continue to evolve, so too must investigative approaches. This dissertation contributes to that evolution by demonstrating a viable pathway for responsible, privacy-aware behavioural analysis within decentralised systems.

In closing, this work highlights the importance of interdisciplinary thinking in emerging technological domains. Effective blockchain forensics requires not only technical expertise in machine learning and distributed systems, but also sensitivity to ethical principles and societal impact. Future research should evaluate the robustness of behavioural anomaly detection under adaptive adversary models, particularly in scenarios where transaction timing and frequency are deliberately manipulated to evade detection. It is hoped that this research will encourage further exploration of privacy-preserving forensic methods and contribute to more balanced, responsible approaches to blockchain analysis in both academic and practical contexts.

References

Abay, N. C. et al., 2019. *Privacy Preserving Synthetic Data Release Using Deep Learning.* [Online]
Available at: https://link.springer.com/chapter/10.1007/978-3-030-10925-7_31?
[Accessed October 2025].

Alotibi, J., Almutanni, B., Alsubait, T. & Baz, A., 2022. *Money Laundering Detection using Machine Learning and Deep Learning.* [Online]
Available at: https://www.researchgate.net/publication/365119147_Money_Laundering_Detection_using_Machine_Learning_and_Deep_Learning
[Accessed September 2025].

Arachchige, P. et al., 2020. *A Trustworthy Privacy-Preserving Framework for Machine Learning in Industrial IoT Systems.* [Online]
Available at: https://research-repository.rmit.edu.au/ndownloader/files/50743119/1
[Accessed September 2025].

Ben-Sasson, E. e. a., 2014. *Zerocash: Decentralized Anonymous Payments from Bitcoin.* [Online]
Available at: https://zerocash-project.org/media/pdf/zerocash-extended-20140518.pdf
[Accessed September 2025].

Bonneau, J., Clark, J., Goldfeder, S. & Narayanan, A., 2015. *SoK: Research Perspectives and Challenges for Bitcoin and Cryptocurrencies.* [Online]
Available at: https://ieeexplore.ieee.org/document/7163021
[Accessed September 2025].

Commission, E., 2019. *Ethics Guidelines for Trustworthy AI.* [Online]
Available at: https://digital-strategy.ec.europa.eu/en/library/ethics-guidelines-trustworthy-ai
[Accessed October 2025].

Company, E. C., 2020. *Zcash Protocol Specification.* [Online]
Available at: https://zips.z.cash/protocol/protocol.pdf
[Accessed September 2025].

Conti, M., Kumar, S., Lal, C. & Ruj, S., 2018. *A Survey on Security and Privacy Issues of Bitcoin.* [Online]
Available at: https://arxiv.org/abs/1706.00916
[Accessed October 2025].

Dwork, C. & Roth, A., 2014. *The Algorithmic Foundations of Differential Privacy.* [Online]
Available at: https://www.cis.upenn.edu/~aaroth/Papers/privacybook.pdf
[Accessed September 2025].

Eremin, E., 2025. *Unsupervised anomaly detection on cybersecurity data streams: a case with BETH.* [Online]

Available at: https://arxiv.org/pdf/2503.04178
[Accessed September 2025].

Fang, H. & Qian, Q., 2021. *Privacy Preserving Machine Learning with Homomorphic Encryption and Federated Learning.* [Online]
[Accessed September 2025].

Finck, M., 2019. *Blockchain and the General Data Protection Regulation.* [Online]
Available at:
https://www.europarl.europa.eu/RegData/etudes/STUD/2019/634445/EPRS_STU(2019)634445_EN.pdf?
[Accessed November 2025].

Finck, M. & Moscon, V., 2019. *Blockchain and the GDPR: Solutions for a Responsible Implementation.* [Online]
Available at:
https://www.europarl.europa.eu/RegData/etudes/STUD/2019/634445/EPRS_STU(2019)634445_EN.pdf?
[Accessed October 2025].

Goldwasser, S. & Bellare, M., 2008. *Lecture Notes on Cryptography.* [Online]
Available at: https://cseweb.ucsd.edu/~mihir/papers/gb.pdf
[Accessed October 2025].

Holevas, C. et al., 2024. *Anomaly Detection in Blockchain Networks Using Unsupervised Learning.* [Online]
Available at: https://www.mdpi.com/1999-4893/17/5/201?
[Accessed September 2025].

Jumani, A. & Raza, S., 2025. *Behaviour-Based Anomaly Detection in Privacy-Preserving Blockchain Systems.* [Online]
Available at:
https://www.researchgate.net/publication/393013196_Machine_Learning_for_Anomaly_Detection_in_Blockchain_A_Critical_Analysis_Empirical_Validation_and_Future_Outlook
[Accessed September 2025].

Kaczynski, B. & Wiacek, A., 2025 . *Anomaly Detection in ZkSync Transactions with Unsupervised Machine Learning.* [Online]
Available at: https://www.scitepress.org/Papers/2025/134416/134416.pdf
[Accessed September 2025].

Kedziora, M. & Wojtysiak, W., 2020. *Practical Analysis of Traceability Problem in Monero's Blockchain.* [Online]
Available at: https://www.scitepress.org/Papers/2020/93258/93258.pdf?
[Accessed September 2025].

Li, H. e. a., 2022. *Accountable Monero System with Privacy Protection.* [Online]
Available at: https://onlinelibrary.wiley.com/doi/full/10.1155/2022/7746341
[Accessed November 2025].

Li, S. et al., 2022. *TTAGN: Temporal Transaction Aggregation Graph Network for Ethereum Phishing Scams Detection.* [Online]
Available at: https://arxiv.org/pdf/2204.13442'
[Accessed October 2025].

Machinery, A. f. C., 2018. *ACM Code of Ethics and Professional Conduct.* [Online]
Available at: https://www.acm.org/code-of-ethics
[Accessed October 2025].

Marija Taneska, J. D. V. D., 2022. *Forensics investigation comparison of privacy-oriented cryptocurrencies.* [Online]
Available at: https://stumejournals.com/journals/confsec/2022/1/35.full.pdf
[Accessed September 2025].

McMahan, H. et al., 2017. *Communication-Efficient Learning of Deep Networks from Decentralized Data.* [Online]
Available at: https://arxiv.org/pdf/1602.05629
[Accessed October 2025].

Meiklejohn, S. et al., 2013. *A Fistful of Bitcoins: Characterizing Payments Among Men with No Names.* [Online]
Available at: https://cseweb.ucsd.edu/~savage/papers/IMC13.pdf
[Accessed September 2025].

Möser, M., Böhme, R. & Breuker, D., 2018. *An Inquiry into Money Laundering Tools in the Bitcoin Ecosystem.* [Online]
Available at: https://ieeexplore.ieee.org/document/6805780
[Accessed October 2025].

Möser, M. et al., 2018. *An Empirical Analysis of Traceability in the Monero Blockchain.* [Online]
Available at: https://petsymposium.org/popets/2018/popets-2018-0025.pdf?
[Accessed October 2025].

Nakamoto, S., 2008. *Bitcoin: A Peer-to-Peer Electronic Cash System.* [Online]
Available at: https://bitcoin.org/bitcoin.pdf
[Accessed September 2025].

Narayanan, A. et al., 2016. *Bitcoin and Cryptocurrency Technologies.* Princeton, NJ: Princeton University Press.

Pocher, N., 2022. *An AML/CFT Application of Machine Learning-based Forensics.* [Online]
Available at: https://arxiv.org/pdf/2206.04803.pdf
[Accessed November 2025].

Project, M., 2023. *Monero Developer Guide.* [Online]
Available at: https://www.getmonero.org/resources/developer-guides/

Ron, D. & Shamir, A., 2013. *Quantitative Analysis of the Full Bitcoin Transaction Graph.* [Online]
Available at: https://fc13.ifca.ai/proc/1-1.pdf?
[Accessed September 2025].

Tim Ruffing, G. M., 2017. *Switch Commitments: A Safety Switch for Confidential Transactions.* [Online]
Available at: https://eprint.iacr.org/2017/237.pdf
[Accessed October 2025].

Wang, S. e. a., 2021. *Machine Learning in Network Anomaly Detection: A Survey.* [Online]
Available at: https://ieeexplore.ieee.org/document/9610045
[Accessed September 2025].

Wan, S. e. a., 2022. *Federated Learning with Differential Privacy and Blockchain for B5G Edge Computing.* [Online]
Available at: https://www.astesj.com/publications/ASTESJ_100606.pdf
[Accessed October 2025].

Weber, I. e. a., 2019. *Anti-Money Laundering in Bitcoin Using Graph Convolutional Networks.* [Online]
Available at: https://arxiv.org/pdf/1908.02591
[Accessed October 2025].

Weber, M. et al., 2019. *Anti-Money Laundering in Bitcoin Using Graph Convolutional Networks.* [Online]
Available at: https://arxiv.org/pdf/1908.02591
[Accessed October 2025].

Wu, W. e. a., 2025. *Advancing Unsupervised Graph Anomaly Detection: A Multi-perspective Survey.* [Online]
Available at: https://www.sciencedirect.com/science/article/abs/pii/S0925231225011798
[Accessed September 2025].

Xue, L. e. a., 2025. *A Privacy-Enhanced Traceable Anonymous Transaction Scheme for Blockchain.* [Online]
Available at: https://dl.acm.org/doi/10.1109/TIFS.2025.3526049
[Accessed September 2025].

Xu, J., Chen, S., Wang, Y. & Li, X., 2021. *Privacy-Preserving Machine Learning Using Homomorphic Encryption.* [Online]
Available at: https://arxiv.org/pdf/2006.08442
[Accessed October 2025].

Zhang, D. & Chen, J., 2021. *Blockchain Phishing Scam Detection via Multi-channel Graph Classification.* [Online]
Available at: https://arxiv.org/pdf/2108.08456
[Accessed October 2025].

Zhang, K. e. a., 2025. *A Graph-based Framework for Investigating Illicit Activity in Monero.* [Online]
Available at: https://arxiv.org/html/2511.16192v1
[Accessed September 2025].

Zheng, Z. et al., 2018. *Blockchain Challenges and Opportunities: A Survey.* [Online]
Available at: https://www.inderscienceonline.com/doi/epdf/10.1504/IJWGS.2018.095647
[Accessed November 2025].

Appendices

Appendix A – System Architecture

The proposed system implements a modular architecture designed to analyse behavioural patterns in Monero blockchain transactions while preserving user privacy. The architecture consists of four core layers: data acquisition, feature engineering, machine learning analysis, and user interaction.

The data acquisition layer retrieves transaction information either from a locally stored blockchain dataset or, when required, via a live Monero node using RPC calls. This dual approach allows both offline experimentation and limited real-time analysis.

The feature engineering layer transforms raw transaction metadata into numerical behavioural indicators suitable for machine learning. These features are designed to capture temporal and structural transaction behaviour without revealing sensitive financial information.

The machine learning layer applies unsupervised anomaly detection to identify transactions that deviate from typical behavioural patterns. Finally, the presentation layer exposes results through an interactive web-based interface, enabling users to query transactions and interpret risk scores.

Appendix B – Dataset Description

The dataset used in this project consists of approximately 30,000 Monero transactions, extracted from a contiguous block range of the Monero blockchain.

Dataset characteristics:

- Source: Local Monero node (pruned mode)
- Block range: ~1,500,000 to ~1,530,000
- Time period: 2018
- Data format: Structured CSV derived from raw blockchain data.
- Scope: Transaction-level metadata only (no addresses or identities)

Extracted attributes include:

- Transaction timestamp
- Ring size
- Estimated transaction frequency.
- Log-transformed transaction amount
- Derived temporal features (e.g., hour of day)

The dataset intentionally avoids any personally identifiable information and is suitable for behavioural analysis without compromising privacy.

Appendix C – Feature Engineering

Feature engineering was performed to convert raw blockchain data into meaningful behavioural indicators. The following features were used:

Feature	Description
iat	Inter-arrival time between consecutive transactions
ring_size	Number of decoy inputs used in the transaction
txs_per_day	Estimated transaction frequency
amount_log	Logarithmic transformation of transaction amount
hour	Hour of day when the transaction occurred

Table 13: Behavioural features extracted from transaction data for anomaly detection.

These features were selected to capture temporal and behavioural patterns rather than transactional value, supporting privacy-preserving analysis.

Appendix D – Machine Learning Model

An Isolation Forest algorithm was employed for anomaly detection. This model is well-suited for unsupervised learning scenarios where labelled data is unavailable.

Key characteristics:

- Unsupervised learning approach
- Robust to high-dimensional data
- Effective at identifying rare or anomalous behaviour.

The model was trained on the extracted features and outputs a continuous anomaly score. A percentile-based threshold (5th percentile) was applied to distinguish normal from potentially suspicious transactions.

This approach avoids reliance on predefined labels and instead learns behavioural norms directly from the data.

Appendix E – Evaluation and Interpretation

The system evaluates transactions using anomaly scores produced by the Isolation Forest model. Lower scores indicate greater deviation from typical behaviour.

Rather than assigning binary labels, the system provides:

- A continuous risk scores.
- A classification (normal or suspicious)
- Feature-level explanations indicating which attributes contributed most to the result.

This approach enhances transparency and interpretability while avoiding overconfidence in classification outcomes. The system is intended to support analytical insight rather than automated enforcement or attribution.

Appendix F – Key Implementation Snippets

F.1 Feature Engineering

```
# Feature extraction from transaction data
def extract_features(tx):
    return {
        "iat": tx["timestamp"] - tx["prev_timestamp"],
        "amount_log": np.log1p(tx["amount"]),
        "ring_size": tx["ring_size"],
        "txs_per_day": tx["txs_per_day"],
        "hour": datetime.fromtimestamp(tx["timestamp"]).hour
    }
```

Explanation:
This function transforms raw transaction data into numerical features suitable for behavioural modelling while preserving user privacy.

F.2 Anomaly Detection Logic

```
# Compute anomaly score using Isolation Forest
features = scaler.transform(feature_df)
scores = isolation_forest.decision_function(features)

threshold = np.percentile(scores, 5)
labels = ["Suspicious" if s < threshold else "Normal" for s in scores]
```

Explanation:
An Isolation Forest is used to assign anomaly scores. Transactions falling below the 5th percentile are classified as anomalous.

F.3 Transaction Lookup and Evaluation

```
def evaluate_transaction(tx_features):
    score = isolation_forest.decision_function([tx_features])[0]
    label = "Suspicious" if score < threshold else "Normal"
    return score, label
```

Explanation:
This function evaluates individual transactions and returns both a quantitative score and an interpretable classification.

F.4 User Interface Integration

```
st.metric("Risk Score", f"{score:.3f}")
st.write("Classification:", label)
```

Explanation:
This connects the model output to the front-end, allowing users to interactively inspect risk assessments.

Appendix G: Source Code Repository

The complete source code developed as part of this dissertation is available via a publicly accessible GitHub repository.

Repository URL:

https://github.com/FizaShaikh293/Portfolio/tree/main/Dissertation

The repository includes:

• Data extraction scripts and preprocessing utilities

• Feature engineering and behavioural analysis modules

• Anomaly detection model implementations

• Streamlit-based visualisation dashboard code

The code is provided to support transparency and reproducibility of the implementation described in this dissertation. All experiments and results reported in the main body of the dissertation were produced using this codebase.