PonziShield:
A Multimodal Real-time System for Detecting Ponzi DApps

190175X - Nimsara Fernando

190369V - Chamod Madhusanka

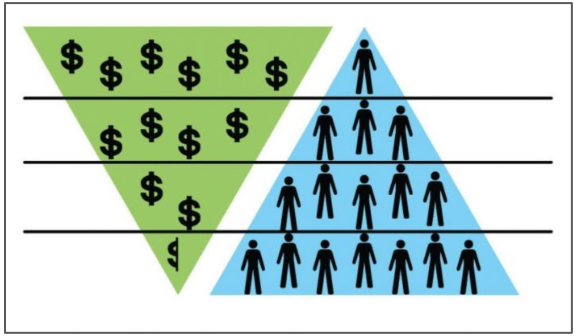
190420V - Sandun Induwara

Internal Supervisor - Dr. Sandareka Wickramanayake

External Supervisor - Dr. Dilum Bandara

BACKGROUND

- Decentralized Applications (DApps) operate on blockchains
- Deterministic, immutable, and transparent
- Ponzi schemes are fraudulent investment schemes that promise high returns to initial investors but rely on capital of new investors to pay off earlier one



MOTIVATION

- DApps have gained rapid popularity due to the industry's adoption, harnessing their decentralized nature.
- Many fraudulent DApps, such as Ponzi schemes and phishing scams.
- In 2019, scammers stole $4.3 billion from millions of victims, and 92% of it came from Ponzi schemes [1].
- The existing solutions provide a method for classifying Ponzi DApps but do not identify them in real-time as they transact.

[1] S. Fan, S. Fu, H. Xu, and X. Cheng, "AI-SPSD: Anti-leakage smart Ponzi schemes detection in blockchain," Information Processing & Management, vol. 58, no. 4, pp. 102587, 2021.

PROBLEM STATEMENT

How to recognize a Ponzi DApp in real time as it transacts, based on its smart contract, transactions, and social media sentiment?

OBJECTIVES

- Detect ongoing Ponzi schemes in DApps in real-time as it transacts.
- Employ social media sentiment towards Ponzi schemes detection.
- Ensuring the reliability of the social media sentiment by employing resistance to fake content exploitations.
- Integrate state-of-the-art fusion techniques to combine smart contract data, transaction records, and social media sentiment for a comprehensive Ponzi schemes detection approach.
- Provide explainability insights into the decision-making process of the Ponzi scheme detection model, ensuring transparency and interpretability in its results.

RELATED WORK

RELATED WORK

Related Papers

Ponzi DApp Detection

[1] Weili Chen, Zibin Zheng, Jiahui Cui, Edith Ngai, Peilin Zheng, and Yuren Zhou. 2018. Detecting Ponzi Schemes on Ethereum: Towards Healthier Blockchain Technology. In Proceedings of the 2018 World Wide Web Conference (WWW '18). International World Wide Web Conferences Steering Committee, Republic and Canton of Geneva, CHE, 1409–1418. https://doi.org/10.1145/3178876.3186046

[2] W. Chen, Z. Zheng, E. C. . -H. Ngai, P. Zheng and Y. Zhou, "Exploiting Blockchain Data to Detect Smart Ponzi Schemes on Ethereum," in IEEE Access, vol. 7, pp. 37575-37586, 2019, doi: 10.1109/ACCESS.2019.2905769.

[3] E. Jung, M. Le Tilly, A. Gehani and Y. Ge, "Data Mining-Based Ethereum Fraud Detection," 2019 IEEE International Conference on Blockchain (Blockchain), Atlanta, GA, USA, 2019, pp. 266-273, doi: 10.1109/Blockchain.2019.00042.

[4] Fan, S., Fu, S., Xu, H., & Cheng, X. (2021). Al-SPSD: Anti-leakage smart Ponzi schemes detection in blockchain. Information Processing & Management, 58(4), 102587. https://doi.org/10.1016/j.ipm.2021.102587

[5] Hu, Teng, Xiaolei Liu, Ting Chen, Xiaosong Zhang, Xiaoming Huang, Weina Niu, Jiazhong Lu, Kun Zhou and Yuan Liu. "Transaction-based classification and detection approach for Ethereum smart contract." Inf. Process. Manag. 58 (2021): 102462.

[6] Wang, L., Cheng, H., Zheng, Z., Yang, A., & Zhu, X. (2021). Ponzi scheme detection via oversampling-based Long Short-Term Memory for smart contracts. Knowledge-Based Systems, 228, 107312. https://doi.org/10.1016/j.knosys.2021.107312

[7] Zibin Zheng, Weili Chen, Zhijie Zhong, Zhiguang Chen, and Yutong Lu. 2023. Securing the Ethereum from Smart Ponzi Schemes: Identification Using Static Features. ACM Trans. Softw. Eng. Methodol. 32, 5, Article 130 (September 2023), 28 pages. https://doi.org/10.1145/3571847

Social Media Analysis

Fake Content Detection

[8] "Kaliyar, R.K., Goswami, A., & Narang, P. (2021). FakeBERT: Fake news detection in social media with a BERT-based deep learning approach. Multimedia Tools and Applications, 80, 11765 - 11788.

[9] "S. Ni, J. Li, and H.-Y. Kao, ""MVAN: Multi-View Attention Networks for Fake News Detection on Social Media,"" IEEE Access, vol. 9, pp. 106907-106917, 2021.

[10] "Y.-J. Lu and C.-t. Li, ""GCAN: Graph-aware Co-Attention Networks for Explainable Fake News Detection on Social Media,"" in Annual Meeting of the Association for Computational Linguistics, 2020.

[11] "Truică, C., & Apostol, E.S. (2022). MisRoBÆRTa: Transformers versus Misinformation. ArXiv, abs/2304.07759.

Sentiment Analysis

[12] "Basiri, M.E., Nemati, S., Abdar, M., Cambria, E., & Acharrya, U.R. (2021). ABCDM: An Attention-based Bidirectional CNN-RNN Deep Model for sentiment analysis. Future Gener. Comput. Syst., 115, 279-294."

[13] "Yan, H., Dai, J., Ji, T., Qiu, X., & Zhang, Z. (2021). A Unified Generative Framework for Aspect-based Sentiment Analysis. ArXiv, abs/2106.04300."

[14] "Salur, M.U., & Aydin, I. (2020). A Novel Hybrid Deep Learning Model for Sentiment Classification. IEEE Access, 8, 58080-58093. [Online]. Available: https://doi.org/10.1109/ACCESS.2020.2982538"

Multimodal Fusion

[15] "Shi, T., & Huang, S. (2023). MultiEMO: An Attention-Based Correlation-Aware Multimodal Fusion Framework for Emotion Recognition in Conversations. Annual Meeting of the Association for Computational Linguistics. [Online]. Available: https://doi.org/10.18653/v1%2F2023.acl-long.824"

[16] "Gandhi, A., Adhvaryu, K.U., Poria, S., Cambria, E., & Hussain, A. (2022). Multimodal sentiment analysis: A systematic review of history, datasets, multimodal fusion methods, applications, challenges and future directions. Inf. Fusion, 91, 424-444. [Online]. Available: https://doi.org/10.1016/j.inffus.2022.09.025"

[17] "Chudasama, V.M., Kar, P., Gudmalwar, A.P., Shah, N.J., Wasnik, P.S., & Onoe, N. (2022). M2FNet: Multi-modal Fusion Network for Emotion Recognition in Conversation. 2022 IEEE/CVF Conference on Computer Vision and Pattern Recognition Workshops (CVPRW), 4651-4660. [Online]. Available: https://doi.org/10.1109/CVPRW56347.2022.00511"

Interpretable Machine Learning

[18] M. T. Ribeiro, S. Singh, and C. Guestrin, ""Why Should I Trust You?": Explaining the Predictions of Any Classifier," in Proceedings of the 22nd ACM SIGKDD International Conference on Knowledge Discovery and Data Mining, 2016. [Online]. Available: https://doi.org/10.1145/2939672.2939778

[19] S. M. Lundberg and S.-I. Lee, "A Unified Approach to Interpreting Model Predictions," ArXiv, vol. abs/1705.07874, 2017. [Online]. Available: https://arxiv.org/pdf/1705.07874.pdf

[20] W. Samek, T. Wiegand, and K.-R. Müller, "Explainable Artificial Intelligence: Understanding, Visualizing and Interpreting Deep Learning Models," arXiv:1708.08296 [cs.AI], 2017. [Online]. Available: https://doi.org/10.48550/arXiv.1708.08296.

[21] R. R. Selvaraju, A. Das, R. Vedantam, M. Cogswell, D. Parikh, and D. Batra, "Grad-CAM: Visual Explanations from Deep Networks via Gradient-Based Localization," International Journal of Computer Vision, vol. 128, pp. 336-359, 2016.

1. Ponzi DApp Detection

Securing the Ethereum from Smart Ponzi Schemes: Identification Using Static Feature

- The researchers contribute by creating a new dataset and method to identify Ponzi schemes in the early stages of their creation.
- Feature selection categories
    - Term frequency count of individual opcode words.
    - Count of N-gram sequences of opcodes.
    - Word2vec embeddings of opcodes.
    - Contract's creator has previously created a Ponzi contract.
- They used SVM, Random forest and XGBoost. selected the models with the best performance on the testset for each kind of features

Zibin Zheng, Weili Chen, Zhijie Zhong, Zhiguang Chen, and Yutong Lu. 2023. Securing the Ethereum from Smart Ponzi Schemes: Identification Using Static Features. ACM Trans. Softw. Eng. Methodol. 32, 5, Article 130 (September 2023), 28 pages. https://doi.org/10.1145/3571847

2. Scam DeFi tokens Detection

DEFITRUST: A TRANSFORMER-BASED FRAMEWORK FOR SCAM DEFI TOKEN DETECTION USING EVENT LOGS AND SENTIMENT ANALYSIS

- The paper aims to identify scam DeFi tokens early stage by analyzing their transaction and social media data.
- For each token on that list, the latest 1080 transfer events are extracted and a selected set of features are calculated.
- For each token, the latest 100 reviews and comments are extracted from following subreddits.
- Using transformer based model it Combines the above two result and predict the trustworthiness.
- Ablation Study removes sentimental part and show results (the best results gives the combination of models)

Gunathilaka, M.D.M.D.P. (June 2023). "DEFITRUST: A TRANSFORMER-BASED FRAMEWORK FOR SCAM DEFI TOKEN DETECTION USING EVENT LOGS AND SENTIMENT ANALYSIS." Unpublished paper, University of Moratuwa. Supervised by Dr. Sandareka Wickramanayake (University of Moratuwa) and Dr. Dilum Bandara (Data61, CSIRO).

3. Multimodal Fusion

MultiEMO: An Attention-Based Correlation-Aware Multimodal Fusion Framework for Emotion Recognition in Conversations

- The paper propose a novel attention-based correlation-aware multimodal fusion framework for emotion recognition in conversations by,
    - Capturing cross-modal mapping relationships across textual, audio and visual modalities.
    - And utilizing bidirectional multi-head cross-attention layers
- In order to mitigate the difficulty of classifying minority and semantically similar emotion classes, a Sample-Weighted Focal Contrastive (SWFC) loss is proposed.
- Also employed a Soft Hirschfeld-Gebelein-Rényi (Soft-HGR) loss to maximize the correlations across three modalities.

"Shi, T., & Huang, S. (2023). MultiEMO: An Attention-Based Correlation-Aware Multimodal Fusion Framework for Emotion Recognition in Conversations. Annual Meeting of the Association for Computational Linguistics.

4. Fake Content Detection

FakeBERT: Fake news detection in social media with a BERT-based deep learning approach

- The paper aims to capture semantic and long-distance dependencies in sentences with bidirectional training approach.
- The proposed model consist of,
  - BERT as a sentence encoder embedding layer
  - Five convolution layers
  - Five max-pooling layers
  - Followed by two densely connected layers
- The authors successfully tested the model on a Kaggle fake news dataset, achieving an accuracy rate of 98.90%.

"Kaliyar, R.K., Goswami, A., & Narang, P. (2021). FakeBERT: Fake news detection in social media with a BERT-based deep learning approach. Multimedia Tools and Applications, 80, 11765 - 11788.

5. Interpretable Machine Learning

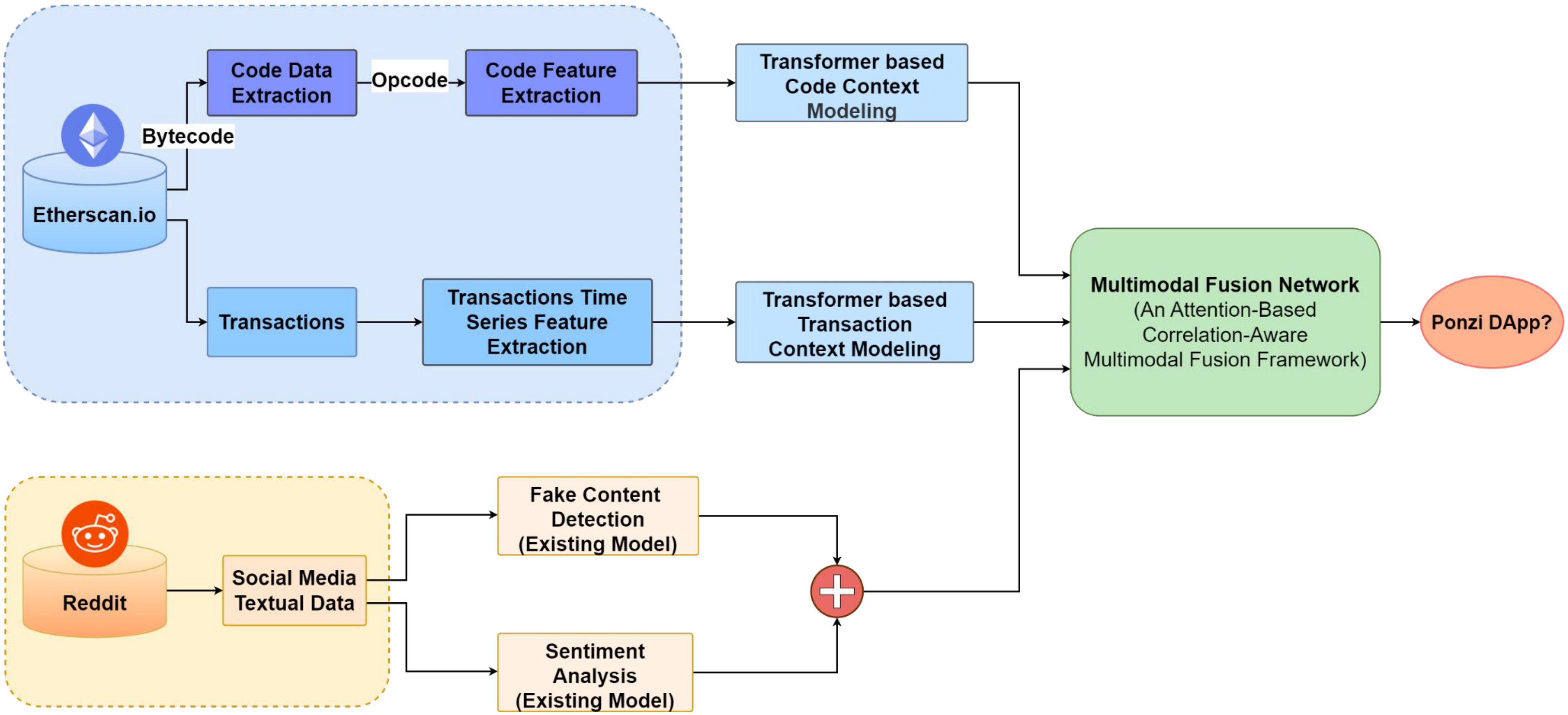
Unified Approach to Interpreting Model Predictions

- A trade-off between model accuracy and interpretability arises in complex models
  - Achieving the highest accuracy often comes at the cost of interpretability
- The authors propose to use Shapley values, as an model-agnostic explanation framework for interpreting complex model predictions.
- The Shapley values are employed as a local explanation technique
  - Approximated using methods such as Shapley sampling values and Kernel SHAP
- The authors define three crucial properties, local accuracy, missingness, and consistency
  - Showing the only additive feature attribution method that satisfies these properties is their method based on Shapley values.

Lundberg, S.M., & Lee, S. (2017). A Unified Approach to Interpreting Model Predictions. ArXiv, abs/1705.07874.

PROPOSED SYSTEM

PROPOSED SYSTEM



LIMITATION & CHALLENGES

Limitations

- No dataset is available for fake news detection in blockchain domain.
- No dataset for sentiment analysis within the blockchain domain.

Challenges

- We incorporate code features, transaction features, and social media sentiment features into our training model. It is a challenge in the creation of a dataset encompassing all 3 modalities for the DApp.
- Possess an unbalanced Ponzi dataset, and as such, we need to employ data balancing techniques.

TIMELINE


TASK TITLE
AUGUST
SEPTEMBER
OCTOBER
NOVEMBER
DECEMBER
JANUARY
FEBRUARY
MARCH
W1 W2 W3 W4
1 Research on related areas
2 Proposal writing and finalized
3 Data Collection and Preparation
4 4.1 Develop Code context model
4.2 Develop Transaction context model
4.3 Develop Social Media Sentiment Analysis model
4.4 Develop multimodal fusion network
4.5 Model Fine-tuning
5 Design and Develop Explainability Framework
6 Evaluation and Comparative Analysis
7 Write the conference paper
Semester 7 exams

CONCLUSION

- Scams, especially Ponzi schemes, in Decentralized Applications (DApps) are a big issue.
- Our research provides a new and effective method to detect these scams in real-time, protecting users from fraud.
- Our solution, PonziShield, examines the codes, analyzes transactions, and monitors social media for suspicious activities, to find Ponzi DApps early.
- PonziShield not only detects scams but also explains why it considers a DApp to be a Ponzi scheme.
- This transparency in our approach builds confidence and trust among users, making DApps a safer environment for everyone.

References

[1] S. Fan, S. Fu, H. Xu, and X. Cheng, "AI-SPSD: Anti-leakage smart Ponzi schemes detection in blockchain," Information Processing & Management, vol. 58, no. 4, pp. 102587, 2021. [Online]. Available: DOI link.

[2] Weili Chen, Zibin Zheng, Jiahui Cui, Edith Ngai, Peilin Zheng, and Yuren Zhou. 2018. Detecting Ponzi Schemes on Ethereum: Towards Healthier Blockchain Technology. In Proceedings of the 2018 World Wide Web Conference (WWW '18). International World Wide Web Conferences Steering Committee, Republic and Canton of Geneva, CHE, 1409–1418. https://doi.org/10.1145/3178876.3186046

[3] W. Chen, Z. Zheng, E. C. . -H. Ngai, P. Zheng and Y. Zhou, "Exploiting Blockchain Data to Detect Smart Ponzi Schemes on Ethereum," in IEEE Access, vol. 7, pp. 37575-37586, 2019, doi: 10.1109/ACCESS.2019.2905769.

[4] Fan, S., Fu, S., Xu, H., & Cheng, X. (2021). Al-SPSD: Anti-leakage smart Ponzi schemes detection in blockchain. Information Processing & Management, 58(4), 102587. https://doi.org/10.1016/j.ipm.2021.102587

[5] Wang, L., Cheng, H., Zheng, Z., Yang, A., & Zhu, X. (2021). Ponzi scheme detection via oversampling-based Long Short-Term Memory for smart contracts. *Knowledge-Based Systems*, *228*, 107312. https://doi.org/10.1016/j.knosys.2021.107312

[6] E. Jung, M. Le Tilly, A. Gehani and Y. Ge, "Data Mining-Based Ethereum Fraud Detection," 2019 IEEE International Conference on Blockchain (Blockchain), Atlanta, GA, USA, 2019, pp. 266-273, doi: 10.1109/Blockchain.2019.00042.

[7] Teng Hu, Xiaolei Liu, Ting Chen, Xiaosong Zhang, Xiaoming Huang, Weina Niu, Jiazhong Lu, Kun Zhou, Yuan Liu, Transaction-based classification and detection approach for Ethereum smart contract, Information Processing & Management, https://doi.org/10.1016/j.ipm.2020.102462.

[8] Zibin Zheng, Weili Chen, Zhijie Zhong, Zhiguang Chen, and Yutong Lu. 2023. Securing the Ethereum from Smart Ponzi Schemes: Identification Using Static Features. ACM Trans. Softw. Eng. Methodol. 32, 5, Article 130 (September 2023), 28 pages. https://doi.org/10.1145/3571847