
Identificação de usuários maliciosos de Bitcoin com Floresta Randômica

Vitor Ramos Cardoso



UNIVERSIDADE FEDERAL DE UBERLÂNDIA
FACULDADE DE COMPUTAÇÃO
BACHARELADO EM CIÊNCIA DA COMPUTAÇÃO

Vitor Ramos Cardoso

**Identificação de usuários maliciosos de Bitcoin
com Floresta Randômica**

Trabalho de Conclusão de Curso apresentado
à Faculdade de Computação da Universidade
Federal de Uberlândia, Minas Gerais, como
requisito exigido parcial à obtenção do Título
de Bacharel em Ciência da Computação.

Área de concentração: Ciência da Computação

Orientador: Ivan da Silva Sendin

Uberlândia - MG

2026

Resumo

A expansão e a consolidação do Bitcoin como sistema financeiro descentralizado introduziram desafios complexos à segurança pública e à conformidade regulatória, decorrentes do pseudoanonimato explorado por agentes maliciosos para a prática de crimes como lavagem de dinheiro, operações em mercados ilegais da *Dark Web* e extorsões por *ransomware*. O presente trabalho teve como objetivo desenvolver e avaliar um modelo supervisionado de aprendizado de máquina capaz de classificar transações e endereços da rede Bitcoin para a identificação automatizada de entidades ilícitas. A metodologia empregou registros públicos consolidados da plataforma *Blockchair*, restritos aos blocos 600.000 a 605.999, combinados às rotulações da base de dados *Bitcoin Address Behavior Dataset* (BABD-13). Induziu-se um classificador baseado no algoritmo de Floresta Randômica com ponderação balanceada de classes, seguido por uma heurística de propagação reversa de contaminação e consolidação por votação majoritária ao nível de endereços. A análise de importância de atributos revelou que parâmetros econômicos, notadamente custos de transação (*fee_per_kwu* e *fee_per_kb*) e volumes monetários transacionados, exerceram o papel mais discriminativo na detecção. Na avaliação transacional individual, o classificador obteve acurácia de 100%, precisão macro de 96% e revocação de 84% para a classe minoritária. Ao integrar o mecanismo de pós-processamento por votação majoritária nos endereços ($\theta = 0,5$), o sistema eliminou os falsos negativos, atingindo uma revocação perfeita de 100% sobre as entidades criminosas com acurácia global de 99%, consolidando-se como uma abordagem eficaz e viável para auditorias de conformidade e investigações forenses digitais em ecossistemas de *Blockchain*.

Palavras-chave: Bitcoin, Floresta Randômica, Votação Majoritaria, Blockchain, Aprendizado de Máquina.

Abstract

The expansion and consolidation of Bitcoin as a decentralized financial system have introduced complex challenges to public safety and regulatory compliance, primarily due to pseudo-anonymity exploited by malicious actors for illicit activities such as money laundering, darknet market operations, and ransomware extortions. This study aimed to develop and evaluate a supervised machine learning model capable of classifying transactions and addresses on the Bitcoin network for the automated identification of malicious entities. The methodology utilized public records extracted from the Blockchair platform—spanning blocks 600,000 to 605,999, integrated with ground-truth labels from the Bitcoin Address Behavior Dataset (BABD-13). A Random Forest classifier was trained using balanced class weighting, followed by a contamination heuristic and address majority voting aggregation. Feature importance analysis demonstrated that economic metrics, particularly transaction fees (`fee_per_kwu` and `fee_per_kb`) and transaction amounts in fiat currency, were the most decisive indicators of suspicious behavior. At the transaction level, the model achieved 100% accuracy, a macro precision of 96%, and a recall of 84% for illicit activities. By incorporating the address-level majority voting scheme ($\theta = 0.5$), the system eliminated false negatives, achieving a perfect recall of 100% on malicious addresses and an overall accuracy of 99%, confirming its practical viability for digital forensics and compliance audits within blockchain ecosystems.

Keywords: Bitcoin, Random Forest, Majority Voting, Blockchain, Machine Learning.

Lista de ilustrações

Figura 1 – Anatomia do sistema de Bitcoin. Adaptado de (NERURKAR et al., 2021)	17
Figura 2 – Modelo UTXO do Bitcoin. Adaptado de (Arkham Intelligence, 2024) .	18
Figura 3 – Aprendizado Supervisionado vs. Não Supervisionado. Adaptado de (AnalystPrep, 2021)	31
Figura 4 – Resumo da Estrutura das Transações	39
Figura 5 – Resumo da Estrutura das Entradas	40
Figura 6 – Resumo da Estrutura das Saídas	40
Figura 7 – Resumo Tipos BABD-13	41
Figura 8 – Peso das Variáveis no Modelo	48
Figura 9 – Matriz de Confusão do Modelo(Transações)	49
Figura 10 – Matriz de confusão no nível de endereço	50

Lista de tabelas

Tabela 1 – Metodologias de análise de contaminação de fundos	26
Tabela 2 – Relatório de Classificação	48
Tabela 3 – Relatório de Classificação(Endereços)	50

Lista de siglas

AML Prevenção à Lavagem de Dinheiro - *Anti-Money Laundering*

BABD Conjunto de Dados de Comportamento de Endereços Bitcoin - *Bitcoin Address Behavior Dataset*

CFT Combate ao Financiamento do Terrorismo - *Combating the Financing of Terrorism*

CPU Unidade Central de Processamento - *Central Processing Unit*

CSV Valores Separados por Vírgula - *Comma-Separated Values*

DBSCAN Agrupamento Espacial Baseado em Densidade de Aplicações com Ruído - *Density-Based Spatial Clustering of Applications with Noise*

DDoS Negação de Serviço Distribuída - *Distributed Denial of Service*

DeFi Finanças Descentralizadas - *Decentralized Finance*

DSA Algoritmo de Assinatura Digital - *Digital Signature Algorithm*

ECDLP Problema do Logaritmo Discreto em Curvas Elípticas - *Elliptic Curve Discrete Logarithm Problem*

ECDSA Algoritmo de Assinatura Digital de Curva Elíptica - *Elliptic Curve Digital Signature Algorithm*

E/S Entrada e Saída

EVM Máquina Virtual da Ethereum - *Ethereum Virtual Machine*

GNN Redes Neurais para Grafos - *Graph Neural Networks*

IBM Corporação de Máquinas de Negócios Internacionais - *International Business Machines*

IoT Internet das Coisas - *Internet of Things*

IP Protocolo de Internet - *Internet Protocol*

KYC Conheça Seu Cliente - *Know Your Customer*

ML Aprendizado de Máquina - *Machine Learning*

NHS Serviço Nacional de Saúde - *National Health Service*

OSINT Inteligência de Fontes Abertas - *Open Source Intelligence*

RAM Memória de Acesso Aleatório - *Random Access Memory*

RC Razão de Contaminação

RIPEMD Resumo de Mensagem Primitivo Europeu de Integridade RACE - *RACE Integrity Primitives Evaluation Message Digest*

SHA Algoritmo de Hash Seguro - *Secure Hash Algorithm*

SMOTE Técnica de Sobreamostragem Sintética de Minoria - *Synthetic Minority Over-sampling Technique*

SVM Máquina de Vetores de Suporte - *Support Vector Machine*

Tor O Roteador Cebola - *The Onion Router*

USD Dólar dos Estados Unidos - *United States Dollar*

UTXO Saída de Transação Não Gasta - *Unspent Transaction Output*

XGBoost Aumento Extremo de Gradiente - *Extreme Gradient Boosting*

Sumário

1	INTRODUÇÃO	11
1.1	Objetivo	12
1.2	Contribuições do Trabalho	13
2	FUNDAMENTAÇÃO TEÓRICA	15
2.1	Blockchain	15
2.2	Endereços e o Modelo UTXO	16
2.2.1	Algoritmo de Assinatura Digital de Curva Elíptica (ECDSA)	18
2.3	O Cenário de Crimes e o Mercado da <i>Dark Web</i>	20
2.4	Mercados Negros Digitais	21
2.5	Mercados Negros Digitais	23
2.6	Análise Forense em <i>Blockchain</i>	24
2.7	<i>Mixers</i> e <i>Tumblers</i>	26
2.8	WalletExplorer	28
2.9	Aprendizado de Máquina	29
2.9.1	Aprendizado Supervisionado e Não Supervisionado	30
2.9.2	Mecanismo de Agregação e Votação Majoritária Baseados em Entidade	31
2.9.3	Conjuntos de Dados em <i>Machine Learning</i>	32
3	TRABALHOS RELACIONADOS	34
3.1	Mensuração de Mercados Negros via Transações Bitcoin	34
3.2	Modelagem Supervisionada para Detecção de Atividades Ilegais	35
3.3	Classificação de Endereços por Aprendizado de Máquina e Votação	35
4	METODOLOGIA	37
4.1	Aquisição dos Dados Rotulados para Análise, Treinamento e Validação	37

4.2	Processamento dos Dados e Engenharia de Atributos	38
4.3	Indução e Inferência do Modelo Preditivo através do Algoritmo de Floresta Randômica	42
4.4	Propagação de Rótulos por Heurística de Contaminação e Con- solidação por Votação por Endereço	46
5	RESULTADOS	47
6	CONCLUSÃO	51
	REFERÊNCIAS	53

Introdução

A criação de uma moeda digital descentralizada, isenta da intermediação de entidades bancárias ou governamentais, vinha sendo cogitada por pesquisadores desde o final da década de 1980 (ANTONOPOULOS, 2017). Contudo, sua viabilidade dependia do cumprimento de requisitos fundamentais, tais como: prevenir o gasto duplo (duplicidade de moeda), assegurar a autenticidade das transações e comprovar a titularidade dos valores, tudo isso sob uma arquitetura distribuída. Nesse contexto, em 2008, o Bitcoin foi proposto por uma pessoa ou grupo sob o pseudônimo de Satoshi Nakamoto, por meio do artigo *Bitcoin: A Peer-to-Peer Electronic Cash System* (NAKAMOTO, 2008). Nessa publicação, Nakamoto introduziu quatro mecanismos que viabilizaram o funcionamento prático da primeira moeda digital descentralizada: i) a rede ponto a ponto (*protocolo Bitcoin*); ii) a *blockchain*; iii) as regras de consenso; e iv) o mecanismo de prova de trabalho (*Proof-of-Work*) (ANTONOPOULOS, 2017). Tais componentes asseguram a integridade e a confiabilidade das operações financeiras — desde que a capacidade computacional dos nós honestos supere a de potenciais atacantes —, preservando o anonimato relativo dos participantes e prescindindo de intermediários centrais.

A consolidação do ecossistema das criptomoedas transformou substancialmente a dinâmica dos sistemas financeiros globais ao possibilitar a transferência de valores de forma descentralizada, sem a mediação de instituições bancárias ou estatais. No entanto, certas características operacionais da rede Bitcoin, em especial o pseudoanonimato e a dispensa de identificação prévia para a abertura de carteiras, propiciaram a proliferação de fraudes financeiras, ataques de *ransomware*, transações comerciais ilícitas na *dark web* e a lavagem sistemática de capitais.

Embora o registro histórico da *blockchain* seja público e imutável, a investigação e o rastreamento manual de fluxos ilícitos tornaram-se inviáveis diante do volume exponencial de transações diárias e do emprego progressivo de técnicas de ofuscação, como o fracionamento em cadeias de descascamento (*peeling chains*) e o uso de serviços de mistura (*mixers* ou *tumblers*). A dependência exclusiva de métodos tradicionais de análise estática ou de consultas reativas a listas de bloqueio (*blacklists*) mostra-se insuficiente para

mitigar os riscos enfrentados por autoridades policiais, agências reguladoras e provedores de custódia e intermediação de ativos digitais (*exchanges*).

Diante desse cenário, justifica-se a pesquisa e o desenvolvimento de mecanismos preditivos baseados em aprendizado de máquina supervisionado (*Supervised Machine Learning*), capazes de identificar padrões comportamentais e econômicos sutis nos metadados transacionais. A integração entre técnicas de modelagem preditiva e rotinas de votação agregada por entidade mitiga as limitações impostas por transações com ruídos e reduz a taxa de falsos positivos, fornecendo subsídios técnicos consistentes para fortalecer a segurança do ecossistema, otimizar a perícia forense digital e apoiar processos de conformidade (*compliance*) na prevenção a crimes financeiros e cibernéticos.

Apesar da natureza descentralizada e pseudoanônima do Bitcoin, certas associações entre endereços tornam-se inevitáveis. É o caso de transações com múltiplas entradas, nas quais a heurística de gasto conjunto revela que os insumos pertencem, com alta probabilidade, ao mesmo usuário. Como o histórico de transações é registrado publicamente na *blockchain*, a identificação do titular de um único endereço pode comprometer outros endereços associados, desvelando o conjunto de suas operações financeiras. Diante disso, modelos de aprendizado de máquina (*Machine Learning* – Aprendizado de Máquina (ML)) têm sido aplicados para identificar padrões de comportamento atípico na rede Bitcoin e rastrear fluxos associados a entidades maliciosas.

Diversos estudos exploram diferentes representações de dados e técnicas de ML voltadas à detecção de anomalias. Por exemplo, no artigo *Anomaly Detection in Bitcoin Network Using Unsupervised Learning Methods* (PHAM; LEE, 2016), Pham e Lee modelam os dados da *blockchain* em duas estruturas relacionais — um grafo de usuários e um grafo de transações — e avaliam três métodos não supervisionados: *k-means*, distância de Mahalanobis e *Unsupervised Support Vector Machine* (Máquina de Vetores de Suporte (SVM)), comparando os agrupamentos obtidos com registros públicos de roubos e fraudes. De forma análoga, Monamo emprega o *k-means* em *Unsupervised learning for robust Bitcoin fraud detection* (UNSUPERVISED..., 2016). Posteriormente, em *A Multifaceted Approach to Bitcoin Fraud Detection: Global and Local Outliers* (MONAMO; MARIVATE; TWALA, 2016), Monamo adota o *k-means* em conjunto com *kd-trees* para analisar valores atípicos sob perspectivas globais e locais, comparando a eficácia dessas abordagens na identificação precisa de atividades suspeitas na rede.

1.1 Objetivo

O objetivo deste trabalho é desenvolver e avaliar um modelo de aprendizado de máquina supervisionado capaz de classificar transações e endereços da rede Bitcoin para a identificação automatizada de usuários maliciosos. Para tanto, busca-se mitigar os efeitos do pseudoanonimato na *blockchain* do Bitcoin por meio do algoritmo de Florestas Randô-

micas (*Random Forest*), integrado a uma heurística subsequente de votação majoritária por endereço. Para atingir o objetivo geral, definem-se os seguintes objetivos específicos:

1. **Adquirir e unificar dados públicos da *blockchain*:** coletar dados brutos estruturados de transações (*transactions*), entradas (*inputs*) e saídas (*outputs*) por intermédio da plataforma Blockchair;
2. **Mapear e rotular as entidades de análise:** integrar os endereços extraídos da *blockchain* à base de dados *Bitcoin Address Behavior Dataset* (Conjunto de Dados de Comportamento de Endereços Bitcoin (BABD)-13) (XIANG et al., 2024), realizando a rotulação binária entre entidades benignas (como corretoras centralizadas e carteiras individuais) e maliciosas (como mercados da *darknet* e esquemas Ponzi);
3. **Implementar a engenharia de atributos:** desenvolver rotinas de processamento em lotes para viabilizar a manipulação de grandes volumes de dados e extrair métricas financeiras representativas das transações (como taxas por unidade de peso – *fee_per_kwu* – e volume financeiro em Dólar dos Estados Unidos (USD));
4. **Treinar e avaliar o modelo preditivo transacional:** ajustar um classificador baseado no algoritmo de Florestas Aleatórias com estratégias de balanceamento de classes, aplicando-o na inferência do caráter lícito ou ilícito de transações individuais;
5. **Desenvolver o mecanismo de votação agregada por endereço:** estruturar uma rotina de agregação histórica que compute a Razão de Contaminação de cada endereço com base em suas transações associadas, aplicando um limiar de decisão para a classificação final da entidade;
6. **Validar a eficácia empírica da abordagem:** mensurar o desempenho preditivo nos níveis de transação e de endereço por meio de métricas estatísticas consolidadas (Precisão, *Recall*, *F1-Score* e Matrizes de Confusão), discutindo a aplicabilidade prática da solução em investigações forenses e em rotinas de conformidade (*compliance*) no setor financeiro.

1.2 Contribuições do Trabalho

As principais contribuições teóricas, metodológicas e práticas desenvolvidas ao longo deste trabalho compreendem:

- **Extração de atributos econômicos discriminativos:** mapeamento e mensuração do impacto de variáveis de custo de rede (*fee_per_kwu* e *fee_per_kb*) e de volume financeiro em moeda fiduciária (USD) na distinção de perfis transacionais, comprovando empiricamente a correlação entre a urgência de liquidação por agentes

maliciosos e a disposição para o pagamento de taxas significativamente superiores à média da rede;

- ❑ **Modelagem supervisionada com balanceamento de classes:** indução de um modelo baseado no algoritmo de Floresta Randômica com ajuste dinâmico de perdas ponderadas (`class_weight='balanced'`), mitigando o severo desbalanceamento intrínseco aos dados forenses da *blockchain* sem introduzir as distorções decorrentes de técnicas sintéticas de sobreamostragem;
- ❑ **Arquitetura de consolidação por votação majoritária:** proposição e implementação de uma heurística de propagação reversa de rótulos preditos com comitê de decisão por entidade ($\theta = 0,5$), mecanismo responsável por mitigar falsos negativos no nível de endereços e alcançar revocação de 100% sobre entidades ilícitas, mantendo uma acurácia global de 99%;
- ❑ **Validação prática e aplicabilidade operacional:** sistematização e validação dos resultados empíricos confrontados com a base BABD-13, demonstrando a viabilidade técnica de emprego da ferramenta em investigações periciais e em rotinas preventivas de Conheça seu Cliente (*Know Your Customer* – Conheça Seu Cliente (KYC)) e Prevenção à Lavagem de Dinheiro (*Anti-Money Laundering* – Prevenção à Lavagem de Dinheiro (AML)).

Fundamentação teórica

2.1 Blockchain

A *blockchain* é uma tecnologia de registro distribuído ponto a ponto (*peer-to-peer*) estruturada de forma descentralizada, que emprega primitivas criptográficas para assegurar a integridade e a imutabilidade dos dados. Nessa arquitetura, as informações são organizadas em uma cadeia sequencial de blocos, na qual cada bloco é identificado univocamente por um resumo criptográfico (*hash*) — gerado comumente por meio do algoritmo SHA-256 — e compreende metadados fundamentais, tais como o tamanho do bloco, o *hash* do cabeçalho do bloco anterior e o conjunto de transações a serem liquidadas. A vinculação encadeada por funções de dispersão (*hash*) inviabiliza a alteração retroativa dos registros sem a invalidação dos blocos subsequentes, de modo que novos blocos só podem ser anexados à cadeia mediante um protocolo de consenso validado pelos nós participantes da rede.

Embora um dos precursores conceituais da tecnologia tenha surgido em 1991, quando Stuart Haber e W. Scott Stornetta (HABER; STORNETTA, 1991) propuseram um sistema de aposição de carimbos de data/hora (*timestamps*) para impedir a adulteração de documentos digitais, a *blockchain* consolidou sua relevância prática apenas em 2008. Nesse ano, Satoshi Nakamoto introduziu a tecnologia como o livro-razão distribuído para registro de transações financeiras no artigo que fundou o Bitcoin (NAKAMOTO, 2008), conforme ilustrado na Figura 1. Em 2014, inspirado pela arquitetura de Nakamoto, Vitalik Buterin publicou a proposta fundacional do Ethereum (BUTERIN, 2014), na qual expandiu a lógica transacional ao introduzir contratos inteligentes (*smart contracts*) executáveis por meio de mensagens com campo de dados opcional, permitindo a execução determinística de funções de estado de propósito geral na própria rede.

Atualmente, a literatura científica sobre *blockchain* concentra-se no aprimoramento de algoritmos de consenso, na preservação de segurança e privacidade e na mitigação de gargalos de escalabilidade. Um dos principais eixos de pesquisa contempla a convergência entre *blockchain* e a Internet das Coisas (*Internet of Things* – Internet das Coisas (IoT)),

como exemplificado pela plataforma IOTA, voltada ao suporte operacional em ambientes restritos de IoT. Paralelamente, o setor corporativo tem implementado redes permissivas para otimizar processos logísticos e de rastreabilidade. Dentre essas iniciativas, destaca-se a *Intel Connected Logistics Platform*, solução concebida para monitorar a cadeia de suprimentos em tempo real, fornecendo telemetria contínua sobre localização geográfica, temperatura e condições de armazenamento de mercadorias (DIFRANCESCO; MEENA; KUMAR, 2023).

2.2 Endereços e o Modelo UTXO

A contabilidade do Bitcoin baseia-se conceitualmente no modelo Saída de Transação Não Gasta (UTXO) (*Unspent Transaction Output*, ou Saída de Transação Não Gasta) e na utilização de endereços criptográficos. Diferentemente dos sistemas bancários tradicionais — que operam sob a lógica baseada em contas, na qual uma instituição centralizada mantém o registro do saldo global de cada correntista —, o Bitcoin adota uma dinâmica análoga ao manuseio de cédulas físicas em uma carteira digital (ANTONOPOULOS, 2017).

Um endereço Bitcoin consiste em um identificador público destinado ao recebimento de valores. Sua geração ocorre de maneira determinística: a partir de uma chave privada (mantida sob posse exclusiva do usuário), deriva-se uma chave pública correspondente que, após ser submetida a funções criptográficas de dispersão (*hashing*), dá origem ao endereço final. Graças a essa arquitetura, uma carteira é capaz de derivar pares de chaves distintos e, por conseguinte, gerar múltiplos endereços para um mesmo titular.

No modelo UTXO, uma transação não debita montantes de um saldo abstrato; em vez disso, ela consome uma ou mais saídas não gastas oriundas de transações precedentes (entradas) e gera novas saídas associadas aos endereços de destino. Suponha-se, hipoteticamente, um usuário com saldo acumulado de 7 BTC, fragmentado em quatro UTXOs com valores nominais de 5, 1, 0,8 e 0,2 BTC. Caso deseje transferir 5,10 BTC, a operação consumirá as UTXOs de 5 e 0,2 BTC (totalizando 5,20 BTC de entrada) e gerará duas novas saídas: 5,10 BTC creditados ao destinatário e 0,09 BTC retornados como troco a um endereço controlado pelo próprio remetente, sendo os 0,01 BTC residuais destinados à remuneração dos mineradores como taxa de rede, conforme ilustrado na Figura 2.

Por serem indivisíveis, as UTXOs de pequeno valor residual tendem a se acumular na carteira com o decorrer das transações, fenômeno que amplia o tamanho em bytes das transações futuras que exijam múltiplos insumos para compor o montante demandado. Diante desse cenário, é frequente a realização de transações de consolidação — operações em que o usuário transfere múltiplos insumos para um novo endereço próprio —, condensando valores fragmentados em uma única UTXO com o propósito de racionalizar o pagamento de taxas futuras e organizar a gestão interna de seus fundos.

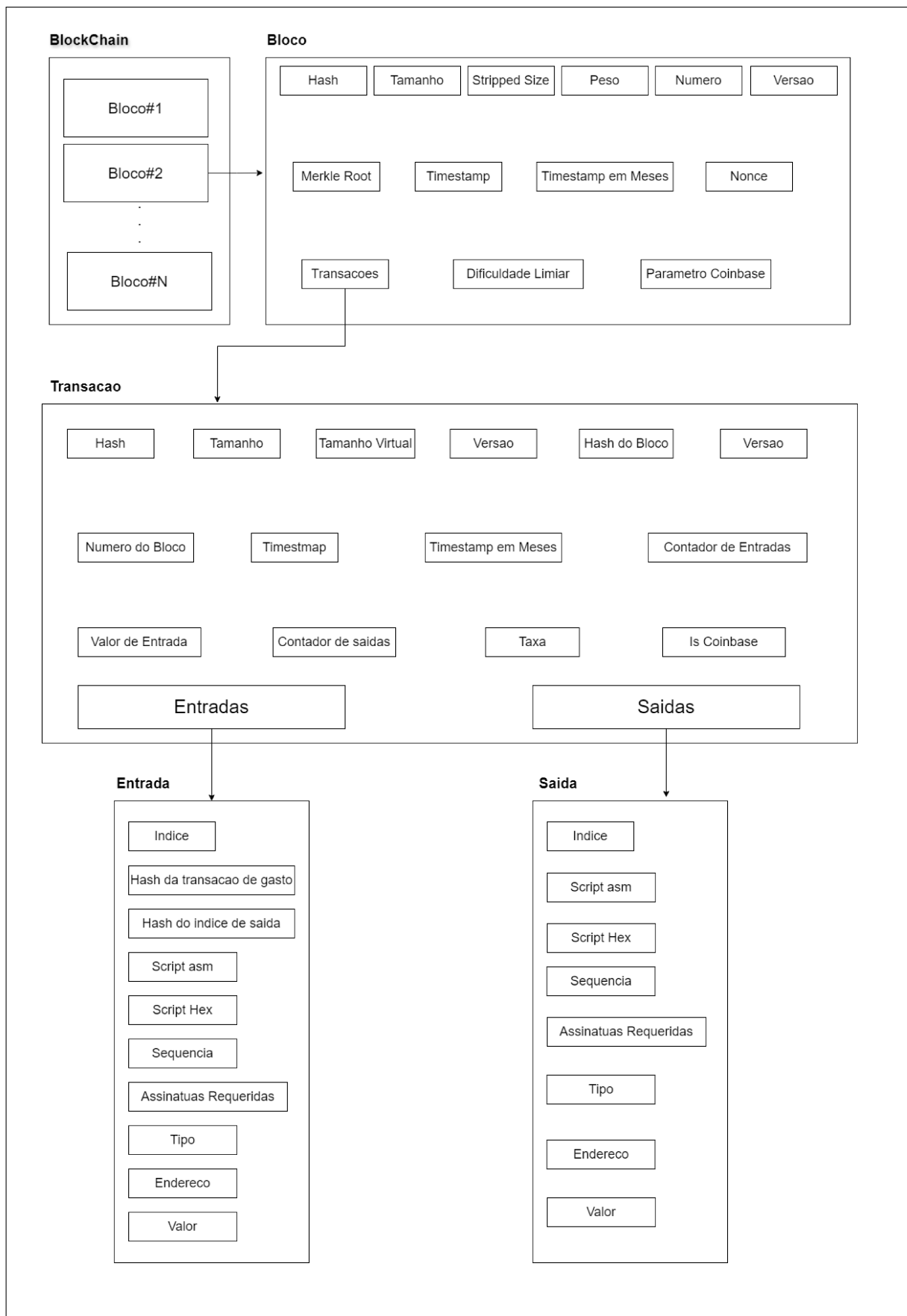


Figura 1 – Anatomia do sistema de Bitcoin. Adaptado de (NERURKAR et al., 2021)

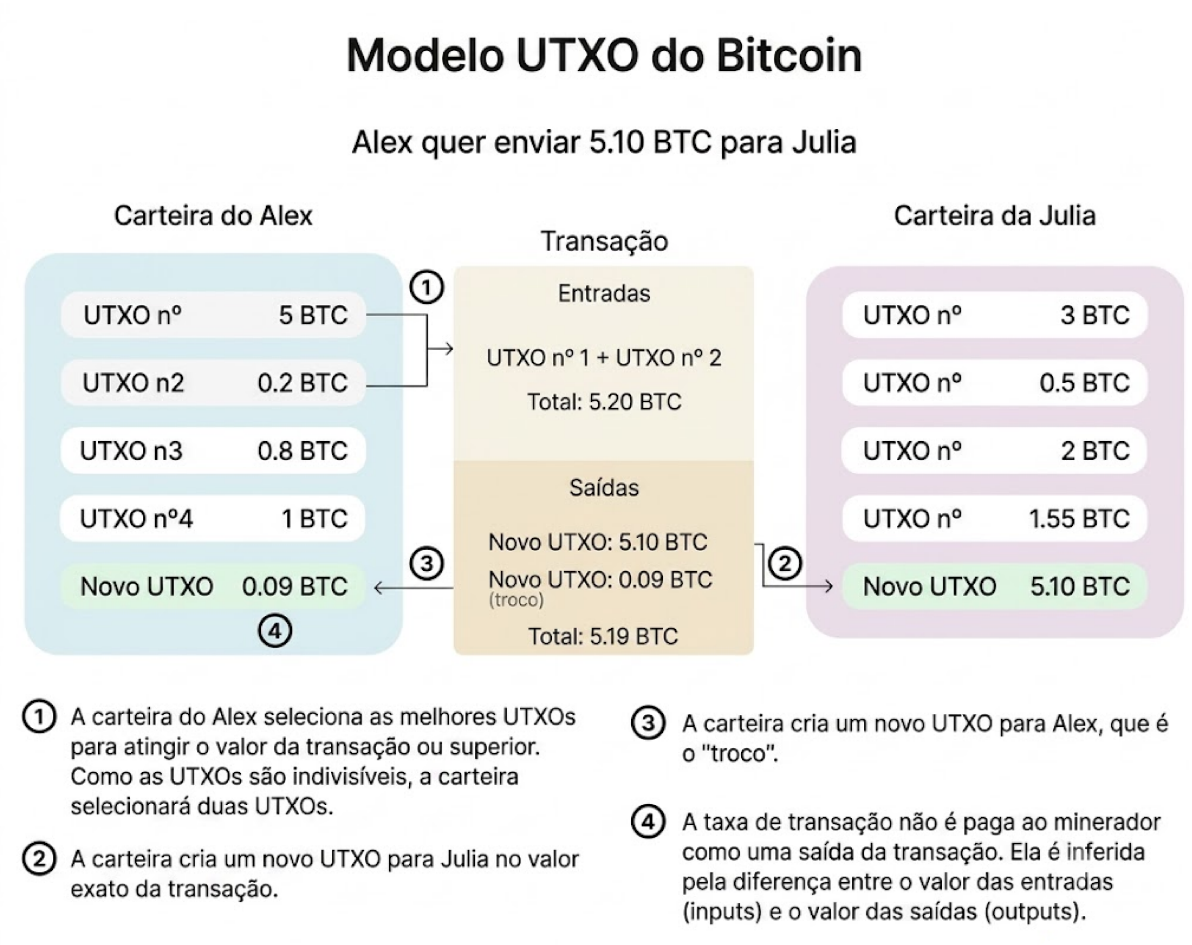


Figura 2 – Modelo UTXO do Bitcoin. Adaptado de (Arkham Intelligence, 2024)

Essa estrutura relacional baseada em grafos de transações — ilustrada na Figura 1 e armazenada publicamente na *blockchain* — caracteriza-se pela presença de múltiplas entradas e saídas. Essa particularidade viabiliza o emprego de algoritmos de aprendizado de máquina, como a Floresta Randômica, para o rastreamento de fluxos financeiros e o agrupamento de chaves (*clustering*), fundamentando-se na premissa heurística de que insumos consumidos em uma transação de múltiplas entradas pertencem, predominantemente, a um mesmo titular.

2.2.1 Algoritmo de Assinatura Digital de Curva Elíptica (ECDSA)

A integridade, o controle de posse e a autorização de transferências de fundos na rede Bitcoin dependem estritamente de criptografia de chave assimétrica. Diferentemente dos sistemas centralizados, nos quais a autenticação ocorre por meio de credenciais validadas por servidores de identidade, o Bitcoin emprega o Algoritmo de Assinatura Digital de Curva Elíptica (*Elliptic Curve Digital Signature Algorithm* – Algoritmo de Assinatura

Digital de Curva Elíptica (ECDSA)) para comprovar matematicamente a titularidade sobre as Saídas de Transação Não Gastas (UTXOs) (ANTONOPOULOS, 2017).

O ECDSA é uma variante do Algoritmo de Assinatura Digital (Algoritmo de Assinatura Digital (DSA)) baseada na álgebra de curvas elípticas sobre corpos finitos. O protocolo Bitcoin adota especificamente a curva parametrizada **secp256k1**, definida pela forma canônica de Weierstrass sobre um corpo primo F_p :

$$y^2 \equiv x^3 + 7 \pmod{p}, \quad (1)$$

em que p é um número primo definido por $p = 2^{256} - 2^{32} - 977$. A escolha da curva *secp256k1* proporciona elevado nível de segurança computacional com chaves compactas de 256 bits, otimizando o espaço de armazenamento demandado na *blockchain* pública.

O ciclo de vida da identidade e da validação financeira de um usuário no Bitcoin fundamenta-se em três etapas operacionais encadeadas pelo ECDSA:

1. **Geração do par de chaves:** a chave privada (k) consiste em um escalar inteiro de 256 bits gerado de forma criptograficamente aleatória. A partir dessa chave, calcula-se a chave pública correspondente (K) mediante a multiplicação escalar de ponto na curva elíptica:

$$K = k \cdot G, \quad (2)$$

em que G representa o ponto gerador predefinido da curva *secp256k1*. Em virtude da intratabilidade do Problema do Logaritmo Discreto em Curvas Elípticas (Problema do Logaritmo Discreto em Curvas Elípticas (ECDLP)), a operação inversa é computacionalmente inviável, tornando impraticável deduzir a chave privada k conhecendo-se unicamente a chave pública K ;

2. **Derivação do endereço:** para mitigar riscos de exposição prematura da chave pública e garantir compatibilidade de formatos, o endereço final exibido na *blockchain* não corresponde diretamente à chave pública em texto claro, mas sim ao resultado de funções criptográficas de dispersão aplicadas consecutivamente sobre ela, notadamente os algoritmos Algoritmo de Hash Seguro (SHA)-256 e Resumo de Mensagem Primitivo Europeu de Integridade RACE (RIPEMD)-160;
3. **Assinatura e verificação de transações:** ao despendar uma UTXO, o titular constrói um *script* de entrada (*scriptSig*) que incorpora uma assinatura digital gerada a partir de sua chave privada (k) e do *hash* dos dados da nova transação.

Qualquer nó validador ou minerador da rede pode verificar a validade da assinatura utilizando exclusivamente a mensagem original, a assinatura digital e a respectiva chave pública do emissor. Sendo a assinatura matematicamente válida, comprovam-se simultaneamente duas propriedades fundamentais: (i) a autenticidade e a posse, evidenciando

que o emissor detém a chave privada atrelada aos fundos transacionados; e (ii) a integridade, atestando que o conteúdo da transação não sofreu adulteração após ser assinado, o que previne ataques de falsificação durante a propagação na rede.

No âmbito da perícia computacional e do aprendizado de máquina, o esquema ECDSA do Bitcoin estabelece uma relação unívoca no momento do gasto. Embora um usuário possa gerar múltiplos endereços a partir de diferentes chaves derivadas de sua carteira, cada assinatura anexada a um insumo expõe publicamente a respectiva chave pública. Essa característica viabiliza a aplicação da heurística de múltiplas entradas (discutida na Seção 2.8), fundamentada no princípio de que chaves públicas distintas que assinam conjuntamente os insumos de uma mesma transação pertencem a uma mesma entidade controladora. A tentativa de ruptura dessa rastreabilidade por meio de técnicas de ofuscação (como *mixers*) ou transações multifacetadas reforça a relevância de se extrair atributos (*features*) comportamentais, permitindo que modelos supervisionados — a exemplo da Floresta Randômica adotada neste trabalho — classifiquem atividades ilícitas mesmo sob as barreiras do pseudoanonimato.

2.3 O Cenário de Crimes e o Mercado da *Dark Web*

Embora o Bitcoin tenha sido concebido como um protocolo de transferência financeira legítimo e descentralizado, a sua natureza pseudoanônima — na qual a identidade civil do usuário não está explicitamente vinculada ao endereço criptográfico na rede — tornou o ecossistema suscetível à proliferação de atividades ilícitas.

Na arquitetura da *web*, costuma-se delimitar as camadas de visibilidade e controle de acesso em três níveis principais:

1. ***Surface Web***: compreende a fração indexada publicamente por mecanismos de busca convencionais (como Google e Bing), englobando portais de notícias, enciclopédias colaborativas e plataformas institucionais abertas;
2. ***Deep Web***: abrange todo o conteúdo não indexado por motores de busca padronizados, incluindo bancos de dados relacionais protegidos por autenticação, repositórios corporativos internos e caixas de correio eletrônico;
3. ***Dark Web***: subcamada restrita da *Deep Web* cujo acesso requer aplicações de sobreposição e protocolos de roteamento especializados, a exemplo da rede O Roteador Cebola (Tor) (*The Onion Router*), projetados para mitigar a rastreabilidade geográfica e assegurar o anonimato de tráfego dos usuários.

A convergência entre o anonimato de rede garantido pelo Tor e o pseudoanonimato financeiro provido pelo Bitcoin viabilizou a consolidação dos *Darknet Markets* (mercados

clandestinos digitais). Historicamente, plataformas precursoras como o *Silk Road* evidenciaram a estruturação de mercados descentralizados para o comércio de substâncias entorpecentes, armamentos, credenciais vazadas e artefatos para ciberguerra (*cyberwarfare*). A fim de obscurecer a origem e o destino do capital, os operadores empregam o fracionamento em sucessivas transações de baixo valor associado a técnicas de ofuscação, como os serviços de mistura (*mixers*) (NERURKAR et al., 2021), caracterizando esquemas clássicos de lavagem de dinheiro adaptados a ativos criptográficos.

Ademais, o Bitcoin é frequentemente empregado por cibercriminosos como meio de pagamento para extorsão de dados (*blackmail*) e resgate em incidentes de *ransomware*. Nesse último modelo, um *software* malicioso (*malware*) cifra os sistemas da vítima até que uma quantia em criptoativos seja depositada em um endereço predeterminado. O episódio paradigmático dessa modalidade ocorreu em maio de 2017 com a disseminação global do *ransomware* WannaCry, que infectou mais de 200 mil dispositivos em 150 países — atingindo corporações globais como FedEx, Honda e Nissan, além da infraestrutura hospitalar do Serviço Nacional de Saúde (Serviço Nacional de Saúde (NHS)) do Reino Unido (Cloudflare, 2026). Para que as chaves de descryptografia fossem teoricamente disponibilizadas, exigia-se o depósito compulsório de quantias em Bitcoin.

Tais incidentes despertam crescente escrutínio de agências reguladoras e autoridades policiais, gerando fricções na adoção pública do protocolo e impactando diretamente as corretoras de ativos virtuais (*exchanges*). Com o propósito de desmistificar preconceitos associados ao ecossistema e assegurar conformidade regulatória, essas intermediárias implementam ferramentas de monitoramento heurístico e aprendizado de máquina para identificar carteiras e transações suspeitas, prevenindo a intermediação involuntária de ilícitos.

Em determinadas circunstâncias, a atuação colaborativa entre corretoras e órgãos de investigação revela-se determinante na elucidação de fraudes complexas. Ilustra essa dinâmica a fraude cibernética perpetrada contra a empresa de tecnologia C&M Software, em que agentes maliciosos desviaram cerca de R\$ 541 milhões e tentaram canalizar os recursos por intermédio de empresas de fachada para posterior conversão em criptomonedas (CNN Brasil, 2026). A movimentação anômala foi identificada inicialmente pelos sistemas de prevenção a fraudes das próprias corretoras, que reportaram o evento às autoridades do Banco Central, possibilitando a contenção tempestiva do esquema financeiro ilícito.

2.4 Mercados Negros Digitais

Os mercados negros digitais (*Darknet Markets*) constituem plataformas comerciais ilícitas hospedadas na camada restrita da internet (*Dark Web*). O funcionamento dessas plataformas baseia-se na convergência de dois pilares tecnológicos: o roteamento por meio da rede Tor (*The Onion Router*) — que mascara o tráfego e os endereços Protocolo de

Internet (IP) de servidores e clientes por meio de camadas concêntricas de criptografia — e o ecossistema pseudoanônimo das criptomoedas, notadamente o Bitcoin, que opera como instrumento de liquidação financeira descentralizado, prescindindo de instituições bancárias regulamentadas.

O marco histórico dessa modalidade de cibercrime organizado consolidou-se em 2011 com o surgimento do *Silk Road*. Investigações forenses subsequentes sobre o histórico transacional dessa plataforma e de seus sucessores — como *Agora*, *Evolution*, *Nucleus*, *Abraxas* e *AlphaBay* — demonstraram que, a despeito da promessa de anonimato absoluto, tais ambientes operavam sob rotinas sistemáticas padronizadas. Um padrão clássico identificado nessas plataformas consistia no fracionamento e na execução reiterada de transações internas com valores nominais fixos de 0,01BTC, heurística concebida para mascarar a correlação de fluxos financeiros entre as carteiras de compradores e vendedores na *blockchain* (HIRAMOTO; TSUCHIYA, 2020).

A dinâmica econômica dos mercados clandestinos na *Dark Web* estruturou-se em torno da distribuição massiva de produtos e serviços ilícitos, organizados em três eixos principais:

1. **Narcotráfico e armamentos:** comercialização ilícita de entorpecentes e armas de fogo, viabilizada por técnicas de ocultação física em remessas postais e logística dissimulada;
2. **Vazamento de dados e fraudes financeiras:** negociação de credenciais de acesso a redes corporativas, bases de dados pessoais exfiltradas de grandes corporações e registros de cartões de crédito clonados prontos para liquidação;
3. **Artefatos maliciosos e infraestrutura cibercriminosa:** fornecimento de ferramentas de intrusão, redes zumbis (*botnets*) voltadas a ataques distribuídos de negação de serviço (Negação de Serviço Distribuída (DDoS)) e locação de infraestrutura no modelo de serviço para campanhas de *ransomware*.

Para realizar o desinvestimento do capital obtido nessas atividades e romper o encadeamento determinístico na *blockchain*, os operadores recorrem a práticas especializadas de lavagem de capitais, com destaque para serviços de mistura (*mixers* ou *tumblers*). Essas ferramentas combinam as saídas não gastas oriundas da *Darknet* a transações legítimas de terceiros mediante estruturas com múltiplas entradas e saídas, buscando inviabilizar a reconstrução analítica e o rastreamento linear dos fluxos de valor.

A despeito da sofisticação dessas práticas de ocultação, as particularidades operacionais dos mercados clandestinos introduzem vieses comportamentais e econômicos discrepantes em relação aos usuários regulares da rede. Conforme evidenciado por Kanemura, Toyoda e Ohtsuki (KANEMURA; TOYODA; OHTSUKI, 2019), os administradores de *Darknet Markets* operam sob constante urgência temporal na liquidação de ativos e dispersão de saldos, visando mitigar o risco de apreensões judiciais ou o congelamento preventivo

de carteiras por órgãos investigativos. Esse imperativo operacional induz tais entidades a arcar com taxas de transação substancialmente superiores à média da rede para assegurar prioridade na validação e inclusão de seus blocos pelos mineradores. Tal anomalia econômica fornece atributos altamente discriminativos durante a etapa de engenharia de atributos, servindo de insumo para que algoritmos de aprendizado de máquina supervisionado — a exemplo do modelo baseado em Floresta Randômica proposto neste trabalho — consigam identificar e segregar transações e entidades ilícitas de forma automatizada.

2.5 Mercados Negros Digitais

Os mercados negros digitais (*Darknet Markets*) constituem plataformas comerciais ilícitas hospedadas na camada restrita da internet (*Dark Web*). O funcionamento dessas plataformas baseia-se na convergência de dois pilares tecnológicos: o roteamento por meio da rede Tor (*The Onion Router*) — que mascara o tráfego e os endereços IP de servidores e clientes por meio de camadas concêntricas de criptografia — e o ecossistema pseudoanônimo das criptomoedas, notadamente o Bitcoin, que opera como instrumento de liquidação financeira descentralizado, prescindindo de instituições bancárias regulamentadas.

O marco histórico dessa modalidade de cibercrime organizado consolidou-se em 2011 com o surgimento do *Silk Road*. Investigações forenses subsequentes sobre o histórico transacional dessa plataforma e de seus sucessores — como *Agora*, *Evolution*, *Nucleus*, *Abraxas* e *AlphaBay* — demonstraram que, a despeito da promessa de anonimato absoluto, tais ambientes operavam sob rotinas sistemáticas padronizadas. Um padrão clássico identificado nessas plataformas consistia no fracionamento e na execução reiterada de transações internas com valores nominais fixos de $0,01BTC$, heurística concebida para mascarar a correlação de fluxos financeiros entre as carteiras de compradores e vendedores na *blockchain* (HIRAMOTO; TSUCHIYA, 2020).

A dinâmica econômica dos mercados clandestinos na *Dark Web* estruturou-se em torno da distribuição massiva de produtos e serviços ilícitos, organizados em três eixos principais:

1. **Narcotráfico e armamentos:** comercialização ilícita de entorpecentes e armas de fogo, viabilizada por técnicas de ocultação física em remessas postais e logística dissimulada;
2. **Vazamento de dados e fraudes financeiras:** negociação de credenciais de acesso a redes corporativas, bases de dados pessoais roubadas de grandes corporações e registros de cartões de crédito clonados prontos para liquidação;
3. **Artefatos maliciosos e infraestrutura cibercriminosa:** fornecimento de ferramentas de intrusão, redes zumbis (*botnets*) voltadas a ataques distribuídos de negação de serviço (DDoS) e locação de infraestrutura no modelo de serviço para campanhas de *ransomware*.

Para realizar o desvinculo do capital obtido nessas atividades e romper o encadeamento determinístico na *blockchain*, os operadores recorrem a práticas especializadas de lavagem de capitais, com destaque para serviços de mistura (*mixers* ou *tumblers*). Essas ferramentas combinam as saídas não gastas oriundas da *Darknet* a transações legítimas de terceiros mediante estruturas com múltiplas entradas e saídas, buscando inviabilizar a reconstrução analítica e o rastreamento linear dos fluxos de valor.

A despeito da sofisticação dessas práticas de ocultação, as particularidades operacionais dos mercados clandestinos introduzem vieses comportamentais e econômicos discrepantes em relação aos usuários regulares da rede. Conforme evidenciado por Kanemura, Toyoda e Ohtsuki (KANEMURA; TOYODA; OHTSUKI, 2019), os administradores de *Darknet Markets* operam sob constante urgência temporal na liquidação de ativos e dispersão de saldos, visando mitigar o risco de apreensões judiciais ou o congelamento preventivo de carteiras por órgãos investigativos. Esse imperativo operacional induz tais entidades a arcar com taxas de transação substancialmente superiores à média da rede para assegurar prioridade na validação e inclusão de seus blocos pelos mineradores. Tal anomalia econômica fornece atributos altamente discriminativos durante a etapa de engenharia de atributos, servindo de insumo para que algoritmos de aprendizado de máquina supervisionado — a exemplo do modelo baseado em Floresta Randômica proposto neste trabalho — consigam identificar e segregar transações e entidades ilícitas de forma automatizada.

2.6 Análise Forense em *Blockchain*

A perícia computacional aplicada a redes *blockchain* fundamenta-se na premissa de que, embora os usuários operem sob o pseudoanonimato de seus endereços criptográficos, a cadeia de blocos é imutável e de acesso público. Assim, a associação de um endereço suspeito a uma entidade real viabiliza a recomposição de todo o seu histórico de transações e a identificação de conexões pregressas, possibilitando o agrupamento de outros endereços controlados pelo mesmo agente. Em determinados cenários, a identificação civil do titular torna-se viável mediante o rastreamento de fluxos transacionais direcionados a interfaces externas à rede que exigem identificação prévia, a exemplo de corretoras de criptoativos (*exchanges*) ou estabelecimentos comerciais que demandem dados de faturamento.

De acordo com (RODRIGUES; SANTOS, 2026), as seguintes abordagens configuram os métodos predominantes na investigação forense em *blockchain*:

1. **Análise de agrupamento (*clustering*) e heurísticas comportamentais:** consiste na agregação de múltiplos endereços de redes baseadas no modelo UTXO (como o Bitcoin) sob a inferência de que pertencem a um mesmo controlador. A principal abordagem baseia-se na heurística de gasto conjunto, que assume que todos os insumos consumidos em uma transação com múltiplas entradas são assinados pelo mesmo titular. No entanto, tal premissa encontra limitações práticas na utilização

de protocolos de privacidade, como transações *CoinJoin* (em que diferentes usuários combinam suas entradas e saídas em uma única estrutura), ofuscando o vínculo determinístico entre pagadores e recebedores;

2. **Rastreamento de fluxos e análise de contaminação:** após o agrupamento dos endereços, investiga-se a trajetória dos recursos financeiros. Diante de valores provenientes de ilícitos cibernéticos (como campanhas de *ransomware*), empregam-se metodologias formais de contaminação (sintetizadas na Tabela 1) para modelar a dispersão do montante ilícito entre transações e endereços subsequentes. Essa abordagem atua de maneira análoga à marcação física de cédulas bancárias, permitindo discernir nós de entrada, intermediação e liquidação;
3. **Modelagem em grafos e análise de redes complexas:** representa a *blockchain* como um grafo direcionado, no qual os vértices correspondem a endereços ou entidades e as arestas traduzem as transações financeiras. O cálculo de métricas de centralidade viabiliza a inferência funcional dos nós: a Centralidade de Grau (*Degree Centrality*) evidencia nós com elevado volume de conexões (como grandes corretoras), ao passo que a Centralidade de Intermediação (*Betweenness Centrality*) expõe nós articuladores indispensáveis em rotas de ofuscação e lavagem de capitais (como serviços de *mixers*);
4. **Inteligência de Fontes Abertas (Inteligência de Fontes Abertas (OSINT)) e cruzamento de metadados:** como a análise estritamente intra-rede raramente revela a identidade civil de um usuário, a elucidação pericial exige a correlação com dados externos. Esse processo contempla desde a indexação de endereços citados em fóruns abertos e na *Dark Web* até a cooperação judicial com corretoras regulamentadas, viabilizando o acesso a registros de KYC e auditoria AML/Combate ao Financiamento do Terrorismo (CFT), além da análise forense de rede voltada à captura de endereços IP de nós propagadores;
5. **Perícia em contratos inteligentes e finanças descentralizadas (Finanças Descentralizadas (DeFi)):** em redes baseadas em contas de estado global (como o ecossistema *Ethereum*/Máquina Virtual da Ethereum (EVM)), a investigação prioriza a lógica de execução do código de contratos inteligentes (*Solidity*). A abordagem subdivide-se em: (i) **análise estática**, que examina o *bytecode* registrado na cadeia à procura de vulnerabilidades preexistentes; e (ii) **análise dinâmica**, que reconstrói a sequência operacional do incidente por meio do rastro de execução (*trace*) da transação, elucidando a manipulação indevida de variáveis de estado.

A perícia forense em *blockchain* recorre, portanto, a heurísticas de grafos e a modelos preditivos para mitigar o pseudoanonimato. Conforme demonstrado por Kanemura, Toyoda e Ohtsuki (KANEMURA; TOYODA; OHTSUKI, 2019), mercados clandestinos

Tabela 1 – Metodologias de análise de contaminação de fundos

Metodologia	Descrição Operacional
FIFO (<i>First-In, First-Out</i>)	Os primeiros fundos creditados à carteira são assumidos como os primeiros a serem liquidados em transações posteriores.
LIFO (<i>Last-In, First-Out</i>)	Os últimos fundos recebidos são considerados os primeiros a serem debitados nas saídas subsequentes.
Poison (Contaminação Direta)	O recebimento de qualquer fração de valor ilícito rotula a totalidade dos fundos e das saídas da carteira como 100% contaminados.
Haircut (Contaminação Proporcional)	O montante contaminado é diluído de forma estritamente proporcional entre todas as saídas geradas pela transação.

apresentam assinaturas econômicas singulares, a exemplo do pagamento de taxas elevadas para assegurar liquidação prioritária nos blocos e da emissão de saídas com montantes fixos. A extração de variáveis discriminativas com base nesses metadados — tais como a taxa por unidade de peso (*fee_per_kwu*), a contagem de insumos e saídas e o volume transacionado em moeda fiduciária — fornece insumos empíricos consistentes para a investigação. Nesse contexto, o emprego de algoritmos de aprendizado de máquina supervisionado, como a Floresta Randômica, consolida-se como um recurso eficaz para a análise pericial em larga escala, viabilizando a classificação precisa de operações financeiras atípicas e a identificação automatizada de carteiras associadas a práticas de *ransomware*, extorsão e fraudes financeiras.

2.7 Mixers e Tumblers

A transparência intrínseca e a publicidade irrestrita da *blockchain* do Bitcoin impõem limites severos a usuários que buscam privacidade em suas atividades econômicas, sejam elas legítimas ou ilícitas. Conforme exposto na Seção 2.6, a vinculação de um endereço criptográfico a uma identidade civil ou a uma infração penal permite que peritos computacionais reconstruam o fluxo das saídas de transações não gastas (UTXOs), identificando a origem e o destino dos valores operados. Em contraposição a essa rastreabilidade determinística, desenvolveram-se serviços especializados de mistura de criptoativos, comumente denominados *mixers* ou *tumblers*.

A finalidade precípua de um *mixer* consiste em romper o encadeamento transacional direto entre remetentes e destinatários, consorciando moedas de origens heterogêneas para inviabilizar a análise linear da cadeia de custódia. Embora tais serviços possam atender

a demandas de salvaguarda de privacidade individual, eles são explorados preponderantemente pelo crime organizado como instrumento de lavagem de capitais oriundos de extorsões por *ransomware*, invasões a corretoras, esquemas de pirâmide financeira e transações em mercados clandestinos da *Dark Web* (SVENDA et al., 2026).

Sob o aspecto arquitetural e operacional, os serviços de mistura subdividem-se em duas categorias principais:

- ❑ **Mixers centralizados:** operam segundo o modelo tradicional de custódia por terceiros. O usuário encaminha frações de Bitcoin sob suspeição para um endereço controlado pelo provedor do serviço. O operador agrega esses montantes a um fundo comum (*pool*), desconta a comissão de intermediação e, após um intervalo de tempo pseudoaleatório, encaminha valores equivalentes — compostos por insumos de outros depositantes — para novos endereços indicados pelo cliente. Esse modelo apresenta vulnerabilidades decorrentes de apreensões judiciais de servidores e do rastreamento de nós operacionais via ferramentas de inteligência em fontes abertas (OSINT);
- ❑ **Mixers descentralizados e ponto a ponto:** dispensam agentes custodiantes ao empregarem primitivas criptográficas distribuídas. A técnica mais proeminente fundamenta-se no protocolo *CoinJoin*, introduzido por Gregory Maxwell em 2013. Nessa abordagem, dezenas de usuários agregam colaborativamente suas entradas em uma transação coletiva massiva que gera saídas de valor padronizado — por exemplo, saídas uniformes de $0,1BTC$. Dada a homogeneidade dos valores de saída, inviabiliza-se a correlação determinística entre entradas e destinos individuais, frustrando a premissa canônica da heurística de gasto conjunto.

Não obstante a eficácia em obscurecer a trilha determinística dos fundos, o emprego de *mixers* e *tumblers* imprime anomalias estatísticas e topológicas na estrutura do grafo transacional da rede. A literatura especializada aponta a emergência de assinaturas transacionais bem definidas, a saber:

1. **Cadeias de descascamento:** fracionamento iterativo de UTXOs volumosas em sucessivas transações de menor monta para transferir valores residuais enquanto o montante principal é progressivamente diluído;
2. **Anomalias tarifárias:** pagamento de taxas de transação desproporcionais com o objetivo de acelerar as confirmações dos blocos da rota de mistura, somado a discrepâncias sistemáticas nos saldos de liquidação causadas pela retenção das tarifas dos operadores;
3. **Nós de alta densidade topológica:** formação de transações com razão desbalanceada e volume incomum de entradas e saídas concorrentes.

Tais evidências estruturais sustentam a viabilidade de detecção orientada a aprendizado de máquina supervisionado. Em vez de se buscar a desanonimização criptográfica direta da transação consorciada — operação muitas vezes matematicamente inviável —, modelos supervisionados baseados em Floresta Randômica exploram a engenharia de atributos financeiros e temporais para caracterizar nós que atuem nos estágios de ingresso, intermediação ou escoamento de *mixers*. A capacidade preditiva de identificar a classe representativa de *tumblers* (Classe 11 na base BABD-13) é componente central da metodologia deste trabalho, fornecendo subsídios automatizados para auditorias de conformidade (*compliance*) e investigações de perícia forense digital.

2.8 WalletExplorer

Um dos principais desafios enfrentados pelo aprendizado de máquina supervisionado aplicado à detecção de ilícitos em *blockchains* decorre do severo desbalanceamento de classes e da escassez de dados históricos rotulados com elevado grau de fidedignidade. Diferentemente do que ocorre com dados estruturados em domínios corporativos convencionais, a identificação dos titulares reais de endereços criptográficos demanda investigações periciais contínuas baseadas em inteligência de fontes abertas (OSINT) e análise forense digital. Nesse contexto, a plataforma WalletExplorer destaca-se historicamente como uma das mais relevantes fontes públicas para a rotulação e atribuição de entidades na rede Bitcoin.

Desenvolvido pelo pesquisador Ales Janda, o *WalletExplorer* opera como um explorador de blocos especializado no agrupamento automatizado de endereços (*clustering*). A ferramenta implementa rotinas algorítmicas fundamentadas na heurística de gasto conjunto, a qual estabelece que, se múltiplos endereços distintos do modelo UTXO forem consumidos concomitantemente para assinar os insumos de uma mesma transação, presume-se que tais chaves estejam sob o controle da mesma entidade ou carteira de *software* (WalletExplorer, 2026).

A relevância acadêmica do *WalletExplorer* reside em sua capacidade de associar esses agrupamentos automatizados (*wallets*) a identidades de serviços e instituições reais catalogadas no ecossistema, abrangendo categorias como:

1. **Mercados clandestinos da *Darknet*:** catalogação e mapeamento sistemático de carteiras e fluxos de liquidação vinculados a plataformas pioneiras, a exemplo de *Silk Road*, *Evolution* e *AlphaBay*;
2. **Serviços de ofuscação:** identificação de endereços controlados por protocolos centralizados e descentralizados de mistura de ativos (*mixers*), cuja finalidade consiste em romper a rastreabilidade do encadeamento transacional;

3. **Plataformas de apostas e jogos de azar:** monitoramento de fluxos transacionais recorrentes e de alta rotatividade característicos de serviços de apostas virtuais;
4. **Corretoras centralizadas (*exchanges*):** delineamento dos grandes agregados de endereços operados por carteiras quentes (*hot wallets*) e carteiras frias (*cold wallets*) sob custódia de intermediários regulamentados.

Em investigações voltadas à classificação e detecção de anomalias por aprendizado de máquina, os dados extraídos do *WalletExplorer* compõem a estrutura central de bases consolidadas na literatura, como o *Bitcoin Address Behavior Dataset* (BABD-13) adotado nesta pesquisa (XIANG et al., 2024). A possibilidade de agregar informações no nível de entidade viabilizada por tais plataformas sustenta a formulação do mecanismo de votação proposto neste trabalho, corroborando a premissa de que a robustez preditiva de classificadores supervisionados baseados em Floresta Randômica é expressivamente ampliada ao se propagar e consolidar as inferências transacionais individuais sobre o histórico conjunto de endereços associados a um mesmo agente econômico (KANEMURA; TOYODA; OHTSUKI, 2019).

2.9 Aprendizado de Máquina

O aprendizado de máquina (*Machine Learning* – ML) constitui uma subárea da inteligência artificial dedicada ao desenvolvimento de algoritmos capazes de inferir iterativamente padrões subjacentes em conjuntos de dados, prescindindo de instruções procedurais expressamente programadas por um operador humano (MÜLLER; GUIDO, 2016).

Os marcos iniciais da área remontam à década de 1950, quando Arthur Samuel, pesquisador da Corporação de Máquinas de Negócios Internacionais (IBM), desenvolveu um programa computacional capaz de aprender a jogar damas autonomamente. Ao longo dos decênios seguintes, o progresso da disciplina enfrentou estagnação decorrente da escassez de dados estruturados e das restrições de poder computacional, limitando a viabilidade comercial das abordagens e restringindo investimentos. A partir do final da década de 1990, contudo, o interesse científico e corporativo pelo aprendizado de máquina experimentou expressiva retomada, impulsionada pelo avanço do poder de processamento e pela expansão da *web*, responsável pela geração de volumes massivos de dados (HURWITZ; KIRSCH, 2018).

Em anos recentes, tais técnicas consolidaram-se em múltiplos domínios: no comércio eletrônico, na modelagem de propensão de consumo; no setor financeiro, na projeção de séries temporais e cotações de ativos; e na segurança cibernética, na antecipação e detecção de ataques em redes corporativas (HURWITZ; KIRSCH, 2018). No contexto da rede Bitcoin — cujo registro público congrega o histórico consolidado de todas as liquidações efetuadas —, métodos de aprendizado de máquina têm sido aplicados com propósitos

analíticos distintos. Por um lado, algoritmos como o *k-means* realizam o agrupamento de endereços que possivelmente compartilham controle comum com base em métricas de similaridade transacional. Por outro lado, modelos supervisionados baseados no comitê de Floresta Randômica operam mediante a construção de múltiplas árvores de decisão durante a etapa de treinamento: durante a inferência, cada árvore avalia individualmente os atributos da transação e emite um voto discriminativo para uma classe (como 0 para instâncias lícitas ou 1 para ilícitas), definindo a predição final do sistema com base no princípio da votação majoritária (FEKADU et al., 2022).

No escopo da segurança computacional e da perícia em redes *blockchain*, o aprendizado de máquina viabiliza o processamento de volumes massivos de dados transacionais, permitindo mapear comportamentos anômalos imperceptíveis por meio de investigações manuais ou regras heurísticas estritamente lineares (NERURKAR et al., 2021).

2.9.1 Aprendizado Supervisionado e Não Supervisionado

Os algoritmos de aprendizado de máquina são categorizados primordialmente a partir da natureza dos dados de entrada e da disponibilidade de anotações prévias, dividindo-se entre paradigmas supervisionados e não supervisionados.

No aprendizado supervisionado, o modelo é ajustado sobre uma base de dados previamente anotada por especialistas. Cada instância de treinamento é modelada por um vetor de atributos pareado a um rótulo canônico, formalizado pelo par ordenado $(\mathbf{x}_i, y_i)$, no qual $\mathbf{x}_i$ representa o vetor de características da transação e y_i a classe categórica correspondente (por exemplo, 0 para entidades benignas e 1 para maliciosas). O objetivo do estimador consiste em mapear uma função de aproximação $f(\mathbf{x}) = y$ capaz de generalizar o padrão aprendido e inferir acuradamente os rótulos de amostras inéditas. As tarefas supervisionadas desdobram-se principalmente em problemas de regressão (quando o alvo assume valores escalares contínuos) e de classificação (quando a variável dependente assume valores discretos e finitos). A classificação é a abordagem central empregada neste trabalho por meio do classificador de Floresta Randômica, complementada na literatura por métodos como Árvores de Decisão, Máquinas de Vetores de Suporte (SVM) e Regressão Logística.

Em contrapartida, no aprendizado não supervisionado, os algoritmos operam sobre distribuições amostrais desprovidas de rótulos predefinidos. A premissa analítica não visa estimar uma classe determinada, mas examinar a geometria intrínseca dos dados para descobrir agrupamentos homogêneos, descontinuidades densitárias ou correlações latentes. Modelos baseados no algoritmo *k-means* ou em redes neurais do tipo *autoencoders* analisam o espaço de representação e agrupam instâncias com suporte em métricas de distância espacial, como a distância euclidiana. Na análise pericial de *blockchains*, métodos não supervisionados são comumente empregados na detecção de valores atípicos (*outliers*) — anomalias globais cujos perfis divergem substancialmente da regularidade transacional

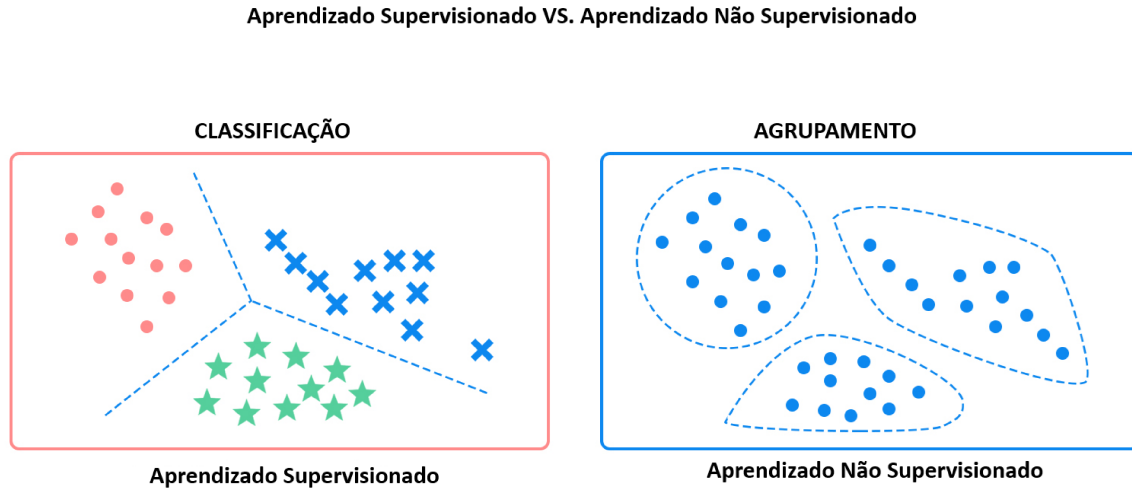


Figura 3 – Aprendizado Supervisionado vs. Não Supervisionado. Adaptado de (Analyst-Prep, 2021)

da rede —, viabilizando triagens exploratórias mesmo quando a tipologia específica do ilícito é desconhecida a priori. Outros métodos representativos dessa classe compreendem o Agrupamento Hierárquico, o Agrupamento Espacial Baseado em Densidade de Aplicações com Ruído (DBSCAN) (*Density-Based Spatial Clustering of Applications with Noise*) e as Florestas de Isolamento (*Isolation Forests*).

2.9.2 Mecanismo de Agregação e Votação Majoritária Baseados em Entidade

Embora algoritmos de aprendizado de máquina supervisionado, como a Floresta Randômica, sejam capazes de inferir rótulos no nível de instâncias individuais (como transações isoladas), a natureza desbalanceada e ruidosa dos dados na *blockchain* pode induzir o classificador de base a falhas pontuais de predição. Na análise de segurança em redes complexas, uma transação legítima pode apresentar temporariamente atributos estatísticos que se assemelham a comportamentos maliciosos (falsos positivos); inversamente, uma transação criminosa pode ser deliberadamente fracionada com vistas a mimetizar operações ordinárias (falsos negativos).

O emprego de sistemas de votação majoritária e agregação por entidade contribui para mitigar os erros cometidos pelos algoritmos de aprendizado de máquina. O princípio fundamental assenta-se na teoria do comitê de decisão e consenso: enquanto uma única transação fornece apenas um recorte instantâneo do comportamento, o histórico consolidado de interações de um determinado nó ou endereço (A_i) reflete o padrão sistemático da respectiva entidade controladora.

No contexto das redes de criptoativos, tais mecanismos operam em duas etapas sequenciais:

1. **Propagação de rótulos por grafo:** dado um conjunto de transações $T = \{t_1, t_2, \dots, t_m\}$ e suas respectivas previsões geradas pelo modelo supervisionado $\hat{y}(t_j) \in \{0, 1\}$, os rótulos inferidos são propagados para todos os endereços A_i que atuaram diretamente como entradas ou saídas dessas operações;
2. **Consolidação da Razão de Contaminação:** o sistema agrega o histórico completo de participações do endereço A_i e computa a proporção de transações classificadas como ilícitas em relação ao seu volume transacional total, definindo a Razão de Contaminação (RC):

$$RC(A_i) = \frac{\sum \text{Transações Preditas como Maliciosas}(A_i)}{\sum \text{Total de Transações}(A_i)}. \quad (3)$$

A tomada de decisão final é regida por uma função de corte parametrizada por um limiar θ , com $0 \leq \theta \leq 1$:

$$\text{Classe}(A_i) = \begin{cases} 1 \text{ (Malicioso)}, & \text{se } RC(A_i) \geq \theta, \\ 0 \text{ (Benigno)}, & \text{se } RC(A_i) < \theta. \end{cases} \quad (4)$$

Dessa forma, à medida que θ converge para zero ($\theta \rightarrow 0$), reduzem-se os falsos negativos à custa da elevação dos falsos positivos; por outro lado, quando θ aproxima-se de um ($\theta \rightarrow 1$), aumentam-se os falsos negativos em prol da redução substancial dos falsos positivos.

Como demonstrado por Kanemura, Toyoda e Ohtsuki (KANEMURA; TOYODA; OHTSUKI, 2019), a aplicação de um esquema de votação ponderado por endereço atenua significativamente o impacto do ruído transacional e eleva as métricas globais de *Recall* e *F1-Score*. Essa abordagem de comitê atua na depuração de falsos negativos no nível de transação: ainda que o classificador falhe pontualmente na identificação de uma transação ilícita isolada, a existência de outras operações devidamente reconhecidas ao longo do histórico do endereço assegura que a Razão de Contaminação ultrapasse o limiar estabelecido, viabilizando a identificação e o isolamento da entidade maliciosa com elevado grau de acurácia.

2.9.3 Conjuntos de Dados em *Machine Learning*

O sucesso preditivo e a capacidade de generalização de qualquer modelo de aprendizado de máquina dependem criticamente da qualidade, da representatividade e do volume do conjunto de dados (*dataset*) utilizado na fase experimental. Uma base de dados estruturada para tarefas supervisionadas é comumente particionada em três subconjuntos

disjuntos com vistas a mitigar o fenômeno do sobreajuste (*overfitting*) e garantir a robustez inferencial do modelo:

1. **Conjunto de treinamento:** corresponde à fração preponderante dos dados (usualmente entre 70% e 80%). Trata-se do subconjunto efetivamente exposto ao algoritmo para a otimização de seus parâmetros internos (a exemplo dos pontos de divisão e limiares de decisão das árvores em uma Floresta Randômica);
2. **Conjunto de validação:** empregado de maneira intermediária para o ajuste fino de hiperparâmetros (como a profundidade máxima das árvores ou o número de estimadores na floresta), auxiliando na seleção da configuração estrutural mais adequada e na prevenção de viés de modelagem;
3. **Conjunto de teste:** fração dos dados mantida sob isolamento estrito durante todo o processo de treinamento e calibração. Atua como simulador de ambiente de produção, sendo consultada exclusivamente na etapa conclusiva para a mensuração imparcial das métricas de desempenho, tais como a Acurácia, a Precisão, a Revocação (*Recall*), a pontuação *F1-Score* e a Matriz de Confusão.

Na literatura científica, diversos repositórios e bases de referência são utilizados para a comparação padronizada de algoritmos. Um dos conjuntos mais emblemáticos na história do aprendizado de máquina é o *Iris dataset*, introduzido pelo estatístico Ronald Fisher em 1936, composto por medições morfométricas (comprimento e largura de sépalas e pétalas) destinadas à discriminação de três espécies do gênero *Iris*.

No domínio específico da análise pericial forense aplicada a criptoativos, a estruturação de bases de dados enfrenta o severo desafio do desbalanceamento de classes, porquanto a volumetria de operações transacionais ordinárias (benignas) na rede Bitcoin supera em ordens de magnitude a proporção de registros comprovadamente atrelados a ilícitos cibernéticos ou financeiros (maliciosos). Diante dessa assimetria amostral, conjuntos de dados especializados como o *Bitcoin Address Behavior Dataset* (BABD-13) (XIANG et al., 2024), adotado neste estudo, atenuam tais limitações metodológicas ao reunir endereços previamente investigados e categorizados por ferramentas de inteligência em fontes abertas (OSINT) e empresas periciais, viabilizando o ajuste consistente de classificadores supervisionados.

Trabalhos relacionados

3.1 Mensuração de Mercados Negros via Transações Bitcoin

No artigo de Hiramoto e Tsuchiya (2020), os autores investigam metodologias para quantificar e mensurar o volume financeiro transacionado em mercados clandestinos digitais. Como plataformas pioneiras na convergência entre o roteamento anônimo da rede Tor e o protocolo Bitcoin, as investigações forenses sobre esses ambientes tornaram-se viáveis a partir da identificação de endereços operacionais vinculados ao *Silk Road*. Neles, observou-se um padrão característico de liquidação interna por meio de transações recorrentes com valor nominal fixo de 0,01 BTC, presumivelmente concebido para desvincular as identidades de compradores e vendedores. Esse mesmo comportamento foi identificado subsequentemente em plataformas sucessoras que compartilhavam rotinas de gestão de carteiras semelhantes.

Tal assinatura econômica, associada à análise relacional das entradas e saídas transacionais, consolidou-se como heurística de referência em investigações posteriores para mapear agrupamentos de endereços conexos, demonstrando que as operações na rede Bitcoin não oferecem o nível absoluto de anonimato comumente pressuposto. Embora esse padrão transacional específico tenha sido descontinuado com o encerramento dos sete mercados analisados — e substituído por moedas focadas em privacidade (*privacy coins*), a exemplo da Monero —, o trabalho de Hiramoto e Tsuchiya (2020) evidenciou que a associação entre heurísticas comportamentais simples e o mapeamento de insumos e saídas possibilita rastrear fluxos e identificar carteiras sob controle de um mesmo agente econômico.

3.2 Modelagem Supervisionada para Detecção de Atividades Ilegais

Em Nerurkar et al. (2021), os autores examinam os desafios metodológicos na classificação pericial da rede Bitcoin, com ênfase nas restrições amostrais de transações analisadas, na escassez de atributos discriminativos e na carência de bases de dados rotuladas com elevado grau de fidedignidade sobre a titularidade dos endereços. Diante dessas lacunas, propõem um arcabouço preditivo supervisionado baseado em Árvores de Decisão, particionado na proporção de 4 : 1 entre os conjuntos de treinamento e teste, avaliando nove atributos estruturais para categorizar transações e endereços em 16 classes distintas sobre um volume amostral expressivamente ampliado da *blockchain*.

O desempenho da abordagem proposta foi confrontado com quatro algoritmos clássicos de referência: Máquinas de Vetores de Suporte (SVM), Regressão Logística, Aumento Extremo de Gradiente (XGBoost) e Floresta Randômica. Em termos de precisão métrica, o método proposto atingiu resultados próximos aos da Floresta Randômica — que se destacou como o classificador de maior precisão global —, enquanto no aspecto de eficiência computacional obteve desempenho comparável ao XGBoost, notório pela capacidade de paralelização de processamento. Por fim, os autores disponibilizaram publicamente as bases de dados consolidadas, fornecendo insumos empíricos padronizados para pesquisas subsequentes na área.

3.3 Classificação de Endereços por Aprendizado de Máquina e Votação

No trabalho de Kanemura, Toyoda e Ohtsuki (2019), os autores propõem um arcabouço metodológico que integra algoritmos de aprendizado de máquina supervisionado a um mecanismo de votação agregada por entidade, visando elevar a precisão na detecção de endereços vinculados a mercados negros digitais. O fluxo analítico estrutura-se em etapas interdependentes: inicialmente, aplica-se a heurística de gasto conjunto aos dados da *blockchain* para correlacionar e agrupar endereços pertencentes a uma mesma entidade controladora. Em seguida, os modelos preditivos são ajustados com base em informações rotuladas provenientes de três fontes principais: a plataforma de inteligência pública *WalletExplorer* e dois fóruns de discussão especializados (o *BitcoinTalk* e uma comunidade restrita na *Dark Web*), dos quais foram extraídos endereços de comprovada atuação ilícita.

O estudo formula um espaço vetorial composto por 73 atributos comportamentais e financeiros extraídos do histórico dos endereços para discriminar entre entidades lícitas e clandestinas. Para mitigar o impacto de ruídos transacionais, implementa-se uma rotina de votação majoritária por entidade: caso a preponderância dos endereços associados a

um determinado agrupamento ultrapasse o limiar de contaminação estipulado, toda a entidade é classificada como maliciosa. Esse comitê de decisão reduz expressivamente as taxas de falsos positivos e falsos negativos, elevando a precisão global do sistema em relação à inferência transacional isolada. Adicionalmente, os autores destacam que os operadores de mercados negros incorrem sistematicamente no pagamento de taxas de mineração superiores à média da rede, utilizando o custo financeiro como mecanismo para assegurar confirmações tempestivas em blocos prioritários.

Metodologia

O objetivo central consiste em mitigar o pseudoanonimato da rede Bitcoin por meio do mapeamento de fluxos transacionais e da posterior classificação de endereços em categorias benignas ou maliciosas, empregando o algoritmo de Floresta Randômica sobre as transações e uma rotina de votação majoritária agregada no nível dos endereços.

O fluxo metodológico estrutura-se em quatro etapas principais: (i) aquisição e unificação dos dados brutos e bases rotuladas para análise, treinamento e validação; (ii) pré-processamento de dados e engenharia de atributos; (iii) ajuste e inferência do modelo preditivo por meio do algoritmo de Floresta Randômica; e (iv) propagação reversa de rótulos por heurística de contaminação com consolidação por votação por endereço.

4.1 Aquisição dos Dados Rotulados para Análise, Treinamento e Validação

A coleta de dados brutos da *blockchain* foi realizada utilizando os registros disponibilizados publicamente pela plataforma Blockchair. Os dados desse repositório incorporam uma variável financeira de alto valor analítico: a conversão do montante transacionado para dólares americanos (USD) com base na cotação cambial do dia da liquidação. Essa padronização mitiga distorções temporais decorrentes da volatilidade histórica do Bitcoin. O recorte temporal adotado compreende o intervalo entre os blocos 600.000 e 605.999, delimitado em razão de sua correspondência direta com as transações dos endereços catalogados no conjunto de dados BABD-13. Os arquivos brutos são segmentados pelas entidades estruturais de transações (Figura 4), entradas (Figura 5) e saídas (Figura 6), distribuídos em formato de valores separados por tabulação e compactados via Gzip (`.tsv.gz`) com partição diária.

A plataforma Blockchair impõe uma restrição de vazão de transferência a usuários gratuitos fixada em 10 kB/s, o que impõe limitações operacionais severas ao descarregamento de arquivos cuja volumetria atinge dezenas de gigabytes. Para automatizar o

processo de requisição e persistência contínua desses dados, desenvolveu-se uma rotina em Python baseada na biblioteca `requests`.

Para o treinamento do classificador supervisionado, faz-se necessária uma base de referência contendo endereços previamente anotados com fidedignidade. Com esse propósito, utilizou-se o *Bitcoin Address Behavior Dataset* (BABD-13) (XIANG et al., 2024), composto por mais de 500.000 endereços distribuídos originariamente em 13 classes funcionais: *blackmail*, *cyber-security service*, *darknet market*, *centralized exchange*, *P2P financial infrastructure service*, *P2P financial service*, *gambling*, *government criminal blacklist*, *money laundering*, *Ponzi scheme*, *mining pool*, *tumbler* e *individual wallet* (codificadas numericamente pelos índices de 0 a 12, conforme ilustrado na Figura 7). Tais entidades participaram ativamente de transações confirmadas entre os blocos 600.000 e 605.999 — intervalo temporal compreendido entre 18 de outubro de 2019 e 23 de novembro de 2019, englobando aproximadamente 12,8 milhões de transações, 28,8 milhões de entradas e 31,6 milhões de saídas. Visando viabilizar a modelagem preditiva binária proposta neste trabalho, as 13 categorias foram agregadas em duas macroclasses: benignas (*cyber-security service*, *centralized exchange*, *P2P financial infrastructure service*, *P2P financial service*, *mining pool* e *individual wallet*) e maliciosas (*blackmail*, *darknet market*, *gambling*, *government criminal blacklist*, *money laundering*, *Ponzi scheme* e *tumbler*).

4.2 Processamento dos Dados e Engenharia de Atributos

Devido à volumetria massiva das tabelas — que superam dezenas de milhões de registros de entradas e saídas —, o carregamento integral dos arquivos brutos na memória Memória de Acesso Aleatório (RAM) provocaria o esgotamento dos recursos computacionais com exceções do tipo *MemoryError*.

Para contornar essa restrição operacional, implementou-se uma rotina de fragmentação baseada na biblioteca *pandas*. O algoritmo realiza o processamento em lotes discretos parametrizados com dimensão uniforme de $N = 500.000$ linhas. Simultaneamente, aplicou-se um filtro de projeção precoce com o argumento `usecols`, descartando já na etapa de leitura atributos redundantes ou sem relevância analítica (tais como `version` e `block_id`). Com vistas a otimizar as taxas de Entrada e Saída (E/S) e dispensar o desempacotamento intermediário em disco, utilizou-se o módulo nativo `glob` em associação ao argumento `compression=gzip` dos métodos de leitura do *pandas*, processando os fluxos binários diretamente da memória.

A gestão do consumo de memória é assegurada pela invocação explícita do coletor de lixo da linguagem Python via módulo nativo `gc` (*Garbage Collector*). A cada lote computado, os identificadores locais são desalocados mediante a instrução `del`, sucedida pela execução da rotina `gc.collect()`, garantindo que o perfil de ocupação da memória

```

===== Transações =====
Total de registros carregados: 12,858,509

Resumo das colunas:
<class 'pandas.core.frame.DataFrame'>
RangeIndex: 12858509 entries, 0 to 12858508
Data columns (total 20 columns):
#   Column                Dtype
---  -
0   hash                  object
1   time                  object
2   size                  int64
3   weight                int64
4   lock_time             int64
5   is_coinbase           int64
6   has_witness           int64
7   input_count           int64
8   output_count          int64
9   input_total           int64
10  input_total_usd        float64
11  output_total           int64
12  output_total_usd       float64
13  fee                    int64
14  fee_usd                float64
15  fee_per_kb             float64
16  fee_per_kb_usd         float64
17  fee_per_kwu            float64
18  fee_per_kwu_usd        float64
19  cdd_total              float64
dtypes: float64(8), int64(10), object(2)
memory usage: 1.9+ GB
None

```

Figura 4 – Resumo da Estrutura das Transações

```

===== ENTRADAS =====
Total de registros carregados: 28,819,847

Resumo das colunas:
<class 'pandas.core.frame.DataFrame'>
RangeIndex: 28819847 entries, 0 to 28819846
Data columns (total 7 columns):
#   Column          Dtype
---  -
0   transaction_hash object
1   time            object
2   value_usd       float64
3   recipient       object
4   is_from_coinbase int64
5   lifespan        int64
6   cdd             float64
dtypes: float64(2), int64(2), object(3)
memory usage: 1.5+ GB
None

```

Figura 5 – Resumo da Estrutura das Entradas

```

===== Saidas =====
Total de registros carregados: 31,650,565

Resumo das colunas:
<class 'pandas.core.frame.DataFrame'>
RangeIndex: 31650565 entries, 0 to 31650564
Data columns (total 8 columns):
#   Column          Dtype
---  -
0   transaction_hash object
1   time            object
2   value           int64
3   value_usd       float64
4   recipient       object
5   type            object
6   is_from_coinbase int64
7   is_spendable    int64
dtypes: float64(1), int64(3), object(4)
memory usage: 1.9+ GB
None

```

Figura 6 – Resumo da Estrutura das Saídas

===== BABD-13 RESUMO CLASSIFICADOS =====	
Tipo	Quantidade
3 - centralized exchange	300000
6 - gambling	105257
1 - cyber-security service	91617
2 - darknet market	13861
11 - tumbler	12412
5 - P2P financial service	9309
0 - blackmail	8686
10 - mining pool	1580
12 - individual wallet	1502
4 - P2P financial infrastructure service	180
7 - government criminal blacklist	27
8 - money laundering	16
9 - Ponzi scheme	15

Figura 7 – Resumo Tipos BABD-13

RAM permaneça estável e linear ao longo de todo o ciclo de execução, independentemente da escala dos arquivos em disco.

O fluxo de preparação, transformação e enriquecimento dos dados estruturou-se em quatro etapas sequenciais:

1. **Unificação e filtragem inicial:** consolidação sistemática dos arquivos diários de mesma natureza extraídos da plataforma Blockchair (gerando tabelas unificadas de transações, entradas e saídas), com descarte de campos irrelevantes e persistência intermediária em matrizes no formato Valores Separados por Vírgula (CSV); simultaneamente, realizou-se a higienização do *dataset* BABD-13, preservando unicamente os registros de endereços e gerando a variável dependente binária `malicious` com valores 0 (benigno) e 1 (malicioso), mapeada a partir do atributo original `labels` mediante a atribuição de valor positivo às classes 0, 2, 7, 8, 9 e 11, e negativo às demais;
2. **Junção relacional de entradas e saídas:** em virtude da segregação canônica do modelo UTXO entre origens e destinos de valor, cada registro de entrada e de saída foi vinculado deterministicamente ao identificador de sua transação correspondente;
3. **Rotulação posicional dos endereços:** execução de uma junção à esquerda (*left join*) entre as tabelas de fluxo operacional e a base de referência BABD-13. Aos endereços ausentes no conjunto de dados atribuiu-se o rótulo nulo (0), adotando-se o pressuposto normativo de ausência de vínculo ilícito conhecido — critério operacional que introduz ruído e viés residual à distribuição amostral;

4. **Estruturação e engenharia transacional:** sumarização dos metadados no nível da transação. Variáveis lógicas booleanas (`is_coinbase` e `has_witness`) foram convertidas em valores binários discretos $\{0, 1\}$. O registro cronológico textual (`time`) foi mapeado na escala contínua de carimbo de data/hora (*Unix timestamp*, em segundos decorridos desde 1º de janeiro de 1970) para viabilizar o particionamento pelas árvores; por fim, consolidou-se a regra de contaminação transacional estrita: caso ao menos uma entrada ou saída de determinada operação estivesse rotulada como maliciosa, a transação integral recebia a classificação maliciosa (1).

4.3 Indução e Inferência do Modelo Preditivo através do Algoritmo de Floresta Randômica

A modelagem preditiva supervisionada foi formulada no nível transacional. O conjunto de dados consolidado foi particionado de maneira pseudoaleatória e reproduzível na proporção canônica de 80% para o subconjunto de treinamento e 20% para o subconjunto de teste, alinhando-se aos padrões consolidados na literatura de aprendizado de máquina forense. Tendo em vista que a rede Bitcoin exhibe acentuada assimetria entre o volume de liquidações legítimas e a incidência de transações ilícitas, empregou-se a amostragem estratificada via parâmetro `stratify=y`, preservando a razão probabilística entre classes em ambas as partições.

A indução do modelo baseou-se na instanciação da classe `RandomForestClassifier`, estruturada com um comitê de 100 árvores de decisão independentes sob o algoritmo de Floresta Randômica. Com o intuito de mitigar o desbalanceamento intrínseco das classes sem recorrer a intervenções sintéticas de sobreamostragem (como o Técnica de Sobreamostragem Sintética de Minoria (SMOTE)) — as quais poderiam descaracterizar a topologia real dos dados forenses —, habilitou-se o parâmetro `class_weight=balanced`. Esse ajuste recalibra internamente a função de perda das árvores, ponderando os pesos de forma inversamente proporcional às frequências de classe e penalizando com maior rigor erros de classificação cometidos sobre instâncias maliciosas.

A etapa computacional foi acelerada mediante o argumento `n_jobs=-1`, instruindo a biblioteca *scikit-learn* a paralelizar o processo de ajuste das árvores em todas as unidades de processamento lógico disponíveis na Unidade Central de Processamento (CPU). Na fase de inferência, cada árvore de decisão formula um voto discreto para a natureza da transação (0 para instâncias benignas e 1 para maliciosas), cabendo ao comitê global da Floresta Randômica consolidar a predição final por maioria simples de votos.

```
1 import pandas as pd
2 import numpy as np
3 import matplotlib.pyplot as plt
4 import seaborn as sns
```

```
5 import joblib
6 from sklearn.model_selection import train_test_split
7 from sklearn.ensemble import RandomForestClassifier
8 from sklearn.metrics import classification_report, confusion_matrix
9 from sklearn.impute import SimpleImputer
10
11 def treinar_e_avaliar_modelo(arquivo_features, arquivo_labels):
12     # =====
13     #1. PREPARACAO DOS DADOS (X e y)
14     # =====
15     print("Carregando e cruzando os datasets")
16     df_features = pd.read_csv(arquivo_features, encoding='utf-8')
17     df_labels = pd.read_csv(arquivo_labels, encoding='utf-8')
18
19     if 'transaction_hash' in df_labels.columns:
20         df_labels.rename(columns={'transaction_hash': 'hash'}, inplace=
True)
21
22     df_final = pd.merge(df_features, df_labels[['hash', 'malicious']],
on='hash', how='left')
23     df_final['malicious'] = df_final['malicious'].fillna(0).astype(int)
24
25     # Separar variaveis (X) e alvo (y)
26     X = df_final.drop(columns=['hash', 'malicious', 'weight', 'size'])
27     # 'hash' e so um identificador, 'malicious' e o alvo, 'weight' e '
size' podem ser redundantes
28     y = df_final['malicious']
29
30     # Guardar os nomes das colunas para usar no grafico mais tarde
31     nomes_das_features = X.columns
32
33     # Preencher dados nulos com 0
34     imputer = SimpleImputer(strategy='constant', fill_value=0)
35     X_limpo = imputer.fit_transform(X)
36
37     # Dividir em Treino (80%) e Teste (20%) com estratificacao
38     print("Dividindo os dados em conjuntos de Treino e Teste")
39     X_train, X_test, y_train, y_test = train_test_split(
40         X_limpo, y, test_size=0.2, random_state=42, stratify=y
41     )
42
43     # =====
44     # 2. TREINAMENTO DO RANDOM FOREST
45     # =====
46     print("\nTreinando o Random Forest")
47     # class_weight='balanced' e fundamental para forçar o modelo a
prestar
```

```
47     # atencao na minoria maliciosa, penalizando mais os erros nessa
48     classe.
49     modelo_rf = RandomForestClassifier(
50         n_estimators=100,
51         random_state=42,
52         class_weight='balanced',
53         n_jobs=-1
54     )
55     modelo_rf.fit(X_train, y_train)
56
57     # =====
58     # 3. AVALIACAO DO MODELO
59     # =====
60     print("Realizando previsoes no conjunto de teste")
61     y_pred = modelo_rf.predict(X_test)
62
63     print("===== RELATORIO DE CLASSIFICACAO =====")
64     print(classification_report(y_test, y_pred))
65
66     # =====
67     # 4. SALVANDO O MODELO TREINADO
68     # =====
69     salvar_modelo(modelo_rf, imputer)
70
71     # =====
72     # 5. VISUALIZACOES (Graficos)
73     # =====
74     sns.set_theme(style="whitegrid")
75
76     # Grafico 1: Matriz de Confusao
77     plt.figure(figsize=(8, 6))
78     cm = confusion_matrix(y_test, y_pred)
79     sns.heatmap(cm, annot=True, fmt='d', cmap='Blues', cbar=False,
80                 xticklabels=['Benigno (0)', 'Malicioso (1)'],
81                 yticklabels=['Benigno (0)', 'Malicioso (1)'])
82     plt.title('Matriz de Confusao do Modelo')
83     plt.ylabel('Classe Real')
84     plt.xlabel('Previsao do Modelo')
85     plt.tight_layout()
86     plt.savefig('matriz_confusao.png', dpi=300)
87     print("-> Grafico da Matriz de Confusao salvo como 'matriz_confusao.
88     png'")
89
90     # Grafico 2: Importancia das Variaveis (Feature Importance)
91     plt.figure(figsize=(12, 8))
```

```

91     importancias = modelo_rf.feature_importances_
92
93     # Cria um DataFrame temporario para ordenar as variaveis da mais
importante para a menos importante
94     df_importancias = pd.DataFrame({
95         'Feature': nomes_das_features,
96         'Importancia': importancias
97     }).sort_values(by='Importancia', ascending=False)
98
99     # Plota o grafico de barras
100     sns.barplot(x='Importancia', y='Feature', data=df_importancias,
palette='viridis')
101     plt.title('Importancia das Variaveis (Random Forest)', fontsize=16)
102     plt.xlabel('Peso da Variavel no Modelo', fontsize=12)
103     plt.ylabel('Feature', fontsize=12)
104     plt.tight_layout()
105     plt.savefig('feature_importance.png', dpi=300)
106     print("-> Grafico de Feature Importance salvo como '
feature_importance.png")
107
108     plt.show() # Exibe os graficos na tela
109
110     return modelo_rf
111
112
113 def salvar_modelo(modelo_rf, imputer):
114     # =====
115     # SALVANDO OS ARQUIVOS
116     # =====
117     print("Salvando o modelo e o imputer no disco")
118
119     # Salva o algoritmo treinado
120     joblib.dump(modelo_rf, 'classificador_darknet_rf.joblib')
121
122     # Salva o tratador de dados ausentes
123     joblib.dump(imputer, 'tratador_dados_ausentes.joblib')
124
125     print("-> Arquivos 'classificador_darknet_rf.joblib' e '
tratador_dados_ausentes.joblib' gerados com sucesso!")
126
127     return modelo_rf
128
129
130 if __name__ == "__main__":
131     arquivo_features_gerado = 'Features_Transacoes.csv'
132     arquivo_labels_gerado = 'Classified_transactions.csv'
133

```

134

```
modelo_treinado = treinar_e_avaliar_modelo(arquivo_features_gerado ,  
arquivo_labels_gerado)
```

Listing 4.1 – Treinamento e inferência do classificador de Floresta Randômica.

4.4 Propagação de Rótulos por Heurística de Contaminação e Consolidação por Votação por Endereço

Como transações individuais podem conter ruídos comportamentais que induzem o modelo de aprendizado de máquina a erros pontuais de predição — gerando falsos positivos ou falsos negativos no nível transacional —, desenvolveu-se uma arquitetura de consolidação agregada no nível de endereços.

Inicialmente, aplica-se a heurística de contaminação baseada em grafos: todas as inferências geradas na etapa precedente pela Floresta Randômica para as transações são mapeadas de forma reversa, propagando os rótulos preditos para todos os endereços criptográficos que atuaram diretamente como entradas (*inputs*) ou saídas (*outputs*) de cada operação analisada.

Em seguida, executa-se o algoritmo de votação majoritária. O sistema consolida o histórico completo de ocorrências de um determinado endereço A_i e quantifica a sua Razão de Contaminação (Razão de Contaminação (RC)), computada por meio da Equação 3. Por fim, estabelece-se a regra de decisão final parametrizada por um limiar fixo de corte por maioria absoluta com $\theta = 0,5$, conforme formalizado na Equação 4 — valor adotado com suporte em avaliações empíricas prévias, por apresentar equilíbrio consistente entre a taxa de acertos e o controle de falsos positivos e falsos negativos.

Essa abordagem fundamenta-se no princípio de que, embora um agente malicioso possa realizar operações esparsas com atributos indistinguíveis dos usuários legítimos, o histórico agregado de suas interações tende a revelar seu perfil anômalo, viabilizando que o mecanismo de votação atenuie os desvios estatísticos intrínsecos ao classificador de base.

Resultados

Os resultados obtidos pelo modelo supervisionado baseado em Floresta Randômica para o nível transacional evidenciam a importância relativa das variáveis na discriminação dos fluxos, conforme ilustrado na Figura 8. Observa-se que métricas econômicas atreladas às taxas de rede e aos volumes financeiros transacionados exercem papel preponderante na capacidade decisória do estimador. O peso substancial atribuído às taxas cobradas por unidade de peso (*fee_per_kwu*) e por *kilobyte* (*fee_per_kb*) reflete um padrão comportamental recorrente de agentes que atuam em mercados clandestinos ou em rotinas de dissimulação patrimonial. Tais entidades — a exemplo de administradores de mercados negros ou operadores de serviços de mistura (*mixers*) — operam sob constante urgência temporal. A necessidade de viabilizar a liquidação tempestiva dos fundos ilícitos, com vistas a mitigar o rastreamento analítico por empresas periciais ou a apreensão de ativos por órgãos reguladores, induz esses atores ao pagamento de taxas de priorização significativamente superiores à média praticada pelos usuários convencionais da rede.

O treinamento e a validação preliminar do modelo de Floresta Randômica concentraram-se no nível das transações individuais registradas na *blockchain*. Após processar e classificar o conjunto de transações da partição de teste, o estimador gerou a matriz de confusão correspondente, que mapeia a distribuição de acertos e erros inferenciais em confronto com os rótulos de referência da base BABD-13.

Com base nas frequências registradas na matriz de confusão transacional, exibida na Figura 9, calcularam-se as métricas de validação sintetizadas na Tabela 2, permitindo mensurar a capacidade preditiva global do modelo supervisionado. Do total de 2.571.702 registros avaliados na partição de teste, o classificador identificou corretamente 2.544.196 transações benignas (verdadeiros negativos) e rotulou erroneamente apenas 1.568 operações ordinárias como suspeitas (falsos positivos). No tocante à classe minoritária, o modelo detectou com êxito 17.542 transações ilícitas (verdadeiros positivos), mas classificou 8.396 eventos maliciosos como legítimos (falsos negativos). Essa configuração reflete elevada precisão, atingindo média macro de 96% e precisão específica de 92% para a classe maliciosa; contudo, a revocação (*recall*) moderada de 68% para a classe ilícita (com média

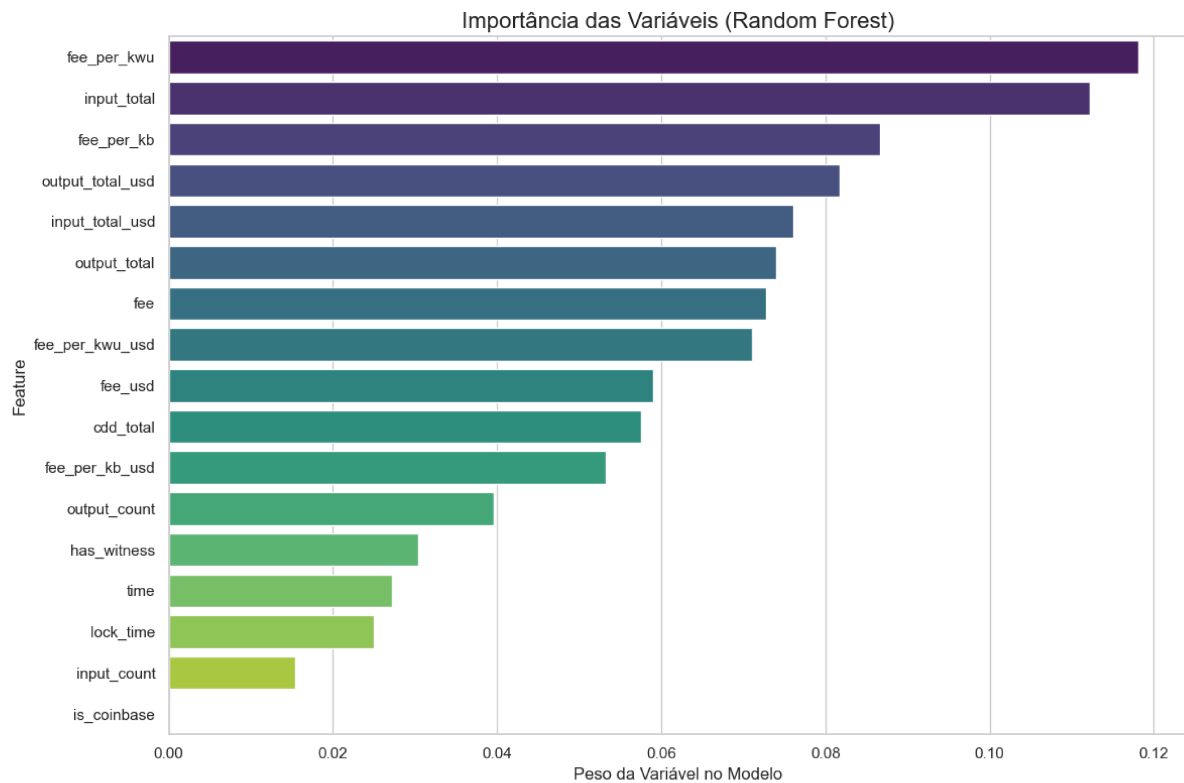


Figura 8 – Peso das Variáveis no Modelo

Classe	Precisão	Recall	F1-score	Suporte
Benigno (0)	1.00	1.00	1.00	2 545 764
Malicioso (1)	0.92	0.68	0.78	25 938
Acurácia			1.00	2 571 702
Média Macro	0.96	0.84	0.89	2 571 702
Média Ponderada	1.00	1.00	1.00	2 571 702

Tabela 2 – Relatório de Classificação

macro de 84%) evidencia o impacto da incidência de falsos negativos induzidos por ruídos comportamentais em transações isoladas. Não obstante, a obtenção de um *F1-Score* macro de 89% (e de 78% para a classe ilícita) demonstra que o modelo induzido pela Floresta Randômica apresenta expressiva capacidade discriminativa para reconhecer padrões anômalos no tráfego da *blockchain*, fornecendo uma triagem preliminar consistente para a etapa subsequente de votação por entidade.

Como se observa na matriz de confusão apresentada na Figura 10, a integração do classificador de Floresta Randômica ao mecanismo de votação majoritária consolidada por entidade mostrou-se altamente eficaz na identificação de atores maliciosos no nível da rede. Do universo de 91.921 endereços únicos avaliados, o sistema classificou corretamente 88.258 endereços legítimos (verdadeiros negativos) e identificou com exatidão a totalidade dos 2.833 endereços ilícitos (verdadeiros positivos). O método não produziu nenhum

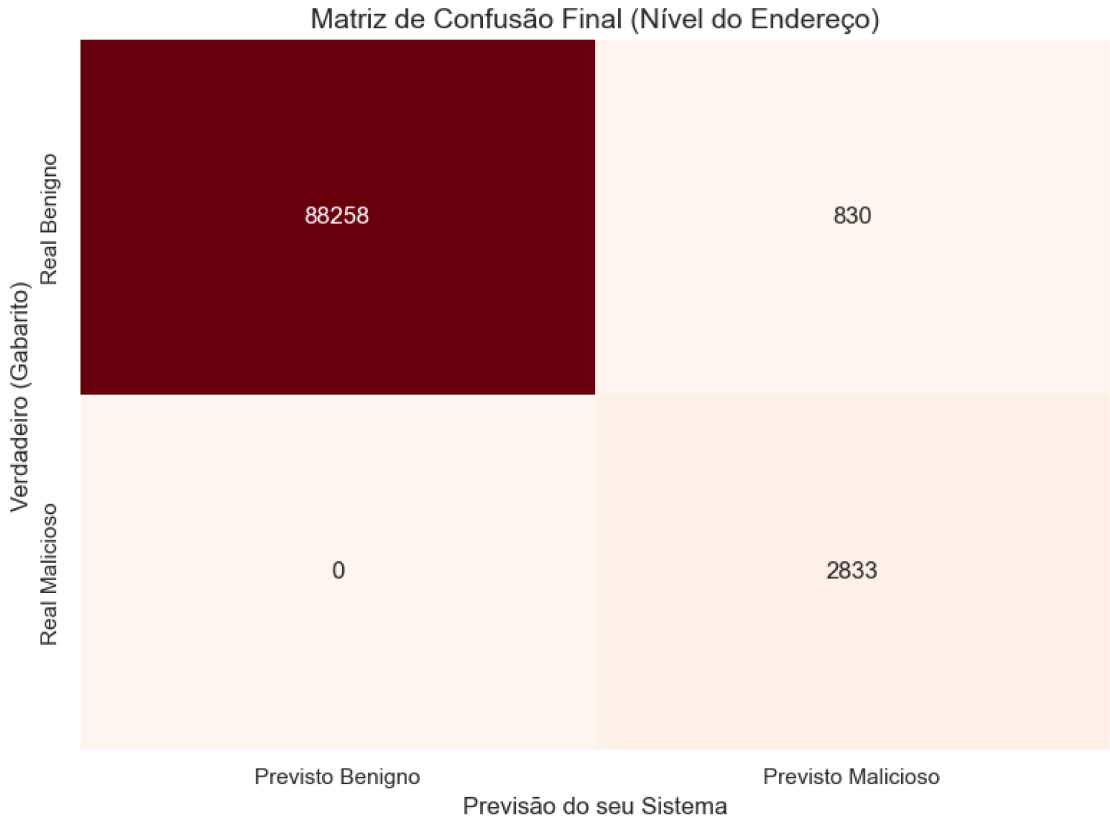


Figura 9 – Matriz de Confusão do Modelo(Transações)

falso negativo ($FN = 0$), registrando apenas 830 falsos positivos — isto é, instâncias benignas que ultrapassaram o limiar de contaminação estipulado. Esse comportamento inverte o padrão observado na etapa transacional isolada, na qual a maior parcela de erros concentrava-se na omissão de operações ilícitas (falsos negativos).

A partir das frequências consolidadas na matriz de confusão, computaram-se as métricas de validação apresentadas na Tabela 3. O modelo supervisionado com mecanismo de votação alcançou acurácia global de 99%, com média ponderada de 99% para precisão, revocação (*recall*) e *F1-Score*. Para a classe minoritária maliciosa, o sistema obteve revocação de 100% (1,00) e *F1-Score* de 87% (0,87), com precisão de 77% (0,77) em decorrência da incidência de falsos positivos. Na média macro, os índices mantiveram-se expressivos, com precisão de 89%, revocação de 100% e *F1-Score* de 93%. Esse perfil de distribuição de erros mostra-se altamente vantajoso para aplicações de inteligência forense e conformidade regulatória (*compliance*), cenários nos quais a garantia de interceptação total dos agentes ilícitos mitiga riscos operacionais severos, justificando o custo de auditar uma margem controlada de falsos alarmes.

Figura 10 – Matriz de confusão no nível de endereço



Classe	Precisão	Recall	F1-score	Suporte
Benigno (0)	1.00	0.99	1.00	89 088
Malicioso (1)	0.77	1.00	0.87	2 833
Acurácia			0.99	91 921
Média Macro	0.89	1.00	0.93	91 921
Média Ponderada	0.99	0.99	0.99	91 921

Tabela 3 – Relatório de Classificação(Endereços)

Conclusão

A partir dos resultados obtidos, conclui-se que a pesquisa cumpriu satisfatoriamente o objetivo de desenvolver e avaliar um arcabouço computacional capaz de classificar transações e mitigar o pseudoanonimato na rede Bitcoin para a identificação automatizada de usuários maliciosos. Por meio da implementação do algoritmo de Floresta Randômica associado a uma heurística subsequente de votação majoritária por endereço, estabeleceu-se uma metodologia robusta e escalável para a análise pericial forense em ambientes de *blockchain*.

Os resultados experimentais corroboram a literatura de referência e expandem a compreensão sobre a dinâmica operacional de agentes ilícitos em redes distribuídas. A análise de importância de atributos revelou que as variáveis econômicas exercem papel preponderante na capacidade discriminativa do classificador de base. Indicadores atrelados aos custos de processamento por unidade de peso (*fee_per_kwu*) e por *kilobyte* (*fee_per_kb*), somados aos volumes agregados transacionados em dólares (*input_total_usd* e *output_total_usd*), consolidaram-se como os preditores mais determinantes. Sob o prisma estatístico, esse comportamento valida a premissa de que operadores de mercados clandestinos, esquemas Ponzi e mecanismos de ofuscação operam sob constante urgência temporal na liquidação de fundos — visando atenuar riscos de rastreamento ou apreensão de ativos —, sujeitando-se ao pagamento de taxas de mineração substancialmente superiores à média da rede.

No nível transacional, o classificador baseado em Floresta Randômica apresentou elevada precisão geral, registrando média macro de 96% de acerto e *F1-Score* macro de 89%. Não obstante, a avaliação individualizada das operações evidenciou uma revocação moderada de 84% na média macro (com 68% na identificação da classe ilícita), demonstrando que a sensibilidade inicial do modelo sofre o impacto de ruídos gerados por transações isoladas de atores maliciosos que mimetizam padrões de transferências legítimas (falsos negativos).

A principal contribuição metodológica deste estudo reside na formulação da rotina de pós-processamento com agregação por entidade. Ao propagar de maneira reversa as infe-

rências transacionais para a estrutura de grafos e aplicar a função de decisão sob limiar de maioria absoluta ($\theta = 0,5$), o mecanismo atenuou os desvios estatísticos do estimador base. No nível de endereços, o modelo alcançou uma revocação de 100% (com a interceptação integral dos 2.833 endereços ilícitos avaliados), atingindo acurácia global de 99% e *F1-Score* ponderado de 99%. Embora a abordagem tenha gerado uma margem controlada de 830 falsos positivos — o que resultou em precisão de 77% para a classe minoritária —, tal distribuição de erro mostra-se amplamente aceitável e vantajosa em cenários periciais e em rotinas preventivas de conformidade financeira (*compliance*), nos quais a omissão de uma entidade criminosa acarreta prejuízos operacionais expressivamente mais graves do que a auditoria manual de falsos alarmes.

No que tange às limitações, destaca-se o enquadramento do problema sob uma classificação binária, premissa adotada para a viabilização empírica do fluxo inicial, o que suprime distinções funcionais entre as tipologias de ilícitos. Para investigações futuras, propõe-se:

1. A expansão da modelagem para uma abordagem multiclasse, contemplando as 13 categorias originais catalogadas na base BABD-13 (discriminando especificamente entre *ransomware*, esquemas Ponzi, mercados clandestinos e outros crimes cibernéticos);
2. O aprofundamento da engenharia de atributos com a extração dinâmica de métricas topológicas de grafos complexos em tempo de execução, a exemplo das centralidades de intermediação e de proximidade;
3. A realização de estudos comparativos entre o classificador de Floresta Randômica e arquiteturas de redes neurais em grafos (*Graph Neural Networks* – Redes Neurais para Grafos (GNN)), com o objetivo de elevar a precisão métrica na camada de endereços e refinar o controle sobre os falsos positivos.

Referências

- AnalystPrep. **Supervised Machine Learning, Unsupervised Machine Learning, and Deep Learning (CFA Level II Study Notes)**. 2021. <<https://analystprep.com/study-notes/cfa-level-2/quantitative-method/supervised-machine-learning-unsupervised-machine-learning-deep-learning/>>. Acesso em: 14 de junho de 2026. Citado 2 vezes nas páginas 4 e 31.
- ANTONOPOULOS, A. M. **Mastering Bitcoin: Programming the Open Blockchain**. 2. ed. Sebastopol: O'Reilly Media, 2017. ISBN 9781491954386. Citado 3 vezes nas páginas 11, 16 e 19.
- Arkham Intelligence. **UTXO Explained: Bitcoin's Most Underrated Innovation**. 2024. <<https://info.arkm.com/research/utxo-explained-bitcoins-most-underrated-innovation>>. Acesso em: 3 de julho de 2026. Citado 2 vezes nas páginas 4 e 18.
- BUTERIN, V. **Ethereum: A Next-Generation Smart Contract and Decentralized Application Platform**. 2014. <https://ethereum.org/content/whitepaper/whitepaper-pdf/Ethereum_Whitepaper_-_Buterin_2014.pdf>. [Online; accessed 15-march-2024]. Citado na página 15.
- Cloudflare. **O que é o ransomware WannaCry?** 2026. <<https://www.cloudflare.com/pt-br/learning/security/ransomware/wannacry-ransomware/>>. Acesso em: 30 de maio de 2026. Citado na página 21.
- CNN Brasil. **Ataque hacker: R\$ 541 milhões foram transformados em criptomoeda, diz PF**. 2026. <<https://www.cnnbrasil.com.br/nacional/centro-oeste/df/ataque-hacker-r-541-milhoes-foram-transformados-em-criptomoeda-diz-pf/>>. Acesso em: 30 de maio de 2026. Citado na página 21.
- DIFRANCESCO, R. M.; MEENA, P.; KUMAR, G. How blockchain technology improves sustainable supply chain processes: a practical guide. **Operations Management Research**, Springer, v. 16, p. 620–641, 6 2023. ISSN 19369743. Citado na página 16.
- FEKADU, R. et al. Machine learning models evaluation and feature importance analysis on npl dataset. 8 2022. Disponível em: <<http://arxiv.org/abs/2209.09638>>. Citado na página 30.
- HABER, S.; STORNETTA, W. S. **How To Time-Stamp a Digital Document I**. 1991. 99-111 p. Citado na página 15.

- HIRAMOTO, N.; TSUCHIYA, Y. Measuring dark web marketplaces via Bitcoin transactions: From birth to independence. **Forensic Science International: Digital Investigation**, v. 35, p. 301086, dez. 2020. ISSN 2666-2817. Disponível em: <<https://www.sciencedirect.com/science/article/pii/S2666281720303887>>. Citado 3 vezes nas páginas 22, 23 e 34.
- HURWITZ, J.; KIRSCH, D. **Machine Learning For Dummies**. Hoboken: John Wiley & Sons, 2018. ISBN 9781119454953. Disponível em: <<https://dn721906.ca.archive.org/0/items/introduction-to-machine-learning/Introduction%20to%20Machine%20Learning.pdf>>. Citado na página 29.
- KANEMURA, K.; TOYODA, K.; OHTSUKI, T. Identification of darknet markets' bitcoin addresses by voting per-address classification results. In: **2019 IEEE International Conference on Blockchain and Cryptocurrency (ICBC)**. Shanghai: IEEE, 2019. p. 154–158. Citado 6 vezes nas páginas 22, 24, 25, 29, 32 e 35.
- MONAMO, P. M.; MARIVATE, V.; TWALA, B. A multifaceted approach to bitcoin fraud detection: Global and local outliers. In: **2016 15th IEEE International Conference on Machine Learning and Applications (ICMLA)**. Anaheim: IEEE, 2016. v. 1, n. 1, p. 188–194. Citado na página 12.
- MÜLLER, A. C.; GUIDO, S. **Introduction to Machine Learning with Python: A Guide for Data Scientists**. Sebastopol: O'Reilly Media, 2016. ISBN 9781449369415. Citado na página 29.
- NAKAMOTO, S. **Bitcoin: A Peer-to-Peer Electronic Cash System**. 2008. <<https://assets.pubpub.org/d8wct41f/31611263538139.pdf>>. [Online; accessed 24-Fevereiro-2024]. Citado 2 vezes nas páginas 11 e 15.
- NERURKAR, P. et al. Supervised learning model for identifying illegal activities in bitcoin. **Applied Intelligence**, v. 51, p. 1–20, 06 2021. Citado 5 vezes nas páginas 4, 17, 21, 30 e 35.
- PHAM, T.; LEE, S. Anomaly detection in bitcoin network using unsupervised learning methods. 11 2016. Disponível em: <<http://arxiv.org/abs/1611.03941>>. Citado na página 12.
- RODRIGUES, C. A. de Q.; SANTOS, S. L. O. dos. **Forensic Investigation Techniques In Blockchain And Cryptocurrencies: A Literature Review For Application In Criminal Investigations**. São Paulo, 2026. v. 10, n. 1, 1–15 p. Citado na página 24.
- SVENDA, P. et al. Coinjoin ecosystem insights for wasabi 1.x, wasabi 2.x and whirlpool coordinator-based privacy mixers. **Proceedings on Privacy Enhancing Technologies**, Privacy Enhancing Technologies Symposium Advisory Board, v. 2026, p. 557–592, 4 2026. Citado na página 27.
- UNSUPERVISED learning for robust Bitcoin fraud detection. In: 2016 Information Security for South Africa (ISSA). Johannesburg: IEEE, 2016. p. 129–134. Citado na página 12.

WalletExplorer. **WalletExplorer: Smart Bitcoin block explorer – Info**. 2026. <<https://www.walletexplorer.com/info>>. Acesso em: 31 de julho de 2026. Citado na página 28.

XIANG, Y. et al. Babd: A bitcoin address behavior dataset for pattern analysis. **IEEE Transactions on Information Forensics and Security**, v. 19, p. 2171–2185, 2024. Citado 4 vezes nas páginas 13, 29, 33 e 38.