Detecção de Fraudes em Criptomoedas utilizando Métodos de Classificação de Séries Temporais baseados em Redes Neurais

Luiz Alfredo Zenon da Mata Caffé[1], **Rogério Zupo Braga**[2], **Lourenço Alves Pereira Júnior**[2], **Cecilia de Azevedo Castro Cesar**[2], **Cesar Augusto Cavalheiro Marcondes**[2]

[1]Marinha do Brasil

[2]Departamento de Sistemas de Computação
Instituto Tecnológico de Aeronáutica – São Paulo, SP – Brasil

{luiz.caffe,rogerio.braga}@ga.ita.br,

{lourenco.junior,cecilia.cesar,cesar.marcondes}@gp.ita.br

Abstract. *This article addresses the challenge of detecting fraud in cryptocurrencies that originate from an Initial Coin Offering (ICO), which accounts for an estimated 78% of fraudulent activity in the cryptocurrency market. By developing five normalized time series based on the transaction tables of collected cryptocurrencies and analyzing the behavior of fraudulent and non-fraudulent cryptocurrencies, this study employs three types of Artificial Neural Networks (Multilayer Perceptron, Convolution Neural Network-Multilayer Perceptron, and Long Short Term Memory-Multilayer Perceptron) for classification. The results show that the proposed method achieves a Recall of 91% for time samples of 20 days after the cryptocurrency is launched on the market.*

Resumo. *Este artigo apresenta um método baseado em modelos preditivos de redes neurais para detecção de fraudes em criptomoedas provenientes de Initial Coin Offering (ICO). Através da análise de Séries Temporais geradas a partir de tabelas de fluxo de transações na rede Ethereum, foram desenvolvidas 5 séries temporais normalizadas que serviram como entrada para os modelos de Redes Neurais Artificiais (RNA) MLP, CNN-MLP e LSTM-MLP projetados para classificação. Dado que 78% das atividades de ICO são fraudulentas, este método é um importante passo em direção à prevenção de fraudes em criptomoedas. Os resultados obtidos na pesquisa foram bastante satisfatórios, com um valor de Recall de até 91% em alguns casos.*

1. Introdução

A tecnologia Blockchain permite a criação de novas formas de financiamento coletivo e a criação das chamadas moedas digitais [Casino et al. 2018]. Com o Blockchain, os nós da rede compartilham a responsabilidade pela validação das transações inseridas, sem a necessidade de uma entidade central confiável para validá-las [Ulrich 2017]. Além do livro-razão público, contratos inteligentes são executados de forma independente e descentralizada, de acordo com uma lógica de intermediação [Szabo 1997]. Assim, ela alavanca uma nova classe de aplicativos que podem melhorar drasticamente a oferta de serviços essenciais.

Essa descentralização permite que *startups* levantem capital para seus projetos rapidamente. O caminho normal para um novo empreendedor é buscar um investidor-anjo ou um empréstimo bancário e depois investimentos mais substanciais em aceleradoras e vendas de ações. Nesse caminho, a empresa não é oferecida ao público em geral. As criptomoedas podem contribuir para esse cenário, pois são acessíveis a qualquer pessoa, independentemente de seu perfil de investimento, classe social e até mesmo legislação do país. *Initial Coin Offering* (ICO) torna possível realizar o equivalente a uma *Initial Public Offering* (IPO). As atividades de ICO começaram em 2013 e atingiram o pico na primeira metade de 2018, impulsionadas pelo aumento das criptomoedas, com movimentação entre 7 e 12 bilhões de dólares americanos em todo o mundo [Chod and Lyandres 2019].

À medida que os investimentos se tornaram mais populares e fáceis de serem realizados, o número de usuários inexperientes e, consequentemente, o potencial de fraude aumentaram. O investidor inexperiente pode alocar seus recursos para várias atividades de ICO sem critérios claros, pensando que uma delas pode aumentar de valor muitas vezes, proporcionalmente ao que foi investido inicialmente. Segundo a Satis Group, em julho de 2018, 78% de todas as ICO's eram fraudulentas. Portanto, encontrar uma solução que resolva ou reduza as atividades fraudulentas é uma questão importante nessa área.

Este artigo apresenta um método para detectar fraudes em criptomoedas, originado da *Initial Coin Offering* (ICO). O método de pesquisa construiu vários modelos preditivos usando redes neurais para classificar séries temporais geradas a partir das tabelas de fluxo de transações e da rede Blockchain Ethereum. Além disso, uma revisão bibliográfica preliminar foi realizada para contextualizar o problema e revelar técnicas de ponta na detecção de fraudes em criptomoedas. As contribuições deste trabalho são (1) Análise Exploratória de Dados das bases de dados de transações de criptomoedas coletadas; (2) Avaliação comparativa entre o desempenho de modelos de classificação baseados em Redes Neurais Artificiais (RNA's) e (3) Aplicação de séries temporais para detectar fraudes nessa área. Entre os resultados obtidos, destacamos a análise de 238 conjuntos de dados de ICO's de criptomoedas, dos quais 136 eram fraudulentos e 102 eram não fraudulentos.

Todos os modelos de classificação de séries temporais foram capazes de detectar fraudes em criptomoedas, alcançando um desempenho de 91% no parâmetro *Recall* para amostras coletadas 20 dias após o lançamento da criptomoeda no mercado. Tal desempenho indica superioridade em relação aos estudos encontrados na literatura para o mesmo parâmetro de *Recall*, que são de 81% [Chen et al. 2018] e 69% [Chen et al. 2019]. O restante do artigo está organizado da seguinte forma: A Seção 2 consiste em uma revisão bibliográfica preliminar, enquanto a Seção 3 aborda a metodologia de pesquisa. A Seção 4 apresenta os principais resultados e as conclusões estão na Seção 5.

2. Trabalhos Relacionados

O processo de revisão bibliográfica preliminar foi realizado com base nas diretrizes de Petersen [Petersen et al. 2015]. Foi realizada uma busca extensa com os termos "*criptomoeda*", "*fraude*"e "*oferta inicial de moeda*", apresentando um total de 1330 artigos. Além disso, uma busca com os termos "*criptomoeda*", "*fraude*"e "*rede neural*"indicou 654 artigos. Restringimos a pesquisa àqueles que propuseram soluções por meio de aprendizado de máquina.

Artigos que destacam os aspectos econômicos do tópico incluem Milne [Milne 2018], Bellavitis et al. [Bellavitis et al. 2021], Campino et al. [Campino et al. 2022], Belitski et al. [Belitski and Boreiko 2021] e Thies et al. [Thies et al. 2021]. Esses autores fornecem uma visão holística do mercado de ICO's, enfatizando as peculiaridades desse mercado, as vantagens lucrativas para investidores, a tecnologia blockchain e a descentralização do sistema financeiro.

Kher et al. [Kher et al. 2020], Bellavitis [Bellavitis et al. 2021], Adhami et al. [Adhami et al. 2018] e Belitski [Belitski and Boreiko 2021] apresentaram teorias, metodologias e aspectos regulatórios relacionados ao desenvolvimento da indústria, cibersegurança em blockchain e ICO's e condições de sucesso para arrecadação de fundos. Esses autores também apontaram características recomendadas para as ICO's, como a disponibilidade de código-fonte e o direito de acesso a serviços e lucros, que permitem aumentar a arrecadação de fundos e reduzir a assimetria de informações relacionadas ao investimento em ICO's.

Em relação a aspectos práticos e exploratórios, Hartmann et al. [Hartmann et al. 2018] estudaram as características de uma atividade ICO que sites de avaliação levam em conta para fornecer maior segurança aos investidores, enquanto Campino et al. [Campino et al. 2022] destacaram a importância de um *whitepaper* bem estruturado e informativo, bem como a importância de estar próximo a determinados mercados com alta disponibilidade de capital financeiro e humano como fatores determinantes para o sucesso de uma ICO. Por outro lado, Thies et al. [Thies et al. 2021] identificaram que a mera existência de múltiplas contas de mídia social em diferentes plataformas não é um sinal de qualidade credível e, portanto, não contribui automaticamente para o sucesso de uma ICO.

Oliva et al. [Oliva et al. 2020] realizaram uma análise exploratória dos contratos inteligentes presentes na rede Ethereum, a fim de ter uma compreensão ampla de todos os contratos implementados lá. As seguintes ferramentas foram usadas por eles e posteriormente por nós: Google BigQuery[1], Etherscan[2], State of the DApps[3] e CoinMarketCap[4]. Uma das descobertas deste artigo é que apenas 0,05% dos contratos inteligentes são responsáveis por 80% de todas as transações que são enviadas aos contratos, o que significa que as transações circulando no Ethereum estão concentradas em uma porção muito pequena de contratos. O estudo indicou que 94,7% dos contratos receberam menos de dez transações. No entanto, os autores não consideraram uma evolução de série temporal para quantificar e detectar a incidência de fraudes. Da mesma forma, Kiffer et al. [Kiffer et al. 2018] destacaram que o ecossistema de contratos inteligentes do Ethereum tem uma considerável falta de diversidade e que a maioria dos contratos reutiliza extensivamente o código.

Chen et al. [Chen et al. 2018] desenvolveram um método baseado em *machine learning* para detectar esquemas Ponzi na rede Ethereum. Eles descobriram que a distribuição de Ether entre investidores é desigual na maioria dos contratos fraudulentos e que o parâmetro GASLIMIT é um fator importante na diferenciação de contratos

[1]https://console.cloud.google.com/bigquery
[2]https://etherscan.io/
[3]http://www.stateofthedapps.com/
[4]https://coinmarketcap.com/

fraudulentos e não fraudulentos. Jung E. et al. [Jung et al. 2019] usaram algoritmos de classificação semelhantes e obtiveram alta precisão na detecção de esquemas Ponzi. Mais tarde, Chen et al. [Chen et al. 2019] realizaram um novo estudo abrangente de contratos de esquemas Ponzi e usaram o método *random forest* (RF) para detectar esquemas Ponzi em contratos inteligentes com maior precisão do que outros métodos de *machine learning*. Um total de 3.780 códigos-fonte de contrato e suas respectivas tabelas de transação foram analisados, e foi obtida uma precisão (*recall*) de 69%. O artigo estimou que cerca de 500 contratos inteligentes Ponzi estão presentes na rede Ethereum.

Fan et al. [Fan et al. 2021] propuseram um método *Anti-leakage Smart Ponzi Schemes Detection in Blockchain* (Al-SPSD), para detectar esquemas Ponzi em redes blockchain, que superou métodos concorrentes com pontuação F1 de 96%. Lei W. et al. [Wang et al. 2021] também propuseram uma abordagem PSD-OL (*Ponzi Scheme Detection via Oversampling-based Long Short-Term Memory for smart contracts*), baseada em LSTM (*Long Short-Time Memory*) com *oversampling*, que também atingiu uma pontuação F1 de 96%. Bartoletti et al. [Bartoletti et al. 2020] estudaram o comportamento na Blockchain Ethereum e detectaram *bugs* intencionais nos códigos-fonte dos contratos, fazendo recomendações para evitar essa fraude.

O estudo de Chen W. et al. [Chen et al. 2021], apontou limitações nas abordagens existentes de detecção de esquemas Ponzi em contratos inteligentes Ethereum, que utilizam aprendizado de máquina baseado em *opcodes* ou padrões de transação de endereço. Tais limitações incluem a necessidade de um grande número de transações para aprendizado de comportamento e falta de interpretabilidade na detecção baseada na distribuição de frequência de *opcodes*. Além disso, essas abordagens são propensas a técnicas de evasão, o que pode resultar em falsos positivos ou falsos negativos. Como solução, os autores propuseram uma nova abordagem de detecção semântica, chamada SADPonzi, que usa aprendizado de máquina para identificar esquemas Ponzi em contratos inteligentes Ethereum com precisão e escalabilidade.

Em outro estudo, Jiahua Xu e Livshits [Xu and Livshits 2019] apresentaram uma análise detalhada de esquemas "*Pump and Dump*"em criptomoedas e demonstraram que é possível prever com cerca de 90% de precisão quais criptomoedas são visadas por esse tipo de fraude. Kamps e Kleinberg [Kamps and Kleinberg 2018] também utilizaram dados públicos de transação para detectar fraudes de manipulação de preços "*Pump and Dump*"em criptomoedas.

Jason Brownlee desenvolveu um método de classificação de séries temporais usando Redes Neurais Artificiais (RNA) [Brownlee 2018], que se mostraram mais eficazes do que outros algoritmos de aprendizado de máquina, como Naive Bayes, KNN e Random Forest, na classificação de séries temporais. O estudo de Brownlee baseou-se em artigos que abordam técnicas de reconhecimento de atividade humana.

Esses estudos demonstram a eficácia de soluções baseadas em técnicas de aprendizado de máquina e aprendizado profundo para melhorar a segurança da rede Ethereum e detectar fraudes em criptomoedas. Eles também apoiaram a coleta de criptomoedas e a montagem de séries temporais em nosso método de detecção de fraudes em criptomoedas.

3. Método de Detecção de Fraude

O principal objetivo deste trabalho é detectar fraudes em criptomoedas originárias de atividades de ICO na rede Ethereum, por meio do desenvolvimento de modelos de classificação baseados em RNA. Para atingir o objetivo, desenvolvemos um método baseado em cinco etapas, conforme ilustrado na Figura 1. As etapas são:

- Elaboração de Hipóteses de Pesquisa;
- Coleta de Criptomoedas Fraudulentas e Não Fraudulentas;
- Análise Exploratória de Dados;
- Montagem de Séries Temporais;
- Montagem de Modelos de Classificação Baseados em Redes Neurais Artificiais - RNA.

As fraudes no mundo real inspiraram as hipóteses de pesquisa. Com base nessas hipóteses, os dados foram organizados no formato de séries temporais, extraídas do fluxo público de transações de cada criptomoeda selecionada. A saída do classificador é um valor booleano (fraudulento ou não fraudulento) usado no treinamento e teste. Detalharemos cada uma dessas etapas abaixo.

Figura 1. Método de Detecção de Fraude

3.1. Hipóteses de Pesquisa

Com base na literatura apresentada, desenvolvemos 5 hipóteses sobre a importância de certos fatores para a identificação de fraudes. Essas hipóteses podem desempenhar um papel decisivo ao orientar os usuários a investir em uma nova criptomoeda específica.

Hipótese 1: NEWHOLDER. Em esquemas fraudulentos, o momento em que a atividade irregular é descoberta é importante porque o número de transações diminui drasticamente, permanecendo relativamente constante ao longo do tempo. Com base nessa observação, nossa primeira hipótese é que o influxo de novos participantes ao longo do tempo é relevante para a detecção de fraudes.

Hipótese 2: NEWUSER. Há um grande volume de transações feitas por usuários recém-criados em esquemas de Pump and Dumps. O objetivo é dar a impressão de que a criptomoeda teve uma grande aceitação porque vários usuários estão comprando. Em vez disso, em esquemas não fraudulentos, o fluxo de transações de novos usuários tem uma distribuição mais uniforme ao longo do tempo. Assim, a segunda hipótese é que o fluxo de transações de novos usuários na rede Ethereum ao longo do tempo é um fator relevante para a detecção de fraudes.

Hipótese 3: BIGHOLDER. Se um usuário possui uma quantidade relativamente grande de ativos, há uma alta possibilidade de que ele seja o proprietário da empresa por trás da criptomoeda e, portanto, quem tomará todas as decisões centralmente. Assim, o valor acumulado que o maior detentor de ativos de criptomoeda tem ao longo do tempo é relevante para a detecção de fraudes.

Hipótese 4: GAS/GASLIMIT. O atributo GAS é uma taxa de transação associada à execução, e GASLIMIT é um valor definido pelos mineradores. Comumente, usuários mal-intencionados geram um volume maior de transações do que usuários não mal-intencionados, aumentando o custo. Assim, os atributos das taxas de transação Ethereum, GAS e GASLIMIT, ao longo do tempo, são fatores relevantes para detectar Esquemas Ponzi.

Hipótese 5: MARKETDATE. Esquemas fraudulentos comumente apresentam uma redução acentuada no número de transações quando a fraude é descoberta. Portanto, quanto menor o período para as transações continuarem, menos provável é detectar fraudes. Assim, é importante realizar estudos em diferentes intervalos de tempo, como 20 dias ou mais.

3.2. Coleção de Criptomoedas

Milhares de criptomoedas são criadas todos os meses, então coletar as criptomoedas mais relevantes para análise não é uma atividade trivial. Inicialmente, os critérios relevantes selecionados foram:

- Token da rede Ethereum;
- Tempo mínimo no mercado de 6 meses, registrando a data em que atingiu 400 transações;
- Pelo menos 1500 transações.

Com base nos critérios acima, foram selecionados 238 conjuntos de dados de ICO de criptomoedas. Após essa seleção inicial, iniciamos a segunda etapa de seleção e filtragem. Novos critérios foram definidos e uma forte validação manual foi realizada para especificar quais das criptomoedas poderiam ser consideradas fraudulentas ou não fraudulentas com segurança. Os critérios para a seleção de criptomoedas não fraudulentas foram:

- Estar no ranking de criptomoedas entre as 400 primeiras. Para essa seleção, foi utilizada a plataforma Coingecko[5], que por sua vez indica as criptomoedas consolidadas no mercado e que, portanto, têm menor risco de fraude;
- Estar na lista de atividades de ICO disponíveis. Para essa seleção, foi utilizada a plataforma Icodrops[6];
- Não ter notícias sobre fraudes na pesquisa da plataforma Google com as palavras-chave: "*ICO*"+ "*scam*" + "*nome da criptomoeda*".

Após a aplicação desses critérios, 102 ICO foram considerados não fraudulentos, 42% do total. Os critérios para a seleção de criptomoedas fraudulentas foram:

- Estar na lista de atividades fraudulentas de ICO em um maior número de sites investigativos: coincurb, dead coins, isthiscoinascam e coinsopsy;
- Ter pelo menos um tópico sobre fraudes no fórum bitcointalk;
- Não ter um site disponível ou ter redes sociais desatualizadas ou inexistentes.

Após esse filtro, começou a terceira etapa: aquisição dos bancos de dados de transações da rede Ethereum. Foi utilizado o aplicativo Etherscan, que contém os detalhes de uma transação com subsequente seleção dos campos relevantes para o estudo. A Tabela 1 resume os campos escolhidos para processamento.

[5]https:// www.coingecko.com
[6]https://icodrops.com/ico-stats/

Tabela 1. Campos das Bases de Dados das Transações de criptomoedas

Campo	Descrição
Timestamp	Data e Hora
From Address	Endereço hash do usuário origem da transação
To Address	Endereço hash do usuário destinatário da transação
Transaction Value	Valor da transação, na criptomoeda ETHER
Transaction Address	Endereço hash da transação
Transaction Nonce	Contador de Nonce
Tkn Src Address	Endereço hash do usuário origem da transação de token
Tkn Dst Address	Endereço hash do usuário destinatário da transação de token
Gas Limit	Valor limite de GAS selecionado pelo minerador do bloco
Gas	Taxa da transação usado pelo minerador do bloco

3.3. Análise Exploratória de Dados

Esta atividade tem como objetivo melhorar as hipóteses elaboradas a partir dos dados provenientes das tabelas de transações. As análises apresentadas abaixo permitiram obter conhecimento para a montagem das séries temporais.

Análise 1: A diferença entre a entrada no mercado e a primeira transação é pequena em criptomoedas não fraudulentas, com uma mediana de menos de dez dias, em comparação com uma mediana de mais de 30 dias e uma variabilidade muito maior no caso fraudulento.

Análise 2: Em criptomoedas fraudulentas, os maiores detentores de títulos frequentemente não têm ligações com contratos ou exchanges (69% contas de usuários). Já em criptomoedas legítimas, principais detentores estão em exchanges, impulsionando o valor, ou em smart contracts que facilitam ICOs (70%), conforme Figura 2.

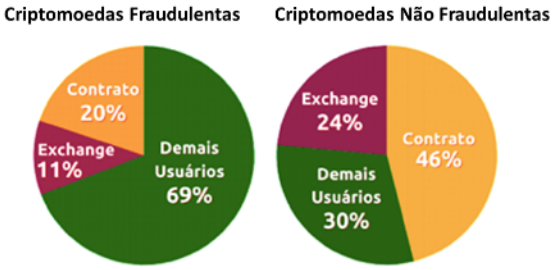


Figura 2. Tipo de conta do maior detentor de títulos

Análise 3: Foi analisado o tempo entre duas transações consecutivas. Ambas as categorias mostraram uma grande frequência de dispersão entre as transações.

Análise 4: O montante total de transações para cada criptomoeda é uma medida importante, uma vez que há uma queda repentina no fluxo de transações no momento em que a fraude é descoberta. O boxplot na Figura 2a mostra a diferença entre os dois casos. Cada ponto representa uma criptomoeda nesta figura, e o boxplot apresenta um resumo estatístico. Note que as criptomoedas não fraudulentas têm muitas mais transações do que as fraudulentas.

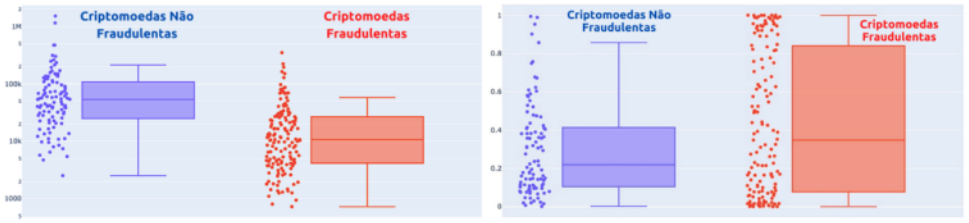
Análise 5: Esta análise investiga o papel das taxas de transação na detecção de fraudes. As criptomoedas não fraudulentas têm o parâmetro GASLIMIT com uma média mais alta

do que as fraudulentas. No caso de GAS, é o oposto.

Análise 6: Criptomoedas fraudulentas têm menos endereços distintos (From Address), porque, sendo controladas por *bots*, reutilizam o mesmo endereço. Por esta razão, calculamos a média de transações únicas de vendedores por total de transações para cada conjunto de dados. As criptomoedas não fraudulentas têm mais vendedores de tokens diversos e fraudulentas têm vendedores repetidos.

Análise 7: Em esquemas de pump and dump, compradores automáticos maliciosos compram títulos para gerar um fluxo de transações, dando uma falsa impressão de que a criptomoeda está sendo bem aceita no mercado. Assim, a média de transações de um único comprador em criptomoedas fraudulentas é maior do que em não fraudulentas.

Análise 8: Criptomoedas fraudulentas tendem a ter uma quantidade relativamente maior de novos usuários na rede Ethereum. Isso ocorre porque pessoas ou *bots* criam contas para realizar atividades fraudulentas. Portanto, calculamos a média de transações de novos usuários de criptomoedas em relação ao total de transações. A figura 2b ilustra essa diferença.



(a) Quantidade total de transações em seis meses de criptomoedas fraudulentas e não fraudulentas – Análise 4

(b) Média de novos usuários em seis meses de criptomoedas fraudulentas e não fraudulentas – Análise 8

Figura 3. Análise exploratória de dados. Ilustra as diferenças entre moedas fraudulentas e não fraudulentas

3.4. Montagem de Séries Temporais

Com as hipóteses de pesquisa levantadas e a análise exploratória dos dados, iniciamos o quarto passo do nosso método: o processo de montagem das séries temporais.

Série Temporal 1. Foi criada uma série temporal chamada NEWHOLDER para verificar a hipótese NEWHOLDER descrita na Seção 3.1. A Equação 1 relaciona o número de novos detentores ao longo do tempo.

$$y = \frac{\textit{número de participantes atual}}{\textit{número total de participantes}} \tag{1}$$

Assim, essa série tem seus valores crescentes e acumulados entre ”0”e ”1”, sendo que o último número sempre terá valor igual a ”1”. A Figura 3 mostra todos os conjuntos de dados usando essa métrica NEWHOLDER. Os dados para criptomoedas não fraudulentas são mostrados em azul e as fraudulentas em vermelho. As linhas mais fortes expressam as médias aritméticas. Cada série temporal possui janelas de 20, 40 e 60 dias para seguir a hipótese MARKETDATE, que estabelece que a janela de tempo entre a data de entrada da criptomoeda no mercado e a data de sua análise é um fator relevante para a detecção de fraudes.

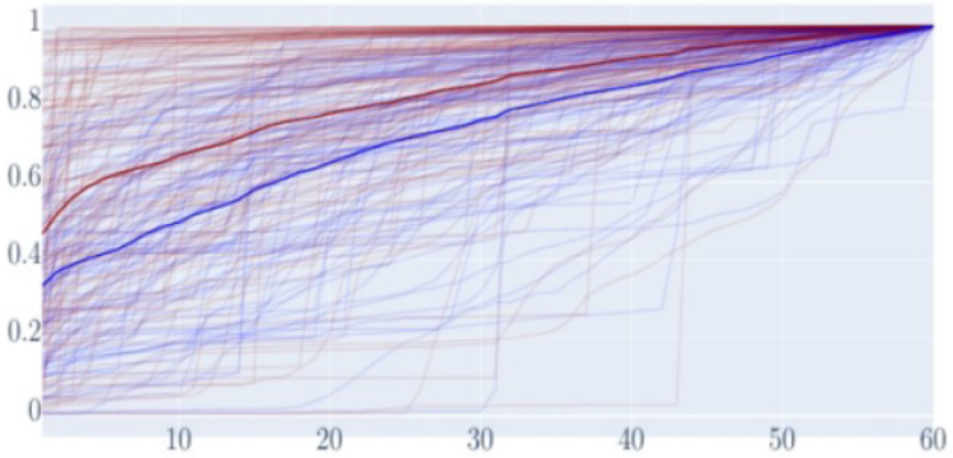


Figura 4. Série temporal 1 com a porcentagem de transações de usuários recém-criados, ao longo de 60 dias. Os dados para criptomoedas não fraudulentas são mostrados em azul e as fraudulentas em vermelho. As linhas mais fortes representam as médias aritméticas

Série Temporal 2. A segunda série está relacionada à quantidade de transações de usuários "recém-criados- NEWUSER. A Equação 2 apresenta o número diário de transações por novos participantes. As criptomoedas fraudulentas têm uma média mais alta do que as não fraudulentas.

$$y = \frac{\textit{número diário de transações de novos participantes}}{\textit{número diário de transações}} \tag{2}$$

Série Temporal 3. A hipótese é que os títulos em criptomoedas fraudulentas permanecem nas mãos do fraudador, que por sua vez, quer atingir o preço máximo e depois vender todos os seus ativos. A série BIGBUYER segue a Equação 3:

$$y = \frac{\textit{saldo do maior comprador de títulos}}{\textit{total de títulos circulante}} \tag{3}$$

Para calcular o maior comprador de títulos e o número total de títulos, foi desenvolvida uma função "*balance*"que rastreia quantos tokens um endereço possui ao longo do tempo. As criptomoedas fraudulentas têm uma fração maior de usuários com ampla propriedade, como mostrado na Figura 4.

Série Temporal 4. O ambiente de taxas de transação medida por GAS pode ser manipulado para obter fraudes ao menor custo possível. O valor de referência é a razão entre GAS, que é um dado instantâneo, e GASLIMIT, o teto máximo de GAS (Equação 4).

$$y = \frac{\textit{total de GAS no dia}}{\textit{total de GASLIMIT no dia}} \tag{4}$$

No caso de fraude, as médias desse valor são mais baixas do que no caso não fraudulento.

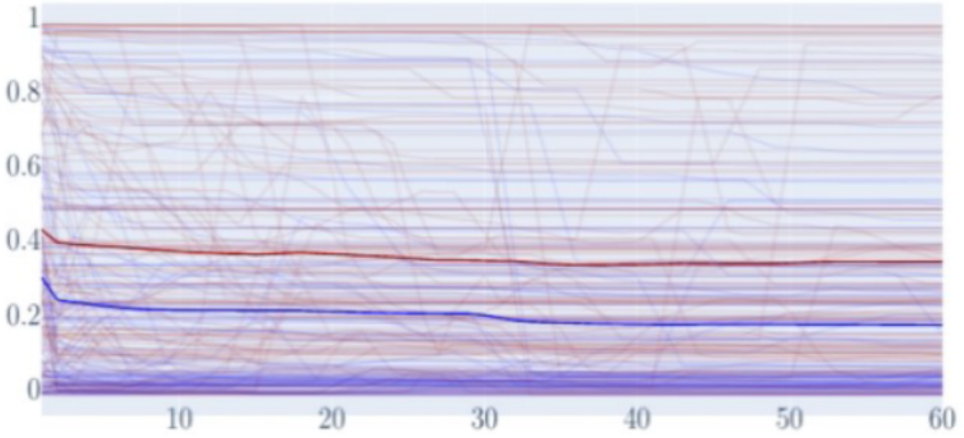


Figura 5. Série temporal 3 com a porcentagem de títulos que cada maior comprador de títulos possui. Os dados para criptomoedas não fraudulentas são mostrados em azul e as fraudulentas em vermelho. As linhas mais fortes representam as médias aritméticas

3.5. Montagem de Modelos de Classificação de Redes Neurais Artificiais - RNA

No último passo do Método de Detecção de Fraude, o modelo de classificação é uma RNA composta por uma ou mais arquiteturas destinadas a classificar os dados de entrada. Neste caso, os dados de entrada representam as séries temporais em arquivos de texto, e a saída representa o desempenho do modelo na classificação das séries. A métrica usada para análise de desempenho foi o *Recall*, definido como o número de verdadeiros (fraudulentos) positivos em comparação com o número total de transações fraudulentas. Essa é uma medida importante na detecção de fraudes porque um *Recall* maior é inversamente proporcional à perda financeira.

Em relação ao número de épocas, uma quantidade foi escolhida que pudesse combinar otimização de tempo com o alcance de desempenho máximo possível, sabendo que a RNA não melhora o índice de *Recall* ou entra em *overfitting* a partir de certo ponto. Portanto, o número de 100 épocas foi escolhido para os modelos MLP e CNN-MLP e 400 épocas para o modelo LSTM-MLP. Observamos que, neste último, devido ao componente de memória longa, mais épocas eram necessárias para que o modelo alcançasse um desempenho mais alto sem *overfitting*. Por fim, o tamanho do lote 128 foi escolhido como o principal. No entanto, houve séries com *Recall* estabilizado ao longo das épocas. Portanto, os tamanhos 128, 64, 32 e 16 foram usados em ordem de preferência. Três modelos de RNA foram projetados: MLP (Perceptron Multicamadas), CNN-MLP (Rede Neural Convolucional - Perceptron Multicamadas) e LSTM-MLP (Memória Curta a Longo Prazo - Perceptron Multicamadas).

Todos os experimentos foram realizados em um computador Intel de 64 bits com oito núcleos e 64GB de RAM, com disco SSD e 2 cartões GPU NVidia 1080i (3000 núcleos). A suíte de desenvolvimento foi o Jupyter notebook, versão 6.0.3, instalado no Python, versão 3.7.3, com bibliotecas TensorFlow, Keras, pandas e NumPy. Foram desenvolvidos nove cadernos do Jupyter, cada um referente a uma janela de tempo (dados de 20 dias, 40 dias e 60 dias), combinados com os três modelos de RNA abordados neste estudo. No total, foram realizados 36 experimentos, resultando em uma combinação de

quatro séries temporais, três janelas de tempo e três modelos de RNA.

4. Resultados do Modelo de RNA

Nesta seção, há uma análise comparativa dos resultados para verificar qual variável (série temporal, janela de tempo e modelo RNA) é melhor para a detecção de fraudes.

4.1. Comparação das Séries Temporais

A figura 5 compara, por meio de um mapa de calor, o valor da métrica *Recall* para cada uma das séries temporais desenvolvidas e as RNA's. Analisando esta figura, os resultados são observados:

- NEWHOLDER: Alcançou mais de 80% de desempenho em 7 dos 9 testes. O modelo LSTM-MLP se destaca, com 91% em 40 dias após a data de entrada da criptomoeda no mercado.
- NEWUSER: Alcançou mais de 80% de desempenho em 8 dos 9 testes. O modelo LSTM-MLP se destaca, com 91% em 20 dias após a entrada da criptomoeda no mercado.
- BIGBUYER: Alcançou mais de 80% de desempenho em 7 dos 9 testes. O modelo MLP se destaca, com 88% em até 60 dias após a entrada da criptomoeda no mercado.
- GAS/GASLIMIT: Alcançou mais de 80% de desempenho em 5 dos 9 testes. Os modelos MLP e CNN-MLP se destacam, com 88% em 60 dias após a entrada da criptomoeda no mercado. O modelo LSTM-MLP não consegue treinar esses conjuntos de dados devido à constante *overfitting* detectado.

ANN/ Series	NEWHOLDER			NEWUSER			BIGBUYER			GAS/GASLIMIT		
	20	40	60	20	40	60	20	40	60	20	40	60
MLP	83%	76%	86%	83%	86%	88%	86%	86%	88%	84%	81%	88%
CNN-MLP	86%	82%	81%	83%	88%	90%	86%	86%	79%	75%	81%	88%
LSTM-MLP	83%	91%	77%	91%	88%	75%	80%	83%	75%	-	-	-

Figura 6. Análise comparativa das métricas de *Recall* por tipo de série.

4.2. Comparação de Janelas de Tempo

Foi feita uma comparação entre os tamanhos das janelas de tempo (20, 40 e 60 dias) para verificar a melhor janela. Pode-se observar que, em geral, há um pequeno aumento no desempenho quando o tamanho da amostra de tempo é aumentado, exceto para o modelo LSTM-MLP, que apresentou uma queda repentina no desempenho durante o treinamento com a série de 60 dias. Estudamos a razão para esse resultado com o LSTM-MLP analisando a matriz de confusão e descobrimos que o desempenho diminuiu durante a série de 60 dias devido a valores atípicos, enquanto obtinha excelentes resultados para 20 e 40 dias.

4.3. Comparação de Modelos RNA

A Tabela 2 descreve a média aritmética dos desempenhos dos três modelos RNA apresentados neste estudo, considerando todas as séries temporais e janelas de tempo. Novamente, os três modelos alcançaram médias semelhantes. Uma análise de nossos resultados por RNA indicou que:

- MLP: O modelo MLP mostrou-se mais uniforme em termos de números. Satisfatório para o reconhecimento de padrões em séries temporais. Em geral, o desempenho aumentou à medida que a janela de tempo foi aumentada.
- CNN-MLP: um rendimento semelhante ao MLP. O modelo CNN-MLP mostrou menos uniformidade, mas obteve resultados expressivos (88% e 90%) em certas condições. Embora o modelo de convolução tenha sido projetado para o reconhecimento de imagens, ele mostrou ser capaz de aplicar o reconhecimento de padrões em séries temporais. O MLP não mostrou um padrão de desempenho uniforme em relação às janelas de tempo abrangidas. Apesar disso, manteve seu desempenho semelhante ao anterior.
- LSTM-MLP: Mostrou um ótimo desempenho para as séries de 20 e 40 dias. Embora tenha sido projetado para armazenar memória ao longo do tempo, não apresentou bons resultados para o reconhecimento de padrões quando aplicado à série mais longa coberta, de 60 dias, como explicado na subseção anterior. O modelo LSTM-MLP mostrou ser a melhor opção neste estudo para reconhecer as séries de curto prazo.

Tabela 2. Tipo de modelo e média aritmética de desempenho

Modelo RNA	MLP	CNN-MLP	LSTM-MLP
Média Aritmética de *Recall*	82.93%	82.87%	82.33%

5. Conclusões

Este trabalho desenvolveu um método para detectar fraudes em criptomoedas baseado na rede Ethereum e resultante de atividades de ICO. A natureza das transações em sequência, ao longo do tempo, e o preço das ações no mercado financeiro justificaram o uso de ferramentas de previsão de séries temporais. Os modelos criados para detecção de fraudes foram desenvolvidos usando o estado da arte em termos de redes neurais para classificar séries temporais. Foram criadas quatro séries temporais (NEWHOLDER, NEWUSER, BIGBUYER e GASGASLIMIT) com base na revisão da literatura submetida a três modelos de RNA projetados para classificação. O trabalho detectou fraudes em esquemas *Pump and Dump* e Ponzi. Ao longo do trabalho, foi realizado um estudo de Análise Exploratória de Dados, que ajudou a selecionar as características mais relevantes das séries. Foram extraídas informações importantes, como a diferença entre a data da primeira transação de criptomoedas e a data de sua entrada no mercado, o tipo de conta (contrato, casa de câmbio ou outros tipos) do maior detentor de segurança e a média de transações de novos usuários criados na rede Ethereum. Foram analisados 238 conjuntos de dados de criptomoedas, 136 fraudulentos e 102 não fraudulentos. Os resultados indicaram a detecção de fraudes em ICO's, atingindo a métrica de *Recall* de 91% para amostras de tempo de 20 dias após o lançamento da criptomoeda no mercado. Na literatura, havia sido relatado um valor de *Recall* de apenas 81%.

Nossas principais descobertas incluem (i) a série com melhor desempenho foi NEWUSER, com base no trabalho de [6]; (ii) a série BIGBUYER indicou que a descentralização das reservas de ativos é um indicador da ausência de esquemas fraudulentos; (iii) a janela de tempo de 40 dias foi, em média, aquela com melhor desempenho; (iv) o modelo MLP apresentou o melhor desempenho na média geral, mas o modelo LSTM-MLP apresentou o melhor resultado individual, exceto para a janela de 60 dias.

Como trabalhos futuros, planejamos explorar o uso de modelos híbridos, como CNN-LSTM-MLP ou CONV-LSTM. É importante esclarecer que o método de detecção de fraude apresentado analisou conjuntos de dados de transações de ICO's que já haviam ocorrido na rede blockchain Ethereum, e não em tempo real, imediatamente após o lançamento das ICO's. Este trabalho pode ser considerado um passo inicial em direção à capacidade de detectar fraudes em ICO's antes que ocorram. Como próximos passos, esperamos ampliar o escopo deste método para outros tipos de criptoativos, como *Non Fungible Tokens* (NFT's) e *Initial DEX Offerings* (IDO's). Além disso, uma automação em tempo real para verificação de transações de tokens, utilizando as classificações baseadas em Redes Neurais Artificiais apresentadas neste método, é desejável para alertar antecipadamente os negociantes de criptoativos sobre possíveis perdas financeiras em transações que exibam comportamentos suspeitos, com base nas hipóteses pesquisadas.

Disponibilidade dos Dados

Os códigos de montagem de séries temporais, modelos de RNA, aquisição de banco de dados, bem como a tabela que contém as informações das criptomoedas coletadas estão disponíveis no repositório público do Github em:

https://github.com/luizzmata/ICOFraudDetection

Referências

Adhami, S., Giudici, G., and Martinazzi, S. (2018). Why do businesses go crypto? an empirical analysis of initial coin offerings. *Journal of Economics and Business*, 100:64–75.

Bartoletti, M., Carta, S., Cimoli, T., and Saia, R. (2020). Dissecting ponzi schemes on ethereum: identification, analysis, and impact. *Future Generation Computer Systems*, 102:259–277.

Belitski, M. and Boreiko, D. (2021). Success factors of initial coin offerings. *J Technol Transf*.

Bellavitis, C., Fisch, C., and Wiklund, J. (2021). A comprehensive review of the global development of initial coin offerings (icos) and their regulation. *Journal of Business Venturing Insights*, 15:e00213.

Brownlee, J. (2018). *Deep Learning for Time Series Forecasting: Predict the Future with MLPs, CNNs and LSTMs in Python*. Machine Learning Mastery.

Campino, J., Brochado, A., and Rosa, A. (2022). Initial coin offerings (icos): Why do they succeed? *Financ Innov*, 8:17.

Casino, F., Dasaklis, T. K., and Patsakis, C. (2018). A systematic literature review of blockchain-based applications: current status, classification and open issues. *Telematics and Informatics*, 35(8):2337–2357.

Chen, W., Li, X., Sun, Y., Huang, N., Wang, H., Wu, L., and Liu, X. (2021). Sadponzi: Detecting and characterizing ponzi schemes in ethereum smart contracts. *Proc. ACM Meas. Anal. Comput. Syst.*, 5(2):26.

Chen, W., Zheng, Z., Cui, J., Ngai, E., Zheng, P., and Zhou, Y. (2018). Detecting ponzi schemes on ethereum: Towards healthier blockchain technology. In *Proceedings of the 2018 World Wide Web Conference*, pages 1409–1418. ACM.

Chen, W., Zheng, Z., Ngai, E., Zheng, P., and Zhou, Y. (2019). Exploiting blockchain data to detect smart ponzi schemes on ethereum. *IEEE Access*, 7:37575–37586.

Chod, J. and Lyandres, E. (2019). A theory of icos: Diversification, agency, and information asymmetry. *Agency, and Information Asymmetry*.

Fan, S., Fu, S., Xu, H., and Cheng, X. (2021). Al-spsd: Anti-leakage smart ponzi schemes detection in blockchain. *Information Processing & Management*, 58(4):102587.

Hartmann, F., Wang, S., and Lunesu, M. (2018). Evaluation of initial cryptoasset offerings: The state of the practice. In *2018 International Workshop on Blockchain Oriented Software Engineering (IWBOSE)*, pages 33–39. IEEE.

Jung, E., Le Tilly, M., Gehani, A., and Ge, Y. (2019). Data mining-based ethereum fraud detection. In *2019 IEEE International Conference on Blockchain (Blockchain)*, pages 266–273. IEEE.

Kamps, J. and Kleinberg, B. (2018). To the moon: defining and detecting cryptocurrency pump-and-dumps. *Crime Science*, 7(1):18.

Kher, R., Terjesen, S., and Liu, C. (2020). Blockchain, bitcoin, and icos: a review and research agenda. *Small Business Economics*, pages 1–22.

Kiffer, L., Levin, D., and Mislove, A. (2018). Analyzing ethereum's contract topology. In *Proceedings of the Internet Measurement Conference 2018*, pages 494–499. ACM.

Milne, A. (2018). Cryptocurrencies from an austrian perspective. In *Banking and Monetary Policy from the Perspective of Austrian Economics*, pages 223–257. Springer.

Oliva, G. A., Hassan, A. E., and Jiang, Z. M. (2020). An exploratory study of smart contracts in the ethereum blockchain platform. *Empirical Software Engineering*, pages 1–41.

Petersen, K., Vakkalanka, S., and Kuzniarz, L. (2015). Guidelines for conducting systematic mapping studies in software engineering: An update. *Information and Software Technology*, 64:1–18.

Szabo, N. (1997). Formalizing and securing relationships on public networks. *First Monday*.

Thies, F., Wallbach, S., Wessel, M., and Benlian, A. (2021). Initial coin offerings and the cryptocurrency hype - the moderating role of exogenous and endogenous signals. *Electron Markets*.

Ulrich, F. (2017). *Bitcoin: a moeda na era digital*. LVM Editora, S.l.

Wang, L., Cheng, H., Zibin, Z., Aijun, Y., and Xiaohu, Z. (2021). Ponzi scheme detection via oversampling-based long short-term memory for smart contracts. *Knowledge-Based Systems*, 228:107312.

Xu, J. and Livshits, B. (2019). The anatomy of a cryptocurrency pump-and-dump scheme. In *28th USENIX Security Symposium (USENIX Security 19)*, pages 1609–1625.